A Case Study: Heartbleed Vulnerability Management and Swedish Municipalities

Shao-Fang Wen(✉) and Stewart Kowalski

Faculty of Information Technology and Electrical Engineering,
Norwegian University of Science and Technology, Gjøvik, Norway
{shao-fang.wen, stewart.kowalski}@ntnu.no

Abstract. In Sweden, the use of open source software (OSS) in public sectors has been promoted by the government in recent years. A number of Swedish municipalities forms interest communities to share OSS information and work together with OSS issues. However, it lacks of studies and evidences that these municipalities have adequate routines for managing warnings and advices from the communities on OSS security incidents. The Heartbleed vulnerability that occurred in April 2014 was a sudden case for these municipalities to take remedial actions to protect their information assets in a timely manner. This work aims to take a socio-technical study of how Swedish municipalities utilizes information channels to handle the OSS security incident and their security posture before, during and after the incident. We conducted a case study for Heartbleed incident management in Swedish municipalities, where three municipalities located in different regions of the country were studied. This study used a qualitative research method combining with Security-by-Consensus (SBC) analytical model as a research paradigm for data collection, and processing and analysis. The result suggests that the socio-technical aspects of open source security should be taken into account in Swedish municipalities for OSS adoption and security incident management.

Keywords: Open source software · Heartbleed · Security incident · Socio-technical · Swedish municipalities · SBC model

1 Introduction

On April 7, 2014, news of the Heartbleed bug hit the world. The Finnish company Codenomicon and Google had independently [16] discovered a bug present in the open source software (OSS), OpenSSL. The vulnerability allowed attackers to remotely get sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling from both clients and servers [12, 17]. In Sweden, the use of open source software in the public sector has been promoted by the government [39]. Several municipalities in different parts of the country formed interest organizations to work together with OSS and issue around it. The Heartbleed vulnerability required these municipalities to take remedial actions to protect their information assets in a timely manner. Because of the great impact of the bug, there were also many different information sources to resort to when solving the problem with the

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 414–431, 2017.
DOI: 10.1007/978-3-319-58460-7_29

bug, both official and unofficial The Computer Emergency Response Team-Sweden, CERT-SE, helps Swedish organizations with security issues. CERT-SE sent out security warnings when serious incidents like the Heartbleed bug occurs [7]. On April 4, 2014, rumors about the Heartbleed bug started to spread across the open source community. Codenomicon published a website, www.heartbleed.com, which contained detailed information about the bug; how to update the software and how to update certificates [16]. Swedish media sources started to disseminate information about the Heartbleed bug to the Swedish population, three days after the Heartbleed website was actually released. The majority of the Swedish newspapers did not share any recommendations to the public [11, 13, 22]. Aftonbladet was the only newspaper that actually recommended the public not to visit any servers that might be using OpenSSL and recommended people not to send any secrets on the net [35]. The Swedish Television (SVT) and the Swedish radio (SR) did recommend people to change their passwords [10, 48]. When it comes to Social Media, on 7th of April Facebook announced a message reassuring Facebook users that protection had been implemented and that they continue to monitor the situation closely [16]. The first tweet about the bug came out on April 7, which was made from Adam Langley. The tweet that was about the bug also referred to the Heartbleed website [26].

The problem is that research shows that half a year after the Heartbleed incident the necessary precautions against Heartbleed from various information sources had not been taken by many users of OpenSSL [50]. This work studied how Swedish municipalities handled the Heartbleed incident and their security posture before, during and after the incident. Specifically, this case study will focus on exploring and describing what procedures surround security incidents with OSS and which sources of information are consulted in the process.

1.1 Heartbleed Bug

The naming of Heartbleed is based on Heartbeat, while the Heartbeat is an extension for the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols, it was proposed as a standard in February 2012 by RFC 6520 [8, 12].

The Heartbeat Extension allows either end-point of a TLS connection to detect whether its peer is still present, and was motivated by the need for session management in DTLS [12]. In 2011, one of the RFC's authors, Robin Seggelmann implemented the Heartbeat Extension for OpenSSL. OpenSSL failed to notice a bug in Seggelmann's implementation and introduced the flawed code into OpenSSL's source code repository on December 31, 2011. The vulnerable code was adopted into widespread use with the release of OpenSSL version 1.0.1 on March 14, 2012. Heartbeat support was enabled by default, causing affected versions to be vulnerable by default [46].

