Electronic Engineering JOURNAL

August 30, 2021

# The Bad Guys are Winning in Cyberspace Here’s One Way to Beat Them

## Can a Small Networking Box From a Tech Company in St. Louis Really Provide an Answer?

*by Steven Leibson*

The news is grim. The number of cyberhack attacks and database breaches mounts with each passing week. It’s costing companies and people some big money and a of pain. Here are some scary stats from a recent Intel White Paper titled “Intel Agilex FPGAs target IF SmartNICs, and 5G Networks”:[1]

“CSO, an online publication for chief security officers, recently estimated that about 3.5 billion people saw their personal data stolen in just the top two of the fifteen biggest breaches during the 21st cent These breaches involved databases at some of the largest companies and brands in the world, including Adobe, eBay, Equifax, LinkedIn, Marriott International, McDonald’s, and Volkswagen. The smallest incident on CSO’s list involved the theft of personal data for 134 million people.”

Data isn’t all that’s at risk, however. Consider this incomplete list of very recent, very successful cyberattacks and their repercussions:

- December, 2020: Hackers inserted malicious code into SolarWinds’ widely used Orion IT management software, causing the exposure of sensitive data at several top US government agencies, including the Pentagon, the Department of Homeland Security, the State Department, th Department of Energy, the National Nuclear Security Administration, and the Treasury; corporatior including Microsoft, Cisco, Intel, and Deloitte; and other organizations including the California Department of State Hospitals and Kent State University.[2]
- February, 2021: An unknown hacker attempted to poison the residents of Oldsmar, Florida (population 13,591) by dangerously increasing sodium hydroxide levels in the town’s drinking wat using remote access to the water treatment facility’s water-treatment equipment via the Internet.[3]

- March, 2021: Hackers compromised more than 150,000 security cameras managed by Verkada a located in gyms, jails, schools, hospitals, and factories. These facilities are owned and operated b some 300 of Verkada's customers. "The attackers obtained credentials that allowed them to bypa our authorization system, including two-factor authentication," wrote Verkada CEO Filip Kaliszan i security update on his company's Web site. The hackers wanted to show that the company wasn' taking security seriously enough. Point taken.[4]
- May, 2021: The DarkSide Russian hacking group broke into Colonial Pipeline's IT network and forc the company to cut the connection between its IT and OT networks, resulting in a shutdown of the company's 5500-mile pipeline system for several days. According to Colonial Pipeline, the compa provides roughly 45% of the fuel used by consumers and businesses on the US East Coast. News the hack and pipeline shutdown triggered panic buying that resulted in massive gasoline shortage and some price gouging in the region affected by the hack. Ultimately, Colonial Pipeline's CEO Joseph Blount admitted to paying a $4.4 million ransom in cryptocurrency to the DarkSide hacker Days later, the Justice Department reported that the FBI had recovered about $2.3 million worth o the ransom payment.[1]

This very public list of successful attacks is by no means exhaustive, and I am certain that many successful attacks have not become public.

The bad guys seem to be winning all too often.

The A-team microprocessor vendors, Intel and AMD, have both put security mechanisms into their la PC processors and server CPUs. Intel calls its security mechanism "SGX" (Software Guard eXtensior and AMD calls its security mechanism "SEV" (Secure Encrypted Virtualization). These mechanisms u strong memory region protection with hardware-driven encryption for the code and data in each protected region to wall off sensitive code from malicious attacks.

However, I'm afraid the news isn't great for these extensions. A little Googling produces ample evider of multiple exploits that can be used against each of these protection mechanisms. Any code or data stored in any memory location in a processor's memory space is vulnerable to attack from code runr on the microprocessor. In addition, many successful hacks do not exploit any weaknesses in the microprocessor's code handling. Hackers often employ social engineering and phishing attacks on human operators to simply steal passwords.

A tech company named Q-Net, located in St. Louis, Missouri, has developed an elegant engineering solution to the security problem for closed (non-public) networks. The name of the solution is the somewhat cryptic "Q-Box," which sounds like it might have been developed by an advanced, omnipot species that popped up on multiple episodes in four different Star Trek series.

The Q-Box is literally a black box that’s slightly larger than an old 10/100 Ethernet hub but has only tv RJ45 Ethernet ports: a “Network” port that connects to the big, bad unprotected network teeming wit cyberattacks and hacking attempts from multinational criminals and state actors, and an “Endpoint” port that connects to the network device or network segment that requires protection. Q-Boxes act li “bump-in-the-wire” devices and provide multiple layers of network security, implemented in FPGA-bas hardware.

A Q-Box does not permit software updates or patches from the network, and that’s a major aspect of Box security. According to Q-Net, the FPGA’s hardware configuration is “immutable.” It cannot be modified via the network because the Q-Box’s hardware configuration is simply not accessible throu the network packet stream.

