www.pipelinepub.com
Volume 18, Issue 2

E-MEID: The Next Thing in Smartphone Security

By: Kevin L. Jackson

Your personal communications network is under vicious attack! The Communications Fraud Control Association (CFCA) biannual survey estimated that global fraud loss in 2019 reached $28.3 billion. This number equates to 1.74 percent of the 2019 estimated global telecom revenues, with the top five fraud types accounting for 54 percent of all fraud losses. This estimate was an increase from the 2017 figures of a total loss of 1.27 percent of global telecom revenues. To put this percentage loss in perspective:

- For AT&T, with $171.8 billion annual revenue in 2020, this number represents a potential revenue loss of $3.1 billion to fraud.
- For Telefonica Group, with a $49.2 billion annual revenue in 2020, this number represents a potential revenue loss of $915 million in revenue to fraudsters and criminals.
- For Vodafone Group, a $50 billion a year business, this number means that $930 million just walked out the front door.

In a more recent statement from Proofpoint, reports of text message scams—or smishing—have increased by nearly 700 percent in the first six months of 2021 compared to the second half of 2020. The company also found three times as many parcel smishing attacks as there were banking smishing attacks.

There are even more reports coming from another malevolent attacker front referred to as facility takeover. This attack is when a fraudster can take control of a mobile phone account, usually after tricking the real customer into revealing personal details. Fraud prevention body Cifas and Mobile UK reported that this form of telecommunications fraud has increased by 88 percent over the past three years, with over 17,500 instances recorded in 2020.

The danger of being victimized by these types of attacks on your everyday life is real, severe, and only getting worse. This unsettling truth is why we're highlighting Enhanced Mobile Equipment IDentifier (E-MEID) mobile device security technology as a top 2022 technology trend.

The E-MEID

A **M**obile **E**quipment **ID**entifier (MEID) number is a globally unique 56-bit identifier for a physical piece of wireless network mobile station equipment. Globally administered by the Telecommunications Industry Association (TIA), MEIDs typically show the manufacturer code and the equipment serial number. The number is permanently affixed to most wireless devices and used to facilitate the identification and tracking of mobile equipment like your smartphone. Assignments are coordinated with International Mobile Equipment Identifiers (IMEIs) to enable global roaming and harmonization between 3G, 4G, and 5G technologies.

An E-MEID is a digital representation of the MEID recorded on a shared digital ledger or blockchain. A blockchain is capable of recording and verifying transactions between two or more parties. This documentation is cryptographically protected and immutable, meaning it cannot be changed without consensus agreement by all participating parties. Blockchain's most famous use case is in the financial industry, which is the foundational technology behind Bitcoin. However, the shared digital ledger concept can apply to any use case where two or more parties maintain verified and auditable transaction records. For smartphone security, the transaction records support the protection and provenance of this personal piece of mobile station equipment.

Enhancing security

By recording the device MEID to a blockchain, a globally unique digital token can represent the associated smartphone or any associated physical or digital asset. This digital token is the E-MEID, and "tokenization" is the name of this process. With the MEID attached to a blockchain, device and network security documentation capabilities expand to include hardware bill-of-material (BOM), software BOM, and software remediation activity. This additional capability can enhance hardware and software supply chain visibility, component provenance, and internal change management processes. The E-MEID can also leverage smartphone geospatial location technology to add time-limited and geofenced functional management capability. These additions can dramatically enhance security and provide near-real-time operational options based on the location of the associated physical or virtual asset. An organization, for example, could disable software running on an E-MEID-provisioned piece of equipment based on its geolocation.

E-MEID can also be used to automate many mobile device management processes. For example, relevant vulnerabilities at a user-specified severity can be automatically detected and recorded using the National Vulnerabilities Database (NVD) maintained by the US National Institute of Standards and Technologies (NIST). This database is the US government's repository of standards-based vulnerability management data. The E-MEID can help automate the recording of relevant vulnerability information on a blockchain and immediately flag it for cybersecurity threat remediation. The distributed ledger can also record digital signatures for validating the initial BOM, any subsequent modifications and automate the collection of equipment supplier

performance data. This capability can monitor and evaluate supply chain security maturity and automate input to external provider performance management processes. The information is also available for rapid identification and response to product recall or required design or configuration changes.