The feature, introduced by Seggelmann, enables arbitrary data to be sent from one end of a connection to another. The receiving end would then ping back an exact copy of that same data to prove that the connection is secure, according to a detailed breakdown by The Register [47]. After the initial Heartbeat message is sent, however, the bug tricks the recipient server into spilling out data from its memory instead of just sending back an exact copy of the original data. In short, it enables the server to "bleed" out extra information after receiving a Heartbeat message. The sensitive information that may be retrieved using this vulnerability includes primary key material contains secret keys, secondary key material contains usernames and passwords used by vulnerable services, protected content contains sensitive data used by vulnerable services, and collateral contains memory addresses and content that can be leveraged to bypass exploit mitigations [19, 46].

The Heartbleed vulnerability was originally found by Neel Mehta, a Google computer security employee, in March 2014 [16]. Upon finding the bug and patching its servers, Google notified the core OpenSSL team on April 1. Independently, a security-consulting firm, Codenomicon, found the vulnerability on April 2 and reported it to National Cyber Security Centre Finland (NCSC-FI). After receiving notification those two groups independently discovered the vulnerability, the OpenSSL core team decided to release a patched version.

The public disclosure of Heartbleed started on April 7, 2014, at 17:49 UTC with the version 1.0.1g release announcement [37], followed by the public security advisory [36] released at 20:37 UTC; both announcements were sent to the OpenSSL mailing list. At 18:55 UTC, National Vulnerability Database (NVD) of NIST (National Institution of Standard and Technology, USA) released a Vulnerability Summary for CVE-2014-0160 [33], which is the official reference to this Heartbleed bug.

1.2 About CERT-SE

In Sweden, the Computer Emergency Response Team (CERT-SE), an organization within the Swedish Civil Contingencies Agency (Myndigheten för samhällskydd och beredskap; MSB), deals with and works preemptively with IT-security incidents that affect society [31]. Their assignment is to deliver information of security incidents to those organizations who sign up their mail services. They also communicate and cooperate with other CERT organizations around the world. CERT-SE aims to work for both the private and public sector such as municipalities. At the occurrence of a major IT-incident CERT-SE sends out a warning to organizations who have subscribed to receive an e-mail "flash warning" about serious incidents. For the Heartbleed incident, CERT-SE, in their "flash warning", recommended users of OpenSSL to upgrade to the new OpenSSL version 1.0.1g. Later in their newsletter, they also instructed users to exchange the certificates for the updated software, and other secret data that could have been disclosed due to the bug [6].

2 Related Works

Most of the recent research in Open Source/Heartbleed incident management has largely technology driven. Wu [49] identified the technical procedures and findings of Heartbleed incident management through a real case analysis in a medical school, including sever inventory audit and risk assessment. The difficulties of detecting the Heartbleed vulnerability by a static or a dynamic analysis technique alone have been identified and discussed in [25]. To address such vulnerabilities, some research works focus on building feasible mechanisms for the detection of Heartbleed vulnerability [23, 27, 44].

Other studies have been conducted in the area of OSS adoption and security management. Ramanathan and Iyer [38] identified the influence of outsourcing on OSS and further investigated the factors that impact the adoption of OSS in global Information Technology outsourcing organizations serviced by Indian IT services providers. Their study adopted positivism research philosophy and qualitative approach. Tosi et al. [45] studied the adoption of OSS in the Public Administration in Italy, including the obstacles of their adoption and willingness of stakeholders to proceed with their introduction. Lundell et al. [28] studied the state of practice with respect to OSS in Swedish companies across the small and medium enterprises and large company sectors that have adopted OSS. They analyzed its implications from a number of perspectives, including business motivations and rationale, individual and organizational motivations, and tensions concerning different values (community vs. corporate values).

There is another study on OSS and its use in Swedish municipalities from the Högskolan in Skövde [3]. Focus in that work was on the risks and possibilities during the transfer from proprietary software systems to introduction of OSS in municipalities. The subject of how to deal with security vulnerabilities in OSS is only fleetingly touched upon in this work. The discussion then concerns support and a worry at the municipalities that the support from OSS providers is not as good as for proprietary software. Focus in the study is on risks during the actual migration of software and not management and daily support of OSS.

