Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of
Promoting Stakeholder Action Against Botnets
and Other Automated Threats

Docket No. 170602536-7536-01
RIN 0660–XC035

COMMENTS FROM THE SECURE SYSTEMS LABORATORY AT THE NYU TANDON SCHOOL OF ENGINEERING

The Secure Systems Laboratory[1] in the Center for Cybersecurity at the New York University Tandon School of Engineering applauds NTIA's efforts to "improve industry's ability to reduce threats perpetrated by automated distributed attacks"[2], and we welcome the opportunity to add some perspective to the issue. As your agency contemplates the best way to address the multifaceted threats to the cybersecurity of Federal networks and critical infrastructure, as touched on in Executive Order 13800, it is important to marshall solutions that have been proven in practice. In a few short years, our lab has garnered practical experience through working with cybersecurity leaders in both the open source development community and commercial providers. In doing so, we have provided solutions to many important real-world problems. In particular, we have considerable expertise in building software update security systems that have been deployed in a wide variety of domains, such as major tech startups, and automobiles.We hope through this RFC to open a gateway for collaboration with your agency through which we can assist in securing the "new generation of connected devices."[2]

---

[1] These comments refer to "Secure Systems Laboratory" for ease of reference. The Secure Systems Laboratory (SSL) at New York University, under the direction of Professor Justin Cappos, works to find practical and deployable solutions to real-world security threats. *See* Secure Systems Lab's website at https://ssl.engineering.nyu.edu/overview.

[2] Dep't of Commerce, National Telecommunications and Information Administration, "Promoting Stakeholder Action Against Botnets and Other Automated Threats" (June 13, 2017) at 27042, *available* at https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-cyber-eo-rfc-06132017.pdf.

A HYPOTHETICAL CYBERATTACK THROUGH IoT

It's 4th of July, 2018. In Washington DC, as every where else in the U.S., people are feeling festive. Families are waiting patiently for the fireworks to light up the sky. However, elsewhere in the city, at the ER of one of largest hospitals in America, doctors and nurses were frantically dealing with a string of unusual number of cases. Patients were thrashing about with explained seizures, losing consciousness due to internal bleeding, hallucinating images of non-existent people, turning blue, and slipping into comas. In only a matter of minutes all these patients would die. Tracing back the cause of all these conditions occurring at once yielded one common source - an overdose of medicines[3]. After closer inspect, the IT department of the hospital confirmed that an automated medical supply system used to automatically dispense medication had malfunctioned due to a piece of malware that had been downloaded and signed as a regular update. The malware converted the individual dosing into functional bots in a botnet in a hacking scheme masterminded by a rogue nation. The scheme was to inject deadly amounts and combinations of medicines into the maximum number of patients in the shortest amount of time.

While such a scenario is, currently, only a work of fiction, we fear that such a scenario is more probable than it might appear to be. Cisco estimates 6 IoT devices per person will be in use by 2020[4] and with the success of organizations like openwireless.org that promote ubiquitous wireless connectivity[5], it won't be long before we are ushered into a world where everything

---

[3] *See* "Symptoms of Drug Overdose" available at https://www.betterhealth.vic.gov.au/health/healthyliving/drug-overdose.

[4] *See* Cisco, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" on Page 3, available at http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[5] *See* "What is Open Wireless Movement", available at, https://openwireless.org/.

from the controls of a kettle to that of a pacemaker could be open to public internet and, thus, vulnerable to adversaries. Companies would be expected to take necessary steps to secure these devices from being easily exploitable. However, if history and experience has shown us anything, it is that hackers will always find ways to exploit bugs and break into repositories, especially if it can lead to a scenario where serious harm can be inflicted upon the targets.

We commend the NTIA for recognizing that "IoT devices are often built and deployed without important security features and practices in place"[6]. In acknowledging this idea, your agency has identified an important new research challenge. To provide some direction for approaching that challenge, we respectfully suggest the following guidelines..

I. NTIA should establish a Security Standard for Software Updates on IoT devices, regardless of the manufacturer or brand of the product, as such a uniform standard would establish a significant barrier for would be attackers.

