Securing 5G Through Cyber-Telecom Identity Federation

Craig Gibson
Trend Micro Reseach

TREND MICRO™
Securing Your Connected World

Published by:

Trend Micro Research

Written by:

Craig Gibson

Stock image used under licensed from Shutterstock.com

Contents

Many industries are keen on taking advantage of the speed, automation, and global reach of 5G, but have little to no direct experience in telecommunication technology. The risks and vulnerabilities in carrier telecommunications will be exacerbated to organizations unprepared and unequipped to handle 5G.

Threat actors and their attacks on decades-old telecommunications technologies will be interoperable within 5G's new cyber-telecom domain. Cyber-Telecom (CyTel) organized crime has an active and full ecosystem spanning the world, and the 5G environment can be their new frontier given 5G's speed, scalability, and global reach. These could also be used to increase the illicit revenues from other less complicated cybercriminal schemes.

The 5G Telecom Network

5G is a global, high-speed network capable of handling the traffic of many different kinds of radio, including satellite. It is a far-reaching topic that may include different and interrelated issues — from laws, standards, politics, and supply chains, among others. It may be easier to discuss 5G as a smaller Local 5G Campus Network, also known as a Non-Public Network (NPN), which may be found in environments like smart factories, smart cities, and other small, controllable regions.

A way to further break down 5G's complexity is to address each element individually. In the context of a 5G network, telecom is a mature, Subscriber Identity Module (SIM) card-based global radio network. SIM cards contain identity, encryption, and even small applications, and act as small computers. Like typical computers, SIM cards can be updated in a way similar to patching.

The new 5G network is data-centric, and with its emphasis on data above all other technology types (even radio), the network can be automated and scalable. The nested tiers of automation can pass data much more easily than in previous, heavily manual generations of network such as 2G, 3G, or 4G. 5G's data-centric nature relies heavily on the nested tiers of software-defined network automation to reduce manual effort and enable the network to handle the huge volumes of data from the Internet of Things (IoT).