In our research work, we aim to use a socio-technical analysis approach to form a view on both technical and social aspects of handling Heartbleed incident and obtain an better understanding of the events and causes of action during this incident.

3 Research Approach and Data Collection

The objective of this research is to study security incident management of OSS in Swedish municipalities. The study attempts to answer the following research question: *How does the socio-technical security posture of Swedish municipalities affect the use of official and unofficial sources' warnings and advice concerning Open Source security vulnerabilities?* Swedish municipalities are the unit of analysis in this case study. The study used an exploratory qualitative and the case study approach, which provides a rich and in-depth analysis of OSS incident management of organizations. Qualitative research method is a field of scientific inquiry that crosscuts various disciplines and subject matters. Usually, it uses qualitative data and involves interviews, observations, and document reviews in order to understand human behavior (social and cultural) and the entire environment [5, 32].

In this case, study the problem statement covers areas of IT-security within open source software at municipalities. The focus was on the IT-department, a particular group of people from the chosen municipality. As we wanted to get input from the users, while still allowing for them to think freely to some extent, we chose to use a semi-structured interview as described by May [30]. With a semi-structured interview, the questions are prepared in advance, but the researcher can ask complimentary questions and have a dialogue with the subject. In order to facilitate elaboration, certain possible follow-up questions were prepared beforehand. As we suspected that the subjects would be unwilling to consider themselves behaving insecurely, we also asked about what their colleagues would do. This also has the benefit of covering more subjects.

3.1 Socio-Technical Framework

In order to create questions on the social element of security, we needed a framework describing security that covered both social and technical issues. In this case study, we adopted a socio-technical framework provided by Stewart Kowalski [24], which contains two basic models: a dynamic model of socio-technical changes, called the socio-technical system (Fig. 1), and a static one, called the security-by-consensus (SBC) model or stack (Fig. 2). At the abstract level, the socio-technical system is divided into two subsystems, social and technical. Within a given sub-system, there are further sub-systems. The former (social) has culture and structures, and the latter (technical) has methods and machines. From the system theory/s point of view, inter-dependencies between system levels make a system adjust for attaining equilibrium. The process is referred to as homeostasis state. For instance, if new hardware is introduced into one of the technical sub-systems, for instance, the machine sub-system, the whole system will strive to achieve homeostasis. This suggests that changes in one sub-system may cause disturbances in other sub-systems and consequently to the entire system.

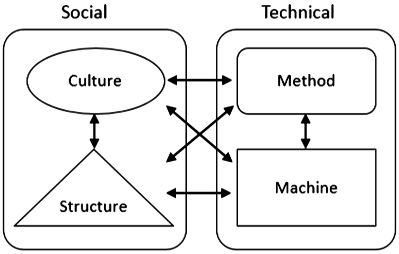

Fig. 1. Socio-technical model (Kowalski [24], p. 10)

Reflecting the static nature of the socio-technical systems, the SBC stack is a multi-level structure that divides security measures into hierarchical levels of control. The social sub-system includes following security measures: ethical and cultural norms, legal and contractual documents, administration and managerial policies, and operational and procedural guidelines. Similarly, the technical sub-system consists mechanical and electronic, hardware, operating systems, application systems, and data. Other aspects are store, process, collect, and communication.

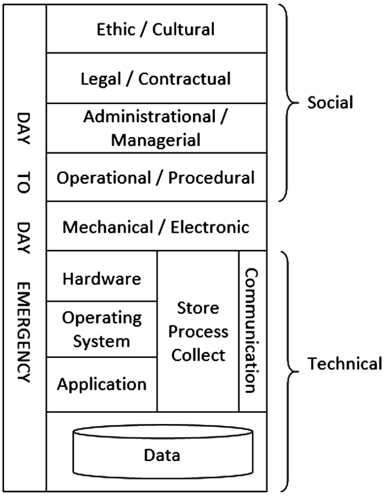

Fig. 2. The SBC model (Kowalski [24], p. 19)

In the socio-technical framework, each system interacts with other systems rather than being an isolated system. Internal and external changes—both social and technical—will affect system security. Therefore, systematic deployment of security measures is required. In particular, this framework has been applied to evaluate threat modeling in software supply chain [1], business process re-engineering [4], a framework for securing e-Government services [19] and an information security maturity model [20]. The application of the socio-technical framework to software analysis is an appropriate and legitimate way of understanding the intrinsic context in open source phenomenon. It provides a way to perform system analysis through a systemic–holistic perspective [21].

