

Enhanced SIM swap security practices via ceremony modeling

Larissa Gremelmaier Rosa, Gustavo Zambonin, and Jean E. Martina

Abstract A SIM swap is a process by which mobile network operators transfer a phone number from one SIM card to another. This is prompted by several factors, including losing the original card, technological upgrades, or other circumstances. The implications of SIM swaps for the security of phone numbers are significant, as they expose owners to risks such as identity theft and financial loss. We characterize a generic SIM swap process as a security ceremony to address such challenges imposed by human-human interactions on top of security protocols. We model the resulting ceremony using the Tamarin prover to concretely identify authentication challenges arising from the introduction of malicious impersonators. We propose a social-based authentication scheme for the SIM swap ceremony to mitigate such challenges and similar attacks described in the literature. Finally, we formally show that our newly proposed ceremony can resist the current attacks.

1 Introduction

A Subscriber Identification Module (SIM) is a smart card that stores essential information for identifying a user on a mobile network [16]. It allows users to access text messaging, voice calls, and internet browsing. Mobile network operators (MNOs) maintain a database that links SIMs to phone numbers [19]. SIM cards can be moved

Larissa Gremelmaier Rosa

Universidade Federal de Santa Catarina, Florianópolis, SC, Brazil, e-mail: `larissa.gremelmaier.rosa@posgrad.ufsc.br`

Gustavo Zambonin

Universidade Federal de Santa Catarina, Florianópolis, SC, Brazil, e-mail: `gustavo.zambonin@posgrad.ufsc.br`

Jean E. Martina

Universidade Federal de Santa Catarina, Florianópolis, SC, Brazil, e-mail: `jean.martina@ufsc.br`

between devices, but damage, loss, or resizing issues may require users to undergo a SIM swap process to retain their phone numbers and data. This procedure involves authenticating the user and issuing a new SIM card [19].

Authentication methods vary, with offline methods relying on official documents and online methods using personal and account information [4]. SIM swap processes are vulnerable to attacks, especially when unauthorized parties access user authentication data. A 2021 ENISA study [4] identifies social engineering attacks on users as the most common threat. Such attacks have resulted in significant financial losses and identity theft in countries like the United States and the European Union [17]. Although empirical studies address SIM swap attacks [19, 17, 13], formal analysis and testing mechanisms are lacking.

We address such limitations by treating the SIM swap process as a security ceremony using the layered model of Bella and Coles-Kemp (2012) (Section 2). We categorize common attacks within the layers and model relevant approaches in the human interface layer using the Tamarin tool, providing a framework for testing modifications to the ceremony (Section 3). To address such attacks, we integrate an alternative authentication method based on social contacts to strengthen the SIM swap process (Section 4) and discuss the consequences of this new model. Finally, we provide several future research directions (Section 5).

2 SIM swap and security ceremonies

We hereafter define the concept of a security ceremony and present the framework we use to categorize and analyze the SIM swap. Shortly after, we describe the operations involved in the process and explain how studies and empirically identified attacks align with this framework. Finally, we justify the choice of the specific layer modeled in our work.

2.1 Security ceremonies

A ceremony is a superset of network protocols, encompassing human-human and human-computer channels, user interfaces, and the exchange of physical objects carrying data [12]. A secure ceremony protects the properties of the protocols against traditional attackers and shields them from threats involving social and physical interactions around the protocols. Bella et al. (2013) discuss the implementation of TLS in browsers as a social-technological challenge. They demonstrate how the complexity of security problems increases when viewed through the lens of social-technical interactions involving the network, server, user, attacker, and browser as components of a security ceremony.

Modeling a ceremony requires addressing its inherent complexity and considering both traditional and novel properties, such as authenticity and secrecy, in addition to

those rooted in the social context of the protocol. Bella et al. (2013) introduced new properties in the TLS ceremony, such as an alert for invalid certificates, highlighting the need for a more intricate model extending beyond basic protocol operations to include interactions between servers, users, and attackers.