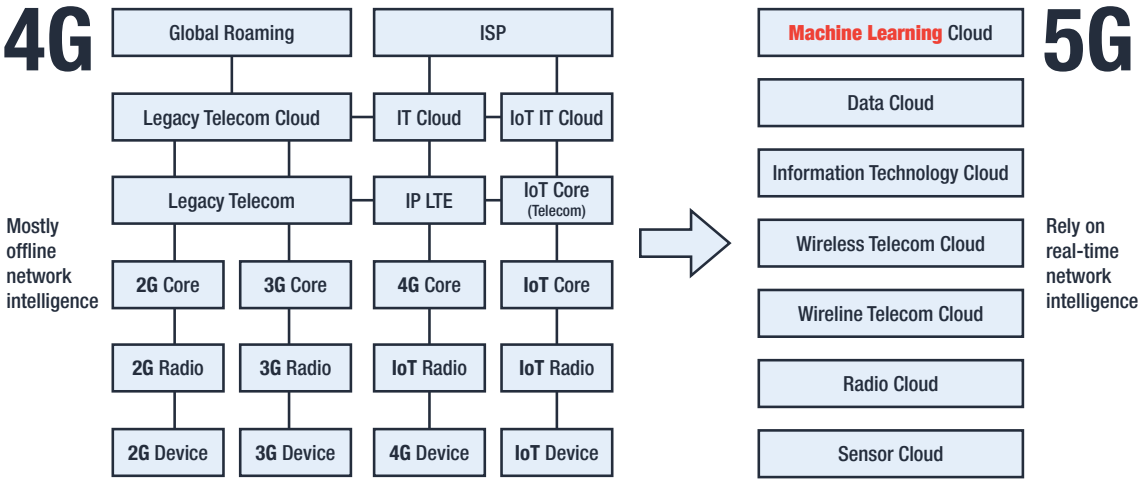

Figure 1. Evolution of telecom architecture: a comparison of 4G and 5G

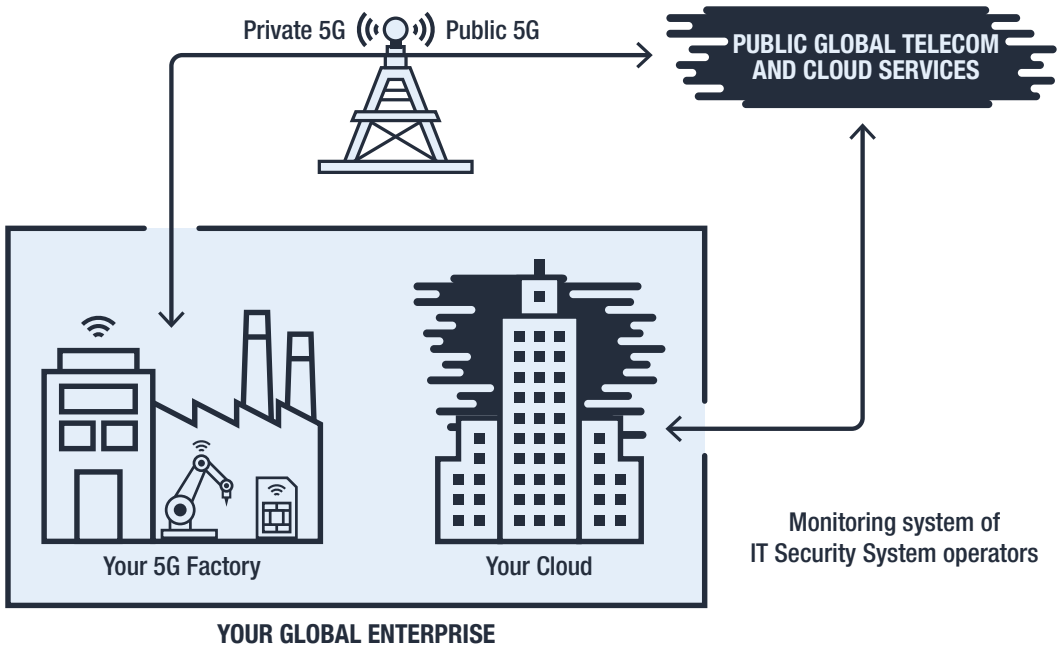

Figure 2. A representation of an NPN

As shown in Figure 2, an NPN has a fundamental vulnerability in its design. The cloud and management traffic of an enterprise passes through various security functions and up through the global IT cloud. This traffic then traverses the global telecom cloud, and then through public and non-public radio networks. There is no IT-visible security monitoring on this part. Many roaming-, long-distance-, radio-, and other CyTel-based attacks can ride on this to compromise the telecom, and therefore the 5G network itself.

We present three examples of active attacks targeting hardware, data, and CyTel.

Hardware-level Attack: SIMjacking

Telecom 5G is a data-centric network, and the risks it poses can come from the traffic a typical IT platform does not have visibility to. This lack of visibility impairs unified telecom-IT traffic authentication and identity required for securing IoT and mobile devices. This expands an attacker's ability to use cellular radio "roaming" (using non-private radio network suppliers for telecom connectivity) to bypass traditional IoT security perimeters.

Roaming can also be used or "forced" as part of an attack. One of the ways this can be done is by using radio or long-distance attacks to change the SIM card and alter its on-board configuration to attach its radio to an attacker-owned or controlled network. In this case, the threat actor can then make simple but important changes to the SIM card, such as its DNS, BGP, and carrier settings. These changes can then open doors to threats: wiretap, malware injection, large-scale fraud, poisoning of machine learning, and supply chain attacks, among others.