3.2 Data Collection

Interview Questions. The interview template that has been made covers specific areas or themes from the problem section to collect data for the research question. Since the research tends to adopt a specific analytical approach called the SBC-model, the interview questions were separated into different categories. Each question is unique and asked only once depending on the respondent. To formulate the questions for the interviews the categories according to the SBC-model were used: Ethical and Cultural, Legal and Contractual, Administration and Managerial, Operational, and Technical. The different categories of questions were not disclosed to the interviewed persons during the interview to prevent the participants from being influenced by them in their answers.

A preliminary test was done on the interview questions, after which slight changes were made on the order in which the questions were asked and how the questions were formulated. By listening to the recording, the researcher became more aware about how the wording and how the formulation of the questions could influence the subject. While the process of developing questions by using the SBC model as a background can be used for most studied organizations, the questions themselves should be adapted to the organization and the people studied.

Below follows a description of the different parts of the SBC-model and a motivation for the questions in each part. The questions were asked in Swedish but translated to English for this paper, and they were not always asked exactly as the same phrases. There might be slight differences in meaning between the languages lost in translation. The actual questions (in both Swedish and English) can be found in Appendix A.

Ethical and cultural: This category handles questions of what is considered morally right and wrong people's values in a society. From the Ethical interview questions, it will be possible to understand if and how social media is a possible tool for the IT-administrators to use. It will also give information about the general handling of IT-risks in the municipality.

Political and legal: Handles questions with regard to how society implements its own laws and rules and its awareness of them. The political and legal interview questions will disclose how well the governments' intent on increasing the use of OSS has been implemented. It will also show if it is political or legal influences of OSS adoption or if it is used on the recommendation from the employees at the IT-department.

Administrative and managerial: Actions aims at creating policies/rules to obtain a high-security level and to ensure activities that facilitate the implementation of policies/rules are in place. The organizational management is important to have for comparison to other municipalities and to show generality for the study. Some of these questions try to clarify the management activities during the Heartbleed incident to understand when and how different information sources were used and how the organization will act in a similar situation in the future.

Operational: This category aims to understand how Heartbleed was handled by concrete security activities at the operational levels.

Technical: This includes computer hardware and software applications. The hardware interview questions will reflect the organization's use of OSS and in what state the applications are in today.

Data Collection

There are 290 municipalities in Sweden [43]. For this case study, the selection of municipality had to be based on certain specific attributes [9]. The criteria were: (1) Municipalities that use OSS. (2) Municipalities that have been affected by the Heartbleed bug; and (3) Municipalities that manage system administration in-house. Sambruk is an organization consisting of Swedish municipalities, formed 10 years ago, with 100 members. Their focus is to coordinate and work together with organizational development and e-governance using open source software and platforms in the municipalities [42]. Because of the use of open source code in the Sambruk interest organization, it was considered a good source to find a suitable candidate for this study within that organization. A selection of Sambruk members around the Stockholm area was contacted to try to convince one or some of them to participate in the case study. The Stockholm area was chosen due to closeness to the interview subjects.

When recruiting municipalities for participation in the study a letter describing the project was sent out to several municipalities, which were known from the Sambruk organization to use OSS. The letter also contained bullet points on subjects that was going to be studied to give the recipient an opportunity to understand the content of the case study.

Three municipalities (M-1, 2, 3) have been considered good candidates for this study because they met the three criteria stated above and the organizations were active on social media like Twitter and Facebook. The result from the case was expected to be representative of other municipalities that meet the three criteria. An investigation of municipalities from and around the Mälardalen region showed that five of eleven municipalities manage their system administration in-house. Municipalities geographically close to each other and belonging to the same County Council (sv. “landsting”) have been found to meet and discuss IT-security. Speculatively, they can indirectly be influenced by each other to embrace the other municipalities’ safety routines and behavior. From the reasons mentioned in this section, results from this report should be possible to generalize to other municipalities that use OSS. Factors that limits how much the findings in the study can be generalized are primarily if the municipalities outsource their IT-administration or not. If they are outsourcing, it can be difficult to know how the security incidents are dealt with. There are a large number of municipalities, judging from collaborations like Sambruk, should encounter the same problems with how to deal with OSS bugs as the studied municipality