To address this, Bella and Coles-Kemp (2012) proposed the *security ceremony concertina*, a multi-layered model that examines the intersections between layers, helping identify interactions between users and technology. This approach facilitates a comprehensive understanding of ceremonies, enabling a structured analysis of threats and user-technology interactions within security protocols. The concertina model categorizes a ceremony into five layers: Informational (L1), Operating System (L2), Human-Computer Interaction (L3), Personal (L4), and Communal (L5). Each layer is connected by interfaces representing interactions, such as the user interface between system and human-computer layers.

2.2 Analysing the SIM swap as a security ceremony

We follow the concertina framework in the sequence and discuss SIM swap in each defined layer. We describe where the attacks found empirically may be categorized within the layers and show how protocols and surrounding infrastructure are connected to the SIM swap ceremony.

Layer 1 (L1) represents the machine-machine communication layer, which includes classic protocols like Authentication and Key Agreement (AKA), Remote SIM Provisioning (RSP), and Transport Layer Security (TLS). In the context of SIM swap, examining this layer involves considering standards defined by entities such as the 3GPP SA WG3 and the GSM Association [1]. Attacks at this layer typically target specific protocols, as demonstrated by Ahmed et al. (2024), who highlight vulnerabilities in RSP sessions caused by compromised servers. Although these protocols depend on TLS tunnels, they are vulnerable to TLS-related issues, yet formal specifications allow for mitigation through updated, formally verified protocol versions [9].

Layer 2 (L2) involves interactions between software processes, such as inter-process communication and session management, including integration with GUIs. In SIM swap, this layer pertains to internal applications used by MNOs, such as ERP systems. Vulnerabilities in this layer, such as poor privilege management and weak authentication protocols, can be exploited to bypass security checks. Suraci et al. (2021) identify problems like insufficient identity and access management and insecure APIs in 5G infrastructures. However, active countermeasures, including coordinated disclosures and projects like the Linux Kernel Self-Protection Project, work to improve security at this critical layer [11].

Layer 3 (L3) focuses on human-computer interaction, specifically how users engage with systems by filling out forms and navigating GUIs. It involves user interaction with MNOs via customer service representatives (CSRs) or self-service platforms for SIM swap. Despite several authentication methods to prevent unau-

thorized SIM swaps, attackers may exploit social engineering or collude with CSRs to obtain sensitive data. This makes prevention challenging, as attackers do not need advanced technical knowledge. Most studies at this socio-technical layer are empirical [19, 4].

Layer 4 (L4) deals with user behavior and identity within a system, focusing on how systems protect user data to ensure authenticity. In the SIM swap process, this layer examines interactions between users and CSRs and how users safeguard their data against social engineering. Although no specific studies address SIM swap in the MNO-user context, research in security and usability [15, 10] highlights the importance of user behavior in security frameworks.

Layer 5 (L5) examines human-human interactions and the societal recognition of ceremonies, including regulations and trust frameworks. Regulatory agencies like the U.S. Federal Communications Commission and ENISA establish standards to protect the privacy and security of users. However, Narayanan and Lee (2023) point out flaws in the legal framework, particularly regarding network security policies.

2.3 Targeting a specific layer

As previously outlined, examining the layers of a ceremony in unison is a complex task; it is common in the literature to define stages or layers of study, as illustrated by the concertina framework. When examining the SIM swap layers and categorizing their studies, we observe that L1 and L2 are largely approached formally, using operating system design methods and formal analyses of protocols such as RSP. In contrast, L3 to L5 are primarily studied empirically. In the literature related to SIM swap, attacks are usually described in the context of authentication methods, especially when attackers can deceive users. Therefore, we argue that a more rigorous analysis of L3 and L4 is needed to study and improve these authentication methods. In our work, we start by L3 and explore how its formalization and possible modifications impact L4.

