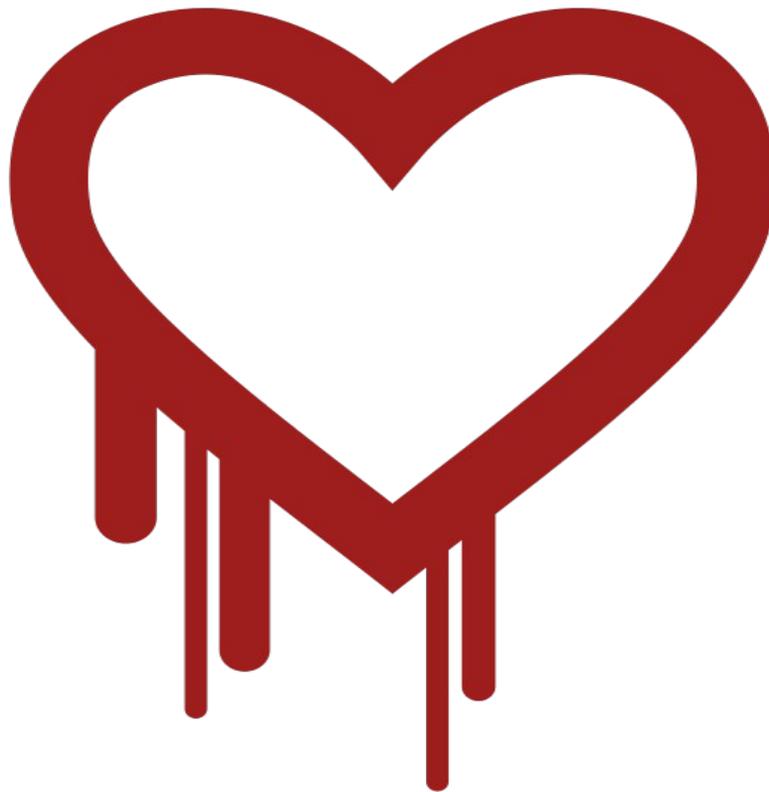


Openforum Academy

White Paper

**Ensuring the security of critical ICT Infrastructure
after Heartbleed: Should we leave it to the
Community or does Government have a role?**



Report

Ensuring the security of critical ICT Infrastructure after Heartbleed: Should we leave it to the Community or does Government have a role?

26 June 2014, Silken Berlaymont, Brussels

Credits:



(Picture)



(White Paper content)

Disclaimer:

This report is prepared by the rapporteur, Dr. Alea Fairchild, for OpenForum Academy (OFA). The summaries of the speaker presentations and panel discussions in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion.

The views expressed in the report do not necessarily reflect those of the rapporteur or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

Foreword

Speakers

Keith Bergelt- Open Invention Network (OIN)

Christian Horchert (fukami) – Chaos Computer Club

Michel Lacroix – DG Connect, European Commission

Moderator: Graham Taylor, CEO of OpenForum Europe

Rapporteur: Dr. Alea Fairchild, Director, The Constantia Institute and Docent, KU Leuven

Graham Taylor opened the event by introducing OpenForum Europe, the topic and speakers. He also explained about the OpenForum Academy and its purpose in creating a debate forum environment. This is a moderated discussion, with an inclusive debate on the topic. We start with brief presentations by three speakers, then opening this up to discussion by the attendees.

Graham introduced the topic as a number of issues: first being the impact of critical infrastructures within enterprise and government, specifically around cloud. He then touched on open source and critical infrastructures, and the development models and their security design. Data governance and ownership on the basis of citizenship was another element of his overview. He also mentioned the questions on the role of policy makers in critical infrastructure and data security. SSL Heartbleed has been a wake-up call for the community, and he will let the speakers provide their input on these topics.

The speakers invited to frame this discussion were:

Keith Bergelt- Open Invention Network (OIN)

Christian Horchert (fukami) – Chaos Computer Club

Michel Lacroix – DG Connect, European Commission

Questions to be addressed include:

- How do we ensure that the necessary resources for the creation and maintenance of reliable, trusted ICT infrastructure are committed, and by whom?
- While the internet is growing to become a public utility, governmental and regulatory support for these efforts is so far mostly absent. What role (if any) should policy makers play in this ecosystem?

Graham then stated that Chatham House Rules will apply, in that the speakers could be quoted, but no other participant in the debates would be quoted in their contributions.

