nCore Communications, Inc.

nCore IoT Security Solution

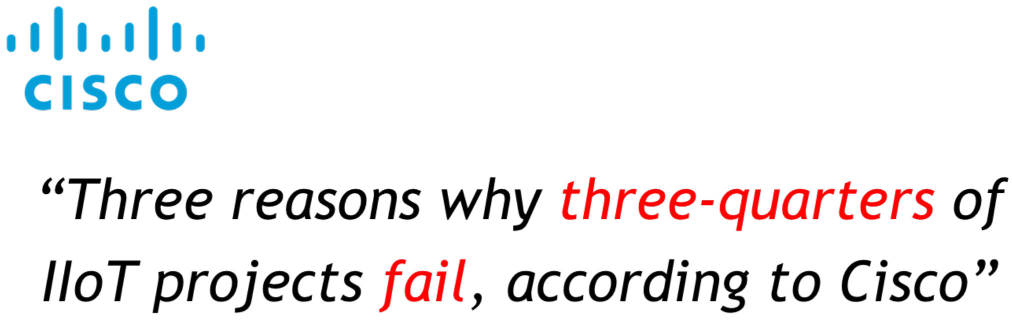
Table of Contents

1. Introduction

This document discusses nCore Communications novel IoT and Industrial IoT security solution and products. The discussion is high level, avoiding a detailed technical description. nCore Communications is happy to provide more information, if required.

2. Background

In May 2018, Cisco announced[1] that 75% of all IIoT projects fail for 3 fundamental reasons, with "security" being number one reason.



"Three reasons why three-quarters of IIoT projects fail, according to Cisco"

#1 reason is SECURITY

At the same time, ARM announced[2] the integration of SIM into their processor fabric (iSIM).

[1] https://enterpriseiotinsights.com/20180504/channels/fundamentals/three-reasons-iiot-projects-fail-tag40-tag99?elqTrackId=6122A53DC12C5A699C8855BF98B62C02&elq=20546dd3dc27422ea9600a355f74369e&elqaid=7060&elqat=1&elqCampaignId=6015

[2] https://www.arm.com/news/2018/02/arm-delivers-integrated-sim-identity-to-secure-next-wave-of-cellular-iot-devices

ARM

"Arm delivers integrated SIM identity to secure next wave of cellular IoT devices"

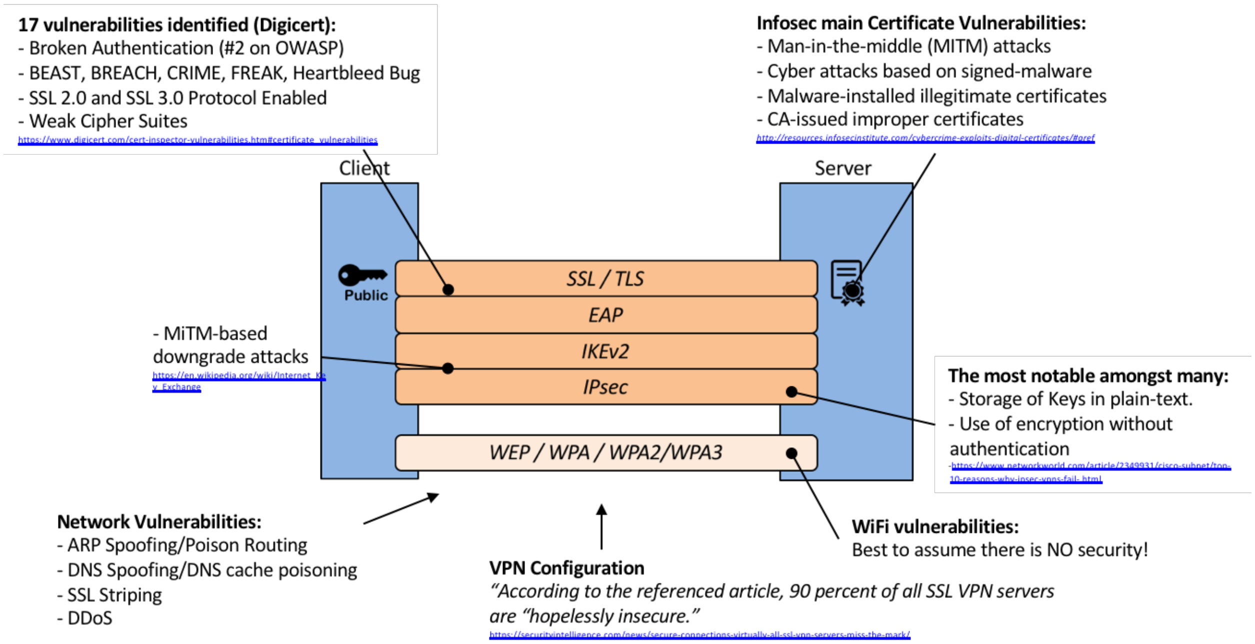
How can we use this for other access technologies?

