SIM / USIM CARDS[1] - AREAS FOR INVESTIGATION

NOTES

1. Target products (any of these are perfect targets for hacking)

- Microprocessor cards
  a. Classis SIM / USIM cards
     Interest of nation states (SIM is a key to communication eavesdropping and geo-tracking, SIM cloning for 2FA)
  b. eSE (virtual SIMs and connected cars in particular)
     Same as above for eSIM, car security
  c. Banking cards (Visa, NFC, etc.)
     Bank key extraction implicates direct financial loss
  d. Government IDs (driving licenses, e-passports, national IDs)
     Potential target for nation states, criminal groups and terrorists
  e. Access cards (DoD relying on smartcards [1] for employee access to facilities, etc.)
     National security at risk
  f. IoT (secure boot / key storage for cloud, secure channel to cloud backend, e-meters)
     Cloud security (Google partnership with a smartcard manufacturer [2], use of eSE in the cloud), IBM X-Force bugs from 2020[2]
- Vendor SW for the above provided to partners / MNOs
  a. Personalization
  b. Deployment
  c. Remote management
  d. SW Update
  e. Gateways

  Potential leaks regarding products operation, proprietary APIs, keys, certificates, vendor network details, easier reverse engineering / product exploration and hacking

2. Key areas for security evaluations

[1] The information provided in this document may apply to 4G and 5G cards (no vendor / reseller were keen to provide / sell us such product samples for investigation)

[2] The X-Force bugs from 2020 triggered our research into Cinterion IoT devices, which resulted in multiple vulnerabilities [3]

- Java Card VM implementation
- Secure OS such as Trusted Logic one (TOS), their cards have CC evaluations, but flawed implementation can have devastating impact (card hack [4] -> reverse engineering [5] -> bug hunting -> remote bug [6])
  Those with access to card samples and keys (partners, MNOs) are able to peek into the cards
- APDU handlers (API directly exposed to attackers – over-the-air and over-the-wire)
- unpublished APIs (such as for privilege elevation - some were noticed in SIM implementations for security disabling / enabling, etc.)
- Remote SIM provisioning
- Software update mechanisms for SIM (newer cards implement these)
- Remote card management (MNOs need it)
- Security of custom applications provisioned into the card (there can be multiple of it, one insecure app can open access to the card)
- Various communication protocols (STK, WIM, BIP, S@T, SCWS), some were found to be vulnerable in the past (Simjacker [7])
- NFC implementation
- Parsers (MMS, CAP file, certificates, etc.)
- Man in the middle attacks (attacker positioned between MNO and a card or at the modem layer)
- USSD, CBS handlers
- Keys storage and security domains
- Side channel attacks
- SW used by MNOs to provision and manage cards / subscribers
- The data exposed to 3rd parties (manufacturers)
- Impact of fake mobile towers / SS7 protocol flaws to card security

REFERENCES

[1] Military CAC: The U.S. Department of Defense DoD Common Access Card
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/usa-dod

[2] Gemalto Gives Google Cloud Platform Customers Flexible Encryption and Key Management
https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/gemalto-gives-google-cloud-platform-customers-flexible-encryption-and-key-management-

[3] Cinterion IoT devices
https://security-explorations.com/cinterion-devices.html

[4] SE-2019-01-GEMALTO, Issues #19 and #33
https://security-explorations.com/materials/SE-2019-01-GEMALTO.pdf

[5] SE-2019-01-GEMALTO-2, Issue #34
https://security-explorations.com/materials/SE-2019-01-GEMALTO-2.pdf

[6] Reverse Engineering Java SIM card
https://security-explorations.com/materials/javasim-reversing.pdf

[7] Simjacker – Next Generation spying via SIM Card Vulnerability
https://www.enea.com/insights/simjacker-next-generation-spying-over-mobile/