

Is Your Milk Safe?
Policy for a New Era of Cyber Crime

Xisen Tian, Naadia Puri, Nicolas Shyne



United States Naval Academy

Table of Contents

1. INTRODUCTION	3
2. PAST PRECEDENCE	3
3. IMPLEMENTATION	5
4. BASIC BUDGET	8
5. CONSIDERATION OF ALL STAKEHOLDERS	9
6. INCENTIVES	10
7. RESULTS	10
8. CONCLUSION	12
9. WORKS CITED	13

INTRODUCTION

The so-called *Internet of Things (IOT)* phenomenon is revolutionizing society with ‘smart devices’ that are interconnected, implement sophisticated algorithms and, most importantly, have network capability. From this, a new era of cyber crime has been born. The hijacking of household smart devices, holding devices for ransom, and theft of private data is rampant throughout the IOT. Hackers take advantage of the loose security measures implemented in household devices to gain access to them. Before the IOT matures much more, we must act to increase public awareness of the risks, increase the resilience of the IOT to withstand the inevitable increase in malicious exploitation, and create attendant policy to ensure and protect the public interest in mitigating the security issues with the IOT.

PAST PRECEDENCE

Although the crimes associated with the IOT phenomenon are new, the underlying issue of rapid release of unsafe products by manufacturers is not. Similar to the automobile boom of the early 20th century, the allure of ease of use and intelligence in household devices has seduced the public into purchasing products while being ignorant to the product’s safety issues. In the long history of automobile-safety standards, many people died in car accidents before there was sufficient attention given to correct the problem, most notably through Congressional investigations that ultimately forced big companies such as General Motors and Ford to enact changes to their automobile design.¹²

The government regulating safety in consumer products is not a new issue. While banking structures and automotive recalls may not seem to coincide with the current cyber threat, there is more to them than meets the eye. Earlier this year when General Motors recalled over eight million cars, they

¹ "History of Car Safety - Automotive Safety Evolution - Road ..." 2013. 9 Nov. 2014
<http://www.roadandtrack.com/the_road_ahead/The-Road-Ahead-Road-Evolution-Of-Safety>

² "Senate passes landmark auto safety bill - History Channel." 2010. 9 Nov. 2014
<<http://www.history.com/this-day-in-history/senate-passes-landmark-auto-safety-bill>>

were fined by the government for endangering the general public. In effect, the government is saying that the producer is not off the hook if the consumer does not do enough research on the project; he onus lies on General Motors if they build a faulty product. In the same way, if a toaster is causing kitchen fires, or a refrigerator is locking out its owners because of a faulty design and security protocol, the responsibility lies with the manufacturer of the product. Countless documents, among them the Software Engineering Code of Ethics and ACM Code of Ethics, stress that software developers must release a product that is perfect as far as their abilities can bring perfection.³⁴⁵ But accountability is not always self enforced, and an important role of the government is to balance public and private interests, in this case those of private corporations. Fines can and should be levied against companies that create faulty products that endanger the public, and immediate recall of all affected products is a reasonable consequence. The recent Bank of America fine also stresses that companies are responsible for creating and distributing goods that do not harm those that buy them. Additionally, it is recommended that a new standard of ethics be written up for the sake of all those who will choose IOT device development as their career field in the future.⁶ All of this idealism, however, is easier said than done.

So how can both consumers and manufacturers be convinced to get on board with our movement? There is precedent in this matter as well, and it is often found in a mix of both incentives and the imposition of liability. Most people are familiar with the *USDA Organic sticker*, which means that a product has addressed all the criteria that the USDA classifies as Organic, and with the *EnergyStar sticker* that states that the EPA has found a particular item environmentally sound.⁷⁸ The

³ Anderson, Ronald E et al. "Using the new ACM code of ethics in decision making." *Communications of the ACM* 36.2 (1993): 98-107.

⁴ "ACM Code of Ethics - Association for Computing Machinery." 2007. 9 Nov. 2014 <<http://www.acm.org/about/code-of-ethics>>

⁵ "Software Engineering Code of Ethics and Professional ..." 2007. 9 Nov. 2014 <<http://www.acm.org/about/se-code>>

⁶ "Bank of America To Pay Record \$16.65 Billion Fine | TIME." 2014. 9 Nov. 2014 <<http://time.com/3153262/bank-of-america-record-16-billion-fine-mortgages-subprime-loans/>>

