UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CIÊNCIA DA COMPUTAÇÃO

Larissa Gremelmaier Rosa

Modeling the SIM Swap Ceremony: Integrating Human Behavior and Formal Analysis

Florianópolis
2024

Larissa Gremelmaier Rosa

Modeling the SIM Swap Ceremony: Integrating Human Behavior and Formal Analysis

Trabalho de Conclusão de Curso submetido ao Curso de Graduação em Ciência da Computação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para obtenção do título de Bacharel em Ciência da Computação.
Orientador: Prof. Jean Everson Martina, Dr.
Coorientador: Gustavo Zambonin, M.Sc

Florianópolis
2024

Larissa Gremelmaier Rosa

Modeling the SIM Swap Ceremony: Integrating Human Behavior and Formal Analysis

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo curso de Graduação em Ciência da Computação.

Florianópolis, 10 de Julho de 2024.

Banca Examinadora:

Prof. Jean Everson Martina, Dr.
Orientador
Universidade Federal de Santa Catarina

Prof^a. Thaís Bardini Idalino, Dr^a.
Avaliador
Universidade Federal de Santa Catarina

Prof. Ricardo Felipe Custodio, Dr.
Avaliador
Universidade Federal de Santa Catarina

À minha família, que tanto amo.

ACKNOWLEDGEMENTS

Gostaria de expressar minha profunda gratidão a todos que contribuíram para a realização deste trabalho de conclusão de curso. Primeiramente, agradeço aos meus pais, Gislaine e Paulo, por sempre estarem presentes em minha trajetória acadêmica e por toda a confiança que sempre depositaram em mim. Vocês são minha inspiração para continuar sempre determinada. Agradeço também à minha irmã, Luiza, por ser minha maior confidente.

Aos meus amigos, que sempre me incentivaram e compartilharam momentos importantes dessa jornada, deixo meu sincero agradecimento. Um agradecimento especial a Mariana, que esteve presente para escutar todos os surtos durante esses anos de graduação e virou noites fazendo trabalho junto comigo. Também agradeço a Thália, ao Roberto, ao Felipe e aos Matheus pela companhia nas aulas e por se tornarem amigos que levarei para a vida, mesmo que acabemos por nos distanciar.

Agradeço ao LabSEC pela oportunidade de fazer parte desse grupo incrível, que me proporcionou um ambiente de crescimento profissional e aprendizado contínuo. Em especial, agradeço ao Pablo Montezano pela excelente gerência e por permitir minha entrada no laboratório, e ao Victor por ser meu parceiro durante toda a experiência no laboratório. Agradeço também a toda a equipe do Hawa, vocês são incríveis.

Por fim, sou extremamente grato ao meu orientador, Professor Jean Martina, e ao coorientador, Gustavo Zambonin, pela orientação, paciência e apoio durante todo o desenvolvimento deste trabalho. Suas contribuições foram fundamentais para o meu crescimento acadêmico e profissional. A todos vocês, meu muito obrigado.

All the world’s a stage,
And all the men and women are merely players
(WILLIAM et al., 1901)

RESUMO

Ao abordar o processo de troca de SIM como uma cerimônia de segurança, nosso estudo oferece uma investigação abrangente, com foco na interação entre protocolos técnicos e entidades humanas. Seguindo uma abordagem em camadas para analisar essas cerimônias, conforme proposto na literatura, exploramos a questão considerando as diferentes camadas a serem examinadas, especificamente as camadas de interação humano-computador e pessoal, empregando modelos formais e avaliação empírica. O objetivo dessas ações é percorrer as várias fases e os atores envolvidos nas operações de troca de SIM, traçando um panorama de vulnerabilidades e oportunidades para melhorar a segurança e a experiência do usuário. Ao mesmo tempo, procuramos ampliar o escopo da análise de cerimônias de segurança para abranger aspectos relacionados ao estudo de nós de entidades humanas, empregando o conceito de máscaras pirandellianas na modelagem dessas cerimônias, que já haviam sido definidas teoricamente. Isso possibilitou o desenvolvimento de um modelo formal de troca de SIM que pode ser empregado para formular melhorias nesse processo que aumentam sua segurança em dois níveis de granularidade. Isso implica uma compreensão das etapas envolvidas no processo, os possíveis ataques que poderiam ser lançados e o comportamento de entidades humanas que poderiam levar a erros no processo. Ao modelar as máscaras Pirandellianas, foi demonstrado como elas podem ser uma ferramenta valiosa para analisar cerimônias. Isso foi feito por meio da integração da compreensão teórica das interações humanas e do comportamento esperado com a análise prática e formal dos protocolos de segurança. O resultado foi o desenvolvimento de uma estrutura robusta para mitigar riscos e otimizar a eficácia dos processos de troca de SIM.

Palavras-chave: Cerimônias de Segurança. Troca de SIM. Interação Humano-Tecnologia.

ABSTRACT

Approaching the SIM swap process as a security ceremony, our study offers a comprehensive investigation, focusing on the interaction between technical protocols and human entities. Following a layered approach to analyzing these ceremonies, as proposed in the literature, we explore the issue by considering the different layers, specifically the human-computer and personal interaction layers, employing both formal models and empirical evaluation. These actions aim to go through the multiple phases and actors involved in SIM swap operations, outlining vulnerabilities and opportunities for improving security and the user experience. Concurrently, we sought to extend the scope of security ceremony analysis to encompass aspects of the study of human entity nodes, employing the concept of Pirandellian masks in modeling these ceremonies, which had previously been defined theoretically. As a result, a formal model of SIM swapping was developed, which may be employed to formulate improvements to this process that enhance its security at two levels of granularity. To achieve this, it is necessary to understand the steps involved in the process, the potential attacks that could be launched, and the behavior of human entities that could lead to errors. Furthermore, the modeling of Pirandellian masks demonstrated how they could be valuable for analyzing ceremonies. Integrating a theoretical understanding of human interactions and expected behavior with the practical and formal analysis of security protocols enabled the development of a robust framework for mitigating risks and optimizing the effectiveness of SIM swap processes.

Keywords: SIM swap. Security ceremony. Human-technology interaction

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF SYMBOLS

$\Leftrightarrow$	Biconditional
$\exists$	Existential quantification
$\Rightarrow$	Conditional
$\wedge$	logic AND
$\forall$	Universal quantification

CONTENTS

1 INTRODUCTION

Digital security is a constant concern where the integrity and confidentiality of data are essential for a wide range of organizations. Several mechanisms have been developed to protect sensitive systems. In this sense, *security protocols* are imperative as it is a set of communication procedures designed to achieve a specific goal in an environment where there is a constant threat of interference from an attacker (AVALLE; PIRONTI; SISTO, 2014).

Given the importance of achieving certain security goals, exhaustive studies to assert the correctness of security protocols are necessary, typically performed through mathematical techniques and tools (AVALLE; PIRONTI; SISTO, 2014; BAU; MITCHELL, 2011). This process consists of (i) defining a protocol model, (ii) understanding the properties it must maintain, (iii) modeling the attacker, and then (iv) subjecting it to a verification technique such as automated theorem proving (BAU; MITCHELL, 2011).

Despite the rigor these protocols undergo in the verification stage, they still fail when applied to real use cases (BELLA; CURZON; LENZINI, 2015). Protocols and their models often disregard socio-technical interactions between users and systems, neglecting the human element when designing security results in vulnerabilities that technical solutions alone cannot solve (BELLA; CURZON; LENZINI, 2015). Understanding the psychology and behaviors of users is crucial in developing effective security measures.

In this sense, security ceremonies emerge as a comprehensive approach that goes beyond traditional protocols, incorporating a variety of factors, from operating systems to human interactions (BELLA; COLES-KEMP, 2012). The concept of a security ceremony allows us to perceive the processes of a Mobile Network Operator (MNO) as multiple examples of such ceremonies. The MNO incorporates several elements presented in ceremonies, including the protocols used in Internet networks, users, customer service representatives, and attackers.

Among these processes, the SIM swap case is an interesting example of how security protocols fail when considered within a wider social context. Before explaining precisely how this happens, we must examine how MNOs operate. Wireless service is linked to a mobile device's SIM card, with MNOs managing the association between phone numbers and SIMs. Each phone number is typically tied to one SIM card and vice versa. SIM cards facilitate the BYOD policy, allowing users to bring their own devices if not locked to another carrier, and a new SIM is purchased (LEE et al., 2020). Users can easily switch devices by transferring service to a new SIM card by providing the new SIM's ICCID to the mobile provider and then inserting it into the new device (LEE et al., 2020).

If a user wishes to move their number to another SIM for some reason that makes it impossible to use the old one, they need to perform a SIM swap operation. However, in a social context, this operation is susceptible to attacks from different human nodes, thus failing to ensure that only the user who owns the telephone line succeeds in completing the goal. For example, a malicious actor can use social engineering to trick or bribe a telephone line operator or customer service representative to assume that they own the SIM number and then perform an illegal SIM swap (ANDREWS, 2018).

This scam is commonly referred to as equivalent in the literature as a SIM swap attack, which can potentially damage its targets. As the phone number is constantly used in the two-factor authentication process, an actor in possession of a user's phone number has the power to gain access to service accounts from banks to cryptocurrency wallets, thus causing losses that could reach millions of dollars (ANDREWS, 2018). Crimes like this are becoming increasingly common, especially with the adoption of eSIM in many countries (KIM; SUH; KWON, 2022).

These frauds could be foreseen or mitigated by studying the SIM swap process as a security ceremony. However, developing methodologies to analyze ceremonies, considering the complexity of human interactions, is a challenge. This is illustrated by a study of the HTTPS protocol running in the Opera Mini browser and its users, conducted by Radke et al. (2011). The authors have shown that usage context can lead to the emergence of various user personas, potentially prompting a system to accommodate multiple security ceremonies. As such, several studies are being undertaken to facilitate the analysis of these ceremonies (BELLA; COLES-KEMP, 2012; BASIN; RADOMIROVIC; SCHMID, 2016).

In particular, the *Security Ceremony Concertina* approach is useful as it breaks down the complexity of this analysis by creating layers and interfaces to communicate across them (BELLA; COLES-KEMP, 2012). This method distinguishes a security ceremony into five layers: (L1) Informational; (L2) Operating System; (L3) Human-Computer Interaction; (L4) Personal; (L5) Communal. Following the definitions brought by this method, the most common studies to model the security protocol are in L1 and L2.

According to the authors, the study of L3 and L4 is complex due to the non-deterministic nature of humans. Research into these layers is domain-specific and involves aspects such as the definition of personas and the modeling of human threats (BELLA; CURZON; LENZINI, 2015; BASIN; RADOMIROVIC; SCHMID, 2016). Most recently, Martimiano & Martina (2022) conceptually defined the idea of using *Pirandellian Masks* as a means of analyzing humans in L4.

1.1 OBJECTIVES

1.1.1 General Objectives

Considering the above, the purpose of our study is to formally model the SIM swap process, incorporating layers L3 and L4 of the Concertina Security Ceremony. Hereafter, it is defined as the SIM swap ceremony. The formal modeling of this ceremony at the L1 and L2 layers was not found in the literature. However, we don't present it in our work as the implementation of this protocol differs between mobile network operators (MNOs) and is not public.

We use those models to compare with the attacks obtained in empirical studies and establish a prototype to test changes to this ceremony aiming to improve its security. At the same time, we strive to contribute to research into such ceremonies, applying methods defined for analyzing these layers and identifying approaches to facilitate their integration into real contexts. More specifically, we build initial implementations of the concept of Pirandellian Masks, explained by Martimiano & Martina (2022), in the context of the SIM swap ceremony and thus understand how we can use them to comprehend specific parts of security ceremonies in terms of human entities and their formal modeling and analysis.

1.1.2 Specific Objectives

1. Review the state of the art in the field of security ceremonies;
2. Identify the steps and entities involved in the SIM swap ceremony;
3. Analyze the types of attacks that can occur during the SIM swap process, such as social engineering and identity manipulation;
4. Use formal modeling and analysis techniques, such as threat models and protocol analysis, to describe the behavior of this ceremony in L3 and L4 of the *security ceremony concertina*;
5. Propose mitigation measures to strengthen the security of the SIM swap ceremony based on the analyses carried out;
6. Identify challenges and successes in modeling and analyzing these layers.

1.2 METHODOLOGY

Our study begins with a bibliographical survey of security ceremonies, including their definition, motivation, and recent studies. At the same time, bibliographical and documentary research is carried out to understand how SIM swap operates from a point of view involving system nodes and human entities, as well as attacks and their consequences. With this research compiled, we build formal models of the exchange of knowledge and interactions between parties, using tools such as Tamarin to verify this correspondence and allow a framework for further studies to be created.

Within the scope of ceremony modeling, we introduce the concept of Pirandellian masks, brought up by Martimiano & Martina (2022). In doing so, we aim to gather evidence on how to implement them efficiently in a formal tool while at the same time providing new data on their use beyond what was mentioned by the original authors, bearing in mind that they have meta-design potential that also involves creating stories within the formalization of ceremony that allow us to understand real-life usage scenarios with a certain similarity. We initially compare the results obtained in the bibliographical and documentary research with the modeled results to validate our modeling.

1.3 PROJECT STRUCTURE

Chapter 2 presents the basic concepts for understanding the investigation developed here, which involves the study of methods for the formal analysis of protocols, theorem provers, and model checkers, as well as concepts involving security ceremonies. This chapter provides a brief literature review to frame our work regarding the state of the art. In Chapter 3, we look at research into SIM swap, their initial modeling considering layer three of the security ceremony concertina, and the results obtained. In Chapter 4, we articulate Pirandellian masks, their implementation in the case of SIM swap, and the results of this modeling stage. In Chapter 5, we discuss the insights from this two-stage effort to understand the SIM swap ceremony, indicating viable future work and improvements.

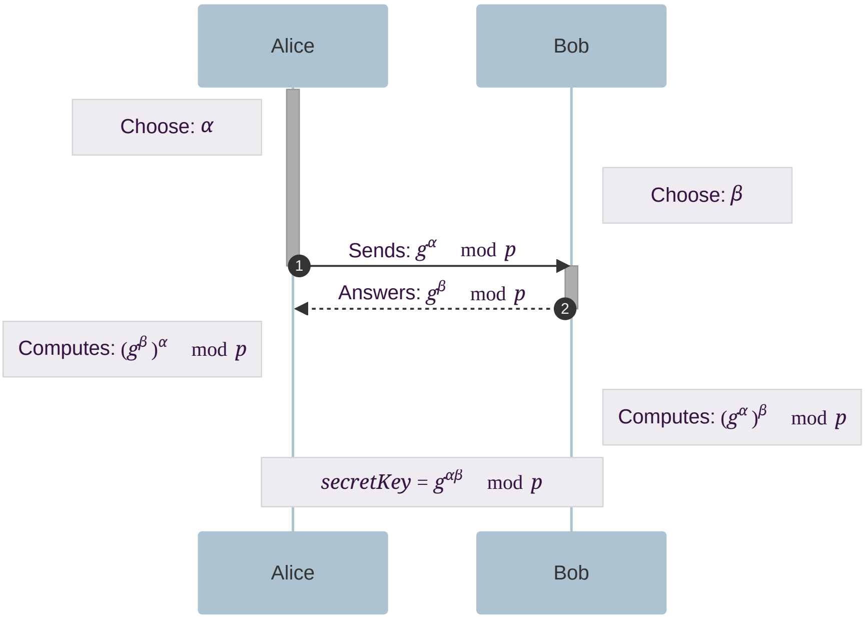
2 THEORETICAL BACKGROUND

In this section, we explain security protocols and describe the process of modeling and formally analyzing them. This serves as a basis for understanding security ceremonies since they complement the original idea of protocols and use many of the bases defined previously for their analysis. Finally, we have undertaken a comparative study of related work to understand the current state of research in the field and identify strategies for our project.

2.1 PROTOCOL MODELLING AND ANALYSIS

Security protocols are designed to allow different actors to communicate securely over an insecure network, thus retaining several properties such as secrecy (messages will only be read by the target actor), authenticity (if a message appears to be sent by an actor, then that actor sent the message), among others (PAULSON, 1998). A classic protocol is the key exchange protocol. It allows two actors, normally called Alice and Bob, to establish a shared secret key that can be used to encrypt and decrypt their messages, ensuring confidentiality and integrity during the transmission of data (SCHMIDT, 2012).

Figure 1 – Diffie-Hellman Key Exchange Example


Alice
Bob
Choose: α
Choose: β
1
Sends: $g^{\alpha} \mod p$
Answers: $g^{\beta} \mod p$
2
Computes: $(g^{\beta})^{\alpha} \mod p$
Computes: $(g^{\alpha})^{\beta} \mod p$
$secretKey = g^{\alpha\beta} \mod p$
Alice
Bob

Source: The author based in (DIFFIE; HELLMAN, 2022)

As we see in Figure 1, a security protocol has actors in different roles; in this case, Alice acts as the initiator of the protocol and Bob as the responder. Also, depending on the role, the protocol will have a set of actions ranging from sending messages to calculating the result of an equation. To illustrate, we see the action of an Alice actor sending a message containing

$g^a \mod p$ to Bob. Bob, in turn, will send $g^b \mod p$, in which both actors must compose the received and sent data to get $secretKey$.

Transitioning from the visualization of the protocol to its security assessment highlights the complexity of this task. We need to divide the initial question "Is this system secure?" into several others that gauge a subset of the properties of the system, such as whether the communication between two parties on the network can resist a Dolev-Yao attacker, a specific attacker model we explain later in our work, and keep the secrecy property (BAU; MITCHELL, 2011). This decomposition of the evaluation process leads to a better-targeted analysis of the individual security aspects, thus providing information on the overall robustness of the protocol against various attack scenarios.

Mödersheim (2018) explains that this process starts from the assumption that a protocol model is present, along with a set of properties to be proven and a model of the attacker, showing the actions he can carry out within the model. According to the author, to define the protocol model with its actions and operations, we need to answer two questions: what do we want to prove, and how do we want to prove it? Once this has been answered, we obtain a set of protocol expressions that can be used within an analysis method, which adheres to a specific way of writing a protocol in formal language.

After addressing "What do we want to prove?" it becomes imperative to define a series of essential elements. This includes identifying the means of communication, the messages exchanged, the participating actors, the occasions when each actor is authorized to send or receive a message, and the constants that identify these actors and messages. As explained by Mödersheim (2018), it is also necessary to establish the basic axioms of the protocol - the assumptions made at the start of its execution - the operations performed, and the underlying equational structure. Designing and mapping this data is an intricate task that requires specialized knowledge and a significant investment of time for the professionals involved in the field.

To illustrate this, let us return to the example of the Diffie-Hellman key exchange (DIFFIE; HELLMAN, 2022). By looking for the elements previously listed, we identified two key players in the protocol: Alice and Bob. In addition, it is essential to have prior knowledge of the constants g and p, which are used to perform the calculations during the key exchange process. It is also imperative to understand the order of operations involved in calculating the $\mathsf{SecretKey}$ and the data needed to calculate this equation, including the public values exchanged between the participants. As the overall complexity of the protocols increases, this mapping becomes more challenging to perform.

Now, we answer "how are we going to analyze this protocol?". One can use pure mathematical methods or computer-aided methods. In the latter case, a language such as F* (ZINZINDOHOUÉ et al., 2017), Isabelle/HOL (PAULSON; WENZEL, 2013) or the one embedded in the Tamarin Prover (MEIER et al., 2013) is defined. Each translates the data that permeates the protocol differently to suit their proof frameworks. Once the model is written in a formal language, we choose which properties we want to ensure it maintains. According to Hollick et al. (2017) and Bau & Mitchell (2011), typical examples of properties are:

Property 1 (Authenticity)**.** Assurance that a message or communication originated from a genuine source.

Property 2 (Integrity)**.** Information will not be modified or corrupted accidentally or deliberately by unauthorized parties.

Property 3 (Confidentiality)**.** Sensitive information will be protected against unauthorized access.

When analyzing a protocol, we choose and code a subset of possible properties using a formal language. These properties are adapted to fit within the operations and states of the target protocol. They will be held against the model of an attacker, where it will be ascertained whether the chosen properties can be broken by this attacker (RAM; ODELU, 2022). Therefore, a precise definition of the threats the system must resist is essential to assess the security of a system. This implies drawing up a threat model that identifies the adverse scenarios that could compromise that security, given that a property may or may not be upheld depending on the model adhered to.

A classical threat model in this area is the Dolev-Yao (DOLEV; YAO, 1983). The Dolev-Yao threat model considers two types of actors: honest actors, who follow the protocol, and the adversary. It is assumed that the network is completely under the control of the adversary, who can record, delete, reproduce, forward, reorder, and completely control the programming of messages, so every message sent or received by the network passes through the adversary (HERZOG, 2005). There are also restrictions on which messages can be derived from others by the adversary, such as the inability to perform cryptanalysis.

Other models documented in the literature are the Rational Attacker and the General Attacker. In the former, each participant can choose to behave according to or against the protocol depending on the benefit that each action brings (ARSAC et al., 2009). Similarly, the latter considers each participant a Dolev-Yao so they can send true or false messages to any other Dolev-Yao in the network at any time. These messages can be produced following the protocol or forged, which brings the possibility of retaliatory or preemptive attacks (ARSAC et al., 2009).

2.2 PROOF METHODS

Having defined the models and properties, we need to verify whether they hold. This requires analysts to use mathematical proofs, usually with the help of automated computational methods, to ensure all protocol details are covered. Using solely mathematics, we can describe and analyze the protocol using Epistemic Logic by modeling the protocol in terms of knowledge (MEYER; MEYER; HOEK, 2004). We often find two main categories of computational auxiliary methods in the literature: model checkers and automated theorem provers (BAU; MITCHELL, 2011). This brings us back to the question of “How are we going to analyze the protocol?” since defining a language for transcribing aspects of the protocol results in choosing a type of proof.

2.2.1 Epistemic Logic

As previously discussed, security protocols perform operations on information distributed over a network. We underlined the necessity of modeling information and its movement within the network. Among the formalisms that enable such modeling, a specific type of logic enables representing information and its subsequent reasoning, known as epistemic logic: the logic of knowledge (DAVIS; MORGENSTERN, 1983).

Meyer, Meyer & Hoek (2004) discuss how we can use epistemic logic operators to specify protocols compactly and exactly, which can then be transposed to codes and other types of formal verification. Specifically, the authors comment on its use in the specification and verification of security protocols, as it helps to formalize and analyze how knowledge is distributed between different participants in a protocol and how this affects the overall security of the system. According to Meyer, Meyer & Hoek (2004), epistemic logic is concerned with modeling and studying knowledge and beliefs.

Rendsvig, Symons & Wang (2019) comment that although any logic seen from an interpretation involving knowledge and beliefs can be called epistemic logic, modal logic is usually used. Modal logic extends propositional logic that analyzes modalities such as possibility and necessity (GOLDBLATT, 1974). Modal logic goes beyond the epistemic model because it is based on the existence of modals, which are operators that qualify the truth of a sentence.

Thus, as described by Fitting & Mendelsohn (2023), it encompasses temporal (operators related to the passage of time) aspects, such as the modals *will be* and *was*, deontic (operators related to obligation and duty) aspects such as *may* and *can* and epistemic (operators related to knowledge and belief) aspects such as *certainly* and *probably*. According to the authors, at least two modal operators are usually chosen to set up a modal logic. For example, Rendsvig, Symons & Wang (2019) choose the modal operators K and B, thus defining formulas of the type $\mathsf{K}_a\phi$ and $\mathsf{B}_a\phi$ to write that "agent a knows ϕ" and "agent a believes that ϕ".

Different modal epistemic systems encompass characteristics of knowledge and have basic axioms that describe their logic. Suppose a system that has the modal operator K, Davis & Morgenstern (1983) and Rendsvig, Symons & Wang (2019) demonstrates the existence of these five possible properties: veridicality, knowledge of the axioms, consequential closure, positive introspection, and negative introspection. The definition of these properties can be seen in Definitions 2.2.1 to 2.2.5.

Definition 2.2.1 (Veridicality)**.** $\mathsf{K}(\phi) \Rightarrow \phi$ or if one knows about ϕ it implies that ϕ is true.

