Solving the problem of unsupported IoT devices through legal requirement

Raymond Dee [#1], Amartya Singh [#2], Jeffrey Qiu [#3], Anthony Innamorato [#4]

Abstract

The Internet of Things (IOT) is an emerging technology sector of technology with significant potential benefits as well as costs. A lack of laws and regulations has allowed a market failure where vulnerable, unsupported IoT devices pollute the internet. We propose a regulatory scheme that would address the market failing and potentially improve the current IoT marketplace.

Introduction

The IoT is experiencing dramatic growth in both the number of devices and the types of devices that are being connected to the internet. These devices contain software and the inevitable vulnerabilities that software has. Technical solutions exist to provide vulnerable IoT devices with security updates but market conditions do not incentivize ongoing updates for existing IoT devices leading societal costs and a growing threat to the wellbeing of the internet. The lack of incentives to provide ongoing security updates can be corrected through a legal requirement that device manufacturers have to provide ongoing security support to IoT devices or disable their ability to connect to the internet. An effective implementation of this idea could result in a reduction in cybercrime and protect the internet as the IoT grows.

Background

The majority of software contains defects. Some defects can be exploited (referred to as *vulnerabilities*) allowing an attacker to perform malicious actions like stealing information or taking control of a compromised computer or device. Ongoing product support, in the form of software updates or patches, is essential to fixing these vulnerabilities. Lacking updates, software can become permanently vulnerable, allowing devices to harm their owners as well as society in general.

The Internet of Things (IoT), which refers to internet-connected devices that are not traditional computers such as smart-thermostats, is estimated to have more than 11 billion devices in 2018[1]. The IoT is projected to continue growing with one estimate suggesting that 100+ billion IoT devices could be connected by 2030[2]. While the IoT is expected to bring great benefits to society, it also presents great risks. Large numbers of vulnerable devices can be compromised and used to attack internet infrastructure and major websites as in the case of the Mirai botnet[3]. Vulnerable devices create serious safety and privacy risks[4] such as insulin pumps and pacemakers that can be hacked[5]. Cybercrime globally is estimated to have costs approaching $600 billion[6]. Compromised IoT devices currently contribute to this number and will have a growing impact as the number of IoT devices dramatically increases.

Despite the costs associated with unsupported, vulnerable devices, there is a lack of incentives to address the problem. Four factors contribute to the lack of incentives. First, a large percentage of costs due to compromised IoT devices is borne by third parties like websites that lose revenues or have to pay for additional distributed denial of service (DDoS) protection. Second, device purchasers seldom understand the risks associated with devices and as a result, are not demanding safer devices or extended support for devices. Third, device manufacturers do not directly bear the costs of vulnerable devices and in many cases have no profit incentive to

---

[1]Gartner. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[2] IHS Markit. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

[3] The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[4] Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[5] The Guardian. https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic

[6] McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

patch vulnerable devices that they previously sold. Finally, there is no liability assigned to unsupported or abandoned devices that are causing harm.

Threat Model

Vulnerable IoT devices present several key risks:

- Participation in DDoS attacks with the following costs:
  - Website downtime / lost revenues
  - Lost productivity due to loss of key services like email
  - Attack mitigation costs
  - Stolen electricity and bandwidth on infected device
  - Reduced IoT device functioning
- Infection by Crypto-miner with the following costs:
  - Stolen electricity and bandwidth on infected device
  - Reduced IoT device functioning
- Data theft and the costs associated with:
  - Stolen intellectual property
  - Violated privacy (How much is your data worth? How much would you charge to be spied on?)
  - Other crimes that are facilitated by data theft like identity theft, extorsion, scams, burglary, etc.
- Safety risks due to device malfunctioning
  - Deaths and damages resulting from infected medical, industrial, and military IoT devices
- Infected IoT devices may facilitate other cybercrimes
  - Infected IoT devices may serve as the initial means of network infections
  - Infected IoT devices may facilitate attacker movements through a network

Design (Solution Overview and Rationale)

To improve incentives in the market for IoT devices and reduce costs associated with unsupported, vulnerable devices, there should be a legal or regulatory requirement that IoT device manufacturers provide ongoing product support sufficient to fix known vulnerabilities (also known as security patches) to internet-connected devices for a set amount of time after which they can choose to continue support or disable the device's ability to connect to the internet. Failure to perform these requirements within a reasonable amount of time would result in a per-device fine. Fines would be used to fund cybercrime law enforcement efforts. Device support requirements and potential fines would help correct the factors leading to bad incentives and market failure in the IoT market.