The Secure Systems Lab believes that software updates are a critical step to ensure software vulnerabilities in IoT devices are patched in a timely manner. Software updates allow manufacturers to remotely and quickly patch bugs, malware and exploitable vulnerabilities in their devices. Fixing these vulnerabilities is one way to keep IoT devices from becoming bots in a bigger botnet attack. However, the security of IoT devices has been rendered even weaker because manufacturers are reluctant to roll out updates to patch bugs. Because many IoT devices are inexpensive, and likely to be replaced after only a few years, manufacturers see developing

[6] National Security Telecommunications Advisory Committee, *Report to the President on the Internet of Things* (Nov. 19, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

updates as economically irrational. However, since software updates can be key in securing IoT devices and preventing their use as bots in the next DDoS attack, such an investment must be encouraged.

Uniform standards can ensure software updates are issued in a timely manner, thus preventing delays in fixing bugs and security holes. Neglecting timely updates has in the past, and can in the future, lead to major cyberattacks worldwide. For example, the recent WannaCry Ransomware Attack[7] was a direct result of updates not being rolled out in a timely manner to patch bugs in the Microsoft Windows operating systems. The attack encrypted files and data and demanded bitcoins as ransom to decrypt the files. WannaCry ended up being one of the biggest hacks in history, bringing police departments, hospitals and several other organizations to their knees. Economic losses are estimated to be more than $4 billion[8]. The need for timely software updates to fix such exploitable bugs and to address malware is very dire in IoTs, since a major attack on this sphere can potentially lead to the IoT devices being controlled as bots in a botnet attack. The NTIA has accurately highlighted the recent Mirai attacks as an example of an exploit of IoT devices. The Mirai Attacks that were "the largest of its kind in history"[9] fortunately did not lead to any loss of life. However, with the surge of IoT devices in the medical, industrial and other sectors, a similar attack could easily lead to loss of life.

Softwares updates must be meticulously handled, and done so with a high degree of caution, as the process itself can be a vulnerability. As powerful and effective as software

---

[7] *See* "Microsoft held back free patch that could have slowed WannaCry," an article in *The Financial Times* available at https://www.ft.com/content/e2786cbe-3a97-11e7-821a-6027b8a20f23?mhq5j=e3.

[8] *See* "'WannaCry" ransomware attack losses could reach $4 billion," a report by CBS News available at http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

[9] *See* "DDoS attack that disrupted internet was largest of its kind in history, experts say," an article in *The Guardian*, available at https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

updates are in patching exploitable bugs and malware, the update process itself can be a vulnerability. For instance, an attacker can perform a man in the middle (MiTM) attack[10]. This is a relatively straightforward attack that can enable attackers to tamper with software updates by intercepting the communication between client and server. This would allow the attacker to distribute malware as updates. Recently, Keen Security Lab, a division of Chinese Internet giant Tencent, demonstrated the vulnerabilities in Tesla's Model S[11]. The exploit required the vehicle to be connected to a hotspot controlled by adversaries, following which an attacker could have assumed control of several vehicle systems. The vulnerabilities that Keen Labs demonstrated could "search for a destination on the car's GPS, control the entertainment and instrument screens, pop the trunk and even hit the brakes while the vehicle was in motion."[11] Although Tesla patched the vulnerabilities, it is not hard to imagine the extreme consequences that could have been had Tesla had not proactively not done so. While all this attack did was intercept connections between server and client, the possibilities of an attack where an adversary controls the repository or the server itself are well beyond imagination. Such an attack extended to IoT devices, which is not hard to conceptualize, could easily install malware on these devices and make the devices work as bots in the botnet to serve the role the attacker had planned.

We, therefore, highly recommend that NTIA set and enforce a security standard to be adopted by device manufacturers and software developers that mandates the use of software updates to reduce potential vulnerabilities.

---

[10] *See* "Man-in-the-middle attack", available at https://en.wikipedia.org/wiki/Man-in-the-middle_attack.