Definition 2.2.2 (Knowledge of the axioms)**.** If ϕ is a logical axiom, a proposition or formula that is assumed to be true without the need for proof, then $\mathsf{K}(\phi)$ is an axiom.

Definition 2.2.3 (Consequencial closure)**.** $[\mathsf{K}(\phi) \wedge \mathsf{K}(\phi \Rightarrow \psi)] \Rightarrow \mathsf{K}(\psi)$.

Definition 2.2.4 (Positive Introspection)**.** $\mathsf{K}(\phi) \Rightarrow \mathsf{K}(\mathsf{K}(\phi))$.

Definition 2.2.5 (Negative Introspection). $\neg\mathsf{K}(\phi) \Rightarrow \mathsf{K}(\neg\mathsf{K}(\phi))$.

Modal epistemic logic systems that assume all five properties are called $\mathsf{S5}$ systems. We can set up systems that use the properties 2.2.1 to 2.2.4, which are called $\mathsf{S4}$. Other systems involve these or other basic properties and define knowledge systems with different goals and assumptions in modal logic. Adding semantics and understanding to these systems means applying theories such as *possible worlds*. As presented by Rendsvig, Symons & Wang (2019), a *possible world* is a complete and consistent state of reality. It can be seen as a way of describing how the world could be rather than how it necessarily is. Each possible world includes a complete specification of all the facts that are true in that world.

We may also add operators and modal structures to known logic, such as first-order logic. First Order Modal Logic is the logic that makes it possible to write, in mathematical language, associations about objects, their properties, and their relations, with the aid of modal operators such as the K and systems as the $\mathsf{S4}$. As we aim to visualize the passage of knowledge between our agents, we use the epistemic modal operator of knowledge, K. We follow the definitions provided by Davis & Morgenstern (1983) that defined a First Order Modal Logic as a predicate calculus in which sentences can be written using terms, formulas, and predicates. Using the work mentioned before as a basis, we can define the necessary parts of this logic as follows:

Definition 2.2.6 (Term). A term is defined as a constant such as 10 and no, a variable that is an undefined entity and written in as S and K or a function that maps many entities to another entity such as $\mathsf{div}(10,5)$ which maps 10 and 5 to the entity 2.

Definition 2.2.7 (Function). A function is the mapping relation of an arbitrary number of entities to another. For example, $f : I\!R \times I\!R \to I\!R \;\; div(x,y)$ is a function that maps two real number entities to another through the $div(x,y)$ function.

Definition 2.2.8 (Predicate). A predicate represents a property or a relation between entities. It can have one or more arguments and is similar to a function. For example, we take the predicate $\mathsf{is\_two}(\mathsf{div}(10,5))$ that holds if the entity passed as argument is entity 2, false otherwise. Predicates assert the truth of a sentence. One can only identify the truth value once a variable is set with a value.

Definition 2.2.9 (Formula). A formula is defined as:

(i) a predicate applied to terms, called an atomic formula; or

(ii) the application of Boolean operators such as $\wedge$ and $\neg$ to a formula; or

(iii) a quantifier followed by a variable and a formula containing that variable, as $\forall y \; \mathsf{true}(y)$.

Definition 2.2.10 (Sentence). A sentence is a formula in which every variable is attached to a quantifier; no free variables exist.

Considering these definitions, the author explains that a term is a particular entity. Considering the model of knowledge, the author also adds the $\mathsf{K}_a\phi$ operator. However, the grammar adopted for writing this operator is $\mathsf{know}(\mu,\phi)$, which expresses the knowledge of a term by symbolizing an actor μ over a formula ϕ. He extends the concept of the $\mathsf{know}(\mu,\phi)$ operator to add another term, T, that represents the period where the knowledge was learned and leads to the definition of $\mathsf{know}(\mu,T,\phi)$.

To represent the use of this logic to model knowledge transfer, the author defines a network written as a tree of free elements with undirected links. The aim of the problem that Davis & Morgenstern (1983) describes is to transform this network into a rooted tree, considering that the elements of this network know which of their neighbors has been chosen as their parent node and that each node U knows that if a node V is its neighbor, either U is the parent of V or the opposite is true. Furthermore, if U is the root, then it has no parent node, and U knows that if it is not the root, it must have a parent node.

Using First Order Modal Logic as defined here, it is possible to model this problem using Equations 2.1 to 2.8. Equation 2.1 models that for every node U and V and a time T, U knows whether V is its neighbor or not. Equation 2.2 concerns the knowledge of a new U about the symmetry of the relation defined by $\mathsf{neighbor}$ and so on. The function $\mathsf{message}$ models the information passed from a node U to a node V in time T about the father relation U knows about. The interpretation of these equations is based both on the modal properties described above and on first-order predicate logic; we may use *possible world* theory to understand properties of knowledge in the modeled network.

$$\forall U,V,T\ \mathsf{Know}(U,T,\mathsf{neighbor}(U,V)) \vee \mathsf{Know}(U,T,\neg\mathsf{neighbor}(U,V)) \tag{2.1}$$

$$\forall U,T\ \mathsf{Know}(U,T,\forall V \mathsf{neighbor}(U,V) \Leftrightarrow \mathsf{neighbor}(V,U)) \tag{2.2}$$

$$\forall U,T\ \mathsf{Know}(U,T,[\mathsf{root}(U) \Leftrightarrow \forall V\ \mathsf{neighbor}(U,V) \Rightarrow \mathsf{father}(U,V)]) \tag{2.3}$$

$$\forall U,T\ \mathsf{Know}(U,T,\forall V,W[\mathsf{father}(V,U) \wedge \mathsf{father}(W,U)] \Rightarrow W=V]) \tag{2.4}$$

$$\forall U,T\ \mathsf{Know}(U,T,\forall V\ \mathsf{neighbor}(V,U) \Rightarrow [\mathsf{father}(U,V) \Leftrightarrow \neg\mathsf{father}(V,U)]) \tag{2.5}$$

$$\forall U,V,T\ \mathsf{Know}(U,T,\mathsf{father}(U,V)) \Rightarrow \mathsf{message}(U,V,T,\mathsf{father}(U,V)) \tag{2.6}$$

$$\forall U,V,T\ \mathsf{Know}(U,T,\mathsf{father}(V,U)) \Rightarrow \mathsf{message}(U,V,T,\mathsf{father}(V,U)) \tag{2.7}$$

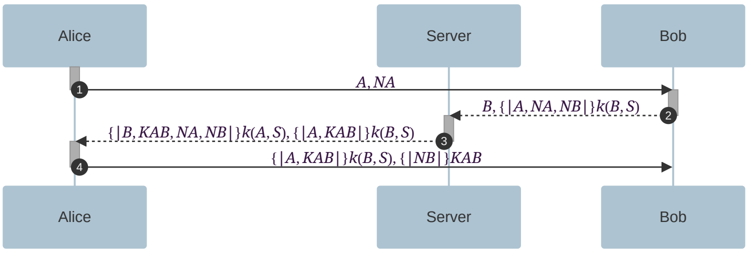
$$\forall U,V,T,X,Y\ \mathsf{message}(U,V,T,\mathsf{father}(X,Y) \Rightarrow \mathsf{Know}(V,T+1,\mathsf{father}(X,Y))) \tag{2.8}$$

Modeling and analyzing a security protocol is similar to the one shown here. In this manner, entities, message transmission, and calculation rules are defined based on the knowledge of a protocol. However, it is necessary to consider and document all the factors involved in the protocol, the attacker's capabilities, and other pertinent details in logical-mathematical language. The modeling of this entire framework tends to increase in complexity and be susceptible to errors on the part of the protocol modeler when the proof of properties is done using pure mathematics. This type of error is less likely to occur in analyses that use computational aids, where the greatest difficulty lies in the model specification, as shown below.

2.2.2 Model Checkers

Model Checkers use the modeling of a protocol as a finite and symbolic state system. In this way, it is possible to prove that the properties hold by showing that there is no sequence of potential actions by an attacker that leads to an insecure state (BAU; MITCHELL, 2011). To illustrate this methodology, we will present the OFMC model checker. As explained in Basin, Mödersheim & Vigano (2005), OFMC uses two formal languages to generate proofs based on protocols: HLPSL and IF. The former is a high-level language that allows protocols to be specified using the Alice-Bob notation. At the same time, the latter is a low-level language that will be transformed into a finite system by the OFMC engine.

Figure 2 – Yahalom Example


Alice
Server
Bob
A, NA
1
$B, \{|A, NA, NB|\}k(B,S)$
2
$\{|B, KAB, NA, NB|\}k(A,S), \{|A, KAB|\}k(B,S)$
3
$\{|A, KAB|\}k(B,S), \{|NB|\}KAB$
4
Alice
Server
Bob

Source: The author based in (PAULSON, 2000)

Let us now consider the Yahalom protocol (PAULSON, 2000), a security protocol designed for key distribution between two agents, typically referred to as A and B, with the assistance of a trusted server referred to as S. The protocol aims to securely distribute a session key KAB between the two agents for secure communications and is used as an example of how OFMC works. Figure 2 introduces the steps in executing the given protocol. In this, A and B are ids for representing Alice and Bob, NA and NB are nonces generated by Alice and Bob, and k(x, y) is the function for calculating a given shared key. In this sense, $k(A,S)$ is a symmetric key known only to Alice and the Server, $k(B,S)$ is a symmetric key known only to Bob and the Server and similar to other equations in Figure 2. Also, the representation $\{\}k(x,y)$ indicates that everything between $\{\}$ is encrypted under $k(x,y)$ key. We use $||||$ under $\{\}$ to differ the set of information being encrypted. We can model this protocol using the HLPSL language defined in Algorithm 1.

Algorithm 1 – HLPSL Yahalom Model

```
1   Protocol Yahalom;
2       Identifiers
3           A, B, S: role; k: function;
4           KAB: symmetric_key; NA, NB: nonce;
5       Knowledge
6           A: B, S, k(A, S);
7           B: A, S, k(B, S);
8           S: A, B, k;
9       Messages
10          1. A -> B: A, NA
11          2. B -> S: B, {|A, NA, NB|}k(B, S)
12          3. S -> A: {|B, KAB, NA, NB|}k(A,S), {|A, KAB|}k(B, S)
13          4. A -> B: {|A, KAB|}k(B, S), {|NB|}KAB
14      Session_instances
15          [A:a, B:b, S:s]
16          [A:i, B:b, S:s];
17      Intruder_knowledge A, B, S; Goal B authenticates S on KAB;
```

Source: (BASIN; MÖDERSHEIM; VIGANO, 2005)

The outlined code in Algorithm 1 shows the declaration of the actors (A, B, and S), their knowledge of each of the system's data, any messages exchanged, and the attacker's knowledge. Session instances declares who will play each role, with i, in line 16 of the Algorithm 1, being the value used to define an attacker impersonating a role. In the case of the Basin, Mödersheim & Vigano (2005) example, the intruder impersonates A defined in line 16 as $A : i$.

After receiving the HLPSL protocol description, OFMC translates the specification into IF. The IF engine analyzes the OFMC code and is the basis for creating the finite state system. For example, the code results in the set of initial states in IF language as shown in Algorithm 2. By passing messages as the transition rules, the protocol will go from one state to another until it reaches the finite state system's end states.

Algorithm 2 – IF initial state for the Yahalom protocol

```
    state(roleA,step0,sess1,a,b,s,k(a,s)).
    state(roleB,step0,sess1,a,b,s,k(b,s)).
    state(roleS,step0,sess1,a,b,s,k).
    state(roleB,step0,sess2,i,b,s,k(b,s)).
    state(roleS,step0,sess2,i,b,s,k).
    i_knows(a).i_knows(b).i_knows(s).
    i_knows(i).i_knows(k(i,s))
```

Source: (BASIN; MÖDERSHEIM; VIGANO, 2005)

For analyzing the attacker, OFMC employs the lazy intruder technique, which symbolically represents the intruder's actions and constraints in a demand-driven manner (BASIN; MÖDERSHEIM; VIGANO, 2005). The properties will be checked using state exploration to systematically analyze the protocol's behavior and interactions between entities. There are various implementations of model checkers, and their approach may vary from the one exemplified

Algorithm 3 – Tamarin Diffie-Hellman Example

```
builtins: diffie-hellman
functions: mac/2, g/0, shk/0 [private]

rule Step1:
    [ Fr(tid:fresh), Fr(x:fresh) ]
    -->
    [
        Out(<g^(x:fresh),
        mac(shk, <g^(x:fresh), A:pub, B:pub>)>),
        Step1(tid:fresh, A:pub, B:pub, x:fresh)
    ]

rule Step2:
    [
        Step1(tid, A, B, x:fresh),
        In(<Y, mac(shk, <Y, B, A>)>)
    ]
    - [ Accept(tid, Y^(x:fresh)) ] -> []

rule RevealKey:
    [] -[ Reveal() ]-> [ Out(shk) ]

lemma Accept_Secret:
    "All i j tid key. Accept(tid,key)@i & K(key)@j
    "=> Ex. l. Reveal() @ l & l < i"
```

Source: (MEIER et al., 2013)

in this work. However, common problems with this approach include false positives/negatives (identifying an attack when there is not one), scalability when the protocol has many states, and the computing power needed to run complex experiments (BAU; MITCHELL, 2011).

2.2.3 Theorem Provers

Meanwhile, an automatic theorem prover is designed to automatically prove mathematical theorems or logical statements with little or no human intervention (PAULSON, 1998). These tools use algorithms and logical reasoning to analyze formal mathematical expressions, logical formulas, or axioms and derive valid conclusions or proofs based on predefined inference rules. We use the Tamarin Prover (MEIER et al., 2013) to show an example of such a program.

A code in Tamarin is called a theory. It consists of three parts: (i) signature, which includes functions, equations, and builtins, which are previous equational systems that can be imported and used; (ii) specification of the protocol and its (iii) properties (KOZMAI, 2016). The protocol specification occurs in the form of multiset rewriting rules, the specification of properties in a guarded fragment of first-order logic, and the signature, with function, equations, and builtins, specifies an equational theory model (MEIER et al., 2013). For the attacker, it has a built-in Dolev-Yao model, which can be modified if necessary.

Protocol modeling in Tamarin works as follows. Defining the equational theory that will be applied in the model is essential. In the example of Algorithm 3, the system of equations known as Diffie-Hellman is used, which is supported by default in the program and incorporates the exponentiation rules needed to generate the SecretKey, as illustrated in Figure 1. In addition, some functions are declared, such as mac(x, y), which accepts two parameters, and shk(), which is private, i.e., it cannot be computed directly by the attacker, and models the SecretKey.

Next, the rules of the protocol are outlined. For this purpose, it is important to recognize that the multiset rewriting system used in Tamarin's works is based on the existence of a universe of facts. Facts are made up of terms and can have the property of being persistent, where they start with !, or linear. A term can be a variable, a function applied to a term, or a constant function within the declared functions and constructs. When a fact is said to be persistent, it can always be consumed as rule input; linear facts are consumed only once and then removed from the multiset. The rules use these facts, comprising input facts, execution traces, and output facts. As an example, let us examine rule Step 1, it receives Fr(tid:fresh) and Fr(x:fresh) as input, it has no trace of execution and outputs facts such Step1(tid:fresh, A:pub, B:pub, x:fresh). Note that we do not use persistent facts in this example. A rule can be triggered without the need for an input fact or finish without generating output facts; we denote this using [ ].

There are also special facts; these are In and Out. These facts are used to transmit messages to the network containing a Dolev-yao attacker, where In stands for input and can only be used on the left side of a rule, Out defines an output and must always be used on the right side of a rule. Another important fact is the Fr as it initializes variables of type fresh, i.e., arbitrary variables whose property is that they will not be repeated between their instances in a Tamarin run. In addition to being defined from their name and being of type fresh, variables can also be public in that they start with $.

Finally, it is necessary to declare lemmas. These lemmas use execution traces to define properties and are declared using first-order logic. The program will execute the rules and run the given protocol to prove the properties, considering that a rule is only executed when all the input facts are present in the system. Rules consume and generate new facts, creating execution traces, which will be used to verify that the defined properties are maintained. Thus, if the automated proof search terminates, it will result in proof that a property is upheld.

While Model Checkers and automatic theorem provers serve similar purposes, each has its own set of limitations. For instance, certain properties may be undecidable, leading to potential incompleteness in the proof process (MEIER et al., 2013). However, whereas Model Checkers may struggle to conclusively demonstrate the absence of successful attacks, automatic theorem provers excel in identifying all possible execution traces (BAU; MITCHELL, 2011).

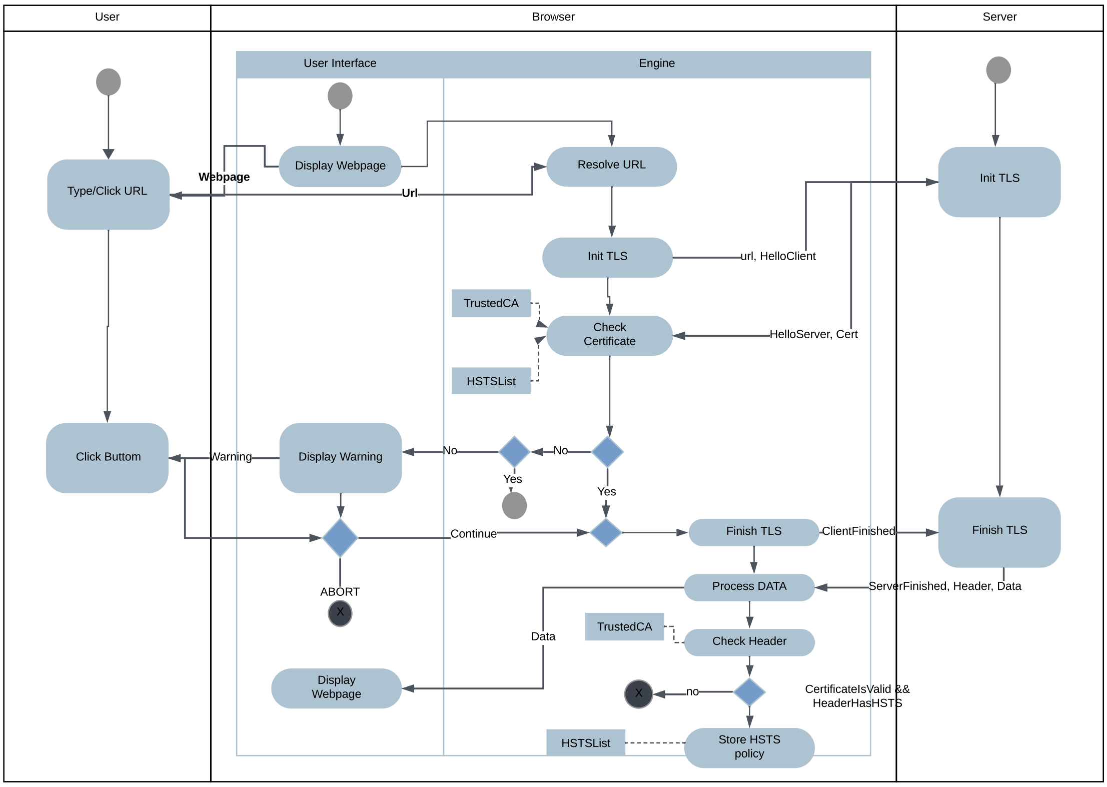
2.3 SECURITY CEREMONIES

Despite all the mathematical formalism applied to the analysis of security protocols, they still fail when implemented in the real world. Radke et al. (2011) has ascribed these failures to a philosophical deficiency in the proof models, whereby complex factors such as social engineering and interfaces between protocols and operating systems are overlooked. Considering these aspects, the concept of a security ceremony is introduced by Ellison (2007).

According to Ellison (2007), a ceremony can be defined as a superset of network protocols, encompassing communication between human-human and human-computer channels, aspects such as user interface, and the exchange of physical objects that carry data. A secure ceremony maintains the properties of its protocols against classic attackers such as Dolev-Yao but also protects against attacks involving social and physical interactions surrounding it.

Consider the research by Bella, Giustolisi & Lenzini (2013). The authors discuss the implementation of TLS in browsers as a social-technological problem in which elements such as the network, the server, the user, the possible attacker, and the browser are seen as parts of a security ceremony. By looking at the given ceremony, described in Figure 3 using UML diagrams, and the protocols in Figure 1 and 2, we notice how the complexity of the security problem increases considerably when we look at the issue from the social-technical perspective.

Figure 3 – TLS Activity Diagram in Chrome



Source: The author based in (BELLA; GIUSTOLISI; LENZINI, 2013)

In addition to the inherent complexity of defining the ceremony model, it is also necessary to consider the properties and attackers from a novel perspective. This implies that fundamental properties such as authenticity and secrecy, as well as those on the social context surrounding the protocol, are subjected to rigorous examination. In the TLS ceremony example, Bella, Giustolisi & Lenzini (2013) introduced new properties as the one below:

Property 4 (Alert when invalid certificate)**.** A user whose browser receives an invalid certificate on a TLS session is warned about this by the browser before the browser completes the session.

It is clear how these properties demand a more extensive and intricate model to be demonstrated, given that they are not grounded upon axiomatic concepts of a protocol, as is common with the properties usually discussed. In the security ceremony example, it is necessary to model not only the operations defined in Figure 3, which cover TLS validation in a browser (such as Chrome), but also the models of honest servers, users, and possible attackers.

Another example of a ceremony is documented in the thesis written by Zacharias (2016), in which we are introduced to the DEMOS-A and DEMOS-2 electronic voting systems. By modeling electronic voting systems as ceremonies, the thesis investigates the impact of human behavior on the system's security. The analysis considers factors such as the audit rate carried out by voters, the privacy implications for administrators auditing public key uploads, and privacy's role in ensuring the voting process's integrity. Analogous to the process of model checkers in protocols, the human entity nodes in the model are separated from the computer nodes and are formalized as finite-state machines with limited power.

More recently, Hatunic-Webster (2019) has used the concept of security ceremonies to create more secure authentication methods against phishing. Phishing is a well-known scam in which attackers try to steal a user's credentials, usually username and password, by adding a fake login page to a trusted web system. They then use the stolen information to gain access to the system. In this sense, Hatunic-Webster (2019) presents the Human Factors in Anti-Phishing Authentication Ceremonies (HF-APAC) Framework.

Looking at the given examples, it becomes clear that we are in direct contact with these ceremonies in the most diverse areas of the digital world. Despite its importance, the field of security ceremonies is still new and has several open issues, mainly related to the addition of human nodes (RADKE et al., 2011). Among these issues, Radke et al. (2011) cites the quest to integrate aspects related to security ceremonies into formal modeling and analysis of protocols. In this sense, efforts are being made to improve the design of security protocols by considering the interaction with human entities, aiming to create more robust and secure systems for all.

Handling human entities in these analyses is a complex problem. People can be influenced by various factors, such as cultural values, and behave differently depending on their context (BELLA; GIUSTOLISI; SCHÜRMANN, 2022). They may be hasty, curious, cautious, and act to the detriment of any of these feelings at different times during a ceremony. Furthermore, by considering humans as an integral part of a model, we open up a new set of possible interactions, such as human-device, human-to-human attacks, and all usability issues.

Recognizing the need to study human behavior to create more robust ceremonies and the difficulty of tackling this problem, several studies have been undertaken to advance the state-of-the-art in modeling human entities. With this in mind, Karlof, Tygar & Wagner (2009) created the concept of conditioned-safe ceremonies. According to the authors, such ceremonies include operations that deliberately condition users to be reflexive, thus protecting themselves from possible attacks. They use the concept of forcing functions, defense in depth, and the use of human tendencies such as rule-based decision-making.