3 SIM swap modelling

We now present our modeling of the SIM swap ceremony within the Concertina framework. Initially, we explain how we abstract the part to be modeled and associated attacks to build a diagram focused on the target layer. Next, we detail the implementation of the mechanisms identified in Tamarin, considering the rules that help carry out the attacks and the basic operations involved.

3.1 Collapsing the concertina at L3

A SIM card holds key user authentication and identification values, such as the authentication key (K_i), ICCID, and IMSI. To simplify the model, we omit additional data. We assume a generic authentication method based on information knowledge, as the literature above shows it is the most common authentication method for SIM swaps. Figure 1 illustrates the basic steps of a SIM swap ceremony at L3, involving the user, CSR, and MNO system. The model focuses on online interactions, where authentication depends on electronic data. The MNO is assumed trustworthy, and the user is presumed to have the necessary authentication data. Communication channels are secure during the SIM swap but may be replayed later.

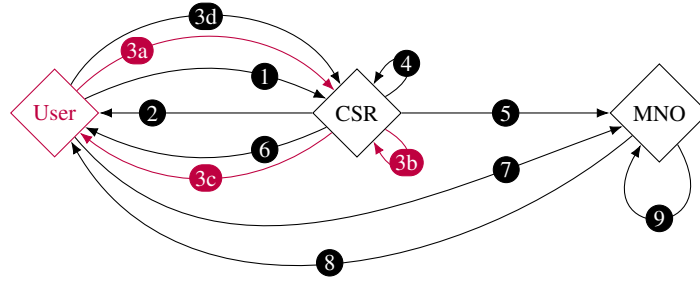


Fig. 1 Generic steps of a SIM swap ceremony in L3 of the security ceremony concertina. Steps performed by an eventual attacker are marked in purple.

We briefly describe the ordered steps of Figure 1: **1** a user requests the CSR of a MNO to initiate the SIM swap ceremony; **2** the CSR requests private account data to the user to perform authentication; **3d** the user sends the requested data to the CSR; **4** the CSR processes the data received by the user and confirms their authentication; **5** it updates the user account data in the MNO with the ICCID of a new SIM card; **6** it sends a new SIM card to the user via an out-of-band mechanism; **7** the user activates the SIM card by authenticating directly with the MNO using K_i and personal data; **8** the MNO sends the IMSI of the new SIM card to the user; **9** it registers the old SIM card as inoperative.

However, SIM swaps are vulnerable to social engineering at L3. Attackers gather the phone number of the target and details about the MNO, then submit an online SIM swap request. Authentication challenges are bypassed through deception, exploiting faulty CSR processes. While such attacks typically occur at L4, their consequences extend to L3. We model the social engineering attack through additional steps in Figure 1: **3a** the attacker intentionally provides incorrect private data; **3b** the CSR processes the data received by the “user” and detects an authentication failure; **3c** it notifies the “user” of a failed authentication attempt and asks for further private data. Final steps mirror the successful ceremony, but the attacker gains control over the phone number of the victim, and the original SIM is disabled.

3.2 *Tamarin model*

We encode the resulting schema in Tamarin, a tool for formal verification of cryptographic protocols [21]. Each actor is modeled as a process, with the exchange of messages formalized as multiset rewriting rules. We recall that a Tamarin security protocol theory consists of three parts: (i) the signature, which includes functions, equations, and built-ins, in the form of an equational theory model [21]; (ii) the specification of the protocol, as multiset rewriting rules; (iii) and properties specification, in a guarded fragment of first-order logic [18]. For the attacker, it has a built-in Dolev–Yao model, which can be suitably modified.

Any private data required for user authentication are defined as nonces, part of a system of equations tallied by human entity nodes. In practice, such random data represents sensitive information only the user holds. In the Tamarin grammar, this is represented by $x:\text{fresh}$ for some information x . Consequently, the resulting model is highly generic and flexible. We tested the model for the following properties, encoded as lemmas in Tamarin:

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.