Unfortunately, ARM's integrated SIM will only provide security for IIoT devices using cellular connectivity such as LTE and 3G. Most industrial IoT devices will be indoors in hard-to-reach places such as factories, hospitals, warehouses, etc. In such environments signal may not be of sufficient quality and quantity to meet the connectivity requirements such as speed, capacity and robustness. There is also the high expense associated with cellular networks, limiting data volumes and prohibiting applications such as patient file transfer, security cameras and large and frequent SW updates.

Fortunately, nCore technology addresses this shortcoming and enables the use of SIM-based security with other types of access technologies such as WiFi, Satellite and Ethernet. This is particularly encouraging since all IIoT devices using ARM processors, will have an iSIM by default, which can now be used with all and any access technology.

3. Why nCore Solution?

A best IoT security is currently based on the conventional Cybersecurity suite shown in Figure 1. Although the current Cybre suite offers the best security to date, it has many vulnerabilities that can be exploited, especially in an IoT setup, as IoT devices are simpler and cheaper than say a personal computer.



17 vulnerabilities identified (Digicert):
- Broken Authentication (#2 on OWASP)
- BEAST, BREACH, CRIME, FREAK, Heartbleed Bug
- SSL 2.0 and SSL 3.0 Protocol Enabled
- Weak Cipher Suites

https://www.digicert.com/cert-inspector-vulnerabilities.htm#certificate_vulnerabilities

Infosec main Certificate Vulnerabilities:
- Man-in-the-middle (MITM) attacks
- Cyber attacks based on signed-malware
- Malware-installed illegitimate certificates
- CA-issued improper certificates

http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/#gref

- MiTM-based downgrade attacks

https://en.wikipedia.org/wiki/Internet_Key_Exchange

The most notable amongst many:
- Storage of Keys in plain-text.
- Use of encryption without authentication

-https://www.networkworld.com/article/2349931/cisco-subnet/top-10-reasons-why-ipsec-vpns-fail-.html

Network Vulnerabilities:
- ARP Spoofing/Poison Routing
- DNS Spoofing/DNS cache poisoning
- SSL Striping
- DDoS

VPN Configuration
"According to the referenced article, 90 percent of all SSL VPN servers are "hopelessly insecure."
https://securityintelligence.com/news/secure-connections-virtually-all-ssl-vpn-servers-miss-the-mark/

WiFi vulnerabilities:
Best to assume there is NO security!

Figure 1: Vulnerabilities with current cybersecurity suite

nCore Communications has patented technology for integrating additional stack layers without the need for SW changes at the driver level. This means nCore solution can be implemented in a device without any SW changes to the operating system or drivers, with just an additional application which resides above the high-level operating system. Figure 2 shows nCore security layer which is based on LTE security protocols and procedures.

