The United States Naval Academy
Annapolis, Maryland

A Policy Proposal on the Security of Networked Consumer Appliances

prepared by
MIDN Kevin Doran, Zane Markel, & William Young

November 8th, 2014

Introduction to The Internet of Things

Moore's law represents an excellent model for visualizing the rapid growth in technology. It postulates that the computing power of systems will experience exponential year-over-year growth. Concurrent with this explosion in processing ability is the unprecedented reduction in price of computing hardware elements, allowing the complexity of embedded systems to grow with similar rapidity. Today, consumer appliances like lights, toasters and refrigerators have joined the ever-growing list of networked, computer-controlled household systems. We call this technological integration in consumer products the "Internet of Things."

With this connectivity comes an unparalleled security vulnerability—the ability for malicious entities to remotely control consumers' products—and its associated threats. Up to this point as a society, we have resolutely affirmed a preference for connectivity over security; it represents a new frontier to settle, a final bastion of freedom in a world afflicted with an insatiable push towards constant surveillance. Unbeknownst to many at its inception, that freedom is being deliberately attacked by unknown criminal entities seeking to take advantage of American citizens and exploit what were once considered to be the most dependable products in one's home. Only by paying a ransom fee are innocent people able to regain control of their own appliances, a premise that is at once both repulsive and wholly unacceptable.

Proposed Course of Action

To confront and halt the current attacks, particularly the ransomware infecting refrigerators across America, the US government must plan and execute “Operation Ripe Food”, a collaborative international law enforcement effort tasked with investigating the identities of the criminal group responsible for infecting the refrigerators with ransomware. Additionally, this group will work with the refrigerator manufacturer to quickly develop a patch to prevent to render the ransomware ineffective against uninfected refrigerators, and the group will also publicize clear instructions informing the public how to remove the ransomware from any currently infected refrigerators. If the investigators discover that the criminal group is responsible for any of other attacks on networked devices, they will similarly develop a patch for uninfected devices and instructions for the public on how to clean infected devices. To avoid alerting the criminals and to avoid worrying U.S. citizens unnecessarily, this operation will be kept secret from the public until the is operation is complete.

To help prevent future attacks on Internet of Things devices, the Department of Homeland Security (DHS) will establish an independent Committee on Consumer Internet Security (CCIS), a temporary committee aimed at researching and developing a standard metric for assessing the security of consumer Internet of Things devices, called the GoldTrident Security Rating (GTSR). This committee will be composed of a

mixture of technology sector experts, business veterans, and select members of government security agencies.

The GoldTrident Security Rating will measure how well a networked device conforms to a set of security standards. Example standards might include using robust encryption in any communication protocols or checks for invulnerability to common attack vectors. Organizations will voluntarily submit their products for GTSR testing; each tested product will earn a rating from a discrete scale ranging from no security to maximum security. A maximum GTSR rating is not meant to guarantee complete security; rather, it guarantees adherence to well established security measures.

After establishing the GoldTrident Security Rating, the CCIS board and funding system will be used to create the permanent Consumer Product Security Administration (CPSA), which will have the dual purpose of periodically reassessing the GTSR and testing consumer products to evaluate their GoldTrident ratings. Over several years, the DHS will gradually decrease CPSA funding. Eventually, the CPSA will become an independent nonprofit organization.

Past Precedent

Operation Ripe Food will be based on Operation Tovar[1], an international law enforcement operation which pooled investigators from the FBI, Europol, UK's National Crime Agency, Crowdstrike, Dell, SecureWorks, Symantec, Trend Micro, and

[1] Krebs, Brian. "'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge," Krebs on Security RSS, June 2, 2014, accessed November 9, 2014.

McAfee to investigate CryptoLocker[2] and the ZeuS Botnet. CryptoLocker was piece of ransomware which encrypted computers and locked their users out until they paid for a key to unlock it. Operation Tovar uncovered and seized the Gameover ZeuS botnet, which was responsible for propagating and controlling CryptoLocker. At its height, Gameover ZeuS had infected between 500,000 and 1 million computers worldwide. The similarity of CryptoLocker to the current ransomware infecting refrigerators, combined with the success of Operation Tovar, indicates that Operation Ripe Food has a high chance of success.

The GoldTrident Security Rating has many parallels to Energy Star, an international standard for energy efficiency in consumer products. Energy Star, originally developed by the EPA, is a voluntary program in which businesses can have their products earn the Energy Star label for meeting certain energy efficiency standards[3]. Like an Energy Star label, a GoldTrident Security Rating on a product shows that the product has been rigorously tested for desirable features that are difficult for consumers to gauge on their own. Also like the Energy Star program, businesses will voluntarily submit products to the CPSA in hopes of having them earn a marketable credential; no regulation will force them to participate. Energy Star has accumulated 18,000 partners from all sectors of the economy and is estimated to have reduced 1,903 million metric tons of greenhouse gas emissions since 1992[4]. In a few decades, the CPSA could make a similar impact on security in networked devices.

