Secure Design: Focusing on the SKT USIM Hacking Incident

Lee Jeongmin
Department of Computer science
and engineering
Korea University
a23493307@gmail.com

I. Introduction

In April 2025, the SK Telecom USIM data breach resulted in the unauthorized leakage of approximately 26.96 million subscriber authentication records, exposing critical IMSI and USIM key information essential to verifying device identity on mobile networks. Unlike ordinary personal data breaches, this incident directly threatened national telecommunications integrity by enabling SIM cloning attacks capable of impersonating users and intercepting communications. A government investigation revealed that the breach stemmed from prolonged, multi-year infiltration facilitated by weak credential management, plaintext storage of authentication keys, inadequate incident response, and fragmented security governance. This case demonstrates the necessity of applying secure system design principles–particularly in critical infrastructure–to prevent privilege escalation, persistent malware implantation, and undetected data exfiltration, underscoring the urgent need for structural, design-level security improvements.

II. Violation of Principles

The attacker's initial foothold was enabled on August 6, 2021, when Server A in the Internet-facing system-management subnet was compromised. This server stored administrator credentials for other management servers **in plaintext**, allowing the attacker to immediately reuse them. This situation reflects a violation of **Safe Defaults and Open design**, as sensitive credentials were not encrypted by default, and **Least Privilege**, because high-privilege credentials were accessible on a host that did not require them. Furthermore, the reuse of the same credentials across multiple systems violated the **Least Common Mechanism** principle, since compromising one shared mechanism enabled compromise to propagate across multiple components. Using these plaintext credentials, the attacker proceeded to access Server B, which also stored plaintext credentials for the HSS management server. By placing highly privileged HSS-level credentials on a general management server, SKT again violated **Least Privilege**, and by storing them unencrypted, violated **Safe Defaults and Open design**. Additionally, because one credential chain granted end-to-end administrative access, **Separation of Duties** was undermined. On December 24, 2021, the attacker used these credentials to log into the HSS management server and deploy BPFDoor to HSS voice-authentication nodes, demonstrating a failure of **Complete Mediation**, as no re-authentication or authorization verification was required before pushing code across multiple core systems. The centralized ability to push updates to multiple authentication nodes also reinforced the violation of **Least Common Mechanism**, as a single compromised control point propagated compromise widely.

In June 2022, the attacker expanded their presence by pivoting from the system-management subnet into the customer-management subnet, deploying WebShells and further implants. The fact that traffic between these network zones was possible indicates insufficient network segmentation, violating the **Least Common Mechanism** principle by allowing shared communication pathways between zones that should have been isolated. Additionally, movement between subnets and deployment of new code occurred without boundary inspection or authorization checks, violating **Complete Mediation**, which requires that every security-relevant access be validated.

When SKT observed an abnormal reboot in February 2022, the company removed some malware but failed to submit the mandatory 24-hour incident report and reviewed only one of six log files on the HSS management server. This incomplete investigation violated **Complete Mediation**, because security events were not thoroughly examined and unauthorized access remained undetected. The failure to follow mandatory reporting procedures also violated **Safe Defaults**, since the reporting rule itself is designed to serve as a default protective action during potential compromise.

The attacker maintained long-term persistence from late 2023 through April 2025 because administrative passwords had no expiration and were not rotated. This violated **Least Privilege**, as long-lived credentials continued to provide broad access once compromised, and **Safe Defaults**, because the system did not enforce credential rotation as a standard safety baseline. Additionally, the lack of re-authentication checks for returning sessions violated **Complete Mediation**, allowing continued trust in already-compromised credentials.

On April 18, 2025, the attacker exfiltrated approximately 9.82GB of USIM subscriber authentication data from three HSS nodes via Server C, which retained outbound Internet connectivity. Because externally routable network paths were shared by core authentication systems, **Least Common Mechanism** was violated. The absence of default blocking of external transfers from core systems violated **Safe Defaults**, and the lack of monitoring or approval for bulk extraction violated **Complete Mediation**.

Critical subscriber authentication secrets, including the USIM key (Ki), were stored in plaintext, violating **Safe Defaults**, which require encryption of sensitive data at rest, and **Open Design**, since the system's security depended on obscurity rather than robust cryptographic protection. Additionally, IMEI and CDR data were temporarily stored in plaintext and log records were missing, preventing traceability and thereby violating **Complete Mediation**, as access to sensitive data could not be audited.

Further weaknesses were found in malware detection and software supply-chain control. The absence of WebShell detection and insufficient EDR coverage violated **Complete Mediation**, because unauthorized remote execution was not continuously validated. The deployment of contractorsupplied software containing dormant malware without verification violated **Complete Mediation** as well, and because procurement and security verification were not organizationally separated, **Separation of Duties** was also violated.

