August 2018 · Jan-Peter Kleinhans

Improving IoT security in the EU

Why pre-market certification is not enough and how to fix it

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Just looking at Internet routers it becomes clear that the Internet of Things (IoT) has a severe IT security problem: global botnets consisting of hacked commercial off-the-shelf (COTS) Internet routers are being used for industrial espionage[1], to mine cryptocurrencies[2], to steal online banking credentials[3], for denial-of-service attacks against websites[4] or to attack critical Internet infrastructure.[5] The increasing ubiquity of IoT devices combined with the fact that the market fails to produce reasonably trustworthy and secure IoT devices[6] was reason enough for the European Union to start regulating this field. The EU Cybersecurity Act (CSA)[7] – which is still being negotiated – heavily relies on the interplay between standardization, conformity assessment and market surveillance: consortia consisting of different stakeholders develop technical standards (cybersecurity certification schemes) and manufacturers can use these schemes to certify their devices and thus prove conformity. Product *safety* is regulated in a similar way since decades in the EU. The achilles heel of this approach is the market surveillance and currently the CSA fails to improve and strengthen this aspect: if regulators allow manufacturers to self-assess their conformity to defined IT security requirements (certification schemes), market surveillance needs the resources and knowledge to identify false claims and sanction bad actors.

Because of its reliance on certification and conformity assessment, the CSA also struggles with the fact that one-time, pre-market certification does not fit well in today's continuous software development realities: The manufacturer of an IoT device with software-defined functionality, has a continuous

[1] Talos Intelligence. 2018. "New VPNFilter malware targets at least 500K networking devices worldwide". https://blog.talosintelligence.com/2018/05/VPNFilter.html

[2] Trustwave. 2018. "Mass MikroTik Router Infection – First we cryptojack Brazil, then we take the World?". https://www.trustwave.com/Resources/SpiderLabs-Blog/Mass-MikroTik-Router-Infection-%E2%80%93-First-we-cryptojack-Brazil,-then-we-take-the-World-/

[3] Radware. 2018. "DNS Hijacking Targets Brazilian Banks". https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/dns-hijacking-brazil-banks/

[4] Sucuri. 2016. "IoT Home Router Botnet Leveraged in Large DDoS Attack". https://blog.sucuri.net/2016/09/iot-home-router-botnet-leveraged-in-large-ddos-attack.html

[5] Manos Antonakakis, et al. 2017. „Understanding the mirai botnet." USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[6] Jan-Peter Kleinhans. 2017. "Internet of Insecure Things". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/de/publikation/internet-insecure-things

[7] EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act). 2017/0225(COD). http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)

obligation towards the user to keep this device safe and secure. In order to estimate if and to what extent the manufacturer meets this obligation, users, market surveillance and other stakeholders need up-to-date, accessible information about the current IT security of the device. To this end, the paper proposes a minimal set of supplementary information that should be easily accessible in order to estimate how much the manufacturer takes care of their devices after the point of sale. This type of information could be made available in several different ways: (1) a central database run by the European Commission to which manufacturers send their data or (2) a decentralized system in which it is the manufacturer's responsibility to maintain a "living document" throughout the product lifetime. Both systems are currently deployed or under development for different areas of regulation. This type of up-to-date information about the security of certified products on the EU Single Market would benefit a variety of stakeholders and significantly strengthen the CSA's proposed certification framework.

1. Introduction

With the Internet of Things (IoT) security vulnerabilities in software can have direct physical consequences – safety and security are now interlinked.[1] It is thus understandable why Europe, with the Cybersecurity Act (CSA), wants to regulate *IT security* of commercial off-the-shelf (COTS) products with the same policy tools that have been used in the past to regulate product *safety*: standardization, conformity assessment and market surveillance.[2] In order to effectively and efficiently strengthen the IT security of COTS products and services available on the EU single market regulators need to adapt these policy tools to the fast-moving software development reality. The following paper argues that traditional conformity assessment is too static and needs to be supplemented with up-to-date information over the lifetime of a product in order to meaningfully assess the trustworthiness of a product or service. Other regulatory fields such as energy efficiency or construction products already address the need of accessible, transparent information for different stakeholders about the conformity of a product or service. The CSA should do the same.