[11] *See* "Car Hacking Research: Remote Attack Tesla Motors", a report by Keen Security Lab of Tencent, available at http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/.

II. NTIA should make compromise-resilience a mandatory component of the IoT update security standards to protect vulnerable endpoints.

Secure Systems Lab strongly believes that any minimum standard for securing software updates must be capable of withstanding cyberattacks from strong adversaries and, at its core, must be compromise resilient. That is, even if attackers compromise a software repository, or the server itself, or if they manage to intercept communication between server and client, the least number of IoT devices are affected and minimal damage can be inflicted upon the affected devices. Such a compromise-resilient framework would allow us to "rapidly deal with newly discovered vulnerabilities,"[12] fix system crippling bugs and combat malware.

Secure Systems Lab recognizes NTIA's commendable effort to secure IoTs and asks them to take a critical look at the two most-commonly implemented approaches before committing to a less than compromise-resilient system. To the best of our research and knowledge, we have yet to see any software update system for IoT that provides compromise-resilience. There are two typical off-the-shelf security systems. One system uses SSL / TLS[13] to encrypt updates in transit. This protects IoT devices from the aforementioned MitM attacks, but does not provide compromise-resilience. This is because attackers who compromise the repository itself can use the online SSL / TLS key to instantly distribute and install malware. The other system uses a single offline GPG / RSA[14] key to sign updates. This is better, but a compromise of this single key breaks the security of the whole system. Often, this

---

[12] *See* Dep't of Commerce, National Telecommunications and Information Administration, "Promoting Stakeholder Action Against Botnets and Other Automated Threats" (June 13, 2017) at 27043, *available* at https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-cyber-eo-rfc-06132017.pdf.

[13] *See* "What is a Secure Systems Lab Certificate", a guide by Symantec, available at https://www.symantec.com/page.jsp?id=ssl-information-center#.

[14] *See* "Public-Key Cryptography," the technique behind GPG and RSA, available at https://en.wikipedia.org/wiki/Public-key_cryptography.

key is kept online because it is inconvenient to frequently sign for new updates using an offline key, thus increasing its vulnerability.

The most common approaches err by having a single point of compromise, which if exploited can make the entire system redundant. In researching ways to make truly compromise-resilient update frameworks, the Secure Systems Lab has developed a number of key principles that govern our designs. The first of these principles is a separation of duties between different servers and repositories. Such an approach minimizes the effect of compromise of any individual repository or server. Our team has learned through experience that every system is exploitable and compromisable[15]. For this reason, we propose a system that would need to be compromised and exploited at multiple points, which would compound the overall level of security. The increased level of security would owe to the fact that different types of information are signed by different parties. An attacker would have to compromise all of the servers and repositories to achieve any lasting damage, which would be a monumentally challenging task for even the best of adversaries.

We have, through research in the past, identified design principles that have truly made software update chains compromise-resilient. We have found that, along with separation of duties, a number of other design principles can makes servers and repositories significantly harder to compromise. We took inspiration from real life, where different keys held by different people must come together to perform safety-critical actions,and designed a system that would need more than just one key to successfully complete the signing process. This way another layer of security is added as the possibility of an adversary gaining all keys would be

[15] *See* "Diplomat: Using Delegations to Protect Community Repositories," a paper prepared by researchers of the Secure Systems Lab, available at https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-kuppusamy.pdf.

rare. We also propose having a way to revoke keys, both implicitly and explicitly, this would provide a solution for when the keys are lost, or worse, stolen. Lastly, we highly suggest having particular keys hosted offline i.e. not accessible from the Internet (e.g. on USB drives kept in a deposit box), where they are impregnable. These offline keys can be instrumental in establishing a root of trust that would be completely secure.

We have implemented these design principles in past projects to secure updates in software repositories[16], and in autonomous vehicles[17]. We are currently working on other applications as well. We strongly believe, that these techniques can all be adapted towards designing a truly compromise-resilient update framework for IoT devices without losing flexibility or functionality.

