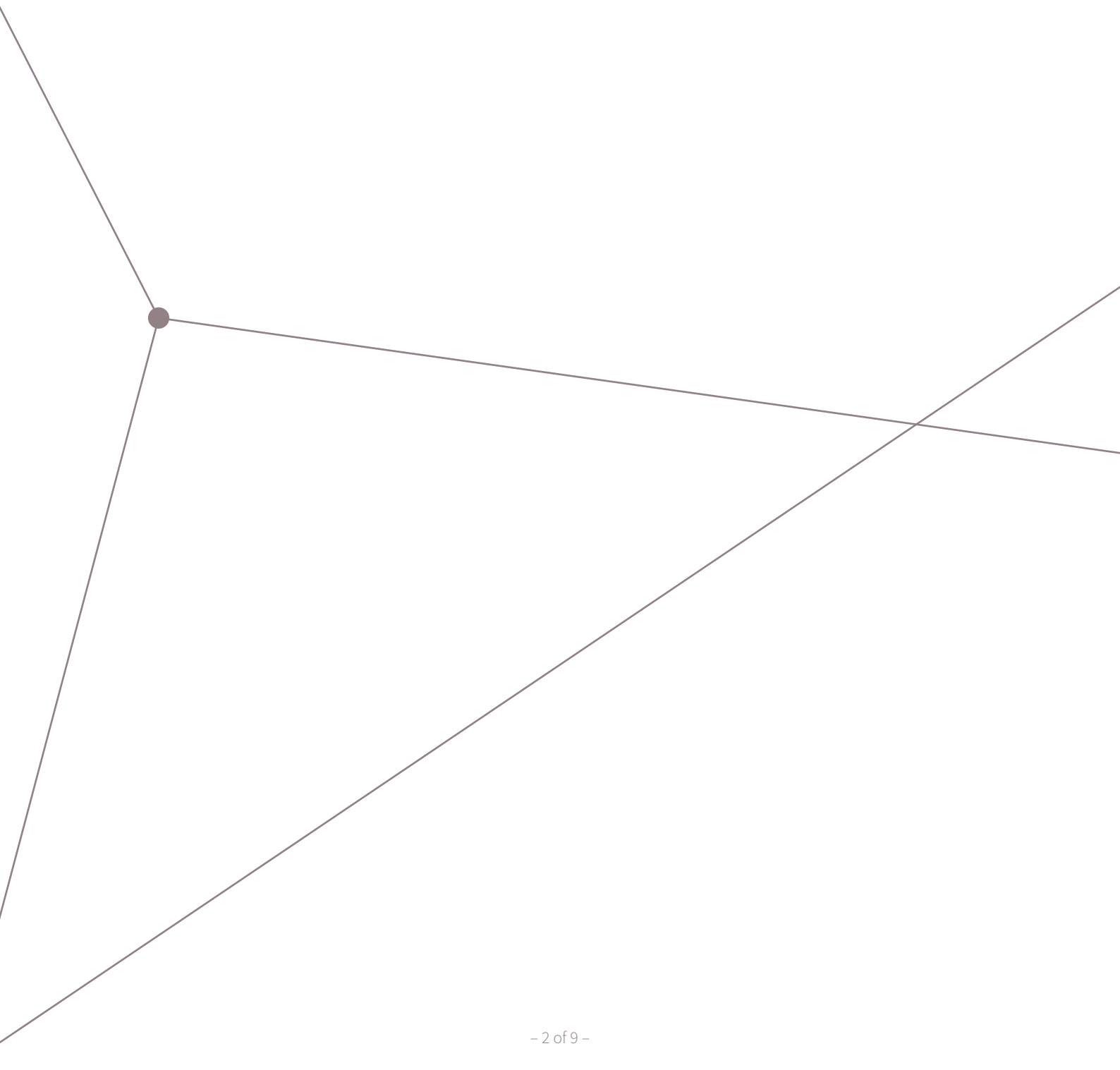
Why Securing Network Equipment is Key to Supporting IoT Infrastructure

Steve Hanna

www.infineon.com/IoT-security

Contents



1. Why Securing Network Equipment is Key to Supporting IoT Infrastructure

IoT device deployments are accelerating, which means a greater attack surface for attackers to gain entry to.

