https://www.iot-now.com/2018/03/16/78856-must-secure-internet-things-someone-gets-hurt/

We must secure the Internet of Things before someone gets hurt

16/03/18

Robert Haim of ACG Research

Posted by Zenobia HegdeMarch 16, 2018

0Share

Dick Cheney, the former vice president of the United States, famously disabled wireless access to his heart pacemaker because he was afraid that terrorists could induce a heart attack. In the 2007 movie "Live Free or Die Hard," criminals blocked traffic and caused accidents by turning all of Washington, D.C.'s traffic signals to green.

Those real-life and fictional attacks on what we now call the Internet of Things (IoT) had the potential to cause loss of life. Considering all the IoT sensors and controls being used around the world today, it's only a matter of time before weak security allows bad actors to seize control, enable dangerous behaviors, or trick human operators into performing the wrong action.

It's only a matter of time. We must secure the Internet of Things before someone gets hurt. But how?

There are many challenges in that areas. For example, identity management. Are you ever exactly sure about which users, devices, or applications are trying to access your data? How can you prove identity within a reasonable doubt, but keep improving confidence that you've trusted the right users, and not, say, a terrorist? That means behavioral monitoring, in real time.

Take the challenge of protecting critical information, which may be regulated by laws or industries – or simply extremely valuable to corporations and to thieves. That data may affect lives immediately (like a medical device) or later (like blueprints to a hydroelectric dam's security systems). How can you be sure that data and those devices are well protected from tampering or illicit access?

Or the networking connections themselves, which link mobile or fixed-line devices back to the data center or the cloud. Are the connections secure? Can hackers gain access by subverting an end-point… and have those connections been tested to be robust, scalable, and impenetrable? Let's find out how.

## Spot the attack. Stop the attack

The challenge in achieving a "secure" network, including the IoT sector, is that "security" is a negative goal, says Robert Haim, principal analyst at **ACG Research**, who focuses on the networking and telecommunications industries.


Mark McGovern

"You're trying to achieve something despite whatever adversaries might do and you don't know what the capabilities of the adversaries are," he explains. Since many IoT endpoint devices don't have enough memory to include sophisticated security software in them. "So what are we going to do?"

There are actually two problems that must be solved, Haim says: "We have to worry about the security of the device itself, and then we also have to think about what we need to do if we get hacked." It doesn't help that 55% of companies don't even know where the threat is coming from, and where the problem is in their network.

## Look at actions, not only identity

Mark McGovern, group leader of threat analytics, **CA Technologies**, says that there's a huge need to watch what people are doing, once given access to a system. What they do is more important than who they are. "Whether it's an existing system that's doing real-time authorisation of 100 million users for a financial institution, or large cable companies, the way that we think about it is not about who you claim to be or the credentials you have, it's what you do."

He explains, "When you meet someone on the street, they may say they are X or they do Y, but reality is, what do you observe them doing over time? That's the level of trust that you afford to people."

CA studies and analyses the actual behavior of the entities authorised to use a system, and flags the things that are inconsistent with the past behaviors of those entities.

"Whether that's an IP address, an endpoint, a login, or a claimed identity, what are the things that are standing out, both against their own behavior, and then the behavior of the population," McGovern says.

“This data reinforces the learning that our systems are doing and the machine learning that we embed in those systems, and also provides value to our customers.”

## Start with threat modeling

“Take any device, like an IoT door lock,” says John Michelsen, chief product officer, **Zimperium**, which makes AI-based mobile threat defense software. “You’ve got to identify at a device level, network level, or application content level, what are the ways that this device could be exploited.” And then you have to block them before you go to market.

It’s a real problem, Michelsen says. “At 2017’s Black Hat, someone proved that 13 of the 15 automated door knobs could be opened within just a few hours of work. At least 70% of IoT consumer IT devices are hackable.”

That’s why you need threat modeling, he says: “First, you do threat modeling. You then identify ways that you’re going to prevent – detect that and go about building a solution around it.”

## Everyone must look outside

Every company has internal security resources for testing software, infrastructure, products, and services, but that’s not enough, says Roark Pollock, senior vice-president, **Ziften**, which offers endpoint security solutions.

“You have to look outside. Look at your partners and be open to them testing your product. They may require you to go through a whole certification process — put yourself through those partner certifications. There are auditing firms for security today. Hire them.”


John Michelson & Roark Pollock

Don’t trust yourself, he insists. Get external experts to double-check your engineers, double-check your code.

“Then look to the community and open source projects to again ensure that there is a community of people that are double-checking, re-checking, pushing on that code.”