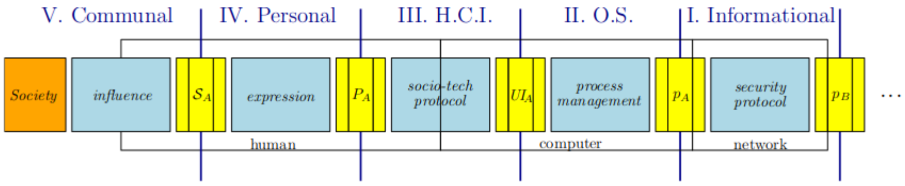
Sempreboni & Viganò (2020) uses Tamarin to study user-generated errors as mutations of the basic ceremony those users should follow. The authors create mutations that involve skipping operations, swapping messages, and adding operations that ultimately affect other agents in the ceremony, creating a complex system for modeling human error. They propose a new tool, X-Men, that inputs a model of the security ceremony in a specific format and executes a Python script to split the model into channel rules, agent rules, and other rules and goals. The security analyst using X-Men can select desired mutations to apply to the agent and different rules. These mutated rules are then merged with the original channel rules and goals to produce various mutated models that can be input to Tamarin for further analysis.

Other efforts along these lines aim to understand the threats that human entities bring to the system indirectly, for example, by interacting with other humans. Bella, Giustolisi & Schürmann (2022) defined a distributed and interacting model of human threats, first in epistemic model logic, and then applied it using Tamarin. In their model, humans can be chatty, cocky, and forgeries, with each of these types of humans being able to perform different actions in the system and between different human entities. Once their scheme was ready, they tested it by modeling the DRS (Deposit-Return Systems) operating in Denmark. They discovered that some important properties of the overall system security are not maintained when human-to-human communication channels involve physical objects and information are exchanged over a network.

2.3.1 Security Ceremony Concertina

Each work discussed covers a small part of what constitutes a security ceremony. The fact that this concept potentially encompasses everything outside the normal protocols brings complexity to the structuring of ceremonies and all the possible threats and models that can be applied to them. Considering those as mentioned earlier, Bella & Coles-Kemp (2012) created the concept of the *Security Ceremony Concertina*. The authors propose that a security ceremony can be conceptualized as a concertina, comprising multiple layers and intersections between them. This structure can be collapsed when studies are proposed from a particular perspective. This approach facilitates identifying interactions between users and technology by generating a model traversing a ceremony's technical and social layers.

Figure 4 – Security Ceremony Concertina Model



Source: (BELLA; COLES-KEMP, 2012)

The proposed layers (shown in blue) and their respective interfaces (shown in yellow) are presented in Figure 4. In the given image, the authors demonstrate the example of a p_B process representing a user Bob, defined by Bella & Coles-Kemp (2012) as a player, interacting with a player A, p_A Alice. For each layer, the yellow interface represents a different aspect of the player. For example, UI_A represents the user interface between the operating system layer and the human-computer one and S_A. represents the player between the personal and communal layers Bella & Coles-Kemp (2012) specify the layers as below:

1. Informational (L1): is the classic protocol explained in section 2.1, which runs in computer processes and executes the operations for communication between actors over an insecure network;
2. Operating System (L2): is the inter-process communication between different processes of the target user computer, mainly the protocol and graphical interface processes;
3. Human-Computer Interaction (L3): is the socio-technical protocol, i.e., the user interacting with the process of a graphical interface. This layer deals with both the technology in the graphical interface as well as the user expressing social competencies, such as trust in the system;
4. Personal (L4): is the user layer, which is the expression of the multiple personas that interact with the technology;
5. Communal (L5): is the layer that represents the user influenced by and influencing society.

This method of visualizing a ceremony is used throughout our work to categorize the studies proposed here and establish a comparison with other works developed. This choice is due to how the concertina can express a "complete security ceremony", allowing a comprehensive analysis of the complexities involved in each study and facilitating comparison with other existing approaches. By adopting this methodology, we aim to understand the structure and challenges of security ceremonies and promote a more detailed evaluation of proposed solutions.

2.3.2 Literature Review

Thus, it is possible to classify the studies previously presented as belonging to the different layers of the ceremony concertina transversal methodology. This helps us to understand the state of the art in security ceremonies and how the present work fits into this panorama. We focus, for the most part, on review research in L3 and L4.

Following this methodology, we define the modeling of the protocols shown in Figures 1 and 2 as relating to L1. This is where most of the classic work in the literature can be found, such as that defined in Schmidt et al. (2012), Haidar & Abdallah (2009) and Canetti & Krawczyk (2001). More recently, work along these lines has extended to the formal verification of protocols applied to the Internet of Things (IoT), such as the case study proposed by Braghin, Lilli & Riccobene (2023) for Z-Wave. In this work, the authors have performed the formal specification of the Z-Wave IoT protocol using the S2 security class.

Working on L3, Johansen & Jøsang (2015) proposes a probabilistic model (rather than the classical non-deterministic one) to model the actions of human agents. In this sense, the authors advocate separating the model of the human from the user interface, using the notion of "personas", defined as a finite set of social and cognitive attributes that make up a person. Their work may be seen as a possible definition of a common actor between L3 and L4, in which the personas will trigger actions in the user interface model presented as a finite state machine.

The study by Basin, Radomirovic & Schmid (2016) focuses on modeling human limitations and errors, considering the problem that the human nodes are the most vulnerable part of the ceremonies. Similarly, Bella, Giustolisi & Schürmann (2022) works on modeling how the interaction between these nodes affects the safety of the ceremony. Finally, Sempreboni & Viganò (2020) models human mistakes as mutation rules. All three works are situated in L3 and L4 of the concertina methodology and attempt to establish an interface between these layers. However, they do not delve into human expressions to gain an understanding of the social context in which they are situated.

Also, by understanding these layers, Pedersen, Johansen & Jøsang (2018) argues that during interaction with ceremonies, users are influenced by their experiences and mental states, leading to biased choices when dealing with protocols. The authors proposed that incorporating behavioral models into the development of systems would facilitate the simulation of authentic human behavior and the design of interfaces that would enable individuals to make more accurate decisions when interacting with automated systems.

Similarly, Bella et al. (2022) says that despite efforts to improve the usability of these ceremonies, end users do not seem to be attracted to them. This study explores whether beautification can make ceremonies more attractive. Three studies were conducted to identify the dimensions of "beautiful ceremonies" and how people perceive them. It concludes that the beauty of security ceremonies lies in the perspective of those who observe them, but there are challenges in balancing security with usability improvements and beautification.

In their respective papers, Pedersen, Johansen & Jøsang (2018) and Bella et al. (2022) address the issue of understanding the human nodes and their interactions within the system from two different theoretical perspectives. Additionally, it would be beneficial to utilize a framework that can be applied to formal analysis to comprehend the impact of human conduct and expressions upon and in response to the ceremony. In this context, the concept of masks proposed by Pirandello can be employed to elucidate the nuances associated with the security ceremony as outlined by Martimiano & Martina (2022).

Pirandellian masks come from the play developed by Luigi Pirandello entitled *Sei personaggi in cerca d'autore* (PIRANDELLO, 2011b) and define the problems of transforming art into reality that make up the action of transposing the idea of a play and its characters into the duality of stage and actors. He discusses the masks that authors must wear to define reality on stage. The authors suggest discussing users and how they understand and interact with security ceremonies to propose solutions incorporating meta-design strategies. The authors conceptually define masks that could be used in the context of the ceremonies and comment on how they could be implemented using Tamarin (MEIER et al., 2013). The work leaves future implementations and how it could be used to design a full framework for studies in L3 and L4 as future work.

In this sense, our work adds to the state of the art by initially implementing these masks in Tamarin within a defined ceremony. Our goal is to gather data on how to use them to build a full framework encompassing the entire ecosystem surrounding Pirandellian masks and their application to understanding human nodes and their relationship with security ceremonies. This proposal differs from others presented for the study of layers L3 and L4 in that it extends the modeling of human nodes to include, in addition to errors, an understanding of human behavior relating to ceremonies in spheres that encompass emotions and behavior. It differs from the work of Pedersen, Johansen & Jøsang (2018) and Bella et al. (2022), as mentioned above, in its concern to add these characteristics within a formal framework.

3 SIM SWAP CEREMONY USE CASE

The SIM swap ceremony is the foundation for our investigations into Pirandelian masks. The ceremony was selected for two reasons: first, it involves different human actors, and second, it has not been formally modeled. This chapter presents empirical studies on the same ceremony and the problems in human entities and their nodes that lead to security failures and fraud. These problems cause financial damage to several users. In addition, we show a formal model of the actions involving these nodes within the ceremony, using Tamarin, to portray how these errors can occur when certain nodes fail. The understanding of the human condition that leads to error is provided in Section 4 and involves the implementation of a subset of the Pirandelian masks.

3.1 SIM SWAP ANATOMY

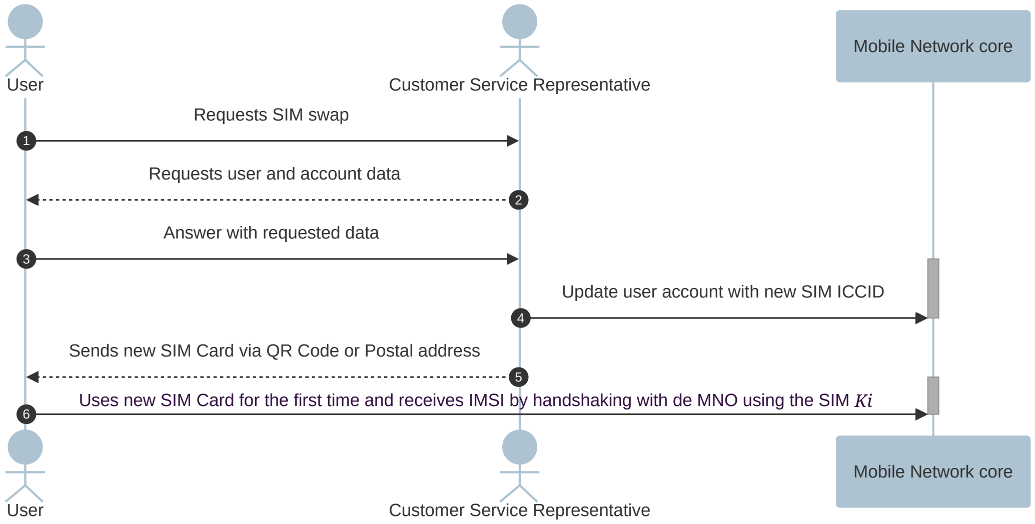
A Subscriber Identification Module, known as a SIM, is a smart card that contains a chip and identifies a user on a particular mobile network. The SIM is usually inserted into a smartphone and allows users to access SMS, internet, voice calls, and more services. As Gudimalla, Kannan et al. (2019) explain, the SIM stores several pieces of information that are fundamental to mobile network operators, such as the International Mobile Subscriber Identity (IMSI), the Integrated Circuit Card ID (ICCID) and the Authentication Key (Ki). SIM cards have processors that can carry out simple tasks such as receiving and forwarding a call request, signing data, etc. They also contain a few kilobytes of RAM and algorithms capable of generating pseudo-random numbers and encryption keys (GUDIMALLA; KANNAN et al., 2019).

Mobile Network Operators, hereafter MNOs, map the SIM cards of their customers to provide the service. In this way, they are responsible for maintaining a database containing the relationship between the phone numbers and the SIM, usually defined as a one-to-one relationship (LEE et al., 2020). Most of the time, the SIM card can be moved between devices and is subject to situations involving damage, loss, or even changing phones, as the SIM card can be of different sizes and needs to be adapted to suit the new device (EKEH et al., 2022; GUDIMALLA; KANNAN et al., 2019).

When something happens that makes it impossible to use the SIM card, the mobile network user can choose to keep their phone number and carry out a SIM swap operation. You can keep your phone number and account while changing SIMs. As commented in the study by Lee et al. (2020), these operations vary according to each MNO and involve authenticating the user using different information. Nevertheless, we have used the data from their study to define the generic operations involved in the SIM swap ceremony, as shown in Figure 5.

Using Figure 5 as a basis for discussion, it is possible to see two human entities actively participating in the portrait ceremony: the user and the customer service representative. In this case, the objective is for the service representative to authenticate the user and for the MNO core to validate the SIM swap. Six steps are involved in the progress of this ceremony towards its objectives. First, a user requests a customer service representative to start the swap process.

Figure 5 – Generic SIM swap Ceremony


User
Customer Service Representative
Mobile Network core
Requests SIM swap
1
Requests user and account data
2
Answer with requested data
3
Update user account with new SIM ICCID
4
Sends new SIM Card via QR Code or Postal address
5
Uses new SIM Card for the first time and receives IMSI by handshaking with de MNO using the SIM *Ki*
6
User
Customer Service Representative
Mobile Network core

Source: The author based in (LEE et al., 2020)

Then, the service representative returns a series of authentication challenges for the user to pass. Once these security questions have been answered, he will request that the old SIM be disconnected from the user account and that a new SIM be connected. Other steps involve the network confirming the SIM swap, returning the request to the user, and defining the IMSI code used to identify a subscriber in a mobile network uniquely.

In practice, the authentication challenges phase varies among implementations. In the United States alone, five types of challenges classes have been identified: personal information, account information, device information, usage, knowledge, and possession (LEE et al., 2020). For instance, the challenge may be to confirm the email address or date of birth provided when registering with the MNO, payment details such as card numbers and recent telephone numbers, or to verify passwords and one-time passcodes sent by email or SMS (LEE et al., 2020).

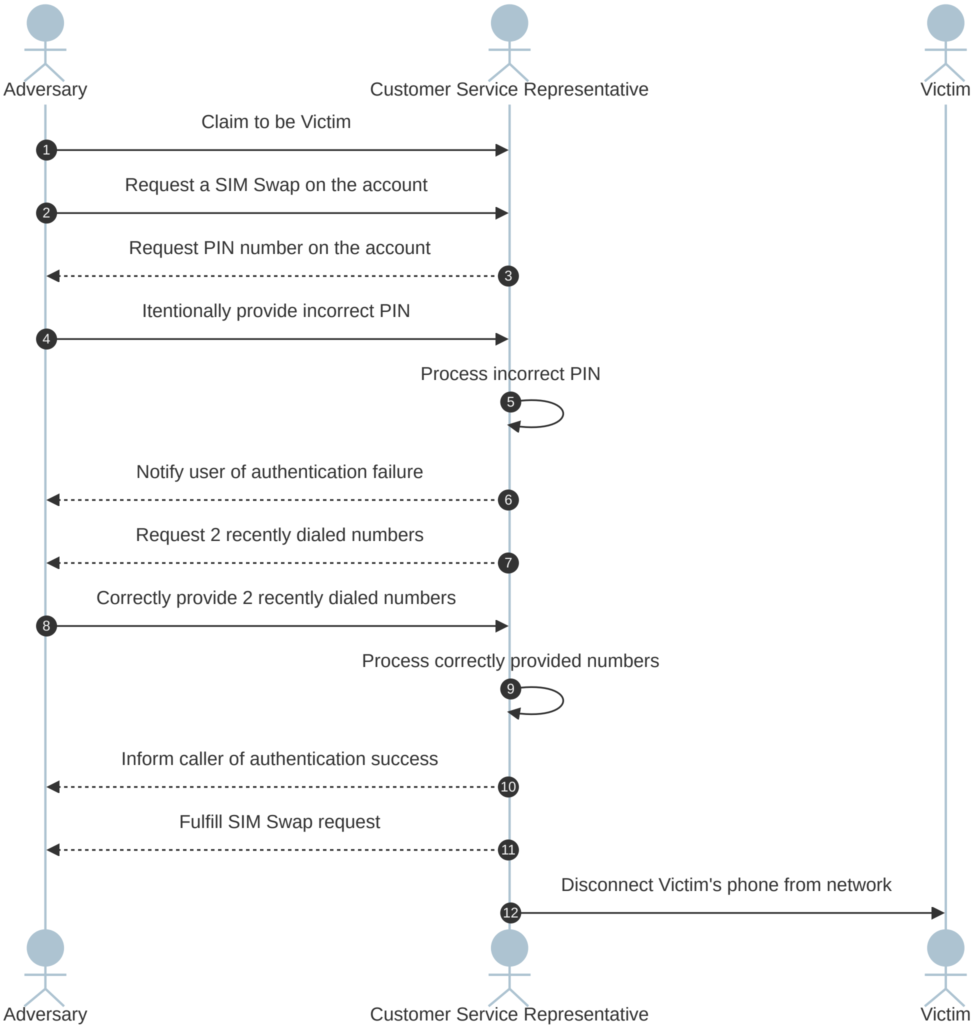
ENISA (2021), known as the European Union Agency for Cyber Security, conducted a study on this issue, looking at how SIM swaps work in 48 MNOs in 22 European Union countries. The study found different procedures for swapping, categorized into offline processes, such as going to an MNO physical shop, and online/telephone-based processes, which involve communicating with a customer service representative remotely. The same study identified challenges for this process, including those reported in the Lee et al. (2020). In addition, ENISA (2021) notes that when user authentication occurs in physical shops, it mainly includes identity checks based on official EU documents.

After authenticating the user, the MNO completes the swap process. According to the ENISA (2021) study, this process also differs between online and offline SIM swaps. In the former case, the physical SIM card is delivered to the postal address provided by the customer, or a QR code is sent online to activate an eSIM. In the offline case, the customer is asked to go to the MNO retail store to receive the physical SIM card or a QR code to activate the eSIM.

3.2 IDENTIFYING ISSUES AND IMPACTS

Although many MNOs worldwide use SIM swap practices, they are insecure and allow attacks using social engineering techniques to steal the phone numbers of arbitrary network users. As explained by Andrews (2018), the attack starts by finding the phone number and the MNO associated with a targeted user. Then, the attacker starts a SIM swap request for that number. Usually, the online form is used to carry out this scam. The attacker is then given a challenge, which they can answer correctly or incorrectly. This is a social problem, as the attacker must somehow convince the operator to make the exchange, which can be done in several ways, including bribery. The attacker starts operating the phone number of the target user by convincing the operator. Figure 6 shows the sequence diagram for this type of attack.

Figure 6 – SIM swap Attack


Adversary
Customer Service Representative
Victim
Claim to be Victim
1
Request a SIM Swap on the account
2
Request PIN number on the account
3
Itentionally provide incorrect PIN
4
Process incorrect PIN
5
Notify user of authentication failure
6
Request 2 recently dialed numbers
7
Correctly provide 2 recently dialed numbers
8
Process correctly provided numbers
9
Inform caller of authentication success
10
Fulfill SIM Swap request
11
Disconnect Victim's phone from network
12
Adversary
Customer Service Representative
Victim

Source: (LEE et al., 2020)

It is important to note that a phase before the attack involves the attacker collecting information about the user and the mobile carrier. This information is needed to respond to the challenges discussed in the previous section correctly and is generally sensitive information about users. Therefore, the attacker must use practices such as social engineering, phishing scams, and other tricks to get the data required to convince the carrier representative that the exchange should be made (JORDAAN; SOLMS, 2011).

Also, the research by ENISA (2021) displays the most likely ways for an attacker to obtain this information. Thus, social engineering on users scores as the most likely item to occur, while social engineering on MNO employees scores as a medium. Ways involving bribing or threatening MNO employees and carrying out cybersecurity attacks on network infrastructure are considered unlikely.

The success of these attacks has affected individuals in several countries, with cases reported in the European Union, the United States, the United Kingdom, Canada, Korea, and Nigeria (KIM; SUH; KWON, 2022). These losses occur because the phone number is employed as one of the two-factor authentication methods commonly used in applications that contain important functionalities (ANDREWS, 2018). Examples include banking applications, where a successful attack leads to direct financial loss.

Vitalik Buterin, the co-founder of Ethereum, had his X (former Twitter) account hacked. The report published by Cointelegraph (2023) indicated that the attackers used the above practices to access the account and publish invalid NFC offers, which tricked several of his followers into buying these NFCs. The total loss to the victims was U$ 691,000. Looking at the 2021 data collection, the Internet Crime Complaint Centre, linked to the FBI, received 1,611 reports of attacks involving SIM swaps (IC3, 2022). These resulted in financial losses totaling $6.8 million.

In Brazil, the 18th Civil Court of São Paulo sentenced Meta, Microsoft, and TIM to pay R$20,000 in damages to a scam victim (HIGíDIO, 2023). None of the companies would take responsibility for the attack during the trial. Meta stated the attacker and the target MNO were to blame, while Microsoft declared the user was responsible for the passwords. The MNO argued it could not refuse the requested operation because the data was correct. The case in question was a portability scam, which differs from the SIM swap scams documented so far in that it involves moving the number to a different SIM and MNO.

The case involving these three companies can serve as a basis for discussing questions about important properties of human societies, such as trust and responsibility. In this sense, it is noticeable that multiple parties are involved when a SIM swap scam occurs. They are the attacker, the victim, the MNO, and the application targeted by the final attack. Considering these parties, Jordaan & Solms (2011) states that responsibility for the damage is denied by each one, which leads to liability problems such as those mentioned in the article above. This implies a loss of trust in these entities.

3.3 MODELLING THE SIM SWAP CEREMONY

Despite being a very important ceremony, SIM swap still suffers from several problems, most of which involve manipulating human entities. Motivated by this, our research aims to formalize this ceremony, focusing mainly on the layers of computer-human interaction (L3 of the security ceremony concertina), where each human entity node talks to another through a network interface and has no physical access to the other.

At this initial stage, we are interested in showing how the human nodes may or may not cooperate with the attacker and thus help the attack discussed in Section 3.2 to take place. Therefore, in the next parts of this research, studies are carried out to include L4 of the concertina ceremony and extend this discussion to use the concept of Pirandellian masks to understand how this cooperation can occur by linking intention and behavior to human entity nodes.

It is important to define that we use the generic SIM swap model shown in Figure 5. Therefore, the information required for user validation is defined as random data part of a system of equations tallied by human entity nodes. This choice was made to make the model as generic as possible. It should also be noted that this modeling will aim to validate the models of this ceremony, which will take place online, i.e., without the human entities meeting in person.

Let us consider the translation of a generic SIM swap into First Order Modal Logic, as explained in Section 2.2.1. This logical description aims to show a ceremony that always works correctly. Still, when passed to the code in Tamarin, rules are added that modify this behavior to accept, for example, that the operator is unreliable or that the data has been attacked. Our goal in writing part of the ceremony in modal logic is to comprehend better the passage of knowledge between different actors of the ceremony and not to make a full model. So, to start with, we can define the entities that will be part of our ceremony as terms, namely:

1. M as an Mobile Network Operator;
2. U as an arbitrary User on a MNO M;
3. C as an arbitrary Customer Service Representative on a MNO M;

Next, we define formulas and sentences for each of these entities. These will be composed to create multiple sets of rules in Tamarin. To begin with, we will present the regulations involved in starting the SIM swap operation for honest U, M and C entities.

$$\forall U,M \;\; \mathsf{know}(M,T,\mathsf{phoneNumber}(U)) \wedge \mathsf{know}(M,T,\mathsf{information}(U)) \tag{3.1}$$

$$\forall U,M,C \;\; \mathsf{know}(M,T,\mathsf{phoneNumber}(U)) \Rightarrow \mathsf{know}(C,\mathsf{phoneNumber}(U)) \tag{3.2}$$

$$\forall U,M,C \;\; \mathsf{know}(M,T,\mathsf{information}(U)) \Rightarrow \mathsf{know}(C,\mathsf{information}(U)) \tag{3.3}$$

The Equations in 3.1 to 3.3 explain the knowledge of the entities U, M, and C, so, for any user and MNO, considering that the user has a SIM in that MNO, then the MNO knows that phone number and information about the user, which implies that a Customer Service Representative with access to that network also understands that data. Note that the knowledge that an entity has about the predicates involving itself has been omitted to make the text more readable.

