In the Boxing Ring
FEB 2021

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the February 2021 edition of In the **Boxing Ring**

This month, our guest contributor - Network Box USA's Chief Technology Officer, *Pierluigi Stella*, is talking about the future of connected devices and the issue of **If you can connect it, protect it**. Typically, IoT devices come with default passwords that are readily available on the Internet and often do not automatically update themselves with the latest software patches. These issues make them vulnerable to security issues. On pages 2 to 3, this, and best practices are discussed in further detail.

In this month's Media Coverage, Network Box was featured in the **South China Morning Post**, **RTHK Radio 3**, and **CDOTrends**. Additionally, security vulnerabilities were found in **Dairy Farm**, **Microsoft 365**, **Nissan**, and **Sonicwall** and **Zyxel** products. Finally, to round-up another eventful year, we have compiled all the key Network Box events in the 2020 edition of **Year in *Focus***.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2021

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

If you can connect it, PROTECT it

by Pierluigi Stella
Chief Technology Officer
Network Box USA

Let's talk about the future of connected devices. About how if you can connect it, then you need to protect it. Allow me to explain. The future of the Internet of Things (IoT) has to be that manufacturers view their devices' security more seriously. There's no other way around it.

First of all, these devices come with default passwords that are normally published on the Internet since users need to download manuals to install or configure them. Once installed, they never really update themselves, and the chances are slim that users might update the software on their own. For me, I counted at least 20 connected devices in my home, and I'm not even a fan. In fact, it took me years to purchase a Nest thermostat or a Ring doorbell. I was recently shopping for refrigerators and came across the Samsung model with a large tablet on the door. You know, the one with which you can create a shopping list and then send it to your phone? Tell me, who's ever going to say, "I need to update my fridge?? "!!

Forget it

That aside, IoT isn't confined only to home gadgets as numerous other industries use portable devices too. Think hospitals with their instruments and medical carts. Or refineries with an entire Operational Technology (OT) department dealing specifically with IoT issues. Sure, these are more likely to be updated with manufacturer passwords changed since someone's job would otherwise be on the line.

All these devices have one thing in common – well, perhaps more than one – but this one thing is certain. They're all based on embedded Linux. Microsoft tried, a decade ago, to fight an impossible battle by introducing Windows ME. And lost. Brutally. Why? Well, let's be real here, nothing beats free. Plus Linux is far superior to any other personal OS, let alone the poorly conceived child of Windows that was ME. The issue of using embedded Linux is that there's no inherent security. Even though Linux **is** great to build security (case in point: all Firewalls today are based on Linux), that doesn't mean it's secure straight from the box. Or that embedded Linux **is** secure.

Not at all

To be clear, embedded means it's been stripped of everything that isn't strictly necessary. A move that's meant to reduce digital footprints, so it fits into very small flash drives.

Yes, I'm oversimplifying

And intentionally so since my focus is on the security aspects. I can't stress enough that if you can connect it, then you absolutely must protect it. There's no other way around it.

Same OS for all (translating into likely the same vulnerabilities as well), default passwords, no updates. The worse cybersecurity scenario, all in one same place. Try telling a Chief Information Security Officer (CISO), "I'm going to give you a network of 1000 devices. They'll all run on the same operating system, unprotected. They'll have the same vulnerabilities. Same default passwords and no, they can't be updated." I guarantee you he'd quit. Right there and then. And yet, this is today's reality for IoT.

This is the primary reason why connected devices are such a cybersecurity nightmare.

Statistics abound on how hackers are exploiting these devices to launch attacks. One such act of aggression which catapulted IoTs to the forefront was a DDoS that involved a million such devices. All of which had been taken over by the one same botnet. Because yes, once you take over one of them, they're just computers.

No more, no less

Computers can be reprogrammed for just about any purpose. The computing capacity these devices hold is unimaginably vast, and certainly much larger than needed for their original purpose because there aren't any smaller CPUs around. Just as I can't really purchase a 500GB HDD these days, I'd also have a hard time acquiring a 'slow' CPU. They simply aren't in the market anymore. Manufacturers utilize what's available. What that often means is quad cores with the computing power of Herculean proportions. Think of it as though we're putting more computing power into a light bulb than we'd need to go to the moon. Imagine that! And when the security isn't sufficient (and, by the way, it never is), things go really, REALLY wrong.