We open the discussion with the comments by **Keith Bergelt** with the Open Invention Network. Keith started his introduction with an explanation of the OIN and the Linux Foundation, who had asked him to speak on their behalf. He provided background on Linux/OSS and its impact in the enterprise and markets, as well as good hygiene in open source development, including copyright licenses, patent licenses, and copyright management. He focused on collaboration and independence as well as patent non-aggression in terms of covenants not to sue (co-opetition). OIN is approaching 1000 licenses and has been involved in technological development of approximately 350 OSS projects. He discussed developers buying into the value of OSS development, and then explained the concept of Heartbleed

and the line of Open SSL code that caused the vulnerability. He described the collaborative culture and how adaptation to this issue was a function of the collaborative community.

He then went into highlights of the Core Infrastructure Initiative (CII) run by the Linux foundation via a discussion on the Linux community and their move to set up with initiative to facilitate investments to identify the problems and to coordinate the code review, infrastructure and audit to address solutions for OSS projects.

CII brought together 4 million USD in capital to assist with the adaptation and healing of the projects impacted. The CII process evaluated which OSS projects could be useful to help address this identified problem and continue to create security authentication roadmap for future direction and address the problems earlier in the process. Each member contributed 100K over three years to contribute. He provided a list of OSS projects that have received initial funding, mainly around SSL, crypto audit, SSH and NTPD implementations. He also showed the list of the advisory board, including kernel developer from Intel and lawyers.

Keith then discussed the impact of Heartbleed SSL and how much of this is human resource cost in building patches, scanning for risk, resetting passwords, and certificate revocation bandwidth. He touched on the stolen data aspect, and the fact the loss is not well defined.

The social phenomenon that is open source and Linux is about the economic principle of increasing returns in turn creating collaborative benefits. He discussed of risk uncertainty and exposure, and complex adaption in the development community. He ended with optimism regarding the viability of OSS projects, the paradigm of collaborative adaptation, and the culture and ethic of development processes with patent non-aggression (OIN).

Christian Horchert (fukami) started his discussion with why his handle is what it is and how it comes from deep thinking (science fiction), and his background in technology security. He is not a paper writer, and has an obsession with DNS. He then explained the Chaos Computer Club.

He is critical on the way the open source community works, but wants to start with the fact that Heartbleed is a benefit to the community to learn from mistakes. When something breaks, you can learn how things could be better. He points out how some historical mistakes can teach us – such for Microsoft for learning to configure and for the secure Windows initiative. This taught us better ways to developing security. So Heartbleed was great in that it could help people to look into the source code of SSL. Only certain parts of the SSL code are okay, but it is not well done. Besides people looking into Open SSL, they also found other serious problems, some of them critical, once Heartbleed SSL was exposed. Outcome should be with very few crypto boundaries, and then should there be more boundaries put in to add protection layers. One boundary is not enough for critical infrastructure.

Vulnerability and disclosure has been shown to be a problem, and many actors came forward in this problem to discuss this, which is a good for security researchers to potentially be able to discuss vulnerability without law enforcement in the U.S. getting involved. Policy needs to be changed so that people can start explaining how things are insecure without policy makers making it criminal to discuss weaknesses in critical infrastructure publicly.

Secure hardware and secure foundation are not there, so running open source on untrusted hardware is not good. He discussed programmable hardware with embedded software, which needs to be addressed in terms of IoE and open source development. He focused on the fact there were many parts to the discussion beyond software development. He ended with saying that being doomed is a good thing, actually. He stated that this discussion was also on how our digital society should develop, and how should these standards be developed and worked with for back-doors by design.

Michel Lacroix began his presentation with a caveat that this is not an official position of the Commission. He started his discussion on incidents vs wake-up call. Personally, he is not convinced this problem was so important and representative of the OSS community, and is a bit of an outlier. Heartbleed can be qualified in his view as a governance problem, the introduction of a custom memory allocator was made the default, did not apparently raise a red flag in the code review. In short, this code was managed by a foundation that did not do its job. Michel commented on the previous comment made by Christian that the code of Open SSL was not good, and he had also heard that it was not highly regarded. So the implication is the community knew and accepted this, which is a governance problem.

As for the wake-up call, it is important is that open source is more and more part of critical infrastructures and we need to be increasingly careful about its security. So a major incident can be welcomed to address this as an issue. If we want to address security in software, we need to adopt more rigorous software engineering approaches. This may meet some reluctance in parts of the OSS community used to concentrate primarily on coding. More techniques from software engineering need to be introduced into the collaborative community as these tools can be of assistance with critical infrastructure development and maintenance. He mentioned funding from DG Connect playing a role in these developments in Europe. He is looking for consultations with open source developers to have openings with the Horizon 2020 programme to look at this.

He commented that how one looks at software in critical infrastructures is similar to approaches such as certification. Certification can be costly, however. He mentioned the bug in the Belgian voting system in the recent May election, and the fact that it had been around for a few years. The government had PWC audited the system, and it should have been addressed.