Suppose the user U initiates the SIM swap on the network M. A customer service agent C is selected to deal with the request and validate the knowledge of this user with a series of questions about his information. We can illustrate this relationship as in Equation 3.4 to 3.6 where it is modeled that if a $\mathsf{initSimSwap}(U,T)$ occurs, this will be known to the M network, which will then trigger a representative C to request information about U from the SIM swap requester, who will be given knowledge of the questions to answer.

$$\forall U, M \ \mathsf{initSimSwap}(U,T) \Rightarrow \mathsf{know}(M, T+1, \mathsf{initSimSwap}(U,T)) \tag{3.4}$$

$$\forall U, C, M \ \mathsf{know}(M, T, \mathsf{initSimSwap}(U,T)) \Rightarrow \mathsf{askForInformation}(U,T,C) \tag{3.5}$$

$$\forall U, C \ \mathsf{askForInformation}(U,TC) \Rightarrow \mathsf{know}(U, T, \mathsf{askForInformation}(U,T,C)) \tag{3.6}$$

With the questions sent to the user U, the next step is to answer them and thus unlock the final stage of the SIM swap. We show a relationship which, indicated by the symbol $\Leftrightarrow$, means that an answer to the SIM swap questions will only be given if some U knows the information about himself and the questions relating to that information.

$$\forall U, C \ \mathsf{answersSimSwap}(U, T+1, C) \tag{3.7}$$

$$\Leftrightarrow \tag{3.8}$$

$$[\mathsf{know}(U, T, \mathsf{askForInformation}(U,C)) \wedge \mathsf{know}(U, T, \mathsf{information}(U))] \tag{3.9}$$

If the SIM card swap response comes through, the customer service agent knows that the response was correct and releases the SIM card swap to the network, sending this knowledge to the user. Note that the part about sending the SIM card has not been demonstrated here, as the main problem reported at this ceremony was user validation.

$$\forall U, C \ \mathsf{answersSimSwap}(U,T,C) \Rightarrow \mathsf{know}(C, T+1, \mathsf{answersSimSwap}(U,T,C)) \tag{3.10}$$

$$\forall U, C \ \mathsf{know}(C, T, \mathsf{answersSimSwap}(U,T,C)) \Rightarrow \mathsf{finishSimSwap}(U, T+1, C) \tag{3.11}$$

$$\forall U, C, M \ \mathsf{finishSimSwap}(U,T,C) \Rightarrow \mathsf{know}(U, T+1, \mathsf{finishSimSwap}(U,T,C)) \tag{3.12}$$

$$\forall U, C, M \ \mathsf{finishSimSwap}(U,T,C) \Rightarrow \mathsf{know}(M, T+1, \mathsf{finishSimSwap}(U,T,C)) \tag{3.13}$$

Once the necessary knowledge for the main part of the ceremony has been gathered, the modeling is done in Tamarin. The way we modeled a protocol using this tool was shown in Section 2.1; a ceremony can be modeled similarly. Note that the rules for passing knowledge between actors, written in Equations 3.1 to 3.13, are used here to guide the development of the code and, thus, the proofs of the properties of the ceremony.

For example, the relations written in the Equation 3.1 to 3.3, which involve user information and MNO knowledge, are written explicitly in the code, as we can see in Algorithm 4. Following the Tamarin grammar, an arbitrary piece of information x about a user U on the network can be defined by Fr(x:fresh). We consider as part of a user information set iccid and

Algorithm 4 – Tamarin InitUserOnNetwork

```

rule InitUserOnNetwork:
    [
        Fr(iccid:fresh), Fr(imsKi:fresh),
        Fr(userId:fresh), Fr(initialUserName:fresh),
        Fr(initialUserPhoneNumber:fresh)
    ]
    --[ InitUser($U, userId) ]->
    [
        !UserAccount($U, userId, initialUserName,
        initialUserPhoneNumber),
        !IMSI($U, userId, imsKi),
        !UserICCID(iccid, userId),
        Out(initialUserName), Out(initialUserPhoneNumber)
    ]

```

Source: The authors

imsKi, which are data about the SIM card used by the user when registering with the MNO, initialUserName and initialUserPhoneNumber as data about the person behind the user, and userId as the ID of a user on an MNO.

This data will be consumed by a rule of type [ ] –[ ]-> [ ], as explained above, and will be sent as knowledge to the MNO, involving data about UserAccount, among others. Furthermore, Tamarin has communication channels for an insecure network that assumes a Dolev-Yao attacker. Using the Out(x) output facts, we can send data that we consider the attacker will know, in this case, a target user's name and telephone number.

We have created similar rules to define a customer service representative in MNO. Another important fact to note is that the entities U, M, and C are represented in Tamarin as prefixed public variables in the form $X. To model the SIM swap itself, four rules have been created, which, similarly to the logical model, include the start of the process, the answering of the authentication questions, the confirmation of the answers by the customer service agent, and the completion by the network, which generates a new iccid and its relationship with the user account, indicating that the process has been successfully finished.

The rule that starts the SIM Swap process, specified in Algorithm 5, receives a Customer Service Representative as input facts, represented by !Operator(O, opId), the data that references the number that will be SIM swapped, In(initialUserPhoneNumber) and a random Fr(seedK:fresh). The first fact is used to define which representative is answering the call. The fact In(initialUserPhoneNumber) comes from a network that the attacker can manipulate, i.e., an attacker or a user can send it. Finally, Fr(seedK:fresh) is used to calculate the security question for a request to maintain its arbitrary properties within the set of possible knowledge-based authentication methods.

When the InitSimSwapWithOperator rule is executed, there will be an execution trace that stores the telephone number and the seed used to define the user security question. Thus, a

Algorithm 5 – Tamarin InitSimSwapWithOperator

```

rule InitSimSwapWithOperator:
    [
        !Operator(O, opId, "REDE"),  In(initialUserPhoneNumber),
        Fr(seedK:fresh)
    ]
    --[InitSimSwap(initialUserPhoneNumber, seedK:fresh)]->
    [
        SimSwapINIT(seedK:fresh, opId, initialUserPhoneNumber),
        Out(question(initialUserPhoneNumber, seedK:fresh)),
        Out(seedK:fresh)
    ]

```

Source: The authors

question is described from the equation $\mathsf{question}(\mathsf{T},\ \mathsf{K})$, which receives a telephone number and a seedK. The output of this first stage of the process is a control fact that indicates to the system that a telephone number has been added and the output to the network of the question and the seedK used to generate the question. This knowledge is placed on the network employing facts of the type $\mathsf{Out}()$, i.e., they may be known to an attacker.

For the next step of the SIM swap, the user must receive the question and then answer it for the Customer Service Representative. The way to obtain approval for this operation is through the relationship $\mathsf{answers}(\mathsf{T},\ \mathsf{K},\ \mathsf{correctAnswer}(\mathsf{question}(\mathsf{T},\ \mathsf{K}))) = \mathsf{permission}(\mathsf{T},\ \mathsf{K})$, where the representative needs to get the $\mathsf{permission}(\mathsf{T},\ \mathsf{K})$ where T is the phone number and K the seedK used to find the question being answered. A user can calculate this because they know the $\mathsf{correctAnswer}(\mathsf{question}(\mathsf{T},\ \mathsf{K}))$. In this way, the answering step receives input facts from the system state indicating that a SIM swap process has been started, and the question asked solves the equation that guarantees the correct answer and permission and sends it to the system.

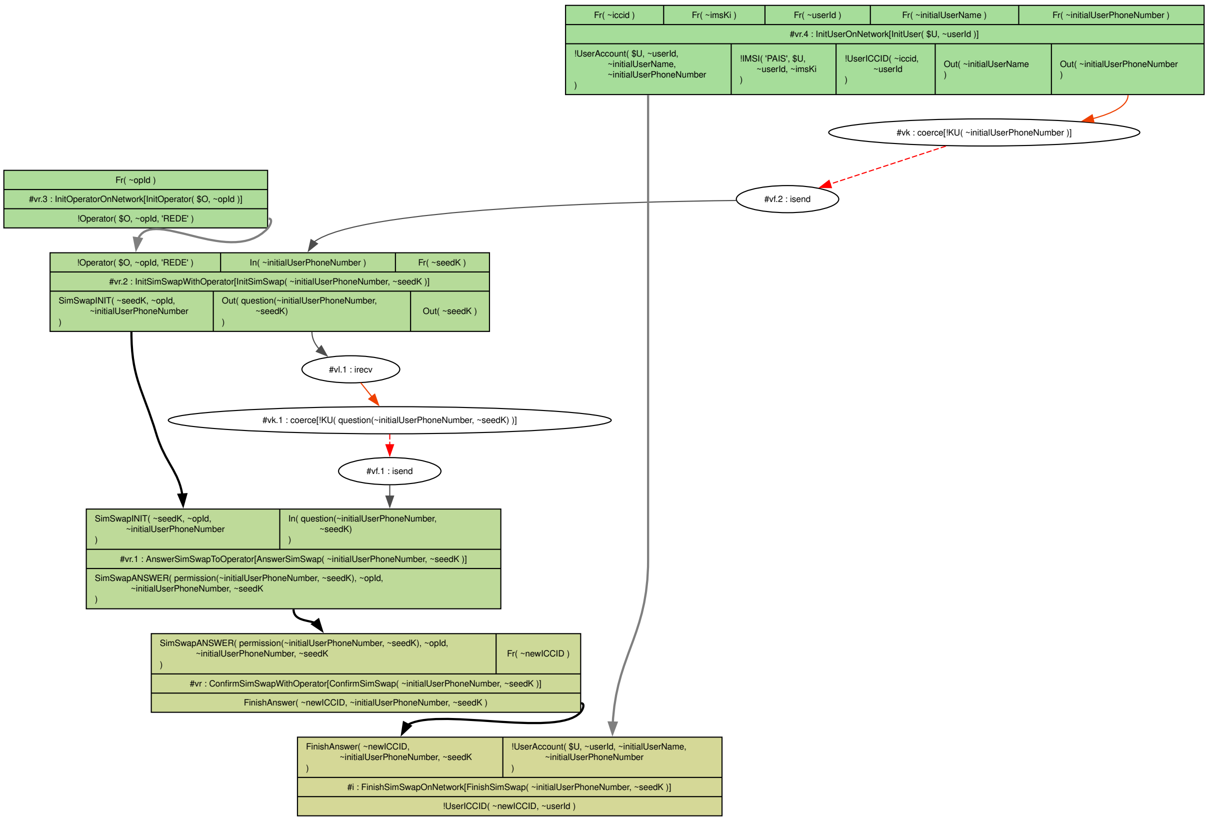
Note that an attacker can get the data needed to calculate these equations and respond correctly in this phase. Rules that model this behavior on the part of an attacker have also been added. The remaining rules refer to how the system finishes the SIM swap. We considered that the information of a user could be attacked and thus discovered, but the customer service representative would always be reliable. We tested the system for two properties:

Property 5 (Authenticity of Initiator)**.** For every completed SIM swap request, an honest user initiates the request and answers the authentication questions correctly.

Property 6 (Knowledge Integrity)**.** It can not be that a Customer Service Representative has approved the SIM swap, and the attacker knows the authentication answers of any user without having carried out an external attack on the data.

The Property 6 holds in all execution traces. However, considering the possibility of a data attack, Property 5, only the owner can perform SIM swap, has two execution traces. The first, shown in Figure 7, is honest and includes all the necessary steps between the actors in the process. The second, shown in Figure 8, exhibits how it is possible to attack the information and allow an attacker to impersonate an honest user.

Figure 7 – Property SIM swap Finish Honestly success case


Fr(~iccid)
Fr(~imsKi)
Fr(~userId)
Fr(~initialUserName)
Fr(~initialUserPhoneNumber)
#vr.4 : InitUserOnNetwork[InitUser($U, ~userId)]
!UserAccount($U, ~userId, ~initialUserName, ~initialUserPhoneNumber)
!IMSI('PAIS', $U, ~userId, ~imsKi)
!UserICCID(~iccid, ~userId)
Out(~initialUserName)
Out(~initialUserPhoneNumber)
#vk : coerce[!KU(~initialUserPhoneNumber)]
#vf.2 : isend
Fr(~opId)
#vr.3 : InitOperatorOnNetwork[InitOperator($O, ~opId)]
!Operator($O, ~opId, 'REDE')
!Operator($O, ~opId, 'REDE')
In(~initialUserPhoneNumber)
Fr(~seedK)
#vr.2 : InitSimSwapWithOperator[InitSimSwap(~initialUserPhoneNumber, ~seedK)]
SimSwapINIT(~seedK, ~opId, ~initialUserPhoneNumber)
Out(question(~initialUserPhoneNumber, ~seedK))
Out(~seedK)
#vl.1 : irecv
#vk.1 : coerce[!KU(question(~initialUserPhoneNumber, ~seedK))]
#vf.1 : isend
SimSwapINIT(~seedK, ~opId, ~initialUserPhoneNumber)
In(question(~initialUserPhoneNumber, ~seedK))
#vr.1 : AnswerSimSwapToOperator[AnswerSimSwap(~initialUserPhoneNumber, ~seedK)]
SimSwapANSWER(permission(~initialUserPhoneNumber, ~seedK), ~opId, ~initialUserPhoneNumber, ~seedK)
SimSwapANSWER(permission(~initialUserPhoneNumber, ~seedK), ~opId, ~initialUserPhoneNumber, ~seedK)
Fr(~newICCID)
#vr : ConfirmSimSwapWithOperator[ConfirmSimSwap(~initialUserPhoneNumber, ~seedK)]
FinishAnswer(~newICCID, ~initialUserPhoneNumber, ~seedK)
FinishAnswer(~newICCID, ~initialUserPhoneNumber, ~seedK)
!UserAccount($U, ~userId, ~initialUserName, ~initialUserPhoneNumber)
#i : FinishSimSwapOnNetwork[FinishSimSwap(~initialUserPhoneNumber, ~seedK)]
!UserICCID(~newICCID, ~userId)

Result of the execution of the rules defined by Tamarin. In this case, we have a successful execution trace where the rules execute and maintain the properties previously defined, successfully finalizing the SIM swap by an honest user.

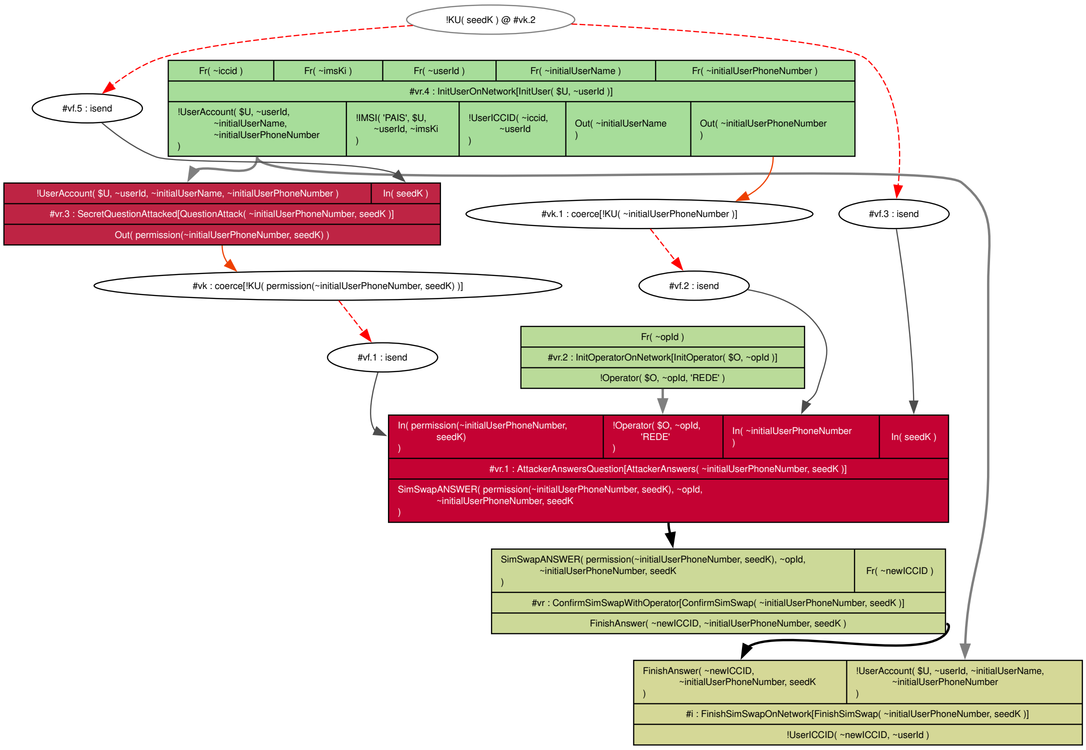
Source: The Author using Tamarin

Examining Figure 8 in particular, we may see that the modeling generates an attack flow that starts with a user entering the network, considering all his data. At this point, the encoding gives the attacker the username and phone number, as we believe this is common knowledge at the start of the attack and necessary to identify the victim. The attacker then attacks the data and uses the operation result (modeled as an output fact) to communicate with an operator on the network and correctly answer the questions that validate the user.

In addition to the attack that actively involves stealing information, we modeled a rogue Customer Service Representative. The execution trace generated is similar to the one mentioned above and consists of the representative forcing the SIM swap without any validation from the user. Similarly, rules were created to help with this type of attack. At this stage, cooperation between the two attacking nodes was not considered.

The interesting thing about these results is that we can see how the formal model of the security ceremony, although still initial, is similar to what was found empirically in the analyses presented in the previous sections, both in terms of how the SIM swap takes place and in terms of how fraud can occur if the human nodes are dishonest. In this way, it can be used to study

Figure 8 – Property SIM swap Finish Honestly attack case


!KU(seedK) @ #vk.2
Fr(~iccid)
Fr(~imsKi)
Fr(~userId)
Fr(~initialUserName)
Fr(~initialUserPhoneNumber)
#vr.4 : InitUserOnNetwork[InitUser($U, ~userId)]
!UserAccount($U, ~userId, ~initialUserName, ~initialUserPhoneNumber)
!IMSI('PAIS', $U, ~userId, ~imsKi)
!UserICCID(~iccid, ~userId)
Out(~initialUserName)
Out(~initialUserPhoneNumber)
#vf.5 : isend
!UserAccount($U, ~userId, ~initialUserName, ~initialUserPhoneNumber)
In(seedK)
#vr.3 : SecretQuestionAttacked[QuestionAttack(~initialUserPhoneNumber, seedK)]
Out(permission(~initialUserPhoneNumber, seedK))
#vk.1 : coerce[!KU(~initialUserPhoneNumber)]
#vf.3 : isend
#vk : coerce[!KU(permission(~initialUserPhoneNumber, seedK))]
#vf.2 : isend
#vf.1 : isend
Fr(~opId)
#vr.2 : InitOperatorOnNetwork[InitOperator($O, ~opId)]
!Operator($O, ~opId, 'REDE')
In(permission(~initialUserPhoneNumber, seedK))
!Operator($O, ~opId, 'REDE')
In(~initialUserPhoneNumber)
In(seedK)
#vr.1 : AttackerAnswersQuestion[AttackerAnswers(~initialUserPhoneNumber, seedK)]
SimSwapANSWER(permission(~initialUserPhoneNumber, seedK), ~opId, ~initialUserPhoneNumber, seedK)
SimSwapANSWER(permission(~initialUserPhoneNumber, seedK), ~opId, ~initialUserPhoneNumber, seedK)
Fr(~newICCID)
#vr : ConfirmSimSwapWithOperator[ConfirmSimSwap(~initialUserPhoneNumber, seedK)]
FinishAnswer(~newICCID, ~initialUserPhoneNumber, seedK)
FinishAnswer(~newICCID, ~initialUserPhoneNumber, seedK)
!UserAccount($U, ~userId, ~initialUserName, ~initialUserPhoneNumber)
#i : FinishSimSwapOnNetwork[FinishSimSwap(~initialUserPhoneNumber, seedK)]
!UserICCID(~newICCID, ~userId)

Result of the execution of the rules defined by Tamarin. In this case, we have an attack execution trace where the rules execute and do not maintain previously defined properties.

Source: The Author using Tamarin

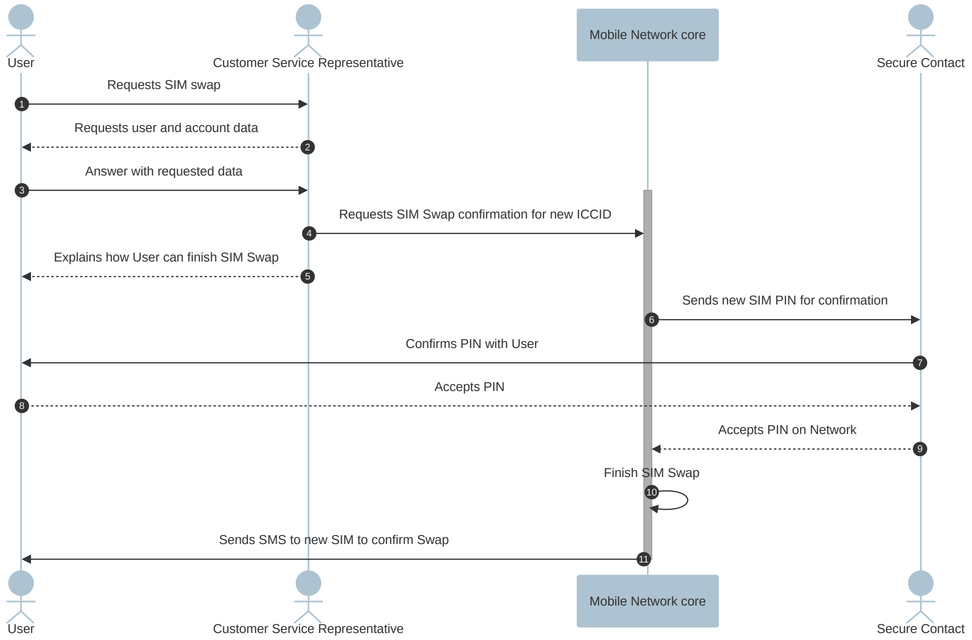
improvements to the system and enable studies to make it more secure.

To illustrate this possibility, we have developed a modified version of the SIM swap ceremony, in which the phase after user verification is updated so that it can only be performed by security contacts. In this sense, users who register on the network specify a set of trusted contacts (whose change ceremony is initially out-of-band). When they need to go through a SIM swap process, the customer service representative validates their information for the network but does not complete the process itself. This validation is done via a confirmation message sent by the MNO network to one of the security contacts of the user without the intervention of an MNO representative, as exhibited in Figure 9.

We believe the trusted contact would not cooperate with an operator or attacker. Still, if they do, it is possible to define that to approve the SIM swap, there must be a consensus between most of the contacts involved, making the process even more difficult and involving attacks on consensus protocols. When this contact receives social confirmation from the user that a SIM swap is taking place, they confirm with the MNO that the process is over.

Incorporating these modifications into the original model in Tamarin entailed amending the final rules on the system, finalizing the SIM swap upon confirmation from the Customer Service representative, and adding new rules. Consequently, upon receipt of the response to a security question, the representative initiates the transmission of a message to the designated security contact via the network yet remains uninvolved in the process. Consequently, sending

Figure 9 – SIM swap with Secure Contact


User
Customer Service Representative
Mobile Network core
Secure Contact
1 Requests SIM swap
2 Requests user and account data
3 Answer with requested data
4 Requests SIM Swap confirmation for new ICCID
5 Explains how User can finish SIM Swap
6 Sends new SIM PIN for confirmation
7 Confirms PIN with User
8 Accepts PIN
9 Accepts PIN on Network
10 Finish SIM Swap
11 Sends SMS to new SIM to confirm Swap
User
Customer Service Representative
Mobile Network core
Secure Contact

Source: The Author

the message was modeled as a secure channel, with the addition of rules that permit the attacker to read the messages but not to insert them.

When it receives the message over the secure channel, the contact follows the flow shown in Figure 9. Inbound and outbound rules for safe communication with this contact are added to talk to the User and confirm the SIM swap on the network. When confirmed, the flow follows similarly to the first experiment. The results show that the attack can begin because these modifications increase the steps needed for the test but keep the same start flow. However, the SIM swap will only occur when an honest user confirms, via a social channel modeled here as a secure channel, that the swap is to the new SIM card already in their possession and with the data indicating part of their PIN.

This new SIM swap can pass both Properties 5 and 6. As a first result of this work, we have an initial model that involves L3 of the security ceremony concertina, adding common attacks carried out by human nodes in the SIM swap, which serves to study improvements in this area. The set of experiments displayed here is available at https://github.com/LarissaGRosa/SIMSwapModel/tree/experiments-section-3. Nonetheless, we are not considering human behavioral and intentional factors that lead to these attacks, which occur in the next section.

