December 2017 · Jan-Peter Kleinhans

Internet of Insecure Things

Can Security Assessment Cure Market Failures?

Stiftung
Neue
Verantwortung

Think Tank at the intersection of technology and society

Executive Summary

Looking at the Internet of Things, the market consistently fails to produce reasonably secure and trustworthy devices. This is especially true for smart home and consumer devices such as Internet routers, door locks, light bulbs and TVs. Manufacturers seem to have little economic incentive to implement secure software development processes or at least follow Security-by-Design principles. This means that billions of severely insecure IoT devices will continue to proliferate the Internet making it far too easy for criminals to exploit those vulnerable devices. Already today's criminals are using large botnets of hundreds of thousands of compromised IoT devices to attack and temporarily take down websites, company servers and critical Internet infrastructure. These severe attacks in recent years prompted governments around the world to start thinking about how to improve the security of IoT devices.

Regulatory intervention will need to address the two dominant market failures: (1) Currently, manufacturers do not need to provide essential information about the security of a device such as for how long it will receive security updates. This information asymmetry between consumers and manufacturers about the security of a device makes it harder for consumers to be aware of the device's security. (2) Criminals use IoT botnets, large networks of hundreds of thousands of compromised IoT devices, to attack websites, company servers or critical Internet infrastructure – never consumers. Thus the costs that are incurred due to software vulnerabilities are external costs since neither manufacturers nor consumers have to bear them.

This paper analyses both market failures and points out unique characteristics of the IoT that explain why criminals will continue to exploit vulnerable devices. In order to effectively cure the market failure, a combination of different efforts such as consumer labels, extended software liability or mandatory baseline requirements as a barrier to the market will most likely be necessary. Policy makers need to understand that all these regulatory interventions rely at some point on a robust and efficient security assessment ecosystem – an orchestrated effort between standardization and certification bodies, security assessment companies, ministries and market surveillance to ensure that manufacturers follow prescribed security requirements. Yet today's dominant security assessment regimes are relatively static, expensive, time-consuming and focused on pre-market certification. All these aspects make them unfit for the IoT.

To contribute to the current policy debate about IoT security, this paper will discuss central aspects of an efficient and effective security assessment ecosystem for the IoT. The results are based on SNV's research, expert interviews and several workshops. The goal is to inform the policy debate and underscore the importance of a responsive, open and modular security assessment for many other policy initiatives such as software liability, consumer labels and baseline requirements.

Introduction

IT security in the Internet of Things has received a lot of attention in recent years. Policymakers realised that the market consistently fails to produce reasonably secure devices – especially when looking at the Consumer Internet of Things (CIoT). Every week new software vulnerabilities are found in CIoT devices such as digital video recorders, surveillance cameras, Internet routers, connected toys or smart TVs. These vulnerabilities are often easily exploitable and criminals quickly produce malware to create botnets out of hundreds of thousands of CIoT devices.[1] Anyone can then rent these botnets to attack websites, production servers or even critical Internet infrastructure. There have been longer and more severe attacks in recent years necessitating further government regulation to improve the security of CIoT devices. The United States of America, the European Union, Germany and others proposed a variety of regulation: Some favor software liability, while others advocate for voluntary consumer labels to increase transparency or even mandate certain security requirements as a market barrier. Most likely a combination of different policy tools, capacity building and consumer awareness will be necessary to make CIoT devices more secure. Yet an important aspect is often overlooked but highly relevant for many of the abovementioned regulatory tools: IT security assessment.

Current IT security assessment is relatively static, slow, costly and mostly relevant for public procurement and the financial industry. In order to be efficient and effective for the Internet of Things, regulators, manufacturers, standardisation and certification bodies need to reinvent IT security assessment for the 21st century. No matter how thorough and elaborate current assessment schemes might be, if they do not address market dynamics specific to the Internet of Things, they will not improve the current status quo. In order to contribute to the current discussion, this paper will analyse why the market fails to produce reasonably secure CIoT devices and shed light on the incentives criminals have to continue to exploit insecure CIoT devices. This paper will then demonstrate why responsive, open and effective security assessment might be the key in solving the market failure. Lastly, central aspects of what healthy IT security assessment ecosystem looks like are discussed.

[1] Aiko Pras et al. 2016. "DDoS 3.0-How terrorists bring down the internet." International GI/ITG Conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance. https://research.utwente.nl/en/publications/ddos-30-how-terrorists-bring-down-the-internet

Why it is hard to keep a smart device reasonably secure?

