Stiftung Neue Verantwortung

Workshop Proceedings

Market Surveillance and IT-Security – What are new roles, responsibilities and information flows based on NLF?

Wednesday, May 29th 2018, Stiftung Neue Verantwortung

On May 29th 2018 SNV organized the workshop *IoT Security and Market Surveillance*. It was the fifth workshop as part of the IT-Security in the Internet of Things project and brought together stakeholders from civil society, academia, companies and ministries. The workshop was held under the Chatham House Rule. As project director Jan-Peter Kleinhans was conducting the workshop. For questions, feedback or critique you can reach him via jkleinhans@stiftung-nv.de.

The workshop had three objectives:

1. Bring together IT security experts and experts in the field of conformity assessment and the NLF/CE system.
2. Analyze and discuss shortcomings of the NLF/CE market surveillance system and how it would need to be modernized in order to be fit for IT security.
3. Explore potentials of a product database to track essential information about the IT security of IoT products sold inside the EU.

To this end the workshop was structured in two sessions: The **first session** explored shortcomings and fundamental problems of the NLF/CE system regarding market surveillance and IoT security. The **second session** focused on brainstorming aspects of an IoT product database. Following is a summary of focal points of the discussion (session #1) and the brainstorming of elements of a database (session #2).

Session #1 – The NLF/CE system and market surveillance for IT security

The discussion of the first session was based on several assumptions and a certain scenario: Assuming that…

- a European IT security certification system for certain consumer IoT products exists
- a researcher finds a security vulnerability in a "certified" consumer IoT product
- the security researcher is neither a conformity assessment body nor a public authority but an "independent individual" (academic security researcher, consumer, hacker, etc.)
- the security researcher wants to inform the manufacturer about the vulnerability and/or (at least) warn the public about an unsecure / unsafe device

- **Consumer representation:** It was argued that consumers lack adequate representation already during the development of technical standards and that they do not have a formal role inside the current CE system. Some participants said that some Standardization Organizations actively involve consumer representatives: DIN established a Consumer Council and on the European level ANEC is supposed to represent a consumer perspective in standardization development. That said, many participants agreed that large international companies will ultimately have more resources and expertise to influence standardization development.

- **Consumer awareness:** The lack of user representation / focus is furthermore the reason why current CE information systems are geared towards market surveillance authorities and test laboratories. (ICSMS and RAPEX) Participants argued that consumers should be better (at all) informed about unsafe / unsecure devices.

- **Fragmented market surveillance:** Market surveillance is done by public authorities and many member states have different approaches how to organize market surveillance nationally (in Germany market surveillance is done on a federal level, thus there are more than 200 German market surveillance authorities). This leads to several hundred market surveillance authorities in Europe.

- **Responsibility of the Distributor:** It was discussed that to date the responsibility of the distributor regarding unsecure IoT products is unclear. If the manufacturer cannot be reached should the distributor then be stopped from selling unsecure devices? Example: The North Rhine-Westphalia consumer protection agency in Germany sued the retailer Media Markt for selling an unsecure and outdated Android smartphone because the smartphone manufacturer Mobistel did not respond. Many participants agreed that at some point the distributor / retailer has to be held accountable for selling unsecure devices – just like it is today already the case for unsafe devices.

- **Ease of use for security researcher:** The participants agreed that it should be as easy as possible for a security researcher to inform the vendor / a public authority / someone about a security vulnerability in an IoT product. Even if there is a preferred way we never know who the security researcher will contact first. Most of the participants agreed that there should by a *central public authority* that the security researcher could contact to disclose the vulnerability.

- **Public authority as Single Point of Contact:** Most of the participants were in favor of a public authority as a single point of contact for security researchers. The security researcher discloses a vulnerability to a central public authority. This authority should not be a new, monolithic European agency, but rather a