4 IMPLEMENTING THE PIRANDELLIAN MASKS

The mapping conducted in Section 3.3 involves user nodes not subject to failures, which is an unrealistic assumption in the real world. Furthermore, it acknowledges that Customer Service Representatives may or may not be malicious but fails to consider the intention of these actors in acting maliciously. Similarly, it recognizes that attackers have the power to gain access to data but fails to demonstrate the relationship between other actors and their role in facilitating this attack. Thus far, we have yet to consider how human actions and attitudes can influence ceremonies. This section will examine how concepts from the literature can be employed to approach the L4 of the security ceremony concertina. Concurrently, the objective is to utilize this novel methodology to enhance our understanding of the SIM swap ceremony, thereby providing further insights into human behavior.

4.1 PIRANDELLO’S WORK AND SECURITY CEREMONIES

In the research by Martimiano & Martina (2022), the concept of Pirandellian masks is applied to the analysis of security ceremonies. The proposal to employ these masks is inspired by the theatrical works of Luigi Pirandello, an Italian playwright who received the 1934 Nobel Prize in Literature for his contributions to the field (NOBEL; OUTREACH, 2024). Pirandello’s plays frequently explored themes related to identity, the reality of human experience, and the malleability of human identity (KAMARZADEH, 2016).

We must comment on the play *Sei personaggi in cerca d’autore* (PIRANDELLO, 2011b) as a starting point for the elucidation of the masks mentioned above and for the metatheatrical analyses that will be used as a parallel for our studies between the L4 and L3 layers of the concertina ceremony. The play comprises six characters narrating their story to a group of actors and their director. The characters seek an author who can transcribe their story into a reality on stage and actors who can represent them. As the play progresses, it becomes evident that the characters often wear metaphorical masks to navigate between the expectations of social norms and the truths of their personal experiences.

As observed by Kamarzadeh (2016), Pirandello frequently employs the "bare mask" concept to illustrate the interrelationships between characters and actors, society and social position. The six characters in the narrative, namely Father, Mother, Stepdaughter, Son, Madame Pace, and Manager, recount the family dramas that led them to the pivotal moment. Each character is imbued with intricate emotional and psychological nuances, exemplifying how their outward personas, or *masks*, frequently conceal more profound and tumultuous inner realities. For example, the father’s masked rationality and control conceal his de facto guilt and despair, while the stepdaughter’s provocative behavior masks her substantial betrayal and abandonment.

Furthermore, as Martimiano & Martina (2022) elucidate, Pirandello comprehends a society propelled by masks that individuals can adhere to of their own volition or that society can impose upon their members. These masks symbolize the disparate identities and roles people assume in various social contexts, reflecting societal expectations and norms. Furthermore, in addition to metaphorically interpreting the concept of masks in relation to societal dynamics, Pirandello also employs this concept in the context of theatrical performance. In his plays, Pirandello presents a narrative in which the actor's inability to embody a specific character fully represents a tension between his authentic self and the role he is expected to perform (PIRANDELLO, 1987). This illustrates the multifaceted complexity of human interactions and the multiplicity of roles that an individual assumes in different social situations.

Pirandello also discusses the discrepancy between the text, originally written by the author, and its subsequent application on stage. In Pirandello's view, this represents a betrayal of the original text (BIASIN; GIERI et al., 1999). In this context, the author perceives a disjuncture between themselves, the director, and the actors involved in creating a play. Even if they attempt to do so, the actor cannot play the character in the way that the author originally intended, as they cannot discern the author's intention or experience the author's initial imagination (PIRANDELLO, 2011a).

As demonstrated by the analysis of Biasin, Gieri et al. (1999), this concept also applies to the characters, who choose not to adhere to the narrative constructed by an actor but instead wish to narrate their own story as characters. Similarly, actors encounter significant challenges when portraying these characters, given that they are humans influenced by their surroundings and cannot fully detach themselves from these influences to fully embody the character they are portraying. In general, Pirandello's work presents a dichotomy between reality and its representation in all the spheres that encompass theatre and, by extension, real life.

In light of the meta-theatrical nature of the work by Pirandello, we intend to establish parallels between theatre and security ceremonies involving both the concept of masks and the idea of clashes between the written and presented theatre pieces. In this context, the author is regarded as the developer of a ceremony, the characters as the concept of a user conceived by the author, and the actors and director's execution of the piece as its use in real life, which similarly betrays the architect's original proposal. The concept by Martimiano & Martina (2022) was therefore inspired by this idea and the subsequent analysis of other works by Pirandello, which further elaborate on the notion of masks and their role in society.

In particular, reference is made to the author's ideas on the use of masks as a metaphor for human behavior, whereby actors (or users) are required to wear these masks throughout the execution of the protocol, thus representing the various roles and personas that they may adopt. Analogous to that described for *Sei personaggi in cerca d'autore*, Martimiano & Martina (2022) delineates six preliminary masks that can be donned by individuals during the execution of a security ceremony as such:

Mask (The Attentive)**.** Represents a user who is mindful and thorough during a security ceremony, carefully following instructions and rechecking credentials, leading to more accurate and successful outcomes as intended by the designers.

Mask (The Careless)**.** This category represents users who disregard security mechanisms, proceed without careful reading or rechecking credentials, and often leave devices unattended. This leads to potential errors and increased time spent redoing steps, adversely affecting the ceremony's success.

Mask (The Fearful)**.** Represents users reluctant to engage with security systems due to distrust in digital devices or their ability to recognize social engineering attacks, leading them to avoid entering personal information and participating in security protocols whenever possible.

Mask (The Naive)**.** Represents beginner users unfamiliar with security ceremonies or technology, requiring clear guidance at each step, risking leaving devices unattended, and highlighting the need for a user-friendly interface to help them complete the ceremony safely.

Mask (The Busy)**.** Represents users who, due to time constraints, do not thoroughly read instructions or recheck personal information, potentially leading to errors and unsuccessful ceremony completion, not from carelessness but from rushed use of resources.

Mask (The Elder)**.** Designed for elderly users who may struggle with understanding and following ceremony steps due to limited familiarity, fear of errors, and slower response times, the Naive and Fearful masks combine elements that highlight the need for adaptable and user-friendly design.

By applying the defined concept of these masks to our context of use and formal modeling in Tamarin, it is possible to extend the analysis of the SIM swap ceremony to a greater degree of granularity. This approach allows us to model various user behaviors and how they interact with the system under different conditions. For example, we can simulate an attentive user who meticulously follows all security prompts and compares their actions to a careless user who may ignore critical steps. This granular analysis will enable us to understand human behavior more comprehensively, identify patterns in user interaction, and assess the impacts of the correct execution of the SIM swap.

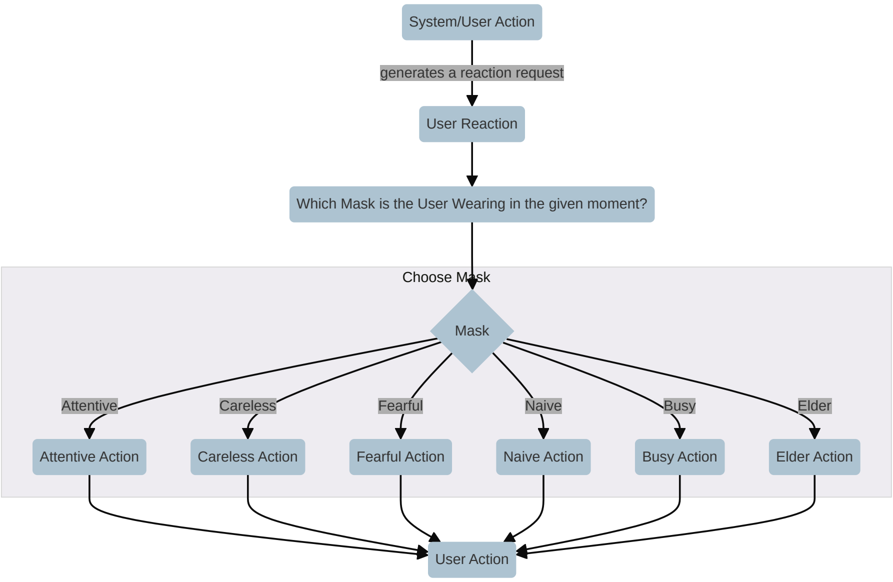
4.2 MODELLING THE MASKS IN TAMARIN

Having established the theoretical foundation of the masks, we must now proceed to formalize their representation and utilize them as a tool for investigating the characteristics of our ceremony from the perspective of their existence. Once more, we are guided by the principles of theatre to comprehend the genesis of this modeling. In theatre, actors respond to external stimuli and engage in actions that constitute the performance on behalf of their characters.

This systematic composition of actions and reactions by the various actors makes the story unfold for the audience. Similarly, we understand actions and reactions as how the human nodes of our protocol can trigger the mask they wear at a discrete point in time during the performance of our ceremony. By formally modeling these interactions, we analyze the impact of different user behaviors on the security and effectiveness of the ceremony.

In this manner, it is established that each action of a ceremony node (regardless of whether it is a user or a system) can trigger a user node reaction. As illustrated in Figure 10, upon learning of a system action, the user is directed to a reaction state (which may be none), and this reaction is contingent upon the decision of a mask that the user can wear to act on the system. In the real world, wearing a mask depends on the individual's emotional state, environment, and knowledge of the ceremony, among other factors. In modeling, the objective is to ascertain how multiple masks act during the ceremony. Consequently, the choice of execution for the test is arbitrary, resulting in the generation of various traces that demonstrate the influence of the choice of a mask in each action-reaction pair on the progression of the ceremony.

Figure 10 – Pirandellian Masks Model Flowchart



Source: The Author

Once the interfaces that trigger the masks and how the execution of the ceremony intersects them through the action-reaction pair have been defined, the next step is to apply it in the SIM swap ceremony. It is necessary to model how the masks may be employed in the formal proof of the defined properties in the target ceremony. This will be achieved using the multiset rewriting theory, which forms the basis of Tamarin, as discussed in Section 2.

It was determined that whenever a rule initiates the insertion of a human node within the model, a permanent fact, designated as `!HumanMask(M, Id, K)` is generated. The parameters `M`, `Id`, and `K`, respectively, represent the identifier of the initiating rule (`M`), an identifier that facilitates the matching of the generated mask to its intended wearer (`Id`), and an arbitrary piece of data used to define information to be utilized by the masks universally (`K`). These parameters were selected to facilitate the adaptation of the existing context of the models developed in Section 3.3.

The input for user action rules will be determined by the `!HumanMask(M, Id, K)` fact and reaction facts generated from human-system interactions. Actions initiated without needing

Algorithm 6 – Pirandellian Mask Rule Tamarin Example

```
rule acceptUserPINAttentive:
    [
        MaskReactant($N, userId, userSecureContact, <action, pinICCID>),
        !HumanMask($N, secureId, userSecureContacts)
    ]
    --[ Eq("accept_this_pin", action),
        Eq(userSecureContacts, userSecureContact)
     ]->
    [
        MaskPerform($N, secureId, userSecureContacts,
        <"confirms_pin", pinICCID>)
    ]
```

Source: The authors

a prior reaction request will rely on the initial fact, supplemented by subsequent facts that provide contextual information. Let us consider as an example the 6 Algorithm, which encodes behavior pertinent to user nodes with the Attentive mask. We see that the input to the execution of the rule is the initial mask fact in conjunction with `MaskReactant`, which is an action of the type `accept this pin` coming from another user node and which generates, after checks by an attentive user on the state of the ceremony, an output fact of type `MaskPerform`.

Consequently, the implementation of the masks was defined by establishing analogous rules for each type of interaction that necessitates an action from a user node or customer service representative. Examples of such interactions include calling the representative, answering security questions, sending messages to trusted contacts, etc. To generate the desired behavior, the users who wear the masks employ several logics, which vary according to the interaction type under consideration. The logic applied in any given case involves a comparison of data, communication with other users, an understanding of execution states, and the execution of different operations that are possible from a human point of view.

Accordingly, for each mask defined, the entire set of interactions is implemented, considering the nuances of the execution logic attached to each one. Concerning the SIM swap, we have implemented a subset of the abovementioned masks in the Attentive, Careless, and Fearful categories. This was due to the level of detail of our modeling, which was designed to be generic and not to detail specific interfaces used by MNOs. Therefore, applying masks involving more complex behaviors is not a priority now.

Concerning the coding of these masks, the trigger and response interface, defined through the input and output facts as `MaskReactant` and `MaskPerform`, remains consistent throughout, thus ensuring transparency for the ceremony model as to which mask is being executed. Nevertheless, upon execution, the masks elicit disparate responses from the users who employ them. Each mask has a different implementation to model the way it influences user interaction, guiding their actions based on predefined behavior patterns.

Take the code in Algorithm 6 as an example. The rule is triggered by a user, identified by its `userId`, sending a reaction fact containing information about who they want to communicate with, that is, the `userSecurityContact`, and the action-data pair of the expected reaction. Once there is a mask for this security contact and considering that this node is wearing the Attentive one, we have checks on the action it is taking and whether the user is communicating with the correct security contact through the `Eq()` method, which in the defined model is a restriction that only allows the rule to be executed if the pair of data passed is equal.

If the Careless mask is employed, this check is not performed, thereby facilitating communication with an unwelcome contact. In the event of fearful behavior, the security contact may be disinclined to proceed with the confirmation action, even in circumstances where all the requisite confirmation has been completed successfully. This may result in the ceremony being aborted at the point of completion. The manner in which each behavior is represented in the ceremony is contingent upon how the mask is executed.

Following the completion of the modeling of the masks in Tamarin, a framework has been established that allows for the independent analysis of each mask's behavior throughout the execution of the ceremony and the aggregation of masks to generate flows of users who change masks during the ceremony. Consequently, it is possible to create different narratives of the ceremony. As with the play performed by the actors utilizing their character's masks, which may betray the original author and diverge from the designer's initial expectations, the same can be said of the narratives generated.

4.3 PIRANDELLIAN MASKS IN THE SIM SWAP CEREMONY

The masks defined in the modeling assume a ceremony that offers these entry and exit facts. Before this, our versions of SIM swap did not consider these mechanisms, so we had to modify the original models to enable the use of masks in their analyses. In addition, the interactions and data flows had to be adjusted to ensure that each mask could be correctly applied and tested in different usage scenarios.

Consider the Algorithms 7 and 8. Both aim to initiate the SIM swap process on an MNO through remote contact with a Customer Service Representative. The rule begins by receiving the data related to the phone number and sending this data to a pre-registered representative in the network, defined by !Operator(O, opId). A seed K is then generated, which selects a question from the network to verify the identity of this user. Concurrently, a log of the action is generated on the network, recording the phone number and the seed K. Finally, the representative makes the question available on the insecure network.

Although the two rules propose to define the same behavior, the rule specified in Algorithm 7 does not require an explicit human action to initiate. From the model's perspective, there must be an entity with knowledge about a user, whether that entity is the user who owns the phone number or an attacker. However, this entity does not necessarily reveal the action taken and the mask that defines a node that initiated such a request. This model aligns with the proposal presented in Section 3.3, which sought to model the ceremony by assuming its users

Algorithm 7 – Rule example before Pirandellian Mask Implementation

```
rule InitSimSwapWithMNORepresentative:
    [
        !Operator(O, opId),
        In(initialUserPhoneNumber),
        Fr(seedK:fresh)
    ]
    --[InitSimSwap(initialUserPhoneNumber, seedK)]->
    [
        SimSwapINIT(seedK, opId, initialUserPhoneNumber),
        Out(question(initialUserPhoneNumber, seedK)),
        Out(seedK)
    ]
```

Source: The authors

Algorithm 8 – Rule example after Pirandellian Mask Implementation

```
rule InitSimSwapWithMNORepresentative:
    [
      !MNORepresentative(O, repId),
      MaskPerform(U, userId, phoneNumber, action),
      Fr(seedK:fresh)
    ]
    --[
        Eq(action, "CALL_CUSTOMER_SERVICE_REPRESENTATIVE"),
        InitSimSwap(U, phoneNumber, seedK)
    ]->
    [
        Status("INIT", repId, userId, phoneNumber, seedK),
        MaskReactant(U, userId, phoneNumber,
        question(phoneNumber, seedK)),
        Out(question(phoneNumber, seedK)),
        Out(seedK)
    ]
```

Source: The authors

would act predictably without understanding the rationale behind their actions.

In contrast, the one defined in Algorithm 8 is designed to follow the model containing Pirandellian masks. Consequently, the requisite action is a human node invoking the function MaskPerform, generating a reaction proposal for type MaskReactant. To execute the rule, the action received must be the type Call Customer Service Representative. This will generate a reaction request that involves answering the calculated question, which is analogous to the process described in the Algorithm 7. It is important to note that attacker nodes can also perform these actions and reactions. Consequently, through the attack modeling rules, we have execution traces of this rule containing actions performed by malicious entities.

Analogous adaptations were implemented in all other rules designed to interact with users or other human nodes. During this process, the model underwent several iterations, during which simplifications were made. For instance, in the second iteration, certain names of facts and variables were modified to enhance their clarity, such as the transformation of the operator fact !Operator into the !MNORepresentative fact. Similarly, system status facts were modified to be standardized and used to circumvent the restrictions for initializing each rule. This was evidenced by the change from the fact SimSwapINIT to Status.

Having completed the adaptation of the ceremony to the use of masks, we conducted a series of analyses to understand the impact of the users who wear them on the progress of the ceremony. To achieve this objective, we initially analyzed the masks individually and, after, collectively for each SIM swap model previously mentioned. This entails examining the impact of a user consistently wearing the same mask throughout the ceremony. Subsequently, we devised a system that allows users to change masks during the execution.

The initial SIM swap model, predicated on the authentication of security questions and the assumption of trust in the operator, yielded the results depicted in Figures 11 and 12 as an illustrative example. The images illustrate the execution of traces of the proof for the property related to the SIM swap carried out by the user, who was the original owner of the phone number. In Figure 11, it can be observed that the Attentive mask enables the user to complete the procedure successfully. Similarly, a user who is careless in their responses to the questions may make an error. However, there are execution traces in which the user responds correctly, and these are the only responses that allow the test to be completed, given how the protocol has been modeled.

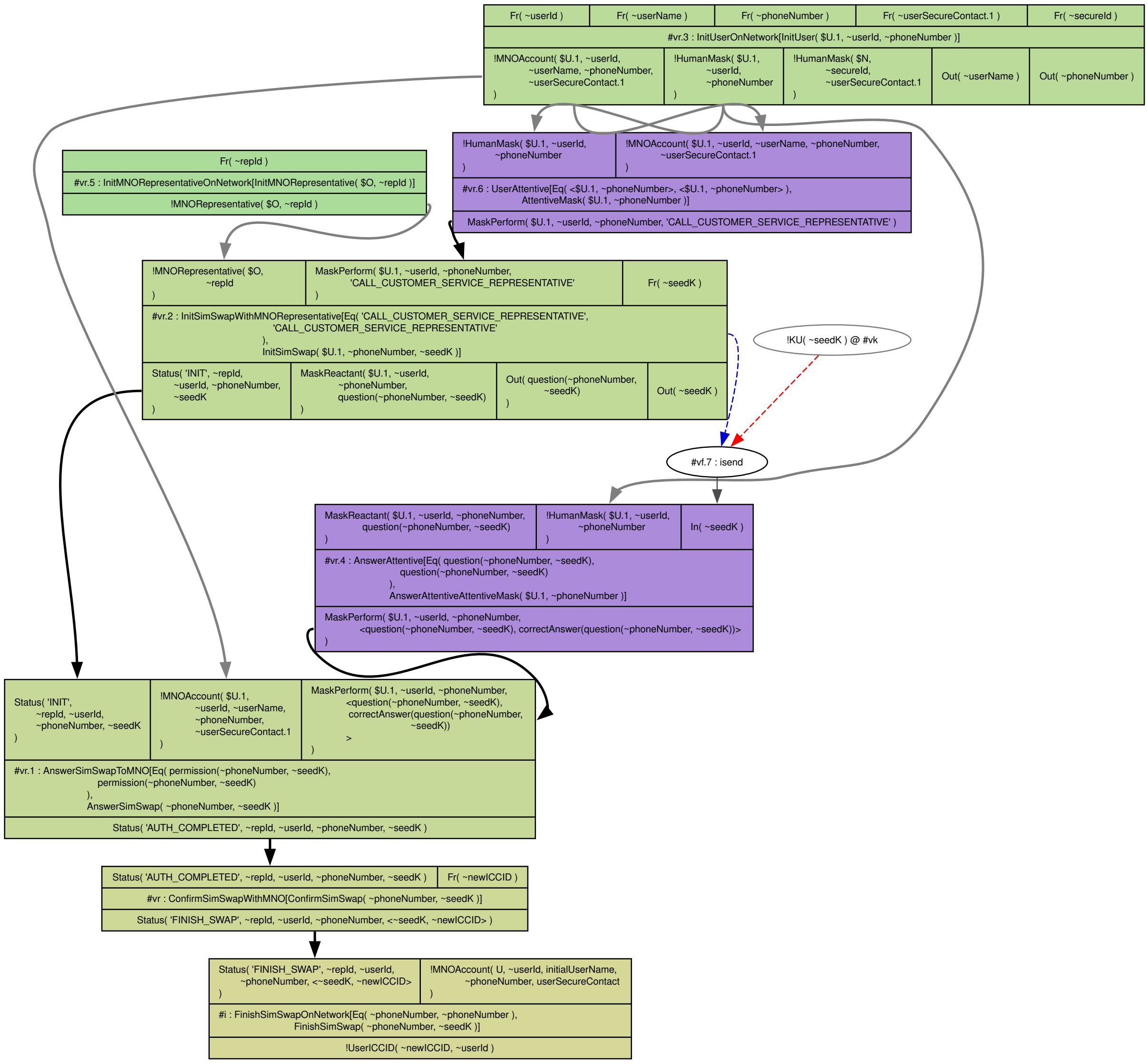
It can be observed that wearing the Fearful mask throughout the execution of the protocol results in the generation of traces that are not finalized by the user's refusal to respond to questions posed to them whilst wearing this mask. Figure 12 illustrates how a user may alter their mask during the execution of the protocol, initially adopting a fearful demeanor and subsequently assuming an attentive stance when prompted to respond to security questions. This changing mask structure allows us to compose human users with complex behaviors.

Given the unreliability of customer service representative nodes and their potential to be represented as actors wearing masks that model their behavior, we have identified a further set of execution traces. In this instance, the operators may act maliciously not out of explicit motivation as in the previous case but because they are wearing the Careless mask and are unaware that the data they have received is insufficient. In this sense, we have execution traces where an honest user may finish the SIM swap even though he had not answered the right question[1]. Similarly; an attack is assumed by the representative when they wear the Fearful mask and are prevented from finalizing the exchange, even though it is legitimate. Thus, no execution trace finishes the process with a representative wearing the Fearful mask.