As homes get smart, cars become connected and factories develop ever more automation, the need for security, safety and reliability become paramount. And it is necessary to maintain user confidence in these devices as they become more integrated into our lives. The mobile operator or telco stands in the core of this as the link to the outside world; how can they act as gatekeeper, protecting users from threats?

There is one thing that has been documented over and over again; that is that security is the number one concern in the minds of IoT customers. This concern is well-founded as IoT attacks – such as the Mirai malware which attacked routers and other IoT equipment and recruited them into a botnet – have become commonplace over the last few years.

Having good IoT security baked into the networking equipment can present revenue opportunities for mobile telco operators as they seek to expand from the commoditized services of basic connectivity to more value-add services.

Good security at the heart of the infrastructure could not only help in avoiding another Mirai, but also reduce any liabilities for damages afterwards. If a telco's network is used as the launching pad for further attacks, those attacked may well sue an operator for negligence in failing to secure their infrastructure. And network disruptions can be avoided.

Figure 1: Top Security Concerns

2. Who are the attackers?

To understand how to defend IoT, we need to understand the attackers and their motivations. There are generally three such motivations. One is for fun and bragging rights – these are like the kids that spray graffiti on walls; annoying, but easily fixed and defended against.

The second motivation is criminal – those that are in it for the money. Mirai is a great example of this because the attackers that infected the routers to form a botnet then reportedly rented out the botnet to be used in a distributed denial of service attack. Cyber criminals generally locate themselves in countries that don't have extradition treaties with the west.

The third motivation is political or nation state related. Sometimes, these are actual nation states themselves who are mounting the attacks, but commonly, they are affiliates of the nation state.

Attacks on the US presidential election and the Ukrainian power grid were reportedly mounted by someone who had a political motivation, and whether they were mounted by a nation state itself or by its "patriotic" individuals matters not if you are on the receiving end of the attack. The line is often blurred because these individuals may have simultaneous employment in a state or a state-owned enterprise.

3. The challenge of securing network equipment

Telcos and mobile operators need to deal with cyber-security to the extent that they want to keep their network reliable, safe and secure and to maintain their user confidence.

Reliability of the network is essential to operators as customers count on their network, whether for streaming media, working in their jobs, or even using the network to navigate a self-driving car. If the network is not reliable, it becomes compromised, customers leave and business suffers. Telecoms is a very competitive business, so equipment has to be reliable and secure.

The biggest challenges faced by mobile operators and telcos are technical. Most network equipment was never designed to operate in such a hostile environment as the one they see today. Attacks today are highly sophisticated, including techniques such as exploitation of zero-day vulnerabilities in routers and firmware attacks.

IoT devices face a similar problem. Manufacturing equipment was often not designed to be connected to the network but has now been connected. Even devices that were originally designed with network connectivity in mind face greater threats than originally planned.

Attackers are constantly raising their capability level. Defenders must do the same.

4. The problem with IoT

The only devices that used to connect with a telco's network were just telephones and mobile phones. But now a mobile network has many things other than telephones connected. In fact, the number of network-connected things exceeds the number of connected people. Many of these things, whether a street light or a connected car, refrigerator or a soda machine, represent a different sort of problem from connected people.

While operators previously just worried about the consumer and what they might do with their mobile phone, with a soda machine you have a device which is out there in the field, maybe for decades, and subject to increasingly sophisticated attacks. These vulnerable things can represent a significant threat to other IoT devices and to the network itself.

The number of devices connected is continuously growing in an exponential manner. If some of these devices become infected, they can just overwhelm the network with traffic. With the recent Mirai outbreak, the amount of traffic was more than 600 megabits per second. And Mirai didn't just infect network routers, it also infected IT connected cameras.