The CSA will establish a framework for IT security certification of products and services in the European Union.[3] This "Cybersecurity Certification Framework" (Articles 43 – 54 of the CSA) defines roles, responsibilities and processes for different actors. One of the goals of the regulation is to establish a market for certified, trustworthy products in the European Union. It is important to mention that the CSA does not define (technical) characteristics of a "secure" or "trustworthy" product. Instead, it simply states by whom and how these cybersecurity certification schemes should be developed and certain requirements a "European cybersecurity scheme" should fulfill. Additionally certification will be voluntary for manufacturers and the framework relies on both Self-Declaration of Conformity (SDoC) and third-party certification. SDoC means a manufacturer can simply state that their product conforms to an existing certification scheme. The possibility of SDoC is cheaper for the manufacturer and avoids the potential bottleneck of third-party certification in regards to time to market. Ultimately European regulators hope that manufacturers adopt cybersecurity certification schemes (either by SDoC

[1] Lily Hay Newman. 2018. "A new pacemaker hack puts malware directly on the device". Wired. https://www.wired.com/story/pacemaker-hack-malware-black-hat/

[2] Jan-Peter Kleinhans. 2018. "Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf

[3] EU Cybersecurity Act – Council General Approach (http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf)

or third-party certification) to gain a competitive advantage on the market.

In theory, IT security certification and conformity assessment has the potential to significantly strengthen the market for trustworthy and secure devices in the EU. To this end the CSA heavily relies on pre-market IT security assessments[4] (third- party certification or SDoC) of the final product or service to determine if and to what extent the manufacturer followed EU certification schemes. Yet this one-time "snapshot" of the security of a device becomes quickly out-of-date in today's rapid software development cycles: A regular internet router might, for example, meet certain security standards at the time of the IT security assessment. To keep the router secure, the manufacturer has to continuously test it against new types of attacks, swiftly react to newly found security vulnerabilities from security researchers and diligently update the device's software. A one-time assessment or certification cannot make claims about the future and to what extent the manufacturer will continue to meet its obligation towards the user to keep the device secure.

2. Why a pre-market security assessment alone is not effective in regulating the fast-moving IoT market

Current regulatory initiatives on the European level rely on some type of security assessment – most often pre-market – to assess the trustworthiness and security of Internet-connected devices.[5] This security assessment is either done by the manufacturers themselves through a SDoC or by an independent third party, a Conformity Assessment Body (CAB). If the outcome of this assessment is positive, the resulting certificate of conformity is then valid for a certain amount of time, in most cases between one and three years. The fundamental challenge of any type of security assessment is that it is just a snapshot at a certain point in time. This snapshot loses more and more of its validity with every software update the IoT device receives.[6] Furthermore a device becomes less secure as the nature of attacks changes.[7]

[4] Jan-Peter Kleinhans. 2017. "Internet of Insecure Things". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/de/publikation/internet-insecure-things

[5] EU Cybersecurity Act (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN)

[6] Ross Anderson and Shailendra Fuloria. 2009. "Certification and Evaluation: A Security Economics Perspective." In 2009 IEEE Conference on Emerging Technologies & Factory Automation. IEEE. https://doi.org/10.1109/etfa.2009.5347129.

