

내 정보는 안전한가요?

-SKT 해킹 사건으로 알아보는 정보보호 3요소

 Google Developer Groups
Sungkonghoe University



Jeongbean Hyun 현정빈
GDG on Campus SKHU 24-25 Server Member

01 SKT 유심 해킹 사건 요약



SKT 유심 해킹 사고 타임라인

- 4월18일: SKT 네트워크 인프라센터에서 트래픽 이상 징후 첫 탐지
- 4월19일: 악성코드 확인 → 문제 장비 격리 → 홈가입자서버(HSS)에서 유출 정황 확인
- 4월22일: 한국인터넷진흥원(KISA)에 공식 신고
- 4월25일: SKT 유영상 CEO 공식 사과 및 유심 무상교체 발표
- 4월28일: 유심 무상교체 본격 시작, 전국 매장 혼란

↻ Sync Letter



- 2025년 4월 발생
- 해커가 SKT의 HSS 서버에 침입
- IMSI, KI, 전화번호 등 유심 인증 정보 유출

02 해킹된 정보, 대체 뭐길래?



IMSI

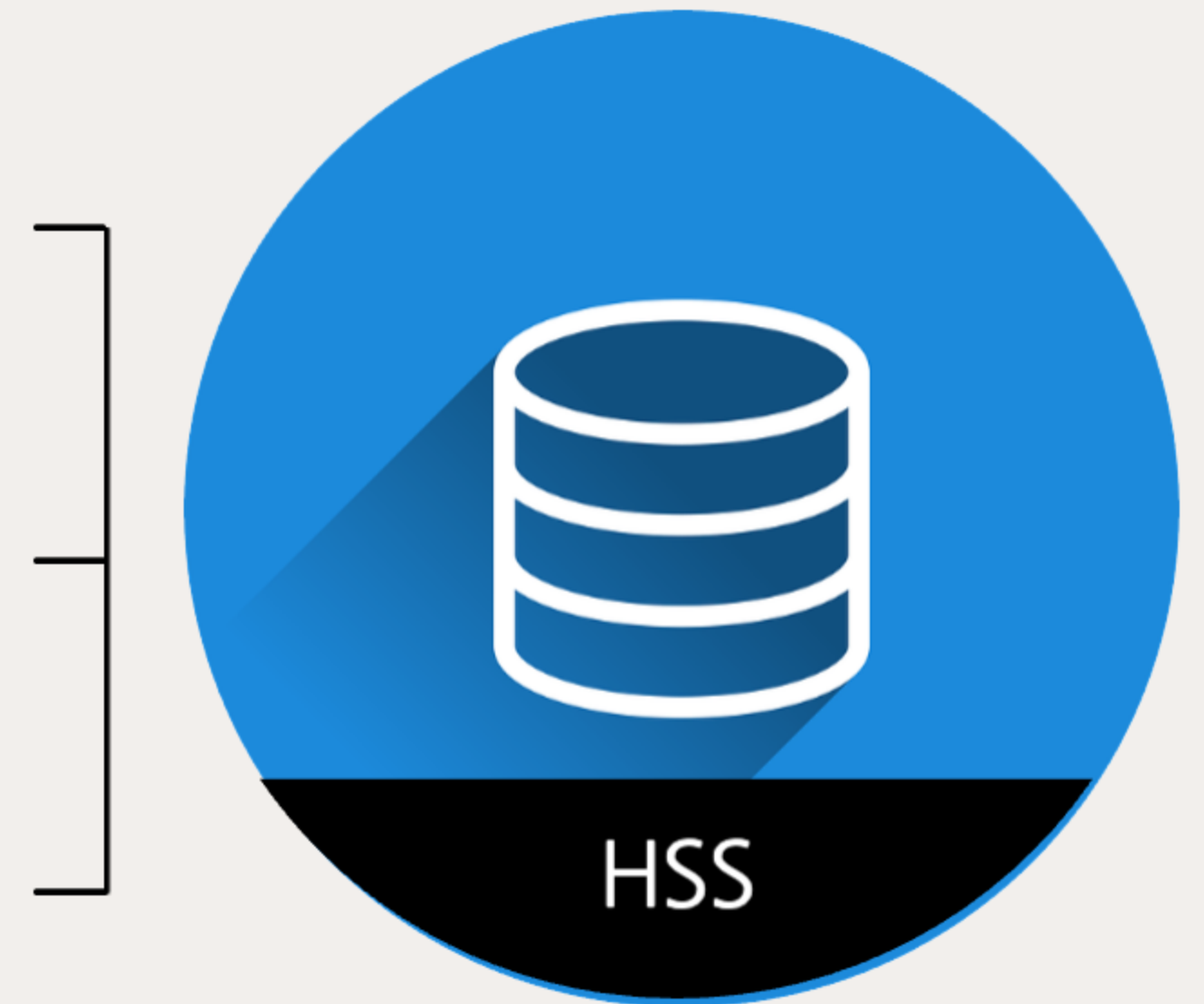
유심에 저장된 국제 고유 사용자 번호
통신망에서 '내가 누구인지' 인증할 때 사용하며, 해커가 복제 유심을 만들 수 있는 핵심 정보