Requiring ongoing security updates for IoT devices would address two causes of market failure; *externalities* and *imperfect information.* Market failures occur when free markets lead to inefficient outcomes. Outcomes are inefficient when society could be made better off by changing the market conditions (rules, taxes, availability of information). Externalities are costs borne by third parties who are not part of a transaction. For example, imagine an IoT camera that costs $40 and never receives security updates after being sold and connected to the internet. It has vulnerabilities that lead to it being infected with malware and becoming part of a botnet. While it continues to function as a camera, it also participates in DDoS attacks on Conservationfund.org causing $10 in damages (website downtime, mitigation costs) per year. The Conservation Fund is the 3rd party because it did not buy or sell the camera. The damages suffered by The Conservation Fund are externalities. Now also imagine that security updates that stop malware can be provided to the IoT camera for $5 per year. In a perfectly free market the IoT camera owner would have no incentive to pay the $5 and prevent $10 in damages to The Conservation Fund, which is inefficient. This is inefficient because $5 in net value could be created by providing security patches for $5 to prevent the $10 in damages. In this example, a market intervention, like requiring security updates for IoT devices, would correct the externality, allow markets to properly function, and make society better off.

Ongoing security updates would also address a second market failure, imperfect information. Imperfect information is the lack of important information that leads to less than ideal decisions and inefficient outcomes. Imagine the same $40 IoT camera that is infected with malware with the option to have security updates that cost $5 per year from the above example. Also imagine that the malware infection will cost the camera owner $10 per year in extra electricity and internet bandwidth per year. In this situation, a well-informed, rational consumer

should purchase the security updates or demand a product that comes with security updates (and pay a higher purchase price up to a point). However, many consumers would not purchase the ongoing security updates due to a lack of important information. Most consumers would not be able to determine the key factors needed to make a good decision like the probability of an unprotected camera getting malware and the costs of the malware to them. How many people would notice that their electric and internet bills went up less than a $1 per month and then be able to connect that small increase to a malware infection in their $40 IoT camera? Not knowing these hidden costs, many consumers would make inefficient decisions. Requiring security updates for internet connected devices would help consumers make better decisions. The price of devices would increase some, but the hidden costs of malware would go down. Prices of IoT devices would not have hidden costs and would better reflect their true costs.

Motor vehicles provide a powerful precedent for using laws and regulation to fix market failures that occur with new technologies like IoT devices. Motor vehicles using public roads are required to meet minimum requirements for both public safety and driver safety[7]. IoT devices using the public internet should meet minimum safety requirements for both public safety and user safety. Manufacturers or importers of vehicles are required to make or import compliant vehicles[8]. Manufacturers or importers of IoT devices should be required to make or import compliant devices. Vehicles have weight limits to prevent damage to public infrastructure[9]. IoT devices should have ongoing security updates to prevent damage to the internet and third-party property. Vehicles are required to have seat belts because imperfect information makes it difficult for consumers to evaluate the costs and benefits of seat belts as a feature[10] IoT devices should have ongoing security updates for the same reason.

Implementation

The proposed solution would require IoT device manufacturers provide ongoing security updates sufficient to fix known vulnerabilities or disable the device's ability to connect to the internet. There are several important issues to address to achieve a working solution.

Key Definitions

- *Manufacturer* refers to the manufacturer or importer of an IoT device. They are considered responsible for both the device hardware and the device software. Provisions the proposed IoT law and regulations would need to clearly assign product liability as has been done with other types of consumer products like children's products[11].
- *Known vulnerabilities* are software vulnerabilities that have been publicly identified and can be found in a commonly used database like the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD).
- *Reasonable amount of time*: Standards for a reasonable amount of time to provide security updates would have to be established but could be based off guidelines related to patching vulnerabilities based on Common Vulnerability Scoring System (CVSS) scores.

Ideally, device manufacturers would sell IoT products that come with automatic, security updates until a certain guaranteed date. Automatic updates are important to ensure that the update occurs and does not place an undue burden on consumers. The guaranteed support date would be prominently displayed on device packaging. After the guaranteed support date, one of several things could happen. The manufacturer could choose to continue supporting the device for free or could sell a security update subscription to device owners. The manufacturer could sell the rights to maintain the device and charge subscription fees to a third-party maintainer. The manufacturer could also determine that it is not profitable to continue supporting the device and would then

---

[7] Motor Vehicle Safety. Title 49, United States Code. Chapter 301

[8] Motor Vehicle Safety. Title 49, United States Code. Chapter 301. Section 30112

[9] Federal Size Regulations for Commercial Motor Vehicles. https://ops.fhwa.dot.gov/freight/publications/size_regs_final_rpt/index.htm#cmv

[10] Motor Vehicle Safety. Title 49, United States Code. Chapter 301. Section 30127

[11] Consumer Product Safety Commission. https://www.cpsc.gov/Business--Manufacturing/Business-Education/Business-Guidance/Retailers-Product-Safety-and-Your-Responsibilities

be required to disable the device's internet connectivity. If the device were an IoT refrigerator, the refrigerator would continue to work, but would no longer be able to connect to the internet. Because consumers would be aware that their devices will possibly lose internet connectivity after a certain date, there would a demand for devices with long support lives. In many cases (like home appliances), there would be a demand for devices that function without internet connectivity. Consumer demand would incentivize manufacturers to make devices with adequate support lives.