Mirai is not the only recent problem for networks. The so-called "Cherry Blossom" tool, reportedly developed by the CIA allowed for an infection of network routers, including top 10 manufacturers. This infection could spread through routers and make it rather difficult for the consumer whose calls and traffic might be monitored, and potentially for the network operator. Operators face a continuous stream of attacks with continuously growing sophistication.

5. Combatting the problem

How does the network operator combat the problem of malware and attacks? Fundamentally, there are three options: Securing the device, the network and the server.

If you can secure the device, you can prevent it from becoming infected, and you help it to resist any infections that might be going around. You can think of this as an inoculation or a vaccination against infection.

Sometimes, protecting the device is not practical. You might have some old equipment out there in the field. This gets worse in industrial networks where it is not unheard of to have 20 or 30-year-old equipment running Windows XP or Windows NT or maybe just DOS or a proprietary operating system. It may not be practical or possible to upgrade equipment before it is fully amortised. In the home, a user may not even realise what equipment is on the network, let alone know how to keep individual devices protected.

This means that, realistically, the other two approaches need to be considered. To secure the network, a security gateway can be put in place. This suits carriers and telco network operators, as security gateways can be rented out on a monthly basis to keep devices secured from external intrusions. While not completely secure, a security gateway is the current best approach to network security. These gateways can start as a firewall and be upgraded over time to include intrusion detection and other capabilities. Should an IoT device get infected, the infection won't spread to other devices if there's a security gateway preventing it from doing so.

The third option is securing the cloud or the server. Here technologies such as artificial intelligence and big data can be used to observe patterns of behavior. Starting with observing a healthy network, such tools can be trained to spot anomalies, such as strange traffic never seen before, traffic going back to known malicious actors, patterns of the traffic or actual content of the traffic that are known to be a signature of an attack. With such patterns identified, actions can be taken such as closing certain ports where there is malicious traffic or blocking a particular endpoint that seems to be infecting others. Cloud security can be used to boost device and network security by diagnosing problems at those levels and providing fixes.