KI

유심 내부에만 저장된 비밀 인증키이다. 통신사와 유심 사이에서 '이 사람이 진짜 고객인지'를 판단할 때 사용됨. 절대 외부로 노출되지 않아야 하는 가장 민감한 정보

전화번호

통신사가 유심과 연결해 사용하는 사용자 ID이다. 유심을 바꿔도 전화번호는 그대로 유지됨.
복제 유심으로 내 번호를 도용당하면, 문자·통화·인증문자 탈취가 가능해짐.



03 정보보호의 기본 원칙



기밀성



허락된 사용자만 정보 접근이 가능해야 한다.

무결성



정보는 변형되지 않아야 한다.

가용성



허락된 사용자는 언제든지 통신 서비스에 접근이 가능해야 한다.

03 정보보호의 기본 원칙 - 기밀성



기밀성



허락된 사용자만 정보 접근이 가능해야 한다.

- 이번 SKT 해킹 사건에서는 HSS 서버에 저장된 IMSI, KI, 전화 번호 등 유심 정보가 외부 해커에게 유출



기밀성 침해에 해당

- 통신망 인증에 사용되는 정보가 유출되면 복제 유심 제작이나 통신망 위조 접속이 가능해지므로, 인증 정보의 보호는 기밀성의 핵심



나만 알아야 할 정보가 유출 된 상황

03 정보보호의 기본 원칙 - 무결성



무결성



정보는 변형되지 않아야 한다.

- 무결성은 정보가 조작되거나 거짓으로 사용되지 않아야 함
- 해커가 유출된 정보로 '복제 유심'을 만들어 통신사 시스템을 속여 가짜 정보로 인증 성공하게 된다면?

 무결성 침해에 해당



인증 시스템이 '가짜 정보'를 '진짜 정보'로 착각할 수 있는 상황

03 정보보호의 기본 원칙 - 가용성



가용성



허락된 사용자는 언제든지 통신 서비스에 접근
이 가능해야 한다.

- 가용성은 서비스가 항상 열려 있어야 한다는 원칙
- 아직 침해되진 않았지만, HSS 서버가 공격받고 마비됐다면?

➡ 전국적인 통신 장애가 발생할 수 있었던 잠재적 위협



가용성 침해 상황은 대규모 사회적 피해로 이어질 수 있음

04 단순한 보안 사고가 아니다



- **보안은 비용이 아니라 의무이다.**

SKT처럼 국민 대다수의 통신망을 관리하는 기업에게 보안은 선택이 아닌 공공 의무

- **공공재적인 시스템에는 공공 기준이 필요하다.**

HSS 같은 인프라 시스템이 정부 점검도 없이 방치된 것은 매우 심각한 문제

- **HSS 유출은 단순한 유심 문제가 아니다.**

통신사의 중앙 인증 서버(HSS)에서 사용자의 인증 정보가 유출된 것은 유심이 도난당하지 않아도, 복제 유심이 만들어질 수 있는 구조적 문제

- **데이터는 사람이자, 신원이다.**

유심 정보는 단순한 번호가 아니라 내가 누군지를 증명하는 수단

[

감사합니다

]

참고자료

IMSI와 IMEI, 도대체 뭐가 다른 걸까?

<https://seok007.tistory.com/entry/IMSI%EC%99%80-IMEI-도대체-뭐가-다른-걸까>

보안의 3요소란_C,I,A

http://www.bomnetworks.com/bbs/board.php?bo_table=secuguide&wr_id=595

보안 뉴스, [SKT 해킹 사태 중간점검] 사건 경위와 현재 상황, 그리고 드러난 문제점

<https://m.boannews.com/html/detail.html?idx=137079>

SK텔레콤 홈페이지

<https://news.sktelecom.com/211829>

SKT 뿐만이 아니었다..KT, LG유플도 '같은 상황' 헉 #뉴스다 / JTBC News

<https://www.youtube.com/watch?v=BnidTbjZq4I>