We created a rule called INITUSERONNETWORK to make the registration of a user at a specific MNO. We model the set of ICCID, IMSI, and K_i to uniquely represent a SIM card, a user identifier on the MNO, their full name, and the phone number. This data is sent to the MNO as knowledge. Using the OUT(x) output facts, we send data that we consider the attacker knows: in this case, the user name and phone number of the target. We created similar rules to define a customer service representative in MNO. The entities USER, MNO, and CSR in Figure 1 are represented in Tamarin as prefixed public variables of the form $\$X$.

To model the SIM swap itself, four rules have been created: (i) the start of the process, (ii) the answering of the authentication questions, (iii) the confirmation of the answers by the customer service agent, (iv) 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. We begin by discussing the rule in Listing 1, as it is the rule that models step ❶ of Figure 1 and may be used to derive all other steps encoded in Tamarin.

```

1 rule initSwapWithOperator:
2   [
3     !Operator(O, opId),
4     In(userPhoneNumber),
5     Fr(seedK: fresh)
6   ]
7   --[ initSwap(userPhoneNumber, seedK: fresh) ]->
```

```

8    [
9      SimSwapInit(seedK: fresh, opId, userPhoneNumber),
10     Out(question(userPhoneNumber, seedK: fresh)),
11     Out(seedK: fresh)
12   ]

```

Listing 1 Initiating SIM Swap with Operator in Tamarin.

The rule receives three input facts. In Line 3, the syntax represents a CSR, which defines which representative is answering the SIM swap request. In Line 4, it is the data that references the phone number to be SIM swapped, which comes from a network that the attacker can manipulate; in other words, a legitimate user or an attacker can perform the request, indistinguishable from the CSR. In Line 5, it is a nonce used to calculate the security question for a request to maintain its arbitrary properties within the set of possible knowledge-based authentication methods.

When INITSWAPWITHOPERATOR is executed, a trace is generated by Tamarin storing the phone number and seed used to define the security question in Line 7. As outputs, there are control facts indicating to the system that a SIM swap started for a specific phone number (Line 9); the production of the question fact, exposed to the network (Line 10); and the SEEDK used to generate the question (Line 11) needed for calculating the question answer in our equational model, as we show later. This knowledge is publicly placed on the network via facts of the type OUT(), i.e., they may be known to an attacker.

These output facts are used for the next step of the SIM swap encoded in Listing 2. To execute the next rule, the user receives the question in Line 10 and must correctly answer it to the designated CSR (Line 5 in Listing 2). The way of answering it follows an equational model. Let T be the target phone number, and K the SEEDK as above. The ceremony proceeds if the relationship between the equations

$$\text{ANSWERS}(T, K, \text{CORRECTANSWER}(\text{QUESTION}(T, K))) = \text{PERMISSION}(T, K),$$

is met. Consequently, the CSR must obtain PERMISSION(T, K).

```

1 rule AnswerSimSwapToOperator:
2   let
3     p = userPhoneNumber
4     c = correctAnswer(question(p, seedK))
5     a = answers(p, seedK, c)
6   in
7     [
8       SimSwapInit(seedK, opId, p),
9       In(question(p, seedK))
10    ]
11  --[ AnswerSimSwap(p, seedK) ]->
12  [ SimSwapAnswer(a, opId, p, seedK) ]

```

Listing 2 User answers SIM swap to Operator in Tamarin.

We modeled `CORRECTANSWER(QUESTION(T, K))` in a way only the user could calculate it unless there were an information attack. In this way, the answering step in our model is performed by the user, who receives as input the question to be answered, as well as the control facts. The user then evaluates the equational model using these facts, answering the SIM swap authentication question and generating new output facts needed to end the process.

We note that an attacker can obtain the data to calculate these equations and respond correctly in this phase. Rules that model this behavior have also been added to the equivalent Tamarin encoding. The remaining rules refer to how the system finishes the SIM swap. We argue that our Tamarin model can accurately simulate L3 as described in the literature. It is available at <https://anonymous.4open.science/r/SIMSwapModel-76B6> as a standalone codebase.