⁷ "ENERGY STAR." 9 Nov. 2014 <<http://www.energystar.gov/>>

⁸ "Organic Agriculture | USDA." 2013. 9 Nov. 2014 <<http://www.usda.gov/organic-agriculture.html>>

government incentivizes the private sector to follow these protocols through generous tax breaks to companies that reach the benchmarks, subsidies, and guidelines to make sure the company can implement the programs, and significant public relations work to get the meaning of the sticker out to the general public. We propose that our “CyberShield” sticker have a set of criteria, based on laws and regulations passed by the US Consumer Product Safety Commission, that a IOT Quality Control Agency will grade products on. By increasing media attention on the “CyberShield” program, we will be able to reassure consumers have a product that is as safe as conventional technology can make it. However, we will also need to explain to the public that “CyberShield” does not mean that the system is completely foolproof. We will have to remind the public that they will still need to constantly monitor for updates and update their systems with patches as fixes are released; otherwise, the onus of responsibility may fall on them. Additionally, we will have to work to ensure that patches are not on fixed time increments, but rather dependent on the security needed by the user. Zero-day exploits are often so successful because the patch to fix them will not be released until a significant time later, when they should instead be based on the time in which the exploit happens.

IMPLEMENTATION

Consistent with the White House’s *2013 Presidential Policy Directive-21* that called for the creation of cyber standards, our proposal is to create a government subsidized committee called the IOT Regulatory Committee that will enforce security standards on smart appliances and gives them ratings based on a set of well documented publicly transparent security standards. We will work with the U.S. Department of Commerce, U.S. Consumer Product Safety Commission (CPSC), and the Department of Homeland Security to set up this committee.

The IOT Regulatory Committee will work with the National Institute of Standards Technology (NIST) whose mission is to “promote U.S. innovation and industrial competitiveness by advancing

measurement science, standards, and technology in ways that enhance economic security and improve our quality of life”.⁹ In February 2013, NIST released a document, “*Framework for Improving Critical Infrastructure Cybersecurity*”, that sets guidelines and consists of practices to promote protection of critical infrastructure of products.¹⁰ NIST will assist our IOT Regulatory Committee in addressing civil liberties and privacy concerns. NIST will help consult us on drafting baseline technical standards that all IOT devices will need to comply with.

We also need to collaborate the Department of Homeland Security and in particular a branch of the National Cybersecurity and Communications Integration Center(NCIS), that focuses on reducing cyber threats and vulnerabilities, publicizing cyber warnings, and responding to cyber incidents. We will utilize their publications in our media campaign for public awareness of cyber security in IOT.

There should be consequences for those who do not implement the safety standards for the IOT. To enforce this, measures will need to be taken with the CPSC. Specifically, we will need to propose or append to existing laws and statutes for devices in this new era of IOT. For example we would need to append sections on software and hardware fail safe measures in the Refrigerator Safety Act which requires refrigerators to have a mechanism (usually a magnetic latch) that enables the refrigerator door to be opened from the inside in the event of accidental entrapment. New laws would need to outline exactly what kinds of security standards apply to the device and enforcement policies for each degree and type of violation of standards. Before these laws can be proposed, our committee will list and categorize IOT products that could injure or kill consumers if left unchecked.

The IOT Regulatory Committee will provide a testimony for the superior security measures enforced by a company’s product which will in turn provide consumer confidence in their purchases. The goal is to motivate companies to be active in implementing security measures during the design

⁹ "National Institute of Standards and Technology." 9 Nov. 2014 <<http://www.nist.gov/>>

¹⁰ National Institute of Standards and Technology (NIST), and United States of America. "Framework for Improving Critical Infrastructure Cybersecurity." (2014).

phase of their smart products. The committee will conduct inspections and consumer-satisfaction surveys to award security-proactive companies. These measures will require contacts in the higher level of government to comply. Specifically, the Secretary of Commerce will need to deal with the potential impacts on American business. We will need the Attorney General's counsel for possible legal actions against noncompliant companies as well as Congressional leadership both in the House and the Senate.

Our vision is that before companies distribute their products, they should pass an inspection process that complies with our standards on cyber security which would be in line with the regulations of the CPSC. If everything meets the safety standards, then the products will be approved and stamped with our seal of approval called "CyberShield". Just as public health demands that children be vaccinated, therefore creating a herd immunity benefiting the collective, this agency functions that same way. Attaining our stamp is similar to the EnergyStar marketing tactic. The CyberShield stamp furnishes the benefit of improved quality, durability and performance. The stamp will give consumers the satisfaction that their money is well spent. Also, the stamp will force the hand of reluctant manufacturers and retailers to make the necessary security investments in their products which customers deserve. Thus, the sticker will be both a part of cybersecurity public-awareness campaign and gives consumers peace of mind.

As mentioned before, a foreseeable roadblock in implementation may be that major American manufacturing companies such as General Electric, Johnson and Johnson or Maytag may not want to comply. Marketing the importance of this sticker may also be difficult to implement since we would need a dedicated team of public relations specialists and admen. However, the likelihood of success is still high enough to move forward. With the dramatic increase in public awareness of the threats posed by cyber hackers, we believe many companies will want to get their appliances approved to provide customer satisfaction and increase demand. This kind of movement will serve to increase public

awareness of what can and should be done to address these threats, improve competition in the market for security services, and create more jobs. Marketing may be a persisting process, but in the end it portrays the relevance of product safety leaving consumers cautious and wary.

