
InZero Technologies
Patented TRIPLiot:
Security INSIDE the device
where it belongs
Keeping the lights on
in IoT security

Introduction: When the lights went out . . .

Over the 4-day period January 9-12, 2017 – shortly before the Presidential Inauguration – 66% of the Washington, DC, Police Camera Surveillance System in the White House area (123 out of 187 cameras) were hacked. This turned out to be a calculated ransomware attack launched by Romanian hackers. The hackers planned to extort over 175,000 accessible accounts.

This breach blatantly exposed an enormous – some say inexcusable – weakness in IoT networks and systems: the delay, difficulty and ineffectiveness of detection-and-correction, in other words, providing required patching and updating when it's most needed. The Washington Post captured the understandable frustration over such conspicuous IoT vulnerabilities:

> *"When hackers took over two-thirds of D.C. police's surveillance cameras . . . two Romanians accused in the hacking planned to use the police department computers to email ransomware to more than 179,000 accounts. The intrusion in the District occurred Jan. 9-12, 2017, and caused 123 of the police department's 187 surveillance cameras to go dark eight days before Donald Trump was sworn in as president . . . Alex Rice, the chief technology officer and co-founder of HackerOne (a California firm that works with companies and the Defense Department to test computer security) . . . said "We have got to hold companies and organizations responsible for implementing basic security practices that make it difficult for criminals. They are tempted by this low-level fruit." (Washington Post)*

. . . And nobody should have been surprised

The explosive growth of IoT has come with a steep price. In the race to develop, sell and connect IoT devices, there was one undeniable pervasive failing: Nobody cared much about device security. The developers didn't care because it takes a real effort to build in security. The sellers wanted to get to market quickly and with low-priced products. Consumers didn't care – originally, anyway – because if there was a failure for any reason, the cost was low enough to simply replace.

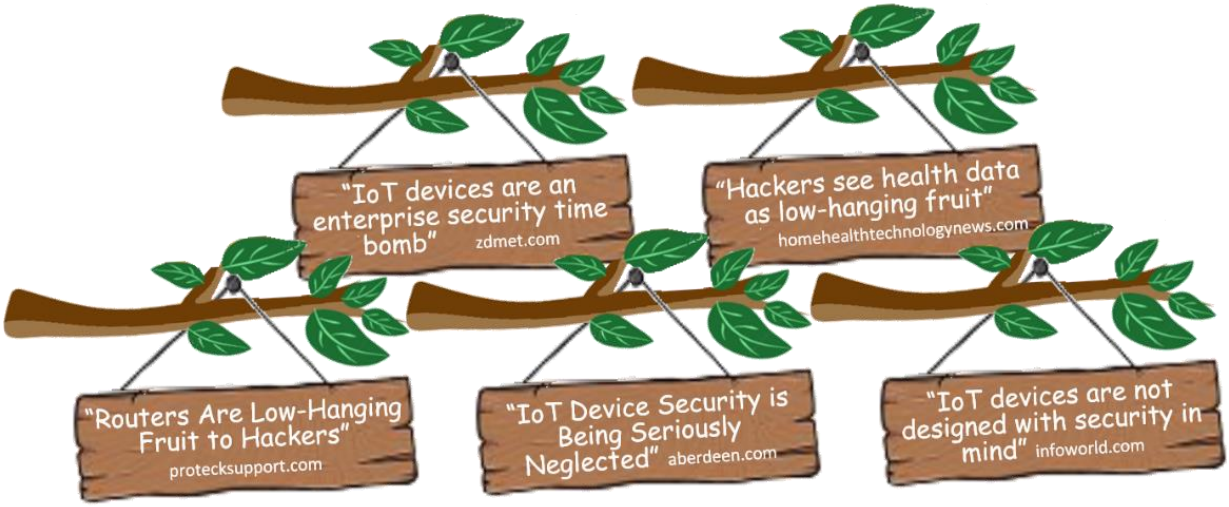
But this distribution chain did not seriously take into account that:

- ✓ IoT devices are just another electronic product that malware can access and use as a conduit to others
- ✓ IoT device operation and management, typically through clouds and hybrid clouds, invites cyber attacks capable of migrating and circulating in such a given ecosystem
- ✓ Relatively harmless initial intrusion can quickly lead to massive system failure

100 Carpenter Drive, Sterling, VA 20164

- ✓ The IoT industry did not anticipate hacker ingenuity and creativity, evidently thinking that hackers would stay focused on traditional data breach like the U.S. OPM, Equifax, Target, Home Depot, etc.
- ✓ No common technology, standards or practical measures were established to fix IoT when it's broken, including when it's broken by being hacked

Now, however, industry researchers are increasingly sounding the alarm bells over the poor state of IoT cyber defense:



We saw this coming . . . and patented the solution

Dedicated to deep-level product security, InZero's patents provide hardware-enforced data and domain isolation and separation in internet-connected devices, whether laptops, tablets, smartphones and IoT devices of every nature and kind. One of these patents, providing for "*Reliable and Secure Firmware Update with a Dynamic Validation for Internet of Things (IoT) Devices"* (U.S. Patent No. 10097563), offers the critical technology solution for the IoT device detection-and-correction shortcoming pervading IoT products across-the-board.