III. The NTIA and the Federal government have a strong role to play in establishing an IOT consortium in which all the stakeholders in the IoT sphere can jointly develop a compromise-resilient security update framework.

The rate at which the IoT industry is scaling up makes us label it the next catalyzing force for innovation in the world of technology. We need to act now to secure interconnected IoT devices**.** We want to work with other stakeholders to design a compromise-resilient system that would allow us to secure the chain of updates that could address security bugs in IoTs, improve the devices' performance, and defend the interconnected web of devices that could redefine everything from manufacturing to medical practices to the way we heat our water.

---

[16] *See* "The Update Framework", a compromise-resilient update framework for software repository, available at https://theupdateframework.github.io/.

[17] *See* "Uptane", a compromise-resilient update framework for Autonomous Vehicles, available at https://uptane.github.io/.

Secure Systems Lab commends NTIA on issuing this RFC and thus seeking a wide variety of different views from all stakeholders of how to secure the sphere of IoT devices, an important first step in the establishment of the consortium proposed above. We believe that such collaboration could hold the key to securing the soon-to-be multi-billion dollar IoT device industry. We believe that security should not be treated as a competitive advantage, and what is needed is an open-consortium of ideas, solutions and proposals from all the stakeholders and experts. Enhancing security, not only of IoT devices but of the entire networked world, could be extremely beneficial to the US economy as well.

Open communication can be instrumental in weeding out security vulnerabilities and allow the cybersecurity field to grow stronger, together, as a collective. We have learned from experience while designing Uptane and The Update Framework that all the stakeholders of a given industry need to work together in an open consortium to build a compromise-resilient framework for securing software updates. We feel that this will be just as crucial for devices in the IoT sphere as well. Unless there is open communication between industry leaders and security experts, we cannot devise a solution that can provide practical implementation and deployment of the compromise-resilience software update framework for IoT devices like the one we recommend.

Secure Systems Lab believes through engaging in open source design and development we can remove economic barriers and promote the open and free exchange of ideas. The best inventions are always a result of open discussion and a free exchange of thoughts and ideas. For this reason, the Secure Systems Lab encourages the development of an open-source platform on which an effective and deployable solution can evolve. The

open-source nature of the project would break down barriers to stakeholder participation, and by making any resulting products royalty-free will ensure we bring the best minds to bear on this problem, regardless of their ability to make an economic commitment. This would, in turn, promote participation from more stakeholders across the board.

CONCLUSION

The NTIA RFC aptly recognizes the need to secure and address "automated and distributed threats to the digital ecosystem"[18] especially security concerns in the "new generation of connected devices (so called Internet of Things (IoT) devices)."[18] NTIA has very accurately called out the gravity of the security threat posed by the potential conversion of these IoT devices to bots. Botnets have been known to be be powerfully disruptive, as was illustrated by the recent Mirai Attacks. To ensure the security of tomorrow's smart devices on the IoT, Secure Systems Lab sincerely hopes that NTIA will give serious consideration to our recommendations in this response to the agency's RFC "Promoting Stakeholder Action Against Botnets and Other Automated Threats."[18] The potential of IoT devices truly excite us. IoT devices have revolutionized industries from small appliance manufacturers to producers of complex medical tools, and its influence will likely be felt in more a diverse array of new products and services in the coming years. They also have changed the way we live in very positive ways through, for example, devices that collect data about their health and promote a more active way of life. Applications of IoT devices to individual's personal lives and industries are just two of the many

[18] Dep't of Commerce, National Telecommunications and Information Administration, "Promoting Stakeholder Action Against Botnets and Other Automated Threats" (June 13, 2017) at 27042, *available* at https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

spheres that IoT devices hold the potential to revolutionize. We are aggressively researching ways to address the current cyber threat to IoT devices and, with input from NTIA, other Federal agencies, and stakeholders from industry, academia, and the open source community, we hope to be successful in securing the next generation of technology.

Respectfully submitted,

SECURE SYSTEMS LABORATORY
NYU Tandon School of Engineering
Brooklyn, New York

Dated: July 6th, 2017