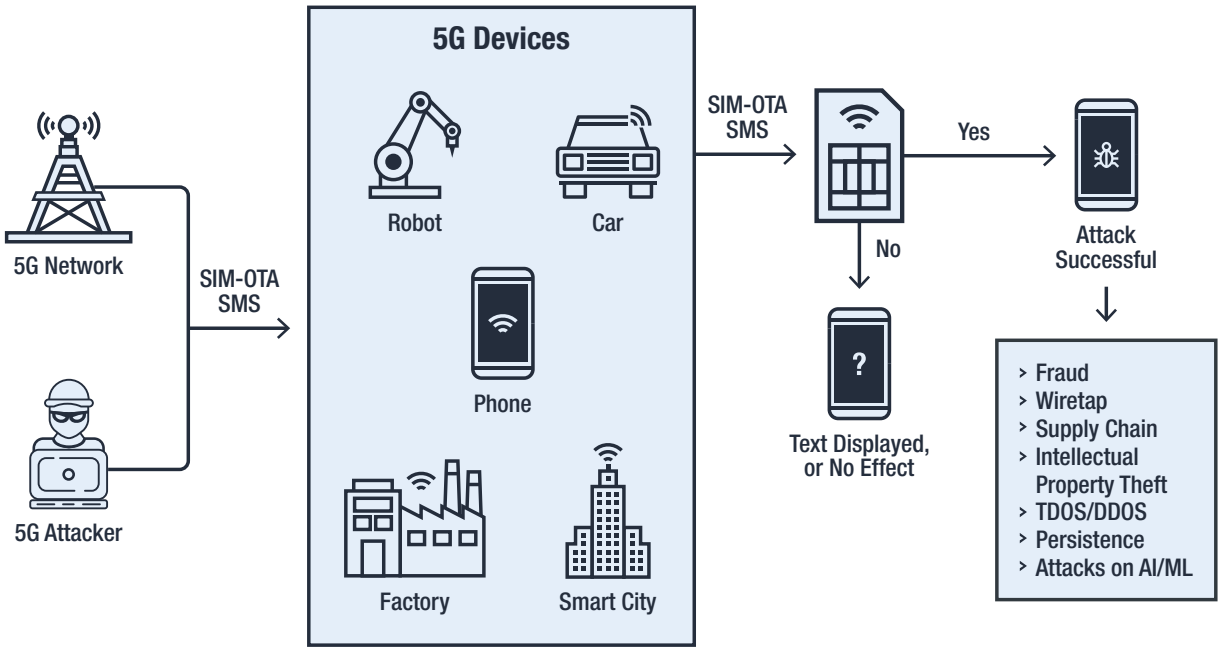

Figure 3. A visualization showing SIM jacking by abusing the SIM-OTA SMS operational technology (OT)

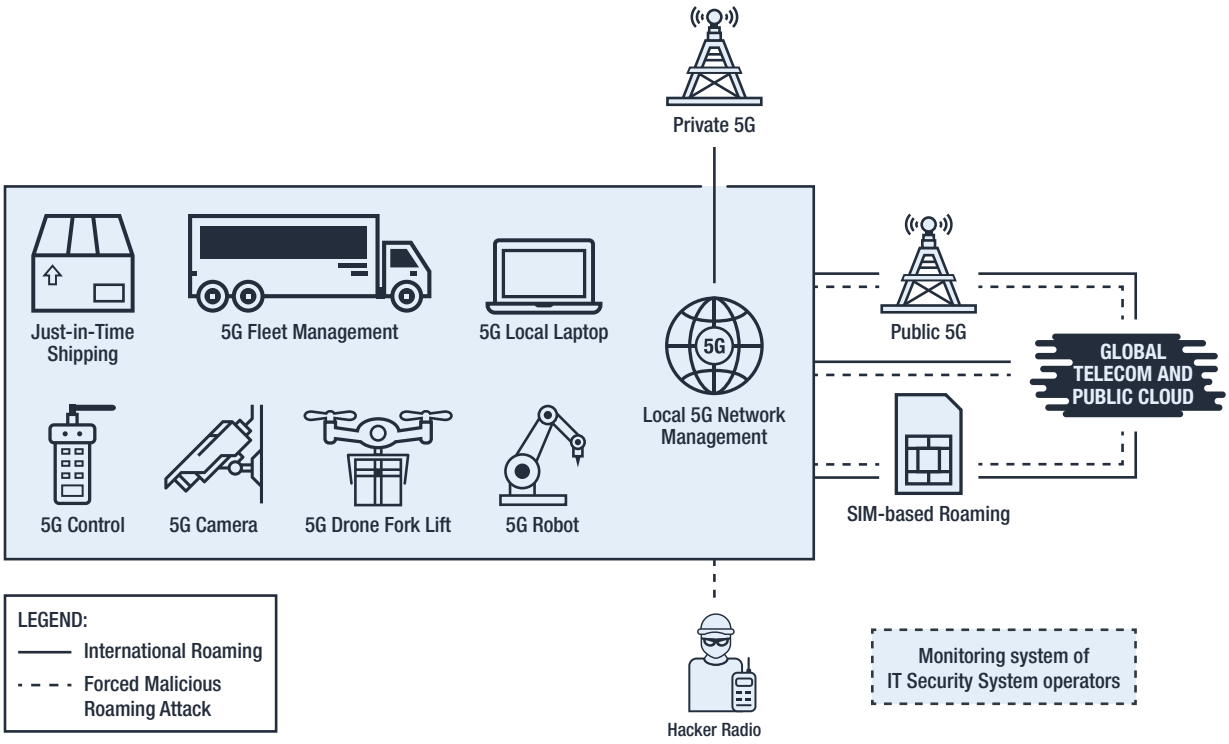

Figure 4. Visualization showing how roaming can be forced to be part of an attack chain

Data-centric, Network-based Attacks

Different kinds of attack similar to identity theft can be carried out in the telecom domain. This includes, but not limited to, illicitly using a victim's identity to download malware, initiate and authorize network-level actions such as identity-driven transactions and billing. Just like a credit card, a SIM card represents a billing relationship and can accrue debt or damage its owner's reputation.