The current trend is to make everything "smart" – toaster, fridge, thermostat, lighting. A company that has built household appliances such as vacuum cleaners or washing machines for decades has a lot of experience in mechanical engineering and physical safety. Yet they do not necessarily know much about secure software development processes. In order to make a "secure" version of a smart washing machine, the manufacturer would need to hire IoT security experts and provide its staff of software developers with costly security trainings. It seems safe to assume that many manufacturers do not invest significant resources to implement a secure software development process. This can be inferred simply from the amount of amateurish and easily exploitable software vulnerabilities found in many smart household appliances.[2]

Furthermore, IT security might constitute a paradigm shift for many traditional household companies. It is not enough to ship a "secure" CIoT device. After the device has been developed and sold, it needs constant maintenance through software updates to keep it secure. This means a decade or more of software support for smart fridges or connected washing machines. That is a paradigm shift. Traditional engineering is focused on *physical safety* which for the most part takes place during the product development phase:

> Is the engine powerful enough for the washing machine?
>
> Are all electronic components properly shielded against leaking water?
>
> Does the power cord fulfill the necessary specification?

These are pre-market considerations that most likely do not change after the device has been sold. This is not true for *IT security*. Once a smart device has been sold and is connected to the Internet, it is exposed to constant, ever changing attacks. There are roughly three considerations that manufacturers have to account for regarding software maintenance:

[2] See for example Anthony Rose and Ben Ramsey. "Picking Bluetooth Low Energy Locks from a Quarter Mile Away". Presentation at DEF CON 2016. https://www.defcon.org/html/defcon-24/dc-24-village-talks.html; Antonakakis et al. 2017. "Understanding the Mirai Botnet". https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

1. An *external software library* receives an important security update: In August 2016 OpenSSL 1.1.0 has been released, a widely used software library to encrypt communication on the Internet. By the end of May 2017, the OpenSSL developers team has already released six security updates. If the manufacturer of a CIoT device chose to implement OpenSSL and started selling the product by summer 2016, the device should have received at least 6 firmware updates by May 2017, just to keep pace with the changes in one software library. If the CIoT manufacturer did not update the implemented OpenSSL library of the sold devices, a "secure" device from summer 2016 might very well be considered "broken" by spring 2017.

2. *Software that has been developed in-house* needs to be tested and maintained.

3. An *external software library stops development* and becomes obsolete. Either the manufacturer continues to test the software library in-house and takes over maintenance or he is switching to a different, still actively maintained software library. The latter might result in rewriting several parts of the device's software.

This is just to illustrate that traditional household manufacturers now have to grapple with how to securely develop and *maintain* smart household goods. But none of this happens. The reality is that especially in the CIoT market, there is a severe lack of regular software updates for devices and adequate software testing by manufacturers. The norm is that devices are already shipped with outdated, insecure software and barely see any update during their lifetime. Two central market dynamics can be identified which result in manufacturers building "smart", yet severely insecure household appliances.

Why the market fails to produce reasonably secure devices

There are two key market dynamics that explain why many CIoT manufacturers have little to no economic incentive to produce reasonably secure devices – information asymmetries and external costs. Both can be categorised as types of market failures[3] and have been well understood and researched for decades in other fields, such as environmental regulation. Any type of government intervention or regulation would need to address these market failures to create incentives for companies to invest in secure software development processes. If not, insecure CIoT devices will continue to "pollute" the Internet.

Software quality and information asymmetries

Over the last couple decades an entire ecosystem of institutions and organisations have been created to focus on product testing. Organisations like Consumer Reports (USA) or Stiftung Warentest (Germany) regularly test and benchmark consumer products to identify poorly engineered or even dangerous products. Many magazines and websites also focus on product reviews for smartphones, laptops and smart home devices. If a consumer wants to buy a new smartphone she can easily compare aspects like display resolution, battery life or camera quality between different models thanks to these tests and reviews. Thus manufacturers pay attention to features that are tested since they want to receive favorable reviews. Historically, these tests and reviews focus on features that can be assessed relatively quickly. But to assess the quality of the software and how secure the manufacturer implemented different features is by far not as straightforward. It requires much more expertise and possibly access to both the documentation and the source code of the device's firmware. Furthermore the security of a CIoT device depends also on other aspects such as the frequency of security patches and for how long security updates will be provided. These and similar aspects cannot be tested at a single point in time. Only the manufacturer has this information. Thus right now the consumer has no meaningful way to assess the security of any CIoT-device. This information asymmetry between consumer and manufacturer about the security of a product leads to a vicious cycle:

1. Since neither the manufacturer nor the different tests and reviews say anything reliable or mandatory about the security of a CIoT device, IT security is not (and cannot be) part of the

[3] Jentzsch, Nicola. 2016. "State-of-the-Art of the Economics of Cyber-Security and Privacy". IPACSO - Innovation Framework for ICT Security Deliverable. No. 4.1. https://www.econstor.eu/bitstream/10419/126223/1/Jentzsch_2016_State-Art-Economics.pdf

consumer's purchasing decision process.[4]

2. Thus at the moment IT security is a feature of CIoT devices that no one pays for.

3. Logically during product development the manufacturer will focus mainly on features that have a direct return on investment value.

The market's inability to resolve information asymmetries on its own is nothing new and has been well researched and understood for decades.[5] Increased transparency for the consumer about aspects such as upgradability and software support time might help to break this vicious cycle – this could be achieved through product labels.[6]

Software vulnerabilities as negative externalities

Negative externalities or "external costs" are costs that a third party has to bear because of an economic transaction between two other parties.[7] Air pollution, overfishing or passive smoking are examples of external costs: A company is polluting the air because of the manufacturing of consumer goods. But neither the company nor the consumer have an incentive to bear the costs of air pollution – they are externalized. Yet society as a whole has to bear the costs of polluted air. Negative externalities exist, because the market failed to allocate costs adequately. In the past, this form of market

[4] Ginger Zhe Jin and Andrew Stivers. 2017. "Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics". http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_50.pdf

[5] Ross Anderson and Tyler Moore. 2013. "The Economics of Information Security". http://www.kentlaw.edu/faculty/rwarner/classes/ecommerce/materials/privacy/materials/economics/Anderson,%20Econ%20of%20Info%20security.pdf

[6] Peter Bihr. 2017. "A Trustmark for IoT". ThingsCon Report. https://github.com/openiotstudio/general/raw/master/publications/a_trustmark_for_IoT_thingscon_report.pdf

[7] Jaffe, A.B., Newell, R.G. and Stavins, R.N., 2005. A tale of two market failures: Technology and environmental policy. *Ecological economics*, *54*(2), pp.164-174. https://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/10267/JaffeetalEcolEcon.pdf?sequence=1

failure has often been addressed through government regulation.[8] Looking at the Internet, software vulnerabilities in poorly developed CIoT devices, just like CO_2 emission, might constitute negative externalities. For more than a decade, security researchers point out the similarities and argue that the concept of external costs might help to inform the policy debate.[9] The similarities become especially clear when looking at IoT botnets. An IoT botnet is created through malware that exploits several vulnerabilities of popular IoT devices. Once a device is infected by the malware, it becomes part of the botnet (Robot Network) and scans the Internet for other vulnerable devices. When the criminals "herded" enough devices, the botnet is then used for a variety of purposes. In the case of the Mirai botnet, 600.000 devices were used to attack websites and Internet infrastructure.[10] The important point is that a botnet never turns against "itself": Cheap and insecure CIoT devices are infected, but the attacks are against websites, company servers or even Internet infrastructure. Thus just like environmental pollution the Internet as an ecosystem can be "polluted" by insecure devices. It is estimated that the Mirai botnet was responsible for $110 million in economic damage.[11] Neither the device manufacturers nor the device owners bore any of these costs – but society as a whole did.

Criminals love the Internet of Things

Both of the aforementioned market dynamics, information asymmetries. and external costs might be true for IT security in general – not just the Internet of Things. Yet the Internet of Things has its own unique characteristics that make it worthwhile for criminal hackers to exploit IoT devices for fame or

[8] Mazzucato, M., 2016. From market fixing to market-creating: a new framework for innovation policy. *Industry and Innovation*, *23*(2), pp.140-156. http://www.progressiveeconomy.eu/sites/default/files/Mazzucato%20Market%20Making%20and%20Shaping.pdf

[9] Bauer, J.M. and Van Eeten, M.J., 2009. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), pp.706-719;

Anderson, R. and Moore, T., 2007. Information security economics–and beyond. *Advances in cryptology-crypto 2007*, pp.68-91. https://archive.nyu.edu/bitstream/2451/23353/2/econ_crypto.pdf

[10] Antonakakis et al. 2017. "Understanding the Mirai Botnet". https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[11] https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

financial gain. This section seeks to analyse these characteristics to better inform the policy debate and identify if and how these aspects could be influenced through the right regulatory mechanisms.