In the context of the SIM swap with social authentication, the process forms three distinct human nodes: the user, the customer service representative, and the security contact. In this context, the validation of this model and the composition of the masks identified a potential attack that did not exist when viewed solely from the perspective of representatives and external

[1] The execution trace is available at https://github.com/LarissaGRosa/SIMSwapModel/blob/main/experiments/results/InitSimSwapWithMNORepresentative_careless_representative.pdf

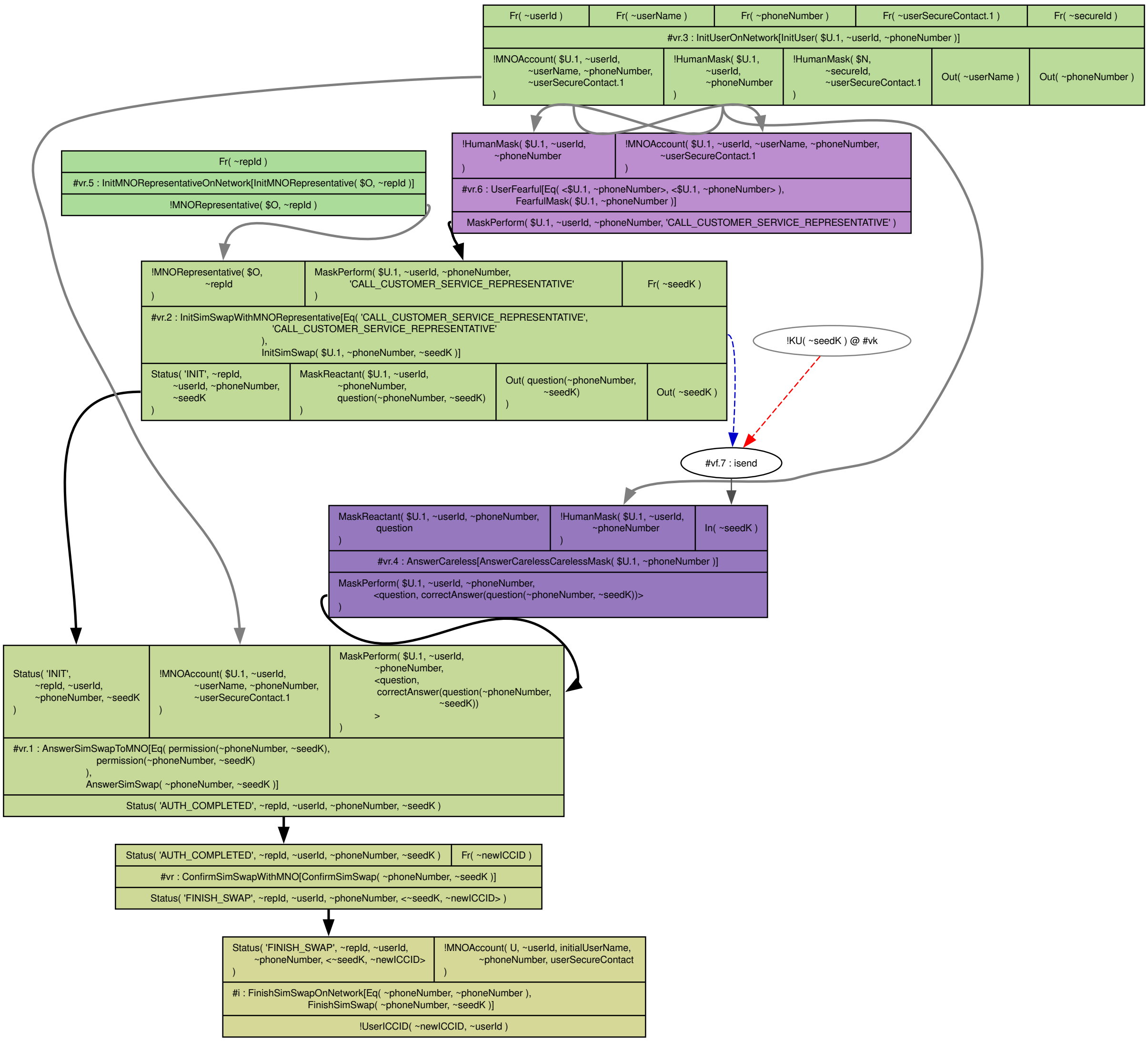
Figure 11 – Attentive Mask in the SIM swap ceremony


Fr(~userId)
Fr(~userName)
Fr(~phoneNumber)
Fr(~userSecureContact.1)
Fr(~secureId)
#vr.3 : InitUserOnNetwork[InitUser($U.1, ~userId, ~phoneNumber)]
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
!HumanMask($U.1, ~userId, ~phoneNumber)
!HumanMask($N, ~secureId, ~userSecureContact.1)
Out(~userName)
Out(~phoneNumber)
Fr(~repId)
#vr.5 : InitMNORepresentativeOnNetwork[InitMNORepresentative($O, ~repId)]
!MNORepresentative($O, ~repId)
!HumanMask($U.1, ~userId, ~phoneNumber)
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
#vr.6 : UserAttentive[Eq(<$U.1, ~phoneNumber>, <$U.1, ~phoneNumber>), AttentiveMask($U.1, ~phoneNumber)]
MaskPerform($U.1, ~userId, ~phoneNumber, 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE')
!MNORepresentative($O, ~repId)
MaskPerform($U.1, ~userId, ~phoneNumber, 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE')
Fr(~seedK)
#vr.2 : InitSimSwapWithMNORepresentative[Eq('CALL_CUSTOMER_SERVICE_REPRESENTATIVE', 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE'), InitSimSwap($U.1, ~phoneNumber, ~seedK)]
Status('INIT', ~repId, ~userId, ~phoneNumber, ~seedK)
MaskReactant($U.1, ~userId, ~phoneNumber, question(~phoneNumber, ~seedK))
Out(question(~phoneNumber, ~seedK))
Out(~seedK)
!KU(~seedK) @ #vk
#vf.7 : isend
MaskReactant($U.1, ~userId, ~phoneNumber, question(~phoneNumber, ~seedK))
!HumanMask($U.1, ~userId, ~phoneNumber)
In(~seedK)
#vr.4 : AnswerAttentive[Eq(question(~phoneNumber, ~seedK), question(~phoneNumber, ~seedK)), AnswerAttentiveAttentiveMask($U.1, ~phoneNumber)]
MaskPerform($U.1, ~userId, ~phoneNumber, <question(~phoneNumber, ~seedK), correctAnswer(question(~phoneNumber, ~seedK))>)
Status('INIT', ~repId, ~userId, ~phoneNumber, ~seedK)
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
MaskPerform($U.1, ~userId, ~phoneNumber, <question(~phoneNumber, ~seedK), correctAnswer(question(~phoneNumber, ~seedK)) >)
#vr.1 : AnswerSimSwapToMNO[Eq(permission(~phoneNumber, ~seedK), permission(~phoneNumber, ~seedK)), AnswerSimSwap(~phoneNumber, ~seedK)]
Status('AUTH_COMPLETED', ~repId, ~userId, ~phoneNumber, ~seedK)
Status('AUTH_COMPLETED', ~repId, ~userId, ~phoneNumber, ~seedK)
Fr(~newICCID)
#vr : ConfirmSimSwapWithMNO[ConfirmSimSwap(~phoneNumber, ~seedK)]
Status('FINISH_SWAP', ~repId, ~userId, ~phoneNumber, <~seedK, ~newICCID>)
Status('FINISH_SWAP', ~repId, ~userId, ~phoneNumber, <~seedK, ~newICCID>)
!MNOAccount(U, ~userId, initialUserName, ~phoneNumber, userSecureContact)
#i : FinishSimSwapOnNetwork[Eq(~phoneNumber, ~phoneNumber), FinishSimSwap(~phoneNumber, ~seedK)]
!UserICCID(~newICCID, ~userId)

Result of the execution of the rules defined by Tamarin. In this case, we have a successful execution trace where the rules execute and maintain the properties previously defined, successfully finalizing the SIM swap by an honest user. We consider, in purple, a user wearing the Attentive mask.

Source: The authors

Figure 12 – Multiple Masks in the SIM swap ceremony


Fr(~userId)
Fr(~userName)
Fr(~phoneNumber)
Fr(~userSecureContact.1)
Fr(~secureId)
#vr.3 : InitUserOnNetwork[InitUser($U.1, ~userId, ~phoneNumber)]
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
!HumanMask($U.1, ~userId, ~phoneNumber)
!HumanMask($N, ~secureId, ~userSecureContact.1)
Out(~userName)
Out(~phoneNumber)
Fr(~repId)
#vr.5 : InitMNORepresentativeOnNetwork[InitMNORepresentative($O, ~repId)]
!MNORepresentative($O, ~repId)
!HumanMask($U.1, ~userId, ~phoneNumber)
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
#vr.6 : UserFearful[Eq(<$U.1, ~phoneNumber>, <$U.1, ~phoneNumber>), FearfulMask($U.1, ~phoneNumber)]
MaskPerform($U.1, ~userId, ~phoneNumber, 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE')
!MNORepresentative($O, ~repId)
MaskPerform($U.1, ~userId, ~phoneNumber, 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE')
Fr(~seedK)
#vr.2 : InitSimSwapWithMNORepresentative[Eq('CALL_CUSTOMER_SERVICE_REPRESENTATIVE', 'CALL_CUSTOMER_SERVICE_REPRESENTATIVE'), InitSimSwap($U.1, ~phoneNumber, ~seedK)]
Status('INIT', ~repId, ~userId, ~phoneNumber, ~seedK)
MaskReactant($U.1, ~userId, ~phoneNumber, question(~phoneNumber, ~seedK))
Out(question(~phoneNumber, ~seedK))
Out(~seedK)
!KU(~seedK) @ #vk
#vf.7 : isend
MaskReactant($U.1, ~userId, ~phoneNumber, question)
!HumanMask($U.1, ~userId, ~phoneNumber)
In(~seedK)
#vr.4 : AnswerCareless[AnswerCarelessCarelessMask($U.1, ~phoneNumber)]
MaskPerform($U.1, ~userId, ~phoneNumber, <question, correctAnswer(question(~phoneNumber, ~seedK))>)
Status('INIT', ~repId, ~userId, ~phoneNumber, ~seedK)
!MNOAccount($U.1, ~userId, ~userName, ~phoneNumber, ~userSecureContact.1)
MaskPerform($U.1, ~userId, ~phoneNumber, <question, correctAnswer(question(~phoneNumber, ~seedK)) >)
#vr.1 : AnswerSimSwapToMNO[Eq(permission(~phoneNumber, ~seedK), permission(~phoneNumber, ~seedK)), AnswerSimSwap(~phoneNumber, ~seedK)]
Status('AUTH_COMPLETED', ~repId, ~userId, ~phoneNumber, ~seedK)
Status('AUTH_COMPLETED', ~repId, ~userId, ~phoneNumber, ~seedK)
Fr(~newICCID)
#vr : ConfirmSimSwapWithMNO[ConfirmSimSwap(~phoneNumber, ~seedK)]
Status('FINISH_SWAP', ~repId, ~userId, ~phoneNumber, <~seedK, ~newICCID>)
Status('FINISH_SWAP', ~repId, ~userId, ~phoneNumber, <~seedK, ~newICCID>)
!MNOAccount(U, ~userId, initialUserName, ~phoneNumber, userSecureContact)
#i : FinishSimSwapOnNetwork[Eq(~phoneNumber, ~phoneNumber), FinishSimSwap(~phoneNumber, ~seedK)]
!UserICCID(~newICCID, ~userId)

Result of the execution of the rules defined by Tamarin. In this case, we have a successful execution trace where the rules execute and maintain the properties previously defined, successfully finalizing the SIM swap by an honest user. In the shades of purple, we consider a user who starts the ceremony with the Fearful mask and switches to Careless but still finishes the ceremony, showing that masks can have correct behavior.

Source: The authors

attackers. This was because it was assumed that the human nodes would not make mistakes[2].

This attack trace assumes that a legitimate exchange occurs by a user in a time window very close to an attack being carried out on their number. Considering the SIM swap model with social authentication in Section 3.3, it can be posited that upon completion of the security question phase, the telephone network initiates a security contact and transmits the PIN of the new SIM for confirmation between peers. Suppose a security contact utilizes the Careless mask in the action-reaction pair to confirm this SIM. In that case, it will fail to verify the user's correct SIM, thereby allowing the attacker's PIN to be changed.

The aforementioned behavior could be circumvented by consensus between multiple security contacts. However, this would increase the ceremony's complexity, potentially causing inconvenience to the user. An alternative solution would be to implement measures that ensure the user is attentive at this stage. One such measure could be to require the user to enter a code sent to them rather than simply confirming it. This approach demonstrates how formal proof and user experience design can be integrated to inform the ceremony between the masks. It is evident from this example that the use of Pirandellian masks can assist protocol and ceremony developers in understanding how these ceremonies are used in real life. This is analogous to the theatre example previously discussed. It is similar to how an author's written plays will be interpreted differently than originally expected by the actors presenting them on stage.

It is also crucial to acknowledge that the execution traces contribute to interpreting the footprint of a user when fitted with masks, thereby adding semantic meaning to the analysis. This is because the semantics of the traces of execution of these masks by a user can be used to compose stories about the use of the ceremony. For example, the execution traces permit the construction of a narrative in which an attentive user, due to an external factor such as distraction, makes an error by wearing the Careless mask. This results in the user becoming fearful and unable to complete the ceremony.

The semantic content of the execution traces provides valuable insight into the optimal design of a ceremony. Understanding the underlying narrative structure makes it possible to develop a ceremony that maximizes the number of stories that lead to its completion. When designing the interface of a ceremony, attention-grabbing mechanisms can be employed to prevent a careless user from finalizing the stage through an error. This approach thus represents a promising avenue for further investigation when developing and analyzing ceremonies.

Nevertheless, integrating the diverse masks into the tests by the various human participants resulted in a more comprehensive and nuanced examination. The previously straightforward process of automatically displaying the Tamarin test results has become more complex, necessitating the proof of properties to be guided by the protocol modeler. This is because each human action and reaction can result in the execution of any mask. The combination of four human actions generates a total of 3^4 distinct execution traces previously represented by a single trace.

The three masks can be used with any of the four actions. Consequently, the number of

[2] The execution trace is available at https://github.com/LarissaGRosa/SIMSwapModel/blob/main/experiments/results/InitSimSwapWithMNORepresentative_social_auth.pdf

potential execution traces will increase based on the number of masks and possible human actions within a ceremony. This is a significant challenge for larger and more complex ceremonies, necessitating further research to enhance the implementation of the masks, thereby reducing the number of traces at higher complexities. The experiments for this section may be found in https://github.com/LarissaGRosa/SIMSwapModel.

5 CONCLUSION

We examined the concepts of security protocols and ceremonies, intending to understand their significance for maintaining security in the digital world, their operational principles, and the open problems associated with them. In this context, we identified the SIM swap ceremony, which is employed by mobile phone operators in the event that a user has a SIM card that is no longer viable for use, either due to theft or misuse. This ceremony was further studied to understand its problems, which, as we saw in our work, can lead to financial loss to users, and also as a model to study new concepts in security ceremony analysis.

In light of the various methods employed by MNOs to standardize this process, we proposed a generic model for transmitting information between the parties, including users, mobile network operators, and customer service representatives. This was initially formulated in epistemic logic and subsequently implemented using Tamarin. As previously demonstrated in Section 3.3, this initial model, which incorporates the potential for attackers to impersonate users and corrupt representatives, exhibited a range of attacks that closely align with those observed in empirical analyses. Furthermore, the model proved to be an effective tool for testing changes to these processes to mitigate the aforementioned problems.

To contribute to this field of study, we have developed a modified version of the conventional SIM swap, in which the process is completed through security contacts. In consideration of the properties and granularity of our model in the L3 layer, where we do not allow for other human behavioral issues besides active attacks, at this point in our study, we have a SIM swap that can overcome all the defined properties. Nevertheless, examining the layers of the concertina system reveals that the granularity of our model can be refined to closely approximate human behavior.

In Chapter 4, we introduce the concept of Pirandellian Masks for modeling human behavior between the L3 and L4 layers of the concertina ceremony as defined by Martimiano & Martina (2022). We looked at how these concepts differed from other approaches to modeling human behavior and showed their implementation using the Tamarin formal verification tool. This initial implementation proved relevant for understanding how different users wearing such masks behave when performing a ceremony and how we can compose such masks and create stories about scenes.

By extending our initial modeling to the use of masks, we identified potential attacks in our modified version of SIM swap, demonstrating the potential of this tool for analyzing ceremonies. By examining the concept of human actions and reactions that occur through a mask, we gain insight into the narratives surrounding the use of ceremonies by their users. This understanding can inform the design of new implementations to maximize the number of success stories. For instance, it is possible to incorporate UX design elements that prompt users to prioritize specific steps in a ceremony. This can help users who wear the Careless mask avoid making mistakes.

However, as a primary consideration, this mask model was developed with SIM swap in mind and with Tamarin, a theorem prover. Consequently, constraints are associated with the number of steps required for proof in Tamarin, as evidenced in Chapter 4. These limitations have a detrimental impact on the number of human actions and masks that can be analyzed. As future work, the objective is to generalize these masks so they can be tested in other ceremonies and ways of proving theorems. It is also necessary to identify methods that reduce the complexity of these proofs.

Consequently, our work, which aimed to model the SIM swap ceremony and contribute to the study of human entities in them, has resulted in a formal description, in Tamarin, of the same protocols at different levels of granularity concerning human behavior. Furthermore, we have included the initial implementation of Pirandellian masks, as proposed by Martimiano & Martina (2022), as a contribution to studying human entities in such ceremonies. As is well known, the modeling process is iterative and can be improved. Consequently, we leave it as future work to further increase the detail of our models on both fronts, namely the study of SIM swap and its problems and the study of human entities through Pirandellian masks.

BIBLIOGRAPHY

ANDREWS, N. " can i get your digits?": Illegal acquisition of wireless phone numbers for sim-swap attacks and wireless provider liability. **Nw. J. Tech. & Intell. Prop.**, HeinOnline, v. 16, p. 79, 2018.

ARSAC, W. et al. Validating security protocols under the general attacker. In: SPRINGER. **Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security**. [S.l.], 2009. p. 34–51.

AVALLE, M.; PIRONTI, A.; SISTO, R. Formal verification of security protocol implementations: a survey. **Formal Aspects of Computing**, Springer, v. 26, p. 99–123, 2014.

BASIN, D.; MÖDERSHEIM, S.; VIGANO, L. Ofmc: A symbolic model checker for security protocols. **International Journal of Information Security**, Springer, v. 4, p. 181–208, 2005.

BASIN, D.; RADOMIROVIC, S.; SCHMID, L. Modeling human errors in security protocols. In: IEEE. **2016 IEEE 29th Computer Security Foundations Symposium (CSF)**. [S.l.], 2016. p. 325–340.

BAU, J.; MITCHELL, J. C. Security modeling and analysis. **IEEE Security & Privacy**, v. 9, n. 3, p. 18–25, 2011.

BELLA, G.; COLES-KEMP, L. Layered analysis of security ceremonies. In: SPRINGER. **Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27**. [S.l.], 2012. p. 273–286.

BELLA, G.; CURZON, P.; LENZINI, G. Service security and privacy as a socio-technical problem. **Journal of Computer Security**, Ios Press, v. 23, n. 5, p. 563–585, 2015.

BELLA, G.; GIUSTOLISI, R.; LENZINI, G. Socio-technical formal analysis of tls certificate validation in modern browsers. In: IEEE. **2013 Eleventh Annual Conference on Privacy, Security and Trust**. [S.l.], 2013. p. 309–316.

BELLA, G.; GIUSTOLISI, R.; SCHÜRMANN, C. Modelling human threats in security ceremonies. **Journal of Computer Security**, IOS Press, v. 30, n. 3, p. 411–433, 2022.

BELLA, G. et al. Perceptions of beauty in security ceremonies. **Philosophy & Technology**, Springer, v. 35, n. 3, p. 72, 2022.

BIASIN, G.-P.; GIERI, M. et al. **Luigi Pirandello: Contemporary Perspectives**. [S.l.]: University of Toronto Press, 1999.

BRAGHIN, C.; LILLI, M.; RICCOBENE, E. A model-based approach for vulnerability analysis of iot security protocols: The z-wave case study. **Computers & Security**, Elsevier, v. 127, p. 103037, 2023.

CANETTI, R.; KRAWCZYK, H. Analysis of key-exchange protocols and their use for building secure channels. In: SPRINGER. **International conference on the theory and applications of cryptographic techniques**. [S.l.], 2001. p. 453–474.

COINTELEGRAPH. **“Sim swap”: Conheça o golpe que roubou 4 Milhões dos Seguidores do Criador da Ethereum**. 2023. Https://exame.com/future-of-money/sim-swap-conheca-o-golpe-que-roubou-r-4-milhoes-dos-seguidores-do-criador-da-ethereum/.

DAVIS, E.; MORGENSTERN, L. Epistemic logic and its applications: Tutorial notes. In: CITESEER. **International Joint Conferences on Artificial Intelligence**. [S.l.], 1983. v. 93.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. In: **Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman**. [S.l.: s.n.], 2022. p. 365–390.

DOLEV, D.; YAO, A. On the security of public key protocols. **IEEE Transactions on Information Theory**, v. 29, n. 2, p. 198–208, 1983.

EKEH, G. et al. Awareness of bvn, sim swap and clone frauds: Methods and controls. **Science World Journal**, v. 17, n. 2, p. 200–206, 2022.

ELLISON, C. Ceremony design and analysis. **Cryptology EPrint Archive**, 2007.

ENISA, E. U. A. for C. **Countering sim-swapping: overview and good practices to reduce the impact of SIM swapping attacks.** Publications Office, 2021. Disponível em: https://data.europa.eu/doi/10.2824/252043.

FITTING, M.; MENDELSOHN, R. L. **First-order modal logic**. [S.l.]: Springer Nature, 2023. v. 480.

GOLDBLATT, R. I. Metamathematics of modal logic. **Bulletin of the Australian Mathematical Society**, Cambridge University Press, v. 10, n. 3, p. 479–480, 1974.

GUDIMALLA, T. K. M.; KANNAN, S. et al. Survey analysis of cloned sim card. In: **Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT)**. [S.l.: s.n.], 2019.

HAIDAR, A. N.; ABDALLAH, A. E. Formal modelling of pki based authentication. **Electronic Notes in Theoretical Computer Science**, Elsevier, v. 235, p. 55–70, 2009.

HATUNIC-WEBSTER, E. Modelling anti-phishing authentication ceremonies. Technological University Dublin, 2019.

HERZOG, J. A computational interpretation of dolev–yao adversaries. **Theoretical Computer Science**, Elsevier, v. 340, n. 1, p. 57–81, 2005.

HIGíDIO, J. **Meta, Microsoft e TIM devem indenizar vítima de golpe do SIM swap — conjur.com.br**. 2023. https://www.conjur.com.br/2023-nov-26/meta-microsoft-e-tim-devem-indenizar-vitima-de-golpe-do-sim-swap/. [Accessed 19-04-2024].

HOLLICK, M. et al. Toward a taxonomy and attacker model for secure routing protocols. **ACM SIGCOMM Computer Communication Review**, ACM New York, NY, USA, v. 47, n. 1, p. 43–48, 2017.

IC3. **Internet Crime Complaint Center (IC3) | Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public — ic3.gov**. 2022. https://www.ic3.gov/Media/Y2022/PSA220208. [Accessed 19-04-2024].

JOHANSEN, C.; JØSANG, A. Probabilistic modelling of humans in security ceremonies. In: SPRINGER. **Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance: 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014. Revised Selected Papers 9**. [S.l.], 2015. p. 277–292.

JORDAAN, L.; SOLMS, B. V. A biometrics-based solution to combat sim swap fraud. In: SPRINGER. **Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers**. [S.l.], 2011. p. 70–87.

KAMARZADEH, S. The impact of anthropology on "six characters in search of an author", the great italian play by luigi pirandello. **Revista Hipótese**, v. 2, n. 1, p. 171–189, 2016.

KARLOF, C.; TYGAR, J. D.; WAGNER, D. A. Conditioned-safe ceremonies and a user study of an application to web authentication. In: **NDSS**. [S.l.: s.n.], 2009.

KIM, M.; SUH, J.; KWON, H. A study of the emerging trends in sim swapping crime and effective countermeasures. In: **2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)**. [S.l.: s.n.], 2022. p. 240–245.

KOZMAI, D. **Converting tamarin to extended alice&bob protocol specifications**. Tese (Doutorado) — Bachelor's Thesis, ETH, Zürich, 2016.

LEE, K. et al. An empirical study of wireless carrier authentication for {SIM} swaps. In: **Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)**. [S.l.: s.n.], 2020. p. 61–79.

MARTIMIANO, T.; MARTINA, J. E. Six characters in search of a security problem: Pirandellian masks for security ceremonies. In: SBC. **Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. [S.l.], 2022. p. 344–357.

MEIER, S. et al. The tamarin prover for the symbolic analysis of security protocols. In: SPRINGER. **Computer Aided Verification: 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings 25**. [S.l.], 2013. p. 696–701.

MEYER, J.-J. C.; MEYER, J.-J. C.; HOEK, W. van der. **Epistemic logic for AI and computer science**. [S.l.]: Cambridge University Press, 2004.

MÖDERSHEIM, S. **Protocol security verification tutorial**. [S.l.], 2018.