[7] Andrew Prout, et al. 2018. „Measuring the Impact of Spectre and Meltdown." arXiv preprint. https://arxiv.org/abs/1807.08703

To avoid the problem of outdated certificates after the device receives software updates some experts propose to focus on a manufacturer's secure software development process.[8] If a manufacturer follows a (certified) secure software development process it is likely that the developed software is of higher quality and that the company has the necessary processes in place in order to quickly and adequately react to newly found vulnerabilities. Thus such a manufacturer is more likely to produce secure and trustworthy products than a manufacturer who does not have these processes in place. Instead of assessing the security of the final product CABs or certifying bodies would assess the manufacturer's software development process and regulators would infer that these manufacturers are more likely to produce trustworthy and secure devices. However assessing the security of the software development process is also no silver bullet:

- Establishing and certifying a secure software development process **takes significantly more time and resources** than assessing the security of the final product – especially in the field of commercial off-the-shelf (COTS) devices.
- Just because a company has a secure software development process does not mean that they **follow this process for every single product they develop.**
- Especially **new businesses and startups evolve quite rapidly over time**, making the certification of a business process at a certain point in time less meaningful.
- Certifying a manufacturer's secure software development process is **one step away** from the regulatory goal of having more trustworthy and secure devices on the European Single Market.

Obviously certification of a secure software development process has its own challenges and shortcomings. Looking at COTS devices a combination of product-based security assessment and mandatory statements from manufacturers regarding their software development processes (i.e. upgradeability) will most likely be necessary to assess the trustworthiness of the product.[9] It is highly likely that the cybersecurity certification schemes, that will be developed under the EU Cybersecurity Act, will account for both product-based security assessment and mandatory statements from manufacturers regarding the development process. Yet any type of one-time assess-

[8] Heitzenrater, Chad, and Andrew Simpson. 2016. "A Case for the Economics of Secure Software Development." In Proceedings of the 2016 New Security Paradigms Workshop on - NSPW. ACM Press. https://doi.org/10.1145/3011883.3011884.

[9] See for example EU Cybersecurity Act, Article 47 (Elements of European cybersecurity certification schemes)

ment or statements from the manufacturer are too static for today's dynamic software-development reality. Both need to be supplemented by up-to-date information about the current trustworthiness of the device.

3. How supplementary information strengthens certification and helps a variety of stakeholders

Assessing the trustworthiness of COTS IoT products in the European single market can be described as a transparency and information problem: such up-to-date information post-certification needs to be available to the market throughout a product's lifetime to meaningfully assess the trustworthiness of the product or service. Such information includes:

- Date and validity of certification (valid, expired, revoked)
- Type of certificate (Self-Declaration of Conformity, third-party assessment)
- Official date of end of security support by the manufacturer
- Current firmware version
- History and changelog of firmware versions
- Unfixed security vulnerabilities (CVE) based on current firmware version[10]
- Single point of contact for security vulnerabilities

With this type of supplementary, up-to-date information a certificate of conformity would remain meaningful for a longer period of time. Furthermore it would reinforce the regulatory effect of the certification scheme by supporting all stakeholders involved:

Consumers: Based on this type of supplementary information the consumer would be able to answer a variety of questions that so far have been left unanswered: How old is the certificate and how thorough was the security assessment (SDoC vs independent third-party certification)? For how long will the product receive security updates? How quickly does the manufacturer fix security vulnerabilities? How vulnerable is the device today? With this type of information the consumer would be able to make a much more informed decision and IT security could actually become a purchasing criterion. Furthermore third parties, such as journalists or test labs (Consumer Reports, Stiftung Warentest, etc.) could use this information for their own reviews.

[10] Common Vulnerabilities and Exposures. https://cve.mitre.org/

Manufacturers: Any type of security assessment costs the manufacturer time and resources. Additionally, a label on the packaging or the product itself might lead to less differentiation between high and low quality manufacturers. This could happen because the security assessment happened at a single point in time and cannot make statements about the future, thus, a consumer might perceive two different products with the same label as equally secure. A manufacturer who focuses on time-to-market might only provide the bare minimum of security updates. But at the time of assessment the product was compliant to the requirements of a certain label. A manufacturer who focuses on quality and premium products might provide security updates on a regular basis thus fixing security vulnerabilities much more quickly. Yet a security assessment can neither predict nor ensure the level of responsiveness of the manufacturer over the lifetime of the product. This means that these two products would have the same type of IT security label but the actual security would differ greatly. In this example the more responsible manufacturer would actually lose its ability to differentiate itself from the competition because the consumer just sees the same label on different products – implying an equal level of security and trustworthiness of both products.