---

[2] Cannell, Joshua. "Cryptolocker Ransomware: What You Need To Know," Malwarebytes Unpacked, October 8, 2013, accessed November 8, 2014.
[3] "About Energy Star," Energy Star, accessed November 8, 2014, http://www.energystar.gov/about.
[4] Ibid.

The National Highway Traffic Safety Administration is a government Executive Branch agency responsible for car safety ratings[5]. Largely a response to the poor safety standards of automobiles in the 1960's, the NHTSA has been instrumental in decreasing highway motor vehicle fatalities.[6] Today, the public trusts the NHTSA for auto safety information and their safety ratings when purchasing vehicles. Like the NHTSA, the CPSA will largely be a reaction to the recent Internet of Things attacks but could become a trusted organization for Internet of Things safety information. Ultimately, the public may come to rely on the GTSR for purchasing Internet of Things products.

Consideration of Stakeholders

As with any policy and its associated implementation, consideration of stakeholders is crucial in comprehending both the roles and responsibilities of the parties involved as well as any penalties stemming from noncompliance. The consumer is undeniably the largest stakeholder in increased product networking security—after all, the purpose of establishing the CCIS/CSPA is centered around the protection of appliance reliability for and personally identifiable information of millions of US citizens.

Our proposal seeks to ensure, above all else, safety of mind throughout operation of consumer products. Private corporations, themselves legal entities,

[5] "About NHTSA," National Highway Traffic Safety Administration, accessed 8 November, 2014.
[6] "America's Experience with Seat Belt and Child Seat Use," Presidential Initiative for Increasing Seat Belt Use Nationwide -- America's Experience with Seat Belt, accessed November 8, 2014.

extend and enhance this safety of mind and constitute the party responsible for complying with federal standards and striving to build the better, safer products that consumers expect. Our proposal's joint private-public organizations (CCIS/CSPA) complement the ethical responsibilities shouldered by corporations with legal responsibilities designed to ensure that the baseline for product security is met. The government's primary role—in fact, its only role—in administering CCIS/CSPA is to provide the legal momentum necessary for establishing new organizations and the social and political momentum necessary for attracting capable partners from all across the technology industry at large. This supplemental momentum will be sufficient to build the foundation of a strong, jointly-operated safety administration not much unlike the NHTSA in its scope and public support.

Noncompliance will not require any action on behalf of the government in this particular scenario. Corporations electing to produce insecure products that fail to meet minimum standards for any class of security certification will ultimately face trial before consumers. Just as unsafe cars are for the most part avoided by conscientious consumers, so too will unsafe appliances be ignored.

Implementation

First, the FBI will contact the other organizations involved in Operation Tovar in order to seek their assistance in Operation Ripe Food. The investigators who collaborated together in Operation Tovar did so expeditiously and successfully and

managed to develop strong group cohesion by the end of the operation. To acquire added experience and capability, the FBI would liaise with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in order to leverage existing industry relationships and gain access to the CCDCOE's highly reputable Computer Emergency Response Teams. Such a partnership would substantially bolster the probing depth of the investigation.

Immediately upon approval, a Committee on Consumer Internet Security (CCIS), a temporary, government-backed research branch, will be established. CCIS will be tasked with arranging a meeting with the chief technology officers, chief information security officers, and other high-ranking officials of major consumer appliance manufacturing and security firms within six months of establishment. From this pool of technology power figures, the committee members shall be chosen, resulting in a healthy mix of technology sector veterans, business experts, and members from select security organizations. Within eighteen months of this meeting, CCIS is expected to have fully researched and developed a uniform scale for assessing the security of networked consumer products—the GoldTrident Security Rating. After the scale is implemented, the CCIS shall exist for an additional twelve months to oversee adjustments and monitor initial feedback from the public.

Exactly three years after the CCIS is established, its responsibilities will shift to the Consumer Product Security Administration (CPSA). CPSA shall retain the board from CCIS but may exercise the power to appoint new members as it sees fit. CPSA will primarily be tasked with maintaining and periodically reassessing the product

safety scale set forth by CCIS, and will report directly to the Department of Homeland Security (DHS) for its first three years of existence. At that point, and for the next two years, CPSA will act as an independent entity and will no longer report to the DHS, instead releasing quarterly reports directly to the public on the state of product security. 6, 12, 36, and 60-month targets will be identified for the release of reviews on the implementation and success of the networked product rating system.

In addition to periodically reassessing the GoldTrident Security Rating and reporting on product security, the CPSA will administer GTSR product tests. Organizations developing consumer networked devices will voluntarily submit their products to the CPSA, which will run each product through a rigorous stress test. Each applicable GTSR security standard will be assessed, and the results will be used in a transparent, objective procedure to produce a GoldTrident Security Rating for each product. Organizations are then free to market their product with its security rating. In order to promote initial adoption, the DHS will initially fund all CPSA tests. As the CPSA transitions into a self-sufficient entity, it will need to charge organizations minor administrative fees for product testing.