NOBEL, P.; OUTREACH, A. **The Nobel Prize in Literature 1934 — nobelprize.org**. 2024. https://www.nobelprize.org/prizes/literature/1934/summary/. [Accessed 20-05-2024].

PAULSON, L. C. The inductive approach to verifying cryptographic protocols. **Journal of computer security**, IOS Press, v. 6, n. 1-2, p. 85–128, 1998.

PAULSON, L. C. The yahalom protocol. In: SPRINGER. **Security Protocols: 7th International Workshop, Cambridge, UK, April 19-21, 1999. Proceedings 7**. [S.l.], 2000. p. 78–84.

PAULSON, T. N. L. C.; WENZEL, M. **A Proof Assistant for Higher-Order Logic**. 2013.

PEDERSEN, T.; JOHANSEN, C.; JØSANG, A. Behavioural computer science: an agenda for combining modelling of human and system behaviours. **Human-centric Computing and Information Sciences**, Springer, v. 8, p. 1–20, 2018.

PIRANDELLO, L. **Tonight We Improvise; And," Leonora, Addio!"**. [S.l.]: Biblioteca di Quaderni d'italianistica, 1987. v. 3.

PIRANDELLO, L. Illustratori, attori e traduttori. Zanichelli, 2011.

PIRANDELLO, L. Sei personaggi in cerca d'autore. Zanichelli, 2011.

RADKE, K. et al. Ceremony analysis: Strengths and weaknesses. In: SPRINGER. **Future Challenges in Security and Privacy for Academia and Industry: 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, June 7-9, 2011. Proceedings 26**. [S.l.], 2011. p. 104–115.

RAM, S. B.; ODELU, V. Security analysis of a key exchange protocol under dolev-yao threat model using tamarin prover. In: **2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)**. [S.l.: s.n.], 2022. p. 0667–0672.

RENDSVIG, R.; SYMONS, J.; WANG, Y. Epistemic logic. 2019.

SCHMIDT, B. **Formal analysis of key exchange protocols and physical protocols**. Tese (Doutorado) — ETH Zurich, 2012.

SCHMIDT, B. et al. Automated analysis of diffie-hellman protocols and advanced security properties. In: **2012 IEEE 25th Computer Security Foundations Symposium**. [S.l.: s.n.], 2012. p. 78–94.

SEMPREBONI, D.; VIGANò, L. X-men: A mutation-based approach for the formal analysis of security ceremonies. In: **2020 IEEE European Symposium on Security and Privacy (EuroS&P)**. [S.l.: s.n.], 2020. p. 87–104.

WILLIAM, S. et al. **As You Like It**. [S.l.]: Sheba Blake Publishing., 1901.

ZACHARIAS, T. **The DEMOS family of e-voting systems: End-to-end verifiable elections in the standard model**. Tese (Doutorado) — PhD thesis, National and Kapodistrian University of Athens, 2016.

ZINZINDOHOUÉ, J.-K. et al. Hacl*: A verified modern cryptographic library. In: **Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security**. [S.l.: s.n.], 2017. p. 1789–1806.

6 APPENDIX A – ARTIGO DO TCC

Modeling the SIM Swap Ceremony: Integrating Human Behavior and Formal Analysis

Larissa Gremelmaier Rosa[1]

[1]Departamento de Informática e Estatística – Centro Tecnológico
Universidade Federal de Santa Catarina (UFSC)

larissa.gremelmaier.rosa@grad.ufsc.br

Abstract. *Our study examines SIM swap as a security ceremony, integrating technical protocols and human interactions. Using formal models and empirical evaluation, we use a layered approach to analyze this ceremony, focusing on human-computer and personal interactions. We investigate phases and agents involved in SIM swapping, identifying vulnerabilities and opportunities for improvement. We expanded the scope to include studies of human entities, applying Pirandellian masks to model these ceremonies. We developed a formal SIM exchange model to increase security on multiple levels, considering process steps, possible attacks, and human behavior. We demonstrate that Pirandellian masks are crucial for ceremonial analysis, integrating theory and practice to optimize the security and effectiveness of SIM exchange.*

Resumo. *Nosso estudo examina a troca de SIM como uma cerimônia de segurança, integrando protocolos técnicos e interações humanas. Utilizamos uma abordagem em camadas para analisar essa cerimônia, focando nas interações humano-computador e pessoais, usando modelos formais e avaliação empírica. Investigamos fases e agentes envolvidos na troca de SIM, identificando vulnerabilidades e oportunidades de melhoria. Expandimos o escopo para incluir estudos sobre entidades humanas, aplicando máscaras pirandellianas na modelagem dessas cerimônias. Desenvolvemos um modelo formal de troca de SIM para aumentar a segurança em múltiplos níveis, considerando etapas do processo, possíveis ataques e comportamentos humanos. Demonstramos que as máscaras pirandellianas são cruciais para análise cerimonial, integrando teoria e prática para otimizar a segurança e eficácia da troca de SIM.*

1. General Information

Digital security is a constant concern where the integrity and confidentiality of data are essential for a wide range of organizations. Several mechanisms have been developed to protect sensitive systems. In this sense, *security protocols* are imperative as it is a set of communication procedures designed to achieve a specific goal in an environment where there is a constant threat of interference from an attacker [Avalle et al. 2014].

Given the importance of achieving certain security goals, exhaustive studies to assert the correctness of security protocols are necessary, typically performed through mathematical techniques and tools [Avalle et al. 2014, Bau and Mitchell 2011]. This process consists of (i) defining a protocol model, (ii) understanding the properties it must maintain, (iii) modeling the attacker, and then (iv) subjecting it to a verification technique such as automated theorem proving [Bau and Mitchell 2011].

Despite the rigor these protocols undergo in the verification stage, they still fail when applied to real use cases [Bella et al. 2015]. Protocols and their models often disregard socio-technical interactions between users and systems, neglecting the human element when designing security results in vulnerabilities that technical solutions alone cannot solve [Bella et al. 2015]. Understanding the psychology and behaviors of users is crucial in developing effective security measures.

In this sense, security ceremonies emerge as a comprehensive approach that goes beyond traditional protocols, incorporating a variety of factors, from operating systems to human interactions [Bella and Coles-Kemp 2012]. The concept of a security ceremony allows us to perceive the processes of a Mobile Network Operator (MNO) as multiple examples of such ceremonies. The MNO incorporates several elements presented in ceremonies, including the protocols used in Internet networks, users, customer service representatives, and attackers.

Among these processes, the SIM swap case is an interesting example of how security protocols fail when considered within a wider social context. Before explaining precisely how this happens, we must examine how MNOs operate. Wireless service is linked to a mobile device's SIM card, with MNOs managing the association between phone numbers and SIMs. Each phone number is typically tied to one SIM card and vice versa. SIM cards facilitate the BYOD policy, allowing users to bring their own devices if not locked to another carrier, and a new SIM is purchased [Lee et al. 2020]. Users can easily switch devices by transferring service to a new SIM card by providing the new SIM's ICCID to the mobile provider and then inserting it into the new device [Lee et al. 2020].

If a user wishes to move their number to another SIM for some reason that makes it impossible to use the old one, they need to perform a SIM swap operation. However, in a social context, this operation is susceptible to attacks from different human nodes, thus failing to ensure that only the user who owns the telephone line succeeds in completing the goal. For example, a malicious actor can use social engineering to trick or bribe a telephone line operator or customer service representative to assume that they own the SIM number and then perform an illegal SIM swap [Andrews 2018].

This scam is commonly referred to as equivalent in the literature as a SIM swap attack, which can potentially damage its targets. As the phone number is constantly used in the two-factor authentication process, an actor in possession of a user's phone number has the power to gain access to service accounts from banks to cryptocurrency wallets, thus causing losses that could reach millions of dollars [Andrews 2018]. Crimes like this are becoming increasingly common, especially with the adoption of eSIM in many countries [Kim et al. 2022].

These frauds could be foreseen or mitigated by studying the SIM swap process as a security ceremony. However, developing methodologies to analyze ceremonies, considering the complexity of human interactions, is a challenge. This is illustrated by a study of the HTTPS protocol running in the Opera Mini browser and its users, conducted by

[Radke et al. 2011]. The authors have shown that usage context can lead to the emergence of various user personas, potentially prompting a system to accommodate multiple security ceremonies. As such, several studies are being undertaken to facilitate the analysis of these ceremonies [Bella and Coles-Kemp 2012, Basin et al. 2016].

In particular, the *Security Ceremony Concertina* approach is useful as it breaks down the complexity of this analysis by creating layers and interfaces to communicate across them [Bella and Coles-Kemp 2012]. This method distinguishes a security ceremony into five layers: (L1) Informational; (L2) Operating System; (L3) Human-Computer Interaction; (L4) Personal; (L5) Communal. Following the definitions brought by this method, the most common studies to model the security protocol are in L1 and L2.

According to the authors, the study of L3 and L4 is complex due to the non-deterministic nature of humans. Research into these layers is domain-specific and involves aspects such as the definition of personas and the modeling of human threats [Bella et al. 2015, Basin et al. 2016]. Most recently, [Martimiano and Martina 2022] conceptually defined the idea of using *Pirandellian Masks* as a means of analyzing humans in L4.

Considering the above, the purpose of our study is to formally model the SIM swap process, incorporating layers L3 and L4 of the Concertina Security Ceremony. Hereafter, it is defined as the SIM swap ceremony. The formal modeling of this ceremony at the L1 and L2 layers was not found in the literature. However, we don't present it in our work as the implementation of this protocol differs between mobile network operators (MNOs) and is not public.

We use those models to compare with the attacks obtained in empirical studies and establish a prototype to test changes to this ceremony aiming to improve its security. At the same time, we strive to contribute to research into such ceremonies, applying methods defined for analyzing these layers and identifying approaches to facilitate their integration into real contexts. More specifically, we build initial implementations of the concept of Pirandellian Masks, explained by [Martimiano and Martina 2022], in the context of the SIM swap ceremony and thus understand how we can use them to comprehend specific parts of security ceremonies in terms of human entities and their formal modeling and analysis.

2. Literature Review

Considering the *Security Ceremony Concertina* layers, we revise the state of the art in the ceremony field, aiming to categorize in the given layers. Considering the ceremony concertina, it is important to define that L1 is about the underlying security protocol and L5 englobes society as a whole. This helps us to understand the state of the art in security ceremonies and how the present work fits into this panorama. We focus, for the most part, on review research in L3, considering human-computer interaction, and L4, human behavior.

L1 is where most of the classic work in the literature can be found, such as that defined in [Schmidt et al. 2012], [Haidar and Abdallah 2009], and [Canetti and Krawczyk 2001]. More recently, work along these lines has extended to the formal verification of protocols applied to the Internet of Things (IoT), such as the case study proposed by [Braghin et al. 2023] for Z-Wave. In this work, the authors have performed the formal specification of the Z-Wave IoT protocol using the S2 security class.

Working on L3, [Johansen and Jøsang 2015] proposes a probabilistic model (rather than the classical non-deterministic one) to model the actions of human agents. In this sense, the authors advocate separating the model of the human from the user interface, using the notion of "personas", defined as a finite set of social and cognitive attributes that make up a person. Their work may be seen as a possible definition of a common actor between L3 and L4, in which the personas will trigger actions in the user interface model presented as a finite state machine.

The study by [Basin et al. 2016] focuses on modeling human limitations and errors, considering the problem that the human nodes are the most vulnerable part of the ceremonies. Similarly, [Bella et al. 2022a] works on modeling how the interaction between these nodes affects the safety of the ceremony. Finally, [Sempreboni and Viganò 2020] models human mistakes as mutation rules. All three works are situated in L3 and L4 of the concertina methodology and attempt to establish an interface between these layers. However, they do not delve into human expressions to gain an understanding of the social context in which they are situated.

Also, by understanding these layers, [Pedersen et al. 2018] argues that during interaction with ceremonies, users are influenced by their experiences and mental states, leading to biased choices when dealing with protocols. The authors proposed that incorporating behavioral models into the development of systems would facilitate the simulation of authentic human behavior and the design of interfaces that would enable individuals to make more accurate decisions when interacting with automated systems.

Similarly, [Bella et al. 2022b] says that despite efforts to improve the usability of these ceremonies, end users do not seem to be attracted to them. This study explores whether beautification can make ceremonies more attractive. Three studies were conducted to identify the dimensions of "beautiful ceremonies" and how people perceive them. It concludes that the beauty of security ceremonies lies in the perspective of those who observe them, but there are challenges in balancing security with usability improvements and beautification.

In their respective papers, [Pedersen et al. 2018] and [Bella et al. 2022b] address the issue of understanding the human nodes and their interactions within the system from two theoretical perspectives. Additionally, it would be beneficial to utilize a framework that can be applied to formal analysis to comprehend the impact of human conduct and expressions upon and in response to the ceremony. In this context, the concept of masks proposed by Pirandello can be employed to elucidate the nuances associated with the security ceremony as outlined by [Martimiano and Martina 2022].

Pirandellian masks come from the play developed by Luigi Pirandello entitled *Sei personaggi in cerca d'autore* [Pirandello 2011] and define the problems of transforming art into reality that make up the action of transposing the idea of a play and its characters into the duality of stage and actors. He discusses the masks that authors must wear to define reality on stage. The authors suggest discussing users and how they understand and interact with security ceremonies to propose solutions incorporating meta-design strategies. The authors conceptually define masks that could be used in the context of the ceremonies and comment on how they could be implemented using Tamarin [Meier et al. 2013]. The work leaves future implementations and how it could be used to design a full framework for studies in L3 and L4 as future work.

In this sense, our work adds to the state of the art by initially implementing these masks in Tamarin within a defined ceremony. Our goal is to gather data on how to use them to build a full framework encompassing the entire ecosystem surrounding Pirandellian masks and their application to understanding human nodes and their relationship with security ceremonies. This proposal differs from others presented for the study of layers L3 and L4 in that it extends the modeling of human nodes to include, in addition to errors, an understanding of human behavior relating to ceremonies in spheres that encompass emotions and behavior. It differs from the work of [Pedersen et al. 2018] and [Bella et al. 2022b], as mentioned above, in its concern with adding these characteristics within a formal framework.

3. SIM swap Ceremony Use Case

The SIM swap ceremony is the foundation for our investigations into Pirandelian masks. The ceremony was selected for two reasons: first, it involves different human actors, and second, it has not been formally modeled. This chapter presents empirical studies on the same ceremony and the problems in human entities and their nodes that lead to security failures and fraud. These problems cause financial damage to several users. In addition, we show a formal model of the actions involving these nodes within the ceremony, using Tamarin, to portray how these errors can occur when certain nodes fail. The understanding of the human condition that leads to error is provided in Section 5 and involves the implementation of a subset of the Pirandelian masks.

A Subscriber Identification Module, known as a SIM, is a smart card that contains a chip and identifies a user on a particular mobile network. The SIM is usually inserted into a smartphone and allows users to access SMS, internet, voice calls, and more services. As [Gudimalla et al. 2019] explains, the SIM stores several pieces of information that are fundamental to mobile network operators, such as the International Mobile Subscriber Identity (IMSI), the Integrated Circuit Card ID (ICCID), and the Authentication Key (Ki). SIM cards have processors that can carry out simple tasks such as receiving and forwarding a call request, signing data, etc. They also contain a few kilobytes of RAM and algorithms capable of generating pseudo-random numbers and encryption keys [Gudimalla et al. 2019].

Mobile Network Operators, hereafter MNOs, map the SIM cards of their customers to provide the service. In this way, they are responsible for maintaining a database containing the relationship between the phone numbers and the SIM, usually defined as a one-to-one relationship [Lee et al. 2020]. Most of the time, the SIM card can be moved between devices and is subject to situations involving damage, loss, or even changing phones, as the SIM card can be of different sizes and needs to be adapted to suit the new device [Ekeh et al. 2022, Gudimalla et al. 2019].

When something happens that makes it impossible to use the SIM card, the mobile network user can choose to keep their phone number and carry out a SIM swap operation. You can keep your phone number and account while changing SIMs. As commented in the study by [Lee et al. 2020], these operations vary according to each MNO and involve authenticating the user using different information. Nevertheless, we have used the data from their study to define the generic operations involved in the SIM swap ceremony, as shown in Figure 1.

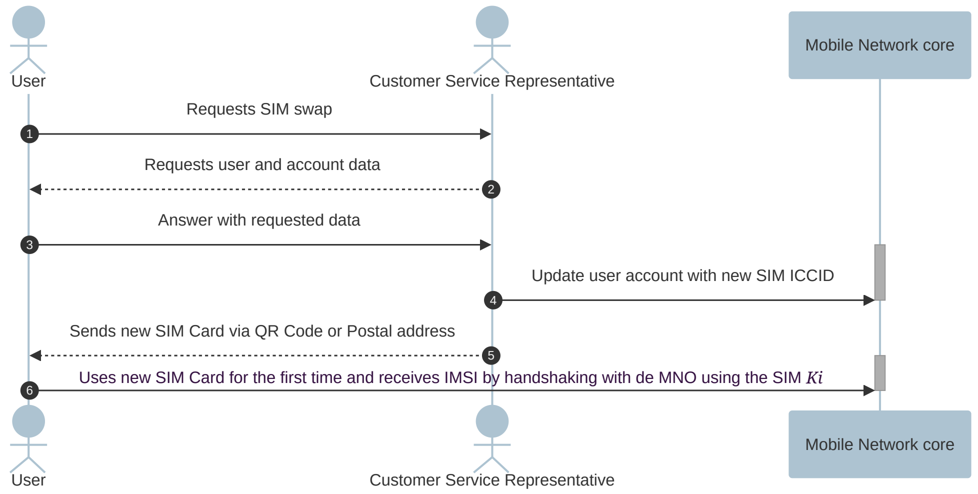

User
Customer Service Representative
Mobile Network core
Requests SIM swap
1
Requests user and account data
2
Answer with requested data
3
Update user account with new SIM ICCID
4
Sends new SIM Card via QR Code or Postal address
5
Uses new SIM Card for the first time and receives IMSI by handshaking with de MNO using the SIM Ki
6
User
Customer Service Representative
Mobile Network core

Figure 1. Generic SIM swap Ceremony based in [Lee et al. 2020]

Using Figure 1 as a basis for discussion, it is possible to see two human entities actively participating in the portrait ceremony: the user and the customer service representative. In this case, the objective is for the service representative to authenticate the user and for the MNO core to validate the SIM swap. Six steps are involved in the progress of this ceremony towards its objectives. First, a user requests a customer service representative to start the swap process. Then, the service representative returns a series of authentication challenges for the user to pass. Once these security questions have been answered, he will request that the old SIM be disconnected from the user account and that a new SIM be connected. Other steps involve the network confirming the SIM swap, returning the request to the user, and defining the IMSI code used to identify a subscriber in a mobile network uniquely.

In practice, the authentication challenges phase varies among implementations. In the United States alone, five types of challenges classes have been identified: personal information, account information, device information, usage, knowledge, and possession [Lee et al. 2020]. For instance, the challenge may be to confirm the email address or date of birth provided when registering with the MNO, payment details such as card numbers and recent telephone numbers, or to verify passwords and one-time passcodes sent by email or SMS [Lee et al. 2020].

[for Cybersecurity ENISA 2021], known as the European Union Agency for Cyber Security, conducted a study on this issue, looking at how SIM swaps work in 48 MNOs in 22 European Union countries. The study found different procedures for swapping, categorized into offline processes, such as going to an MNO physical shop, and online/telephone-based processes, which involve communicating with a customer service representative remotely. The same study identified challenges for this process, including those reported in the [Lee et al. 2020]. In addition, [for Cybersecurity ENISA 2021] notes that when user authentication occurs in physical shops, it mainly includes identity checks based on official EU documents.

After authenticating the user, the MNO completes the swap process. According to the [for Cybersecurity ENISA 2021] study, this process also differs between online and offline SIM swaps. In the former case, the physical SIM card is delivered to the postal address provided by the customer or a QR code is sent online to activate an eSIM. In the offline case, the customer is asked to go to the MNO retail store to receive the physical SIM card or a QR code to activate the eSIM.

Although many MNOs worldwide use SIM swap practices, they are insecure and allow attacks using social engineering techniques to steal the phone numbers of arbitrary network users. As explained by [Andrews 2018], the attack starts by finding the phone number and the MNO associated with a targeted user. Then, the attacker starts a SIM swap request for that number. Usually, the online form is used to carry out this scam. The attacker is then given a challenge, which they can answer correctly or incorrectly. This is a social problem, as the attacker must somehow convince the operator to make the exchange, which can be done in several ways, including bribery. The attacker starts operating the phone number of the target user by convincing the operator.

The success of these attacks has affected individuals in several countries, with cases reported in the European Union, the United States, the United Kingdom, Canada, Korea, and Nigeria [Kim et al. 2022]. These losses occur because the phone number is one of the two-factor authentication methods commonly used in applications that contain important functionalities [Andrews 2018]. Examples include banking applications, where a successful attack leads to direct financial loss.

Vitalik Buterin, the co-founder of Ethereum, had his X (former Twitter) account hacked. The report published by [Cointelegraph 2023] indicated that the attackers used the above practices to access the account and publish invalid NFC offers, which tricked several of his followers into buying these NFCs. The total loss to the victims was U$ 691,000. Looking at the 2021 data collection, the Internet Crime Complaint Centre, linked to the FBI, received 1,611 reports of attacks involving SIM swaps [IC3 2022]. These resulted in financial losses totaling $6.8 million.

4. Modelling the SIM swap ceremony

Despite being a very important ceremony, SIM swap still suffers from several problems, most of which involve manipulating human entities. Motivated by this, our research aims to formalize this ceremony, focusing mainly on the layers of computer-human interaction (L3 of the security ceremony concertina), where each human entity node talks to another through a network interface and has no physical access to the other.

We are interested in showing how the human nodes may or may not cooperate with the attacker and thus help the attack discussed previously. Therefore, in the next parts of this research, studies are carried out to include L4 of the concertina ceremony and extend this discussion to use the concept of Pirandellian masks to understand how this cooperation can occur by linking intention and behavior to human entity nodes.

It is important to define that we use the generic SIM swap model shown in Figure 1. Therefore, the information required for user validation is defined as random data part of a system of equations tallied by human entity nodes. This choice was made to make the model as generic as possible. It should also be noted that this modeling will aim to validate the models of this ceremony, which will take place online, i.e., without the human entities meeting in person.

We model and analyze our ceremony using the Tamarin prover [Meier et al. 2013], a tool for a formal model of security protocols that can be used in the ceremony context. Following the Tamarin grammar, an arbitrary piece of information x about a user U on the network can be defined by Fr(x:fresh). We consider as part of a user information set iccid and imsKi, which are data about the SIM card used by the user when registering with the MNO, initialUserName and initialUserPhoneNumber as data about the person behind the user, and userId as the ID of a user on an MNO.

A Tamarin rule of type $[\ \ ]--[\ \ ]->[\ \ ]$ will consume this data and send the information as knowledge to the MNO involving data about UserAccount, among others. Furthermore, Tamarin has communication channels for an insecure network that assumes a Dolev-Yao attacker. Using the Out(x) output facts, we can send data that we consider the attacker will know, in this case, a target user's name and telephone number.

We have created similar rules to define a customer service representative in MNO. Another important fact to note is that the entities U, M, and C are represented in Tamarin as prefixed public variables in the form $X. To model the SIM swap itself, four rules have been created, which, similarly to the logical model, include the start of the process, the answering of the authentication questions, the confirmation of the answers by the customer service agent, and the completion by the network, which generates a new iccid and its relationship with the user account, indicating that the process has been successfully finished.

The rule that starts the SIM Swap process receives a Customer Service Representative as input facts, represented by !Operator(O, opId), the data that references the number that will be SIM swapped, In(initialUserPhoneNumber) and a random Fr(seedK:fresh). The first fact is used to define which representative is answering the call. The fact In(initialUserPhoneNumber) comes from a network that the attacker can manipulate, i.e., an attacker or a user can send it. Finally, Fr(seedK:fresh) is used to calculate the security question for a request to maintain its arbitrary properties within the set of possible knowledge-based authentication methods.