Pollock isn’t impressed by any company that assumes that it can do it all themselves in regard to security. “I think it’s critical to get outside help.”

## Use artificial intelligence to police identity

Hank Skorny, senior vice-president, **Neustar**, an identity-management company, says that it begins with determining the identity of users (or devices or applications) that are accessing IoT devices or their data. But it doesn't stop there. "You have to establish identity. You also have to always call that into doubt, because identity is only a probability, never truly definitive."

How do you improve confidence in that probability? "Employ machine learning and artificial intelligence," he says, while constantly looking at monitoring whatever system that you've been building.

"You're not simply going to identify somebody or determine a device or whatever. You're going to police it. The only way you can police a nanosecond-scale world is by using computational machine learning and artificial intelligence, the constantly looking for those patterns of evil behaviour — stopping it faster than a human ever could.

## Prove trust across multiple domains

Some data is protected by law – think about military secrets or the personally identifiable information about health, covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States. There's other information, though, that's extremely sensitive, even if not covered by specific regulations. Consider data about the performance of professional athletes: It's not HIPPA health information, but it's crucial intelligence for billion-dollar sports teams.

**Zebra Sports** is a business that collects practice-time and game-day telemetry on American football players, explains John Pollard, the company's vice president, and the company had to work hard to score goals with the National Football League (NFL).

"One of the criteria that the NFL went through in evaluating various technologies was certainly security," he says. "We collect a lot of information, and have to transfer that information into software and services so that our clients in the primary verticals can evaluate that information. The NFL certainly embodies that as well. Because we're capturing information that has never been captured before for a professional sport, we're talking about acceleration, deceleration, change of direction, proximity over an aggregate amount of time."


John Pollard

Helping Zebra score points: Its rich experience in IoT in retail, transportation, logistics, manufacturing, and healthcare.

“Our heritage working with those industries certainly helped us build a valid case to be a partner with the NFL in capturing that type of information,” says Pollard.

The security lesson here, says Pollard is that just because it’s sports doesn’t mean that it’s vital. The same principals apply to, say, military or commercial IoT as to the NFL. Telemetry for a football player is no different than telemetry for a security guard, or even a missile. The first parameter is to make it secure.

## Create trust zones — and enforce them

Not all users are created equally, and not all users require the same information from an IoT device. Hospital IT staff needs to verify that data from a dialysis pump is being captured by the correct application and stored in the correct patient’s records… but they do not need to see the data, and in fact, HIPAA may forbid their access. Similarly, the IT staff need to verify that the doorway into a secured part of a building works properly, but again, they may not be authorised to open the door themselves.

“If you look at the number of people who interact with that door lock, the roles, the responsibilities, that’s where the trust zones keep building up,” says Sanjeev Datla, chief technology officer, **Lantronix**, which builds industrial IoT technology. “What are the different levels of access for the door administrator? For the nurse as he or she interacts with the dialysis machines?”

And what about the field service technician who comes to accesses or service the machine? “Know the roles and responsibilities about what to permit, and what not to permit,” he says.

Datla insists that it’s not simple. “You have an infusion pump with an Ethernet port. What are the rings of trust, or access controls, if you will, around that port? And how is it tested?” As CA’s Mark McGovern said above, this must be more sophisticated than simple access control lists.

“We look for behavioral analysis,” says Datla, “Okay, this person is not supposed to do this at this time. So when they do that, what do you do about it? How do you raise an alert, and get approval or a block from a higher level?”

## Never forget: everything is connected

“IoT devices are getting smarter and smarter,” says Ziften’s Pollock. “We’re not talking about dumb micro-controllers for control units that are air-gapped any more. We’re talking about smart sensors in the network. We’re talking about smart gateways.”


Hank Skorny

What's more, he points out, "Many IoT devices are fully functioning PCs for all practical purposes, yet we don't treat those devices the way we treat regular PCs on our enterprise networks."

"Look, if you're going to have all these connected devices, you've got to be able to monitor both the state of that device and the hygiene of that device. It must be hardened on your environment."

Echoing previous comments, Pollock insists that companies must monitor IoT devices for behavior, not only access control. "Look for outliers from a behavior standpoint and start to identify what's happening with that device and what it's doing. Focus in on those outliers with the long tail of the curve on what's happening. Identify devices that are doing something that's out of the ordinary, and look at those and investigate those as potential issues."

Because, after all, with IoT devices and IoT applications vulnerable to attack, lives *will* be at stake.

*The author is Robert Haim, principal analyst – Business Analysis & IoT, ACG Research*