# CSIRTs are to Product Security as Ferries are to Islands

Speakers: Erka Koivunen, Head of CERT-FI
Anu Puhakainen, Head of Ericsson PSIRT

## *Introduction to both CERT teams*

Ericsson Product Security Incident Response Team has been officially founded in 2004. It has been accredited by TERENA in 2005 and FIRST 2006. It is a corporate team with global responsibility, core team located in Finland. Ericsson PSIRT is single interface for *product vulnerabilities and security incidents* concerning Ericsson delivered products and solutions to the operators. Ericsson PSIRT is NOT responsible for Ericsson internal IS/IT network, nor do we focus on specific mobile terminal issues or mobile malware – unless it related closely to the incidents taking place in the mobile network side.

CERT-FI (CERT Finland) is the national computer security incident response team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. CERT-FI currently celebrates its 10 year anniversary. Already since its early days, CERT-FI has been involved with vulnerability coordination.

## *Myths about PPP*

There are lot of argument against PPP and why it does not work. What are these myths that people often refer to in both sides and can these myths be Confirmed, Plausible or Busted?

### Myth #1: Regulators should be kept at arm’s length

As vendor CERT the argument against PPP and sharing e.g. vulnerability information you hear from time to time is that

- “Authority will come up with new regulations when they learn more how systems work and what are the issues”

  Based on our experience this is jus a belief, not a fact i.e. “busted”. It adds value to share information and discuss technical details as then in both sides you understand better the other parties’ viewpoints. One example of this type of discussion we have had it related to GSM vulnerabilities triggered by presentations given in various seminars during the past years. Openly sharing knowledge on standardization, specifications, technical details, development and business aspects led to common understanding on the overall situation, leaving a bit aside the organizational roles during the discussions.

- Big Brother Society vs. Security Threats (such as terrorism)
- Cyber Security Posture: ad-hoc or strategic?

- National legislation vs. global business interests

  It is true that national legislation may conflict with global business interests. There are also cases where national legislation is contradictory and conflicting with each other in different countries. A vendor (CERT) needs to operate in all those countries and understand the national aspects of legislation (e.g. privacy rules) no matter how different they are. Global business interests drive the decisions in product level and compromises are bound to happen.

  In these cases PPP can help to formulate an understanding in both in national level and the bigger picture, where the players can together discuss what is reasonable to achieve in national level vs global level.

**Myth #1: Busted**

**Myth #2: Businesses treat security as expenditure**

For public sector player the commercial organization many times looks like they are reluctant to act on security, whether it is fixing vulnerabilities discovered in their products or something else more pro-active. The claim often heard is

- ”For commercial organization business interest **always** overrules security requirements”

  It is true that commercial interests **may** overrule some security requirements and that may lead to downplaying the importance of security or a single vulnerability. E.g. decisions to fix vulnerabilities in commercial products are done many times by risk based approach. It considers the installed based, severity of the vulnerability, its exploitability and likeness to be exploited and other possible mitigation methods. If the vendor decides to bear the risk instead of fixing a particular vulnerability, it may look like to outside world like business interest override security or vendor is reluctant to act on security. This perception is also due to lack of transparency of actions, as many of the items listed as decisions factors above are company confidential information. By talking about these within PPP helps to gain understanding on both sides how the players think.

- Quality Control (regression bugs, anyone?) and Fixing Vulnerabilities

  Another viewpoint for stating that businesses treat security as expenditure, is that it may take enormously long to release a patch once zero day has been found. For a individual security researcher processes for a big corporation are not seamless. Already due to regulator interest e.g. in US and India, the vendors shall be able to show excellent supply-chain security and good discipline in security in product development lifecycle. Alone these requirements usually mean that even a “hot fix” or “quick fix” takes couple of days, if not weeks, to release.

Let’s consider an imaginary case, where vulnerability is found in telecom equipment that is used in mobile network, radio part. The vulnerability is considered severe and there is quick decision that it needs to be fixed. Imagine if this particular product series in question has installed base of few hundred thousands nodes across the world.  There might be 2-4 release tracks that need to be maintained. What if there is a need to change something in the underlying design, not “just fixing the vulnerability”? The implementation and testing of the patch, however critical and urgent it is, has to go according to secure development and supply-chain handling. The deployment in the field is not only a challenge to the vendor, but in this case to the actual mobile operators.

- Upstream vs. Downstream

- ”Seven Bad Habits of Vulnerability Response”

**Myth #2: Busted**

**Myth #3: Security researchers hate vendors**

- Media stunts vs. genuine research
- Research interests vs. end users’ right to security

Researchers have freedom of focusing their investigations on whatever they decide and they have full rights to publish the results of their work. Actually it is most often required e.g. by the universities because researcher’s work is paid from public funds. However, sometimes the disclosure is closer to irresponsible than responsible. Sometimes disclosure is done only because of media coverage and creating more presentation opportunities for the researcher.

There have been cases when the researcher has been reluctant to talk with the vendor and vice versa. There might be a good role e.g. for a national CERT to be an active middleman bridging the gap and different interests and thereby actively engage both parties in the process – because that is what is needed. Reasonable people come up with reasonable solutions when giving the opportunity.

Example: Sockstress coordination that took more than a year, Stonesoft evasion techniques

- ”Radical Collaboration” vs. chicanery

**Myth #3: Busted**

## *Conclusions*

PPP can be successful and have fruitful results:

- It’s all about people skills, people!
- It’s all about communications! Remember to listen to the other party and try to genuinely understand their viewpoints.
- Be open, left behind your roles for once and talk about facts without getting emotions and organizations roles and objectives involved.