Computing power and connectivity

Every year computing power becomes cheaper[12] and more energy efficient.[13] Because of this, even small CIoT devices can now run general purpose operating systems and powerful software. Additionally, connectivity also becomes cheaper: in contrast to smartphones or Laptops, CIoT devices are often constantly connected to the Internet. This provides criminals with more time and opportunity to hack CIoT devices. Once hacked, it furthermore means that the criminals can utilise the exploited CIoT device more reliably compared to laptops or smartphones.

Persistence

If a criminal wants to make money by renting out botnets for different types of attacks or fraud she wants a relatively consistent number of zombies (infected devices) for her botnet. Dropping from 300.000 to 270.000 zombies in one night might not be a problem – losing half of your zombies in an hour is. Persistence, how long a device stays infected after exploitation, is important to criminals. The average CIoT device has several benefits regarding persistence compared to desktop PCs or laptops. One is the lack of usability and convenience regarding software updates: While consumers are accustomed to updating laptops with a click of a button (Microsoft's Patch Tuesday) this is not at all the case for CIoT devices. If those devices have an update mechanism at all, it is often times neither intuitive nor convenient: In order to update an Internet router, the user usually has to manually check the vendor's website, search for the router model, download the updated firmware version, upload it to the router via its own website and then click "Update Firmware". Of course, there are companies who provide fully automatic updates (e.g. AVM FRITZ!Box, Telekom Speedport) but they seem the excepti-

[12] William D. Nordhaus. 2007. "Two Centuries of Productivity Growth in Computing". http://www.econ.yale.edu/~nordhaus/homepage/nordhaus_computers_jeh_2007.pdf

[13] Jonathan Koomey and Samuel Naffziger. 2015. "Moore's Law Might Be Slowing Down, But Not Energy Efficiency". https://spectrum.ieee.org/computing/hardware/moores-law-might-be-slowing-down-but-not-energy-efficiency

on to the rule.[14] Poorly designed or nonexistent update mechanisms make it impossible or at least highly unlikely for vulnerable CIoT devices to ever get updated by the consumer. Another reason why CIoT devices stay infected relatively long is the simple knowledge about a malware infection: Several studies and surveys indicate that companies struggle with long dwell times – the time an attacker can spend unnoticed in a system or network – of 100 days on average.[15] If a company with dedicated IT staff and network administrators needs 100 days to figure out that their systems have been compromised, how long might it take a home user to realise that their router is part of a botnet? Today's CIoT devices often lack any meaningful logging or analysis capabilities which makes it almost impossible, even for tech savvy consumers, to identify a compromised device inside their network. All these aspects contribute to the fact that once a CIoT device is infected, chances are that it will stay infected for a long time.

Class breaks

It is common practice, not just for CIoT manufacturers, to buy so called *white label* devices from Original Equipment Manufacturers (OEM) to then rebrand and sell them under their own name to consumers. CIoT devices from seemingly different brands are actually produced by the same OEM. This means, that they run essentially the same software. Criminals right now just need to find a software vulnerability in a popular OEM device to be able to exploit this entire "class" of CIoT devices from a variety of different brands. In 2016, a security researcher found software vulnerabilities in certain models of Internet-connected Digital Video Recorders (DVRs) from an OEM called TVT. This OEM sold these *white label* DVRs to more than 70 different companies.[16] These DVRs might look different but the software base is identical. The now infamous attacks from the Mirai botnet during autumn 2016 were also largely possible because of security flaws in DVRs and Internet-connected cameras from two Chinese OEMs – Dahua[17] and Hangzhou Xiongmai Technolo-

[14] Consumer Reports. 2016. "How Outdated Router Firmware Puts You at Risk". http://www.consumerreports.org/wireless-routers/outdated-router-firmware-poses-security-risk/

[15] Mandiant. 2017. "M-Trends 2017". https://www2.fireeye.com/rs/848-DID-242/images/RPT-M-Trends-2017.pdf

[16] Rotem Kerner. 2016. "Remote Code Execution in CCTV-DVR affecting over 70 different vendors". http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.htm