Budget

Our proposal cannot be implemented without first developing a sound budget that can be reasonably afforded by all funding parties. As with any law enforcement operation, the expenses of Operation Ripe Food will be covered by the employers of

the investigators collaborating on the operation. While the private corporations supporting the investigation do not have a budget for law enforcement directly outlined, they all have salaried forensics investigators. These corporations will treat Operation Ripe Food as it is: a high-priority computer forensics investigation. Through this plan, Operation Ripe Food will be implemented without any additional cost to taxpayers or consumers.

CCIS will require an initial government investment, but the administration will become self-sufficient as it transitions into a nongovernmental organization. Initially, the Department of Homeland Security will provide 75% of the budget for CCIS. The additional 25% will be provided by the private sector corporations in technology and consumer product markets hoping to demonstrate a commitment to improve product security. Over the next three years, the DHS will aim to gradually decrease its funding until the private sector supports 50% of its operations.

When the CCIS transitions into the CPSA, it will begin charging corporations to have their products tested for a GoldTrident Security Rating. As this revenue stream grows, the CPSA will wean itself from DHS funding. Eventually, GTSR testing will become the primary revenue source for the Consumer Product Safety Administration, at which point it can transition into an independent nonprofit security testing organization.

Incentives

Consumers are willing to pay for security; the American people want to feel safe. This reality is evident in the consumer market. One has to look no further than the automobile industry and the rapid implementation of seatbelts and airbags to discover a relevant example. Apple has also recognized the value consumers place on security. One of the primary features of its recently released iOS 8 is its comprehensive encryption scheme[7]. This feature contributes to Apple's ability to sell its products at a premium over its primary competitors. Indeed, shortly after Apple announced the encryption scheme in iOS 8, Google responded with an announcement that Android devices would soon enable similar comprehensive encryption by default[8]. The interplay between price and security is not much unlike that between price and value. Thus, we must make an important distinction; namely, when perceived security is on the line, consumers are willing to pay higher prices for otherwise equivalent products.

Our organization and nonprofit board CPSA is designed to research, maintain, and update the product market security standard that is set for the industry. Products that fail to meet the minimum security standards set by the board will not earn a seal of approval and will be awarded a delinquent rating. As one would expect, reasonably knowledgeable consumers will not invest their money in substandard products. Most

[7] Farivar, Cyrus. "Apple expands data encryption under iOS 8, making handover to cops moot," Ars Technica, September 18, 2014, accessed November 8, 2014.
[8] Hern, Alex. "Apple defied FBI and offers encryption by default on new operating system," The Guardian, October 17, 2014, accessed November 8, 2014.

importantly, consumers who lack technological savvy will follow the exact same course of action—numerical ratings and "seals of approval" are extraordinarily powerful tools of suggestion, wielding the power to influence and persuade. It is unnecessary, then, to incentivize consumer purchases much beyond the GTSR. Companies that ignore the GTSR will lose the revenue that security-conscious consumers once contributed and will eventually lose the public's trust.

Our goal is to effect a "tipping point" for consumer product security in the sphere of public awareness. As soon as one product is known to be more secure, the market will be naturally driven in this direction; likewise, insecure products will drive away most potential consumers. The baseline for security is going to be continually reset at a higher mark as companies compete to raise the average security standard in consumer appliances. Competition such as this will further incentivize organizations to test and improve their product lines to avoid irrelevance and maintain a desirable inventory turnover.

In the end, we envision the inception of a self-perpetuating, cyclical push towards improved security wherein the government can sit back and do little once it has started the proverbial fire. The key incentivizing component is undoubtedly support from corporations in establishing the CCIS and CSPA—without the cooperation of the technology industry and the immense public support that it commands, persuading producers of networked consumer appliances to intentionally reduce profit-margins in the short term to effect greater security and sales in the long term is a difficult case to argue.

Results

In the short term, Operation Ripe Food will develop and publish instructions to allow consumers to unlock their compromised refrigerators. Through collaboration with international computer emergency response units, the investigators will ideally uncover the criminal group (or groups) responsible for the attack with haste and forward their collected evidence as a detailed report to all appropriate law enforcement organizations. (The exact process of assessing jurisdiction falls outside the scope of this implementation and shall instead be studied by collaborating factions.) Several years later, the Committee on Consumer Internet Security will publish a report specifying the GoldTrident Security Rating, a metric designed to help consumers determine the security of networked appliances available in the marketplace relative to an established standard. Following this, the Consumer Product Safety Administration will begin accepting consumer products from producers for security evaluations and white-hat penetration testing.

Ideally, by the three year mark, the CPSA will have a significant public following with a clear dataset demonstrating a marked increase in product security and consumer confidence. Ultimately, the GoldTrident Security Rating could become the primary standard used by consumers to make sound security decisions in their networked product investments. After ten years, given that CPSA has operated successfully in accordance with the implementation and spirit of this policy proposal,

the public will possess a renewed trust in networked consumer products—a trust that enables individual consumers to feel safe and protected with the products in their own homes and businesses, immune to the destructive forces residing silently and replete with ill-intent on the world wide web.