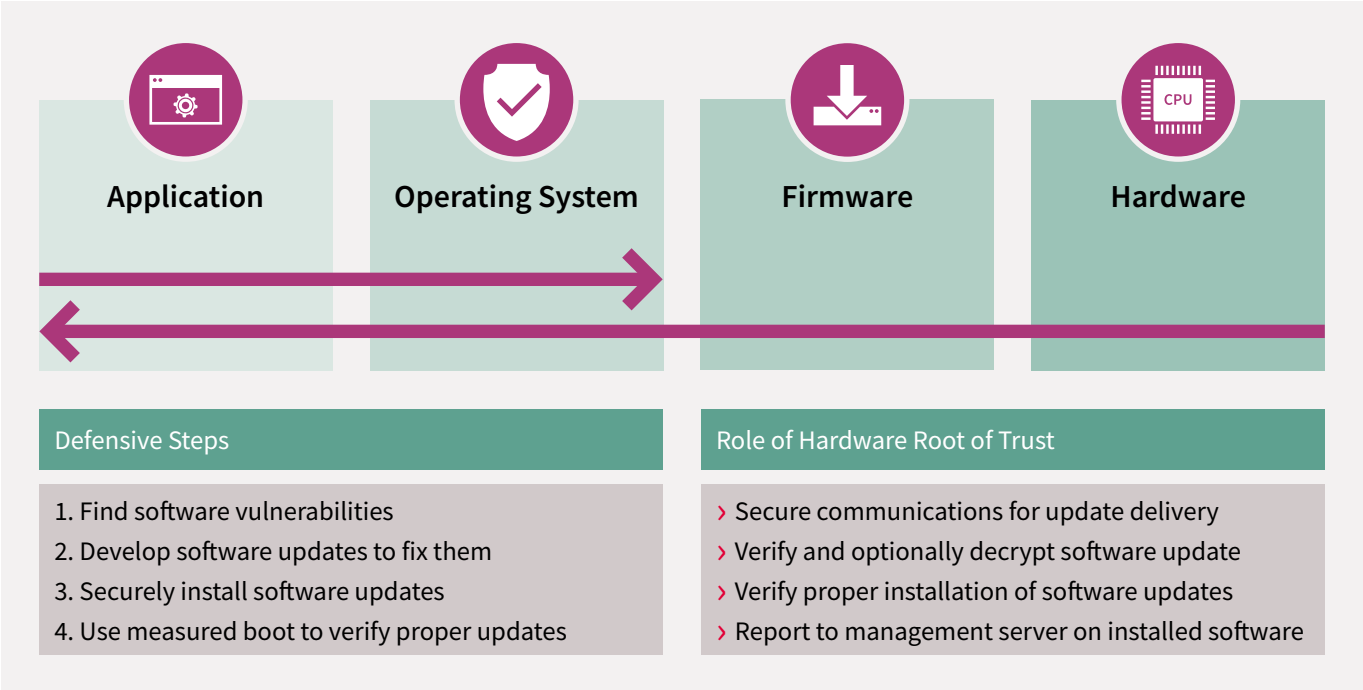


Figure 2: Blocking Software Attacks

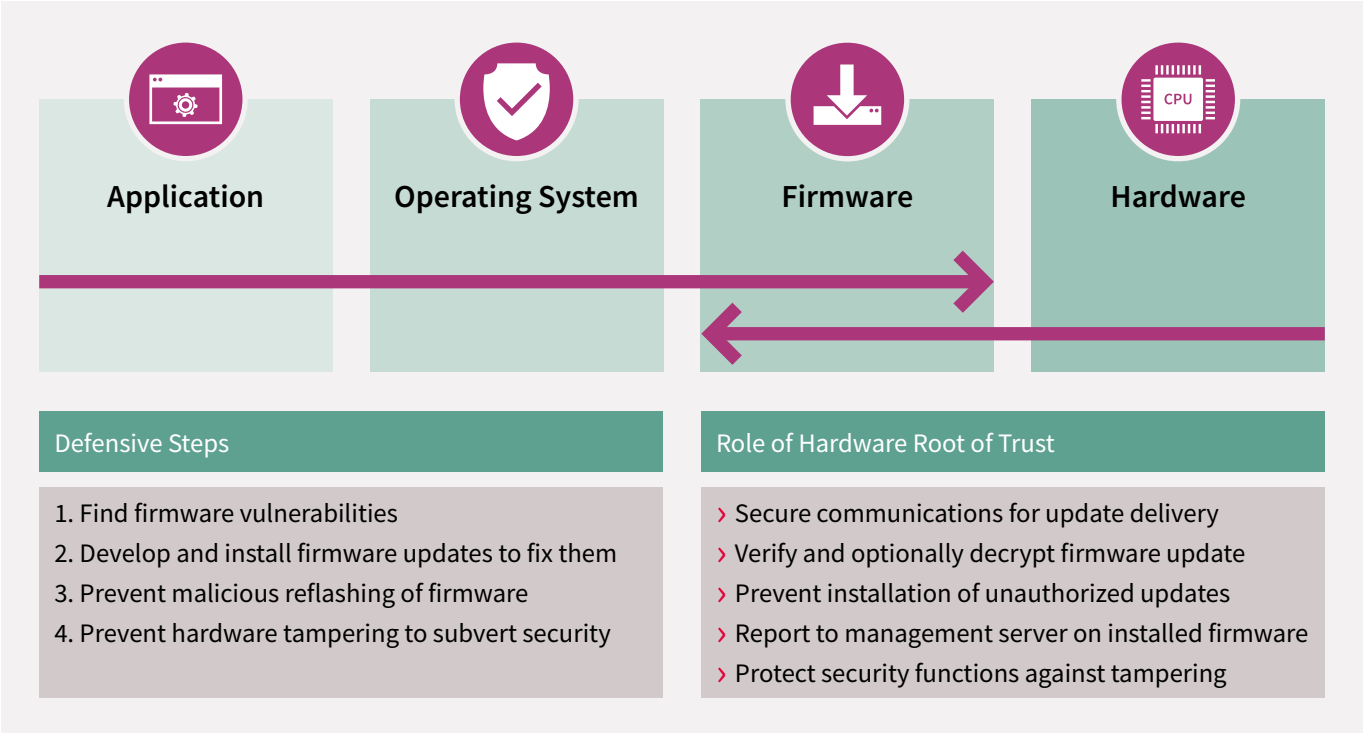


Figure 3: Blocking Firmware and Hardware Attacks

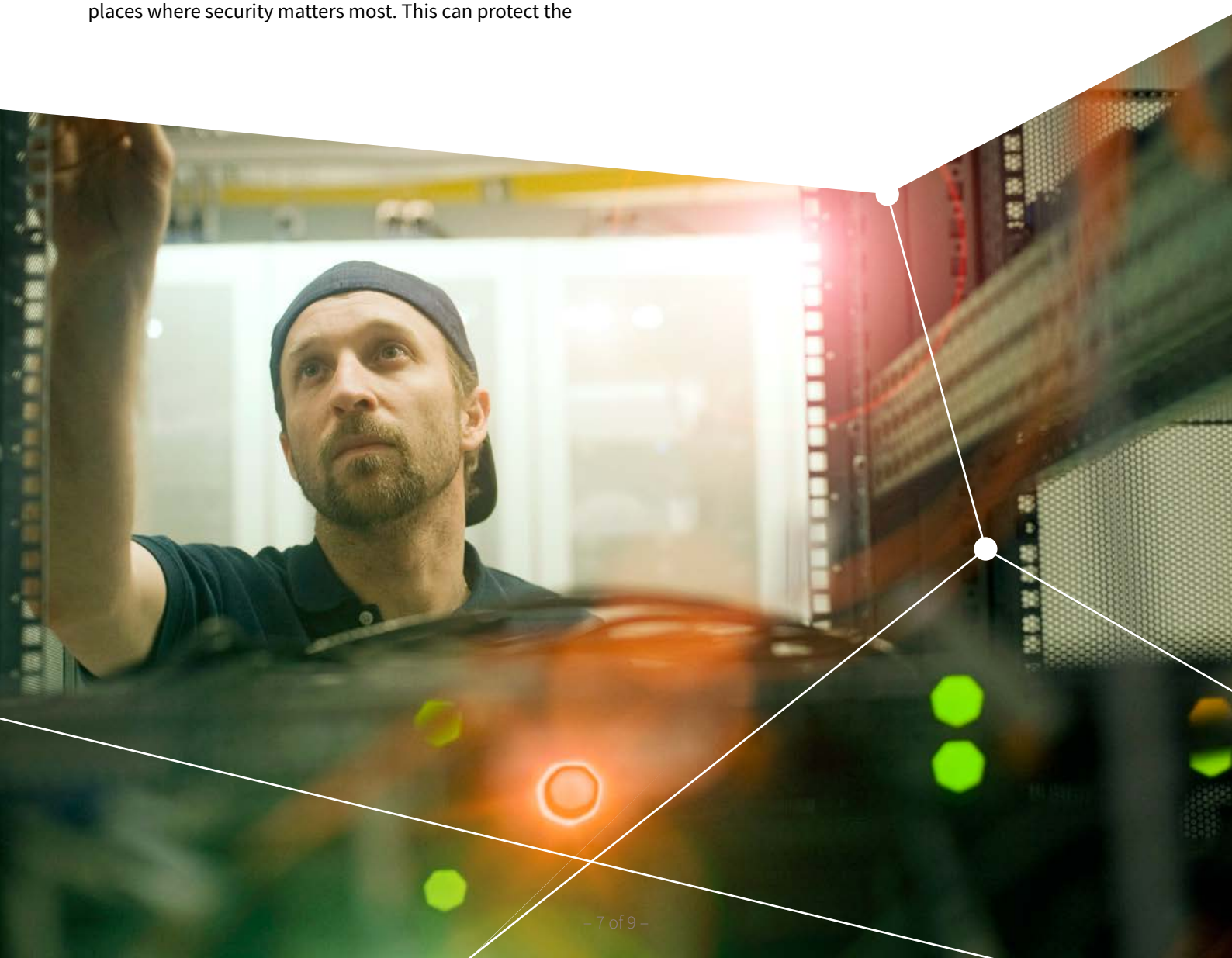
While those three layers of security are in place - at the device, the network, and the server - why is hardware security necessary in each of those layers? If we don't have hardware, we're just counting on the software to do the job instead. Unfortunately, software has bugs, and some of those bugs are vulnerabilities. According to years of research carried out by researchers such as Capers Jones, commercial software has about five bugs per function point or roughly a thousand lines of code. Even in the aerospace industry, there are still around one or two bugs per function point. This number never gets down to zero, even with the most intensive testing and design efforts. So the odds that you're going to get it to zero in an IoT device are pretty slim.