Market Surveillance: Supplementary information could make market surveillance significantly more effective. Market surveillance could focus on devices which have not received security updates for a long time. Or devices that have unfixed security vulnerabilities for a certain amount of time. To better inform the market, devices that have been tested and are considered insecure could be marked.

Security researchers: Security researchers would benefit from a single point of contact for responsible disclosure of security vulnerabilities. Especially for off-the-shelf consumer IoT devices it is often not easy to find the contact details of the manufacturer thus making it unnecessarily tiresome for a researcher to disclose security vulnerabilities.

Distributors: In cooperation with market surveillance activities distributors could benefit from supplementary information by being informed about insecure devices. Since EU policy makers are currently discussing the responsibilities of distributors for selling insecure products, providing distributors with more and easily accessible information about the security of the device should be mandatory.

Regulators: With the help of such supplementary information regulators could more easily evaluate the effectiveness of different cybersecurity certification schemes and identify gaps or product categories in which schemes are not yet readily available or accepted.

4. How to provide supplementary information for compliance, transparency and trust

There are many different ways to gather, store and access different types of supplementary information. Interestingly, different areas of compliance like the regulation of construction products, radio frequencies or energy efficiency already developed some approaches:

- **A central database**
  With the energy labelling regulation (Regulation (EU) 2017/1369)[11] the idea of a central, open product database run by the European Commission was introduced. The database consists of a public and non-public part and holds technical information about the energy efficiency of certain products sold on the EU Single Market. The non-public part holds the technical documentation of the products. It is the manufacturer's responsibility to provide all the necessary information and keep it up to date.

  The advantage of an **open and machine-readable** database would be that third parties could develop user interfaces and apps to enable different stakeholders to retrieve information that is of interest to them. Dividing the database in a **public and non-public part** encourages manufacturers to provide in-depth technical documentation to certain stakeholders such as market surveillance authorities and regulators. Obviously as much information as possible should be stored in the public part of the database. What type of information the manufacturer needs to provide could furthermore be determined by the relevant cybersecurity certification scheme and further depend on the assurance level. The downside of a central database is that it creates a **single point of failure** and companies have to trust the Commission to keep the data safe and secure against unauthorized access.

[11] Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=uriserv:OJ.L_.2017.198.01.0001.01.ENG

The **Radio Equipment Directive** (2014/53/EU)[12] follows a similar approach: Article 5 in combination with Article 3 establishes a "central system" run by the Commission to register radio equipment within certain categories. Even though the Commission did not yet specify the product categories for which Article 5 and Article 3 are applicable, the intention behind a central registration is to better support market surveillance.[13]

- **A Living document**
  The **"Smart CE Marking"** for construction products[14] links a physical product to a digital, machine- and human-readable statement of conformity from the manufacturer. Instead of registering products in a central database, each manufacturer would be responsible for (hosting) their own documents. Such a decentralized system creates little administrative overhead and avoids any single point of failure. The lack of a central database means that meta analysis and search queries are harder to implement, but not impossible.

In summary, a central database run by the European Commission creates administrative overhead and forces companies to trust the Commission. But it also makes meta analysis and searches easily accessible for a variety of stakeholders. A decentralized system in which every company is responsible to host the necessary information on their own avoids a single point of failure but makes it harder, if not impossible, to analyse the metadata of all relevant products on the EU single market.

