BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time. • **March 2017**

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

The Terrorist in Your Toaster: The Next Generation of IoT Hacking

Written by Nick Espinosa | Originally published at www.smartfile.com

When I was five, my parents got me a robot. Connected to a wired controller, I could move it back and forth, raise its arms, flash lights and plenty of other awesome things that would spark any child's imagination. I loved that robot even though it sucked in a few different ways.

It made me want to improve it and I would dream of ways it could be better, like having it talk to other robots and machines (I was a tad too young for The Terminator at this point) or making it do things for me. Thanks to the internet and the advancement of robotics, my boyhood dreams are coming true.

We are at the dawn of this era and the Internet of Things (IoT) explosion is the foundation for this advancement. Sadly, though, we must take the good with the bad. As we make our lives more convenient with IoT devices, we must also take notice of the increasing cybersecurity threats and issues accompanying this evolution.

It Starts at the Development Stage

A while back, I wrote an article about how many popular apps had some serious cybersecurity flaws because while they were beautifully designed and engineered, security was essentially an afterthought. These developers failed to include security experts in the design and thus sacrificed this critical point, putting all of their users at risk.

Unfortunately, this issue is also rather pervasive in the IoT world. In speaking with several IoT developers at conferences and also one-on-one with developers who are looking to collaborate with me, there is an overwhelming assumption that the end user of the device will secure it themselves.

This may mean the developers assume that changing the password or putting it behind a firewall is something everyone is going to do. Nothing could be further from the truth! When it comes to security, a poor development strategy is a surefire way to end up on a list that shows the world just how easy it is to break into your device.

It Continues to the End User Stage

The IoT development community should never make the assumption that the end user is tech savvy enough, especially when roughly 60% of all Millennials have "low" technology skills! Most users just want things to work and to be as easy as possible. Unfortunately, developers build to this standard without much thought of how vulnerable this makes everyone.

Consider the average user for a moment. This person knows how to use their mobile phone to make calls, text/IM and run apps. They'll have a Smart TV and can use Netflix and other streaming services. They run applications on their PC or Mac without issues. Odds are they're using the wireless router their ISP has provided them. They're happy as clams using the technology they love, until something goes wrong.

The average user cannot fully troubleshoot their own issues or have the knowledge to fully assess why their technology isn't doing what they want. Combine that with insecure IoT devices they had no problem getting on their Wi-Fi using all the default options and we've got a massive breeding ground for hacker malfeasance.

Now consider that 24 BILLION devices will be online by 2020 and we can start to see why this is a looming problem. With so many insecure devices out there, we're literally sitting on a ticking time bomb and we've already seen some small test explosions.

IoT Devices Unite! …and Kill Your Target.

As a result of these development shortcomings, we have seen some major attacks in 2016 that are essentially the beginning of this issue. As more relatively insecure

devices come online we will see larger and larger attacks unless something is done now.

In the fall of 2016, a new malware infection called Mirai began infecting hundreds of thousands of IoT devices, usually CCTV systems and DVRs, by finding them on Shodan, a search engine for open IoT devices (seriously go search to see if you're exposed; I can't recommend this enough).

Mirai would find these devices and test them using a list of default passwords. Once it found it could properly login, which it found A LOT, it would infect the firmware of the device(s), giving its creator complete control.

The creator did what is now known as the largest Distributed Denial of Service (DDoS) attack in the history of the internet. Using over 150,000 infected devices, the hacker was able to direct the combined bandwidth of all of the devices' internet connections worldwide against various targets.

Brian Krebs, the security researcher, was hit first and knocked out after a valiant effort by his host to fend it off. Then the site OVH was hit and knocked out with levels of attacking bandwidth reaching 1Tbps in size. Dyn DNS was also hit which wreaked havoc with many popular U.S. sites and services like Starbucks, Netflix, CNN and more.

If only 10% of all devices were infected by 2020 then we would still have a 2.4-billion infected devices problem. We need to act now.

All of This Can Mostly Be Avoided

Mirai, as it was programmed, would have never been an issue if the default passwords on devices were changed. That's it! Hundreds of thousands of infections avoided because someone thought to change a password. This is only the start of a good cybersecurity policy for IoT, but there is plenty more that can be done on both developer and user sides. Let's explore some of the solutions that help protect many of the devices we're all going to inevitably be using.

Point 1: Password Policy and Control

This is a tip for developers and users alike. Developers, I know it's easier to just use admin/admin on the zillion devices you're installing your OS/firmware on, but it's not acceptable anymore. Instead, randomize the password based on the serial number of the device or another method that will ensure that every unit has its own unique UI access password.

Users, check your devices and never keep any default passwords. Also never use a password that you would use for other things like banking. If the IoT device has poor hashing of passwords that password may be captured by an experienced hacker.

Point 2: Use Proper Encryption

I can't stress this one enough for developers. Encrypt the firmware in the system so it can only run when paired with the hardware it's connected to. This will help prevent spoofing and needless access to the coding of the device.

If I cannot clone your firmware to see where the flaws are then your device is way more secure and the cost increase is mitigated by the marketing campaign you could have in advertising why you have safe IoT devices!

Point 3: Internal Firewalls Go A Long Way!

Developers, if your IoT device is configured to send traffic on specific ports then why not lock down the rest to prevent attack? You could even go so far as to find an intuitive way to create a network whitelist so only specific computers or devices can interact with your IoT device. Token authentication or a similar method would stop any remote hackers for getting easy access!

Point 4: Isolating IoT Can Limit The Threat

Like everyone else, I also have IoT devices, however, all of mine are on their own wireless network and separate from my computers and tablets. Further, I have enabled bandwidth control on that wireless network so the IoT devices will only get the exact bandwidth they need.