To ensure compliance and prevent abandoned IoT devices from polluting the internet and harming consumers, there must be a system of financial incentives. A fine would be imposed on manufacturers who fail to fulfill their obligations to continue supporting devices or disable them. The fine would be based on the number of devices that are being abandoned (not supported and not disabled) would be set to a value that approximates the value of the damage they will do statistically. Levies from the fine would fund efforts to fight cybercrime, such as an FBI cybercrime unit. To ensure that manufactures do not escape financial responsibility through bankruptcy or by locating assets outside of US jurisdiction, they would be required to 1) set aside funds necessary to cover potential per-device fines in an escrow account or 2) purchase insurance that covers potential per-device fines. In the event that a device manufacturer is violating the law, the escrow account would be seized or the insurance policy would be forced to pay out.

The proposed security update requirement would align incentives and work well is a variety of possible scenarios. In the event of manufacturer bankruptcy, if its products or brand are popular, the manufacturer could sell their intellectual property and codebase to another company that would responsibly maintain security updates or if necessary, disable their internet connectivity. If the manufacturer cannot sell their intellectual property and have an escrow account, they would have an incentive to responsibly disable devices to avoid losing the funds deposited in the escrow account. If they purchased an insurance policy, their insurer would have an incentive to sue them for ownership of their codebase so that the insurer could responsibly disable the devices and avoid having to pay the government fine. Insurers would have incentives to research their clients and only insure responsible manufacturers. Insurers would also have incentives to insure importers who import from countries with functioning legal justice systems where contracts can be effectively enforced.

Evaluation

The proposed solution addresses a problem that is only going to get worse as the IoT grows. Laws and regulations requiring internet-connected devices to have ongoing security updates have a strong economic rationale with historical precedents like regulating motor vehicles. We are currently unable to fully quantify the benefits that out solution would provide. To do so, we need to develop a reasonable estimate regarding the possible reduction in future cybercrime that would result from ongoing security updates for IoT devices relative to a future without updates. For estimate costs, we need to quantify the additional costs that would result from companies providing security patches for a longer period of time. Additionally, we would need to estimate the costs associated additional government bureaucracy, enforcement costs, and regulatory administration.

Conclusion

Similar to how the Industrial Revolution had massive benefits but came presented challenges with environmental pollution, the Internet of Things will have significant benefits but also presents challenges with digital pollution in the form of abandoned, vulnerable IoT devices. Technical solutions to these IoT problems exist but we need to adjust the current economic incentives ensure that technical solutions are applied. Fixing the current economic incentives will requiring updating our laws and regulations related to internet-connected devices.

References

1. Gartner. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
2. IHS Markit. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf
3. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
4. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
5. The Guardian. https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic
6. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

7. https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/
8. CNBC. https://www.cnbc.com/2018/03/01/thousands-of-iot-devices-can-be-hacked-to-mine-cryptocurrency-avast.html
9. The Inquirer. https://www.theinquirer.net/inquirer/news/2358141/80-percent-of-iot-devices-are-vulnerable-to-data-theft-says-hp
10. IoT Tech News. https://www.iottechnews.com/news/2018/may/15/research-us-consumers-smart-home-device/
11. Motor Vehicle Safety. Title 49, United States Code. Chapter 301
12. Motor Vehicle Safety. Title 49, United States Code. Chapter 301. Section 30112
13. Federal Size Regulations for Commercial Motor Vehicles. https://ops.fhwa.dot.gov/freight/publications/size_regs_final_rpt/index.htm#cmv
14. Motor Vehicle Safety. Title 49, United States Code. Chapter 301. Section 30127
15. Consumer Product Safety Commission. https://www.cpsc.gov/Business--Manufacturing/Business-Education/Business-Guidance/Retailers-Product-Safety-and-Your-Responsibilities
16. https://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to-build-iot-solution
17. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
18. https://blog.securityevaluators.com/explaining-the-internet-of-things-iot-cybersecurity-improvement-act-of-2017-912954d5c6e9
19. https://www.congress.gov/bill/115th-congress/senate-bill/1691/text
20. https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/software-updates-important/
21. https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/
22. https://www.first.org/cvss/specification-document
23. https://www.first.org/cvss/cvss-based-patch-policy.pdf
24. https://www.hackerone.com/blog/Vulnerability-Disclosure-Policy-Basics-5-Critical-Components
25. https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
26. https://www.iottechnews.com/news/2018/may/15/research-us-consumers-smart-home-device/
27. https://www.theinquirer.net/inquirer/news/2358141/80-percent-of-iot-devices-are-vulnerable-to-data-theft-says-hp
28. https://www.cnbc.com/2018/03/01/thousands-of-iot-devices-can-be-hacked-to-mine-cryptocurrency-avast.html
29. https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/