

TACTICS PREPAREDNESS

SKILLS AND SURVIVAL FOR ALL SITUATIONS



A FIGHT FOR YOUR LIFE GOES DOWN FAST AND HARD - LEARN TO USE YOUR NATURAL REACTION TO FLINCH AS A BASIS FOR AN EFFECTIVE DEFENSE.

BE YOUR OWN

BODYGUARD

WITH TONY BLAUER'S SPEAR

BY: CHRIS GRAHAM / PHOTOS COURTESY TONY BLAUER www.blauerspear.com

On a warm winter day I walked into Jayson Keel's CrossFit Jackson in Jackson, Tennessee.

After a few years of coordinating schedules, I finally had the opportunity to attend one of Tony Blauer's training events.

Be Your Own Bodyguard (BYOB) is a one day crash course in modes of criminal attack and using your body as effectively as possible to prevail against one of these attacks. The insights taught are compatible with any viable fighting system and are intended to

augment (not replace) your preferred defensive tactics.

The training started with a PowerPoint lecture. Blauer stated that fear functions as either a fuel for action or as an inhibiting weight. He asserted that how you manage fear affects all aspects of your life, from who you marry to where you work. He pointed out that people have to perform gun takeaways comparative-

ly rarely, but they are faced with managing fears every day of their lives.

Blauer suggested that the concept of situational awareness must be rethought. Simply telling someone to have or improve situational awareness is unreasonable. Honestly acknowledging when and where your situational awareness is limited is critical. Blauer also explained that self-de- *continued on next page*



The last few years have seen a slew of products released that are “smart” or at least aware of a world outside of the confines of the hardware.

As smartphones became ubiquitous, product designers realized that instead of spending significant dollars on user interfaces to products, they could leverage a smartphone app instead. For those of you who remember the first Fitbit pedometer, it has a small LED display, one button, and a set of charging leads. The magic of data analysis, collection and health management happens via their smartphone app. You don't need a fancy full-color display because you have a smartphone to do that for you.

This method has been the answer to modernizing many systems that act more like industrial control systems than computers. Just perusing your local hardware store should yield lots of smart products such as sprinkler systems, home alarm systems, garage door openers, thermostats, smoke detectors, light bulbs, small appliances, home automa-

tion and door locks. These devices belong to a new class of systems called The Internet of Things (IoT). The degree in which IoT devices interact with the outside world varies by product and communication techniques, but most of these devices will leverage technologies like Bluetooth, ZigBee and Wi-Fi to do this. The question is, are these technologies safe for me to use? What's the risk to me?

WHO DO YOU TRUST?

In the most basic sense, a DirecTV receiver (or really any type of set-top pay TV system) is a computer that streams content delivered over the air or over a wire. In the case of DirecTV, it is a computer with Linux installed to deliver services to subscribers like us. Linux is a free operating system that started as a hobby by then University of Helsinki student Linus Torvalds, deriving most of its' likeness

from the UNIX operating system created by AT&T's Bell Labs. Since its' release, it has been popular in deployments due to its free licensing, the huge community of developers that support it and the general availability of Linux across a wide range of hardware. It's proliferation lead to many companies adopting variants of Linux to power devices like DirecTV Receivers and embedded devices. If you are one of the millions of people with an Android phone, congrats! You are also a Linux user. Android leverages components of Linux to make your smartphone work.

But there is a darker side to Linux, namely that it is one of the platforms of choice used by hackers globally. As a security consultant, I had a number of Linux laptops and servers at my disposal to perform my duties as a penetration tester. I regularly used Linux platforms to break into corporate networks (where I

BY: DR. BRANDEN R. WILLIAMS



ALL LOGOS ARE REGISTERED TRADEMARKS OF THEIR RESPECTIVE COMPANIES

was paid to do so) either over the Internet or by leveraging unprotected network jacks or wireless networks. I once broke a major healthcare provider's wireless network in a matter of minutes, which earned me a sideways look from the then information security director. If someone were to ask me to start breaking into a computer system today, I would probably start by leveraging a Linux-based computer to gather my toolkit together. Thanks to the popularity of the platform as a penetration testing launchpad, there is no shortage of tools available to someone who knows how to use them.