4 Evaluation and proposed enhancements

By executing the aforementioned Tamarin encoding, we verify that Property 2 holds in all execution traces. However, Property 1, which ensures only the owner can perform a SIM swap, has two divergent execution traces after running our model using Tamarin. The first represents an honest process, including all necessary interactions between actors. The second reveals a possible attack where an adversary impersonates a legitimate user by exploiting stolen data.

Additionally, we modeled an attack scenario involving a rogue CSR to test whether we could verify other attacks in the process. In this case, the CSR bypasses user validation and directly facilitates the SIM swap. The resulting execution trace mirrors the prior attack but excludes explicit cooperation between attackers. These findings demonstrate that our formal security ceremony model aligns with empirical observations, capturing both the legitimate SIM swap process and vulnerabilities to fraud. This model provides a foundation for studying system improvements and enhancing security measures.

4.1 Authentication methods discussion

In light of the limitations of methods involving ownership and knowledge bases within the context of the SIM swap ceremony, it is necessary to consider alternative approaches, such as one-time password tokens or methods that involve receiving an activation code on a secure device. However, if the device is misplaced or stolen, the user cannot perform a SIM swap at will. On the other hand, usual passwords can be employed. Still, it is relatively easy for a person to forget a secret that is not regularly used, which also renders this mechanism ineffective [24] since SIM swaps rarely occur in frequent succession.

The potential for utilizing biometric factors exists. Nevertheless, the deployment of biometric authentication is confronted with several challenges, including discrepancies between the biometrics registered and those presented, compounded by the use of inaccurate equipment and the prevalence of privacy concerns [23]. Furthermore, the advent of novel AI image techniques has elevated the risks of biometric forgery, rendering the system more susceptible to malicious interventions.

4.2 Social authentication proposal

One form of authentication particularly suited to this ceremony is based on social interaction. We propose the utilization of voucher-based social authentication, wherein users initiate interactions with trusted contacts to gain access to systems. This process entails the collection of voucher codes from a pre-selected group of contacts or using alternative procedures, such as video or voice calls, to corroborate the identity of a user [3]. The involvement of trusted contacts verifies the legitimacy of the user and serves as a second factor in the SIM swap authentication process.

Figure 2 shows our proposal of 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 setup ceremony is initially out-of-band. When they need to go through a SIM swap process, the CSR 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 to a security contact of the user without the intervention of a CSR.

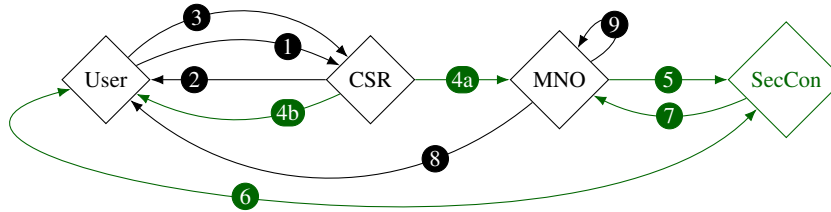


Fig. 2 Modified SIM swap ceremony with social authentication via secure contacts.

Steps 1–3, which constitute the initial authentication stage of the ceremony, remain unchanged from Figure 1. Other steps are modified as such: 4a the CSR requests SIM swap confirmation for a new ICCID to the MNO but does not finish the process; 4b asynchronously, it returns the protocol number of the SIM swap operations to the user and initiates the secure contact procedure; 5 the MNO processes the requisition from the CSR and generates a confirmation code that is sent to the secure contact; 6 a secure contact and the user exchange information through an out-of-band channel to confirm the original requisition; 7 the secure

contact answers the MNO request. Analogously, steps 8–9, in which the MNO manages the old and new SIM cards, remain unchanged.

4.3 Social authentication in Tamarin

Incorporating these modifications into the original model in Tamarin entailed amending existing rules, finalizing the SIM swap upon confirmation from the CSR, 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 the secure contact receives the message over the secure channel, it 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 initial steps.