But there is a higher level of security with hardware: security that is evaluated independently and verified to provide the best security available; security that has been able to resist attacks for years, and in some cases, decades.

This is security that is used in smart cards, passwords, other places where security matters most. This can protect the most important things such as cryptographic keys, protocols, and communications protocols. Hardware security provides the foundation to protect devices from being imitated by attackers, inject malicious messages into the communications stream, or even compromise security critical devices such as a router, switch, or security gateway.

There is a special challenge with network equipment; downtime is something to be avoided at all costs. Many operators will leave such equipment running rather than install security updates provided by the manufacturer. This means that the network equipment may be out of date with respect to updates at the extent that the updates are available.

This is a hidden problem lurking in the shadows of the data centers and operator switching rooms and one of the reasons why it's so challenging to secure network equipment and so important to include hardware security as another line of defense.



6. The network is the key to greater security

With the amount of legacy equipment that is likely to keep running for another 20 years, we can't rely on IoT devices to protect themselves, so the network has a central role to play in keeping things secure.

Network security can block most attacks, but it needs a solid foundation in firewalls and switches and routers, many of which have a critical role to play in security.

Having on-chip security is important in such use cases as device identity and also in more sophisticated areas such as zero touch provisioning or remote software integrity management.

The number one use case is device identity, that is, being confident that you're talking to the right device; that's essential when we talk about securing network equipment.

The second use case is secured communication; the ability to communicate with the network equipment without having to worry that somebody is going to highjack a session or be able to see data sent back and forth.

The last common use case is secured software and firmware updates. While it is important that PCs on the network are kept up to date to guard against attacks, updates are infrequently installed on network equipment. These updates have to be pushed down to equipment and installed in a secure manner, otherwise the attacker can push down their own "updates", leaving equipment vulnerable. Therefore, there needs to be a secured software and firmware update mechanism for network equipment and IoT devices, something that on-chip security can provide.