He then discussed financing and the development of critical infrastructure by the government. There may be mechanisms of developing for the public sector having a knock-on effect for the rest of the infrastructure. But we are still short of the governance that is critical for someone to take over and manage in the long run.

So far we have been discussing components that are critical. But in future, software will be addressed more from a component view and that it will be difficult to assess some of the security properties of the interconnections of the components. So Michel concluded that progress on interoperability will be helpful in address infrastructure development.

Graham opened up the discussion to the floor with his own thoughts. Open source got a bit of a hammering , and he mentioned a quote about taking people off projects when delayed, not adding people, as people can cause the delays. OSS is not always stellar, and should be considered as

potentially flawed as proprietary software. How big a difference would it have been if Heartbleed SSL was proprietary and not OSS?

Christian thought making some open is not necessarily better. Another participant coming from EU projects reflected that development is a failure and you will be wrong the first time, and change from the experience and discussed the concept of uncertainty and risk/failure in development. Code, badly written or that smells, is badly written to the future standards. **Christian** did not agree with this comment.

A participant stated that we are doing integration of technologies, and the discussion then changed to a discussion of procurement of technology and development standards. **Graham** moved the discussion to a comparison of proprietary vs open source as part of the procurement process. Does it matter if it is open source? Does it impact governance?

Christian went back to the fact there is good code out there. The discussion went on to how the crypto code is not stable, and then you see how it can be broken and that it is complicated for those who do not understand what it should do. There are not many cryptographers writing code, which is a challenge. Given the lack of understanding of aspects of the code, misunderstandings occur.

Graham went back to the criticality of SSL and the lack of governance. One participant thought Heartbleed was a design problem. And it needs to have been audited and scrutinized.

Another person who develops suggested that it may not be a problem specific to open source when it comes to governance. However he suggested it was the community had very small numbers of contributors and that having more contributors, more governance and more quality can be related to each other. There are ways to get closer by mandatory review of code and other governance processes. He addressed other commercial software company issues, and discussed if there is a tradeoff between proprietary vs open source is a strong “maybe”.

Graham moved the discussion on others, one who mentioned about the size of the community that developed the SSL code, and that open code does not necessarily mean open source community. He also discussed governance, and developing forks for the SSL code, and if there is a need for a big governance structure. Organised processes can also be open and transparent for other to see and benefit from the collaboration.

Graham took the conversation back to the critical infrastructure and how the contributors quickly found the funds to help address the issue. A contributor said that money does always address the issue, and a further contributor added commentary on the quality of governance being important as stated by a previous speaker.

A person brought up **Michel's** point on verification and regulatory approaches and questioned in terms of the Commission's role in being involved in the oversight of critical code development. Could the Commission be more actively involved from their own projects to help release and quality governance? He mentioned technical committees and responsible code authorship as possible paths. **Michel** mentioned the framework of the research programme as one mechanism, but one of his points was that in defining the research programme, they could add more of the community to add aspects of governance and quality to the definition of the projects.

Graham brought up that neither European companies nor vendors were involved in the Linux Foundation, and how the Commission could be involved in getting the EU more active in the OSS community. Facilitation to the community and pushing collaboration should be a future part of EU projects.

One question from a participant was regarding governance models from a previous participant, and was wondering if model development exists for procurers to see how governance plays a part in security. Coverity is starting to assist in these governance issues, for example.. Another point was made it was not volume of people examining, but transparency to the rest of the community when it does occur is faster in the OSS community than in proprietary world. **Keith** added that open source is very good at self organization but not good at self governance. Accountability also brings obligations to catch and be hyper critical and reflective. He focused on the Linux economic contribution to the OSS community.

One participant discussed the role of government as extra pairs of eyes and resolution to the issues that arise. Another went back to the point of OSS vs proprietary when security issues arise, and but being public is embarrassing but good for resolution. He stated that the Linux Foundation initiative is good, but a few years late. Solutions can have more emphasis on governance and code review, but also suggests the role of what other governments have been doing would be good lessons for the Commission, including financial incentives to the suppliers to enforce governance. However, this person was also discussing criteria for non-legal entities to participate.

Graham summarized that the core issue is governance, and why commercial companies have perhaps different drivers. He spoke about what open source is about, and the community needs to include end users more in these kinds of projects and security issues. He thinks that the community can learn a lot from this Heartbleed SSL situation. He then asked the other three speakers for any final comments.

Michel focused on security as an important property and how to try to get a higher level of sophistication of tools for OSS development.

Christian did not agree on the tool automation, but was looking at crypto complexity as an issue and the need for audit and governance as being important and the environment to be able to talk about vulnerability.

Keith added community participation obligated the need for creative tension and involving in self regulation and it needs to improve. How we have responded to the problem is important, as well as finding the problem.

Graham then concluded the discussion.