I was giving a talk at a conference about network security and someone asked me how many different networks I had in my house. I told them that I was an edge case, with five separate networks, all governed by

a single firewall that controlled how traffic can move from one to the other. I built this setup years ago to prove a point to many of the companies asking for expert security advice and it allowed me to speak with authority on how to build virtual secure areas inside of a corporate network. When they laughed and asked why I would ever maintain something like that, I asked them if they trusted their pay TV provider. They looked at me funny, and I said, “Remember, that device is just a Linux machine sitting on your network. Whether malicious intent or just poor design, anyone with access to that system can now do a number of nasty things to any device connected to the same network.” Do I think AT&T is going to launch attacks on my home network on purpose? No, but the capability is there. Given the size of AT&T and their history,

I'm not sure why I would trust their devices implicitly inside my home.

With smart device product releases increasing by the day, the problem is only compounding itself. Take as an example two very serious vulnerabilities from 2014 that still exist

in many systems today. One is called Heartbleed¹, the other is called Shellshock². The first allows a criminal to gain access to key material that can be used to decrypt information that you expect to be kept safe, and the other allows for a remote user to completely take over a device running a broken version of the BASH shell—software present on most Linux systems. The reason why these vulnerabilities are still viable is because many smart devices cannot be updated with patched versions of the software or use poor communication techniques when communicating telemetry to their designers. You have a right to be worried as bugs like this could lead to the disclosure of personal information (or information that could be used to de-anonymize information to identify you specifically) or could just lead to a slow internet connection as the device is used as an attack platform.


YOUR HOME NETWORK IS A LAUNCH PAD

A popular kind of cyber attack is called a Denial of Service (DoS) attack, where packets are crafted in a way that either overwhelm or crash bits of code that prevent legitimate users from accessing key resources. An example of this would be an attack against CNN or Amazon that would overwhelm their services such that you and I could not get their websites to load in our browsers. When these types of attacks are launched from a single



CABLE TV ON-DEMAND SYSTEM HOOKED INTO THE HOMEOWNER'S WIRELESS INTERNET.

"ANYONE WITH ACCESS TO THAT SYSTEM CAN NOW DO A NUMBER OF NASTY THINGS TO ANY DEVICE CONNECTED ON THE SAME NETWORK."



FREERANGESTOCK - YABOONPICS



THE EASIEST THING

is to set up a guest network inside your house and put all of your IoT devices there if you want to use the functionality available to smart devices.

place, they can be fairly easy to stop by blocking the computers they are coming from. Attackers figured this out and made the attack worse by distributing it to many computers—a Distributed Denial of Service (DDoS) attack. In this case, it becomes difficult to understand what is legitimate traffic and what is attack traffic because the requests are made to look like general users. Stopping DDoS attacks has become such a combination of art and science that a small cottage industry of players began offering services to stop these kinds of attacks. When it comes to silencing a voice on the Internet or overloading systems that conduct business, DDoS is extremely effective.

Last month the prominent information security journalist Brian Krebs reported that a sophisticated DDoS attack took his site offline for a period of time—a historically-unmatched attack with the amount of traffic it generated. After further investigation, it turns out that the main culprit behind this attack was a network of compromised IoT devices that were taken over and given instructions to flood his site. According to Motherboard, hundreds of thousands of devices were known to be compromised and hackers are battling each other to maintain control of

these poorly secured devices³. The network of compromised devices has increased steadily after the hackers rumored to have taken down Krebs' site released the source code to the software used to command the compromised devices. The worst part is that the good guys are not sure how to stop this incredibly effective style of attack, and the end is not in sight.

WHAT CAN YOU DO?

In some cases, you must provide Internet access to the devices you want to use in your home. For example, if you want to stream any sort of entertainment from an Apple TV or Roku device, you must provide it with a way to reach the Internet. Other devices, such as the August Door Lock, do not require Internet access to work and will leverage your smartphone to toggle the lock and update its internal software. Depending on your level of networking knowledge, the easiest thing is to set up a guest network inside your house and put all of your IoT devices there if you want to use the functionality available to smart devices. It may require you switching networks on your smartphone or your computer every so often to access services provided by the smart device.

The best advice I could give you is to understand the technology you are using before deploying it. Not all technology is easy to use, so if you decide to deploy anyway, just remember that the device could be used in an attack against others as easily as it could be used against you. For more information on Internet of Things hacking, you can see this aggregation of talks given at this year's Black Hat conference in Las Vegas: <http://brando.ws/BHIoT2016> ✓

BIO

Branden R. Williams (www.brandenwilliams.com), DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow, and technology executive sought after by global companies to consult on their digital business initiatives. His latest book on PCI DSS v3.2 Compliance is due out later this year.

NOTES

1. <http://heartbleed.com>
2. [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))
3. <http://brando.ws/loS2016>