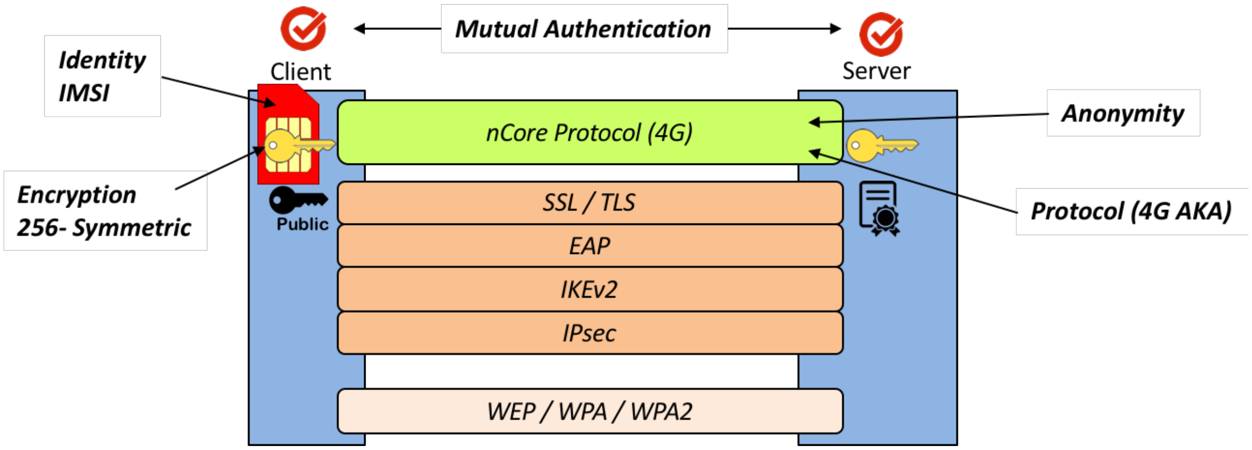


Figure 2: nCore Communications' Cybersecurity suite with additional protocol layer

nCore Communications additional security layer does not replace the existing ones, rather it compliments and fortifies the existing security layers. For example, after mutual-authentication and key generation by nCore procedures, the generated sessions keys can be used in existing layers such as IPsec (IKEv2) or WiFi WPA2 to provide a more secure session (Figure 3).

