

# Enhanced SIM swap security practices via ceremony modeling

Larissa G. Rosa, Gustavo Zambonin M.Sc.,  
Prof. Jean Martina

Universidade Federal de Santa Catarina

October 13, 2026

# Introduction: Motivation and Approach

## Context

- ▶ SIM cards identify users on mobile networks [11]
- ▶ Enable messaging, calls, and internet access
- ▶ Linked to phone numbers by MNO databases [13]

## SIM Swap Process

- ▶ Needed after damage/loss or size incompatibility
- ▶ Requires user authentication and new SIM issuance [13]
- ▶ Vulnerable to attacks (e.g., social engineering) [3]

## Problem

- ▶ Lack of formal analysis and testing mechanisms [13, 12, 9]
- ▶ Financial loss and identity theft risks in the US and EU [12]

# Introduction: Contributions

## Our Contribution

- ▶ Model SIM swap as a *security ceremony* [4]
- ▶ Analyze attacks via ceremony layers
- ▶ Use Tamarin to model the human interface layer
- ▶ Propose to use social contact-based authentication
- ▶ Discuss future research directions

# Security Ceremonies

## Definition

- ▶ Ceremonies extend protocols to include human-human and human-computer interactions [8].
- ▶ Secure ceremonies address both technical and social threats.

## Motivation

- ▶ Example: TLS implementation involves users, servers, and browsers [5].
- ▶ Complexity increases with social-technical components.

## Concertina Model [4]

- ▶ Multi-layer model: Informational (L1) to Communal (L5)
- ▶ Layers linked via interfaces (e.g., GUI between human and system)
- ▶ Enables structured analysis of socio-technical protocols

# Analyzing SIM Swap as a Security Ceremony

## **Approach**

- ▶ SIM swap analyzed using concertina layers (L1–L5)
- ▶ Attacks mapped to specific ceremony layers
- ▶ Framework reveals infrastructure and protocol connections

## **Purpose**

- ▶ Understand where and how threats emerge
- ▶ Categorize vulnerabilities across technical and social dimensions

# Ceremony Layers L1–L2

## **L1 – Informational Layer**

- ▶ Protocols: AKA, RSP, TLS
- ▶ Vulnerabilities from server compromise [2]
- ▶ Standards by 3GPP and GSM Association [1]

## **L2 – Operating System Layer**

- ▶ MNO internal apps (e.g., ERP)
- ▶ Issues: privilege escalation, weak auth, insecure APIs [15]
- ▶ Defenses: KSPP, coordinated disclosure [7]

# Ceremony Layer L3 – Human-Computer Interaction

## Focus

- ▶ GUI interactions during SIM swap (CSR and self-service)
- ▶ Attack vectors: social engineering, CSR collusion
- ▶ User deception often circumvents security

## Insights

- ▶ No technical expertise needed for attacks
- ▶ Heavily studied via empirical methods [13, 3]

# Ceremony Layers L4–L5

## **L4 – Personal Layer**

- ▶ Focuses on user behavior and identity
- ▶ Addresses data protection and susceptibility to social engineering
- ▶ Supported by usability/security research [10, 6]

## **L5 – Communal Layer**

- ▶ Involves social norms, laws, and trust frameworks
- ▶ Key institutions: FCC, ENISA
- ▶ Legal gaps highlighted in network security policy [14]