The Interviews

The interviews all started with an explanation of the study, ethical aspects etc. During the interviews, other questions than the pre-developed were asked, which was expected in advance. The interviews lasted between 35 and 55 min. They were taped and later transcribed and then sent to the subjects in order to see that there were no major misunderstandings or misquotes after which the interviews were analyzed using qualitative methods. This was sent using e-mail due to practical reasons but it is notable that poor e-mail security might danger the anonymity of the subjects. Different themes and categories in the answers were apparent, and in some cases, the subjects answered in such a way that the answers could easily be compared; in those cases, a comparative analysis was made.

3.3 Ethical Aspects

During the study, the participants were introduced to the subject and the authors. None of the participants were forced to take part and signed the form of consent. At the start of the interview, the subjects were informed again about the aim and method of the study, both orally and in a written document. They were also informed that the interviews would be taped and the tapes stored, but that they would remain anonymous in the study and on the tapes, how the material would be published and also that they could abort the study at any time, without needing to give a reason. Both the subject and the researcher then signed the document. The subjects were also offered a chance to see the transcriptions from their own interviews to ensure that there were no misunderstandings or misquotes.

All the interviews were recorded and the participants were informed about that. After transcription, the results of the interviews were sent to the interviewees for correction of misinterpretation. One ethical concern was that it would be discovered during the study that the studied organizations had not dealt with the Heartbleed bug in a proper way. To be on the safe side, all the organizations were informed about the proper procedure to deal with Heartbleed after the interviews if it was not apparent during the interview that they had updated their systems in a proper way.

4 Findings: Data Analysis and Results

Eight interviews were done. The interviewees all came from IT department: three was female and five were male. The ages were between 25 to 50 years. They had been in IT fields for 4 to 15 years. Below is a summary of the results and analysis in this study. The form used for the analysis is set by the SBC categories.

Ethical/Cultural: All subjects expressed the security awareness of adoption of open source software. Each OSS had a dedicated system administrator, who was responsible to overlook the system and make sure that the patches were applied routinely and effectively. There was no restriction in the use of social media in these three municipalities. Despite that social media delivered the quicker news about Heartbleed than CERT-SE [16], municipalities still relied on the information source of CERT-SE. where they believe they can find trustworthy information. While the Heartbleed occurred, IT departments took most actions in dealing with the vulnerability. There was no information sent out to the users about the bug during and after the incident in M-1 and M-2. M-3 had a simple description of IT measurements in their system maintenance notice, but also did not mention Heartbleed bug in this announcement.

Legal/Contractual: There were no known political or legal pressures or incitements to use OSS in respondent units. It is interesting to note that the promotion of OSS in the public sector by the Swedish government [39] had not fully reached some organizations. There was also no known knowledge about political strategies to implement OSS in the organizations. While there was information on OSS adoption, the documents were not known by most of the subjects, and their actual influence on the day-to-day security work was probably very slight.

Administrational/Managerial: In Swedish municipalities, the IT manager worked on the strategic, tactical, and operational levels. There was an established practice to manage IT systems and OSS products, including audited IT systems periodically, identified people to be responsible for keeping track of OSS products and assessed risks of IT systems. The chain of command at each municipality with regard to report hierarchy was clear. IT managers in the county met up regularly and exchange information about e.g. security incidents like Heartbleed and how to deal with security problems in general that were encountered in their organizations. It helped municipalities network with each other and learn from experiences.

Operational/Procedure: People in charge of maintaining OSS subscribed themselves to respective mailing list from CERT-SE. They would check the threads posted in social media in day-to-day operations, however, when emergency incidents came in, it was thought that they would take longer time for them to filter through all information sources of social media to deal with the security incident. Compared to proprietary software support where they called customer support and know whom they talk to and trust that the support person can solve the problem that they have. There seemed to be a reluctance to contact OSS support even though they thought that they probably would obtain the same service.