The technology provides the three critical functions generally missing in today's products:

(1) AUTOMATIC CONTINUOUS UPDATE – Device firmware updates that either become available in the ordinary course of development, or more importantly, which constitute patching of a discovered vulnerability or worse, of a breach. As determined by the organization, the automatic update is executed either by sys admin policy or automatically.

(2) AUTOMATIC CONTINUOUS INTEGRITY CHECK – Real-time, continuous firmware code check to assure that the firmware constitutes the actual, intended firmware code and has not been altered.

100 Carpenter Drive, Sterling, VA 20164

(3) AUTOMATIC CONTINUOUS MONITORING – Real-time, continuous monitoring for unauthorized traffic, i.e., stranger danger and upon alert, immediate firmware replacement.

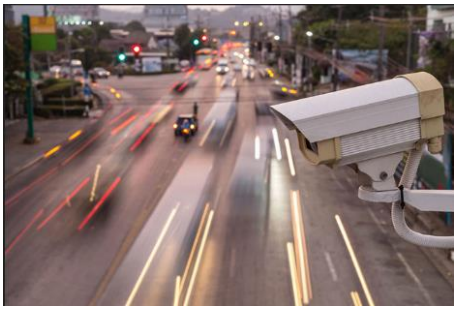
The patented methodology offers advanced security, improved IoT usability, and reduced cost of IoT repair:

(1) ADVANCED SECURITY - The automatic and continuous execution of TRIPLiot provides the significant security advantage of assuring IoT systems are properly patched and up-to-date. Furthermore, the TRIPLiot security functions employ hardware-enforced security extensions like ARM TrustZone or Bare-Metal Hypervisor Mode – TRIPLiot is not mere commercial software. This patented hardening of key security functions prevents malware from taking over the system and overcoming security functions.

(2) IMPROVED USABILITY - In addition, each TRIPLiot function is performed automatically in real-time to eliminate the potentially disruptive downtime typically caused in update activity, not only for scheduled updates but also in the event that an integrity check or monitoring reveals either code firmware alteration or suspicious behavior.

(3) REDUCED COST - Furthermore, if for any reason a TRIPLiot IoT device in the field experiences any firmware problem, there is no need to physically access the device because the firmware image can be remotely replaced.

Use-case Examples



1. CCTV IP NETWORK SURVEILLANCE SYSTEMS. High-security locations employ continuous CCTV monitoring and video storage, including through cloud systems which are appropriate for our patented technology, generally described as "IP Network Surveillance" systems, because they use Internet Protocol to transfer data to and from the cameras. These require continuous operation and, furthermore, are attractive candidates for hacking, including as ransomware targets, as we described in the DC Police breach above.

If the CCTV system had employed TRIPLiot, the video recordings would not have experience downtime, the incoming malware would have been detected by the patented integrity check, and clean operating firmware automatically would have been installed as soon as any camera malfunctioned.

100 Carpenter Drive, Sterling, VA 20164

Using TRIPLiot, the delay and difficulty in "*keeping the lights on*" is eliminated.

2. SMART CITIES. Increasingly, municipalities are migrating to IoT services to improve efficiency and quality of life. At or near the top of the list, for one example, is traffic monitoring. The principal objective is to permit efficient traffic flow by continuous roadway and intersection monitoring with real-time adjustments to speed flow. Thus, traffic coordination is dependent on continuous IoT operation and intended adjustments, both of which require the kind of ongoing reliability encompassed by TRIPLiot. Examples include:

> ***Portland Installs Smart City Sensors to Reduce Traffic Deaths*** *-* engineering.com.
> *"We are at the forefront of using advanced technology to make our cities safer for pedestrians, cyclists and drivers, helping people more easily get around, save time and reduce the possibility of crashes," said Mayor Ted Wheeler.*
>
> ***Dallas Partners with Ericsson for Smart Traffic Solutions System*** *- smart citiesdive.com. Congestion has been a long-term struggle in the city, and the Dallas Innovation Alliance is already working in the West End to improve multi-modal transit and accessibility. Logistics companies list traffic congestion as one of their top concerns and traffic has been shown to cost consumers hundreds of billions of dollars each year — and $2.9 billion in Dallas alone.*
>
> ***Smart City Era Promises Big Improvement for Urban Ecosystems*** *- blogs.intel.com.*
> *Smart traffic systems, including dynamic traffic control and connected parking, "will yield a mobility savings of 60 hours a year".*

With the good comes the bad – these improvements attract the cyber criminal:

> ***Cities Are Getting Smarter—And Much Easier To Hack*** *- dailydot.com.*
> *Anyone who makes devices in the extremely competitive tech space is in a hurry to get their products to market, and they aren't economically invested in putting in security. Adding security and testing it against known vulnerabilities increases cost to development and delays the launch.*
>
> ***How Hackers Could Turn a 'Smart City' Into A House of Cards*** *- foxnews.com/tech.*
> *Some smart cities use connected power meters, but the city usually mandates that these meters connect via a consumer mobile network using a SIM card that's similar to the one in your smartphone. A hacker could find a way to shut down the power to an entire city, possibly by compromising only one of those meters.*

100 Carpenter Drive, Sterling, VA 20164

Smart city systems are riddled with critical security vulnerabilities *- zdnet.com. Researchers have uncovered countless zero-day bugs which can be used to kill our critical city systems.*

Using TRIPLiot, there is no hit or miss in keeping the smart city going.