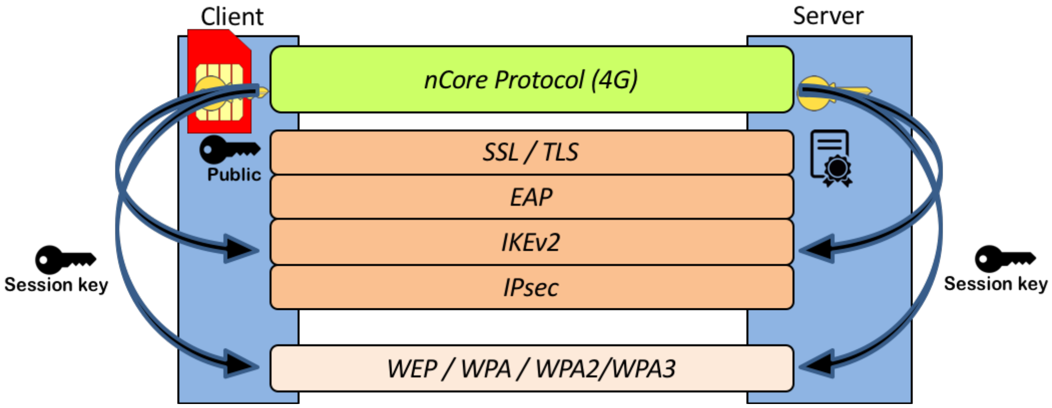


Figure 3: nCore protocol layer is used to fortify the existing security layers

4. nCore Products

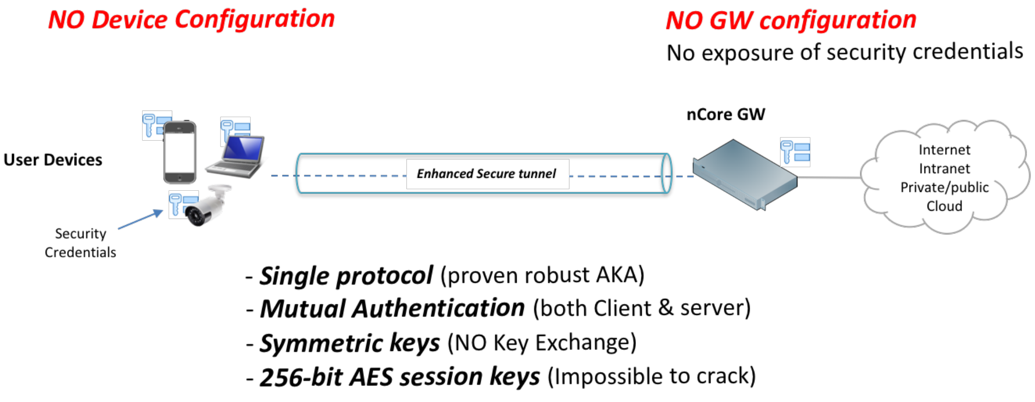
Based on its unique patented technology, nCore has developed a number of products. These products are in IIoT and LTE-WiFi convergence areas, providing a unified security based generic platform.

4.1 Security Gateway

nCore Communications security gateway (nCore GW) is shown in Figure 4. The security protocols and algorithms used in this gateway is based on the protocols and procedures shown in Figures 2 and 3. The “security Credential” shown in Figure 4 is similar to a SIM-Card, eSIM, iSIM or SW-SIM, which is SW implementation of a SIM module. SW-SIM is an nCore innovation that can be generated automatically and provisioned remotely over-the-air (OTA). The gateway is virtualized, which means it can run on dedicated HW or in the Cloud.

Apart from the best-in-class security, the other advantage of the nCore security gateway is that, unlike conventional VPN gateways, nCore gateway does NOT require any configurations, either at the device or the network side. The SW-SIM credentials are automatically generated and transferred to the device, alleviating the need for any human involvement, which often is a security risk.

Currently nCore Communications has device SDK and Apps for Android, Windows 10 and all Linux operating systems.



- ***Single protocol*** (proven robust AKA)
- ***Mutual Authentication*** (both Client & server)
- ***Symmetric keys*** (NO Key Exchange)
- ***256-bit AES session keys*** (Impossible to crack)

Figure 4: nCore Security gateway

4.2 SW-SIM Auto-Provisioning Function

nCore Communications has also developed a SW implementation of SIM card for devices that do not support a physical SIM entity. To make the provisioning task easy for an operator and to remove humans from the provisioning of security credentials, nCore has developed SW-SIM auto-provisioning function, where the SIM credentials are generated automatically and transferred to the device in 3 easy steps (Figure 5).

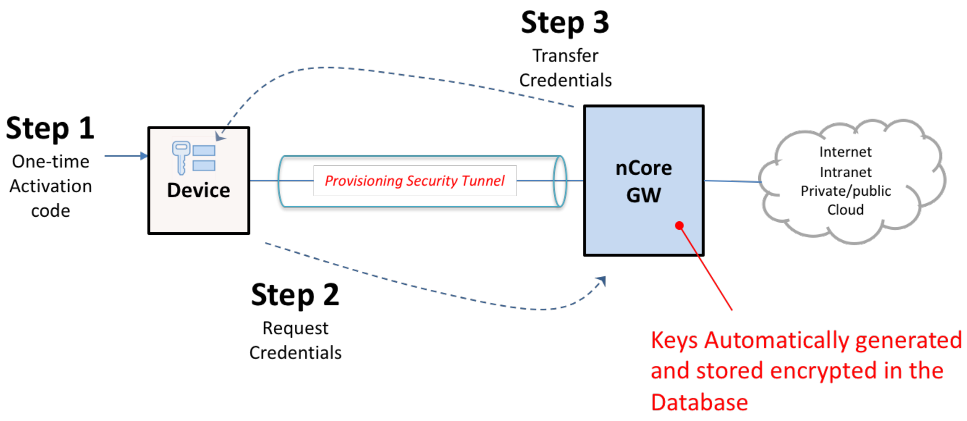


Figure 5: nCore SW-SIM Auto-Provisioning function

nCore Auto-Provisioning SW-SIM function is integrated with the nCore security gateway.