[17] Level 3 Threat Research Labs. 2017. "Attack of Things!" http://www.netformation.com/level-3-pov/attack-of-things-2

gy.[18] Thus for criminals it is much more interesting to find exploits for popular OEM devices as it potentially means breaking into an entire class of devices. A thriving OEM ecosystem furthermore means that software updates might take a long time to reach the device: Even if the OEM releases a software update for a certain *white label* device, it's the vendor's responsibility to push this update to its own devices. So in the case of a software vulnerability in TVT's DVRs, all 70 companies would need to cooperate with TVT in order to push any software update to the devices. This takes time and coordination on a scale that has not been seen before. Outsourcing the manufacturing process of entire CIoT devices or modules to OEMs might be common practice and economically the right decision. Yet the way the current OEM market works, makes exploiting CIoT devices very attractive for criminals with one exploit providing access to countless devices from different companies and once exploited it's unlikely that any software patch will arrive in time.

This section illuminated why criminals will most likely continue to exploit insecure Internet of Things devices.[19] Two current characteristics, high persistence and the slow OEM ecosystem, might be improved through effective regulation. The next section will provide a short discussion how and which type of regulation might be able to address the different market dynamics.

How might regulation help?

The last two sections illustrated why the market fails to provide reasonably secure CIoT devices and why criminals will continue to exploit these insecure CIoT devices. Before discussing the different policy options, it's important to understand that there are two separate problems regarding insecure CIoT devices: (1) What should be done with all the insecure CIoT devices that are on the Internet right now? (2) How to improve the security of future CIoT devices? This paper will focus on possible policy solutions to the second question.

The problem of insecure Information and Communications Technology (ICT) is nothing new. Decades ago, IT security experts warned about the insecurity

[18] Zach Wikholm. 2016. "When Vulnerabilities Travel Downstream". https://www.flashpoint-intel.com/blog/cybercrime/when-vulnerabilities-travel-downstream/

[19] Roey Tzezana. 2016. "Scenarios for crime and terrorist attacks using the internet of things." European Journal of Futures Research. https://link.springer.com/article/10.1007/s40309-016-0107-z

of computer systems on the Internet.[20] Governments around the world are trying to improve the security specifically of IoT devices through a variety of proposed regulation, for example: The National Telecommunications & Information Administration (NTIA), part of the United States Department of Commerce, started a *Multistakeholder Process on Internet of Things Security*[21] with request for comments and four dedicated working groups for specific issues such as *upgradeability*. Furthermore, in August 2017 the US Senate introduced legislation to establish minimal security requirements for public procurement.[22] The European Commission's Directorate-General for Communications Networks, Content and Technology (DG Connect) recently proposed legislation addressing IoT security.[23] The German government wants to improve IoT security by working on labels for trustworthy IoT devices.[24] Apart from governmental initiatives, there are also many industry associations, consumer protection organisations, and expert communities which try to promote best practices[25], establish voluntary trustmarks or simply raise awareness[26] about the dangers of severely insecure CIoT devices.

[20] L0pht. 1998. "United States Senate Testimony". https://www.youtube.com/watch?v=VVJldn_MmMY

[21] The Department of Commerce's Internet Policy Task Force is conducting a review of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things. https://www.ntia.doc.gov/category/internet-things

[22] Internet of Things (IoT) Cybersecurity Improvement Act of 2017. https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

[23] European Commission. Proposal for a Regulation: Cybersecurity Package. COM(2017)477. https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

[24] Cybersecurity Strategy for Germany. 2016. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/2016/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=2

[25] Open Web Application Security Project: Top Ten. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[26] Verbraucherzentrale Bundesverband. 2017. "Hintergrundpapier des VZBV zum Thema Smart Home." https://www.vzbv.de/sites/default/files/downloads/2017/09/05/170905_hintergrundpapier_smart_home.pdf

Most of the initiatives from governments try to address one or more of the following aspects:

- Decrease information asymmetry between consumer and manufacturer through transparency by (voluntary) trust marks like **consumer labels**.[27] Many actors[28] are thinking about trustmarks and how they could help to improve the security of CIoT devices. Developing meaningful trustmarks for consumers will be an important step in the next years, yet they might not efficiently internalise external costs.

- **Software liability** can increase the accountability and responsibility of the manufacturer and creates incentives for him to internalise external costs.[29] The success of software liability laws seems to be dependent on a lot of other factors such as the possibility of class action lawsuits.