3. CRITICAL MEDICAL DEVICES.

Telemedicine is not immune to cyber risk. The devastating consequences are not lost on critical care professionals:

"It's official: Hearts can be hacked" *money.cnn*. *Implanted cardiac devices were found to be hackable by the FDA.*

The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks.

The maker acknowledged that there were "*severe cyber security flaws in the devices*" and even the patch issued would only "*automatically vibrate to tell the patient when something was wrong".* TRIPLiot will automatically update on detecting abnormal behavior, not relying on the patient to alert staff who in turn would need to alert system administrators.

In the *2018* Heart Rhythm Society's Leadership Summit, its White Paper entitled "*Cybersecurity Vulnerabilities of Cardiac Implantable Electronic Devices*" echoed the risk:

Cybersecurity, including device security, is an industry-wide challenge and all implanted devices with remote monitoring have potential vulnerabilities," . . . In some cases, such as the WannaCry ransomware attack, medical equipment can be affected without being the primary target of an attack. WannaCry targeted computers running an outdated version of the Microsoft Windows operating systems of which users failed to install updates to patch known vulnerabilities... As a result, network-connected medical devices across the United States running on this operating system were affected and taken off-line for remediation.

Using TRIPLiot, telemedicine doesn't have to be taken offline for remediation.

100 Carpenter Drive, Sterling, VA 20164

Moreover, the need for in-device telemed updating was brought home when a software update process was found littered with malware that required a complete shutdown:

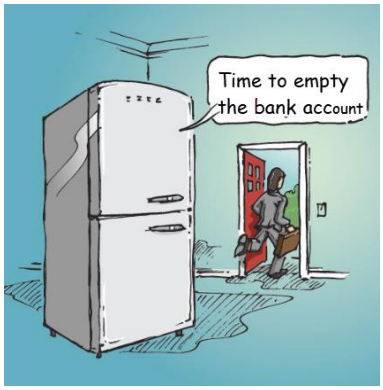
*"**Software Update Site for Hospital Respirators Found Riddled With Malware**" - threatpost.com*

> *A Web site used to distribute software updates for a wide range medical equipment, including ventilators has been blocked by Google after it was found to be riddled with malware and serving up attacks. The infected Web sites, which use a number of different domains, distribute firmware updates for a range of ventilators and respiratory products . . . were found to be infected and pushing malicious software to visitors' systems . . .serving "content that resulted in malicious software being downloaded and installed without user consent.*

TRIPLiot puts device updating where it belongs, in the device itself and controlled at the sys admin level – not through easily accessible internet websites.

Using TRIPLiot, the delay and difficulty in "*keeping the lights on*" is eliminated.

4. EVERYDAY IoT.



Cloud-based IoT management only increases the risk that mundane devices lie at the bottom of a massive IoT attack, as occurred to Amazon Web Services and other cloud players in late 2016. (datacenterdynamics.com).

The vulnerability of every IoT device couldn't be more obvious than the risk presented by the common household appliance.

"When Refrigerators Attack . . ." Anyone assuming that the smart refrigerator cannot communicate with – and therefore infect – other network-connected IoT devices, including home security, should take a few minutes to read our blog: "*When Appliances Attack…and Sometimes Kill*"- workplacetablet.com.

> *Most hacks are done by relying on the codes/usernames/passwords being the default ones. Most people don't think about updating the passwords on their refrigerators. No, the hackers aren't interested in making themselves a spam sandwich; they are more interested in using this as an access point to get into the more tasty stuff on your computer or smart phone. Dishwashers, clothes dryers and coffee makers are all possible access points. More and more appliances are coming online every day. In short, they've got you surrounded.*
>
> *"In a study spanning two years, [researches] Erven and his team found drug infusion pumps–for delivering morphine drips, chemotherapy and antibiotics–that can be remotely*

100 Carpenter Drive, Sterling, VA 20164

> *manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care*."

The mundane IoT device needs TRIPLiot as much as IT security systems, smart cities, telemed, factories, and critical infrastructure.

Our First Prototype: IP Camera Security

The first practical implementation of TRIPLiot is IP camera security systems. Our demonstration prototype, to be finished shortly, employs popular ARM processor technology. This will result in relatively easy adoption in the numerous IP security camera systems that employ ARM processors, making TRIPLiot an extremely efficient technology licensed by the product OEMs and their developers.

Conclusion: As IoT grows, there will be winners and losers . . .

TRIPLiot doesn't compromise IoT device performance in any way – just the opposite, it is the patented technology that gets rid of the unacceptable device updating and reliability problems that pervade IoT systems.

Nothing keeps the lights on more than TRIPLiot.

InZero Technologies, LLC

100 Carpenter Drive, Sterling, VA 20164