4.3 EPC Gateway

Since all nCore algorithms are based on LTE procedure and protocols, nCore GW can also be used as an "interworking gateway" for attaching any device to an LTE Core network (Figure 6). Unlike an ePDG, which is used for WiFi-Calling with Smartphones, nCore gateway can connect any device to LTE core (EPC), be it an IoT device, Laptop, Tablet or Smartphone. Further, the connection is direct through an *S1* interface, without the need for handset modification or additional interworking functions.

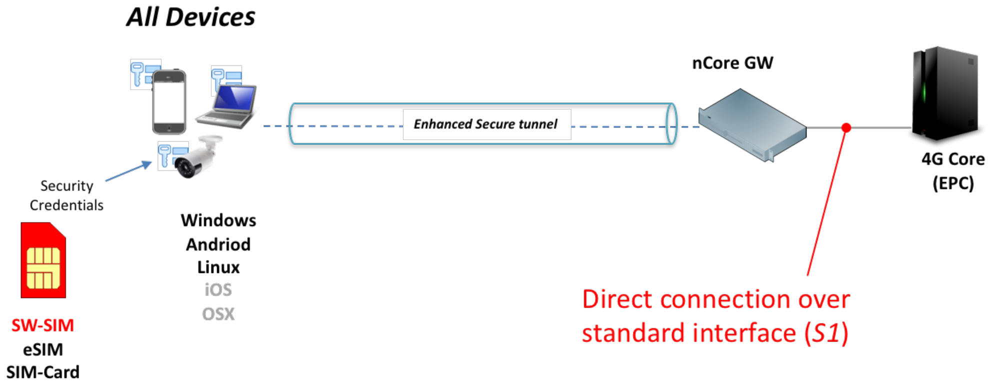


Figure 6: “nCore GW” as an LTE interworking gateway

5. Example Use-Cases

The following are two examples of two different use-cases for IoT and LTE-WiFi Convergence areas.

5.1 Universal IoT Platform

For an IoT operator to succeed, it will need to provide the most optimum and cost-effective connectivity scheme for the different operating environments. While for terrestrial outdoor environments cellular connectivity is the most suitable one, in indoor and hard-to-reach places WiFi may be more suitable and cost-effective. However, each access technology will have a different security scheme, which may or may not meet the requirements. For example, while cellular systems enjoy a very secure network, WiFi connected devices are very vulnerable.

nCore communications Security Gateway and device SDK, together provide a secure tunnel from device to the gateway (and beyond), all based on SIM and LTE protocols and procedures. The tunnel will transverse any IP network, regardless of the access technology, providing a unified security scheme for whatever the chosen connectivity technology is (Figure 7). Further, the platform is capable of connecting any device with any given operating system.

