Cybersecurity Briefing 6/14/16

Zachary Nandapurkar

How Safe are Our Most Powerful Weapons

Recently in 2014, Comedian John Oliver ripped to shreds the defense system responsible for protecting most of America’s nuclear stockpile. Citing multiple times that they are “the most dangerous things on Earth,” he spent a segment of his show researching how exactly these weapons of mass destruction are protected.1 The results were far from something the American public would like to hear. For example, an officer inserting a floppy disk into the mainframe that controls them apparently still activates some nuclear systems. Also, a well-kept secret is that we accidently dropped nuclear bombs on ourselves a couple of times in places like North Carolina, only to find ourselves lucky that they did not detonate.1

The Department of Defense has three main operations when it comes to protecting systems and networks. To support its missions in protecting its controls, it has to work on assessing potential threats outside of cyberspace to boost collective intelligence efforts and defend U.S. interests. For example, the Department of Defense works with many different areas of the U.S government, taps into resources within the private sector, and works with other countries to share and gather data, build alliances and partnerships, and create different protocols that shape how the data is stored and protected.4

The President ultimately makes the choice when it comes to how the DoD must allocate its resources. In cyber it has 3 main areas to cover. First, it must defend its own “networks, systems, and information.” The U.S. military finally realized however, by 2011 that its dependence on cyberspace for defense operations was too great not to declare cyberspace as an operational domain for purposes of organizing, training, and equipping U.S. military forces. With this it finally opened up the idea of cyberspace as a battleground for war, albeit possibly a little later than the government would’ve liked it to happen. First, the Defense Department has the large project of securing its own networks against attack and implement a recovery plan to quickly recover data if security measures fail. To this end, DoD must continually monitor its its vast amount of systems to make sure that the Department of Defense Information Network (DoDIN) is completely secured (or at least as secure as possible). When inevitably DoD detects any sign of hostile activity within its networks, DoD claims to have quick-response capabilities to minimize the damage and re-secure its complete network. This mission is undoubtedly the majority of the DoD’s focus as failure to do so could result in serious catastrophe.4

In serving this mission, the department of Defense has created the U.S. Cyber Command that serves solely to protect the DoD’s cyberspace. It names four main trends that contribute to likelihood of a major cyber breach which are that first autocratic governments such as China and North Korea that view the open Internet as a lethal threat to their regimes. Next they have to take into account ongoing campaigns such to steal intellectual property, like Wikileaks or Anonymous. Then there are disruptions by a range of actors whom could be random people that range from denial-of-service attacks and network traffic manipulation to the use of destructive malware. Lastly they also are concerned with states that develop capabilities and attain system access for potential hostilities. This is specifically concerning the Russians perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage.5

In terms of some specific Cyber Attacks that Cyber Com is trying to assess, two specific vulnerabilities seem to stand out in their report. One is called the Heartbleed vulnerability that “allows attackers to steal information, even though it usually is encrypted, that’s used to secure the Internet for applications such as Web, e-mail and instant messaging, among others. Attackers can eavesdrop on communications, steal data directly from the services and users, and impersonate services and users.” Going more in depth, the Heartbeat bug tests TLS/DTLS secure communication links by letting a computer at one end of the connection send a “Heartbeat Request”, which consists of a payload, along with the payload's length which is a 16-bit integer. The receiving computer then must send exactly the same payload back to the sender in order for it to be verified.7

Since affected versions of OpenSSL allocate memory space for the message to be returned based on the length field in the requesting message, without regard to the actual size of that message's payload, the message returned consists of the payload, possibly followed by whatever else happened to be in the allocated memory buffer.7

Heartbleed is therefore put in the use by the attacker sending out a malformed heartbeat request with a small payload and large length field to the victim in order to elicit the their response, which allows attackers to read up to 64 kilobytes of the victim's memory.7