A hijacked SIM card can also be used to change the device's activity profile and thus how it's treated by the network. This may consequently prohibit the device from performing certain tasks, degrade its performance, or, in extreme cases, adversely affect the entire 5G campus network. When this kind of attack is performed by large number of devices (a salami attack), but slowly and patiently (a low-and-slow attack), the network will not be able to identify that an attack is occurring until it is too late. With time, the network's baseline will be used to make trend-based rules governing the network. The blind spots will widen when these poisoned rules govern the network, and with time these blind spots will be big enough to allow for more significant attacks.

This class of attack is evolving in the cybercriminal underground with the emergence of SIM-jacking malware and its capability for scalable automation. With 5G, SIM-jacking malware's impact can become more scalable and increase the speed with which it can modify trusted, SIM-authorized traffic in the network.

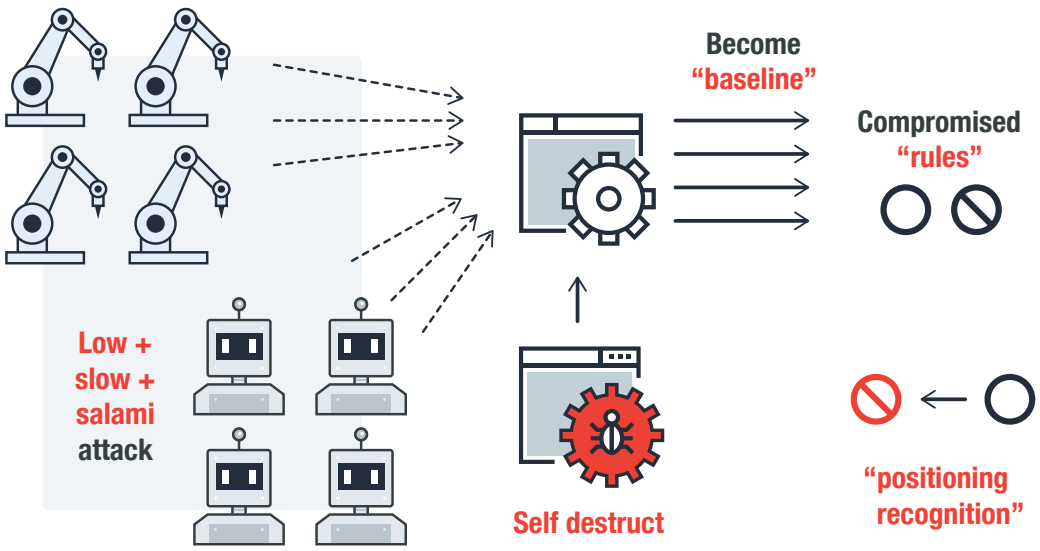

Figure 5. Visualization of how a combination of salami and low-and-slow attacks can poison rules governing a 5G network

Gaps in Handling Identities in IT and Telecommunications

There is a gap or disparity between how identity is handled in IT and telecommunications. Most identities in the latter are handled by the SIM card, while identities in IT has very little visibility, if none at all. Identity is managed at the hardware level by the SIM card, and at the application level in IT, which can be easily exploited by telecom attacks. Perpetrating identity theft on the SIM can be carried out, for example, since the IT-based identity trusts the device's hardware, which, in turn, trusts the SIM's identity.

Another gap that can be exploited is in the unified identity assurance between IT and telecommunications. The latter is driven by devices and network process standards, both of which have the risk of having contaminated data slip into an organization, which can consequently affect its operations. Examples of this include techniques to bypass antifraud measures in order to perpetrate international revenue sharing fraud (IRSF) and planned bust-out schemes. Threat actors can also modify statistics by introducing statistical noise to alter the threshold and prompt an alert or similar interferences that can distract the enterprise's systems. These distractions can have real-world effects: changing the functions of the network, hiding attacks via statistical blind spots, and altering products coming off a production line. Supply chain attacks can also be carried out on data as well as physical devices and products dependent on that data.

A Solution: Cyber-Telecom Identity Federation

There are three elements of integrity that must be unified as a single response to bridge the aforementioned gaps: data network, SIM and device, and roaming.