- Internalise negative externalities for the distributor by increasing the accountability and responsibility of the distributor through **distributor liability**. So far it is not clear which role the distributor should play. Interestingly, first lawsuits against distributor who are selling obviously insecure devices are brought to court.[30]

- Improve the security of IoT devices by introducing **mandatory baseline requirements** as a market barrier for certain product categories. A market barrier is a strong regulatory tool that is extensively used to ensure physical safety. The EU's CE mark is often seen

[27] Gilad L. Rosner. 2014. "Trustmarks in the Identity Ecosystem: Definitions, Use, and Governance". Commissioned by the UK Identity Assurance Programme and the Open Identity Exchange. https://ssrn.com/abstract=3054056

[28] See for example Consumer Reports' "The Digital Standard" (https://www.thedigitalstandard.org/); the community lead #iotmark (https://iotmark.wordpress.com/principles/) or the IoT Security Foundation's "Best Practice User Mark" (https://www.iotsecurityfoundation.org/best-practice-user-mark)

[29] Alan Butler. 2016. "Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices". https://repository.law.umich.edu/cgi/viewcontent.cgi?httpsredir=1&article=1193&context=mjlr

[30] David Meyer. 2017. "Insecure Android smartphone leads to court case for electronics retailer". http://www.zdnet.com/article/insecure-android-smartphone-leads-to-court-case-for-electronics-retailer/

as a role model and indeed the commission's proposal for a Cybersecurity Certification Scheme[31] partly incorporates and references CE mark legislation.

- Make it easier and cheaper for manufacturers to pay attention to Security by Design by releasing **guidelines or best practices**.[32]

Why security assessment is the foundation

The previous section categorised some of the currently debated policy options and discussed how those would address the previously identified market failures. This section first demonstrates how the the policy options rely on an efficient and effective security assessment "ecosystem". It is then argued why conventional pre-market certification is neither effective nor efficient to improve the security of CIoT devices.

Some form of security assessment is needed for voluntary consumer labels, mandatory requirements as a market barrier and extended product liability laws. Thus policy makers, standardisation and certification bodies, companies and consumer protection organisations need to talk about pillars of an effective and efficient security assessment ecosystem.

- Even if **voluntary consumer labels or other trustmarks** are based on self-certification by the manufacturer, at some point consumers will complain about a product. In order to not lose the consumers' trust in the label, a complaint will need to lead to an independent security assessment by a third party. Since the IoT market is still young and rapidly growing – McKinsey estimates a worldwide economic impact of $4 - $11 trillion dollars per year by 2025[33] – the number of complaints will also grow significantly. Thus if commu-

[31] European Commission. Proposal for a Regulation: Cybersecurity Package. COM(2017)477. https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

[32] ENISA. 2017. "Baseline Security Recommendations for IoT". https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

[33] McKinsey Global Institute. 2015. "The Internet of Things: Mapping the Value beyond the Hype". https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

nities, business associations or governments are talking about consumer labels, they also need to think about scalable security assessment.

- The same goes for **mandatory security requirements as a market barrier**, similar to the current CE mark for physical safety aspects. Since in this case it is mandatory for companies to pass the security assessment, there might be stronger competition between the independent assessment bodies to provide the service cheaper and quicker than the rest. These market dynamics of the security assessment ecosystem itself have to be taken into account.

- **Software liability** will also rely to some extend on an efficient and effective security assessment ecosystem. If a company is sued because of an insecure CIoT device independent security assessment will be necessary to prove if the company did everything in its power to develop and maintain a reasonably secure device or if it can be accused of negligence or wrongdoing.

Some form of product security assessment can thus be seen as the foundation for improving IoT security. The problem with currently popular security evaluation schemes like Common Criteria[34] is that they certify a product at a single point in time, they are very static, resource heavy and do not encourage re-certification. This creates an incentive for manufacturers and operators to not update an IT system after it (finally) received the certification. Especially hackers and security researchers are very sceptical about the effectiveness of current certification schemes like Common Criteria. They argue that security evaluation and certification did not save us from WannaCry[35], Petya[36] or any other major malware campaign which is true. This is partly due to the fact that many of the current *security* certification schemes rely heavily on static, slow concepts from *safety* evaluation – this simply does not work.[37] The concept of certification is not wrong, the way in which it is applied is wrong:

[34] The Common Criteria. http://www.commoncriteriaportal.org/

[35] Symantec Security Response. 2017. "What you need to know about the WannaCry Ransomware". https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