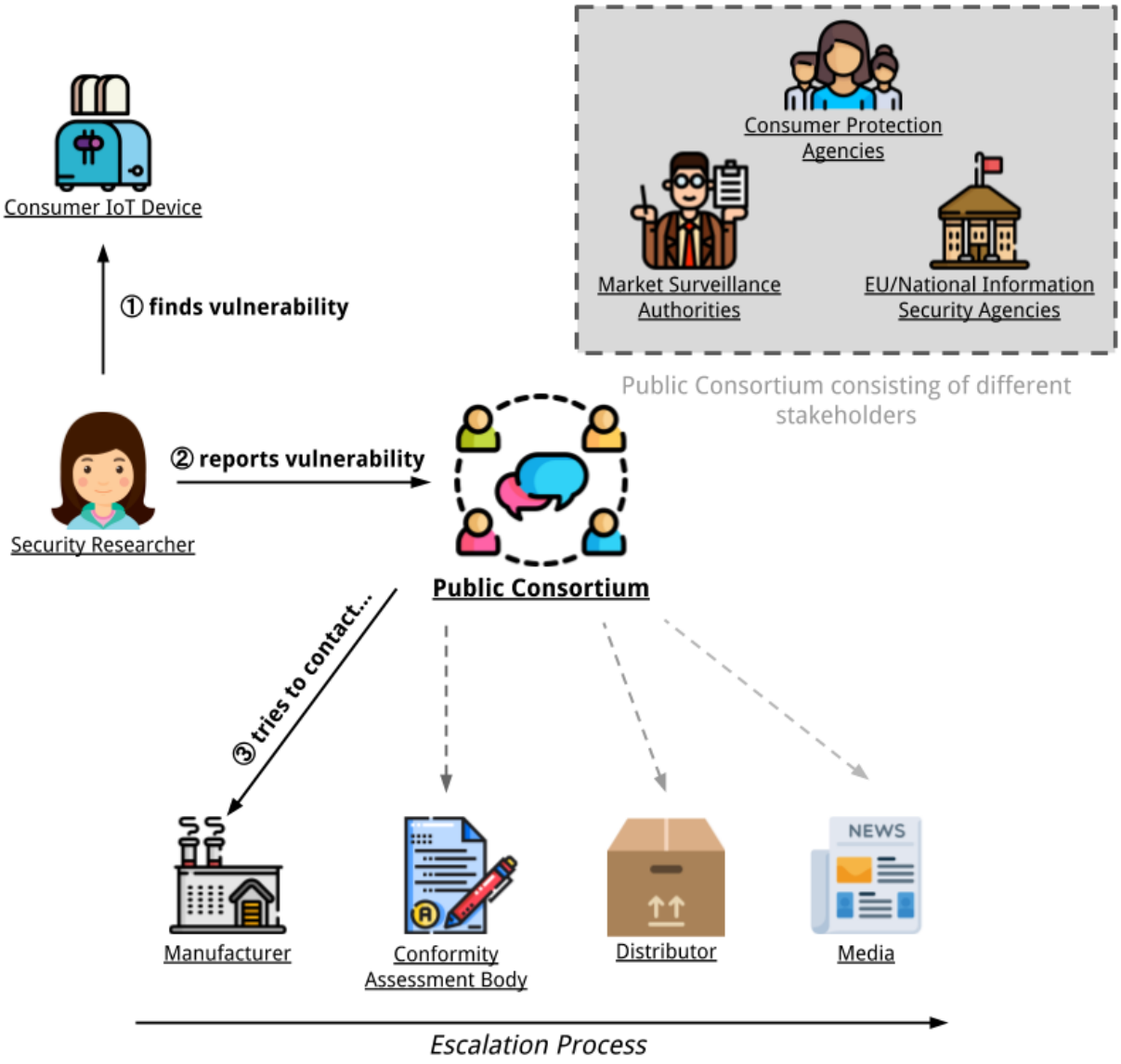
platform / collaboration of European market surveillance authorities, information security agencies and other stakeholders. The public authority tries to contact the manufacturer of the vulnerable IoT product and assesses the risk of the security vulnerability to coordinate the public disclosure. Many participants saw a public authority with close connections to market surveillance and information security agencies best suited to assess the potential impact of a security vulnerability: How many devices are vulnerable? How easy would it be to fix the vulnerability? How likely is it that X% of devices are patched after Y amount of days/weeks/months?

Additional thoughts: Such a public authority / consortium would need to strike the right balance between in-depth risk assessment of any security vulnerability and close ties to manufacturers and vendors to inform them about disclosed vulnerabilities. Furthermore such an entity would need to be highly transparent and accountable to gain the trust of the public in general and security researchers in particular to not misuse security vulnerabilities for law enforcement/intelligence agency purposes.

- **Information flows based on a public consortium as single point of contact:** an aforementioned public consortium as a single point of contact for security researchers would serve different needs…

  - It is completely up to the security researcher if she wants to contact the consortium or go directly to the manufacturer. **No "mandatory" reporting.**
  - The consortium would forward the vulnerability report to the manufacturer thus **protecting the security researcher's identity** in case the company tries to suppress the vulnerability report based on IPR claims – this regularly happens today and is a serious obstacle to independent security research.
  - The security researcher would not waste time to **find out who the actual manufacturer / OEM** of the IoT product is.
  - With market surveillance authorities and information security agencies as part of the consortium, the consortium is in a much **better position to assess the risk and potential impact** of a security vulnerability compared to the security researcher herself who is focused on a single device /product family.
  - If the manufacturer is unresponsive the consortium could **warn distributors** about a vulnerable device that should not be sold on the European market (if the severity of the vulnerability is high).
  - If the manufacturer is unresponsive but the device has undergone a 3rd party security assessment by a conformity assessment body (CAB), the consortium could **contact the CAB since they might have a direct working relationship with the manufacturer**.

- If everything else fails and the severity of the vulnerability is high, the consortium could **work with media to warn and inform consumers** about the vulnerability.



Session #2 – potential of a product database

The second session brainstormed the idea of a central device database that tracks security relevant information about (certified) devices. *See the workshop input paper for more information about the database.*

- **Software support and vulnerabilities**
  - Date of end of support (and functionality after end of support)
  - For how long are *security updates* guaranteed?
  - Expected lifetime / life expectancy
  - Latest firmware version, history of firmware versions and changelogs
  - Known and (until now) unpatched vulnerabilities (CVE ?)
  - Point of contact for security vulnerabilities / is there a bug bounty program?
  - Validity status of (3rd party) security assessment: *valid until, invalid, revoked*
  - Warnings from vendor / conformity assessment body / market surveillance
  - If high-risk vulnerabilities: list of informed parties

- **Transparency**
  - Product identification: unique ID, vendor, point of contact, version, name of different variants
  - "Bill of materials": 3rd party components (SW libraries, HW modules, etc.)
  - OEM / white label device: list of vendors / resellers
  - Source code including tool chain encrypted with escrowed key.

- **Privacy / Capabilities**
  - What data is collected / processed / transmitted / shared?
  - Functionality without external dependencies? (offline)
  - Ability to choose service provider?

- **Administrative information**
  - Type of certification (SDoC vs 3rd party)
  - if 3rd party assessment: Name/contact info of conformity assessment body
  - if self-assessment (SDoC): reference to guideline / technical report
  - applied scheme (Cybersecurity Act) and risk-assurance level
  - "intended use": categories / scenarios
  - Installation location (How to recognize the device)
  - *Connection to other information systems (RAPEX / ICSMS)*