Data Network Integrity

Attacks like SIM jacking affect the integrity of the device's data traffic. An approach to protecting the integrity of a 5G, data-centric network is to make the identity of devices in both the telecommunications and IT domains portable (or visible) to IT Identity and Access Management (IAM) systems, even when roaming. The multiple systems where this identity is ported to are considered to have Federated Identity and Access Management models (FIdAM) between each other. This unity allows an existing security solution to be applied to IoT traffic coming from devices that may be SIM-jacked or otherwise successfully compromised by exploiting vulnerabilities. FIdAM is a means of bridging traditional IT security architectures with those from telecommunications through a Zero-Trust Architecture (ZTA) proposed by the National Institute of Standards and Technology (NIST).

Federating the telecom- and IT-enabled device identities, for example, allows existing security solutions to see into the traffic of 5G-enabled IoT devices and detect known malicious behaviors. A way to implement this is the use of a distributed ledger placed within the SIM as an application. This can apply ledger-based and IT-visible encryption to both the data coming from the device and further secure the device's firmware. If the firmware has been altered (i.e., from a roaming attack), this can be verified during the FIdAM authentication process. These help detect and address the potential hardware-level impact of SIM jacking and similar IoT attacks.

SIM and Device Integrity

A means of portable identity can be implemented within the SIM itself, in addition to the traditional telecom-visible information. This additional information is a security-oriented distributed ledger similar to the SIM global authentication security architecture in use globally for decades. This distributed ledger is an application within the SIM that is a visible (portable) identity that can be used in FIdAM models

for authentication of devices and people. This ledger can be used to assert firmware integrity; provide a unique, SIM-based device identity even when the telecom carrier has assigned identical keys to all devices (a difficult-to-detect telecom misconfiguration error); and tie both the SIM card and the entire IoT-based telecom domain into the IT security architecture.

Roaming Integrity

SIMs are part of the global telecom architecture that enables roaming to occur. For decades, SIMs have functioned as a telecom-visible distributed ledger visible to the telecom function called Global Titles, with their corresponding Global Roaming Exchange (GRX). While this function is critical to the implementation of telecom security, it does not bridge into the IT domain. The use of a blockchain-derived, distributed-ledger function on the SIM allows a blockchain's SIM-like security architecture to be enforced even when the device is roaming or affected with forced-roaming telecom attacks.

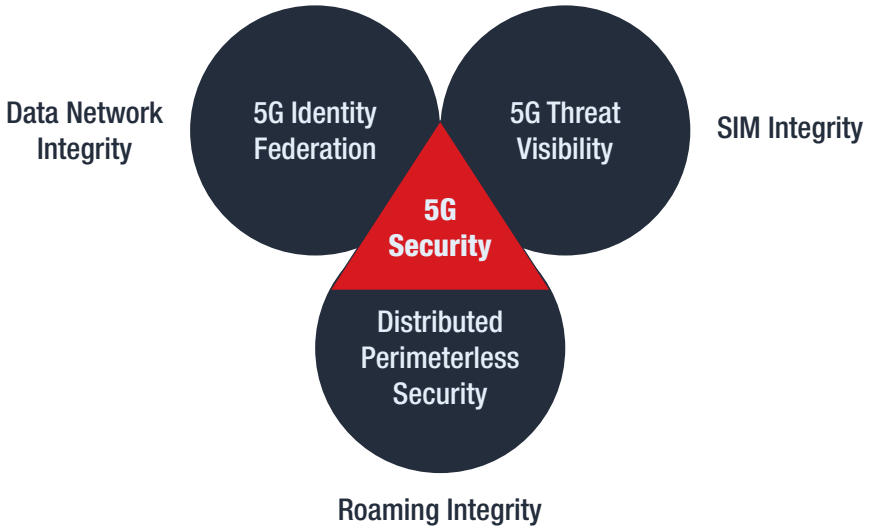

Figure 6. Visualization of an approach to 5G security

5G security should not be an afterthought

5G is a response to the need for bandwidth, consistency, and speed, especially in an era where mobile and IoT devices are ubiquitous among enterprises and industrial facilities increasingly move toward digital transformation. But like any nascent and dynamic technology, it doesn't come with security and privacy risks — which can have significant repercussions given the kind and vast amount data that 5G is poised to collect, process, and interpret.

Security strategies, technical skills, and additional technologies are needed to ease the organization's transition to adopting 5G and fully reaping its benefits. ZTA's core principle is to maintain security even when the device is uncontrolled, moving down the road, or travelling outside the network perimeter. The federated cyber-telecom identity model is an approach to 5G security that provides a single and coherent security architecture for protecting the identity, access to, and integrity of data and other components and technologies within 5G networks.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™

Securing Your
Connected World