[36] Brian Krebs. 2017. "Petya Ransomware Outbreak goes Global". https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/

[37] Kai Rannenberg. 2000. "IT Security Certification and Criteria". In *Information Security for Global Information Infrastructures*. https://link.springer.com/content/pdf/10.1007/978-0-387-35515-3_1.pdf

To receive *safety certification* and comply with the necessary safety requirements the manufacturer of a washing machine will follow relevant norms and guidelines already during product development. Then, after the development cycle, there may be several evaluations of the product. If successful, the manufacturer receives the necessary safety certificates for this particular model. This static, thorough pre-market certification seems effective to assess the safety of a product – the laws of physics do not suddenly change after the consumer bought her new washing machine.

This type of pre-market certification at a single point in time is not effective to assess the *security* of a CIoT device. As argued in the previous section, IT security is a process that needs constant improvement. Once the smart washing machine is sold and connected to the Internet it is under constant attack. The threat landscape quickly changes as new attacks are developed. As demonstrated before, without thorough software maintenance a reasonably secure CIoT device might become inherently insecure from one day to the next. In order to become meaningful for IT security, evaluation and certification needs to evolve.[38] It needs to be reinvented to fit the 21st century. And that means paying attention to the entire product life cycle.

The following section will discuss central questions for a responsive and dynamic security assessment ecosystem for the Internet of Things – especially for cheap, mass-market CIoT devices.

Challenges for a 21st century security assessment

Technical Standards

The technical standards against which the assessment is done should be open and developed by all stakeholders.[39] Open standards make it easier for startups and small companies to prepare themselves for a security assessment. The German Federal Office for Information Security for example star-

[38] Aurelien Francillon. 2016. “Trust, but verify: why and how to establish trust in embedded devices”. In Design, Automation & Test in Europe Conference & Exhibition (DATE). http://www.eurecom.fr/en/publication/4801/download/mm-publi-4801.pdf

[39] Irene Kamara, Thordis Sveinsdottir and Simone Wurster. 2015. “Raising trust in security products and systems through standardisation and certification: the CRISP approach.” ITU Kaleidoscope: Trust in the Information Society. http://ieeexplore.ieee.org/abstract/document/7383632/

ted an open, multi-stakeholder process in summer 2017 to develop security guidelines for Internet routers. Technical Standards furthermore need to incorporate "dynamic" elements by making statements about the future, such as:

- How long will the manufacturer provide security updates?
- How quickly will the manufacturer provide a security patch once a vulnerability has been discovered?

These aspects cannot be assessed in a traditional way but need to be tracked over the lifetime of a product through market surveillance.

Volatility and Proportionality

Time, money and resources invested to successfully receive a certificate should be proportional to the product's price, lifetime and physical criticality – that being the potential for catastrophic damage. Proportionality helps the certification scheme to be efficient and effective for many different product categories: A compromised smart baking oven could potentially burn down an apartment and severely harm consumer. Thus the security assessment should be more detailed and in-depth than that of a smart surveillance camera. Furthermore the certifying authority should have ease to revoke certificates to encourage manufacturers to provide timely software updates.

Re-Evaluation

To discourage the practice of "certificate-stacking", as it hinders innovation and development, manufacturers should have an economic incentive to let their products be re-evaluated. "Certificate-Stacking" is related to proportionality: If it is expensive and time-consuming to obtain the necessary certification, manufacturers will "sit on" the certification for as long as possible. Operators also "collect" certification and avoid software updates if that means losing the necessary certification.[40]

Market Surveillance

Strong and responsive market surveillance is key to an effective security assessment ecosystem. It must be easy and transparent to responsibly disclose a security vulnerability of a product or to complain about a product

[40] Steven J. Murdoch, Mike Bond and Ross Anderson. 2012. "How certification systems fail: Lessons from the Ware report." *IEEE Security & Privacy*. http://www.cl.cam.ac.uk/~rja14/Papers/ieeesp12warereport.pdf

or manufacturer. Informing the manufacturer about a security vulnerability must automatically trigger further actions – a lot of work has already been done around Coordinated Vulnerability Disclosure.[41]

Certifying Organisation

As mentioned before, products will need different levels of security assessment – based on different factors such as price, potential for physical harm, lifetime, etc. Thus assessment bodies also need different levels. To exemplify: It should be relatively easy to acquire the licence to assess the security of a connected teddy bear or a smart toothbrush. For an assessment body to acquire the necessary licence to assess the security of a connected baking oven or a smart doorlock should be harder. Especially cheap connected devices will potentially proliferate the Internet, this creates the opportunity for a new industry of assessment bodies: Already today, countless security researchers find vulnerabilities in mass-market smart devices and inform manufacturers about those. This could be institutionalised by making it easy to obtain a licence for security assessment – the lower the price and potential for physical harm of a device, the easier it should be to receive a security assessment licence.