Finally, governance and forensic readiness limitations prevented effective oversight. CISO authority did not extend to network infrastructure, violating **Complete Mediation** and **Separation of Duties**, as security oversight was fragmented. Logging retention and asset inventories were incomplete, further violating **Complete Mediation** by preventing reliable auditing. Even after a forensic preservation order, systems were modified, demonstrating another failure of mediation. The delayed and incomplete incident reporting continued the violation of **Safe Defaults**, as legally required reporting mechanisms function as baseline safety controls.

III. Design Suggestions

All administrative credentials for HSS and other core management servers must be stored encrypted by default using hardware-backed key stores or vaults (e.g., HSM, KMS, or Vault). Role-based access control (RBAC) should be strictly enforced so each account holds only the minimum privileges required for its function, and all high-impact operations (software installation, configuration changes, data export) must require multi-factor authentication (MFA) plus just-in-time privileged elevation (JIT), ensuring re-authentication and explicit authorization on each sensitive request. These measures address **Safe Defaults, Least Privilege, and Complete Mediation** by eliminating insecure baseline states, reducing over-granted permissions, and forcing per-operation verification.

Network architecture must implement strict segmentation between system-management and customer-facing domains using both Layer-3 and Layer-7 controls, with a default-deny posture for cross-segment communication. Subnet-to-subnet flows should require explicit, logged, per-request authorization and be subject to east-west traffic inspection and micro-segmentation to block lateral movement. By minimizing shared mechanisms and introducing per-request mediation at boundaries, this design prevents a compromise in one zone from being used as a pivot to other zones.

Logging, detection, and forensic processes must be hardened so that all authentication events, configuration changes, administrative sessions, and data access are centrally logged in tamper-resistant storage and retained for at least the legally required period. Incident detection should trigger automated containment and reporting workflows (including automatic 24-hour notification), and any preservation order must immediately enforce system lockdown to prevent post-incident modification. These controls implement **Complete Mediation and Safe Defaults** by guaranteeing that every relevant action is observable, auditable, and subject to protective defaults.

Critical authentication material–USIM keys (Ki), IMSI mapping, and other subscriber secrets - must never be stored or processed in plaintext. Such secrets should be managed using standardized cryptographic safeguards (HSMs or equivalent secure enclaves) and schema designs aligned with GSMA/3GPP recommendations so that the system remains secure even if architectural details are exposed. Temporary working copies must be encrypted in memory where feasible and reliably erased after use. This follows **Open Design** and **Safe Defaults** by ensuring security derives from cryptographic design rather than obscurity.

Procurement and software deployment pipelines must include mandatory supply-chain security checks: code signing verification, integrity checks, sandboxed pre-deployment testing, and provenance validation for contractor packages. Production hosts–especially those in authentication and signaling paths–must run EDR/XDR with WebShell and backdoor detection capabilities. Procurement and security approval functions must be organizationally separated so that no single team can introduce unvetted software into production. These steps satisfy **Complete Mediation and Separation of Duties** by establishing independent verification gates and continuous runtime mediation.

Governance should be centralized at the enterprise level under a CISO with authority across both IT and network domains, while operational tasks remain distributed to specialist teams. Centralized policy, audit, and incident-response authority prevents fragmented controls and ensures consistent enforcement of security rules across all asset classes. This arrangement upholds **Separation of Duties** while enabling effective **Complete Mediation** through a single accountable policy authority.

Default-deny egress controls must be applied to all HSS and core authentication nodes so that outbound Internet access is blocked unless an explicit, time-limited, auditable exception is granted. Any required external transfer of sensitive datasets must pass a three-step process: documented justification and approval, issuance of a temporary, scoped transfer token, and comprehensive packet-level logging of the transfer. This **Safe Defaults and Least Common Mechanism** approach prevents bulk exfiltration even when inner nodes are compromised.

Finally, these technical and organizational measures should be codified into continuous compliance and verification programs: periodic red-team exercises focused on credential theft and lateral movement, automated policy-as-code checks in CI/CD, supplier security scorecards, and regular audits of logging retention and forensic readiness. Together, these controls operationalize the Eight Design Principles–ensuring **secure defaults, minimal shared mechanisms, strict mediation** of every access, **least privilege, separation of duties**, robust cryptographic design, and practical ease of adherence–so that the telecom's critical infrastructure resists, detects, and recovers from attacks of the type observed in the SKT USIM incident.

References

This report was prepared based on the lecture materials provided by the professor, the investigation and press documents uploaded to LMS by the TA for this course, and additional reference materials from external video sources.

[1] Ministry of Science and ICT. (2025). *MSIT Releases Final Investigation Results on SK Telecom Data Breach*. Retrieved from https://www.msit.go.kr/eng/bbs/view.do?nttSeqNo=1139&bbsSeqNo=42

[2] Coding Apple. (2025, april 30). *SKT USIM Data Breach Analysis and Security Implications* [Video]. YouTube. https://www.youtube.com/watch?v=4Xze-DEGN7c

[3] Korea University, Center for Software Security and Assurance (CSSA). (2025). *Information Security (COSE 354-01) Lecture Slide #01* [Lecture slide].