The other is called the Shellshock is a vulnerability that “gives attackers the ability to run remote commands on a system.” Basically, users of a system have the ability to execute commands that should not be accessible to them. This happens through a feature called "function export", where command scripts created in one instance of Bash can be shared with lesser instances. The feature is put into effect by encoding the scripts within a table where the table is shared between the instances, known as the “environment variable list." Each new instance of Bash scans this table for encoded scripts, then they package each one into a command that defines that script in the new instance, and finally executes that command. These however, were found on DoD software and were swiftly and quietly handled by Cyber Com.6

Despite what John Oliver claims about our lack of care for these weapons, which is based solely on news reports, the U.S. government claims that the cyber defense systems protecting our nuclear stockpile from an outside breach are top notch. A report by the Nuclear Threat Initiative highlights four layers to the cyber security behind nuclear weapon defense.

* Firewalls are the first layer of defense and are placed at various levels of the network on which the nuclear weapons sit. They are an effective measure to block off unwanted port entry from the global network and mainly protect from any hackers physically gaining remote access.
* Since viruses can still get through ports that were intended to be left open, firewalls are not an effective defense mechanism for them. Therefore, cutting edge anti-virus software is built specifically for nuclear systems and installed on the computers within the network that control them.
* Anti-Virus software and firewalls as many may realize, still cannot prevent all attacks or even every type of exploit posed to a nuclear system. Therefore, all nuclear systems also have intrusion detection systems to alert in case of a new undetectable virus, or certain worms that disguise themselves as other programs to beat anti-virus.
* Finally the government will employ ethical hackers and pay for ethical hacking services to manually monitor attacks and also to continue to test the capabilities of the nuclear defense systems to locate the weaknesses before malicious hackers are able to do so.2

While it may sound like these highly sought after nuclear weapons may not have much more cyber defense capability than a simple personal computer, U.S. News and World report claims the system is extremely effective. According to their statistics, the computer systems of the agency that controls the United States’ nuclear weapons stockpile are under constant attack. To be exact, they apparently face somewhere around the region of 10 million attempted attacks per day. Of these however, only one hundredth of one percent can be called a successful attack against just the outer computing structure itself, let alone the systems that allow nuclear launch.3 Cybersecurity experts also added that the launch systems are disconnected from the standard internet, and it would therefore be easier to hack into the Department of Energy and “build a bomb from scratch.”3

While it remains that no system is completely immune to cyber attacks, it seems as though the most risk any system faces currently stems from human error on the side of the nuclear weapons themselves, and not from an outsider able to infiltrate the systems.

Works Cited

1. Hartsell, C. (2014) *John Oliver: Americans are nuclear weapon Hoarders*. Available at: http://www.huffingtonpost.com/2014/07/28/john-oliver-nuclear-weapons-last-week-tonight\_n\_5626532.html (Accessed: 14 June 2016).
2. Chamales, G. (2015) *A new approach to nuclear computer security*. Available at: http://www.nti.org/media/pdfs/A\_New\_Approach\_to\_Nuclear\_Computer\_Security.pdf?\_=1445875704&\_=1445875704 (Accessed: 14 June 2016).
3. Koebler, J. (2012) *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*. Available at: http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily (Accessed: 14 June 2016).

HIS PAGE LEFT INTENTIONALLY BLANK (2015) Available at: http://www.defense.gov/Portals/1/features/2015/0415\_cyber-strategy/Final\_2015\_DoD\_CYBER\_STRATEGY\_for\_web.pdf (Accessed: 15 December 2016).

1. Cybercom chief: Cyber threats blur roles, relationships (2015) Available at: http://www.defense.gov/News/Article/Article/604225 (Accessed: 15 December 2016).
2. *ShellShock: All you need to know about the bash bug vulnerability* (2016) Available at: https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability (Accessed: 17 December 2016).
3. Nieva, R. and 0700, 00 - (2014) *Heartbleed bug: What you need to know (FAQ)*. Available at: https://www.cnet.com/news/heartbleed-bug-what-you-need-to-know-faq/ (Accessed: 17 December 2016).