Another point of interest is that there is still debate as to whether software is considered a good or a service. The Uniform Commercial Code (UCC) allows liabilities to be paid back for goods, but consider services to be of public benefit and so beyond the scope of recrimination. In order to allow damages to be paid back there would have to be a committee ruling stating that software is a good that a consumer pays for. In order to bring a successful suit to bear, a possible plaintiff would have to prove misrepresentation of the software's capability, negligence on the part of the designers, and possible malpractice in terms of malicious intent. The main difference a court would look for in the service-or-good debate is whether a software is something a company releases for the intent of improving the life of the general public, or whether the software is just as good as an application bought in an online store.

BASIC BUDGET

The U.S. government subsidizes many sectors of business vital to the economy and to our national well-being. The New York Times states that 80.4 billion dollars are distributed to 1,874 companies every year.¹¹ Of those, 48 companies have received more than 100 million in state grants since 2007. The Department of Commerce provides funding of 70 million annually to the *Technology Innovation Program(TIP)*, which promotes innovation through research in the U.S.¹² With the rising concern and importance of cybersecurity playing a role on the welfare of our nation, our policy plans to be government subsidized as well. But more importantly, to a greater degree, our plan will rely on the

¹¹ "Explore Government Subsidies - The New York Times." 2012. 9 Nov. 2014
<<http://www.nytimes.com/interactive/2012/12/01/us/government-incentives.html>>

¹² "Technology Innovation Program, Home." 2008. 9 Nov. 2014 <<http://www.nist.gov/tip/>>

creation of a market for security services that benefits all sides. The consumer will benefit from improved awareness of security and the ability to select products based on security features as much as the primary attributes of the “thing” in question. Vendors will benefit from the creation of a market for security attributes and the buy-down of their liability for security vulnerabilities that would otherwise remain in their products. And ultimately the government, in fostering this arrangement, will better serve the public interest.

CONSIDERATION OF ALL STAKEHOLDERS

End users play the biggest roles as they are the ones most affected by this era of cyber crime, and need to accept that they have a duty to their families to purchase security for their IOT devices. Manufacturers and distributors hold the responsibility of making sure their employees are installing updates and repairing defects. Manufacturers must stop the habit of prematurely releasing software containing bugs that will need patching later. We propose that this problem be solved from a bottom-up approach in which employees are held accountable to the Software Engineering Code of Ethics and Professional Practice. The code of ethics stipulates that it is the duty of the designer to create safe and effective software and that they have a duty to both the public and their employers to thoroughly test and spell out the limitations of the products. If employees or contractors violate the code of ethics, the employer should be mandated to enforce disciplinary actions up to the termination of the employee or cancellation of the agreement/contract. The IOT Regulatory Committee will also have a subcommittee to work with US-CERT to investigate violations of the code of ethics.

INCENTIVES

By establishing incentives, we will encourage companies and consumers to use this policy as an enhancement mechanism for their products. The following are incentives we will create:

- Providing cash rebates and tax free incentives to customers who buy stamped merchandise.
- Advertising products with our stamp, motivating manufactures to comply
- Awarding manufacturers based on customer satisfaction and standards met
- Holding complimentary informational conferences in major cities

RESULTS

Our short term goals address the immediate threat of existing vulnerable smart devices. The solution to this problem is not simple and in fact is procedural. The first step is to put a halt to the distribution of the smart devices that have been reported to be vulnerable. Next, we must quarantine the products for analysis. For all we know the information that the cyber terrorists have could lead to them getting even more information. There is no way to reverse what the cyber terrorists have done, but quarantining the systems down prevents any further loss of information.

In addressing the bottom up approach of holding employees and manufactures accountable for designing secure devices we'll first see how well designers and engineers follow the aforementioned existing standards. After seeing which clauses are effective in the different codes, we'll draft a code of ethics tailored to the IOT. It will still be based on established codes of ethics in software design and computer design in terms responsibilities of designers to the public and their employer. However, our code of ethics will address the importance of testing cohesion and coupling of software and hardware security in IOT devices and stress the responsibility of manufacturers to hold themselves accountable for testing and maintaining their products. Ours will stress constant monitoring and research of vulnerabilities during the maintenance phases of a product's lifespan.