Technical: There was a good security coverage on open source products in IT departments, such as installed OSS in intranet only, enabled firewall and updating the patch routinely. However, employees at each municipality that has a municipality owned computer can download any software to that computer. There was no specific policy or technical mechanism for the control of downloading OSS in personal computers.

Using the data acquired in the interviews, we made a judgment on the readiness of the areas surveyed based on frequency of answers, and the impact of the vulnerabilities. It can be seen in Fig. 3 below. On a scale from 0–10, the answers were rated on impact on security. The higher the rating the better influence on security.

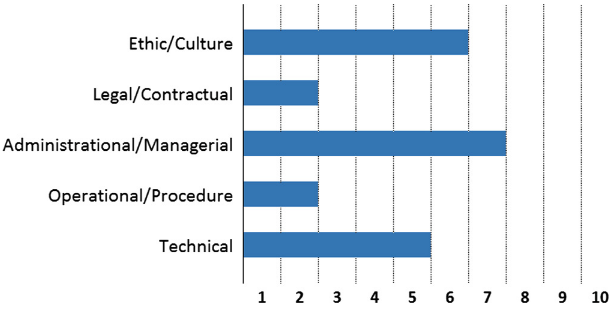

Fig. 3. Result of SBC interpretation

To make it easier to discuss both technical and social aspects of a security incident we use a coordinate system proposed by Alsabbagh and Kowalski [2] which aims to visualize the relationship between operational environment threat metrics and organizational security posture. Using the result from the study, the coordinate system is presented in Fig. 4. In the right-hand part of the graph, the severity of the security incident is displayed, from a social and technical aspect. The left-hand side of the graph shows the perceived posture of the organization towards the security threat studied. The range is set from 1 to 5 on all axis, where the low numbers corresponds to low threat/posture on the x-axis and from less to more complex problems on a social and technical level on the y-axis [2].

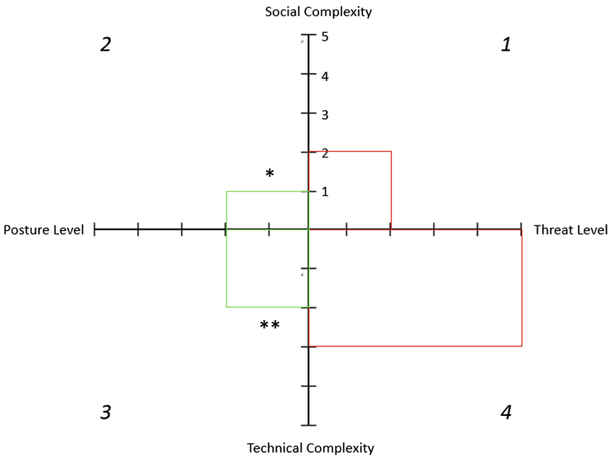

Fig. 4. IS warning coordination system

According to Symantec Security Response [15], by the time of Heartbleed vulnerability announcement, a spam campaign was uncovered using Heartbleed as a way to scare users into installing malware onto their computer. The spam requested that the user run the Heartbleed bug removal tool that was attached to the email in order to "clean" their computer from the infection. This social engineering targets users who may not have enough technical knowledge to know that the Heartbleed bug is not malware and that there is no possibility of it infecting computers. The complexity of this social threat was estimated to level two since attackers have to obtain only employee email addresses, and compose and sent email. This kind of attack is more a discrediting rather than a financial or operational attack so that the severity level suggested here was deemed level two. The technical complexity for causing the problems with the incident was judged to be level 3 because a sample of proof-of-concept scripts was available to be retrieved [14, 29]. Attackers equipped with a certain level of technical skills could use the script to dump a bit of RAM from a vulnerable server. This technical threat could have been very critical if confidential information were disclosed which puts the threat level at four.

The social security posture of the organization was to be medium-low (level 2), since the responsibility and ownership of system administrators were high, however, there was no enough information revealing to users in order to enrich their knowledge and raise security awareness. The complexity of social posture was estimated heuristically to a level 1 because only one official information source was used to find information about how to deal with Heartbleed vulnerability, and there was no political or legal knowledge in implementation OSS in organizations. Both the levels of technical posture and complexity were set to two since the standard countermeasures have been made only within IT systems.