However, the SIM swap only occurs 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 ceremony achieves Properties 1 and 2 within all Tamarin execution traces. We remark that while these mechanisms function optimally within an ideal scenario, their efficacy is contingent upon the safety of the individuals involved in the process [14] and the way the secure contacts are updated.

To address this, we suggest distributing a user-generated secret in chunks across various geographical contexts, using Bluetooth for automated distribution without user intervention. The correctness of the assembled secret can be verified through asymmetric encryption. Two options for updating contacts emerge: one where users receive periodic notifications to approve potential security contacts before submission to the MNO and another where MNOs receive these contacts directly, albeit with potential privacy concerns. After initial authentication, users confirm a subset of the secret to finalize the process. However, a full description and formalization of this model is out of the current scope and is left as future work.

5 Conclusion

As the ceremony depends on the actions of human participants, the behavior of these individuals introduces an additional layer of complexity. Despite examining factors such as human error and the potential for interaction between these entities to result

in system breaches [5, 8], the field of security ceremonies still lacks methodologies capable of capturing this complexity for further analysis.

To this end, we analyzed the security limitations of the SIM swap procedure within the security ceremony concertina framework, translating a target layer (L3) into Tamarin for verification. Our model aligns with real-world analyses, capturing the mechanics of SIM swap fraud and addressing socio-technical vulnerabilities. To mitigate these issues, we proposed a revised SIM swap ceremony incorporating social authentication, where trusted contacts validate the process, adding a robust layer of security against reported attacks.

However, fully capturing and analyzing all potential weaknesses of social authentication in the SIM swap ceremony from a formal perspective is not yet feasible. We suggest that future work focuses on developing more advanced methodologies for modeling human behavior and social interactions, allowing for a deeper understanding of the social dynamics that can affect the security of such ceremonies when considering social-based authentication.

In addition to further refining the SIM swap models in L3 of the concertina, it is possible to establish formal structures that enable modeling of the ceremony in L4 through capturing human behaviors. To this end, we suggest examining ideas such as applying Pirandellian masks [20] to our model. Further, it is feasible to map other ceremonies within the MNOs that exhibit analogous characteristics and ascertain the potential for improving their authentication on a comprehensive scale. This approach paves the way for future research into refining authentication methods, especially in scenarios where human behavior plays a crucial role.

References

- [1] 3rd Generation Partnership Project. 3GPP Specifications per WG: S3, September 2024. URL <https://archive.is/LSDSJ>. Access date: 2024-09-19.
- [2] Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, and Tuomas Aura. Security Analysis of the Consumer Remote SIM Provisioning Protocol. *ACM Transactions on Privacy and Security*, 27(3):1–36, 2024. doi: 10.1145/3663761.
- [3] Noura Alomar, Mansour Alsaleh, and Abdulrahman Alarifi. Social Authentication Applications, Attacks, Defense Strategies and Future Research Directions: A Systematic Review. *IEEE Communications Surveys & Tutorials*, 19(2): 1080–1111, 2017. doi: 10.1109/comst.2017.2651741.
- [4] Georgia Bafoutsou, Slawomir Bryska, and Marnix Dekker. Countering sim-swapping: Overview and good practices to reduce the impact of sim-swapping attacks. Technical report, European Union Agency for Cybersecurity (ENISA), December 2021.
- [5] David Basin, Saša Radomirović, and Lara Schmid. Modeling Human Errors in Security Protocols. In *Proceedings of the IEEE 29th Computer Security Foundations Symposium, CSF 2016*, pages 325–340, June 2016. doi: 10.1109/CSF.2016.30.