So what's our solution to this?

In a company environment, that CISO, if he hasn't resigned yet, may attempt to bolster the devices with security updates. He might change passwords, and possibly even protect access to them with proper firewalls, IPS, etc. But that's not going to be the situation in a home or a small office where you'll typically barely even find an unattended firewall. And definitely zero security expertise. In such an environment, those devices remain unsecured and as vulnerable as when they came out of the box. The only solution is for them to be secure from the time they leave the manufacturing plant. Straight out of the box, as the expression goes.

One other idea is to get rid of default passwords

Generate some type of QR code, allowing the user to "find" the access code online. Or write that unique password on the box itself. Hold on, don't scream just yet. This isn't as bad an idea as it may sound. If the password to my Ring doorbell was written on the cardboard box it came with, and no hacker would know that. It'd be a random, long string password that was automatically generated when the device was manufactured — and then printed on the box. Who'd see it once it was installed? And even if you saw it at the store, what good would that do? The analogy would be like finding a door key in the park. You wouldn't know which house it belongs to, and as such, it doesn't pose a threat. On the flipside, that Ring doorbell now has a password that's long, random, and doesn't need to be changed.

Updates too can be automated.

My ISP already does that for their router

Once in a while, especially in the middle of the night, that thing sounds like it's being possessed by demons. The first time I heard it, I thought it'd been hacked!! Then I learned that it was the ISP running an update. My security dashboard does the same, and one time, they decided to do it in the middle of the day just as I was trying to turn it on because I needed to leave the house. Very annoying. I had to wait 5 minutes, sitting on my couch, patiently watching that thing go through the motions until it was done and ready again. That being said, I did feel assured that at least those devices were being updated. I'm fairly certain some of the updates were security-related, and that's good.

Manufacturers must take ownership of updating these devices

They cannot leave it to the general public because that simply isn't going to happen, leaving them (and their owners) completely vulnerable. This is what Microsoft had to do with their Windows computers. This is also what IoT manufacturers will need to do if they wish to ensure their devices aren't taken over by hackers in the time it takes to say 'hacked'.

In the interim, if you can, change all the passwords to all the devices in your house and update their firmware.

YES, I KNOW — I can only dream.

Network Box HIGHLIGHTS

Network Box
Year in *Focus* 2020

2020 was an eventful year for Network Box. The past year saw the opening of two new offices in **Austria** and **Spain**. In addition to upgrades to the **E-Series** hardware units, the **M-255i** was launched for small offices that require a high volume of storage. Furthermore, **NBSIEM+** (Network Box Security Incident and Event Management+), and the upgraded **Dark Web Monitoring Service** was released.

As a special end-of-year summary, Network Box has complied all the key events of the last twelve months in the 2020 edition of *Year in Focus*.

LINK: https://network-box.com/sites/default/files/files/Year_in_Focus_2020.pdf

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Network Box Media Coverage and Security Headlines

SCMP
Amid privacy concerns, WhatsApp users face one question: to switch, or not to switch?
LINK: https://bit.ly/2NDo7XK

RTHK Radio 3
Backchat with Hugh Chiverton: *WhatsApp*
LINK: https://bit.ly/2YmuDnW

CDOTrends
Virtual Patching Explained
LINK: https://bit.ly/3aeL7E7

Bleepingcomputer
Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack
LINK: https://bit.ly/3adPBef

The Hacker News
SonicWall Hacked Using 0-Day Bugs In Its Own VPN Product
LINK: https://bit.ly/2KXu3tF

SC Media
SolarWinds attack opened up 4 separate paths to a Microsoft 365 cloud breach
LINK: https://bit.ly/3t91E51

Bleepingcomputer
Nissan NA source code leaked due to default admin:admin credentials
LINK: https://bit.ly/3t4wsUF

ZDNet
Backdoor account discovered in more than 100,000 Zyxel firewalls, VPN gateways
LINK: https://zd.net/2MxdLZ8