5. Design considerations for future approaches

Regardless of the benefits and shortcomings of the different approaches, supplementary information over the product lifetime is desperately needed. When a manufacturer produces an IoT device with software-defined functionality, the manufacturer has a continuous obligation towards the user to keep this device safe and secure. Ultimately the user, market surveillance and (to some extent) regulators simply want to know whether or not the manufacturer takes care of its device after the point of sale. IT security certification or conformity assessment can make sure that the manufacturer fol-

[12] Radio Equipment Directive 2014/53/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

[13] TÜVSÜD. 2015. "New Radio Equipment Directive Means Change". https://www.tuv-sud.com/home-com/resource-centre/publications/e-ssentials-newsletter/telecommunications-e-ssentials/vol.-4/new-radio-equipment-directive-means-change

[14] European Committee for Standardization. 2018. "CEN/WS 'Smart CE marking'". https://www.cen.eu/News/Workshops/Pages/WS-2017-014.aspx

lowed certain standards and best practices *before* the product was sold. Yet neither mechanism can vouch for the time *after* the product has been sold. This gap needs to be addressed and one way would be through specific, up-to-date, supplementary information the manufacturer has to provide over the lifetime of the product. Following are key design considerations when developing such a system:

- **Easily accessible link on the product:** The data (no matter how and by whom it is stored) should be accessible via a **QR-Code** on the product package and the product itself.[15] Additionally the **EAN (European Article Number)** could be used by online distributors to retrieve information and display it alongside the product description on the distributor's website.

- **Open and machine-readable:** Supplementary information should be provided in an open and machine-readable way to enable stakeholders to freely work with the data.

- **Integrating and benefitting all stakeholders:** Current European information sharing systems like RAPEX[16] or ICSMS[17] only serve market surveillance authorities. Any future approaches should benefit all stakeholders, especially consumers, and should not be limited to market surveillance authorities. As mentioned before such a system would not just establish a certain level of **transparency** on the market but would also enable a **flow of information between different stakeholders** such as: (1) Market surveillance could warn distributors about insecure products for which the certificate has been revoked. (2) Manufacturers would be able to communicate directly to consumers by better informing them about the security of their product. (3) Security researchers could more easily inform market surveillance about presumably insecure products, thus better focusing their limited resources.

[15] Jean-Pierre Nordvik and Gianmarco Baldini. 2018. "EU R&D in cybersecurity certification". Presentation at EESC public hearing. https://www.eesc.europa.eu/en/news-media/presentations/eu-rd-cybersecuritys-certification

[16] European Commission. Rapid Alert System for dangerous non-food products. https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=main.listNotifications

[17] European Commission. internet-supported information and communication system for the pan-European market surveillance. https://webgate.ec.europa.eu/icsms/

6. Conclusion – Everybody would benefit

In essence, everybody would benefit from accessible and transparent information about the security and trustworthiness of certified COTS devices in the EU Single Market. It would help regulators ensure that the regulatory goals of the Cybersecurity Act are met. It would provide market surveillance with a platform to use their limited resources more efficiently, and to more easily identify potentially bad actors on the market. But it would also help manufacturers communicate more effectively with consumers – much more than what would be possible with a simple, static label on the product package. Lastly, any approach that provides up-to-date supplementary information after the security assessment would strengthen the enforcement of IT security requirements set out in future European cybersecurity certification schemes. This would be especially helpful since the CSA so far lacks any meaningful market surveillance or enforcement aspect.

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. Read more.

About the Project

The project IT-Security in the Internet of Things analyses and develops economic incentives for IoT manufacturers to implement secure software development processes and follow Security-by-Design principles. To this end different policy tools such as extended product liability, voluntary consumer labels or mandatory baseline requirements as market barrier are analysed and discussed in multi-stakeholder, expert workshops. In these workshops participants from academia, private companies, ministries and civil society critically discuss the problem analysis, brainstorm ideas how to improve the current status quo and critically assess the effectiveness of policy proposals. All workshops are held under the Chatham House Rule. These workshops, expert interviews and desk research are the basis for the project's policy papers.

Author

Jan-Peter Kleinhans
Project Director IT-Security in the Internet of Things
jkleinhans@stiftung-nv.de
Twitter: @jpkleinhans
+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