# Targeting a Specific Layer

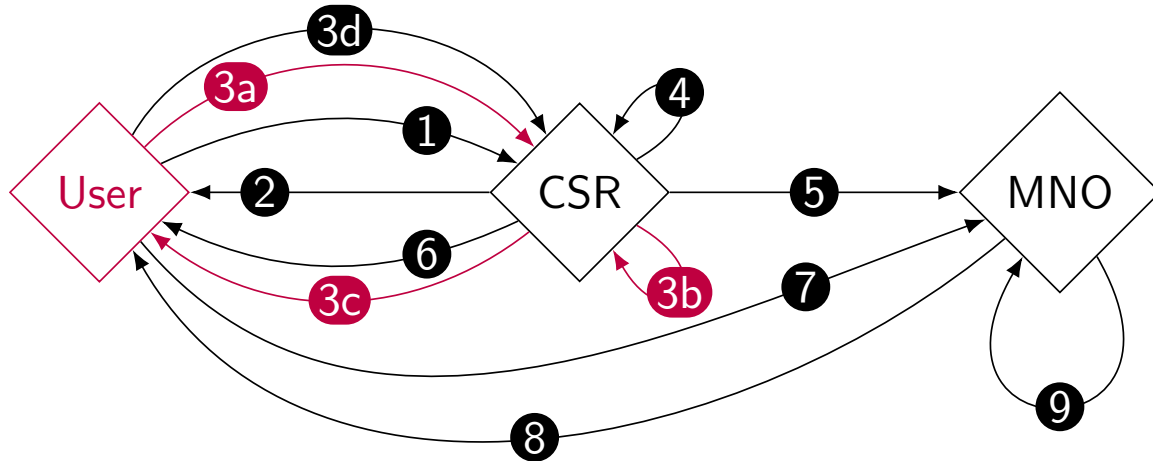
## Layer Focus

- ▶ L1 and L2 have formal studies and protocol analysis
- ▶ L3–L5 often lack formal modeling

## Our Approach

- ▶ Formalize L3 using Tamarin
- ▶ Explore its effect on L4
- ▶ Objective: Capture ceremony structure and simulate potential attacks.

# Modelling SIM Swap in L3 Layer



**Steps:** ①—⑨ outline a typical SIM swap procedure.

# SIM Swap Ceremony Step-by-Step

- ▶ ① A user requests the CSR of an MNO to initiate the SIM swap.
- ▶ ② The CSR requests private account data to authenticate the user.
- ▶ ③d The user sends the requested data to the CSR.
- ▶ ④ The CSR processes and verifies user data to confirm authentication.
- ▶ ⑤ The CSR updates user account with new SIM card ICCID at the MNO.
- ▶ ⑥ The CSR sends the new SIM card to the user via an out-of-band method.
- ▶ ⑦ The user activates the new SIM by authenticating directly with the MNO.
- ▶ ⑧ The MNO provides the IMSI of the new SIM to the user.
- ▶ ⑨ The MNO marks the old SIM card as inoperative.

## Steps involving the attacker (purple):

- ▶ ③a Attacker sends forged user data to impersonate the victim.
- ▶ ③b Attacker loops or reuses previous authentication responses.
- ▶ ③c Attacker tricks the CSR into updating SIM info.

# Tamarin Modelling Approach

- ▶ Tamarin is used to model protocol behavior and verify security goals.
- ▶ Each actor (user, CSR, MNO) is a process.
- ▶ Protocol logic encoded via rewrite rules and logical properties.
- ▶ Attacker follows a Dolev–Yao model but can also simulate social behavior.

# Security Goals Formalized

## Authenticity of Initiator

Only an honest user can initiate a valid SIM swap and complete authentication.

## Knowledge Integrity

A CSR should only approve a swap if the correct authentication data is provided by the source.

# Model Evaluation with Tamarin

- ▶ Property Knowledge holds in all traces — correct knowledge is required.
- ▶ Property Authenticity of Initiator fails in some traces — an attacker can impersonate the user.
- ▶ Two key scenarios emerge:
  - ▶ Honest ceremony: proper interactions among user, CSR, and MNO.
  - ▶ Attack trace: adversary uses stolen data to deceive the CSR.

# CSR Bypass Attack

- ▶ We simulate an insider threat via a rogue CSR.
- ▶ CSR skips validation and approves a fraudulent SIM swap.
- ▶ Attack mirrors previous results but removes need for attacker-user cooperation.
- ▶ Confirms model reflects real-world vulnerabilities in customer support flows.

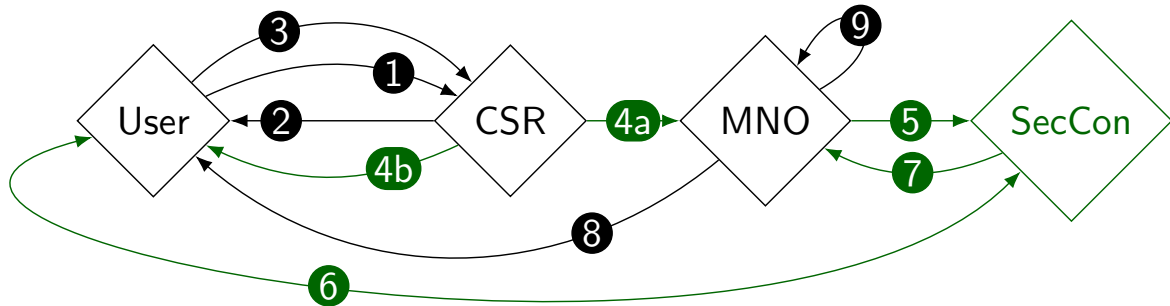
# Authentication Methods: Limitations

- ▶ **Knowledge-based:** Weak due to infrequent use and forgetfulness.
- ▶ **Token-based (e.g., OTP):** Fails if the user has lost access to the original device.
- ▶ **Biometric-based:**
  - ▶ Vulnerable to sensor mismatch, spoofing, and privacy risks.
  - ▶ Increasingly challenged by AI-generated forgeries.