2022 smartphone security advancements

Solutions enabled by this exciting security technology include protection against vishing and smishing attacks, smartphone SIM-jacking and unlicensed use of streaming digital media. SIM-jacking essentially takes control of someone's phone number and tricks a carrier into transferring it to a new phone. Vishing is used to describe an attempt to commit fraud using a voice call, while smishing is a fraud attempt using SMS text messaging.

Crypto Gabriel from Forward Edge AI uses the E-MEID to digitally document smartphone device identification, verify personal contact devices, and detect counterfeit smartphones on the wireless network. This advanced smartphone security suite also uses swarm intelligence, AI, machine learning, natural language processing, and the power of 5G networks to stop vishing and smishing on all devices and across all service providers. Another platform function, called $DigitalNames, documents and verifies access to cryptocurrency rewards earned by the user for reporting phone-based scams and robocalls.

COMSovereign, a US-based pure-play communications provider, is pairing its eSIM technology with the E-MEID to deliver next-generation wireless network security. Most smartphones currently use a physical Subscriber Identity Module (SIM) card. An embedded SIM (eSIM) is a programmable SIM embedded directly into a device. They cannot be removed and enable instant network connectivity, customization, remote provisioning, and global roaming between eSIM capable network service providers. The eSIM can deter SIM-jacking, but the COMSovereign eSIM also collects pertinent network security data for immutable and cryptographically protected storage on the E-MEID blockchain. This data can provide a verifiable record of network security operations, automated software vulnerability alerts, software provenance insight, change management process documentation, hardware or software component changes, and mobile device traceability data.

Total Network Services and Rypplzz are using the E-MEID to guard against unlicensed digital streaming content use. The companies combine $DigitalNames and a new media file format, called MFX, to prevent streaming content piracy caused by lost or stolen passwords, rootkit modified smartphones, or other malicious or illegal acts. MFX is a new media file format that has internal artificial intelligence (AI) scripting. AI constantly communicates with the management platform using its own decentralized global data network. This approach delivers complete content management and online distribution capabilities. The E-MEID documents and verifies licensed content consumption from the device while $DigitalNames documents authorized access to the content by the user. Rypplzz-embedded geospatial management services are used to geofence access to streaming content or disable access based on device location.

The E-MEID can also help address the telecommunications industry's supply chain security challenge. According to recent reports, the industry annually sells approximately $140B in counterfeit parts. This supply chain security failure results in 6.5 percent of ICT products having counterfeit parts and nearly 20 percent of mobile phones shipped being fake. As a consequence, the TIA is leading an initiative that goes beyond current organizational information security standards. The industry think tank sees the current standard as not specific enough to address potential security vulnerabilities in the supply chain. This challenge is why the TIA initiated its Supply Chain Security 9001 Standard development work in 2020. The effort represents a comprehensive approach to improving supply chain security by incorporating proven elements of existing industry-driven standards and adding new ICT requirements that address modern networks and their supporting technologies. A recent SCS9001 pilot project showed that the E-MEID could be used to automate the documentation of five of the 11 recommended security evaluation metrics.

In summary, the E-MEID can be used to improve many facets of wireless network security, including the automated detection of counterfeit smartphones, smartphone software vulnerability monitoring, malicious modification of smartphone software, smartphone vishing and smishing attacks, and unlicensed use of digital streaming content.

To learn more about how your organization could leverage this blockchain-enabled technology, please visit Total Network Services at https://TNSCorp.io or contact Kevin L. Jackson at Total Network Services kevin@TNSCorp.io.

_____

TIA does not endorse TNS or the solutions it proposes. TIA is technology and vendor neutral. The MEID is managed by TIA and the "enhanced" aspects proposed by TNS are products and services that utilize the MEID but are not standardized by TIA engineering committees nor approved or marketed by TIA.