Devices connected by configured Q-Boxes are allowed to communicate with each other, but no other devices can communicate or even see the network devices shielded by Q-Boxes, even when they’re o the same network. Unprotected network devices on the Network side of the Q-Box cannot ping, discover, or otherwise communicate with devices connected to the Endpoint port. The theory is that simply can’t attack what you can’t see. Therefore, the first Q-Box protection layer is stealth.

The second protection layer is authentication. When you initially configure a Q-Net security network based on Q-Boxes, you define permissions that allow only certain protected devices to interact over t network. The Q-Box simply drops packets received from unprotected network devices or from protec network devices that lack the proper permissions. Only packets from authorized sources get through the Q-Box hardware gauntlet.

The third protection layer is encryption based on AES-256 with symmetric keys. The Q-Box changes keys after every packet or transaction – as frequently as 1 million times per second – using a just-in-time key-generation mechanism. These keys are stored only within the Q-Boxes themselves, so there no external key repository to hack. Good luck decrypting a packet stream where every packet is protected with a unique AES-256 key.

Because decrypting a packet stream that has been encrypted with a different key for each packet or transaction is so difficult, Q-Net claims that Q-Box protection is resistant to quantum decryption. In theory, that impressive claim is true. However, we don’t yet have commercial quantum computers, so the jury’s still out on that claim as a practical matter. Nevertheless, it seems clear that the Q-Box provides significantly better network packet security than software-based measures.

You can protect existing computers and devices that use point-to-point network communications simply by inserting a Q-Box between each endpoint and the network. The Q-Box operates independen of the connected endpoint device and has no impact on existing network configurations with the exception of a little added latency. However, because it’s based on an FPGA-based hardware implementation, the Q-Box adds only microseconds to network latency.

However, you don’t need to install one Q-Box per protected device. Each Q-Box can protect as many a 2000 network endpoints by connecting a Q-Box to a network router or switch. If you connect the Q-Bo Network port to a WAN router, the protected network segments can be located anywhere in the worl Note that networked devices communicating with each other on the same protected segment are trading packets in the clear and are therefore not protected from each other.

You can use the Q-Box to protect a wide range of networked devices including:

- Servers and PCs connected to IT and Operational Technology (OT) networks
- Financial equipment ranging from bank ATMs and credit card POS terminals to Lotto machines at the corner bodega and slot machines in casinos
- Equipment connected to OT networks in buildings and factories, industrial plants, and utilities,

including IoT devices such as PLCs and other industrial controllers, lighting systems, security cameras and systems, and even robotic equipment
- Networked military and defense equipment

You won't be using Q-Boxes to protect public-facing equipment such as Web servers that must deal v packets from all sources. Q-Boxes are designed for creating private networks and keeping them priva Packets from unauthorized sources simply disappear into the ether within networks protected by Q-Boxes.

The original Ethernet LAN protocols and the early Internet were developed during more egalitarian times, before anyone realized that billions of people, including armies of people with malicious intent might have access to every device in global cyberspace. Poisoning a town's water supply or shutting the gasoline spigot for millions of people from another continent using nothing more than a laptop computer or mobile phone was the stuff of superspy movies and cyberpunk science fiction back ther Today, it's frequently headline news.

As a result of our lack of foresight when developing network standards, we've spent decades playing escalating cat-and-mouse game with the bad guys by developing network protocol security patches other stopgap measures. Every time your PC or laptop gets zapped by a Microsoft Windows update, can bet that another batch of security patches have been added to your computer. More patches are the way, guaranteed. It's all part of the game.

Q-Net's Q-Box looks like a very interesting way to retrofit existing private networks with very strong security that could have been built into networking protocols but wasn't. However, a retrofit using Q-Boxes certainly might not be the right way to protect networking equipment being developed today, a we'll explore this topic in more depth in future EEJournal articles (For example, see Max Maxfield's "Secure Your Data at Rest, Stupid!"), so please stay tuned.

Meanwhile, I'm wondering how concerned you are about these security challenges to equipment that you're designing now and preparing to put into the field. Why not leave a comment and let me know? Your ideas might find their way into a future security-related design article.

References

1. "Intel® Agilex® FPGAs target IPUs, SmartNICs, and 5G Networks," https://www.intel.com/content/dam/www/central-libraries/us/en/documents/agilex-fpgas-targe ipus-smartnics-5g-networks-white-paper.pdf
2. "SolarWinds Hack Victims: From Tech Companies to a Hospital and University," The Wall Street Journal, https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospi and-university-11608548402
3. "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," Wired, https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. "Hackers just pulled off one of the most mind-boggling hacks of 2021 so far," BGR Media, https://bgr.com/tech/security-cameras-hacked-verkada-customers-exposed/