When the InitSimSwapWithOperator rule is executed, there will be an execution trace that stores the telephone number and the seed used to define the user security question. Thus, a question is described from the equation question(T, K), which receives a telephone number and a seedK. The output of this first stage of the process is a control fact that indicates to the system that a telephone number has been added and the output to the network of the question and the seedK used to generate the question. This knowledge is placed on the network employing facts of the type Out(), i.e., they may be known to an attacker.

For the next step of the SIM swap, the user must receive the question and then answer it for the Customer Service Representative. The way to obtain approval for this operation is through the relationship answers(T, K, correctAnswer(question(T, K))) = permission(T, K), where the representative needs to get the permission(T, K) where T is the phone number and K the seedK used to find the question being answered. A user can calculate this because they know the correctAnswer(question(T, K)). In this way, the answering step receives input facts from the system state indicating that a SIM swap process has been started, and the question asked solves the equation that guarantees the correct answer and permission and sends it to the system.

An attacker can get the data needed to calculate these equations and respond correctly in this phase. Rules that model this behavior on the part of an attacker have also been added. The remaining rules refer to how the system finishes the SIM swap. We considered that the information of a user could be attacked and thus discovered, but the customer service representative would always be reliable. We tested the system for two properties:

Property 1 (Authenticity of Initiator) *For every completed SIM swap request, an honest user initiates the request and answers the authentication questions correctly.*

Property 2 (Knowledge Integrity) *It can not be that a Customer Service Representative has approved the SIM swap, and the attacker knows the authentication answers of any user without having carried out an external attack on the data.*

The Property 2 holds in all execution traces. However, considering the possibility of a data attack, Property 1, only the owner can perform SIM swap, has two execution traces. The first trace is honest and includes all the necessary steps between the actors in the process. The second trace exhibits how it is possible to attack the information and allow an attacker to impersonate an honest user.

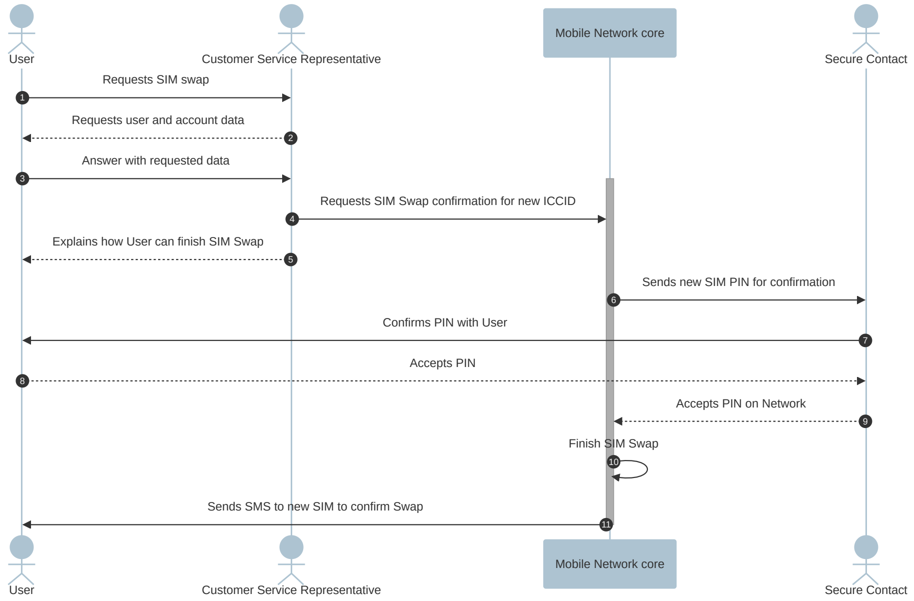
We may see that the modeling generates an attack flow that starts with a user entering the network, considering all his data. At this point, the encoding gives the attacker the username and phone number, as we believe this is common knowledge at the start of the attack and necessary to identify the victim. The attacker then attacks the data and uses the operation result (modeled as an output fact) to communicate with an operator on the network and correctly answer the questions that validate the user.

In addition to the attack that actively involves stealing information, we modeled a rogue Customer Service Representative. The execution trace generated is similar to the one mentioned above and consists of the representative forcing the SIM swap without any validation from the user. Similarly, rules were created to help with this type of attack. At this stage, cooperation between the two attacking nodes was not considered.

The interesting thing about these results is that we can see how the formal model of the security ceremony, although still initial, is similar to what was found empirically in the analyses presented in the previous sections, both in terms of how the SIM swap takes place and in terms of how fraud can occur if the human nodes are dishonest. In this way, it can be used to study improvements to the system and enable studies to make it more secure.

To illustrate this possibility, we have developed a modified version of the SIM swap ceremony, in which the phase after user verification is updated so that it can only be performed by security contacts. In this sense, users who register on the network specify a set of trusted contacts (whose change ceremony is initially out-of-band). When they need to go through a SIM swap process, the customer service representative validates their information for the network but does not complete the process itself. This validation is done via a confirmation message sent by the MNO network to one of the security contacts of the user without the intervention of an MNO representative, as exhibited in Figure 2.

Figure 2. SIM swap with Secure Contact


User
Customer Service Representative
Mobile Network core
Secure Contact
1 Requests SIM swap
2 Requests user and account data
3 Answer with requested data
4 Requests SIM Swap confirmation for new ICCID
5 Explains how User can finish SIM Swap
6 Sends new SIM PIN for confirmation
7 Confirms PIN with User
8 Accepts PIN
9 Accepts PIN on Network
10 Finish SIM Swap
11 Sends SMS to new SIM to confirm Swap
User
Customer Service Representative
Mobile Network core
Secure Contact

We believe the trusted contact would not cooperate with an operator or attacker. Still, if they do, it is possible to define that to approve the SIM swap, there must be a consensus between most of the contacts involved, making the process even more difficult and involving attacks on consensus protocols. When this contact receives social confirmation from the user that a SIM swap is taking place, they confirm with the MNO that the process is over.

Incorporating these modifications into the original model in Tamarin entailed amending the final rules on the system, finalizing the SIM swap upon confirmation from the Customer Service representative, and adding new rules. Consequently, upon receipt of the response to a security question, the representative initiates the transmission of a message to the designated security contact via the network yet remains uninvolved in the process. Consequently, sending the message was modeled as a secure channel, with the addition of rules that permit the attacker to read the messages but not to insert them.

When it receives the message over the secure channel, the contact follows the flow shown in Figure 2. Inbound and outbound rules for safe communication with this contact are added to talk to the User and confirm the SIM swap on the network. When confirmed, the flow follows similarly to the first experiment. The results show that the attack can begin because these modifications increase the steps needed for the test but keep the same start flow. However, the SIM swap will only occur when an honest user confirms, via a social channel modeled here as a secure channel, that the swap is to the new SIM card already in their possession and with the data indicating part of their PIN.

This new SIM swap can pass both Properties 1 and 2. As a first result of this work, we have an initial model that involves L3 of the security ceremony concertina, adding common attacks carried out by human nodes in the SIM swap, which serves to study improvements in this area. The set of experiments displayed here is available at `https://github.com/LarissaGRosa/SIMSwapModel/tree/experiments-section-3`. Nonetheless, we are not considering human behavioral and intentional factors that lead to these attacks, which occur in the next section.

5. Implementing the Pirandellian Masks

The mapping conducted in Section 4 involves user nodes not subject to failures, which is an unrealistic assumption in the real world. Furthermore, it acknowledges that Customer Service Representatives may or may not be malicious but fails to consider the intention of these actors in acting maliciously. Similarly, it recognizes that attackers have the power to gain access to data but fails to demonstrate the relationship between other actors and their role in facilitating this attack. Thus far, we have yet to consider how human actions and attitudes can influence ceremonies.

Inspired both by the problem of modeling human actions and nodes in security ceremonies and by the play *Sei personaggi in cerca d'autore*, [Martimiano and Martina 2022] delineates six preliminary masks that individuals can wear during the execution of a security ceremony. These masks are the Attentive, the Careless, the Fearful, the Naive, and the Busy.

By applying the defined concept of these masks to our context of use and formal modeling in Tamarin, it is possible to extend the analysis of the SIM swap ceremony to a greater degree of granularity. This approach allows us to model various user behaviors and how they interact with the system under different conditions. For example, we can simulate an attentive user who meticulously follows all security prompts and compares their actions to a careless user who may ignore critical steps. This granular analysis will enable us to understand human behavior more comprehensively, identify patterns in user interaction, and assess the impacts of the correct execution of the SIM swap.

We must now proceed to formalize their representation and utilize them as a tool for investigating the characteristics of our ceremony from the perspective of their existence. As [Martimiano and Martina 2022], we are guided by the principles of theatre to comprehend the genesis of this modeling. In theatre, actors respond to external stimuli and engage in actions that constitute the performance on behalf of their characters.

This systematic composition of actions and reactions by the various actors makes the story unfold for the audience. Similarly, we understand actions and reactions as how the human nodes of our protocol can trigger the mask they wear at a discrete point in time during the performance of our ceremony. By formally modeling these interactions, we analyze the impact of different user behaviors on the security and effectiveness of the ceremony.

In this manner, it is established that each action of a ceremony node (regardless of whether it is a user or a system) can trigger a user node reaction. Upon learning of a system action, the user is directed to a reaction state (which may be none), and this reaction is contingent upon the decision of a mask that the user can wear to act on the system. In the real world, wearing a mask depends on the individual's emotional state, environment, and knowledge of the ceremony, among other factors. In modeling, the objective is to ascertain how multiple masks act during the ceremony. Consequently, the choice of execution for the test is arbitrary, resulting in the generation of various traces that demonstrate the influence of the choice of a mask in each action-reaction pair on the progression of the ceremony.

Once the interfaces that trigger the masks and how the execution of the ceremony intersects them through the action-reaction pair have been defined, the next step is to apply it in the SIM swap ceremony. It is necessary to model how the masks may be employed in the formal proof of the defined properties in the target ceremony. This will be achieved using the multiset rewriting theory, which forms the basis of Tamarin [Meier et al. 2013].

It was determined that whenever a rule initiates the insertion of a human node within the model, a permanent fact, designated as `!HumanMask(M, Id, K)` is generated. The parameters `M`, `Id`, and `K`, respectively, represent the identifier of the initiating rule (`M`), an identifier that facilitates the matching of the generated mask to its intended wearer (`Id`), and an arbitrary piece of data used to define information to be utilized by the masks universally (`K`). These parameters were selected to facilitate the adaptation of the existing context of the models developed in Section 4.

The input for user action rules will be determined by the `!HumanMask(M, Id, K)` fact and reaction facts generated from human-system interactions. Actions initiated without needing a prior reaction request will rely on the initial fact, supplemented by subsequent facts that provide contextual information.

Consequently, the implementation of the masks was defined by establishing analogous rules for each type of interaction that necessitates an action from a user node or customer service representative. Examples of such interactions include calling the representative, answering security questions, sending messages to trusted contacts, etc. To generate the desired behavior, the users who wear the masks employ several logics, which vary according to the interaction type under consideration. The logic applied in any given case involves a comparison of data, communication with other users, an understanding of execution states, and the execution of different operations that are possible from a human point of view.

Accordingly, for each mask defined, the entire set of interactions is implemented, considering the nuances of the execution logic attached to each one. Concerning the SIM swap, we have implemented a subset of the abovementioned masks in the Attentive, Careless, and Fearful categories. This was due to the level of detail of our modeling, which was designed to be generic and not to detail specific interfaces used by MNOs. Therefore, applying masks involving more complex behaviors is not a priority now.

Concerning the coding of these masks, the trigger and response interface, defined through the input and output facts as `MaskReactant` and `MaskPerform`, remains consistent throughout, thus ensuring transparency for the ceremony model as to which mask is being executed. Nevertheless, upon execution, the masks elicit disparate responses from the users who employ them. Each mask has a different implementation to model how it influences user interaction, guiding their actions based on predefined behavior patterns.

6. Pirandellian Masks in the SIM swap Ceremony

The masks defined in the modeling assume a ceremony that offers these entry and exit facts. Before this, our versions of SIM swap did not consider these mechanisms, so we had to modify the original models to enable the use of masks in their analyses. In addition, the interactions and data flows had to be adjusted to ensure that each mask could be correctly applied and tested in different usage scenarios.

During this process, the model underwent several iterations, during which simplifications were made. For instance, in the second iteration, certain names of facts and variables were modified to enhance their clarity, such as the transformation of the operator fact !Operator into the !MNORepresentative fact. Similarly, system status facts were modified to be standardized and used to circumvent the restrictions for initializing each rule. This was evidenced by the change from the fact SimSwapINIT to Status.

Having completed the adaptation of the ceremony to the use of masks, we conducted a series of analyses to understand the impact of the users who wear them on the progress of the ceremony. To achieve this objective, we initially analyzed the masks individually and, after, collectively for each SIM swap model previously mentioned. This entails examining the impact of a user consistently wearing the same mask throughout the ceremony. Subsequently, we devised a system that allows users to change masks during the execution.

The initial SIM swap model, predicated on the authentication of security questions and the assumption of trust in the operator, yielded the execution of traces of the proof for the property related to the SIM swap carried out by the user, who was the original owner of the phone number. We observed that the Attentive mask enables the user to complete the procedure successfully. Similarly, a user who is careless in their responses to the questions may make an error. However, there are execution traces in which the user responds correctly, and these are the only responses that allow the test to be completed, given how the protocol has been modeled.

It can be observed that wearing the Fearful mask throughout the protocol's execution generates traces that are not finalized by the user's refusal to respond to questions posed to them while wearing this mask. We also noticed how a user may alter their mask during the protocol's execution, initially adopting a fearful demeanor and assuming an attentive stance when prompted to respond to security questions. This changing mask structure allows us to compose human users with complex behaviors.

Given the unreliability of customer service representative nodes and their potential to be represented as actors wearing masks that model their behavior, we have identified a further set of execution traces. In this instance, the operators may act maliciously not out of explicit motivation as in the previous case but because they are wearing the Careless mask and are unaware that the data they have received is insufficient. In this sense, we have execution traces where an honest user may finish the SIM swap even though he had not answered the right question[1]. Similarly; an attack is assumed by the representative when they wear the Fearful mask and are prevented from finalizing the exchange, even

[1] The execution trace is available at `https://github.com/LarissaGRosa/SIMSwapModel/blob/main/experiments/results/InitSimSwapWithMNORepresentative_careless_representative.pdf`

though it is legitimate. Thus, no execution trace finishes the process with a representative wearing the Fearful mask.

In the context of the SIM swap with social authentication, the process forms three distinct human nodes: the user, the customer service representative, and the security contact. In this context, the validation of this model and the composition of the masks identified a potential attack that did not exist when viewed solely from the perspective of representatives and external attackers. This was because it was assumed that the human nodes would not make mistakes[2].

This attack trace assumes that a legitimate exchange occurs by a user in a time window very close to an attack being carried out on their number. Considering the SIM swap model with social authentication in Section 4, it can be posited that upon completion of the security question phase, the telephone network initiates a security contact and transmits the PIN of the new SIM for confirmation between peers. Suppose a security contact utilizes the Careless mask in the action-reaction pair to confirm this SIM. In that case, it will fail to verify the user's correct SIM, thereby allowing the attacker's PIN to be changed.

The behavior mentioned above could be circumvented by consensus between multiple security contacts. However, this would increase the ceremony's complexity, potentially causing inconvenience to the user. An alternative solution would be to implement measures that ensure the user is attentive at this stage. One such measure could be to require the user to enter a code sent to them rather than simply confirming it. This approach demonstrates how formal proof and user experience design can be integrated to inform the ceremony between the masks. It is evident from this example that the use of Pirandellian masks can assist protocol and ceremony developers in understanding how these ceremonies are used in real life. This is analogous to the theatre example previously discussed. It is similar to how an author's written plays will be interpreted differently than originally expected by the actors presenting them on stage.

It is also crucial to acknowledge that the execution traces contribute to interpreting the footprint of a user when fitted with masks, thereby adding semantic meaning to the analysis. This is because the semantics of the traces of execution of these masks by a user can be used to compose stories about the use of the ceremony. For example, the execution traces permit the construction of a narrative in which an attentive user, due to an external factor such as distraction, makes an error by wearing the Careless mask. This results in the user becoming fearful and unable to complete the ceremony.

The semantic content of the execution traces provides valuable insight into the optimal design of a ceremony. Understanding the underlying narrative structure makes it possible to develop a ceremony that maximizes the number of stories that lead to its completion. When designing the interface of a ceremony, attention-grabbing mechanisms can be employed to prevent a careless user from finalizing the stage through an error. This approach thus represents a promising avenue for further investigation when developing and analyzing ceremonies.

[2] The execution trace is available at `https://github.com/LarissaGRosa/SIMSwapModel/blob/main/experiments/results/InitSimSwapWithMNORepresentative_social_auth.pdf`

Nevertheless, integrating the diverse masks into the tests by the various human participants resulted in a more comprehensive and nuanced examination. The previously straightforward process of automatically displaying the Tamarin test results has become more complex, necessitating the proof of properties to be guided by the protocol modeler. This is because each human action and reaction can result in the execution of any mask. The combination of four human actions generates a total of 3^4 distinct execution traces previously represented by a single trace.

The three masks can be used with any of the four actions. Consequently, the number of potential execution traces will increase based on the number of masks and possible human actions within a ceremony. This is a significant challenge for larger and more complex ceremonies, necessitating further research to enhance the implementation of the masks, thereby reducing the number of traces at higher complexities. The experiments for this section may be found in `https://github.com/LarissaGRosa/SIMSwapModel`.

7. Conclusion

Our study delved into security protocols and ceremonies, focusing on their role in digital security, operational principles, and ongoing challenges. Specifically, we explored the SIM swap ceremony used by mobile network operators (MNOs) when a SIM card becomes unusable due to theft or misuse. We identified issues that can lead to financial loss and proposed it as a model for analyzing security ceremonies.

We introduced a generic information transmission model to enhance understanding and standardization of the SIM swap process across stakeholders like users, MNOs, and customer service. Initially framed in epistemic logic and implemented in Tamarin, this model demonstrated its efficacy by uncovering potential vulnerabilities such as user impersonation and representative corruption, aligning closely with empirical findings.

Additionally, we introduced the concept of Pirandellian Masks to model human behavior within the SIM swap ceremony, particularly focusing on layers $\mathsf{L3}$ and $\mathsf{L4}$ of the ceremony's structure. This innovative approach, adapted from previous work, utilized Tamarin for formal verification, revealing insights into user behavior variations during ceremonies and their impact on security protocols.

Our research aims to refine these models further, particularly in integrating more realistic human behaviors and exploring broader applications beyond SIM swap ceremonies. We strive to address complexities in theorem proving and expand the applicability of Pirandellian Masks across different security contexts, thereby enhancing the robustness and effectiveness of security protocols in digital environments.

References

Andrews, N. (2018). " can i get your digits?": Illegal acquisition of wireless phone numbers for sim-swap attacks and wireless provider liability. *Nw. J. Tech. & Intell. Prop.*, 16:79.

Avalle, M., Pironti, A., and Sisto, R. (2014). Formal verification of security protocol implementations: a survey. *Formal Aspects of Computing*, 26:99–123.

Basin, D., Radomirovic, S., and Schmid, L. (2016). Modeling human errors in security protocols. In *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, pages 325–340. IEEE.

Bau, J. and Mitchell, J. C. (2011). Security modeling and analysis. *IEEE Security & Privacy*, 9(3):18–25.

Bella, G. and Coles-Kemp, L. (2012). Layered analysis of security ceremonies. In *Information Security and Privacy Research: 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings 27*, pages 273–286. Springer.

Bella, G., Curzon, P., and Lenzini, G. (2015). Service security and privacy as a socio-technical problem. *Journal of Computer Security*, 23(5):563–585.

Bella, G., Giustolisi, R., and Schürmann, C. (2022a). Modelling human threats in security ceremonies. *Journal of Computer Security*, 30(3):411–433.

Bella, G., Ophoff, J., Renaud, K., Sempreboni, D., and Viganò, L. (2022b). Perceptions of beauty in security ceremonies. *Philosophy & Technology*, 35(3):72.

Braghin, C., Lilli, M., and Riccobene, E. (2023). A model-based approach for vulnerability analysis of iot security protocols: The z-wave case study. *Computers & Security*, 127:103037.

Canetti, R. and Krawczyk, H. (2001). Analysis of key-exchange protocols and their use for building secure channels. In *International conference on the theory and applications of cryptographic techniques*, pages 453–474. Springer.

Cointelegraph (2023). “sim swap”: Conheça o golpe que roubou 4 milhões dos seguidores do criador da ethereum. https://exame.com/future-of-money/sim-swap-conheca-o-golpe-que-roubou-r-4-milhoes-dos-seguidores-do-criador-da-ethereum/.

Ekeh, G., Afolabi, Y., Uche-Nwachi, E., Ekeh, L., and Eze-Udu, E. (2022). Awareness of bvn, sim swap and clone frauds: Methods and controls. *Science World Journal*, 17(2):200–206.

for Cybersecurity ENISA, E. U. A. (2021). *Countering sim-swapping: overview and good practices to reduce the impact of SIM swapping attacks.* Publications Office.

Gudimalla, T. K. M., Kannan, S., et al. (2019). Survey analysis of cloned sim card. In *Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT)*.

Haidar, A. N. and Abdallah, A. E. (2009). Formal modelling of pki based authentication. *Electronic Notes in Theoretical Computer Science*, 235:55–70.

IC3 (2022). Internet Crime Complaint Center (IC3) — Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public — ic3.gov. `https://www.ic3.gov/Media/Y2022/PSA220208`. [Accessed 19-04-2024].

Johansen, C. and Jøsang, A. (2015). Probabilistic modelling of humans in security ceremonies. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance: 9th International Workshop, DPM 2014, 7th International Workshop, SETOP 2014, and 3rd International Workshop, QASA 2014, Wroclaw, Poland, September 10-11, 2014. Revised Selected Papers 9*, pages 277–292. Springer.

Kim, M., Suh, J., and Kwon, H. (2022). A study of the emerging trends in sim swapping crime and effective countermeasures. In *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*, pages 240–245.

Lee, K., Kaiser, B., Mayer, J., and Narayanan, A. (2020). An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 61–79.

Martimiano, T. and Martina, J. E. (2022). Six characters in search of a security problem: Pirandellian masks for security ceremonies. In *Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 344–357. SBC.

Meier, S., Schmidt, B., Cremers, C., and Basin, D. (2013). The tamarin prover for the symbolic analysis of security protocols. In *Computer Aided Verification: 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings 25*, pages 696–701. Springer.

Pedersen, T., Johansen, C., and Jøsang, A. (2018). Behavioural computer science: an agenda for combining modelling of human and system behaviours. *Human-centric Computing and Information Sciences*, 8:1–20.

Pirandello, L. (2011). Sei personaggi in cerca d'autore.

Radke, K., Boyd, C., Gonzalez Nieto, J., and Brereton, M. (2011). Ceremony analysis: Strengths and weaknesses. In *Future Challenges in Security and Privacy for Academia and Industry: 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, June 7-9, 2011. Proceedings 26*, pages 104–115. Springer.

Schmidt, B., Meier, S., Cremers, C., and Basin, D. (2012). Automated analysis of diffie-hellman protocols and advanced security properties. In *2012 IEEE 25th Computer Security Foundations Symposium*, pages 78–94.

Sempreboni, D. and Viganò, L. (2020). X-men: A mutation-based approach for the formal analysis of security ceremonies. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 87–104.

7 APPENDIX B – CÓDIGO FONTE DO TCC

The code developed is available at **https://github.com/LarissaGRosa/SIMSwapModel/tree/main** and **https://github.com/LarissaGRosa/SIMSwapModel/tree/experiments-section-3**. Before running the experiments, make sure you have Tamarin Prover installed. To run the experiments, execute `make prove`. This makefile tag will execute the Tamarin Prover code and perform the formal analysis of the SIM swap ceremony. Use `make clean` to delete the generated result files.

1. Ensure that Tamarin Prover is installed on your system;
2. Clone this repository to your local machine;
3. Navigate to the cloned directory;
4. Run the experiments by executing `make prove` in a terminal;
5. Review the output generated by Tamarin Prover for the analysis results.