print | close

Changing the Mindset in IoT Manufacturing

Electronic Design

Mike Lynch

Thu, 2016-12-08 10:46

In creating Facebook, Mark Zuckerberg popularized the motto: “Move fast and break things.” And it wasn’t long before this mindset was adopted at many other Silicon Valley companies.

In a way, this guiding mantra was liberating for product developers. The saying acknowledged the inevitability of mistakes when making new products and, instead of punishing people for them, encouraged learning from them and moving on.

Unfortunately, it also encouraged a mindset that was potentially reckless. “Move fast and break things” works when making an inconsequential app like Farmville, but is catastrophic when producing a jet turbine, or when it comes to bringing an internet-connected device to market without securing it first.

Related

7 Things to Know About IoT Security

The Biggest Security Threats Facing Embedded Designers

End-to-End IoT Security Starts with the Infrastructure

According to Gartner, approximately 5.5 million new IoT devices are connected each day in 2016, an increase of 30% from 2015, bringing the worldwide total to 6.4 billion connected things for the year. If current growth rates hold, the number of connected devices is expected to reach 20.8 billion by 2020. That’s almost three devices for every person on Earth.

We’re now seeing the consequences of this growth in IoT devices and their rush-to-market mindset in the wave of cyberattacks that occurred across America on October 21. These enormous attacks on web infrastructure providers Dyn and Amazon Web Services, which temporarily brought down internet giants like Twitter, PayPal, and Netflix, were made possible by millions of new internet-connected devices (called the “Internet of Things” or IoT) like cameras, baby monitors, kids toys, and home routers, secured with incredibly obvious passwords, or worse, reusing the device’s default password.

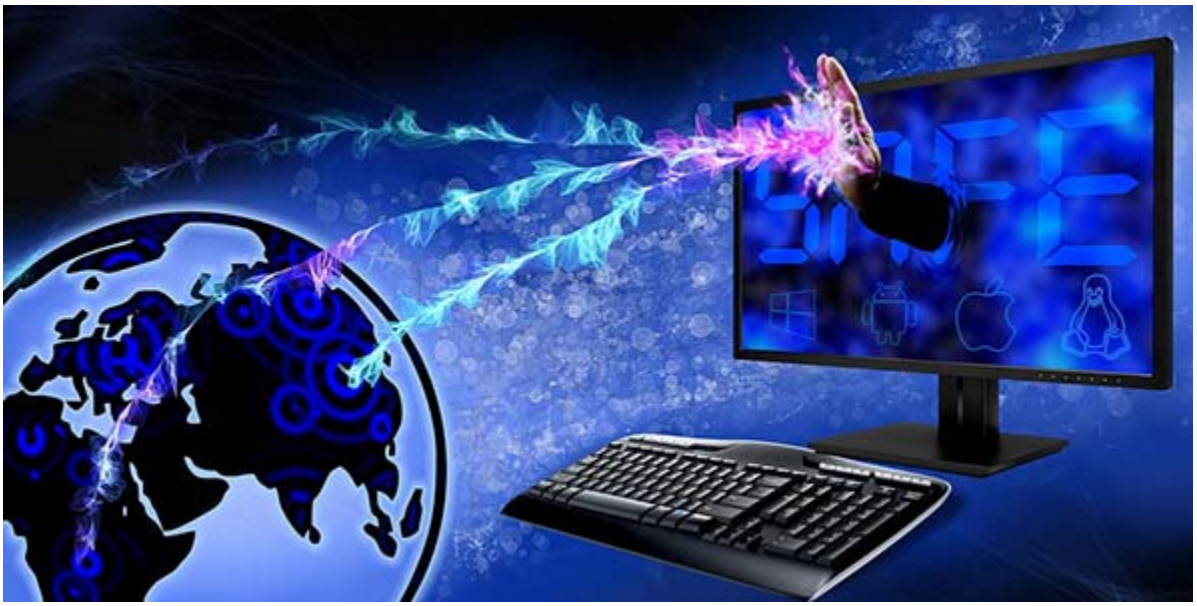
Despite continual prompting about the importance of strengthening passwords on all one’s devices, people continue to disregard these warnings as was proven in this recent hack.

Many Security Holes Being Opened at Once

This recent attack was orchestrated by a piece of malware called Mirai, which exploits the 63 default user names and passwords left unsecured in thousands of internet-connected devices. The malware searches the web for these devices and, after gaining access, seizes control by turning them into “bots” for its own use from a central

ımand center.

Thousands of these bots can then be instructed to flood a targeted website with traffic until it buckles and collapses under the load. Such attacks, known as distributed denial of service (DDoS), are common but have been made more powerful by the ability of hackers to take advantage of weak passwords in IoT devices. It is suspected that almost half a million devices are infected with Mirai and roughly 10% of them were used in the attacks on that Friday.



It's also suspected that the attacks were launched using compromised DVRs and IP cameras made by one Chinese company, XiongMai Technologies**.** These devices were purchased by vendors and used as components to make other products. In effect, one company's entire product line has been weaponized.

Even worse, these particular devices' passwords can't be changed by either manufacturers or customers. They have been hardcoded into the firmware and cannot be disabled. As such, they remain a danger for compromise and use in cyberattacks until they're completely unplugged from the internet.

What's Next?

The size and scale of these attacks have a lot of security professionals on edge asking, "What's next?" A cyberattack in a world filled with billions of connected devices might be used for more than bringing down Twitter. All of these connected devices could be a conduit for bringing down the power grid of a large city, shutting down medical devices throughout a hospital system, or terrorists hacking into a self-driving car carrying a foreign dignitary in an attempted assassination.

It's clear that in a rush to get new connected devices to the public, manufacturers and designers have developed them without the necessary security to protect them from unauthorized use and neglected the potential consequences.

There are a couple of underlying reasons for this behavior. First, device security isn't necessarily a core competency of product designers and manufacturers who are primarily concerned with getting a product built and delivered to market. They may simply be unaware of the complications they're potentially introducing downstream.

Further, those involved in the manufacture of IoT devices may not have executive-level or board support to

us on developing security standards. Security is often viewed as an unnecessary expense by many anizations, one that cuts into margins. Both of these factors combine to create a situation where security is at best an afterthought, and at worst, cavalierly disregarded.

If there's a silver lining to these DDoS attacks, it's that it has called attention to these gaps and lapses of security present in these devices and the change of mindset required to correct it.

As the IoT grows, traditional manufacturing organizations will need a top-down, C-level emphasis on IT security. To do so requires sophisticated technology and an investment in people that fully understand the risks inherent in pushing these devices to market. "Move fast and break things" will inevitably need to become "move cautiously and make sure we aren't blowing things up" (or perhaps, helping others blow things up). In today's always-connected world, we need to have the mindset that we're all involved in security.

Source URL: http://electronicdesign.com/iot/changing-mindset-iot-manufacturing