7. Conclusion

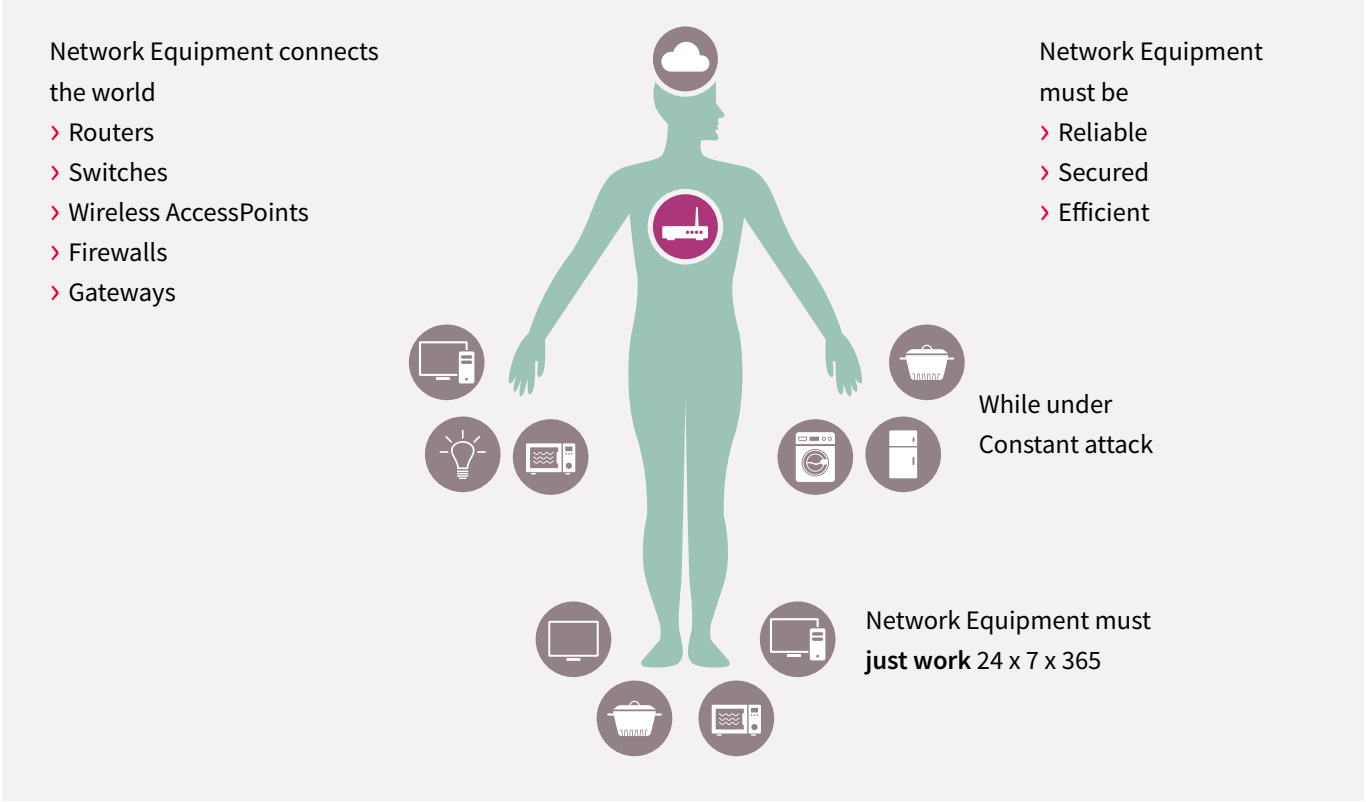


Figure 4: Network Equipment:The Nervous System of the Connected World

Attacks on devices and other endpoints are growing more frequent and sophisticated every day. Having good security built into network equipment can play a vital part in protecting infrastructure. Network equipment manufacturers need to up their game in the fight against this greater level of threat.

With the right security in place, mobile and telco operators can help customers secure IoT devices against today's threats. This means that they can offer value-added services to customers, such as a secured gateway for residential and business customers.

If security is done correctly, it can pay dividends. Having a high level of security within the network can help in building trust in your company. And trust always leads to an on-going, fruitful relationship between an organisation and its customers.

Why Infineon?

Infineon should be on the list of any customer when it comes to hardware security as we have the broadest experience in the area. We have decades of experience with securing embedded systems, including such security critical devices as automated teller machines. Infineon has the broadest range of products as well, from very simple products that are used to authenticate printer cartridges all the way up to the most sophisticated products that are used to protect servers and cloud.

Some of the largest network equipment manufacturers and cloud providers use Infineon's security for their systems. Infineon has a deep portfolio of products available, combining strong security with cost efficiency.