# Social Authentication Proposal

- ▶ Introduce **voucher-based social authentication** to the SIM Swap context.
- ▶ Users select trusted contacts to confirm identity.
- ▶ MNO validates request; MNO contacts security contacts directly.
- ▶ Increases friction for attackers without imposing regular burden on users.

# Modified SIM Swap with Social Authentication



- 4a CSR requests SIM swap from MNO, does not finalize it.
- 4b CSR sends protocol number to user and starts secure contact procedure.
- 5 MNO sends confirmation code to security contact.
- 6 User and contact confirm request via out-of-band channel.
- 7 Secure contact replies to MNO.

# Modelling Social Authentication in Tamarin

- ▶ Extended model adds secure communication with security contact.
- ▶ CSR no longer finalizes the swap — only forwards the request.
- ▶ Secure contact interaction is modeled with additional safe rules.
- ▶ SIM swap only occurs if a trusted party confirms via a secure channel.

# Security Properties Achieved

- ▶ All traces in the new model satisfy our defined properties.
- ▶ Honest confirmation through a separate, secure route adds robustness.
- ▶ Attack is blocked unless all trusted steps are followed.

# Limitations and Future Directions

- ▶ Model assumes safety of trusted contacts and initial setup.
- ▶ Secure contact management remains an open challenge.
- ▶ Ideas for improvement:
  - ▶ Distribute secrets via Bluetooth across regions/devices.
  - ▶ Use asymmetric encryption to verify secret assembly.
  - ▶ Enable contact update via user-approved or MNO-based systems.
- ▶ Full formalization of this scheme is future work.

# The end

Thank you for your time



3rd Generation Partnership Project.

3GPP Specifications per WG: S3, Sept. 2024.

Access date: 2024-09-19.



A. S. Ahmed, A. Peltonen, M. Sethi, and T. Aura.

Security Analysis of the Consumer Remote SIM Provisioning Protocol.

*ACM Transactions on Privacy and Security*, 27(3):1–36, 2024.



G. Bafoutsou, S. Bryska, and M. Dekker.

Countering sim-swapping: Overview and good practices to reduce the impact of sim-swapping attacks.

Technical report, European Union Agency for Cybersecurity (ENISA), Dec. 2021.



G. Bella and L. Coles-Kemp.

Layered Analysis of Security Ceremonies.

In D. Gritzalis, S. Furnell, and M. Theoharidou, editors, *Information Security and Privacy Research (SEC 2012)*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 273–286, June 2012.



G. Bella, R. Giustolisi, and G. 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.



L. Coles-Kemp.

Inclusive Security: Digital Security Meets Web Science.

*Foundations and Trends® in Web Science*, 7(2):88–241, Dec. 2020.



K. Cook and A. Popov.

Linux Kernel Self-Protection Project, Sept. 2024.

Access date: 2024-09-19.



C. Ellison.

Ceremony Design and Analysis.

*Cryptology ePrint Archive*, Report 2007/399, Oct. 2007.



FBI Internet Crime Complaint Center (IC3).

Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public.

Alert Number I-020822-PSA, Feb. 2022.

Access date: 2023-02-10.



M. Grobler, R. Gaire, and S. Nepal.

User, Usage and Usability: Redefining Human Centric Cyber Security.

*Frontiers in Big Data*, 4(583723), Mar. 2021.



T. K. M. Gudimalla, V. P, and S. Kannan.

Survey Analysis of Cloned SIM Card.

*In Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT) 2019*, Aug. 2019.



M. Kim, J. Suh, and H. 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, Aug. 2022.



K. Lee, B. Kaiser, J. Mayer, and A. 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, Aug. 2020.



A. Narayanan and K. Lee.

Security Policy Audits: Why and How.

*IEEE Security & Privacy*, 21(2):77–81, Apr. 2023.



C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera.

A stakeholder-oriented security analysis in virtualized 5G cellular networks.

*Computer Networks*, 184(107604), Jan. 2021.