For long term goals our committee will work on establishing IOT standards that address Principles of Secure Design used in Industry.¹³ We will use the following basic standards:

¹³ "Design Principles | Build Security In." 2013. 9 Nov. 2014
<<https://buildsecurityin.us-cert.gov/articles/knowledge/principles/design-principles>>

- Product Capabilities Full Disclosure: Consumers should be made aware of all of their product's capabilities and the type of information it collects before purchasing it.
- Fail Securely: Compromised devices must either shutdown or reset themselves so that they cannot be further compromised. For example, a “dumb-switch” that shuts down network capabilities software components to reduce the smart device to its conventional counterpart.
- Firewalls: Devices that have network access must have firewalls to filter traffic.
- Least Privileged Principle: Limit access to network resources and devices so that smart devices don't have excessive access to a home network.
- Logging capability: Devices must be able to log their activity and have Intrusion Detection/Prevention Software tuned to their logs.
- Attestation Measures: System must not lie about their current state
 1. Trusted Platform Module (TPM) implementation in devices that deal with sensitive data and log devices¹⁴

Consumer education is another focus. Consumers must be made aware of the security features of products they might buy and be given some means to choose amongst them, Education plays a key role in the movement to secure the IOT and serves as a long term solution. The Mandiant Report exposes information that can be useful for security. They warn how organizations can protect themselves from attacks. Therefore reporting crimes, like in the Mandiant Report, is a viable way to inform the public on taking certain precautions in purchasing products. Data compromised by hackers, computer viruses, or other incidents can affect our lives in ways that range from inconvenient to life-threatening. That is why prevention is key. However, prevention begins with education. Our proposed program will focus on creating ad campaigns for popular radio stations, television channels, and newspapers. Ubiquitous popular social media sites such as Facebook, Twitter, Youtube, and

¹⁴ "Windows Trusted Platform Module Management Step-by ..." 2010. 9 Nov. 2014
<[http://technet.microsoft.com/en-us/library/cc749022\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc749022(v=ws.10).aspx)>

LinkedIn will help get the word out, expand the audience, share content easier, and serve as an efficient way to communicate. This raises public awareness, helping Americans in properly safeguarding their products.

CONCLUSION

Through establishing a standards enforcement committee, we will ensure product safety mechanisms by awarding good manufactures and penalizing manufactures responsible for unsafe smart devices. In these uncertain times, where it seems not even our homes are under our own control, we must do what we can to end the immediate threat and protect generations to come. Just as our adversaries will constantly be developing their tools, their threats, and their methods for threatening our livelihood, we too must constantly be developing our defenses to ensure that we can meet the threats of the new century. The enemy is new, and with novelty comes fear in the inability to understand. But through discipline and the promotion of innovation, these policies will ensure that those who wish to harm us have something to fear as well.

WORKS CITED

- "ACM Code of Ethics - Association for Computing Machinery." 2007. 9 Nov. 2014
<<http://www.acm.org/about/code-of-ethics>>
- Anderson, Ronald E et al. "Using the new ACM code of ethics in decision making." *Communications of the ACM* 36.2 (1993): 98-107.
- "Bank of America To Pay Record \$16.65 Billion Fine | TIME." 2014. 9 Nov. 2014
<<http://time.com/3153262/bank-of-america-record-16-billion-fine-mortgages-subprime-loans/>>
- "Design Principles | Build Security In." 2013. 9 Nov. 2014
<<https://buildsecurityin.us-cert.gov/articles/knowledge/principles/design-principles>>
- "Energy Star". 9 Nov. 2014 <<http://www.energystar.gov/>>
- "Explore Government Subsidies - The New York Times." 2012. 9 Nov. 2014
<<http://www.nytimes.com/interactive/2012/12/01/us/government-incentives.html>>
- "History of Car Safety - Automotive Safety Evolution - Road ..." 2013. 9 Nov. 2014
<http://www.roadandtrack.com/the_road_ahead/The-Road-Ahead-Road-Evolution-Of-Safety>
- "National Institute of Standards and Technology." 9 Nov. 2014 <<http://www.nist.gov/>>
- National Institute of Standards and Technology (NIST), and United States of America. "Framework for Improving Critical Infrastructure Cybersecurity." (2014).
- "Organic Agriculture | USDA." 2013. 9 Nov. 2014 <<http://www.usda.gov/organic-agriculture.html>>
- "Senate passes landmark auto safety bill - History Channel." 2010. 9 Nov. 2014
<<http://www.history.com/this-day-in-history/senate-passes-landmark-auto-safety-bill>>
- "Software Engineering Code of Ethics and Professional ..." 2007. 9 Nov. 2014
<<http://www.acm.org/about/se-code>>
- "Technology Innovation Program, Home." 2008. 9 Nov. 2014 <<http://www.nist.gov/tip/>>
- "Windows Trusted Platform Module Management Step-by ..." 2010. 9 Nov. 2014
<[http://technet.microsoft.com/en-us/library/cc749022\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc749022(v=ws.10).aspx)>