- [6] Giampaolo Bella and Lizzie Coles-Kemp. Layered Analysis of Security Ceremonies. In Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, editors, *Information Security and Privacy Research (SEC 2012)*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 273–286, June 2012. doi: 10.1007/978-3-642-30436-1_23.
- [7] Giampaolo Bella, Rosario Giustolisi, and Gabriele Lenzini. Socio-technical formal analysis of TLS certificate validation in modern browsers. In *2013 Eleventh Annual Conference on Privacy, Security and Trust*, pages 309–316, July 2013. doi: 10.1109/PST.2013.6596067.
- [8] Giampaolo Bella, Rosario Giustolisi, and Carsten Schürmann. Modelling human threats in security ceremonies. *Journal of Computer Security*, 30(3): 411–433, 2022. doi: 10.3233/JCS-210059.
- [9] An Braeken. Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability. *Computer Networks*, 181(107424), November 2020. doi: 10.1016/j.comnet.2020.107424.
- [10] Lizzie Coles-Kemp. Inclusive Security: Digital Security Meets Web Science. *Foundations and Trends® in Web Science*, 7(2):88–241, December 2020. doi: 10.1561/18000000030.
- [11] Kees Cook and Alexander Popov. Linux Kernel Self-Protection Project, September 2024. URL <https://archive.is/RFDBO>. Access date: 2024-09-19.
- [12] Carl Ellison. Ceremony Design and Analysis. Cryptology ePrint Archive, Report 2007/399, October 2007. URL <https://eprint.iacr.org/2007/399/20071021:182434>.
- [13] FBI Internet Crime Complaint Center (IC3). Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public. Alert Number I-020822-PSA, February 2022. URL <https://archive.is/4KAAd>. Access date: 2023-02-10.
- [14] Neil Zhenqiang Gong and Di Wang. On the Security of Trustee-Based Social Authentications. *IEEE Transactions on Information Forensics and Security*, 9(8):1251–1263, 2014. doi: 10.1109/TIFS.2014.2330311.
- [15] Marthie Grobler, Raj Gaire, and Surya Nepal. User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, 4(583723), March 2021. doi: 10.3389/fdata.2021.583723.
- [16] Tirumala Krishna Mohan Gudimalla, Vipin P, and Suthendran Kannan. Survey Analysis of Cloned SIM Card. In *Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT) 2019*, August 2019. doi: 10.2139/ssrn.3431642.
- [17] Myoungsoon Kim, Joon Suh, and Hunyeong Kwon. 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, August 2022. doi: 10.1109/BCD54882.2022.9900510.
- [18] Dorela Kozmai. *Converting Tamarin to extended Alice&Bob protocol specifications*. Bachelor’s thesis, ETH Zürich, 2016.

- [19] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 61–79, August 2020. URL <https://www.usenix.org/conference/soups2020/presentation/lee>.
- [20] Taciane Martimiano and Jean Everson Martina. Six Characters in Search of a Security Problem: Pirandellian Masks for Security Ceremonies. In *Proceedings of the 22nd Brazilian Symposium on Information and Computational Systems Security*, pages 344–357, September 2022. doi: 10.5753/sbseg.2022.225346.
- [21] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In Natasha Sharygina and Helmut Veith, editors, *Computer Aided Verification (CAV 2013)*, volume 8044 of *Lecture Notes in Computer Science*, pages 696–701, July 2013. doi: 10.1007/978-3-642-39799-8_48.
- [22] Arvind Narayanan and Kevin Lee. Security Policy Audits: Why and How. *IEEE Security & Privacy*, 21(2):77–81, April 2023. doi: 10.1109/MSEC.2023.3236540.
- [23] Maria Papathanasaki, Leandros Maglaras, and Nick Ayres. Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*, 0, 2022. doi: 10.5772/acrt.08.
- [24] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the ‘Weakest Link’ — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19(3):122–131, 2001. doi: 10.1023/A:1011902718709.
- [25] Chiara Suraci, Giuseppe Araniti, Andrea Abrardo, Giuseppe Bianchi, and Antonio Iera. A stakeholder-oriented security analysis in virtualized 5G cellular networks. *Computer Networks*, 184(107604), January 2021. doi: 10.1016/j.comnet.2020.107604.