No reason to give them access to huge amounts of the bandwidth when they require well under 1Mbps each function properly. This way any hijacked IoT device cannot spread infections to anything else on my network nor am I giving a hacker access to the full amount of bandwidth I have.

Point 5: Make Smart Choices

Users, I know that having a frying pan that links to your mobile phone will really up your cooking game, but wait a bit if you can. Read the reviews, see what kind of security the frying pan's makers have put into the pan.

After all, it's not just about making the best scrambled eggs. It's also about making the best scrambled eggs while preventing your frying pan from attacking targets on the internet. (Honestly, I never thought I'd write that sentence.)

So, developers, get to work! Create brilliant things but create them securely. Users, do your homework or ask for help. Let's not help the bad guys with a lack of thoroughness!

7 "Lucky Charms" To Dodge A Data Disaster

You stride into the office early one Monday morning. You grab a cup of coffee, flip on your computer and start checking e-mail…

A note pops up that rivets your attention:

"Your files have been encrypted. Send $5,000 within five days or they will all be destroyed."

You start sweating as your throat constricts and your chest tightens. Sure enough, every time you try to open a document, the same message appears. Your phone rings. It's Bob in accounting, and he's having the same problem. All files across your entire network have been encrypted. You contact the local police.

They suggest you call the FBI. The FBI says they can't help you. What do you do next?

a) You pay the five grand, desperately hoping you'll get your data back.

b) You calmly call your IT pro, who says, "No problem, your backups are all current. But that is when he finds out backups LOOKED like they were running when in fact they were not working." You can hear the panic in his voice.

c) You calmly call your IT pro, who says, "No problem, your backups are all current. No files were lost. Everything will be restored by noon, if not sooner."

If your answer is "c," you breathe a sigh of relief and get back to work as your backup plan kicks in…

Ransomware attacks are more common than ever, especially at smaller companies. That's because small companies make easy marks for hackers. The average small business is much easier to hack than high-value, heavily fortified targets like banks and big corporations. According to Time magazine, cybersecurity experts estimate that several million attacks occur in the US alone every year. And that figure is climbing.

So how can you make sure you never have to sweat a ransomware attack or other data disaster? One sure solution is having a solid backup plan in place. When all your data and applications can be duplicated, you have plenty of options in the event of an attack.

Here then are seven ways to make sure you're in good shape, no matter what happens to your current data:

Insist on regular, remote and Redundant processes. A good rule of thumb is 3-2-1. That means three copies of your data is stored in two off-site locations and backed up at least once per day.

Don't cheap out on disk drives. Less expensive arrays that save money can leave your data at risk. Get features like a redundant power supply and hot spare disks.

Guard against human error. Make sure people doing backups know exactly what to do. Take people out of the loop and automate wherever possible. And watch for situations where backups aren't a part of someone's regular duties.

Check backup software settings routinely. When new software or updates are put into service, a change in the way the settings are configured can cause incomplete backups, or backups that fail. Do the people who maintain your backups include this on their regular to-do list?

Make sure critical files aren't getting left out. As resources are added and priorities shift, documents and folders can get misplaced or accidentally left off the backup list. Insist on a quarterly or annual meeting with your backup management team to make sure all mission-critical files are included in your organization's data recovery systems.

Address network issues immediately. Any component in your network that isn't working properly can introduce another point of failure in your backup process. Every juncture in your network, from a misconfigured switch to a flaky host bus adapter, can hurt your backups.

Ask for help with your data backup and recovery system. You cannot be expected to be an expert in all things. Yet data is the backbone of your business – its protection and recovery should not be left to chance. Leverage the knowledge, skill and experience of an expert who stays current with all the latest IT issues. Data Recovery Review Reveals Backup System Vulnerabilities.

Email sbernstein@bssi2.com TODAY or call 847-551-4626 by March 31 for a FREE Data Recovery Review, ordinarily a $300 service. We'll provide you with a complete on-site assessment of your current backup system to check for and safeguard against any gaps that could prove financially lethal to your business.

March 2017#

35 Aztec Court
South Barrington,
IL 60010

(847) 551-4626

www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"Serendipity is up, fluke is doing well, but I'm a little concerned about our dumb luck."

Shiny New Gadget of the Month

Handheld? Console? No, It's…Switch!

Nintendo's long-awaited new gaming platform Switch should be available any day now, if it isn't already. It combines the best elements of handheld
games with a home console. Handheld, the gamepad is the screen. Slip it into its dock and it plays on your TV.

The gamepad comes with two detachable "Joy-Cons." One player can hold a Joy-Con in each hand, two players can each take one, or bring in more
Joy-Cons and multiple people can play.

If you're on the go, pull out the "kickstand" on the back of the gamepad and prop it up on an even surface for easy viewing. There's a slot on the side for game cards and a USB-C port for quick charging.

Because it has greater processing power than the Wii U, you'll have no trouble playing Legend of Zelda: Breath of the Wild, Super Mario and a host of your other favorite Nintendo games.

The Lighter Side….

My therapist says I have a preoccupation with vengeance. We'll see about that.

I think my neighbor is stalking me as she's been googling my name on her computer. I saw it through my telescope last night

Strong people don't put others down. They lift them up and slam them on the ground for maximum damage.

Money talks ...but all mine ever says is good-bye.

You're not fat, you're just... easier to see.

If you think nobody cares whether you're alive, try missing a couple of payments.

I want to die peacefully in my sleep, like my grandfather.. Not screaming and yelling like the passengers in his car.

I find it ironic that the colors red, white, and blue stand for freedom until they are flashing behind you.