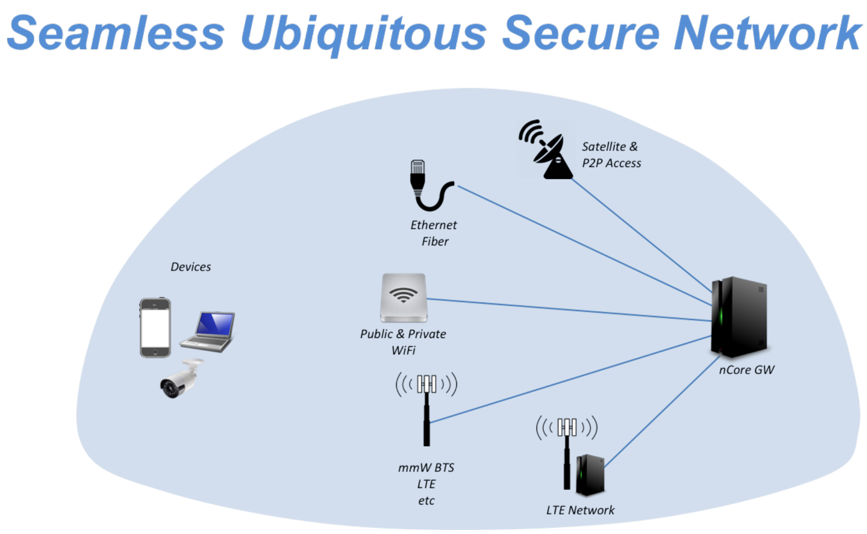


Figure 7: Universal IoT platform with unified security

5.2 LTE-WiFi Convergence Platform

Currently, only an ePDG can enable a Smartphones to attach to an LTE core network. However, using nCore gateway as an EPC Interworking Gateway, an operator can attach any device, with SW-SIM or a HW SIM, to an LTE core network (EPC).

Further, unlike ePDG, the ability to attach a Smartphone to LTE core is not limited to 4G handsets. With nCore Gateway, any Smartphone (3G, 2G or other technologies such as CDMA)) can attach to an LTE core network via WiFi AP, as long as they have WiFi capability. All other devices with varying operating systems can also made to attach to an LTE core network, based on LTE procedures and protocols (Figure 8).

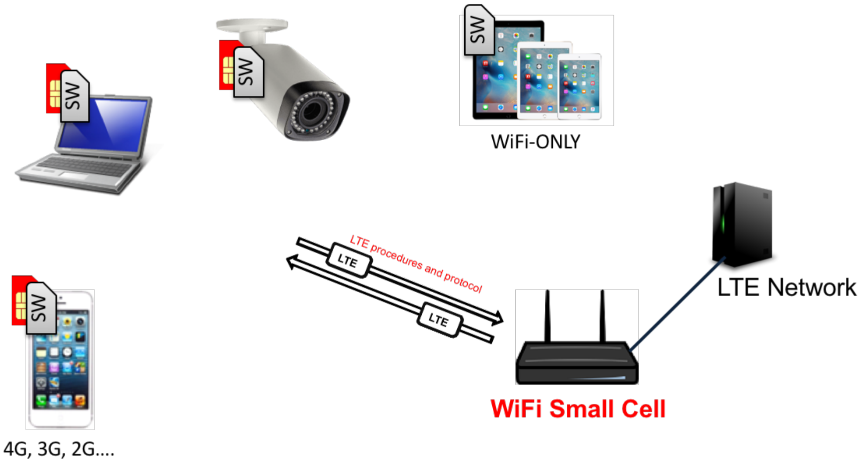


Figure 8: LTE-WiFi convergence platform connecting any device

6. Conclusions

nCore Communications' disruptive technology has opened new possibilities market opportunities. nCore products address two major pain-points in the communications industry, 1) security and 2) integration with a robust mobile platform such as LTE EPC.

nCore's security gateway is a SIM based VPN, which provides the most secure tunnel in the industry. nCore security algorithms are based on an additional protocol layer from a proven technology such as LTE (4G). This additional layer is complementary to the current cybersecurity suite, and by reinforcing it, provides a virtually un-hackable security at IP layer. Since the security is at connectivity and IP layers, it is ideal for IoT devices.

nCore EPC Interworking Gateway is another product that addresses a long-standing pain-point, mainly how to integrate WiFi and other access technologies with an LTE core network?
nCore technology enables seamless integration of all type of access technologies such WiFi, ethernet, Satellite etc., with an LTE core network. Further, nCore technology enables **any** device and operating systems to attach to an LTE core network (not only Smartphones).

nCore SW-SIM along with its auto-provisioning function has removed the need for manual provision of HW SIMs, or the need for a physical SIM entity.