Responsibilities and economic incentives

A clear division of responsibilities between actors and a focus on economic incentives is crucial for the success of a security assessment ecosystem.[42] These aspects include:

- Assessment bodies having an economic incentive to be compliant to the standard against which they want to certify a product. If manufacturers know that it is easier to get a certificate from a certain organisation without repercussions they will do it.

- Clear definition of liable parties if a certified product is not compliant to the standard.

[41] Allen D. Householder, et al. 2017. “The CERT® Guide to Coordinated Vulnerability Disclosure”. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

[42] Eireann Leverett, Richard Clayton and Ross Anderson. 2017. “Standardisation and Certification of the ’Internet of Things’”. http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_23.pdf

- Setting incentives for security researchers or third parties in general to search for and responsibly disclose security vulnerabilities to the ecosystem.

- Identifying incentives for standard setting bodies to make technical standards for certificates meaningful and effective.

These are just a few considerations that should set the tone when thinking about security assessment for the Internet of Things. The IT security community can also learn from other fields like public transport or environmental protection: In 2017 the EU updated the European Energy Efficiency Label[43] and decided to implement QR-Codes on the products that link to a central database in which additional information about the product is stored. For security assessment, such a database could also store valuable information:

- single point of contact for vulnerability disclosure

- tracking firmware update history

- informing about known vulnerabilities

- statement about end of support timeframe and what happens after the support has ended.

A QR-Code that links to a central database is a tiny puzzle piece in the bigger picture of an effective and efficient security assessment ecosystem. Yet, it needs these types of small, effective ideas to improve the current status quo of security assessment.

Conclusion

Governments, industry associations and different interest groups have started to tackle the issue of insecure CIoT devices. There is no one size fits all approach to these issues and the more diverse people's backgrounds are that work on these issues the better society's chances are of getting the policy solution right. But, no matter if one favors strong software liability, voluntary consumer labels or mandatory security requirements – at some point

[43] European Union. Regulation 2017/1369. "setting a framework for energy labelling and repealing Directive 2010/30/EU". http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1369&from=EN

someone needs to actually assess the security of CIoT devices. The current certification schemes are not up to the task. They are slow, costly and do not scale down to be meaningful for 20€ webcams or 100€ Internet routers. They create little incentives for outsiders to contribute through vulnerability disclosure. And worst of all they are static pre-market instruments that do not work in a very dynamic security reality. Evaluation and certification can be a powerful instrument to improve the security of CIoT devices. However, in its current form it is severely underperforming. Designing an IT security assessment ecosystem that is responsive, open and effective for the Internet of Things is a pressing, time sensitive challenge that forces policy makers, standardisation and certification bodies, private companies and civil society to work together.

Note: The author is thankful for critical feedback and valuable input from Johanna Famulok, Sven Herpig, Jonathan Jones, Philippe Lorenz, Leonie Tanczer and Thorsten Wetzling. The author furthermore thanks all the participants from the workshop *EU's Cybersecurity Certification Scheme*, October 11th, 2017.

About Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organisation adopted a concept of mixed funding sources that include foundations, public funds and businesses.

Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organise conferences that address these issues and further subject areas.

About the Project

The project IT Security in the Internet of Things analyzes and develops economic incentives for IoT manufacturers to implement secure software development processes and follow Security-by-Design principles. To this end different concepts such as extended product liability, voluntary consumer labels or mandatory baseline requirements as market barrier are analysed and discussed in multi-stakeholder, expert workshops.

About the Author

Jan-Peter Kleinhans is leading the Internet of Things-Security Project at Stiftung Neue Verantwortung. Before joining SNV he was an intern at Netzpolitik.org. He is a Transatlantic Digital Debates (TDD) Fellow, holds a master’s degree in communication theory from Uppsala University and a bachelor’s degree in information systems from Darmstadt University of Technology.

jkleinhans@stiftung-nv.de
+49 (0)30 81 45 03 78 99

Imprint

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de