To be able to resolve the potential threat, the posture level should be on the same level as the threat to be able to deal with the problem. If the solution of the threat is less than the actual threat the capability of the organization is not enough to deal with the potential security problem. In this research, the threat level was a lot higher than the low posture level of the organization. This gap between threat and posture is represented by the stars in the Fig. 4. To bridge the gaps (*social, **technical) and be better prepared for security incidents like Heartbleed the municipality would have to take preventative measures that are discussed in the next section.

5 Discussion

The purpose of this study is to investigate whether the socio-technical security posture of Swedish municipalities affects the use of official and unofficial sources' warnings and advice concerning open source security vulnerabilities. It can be shown that even though the municipalities in this study used social media when keeping track of problems with OSS-security incidents they still follow the recommendation that CERT-SE gave. The reason for this seems to be a trust in the official information from CERT-SE in combination with an insecurity of how truthful information from unofficial sources like social media sources on the internet are.

However, several sources in social media conveyed the right course of action to deal with Heartbleed from the start and was faster to publish the news than CERT-SE. To avoid a situation where only one official source of information is trusted it would be beneficial to track other alternative sources when seeking solutions to security vulnerabilities which would mitigate the gap of social complexity in Fig. 1 (*social improvement). Another important aspect is to also follow up on incidents to both make sure that proper preventative measures against the vulnerability has been taken and also improve management of open source downloading and patching (**technical improvement). With the large amount of municipalities using OSS and the government, promoting its use there could also be a national policy on how to deal with OSS in organizations. In March 2015, almost a year after the Heartbleed incident, the Swedish "Riksrevisionen" handed in a petition to the government in which they wanted to have better rules implemented for security management; supervision of security management in the public sector and sanctions for those who don't comply with the regulation should be introduced [41]. These requests are in line with a European Union (EU) directive to ensure a high level of internet- and information security (IS) throughout the EU [40]. The Government also wants to start a national incident report system [41]. An incident report system, from a general Safety, Health, and Environment perspective, used right, will be able to pick up on small "not so dangerous"-events and by learning from those more severe incidents can be avoided [31].

The SBC model result shows a low rating in the Legal/Contractual and Operational categories. This rating could be remedied by the government when they propose a transfer from proprietary software to OSS to reflect over what kind of risks the municipalities run when doing so and make sure that proper policies are in place for operational employees to follow. The security problem that can be seen in connection to the use of OSS in the public sector, stem from a lag in development in method, culture, and structure compared to machine from a socio-technical perspective. The technology is implemented as the software but the method for dealing with a security incident due to a software bug is not robust when the user doesn't have clear methodology for solving the problem i.e. the user doesn't know where to find information about a security incident [24]. A strong culture in an organization forms when the employees follow the rules that are set up for the work processes. In the Heartbleed case, the studied municipalities had to change their routines after the incident, which is a sign of that the original rules were not adequate to deal with the new process of dealing with OSS vulnerabilities. The municipality management in question took the experience with Heartbleed to heart and improved their routines. That type of behavior is evident of good leadership and improves on the structure in the organization [31].

6 Conclusion and Recommendation

In this study, we use conducted a socio-technical study for Heartbleed incident management in Swedish municipalities and used qualitative research method combining with SBC analytical model as a research paradigm. Findings in this study compares to the study from Högskolan in Skövde by Andersson [3] in which the municipalities also were under the impression that OSS support is inferior to support from proprietary software providers. This belief is contradicted by O'Reilly [34] who claims that many OSS has a proven track record of support over many years. The Sonatype survey [18] showed that many of the private organizations didn't have an OSS policy. This study indicates that it might be true for the municipalities, but a larger study needs to be made to confirm that. In the Sonatype study, the general perception was that it is difficult to know how much of the software used in the organization actually contains OSS. A societal consequence of this work could be that municipalities look into how they handle OSS vulnerabilities, which will lead to better policies on OSS bug management. Better OSS security will also derive more secure systems for employees at the municipalities and municipality residents.

The research area could benefit from a more extensive survey into how OSS is managed in the Swedish municipalities with a higher number of municipalities involved. Such a study would give a better understanding of the extent of the problem with OSS management. In such a project, it might be difficult to verify specific information sources to deal with OSS bugs since different incidents would need to use various information sources. It is probably more interesting to develop a process on how to act in the discussed situation and make sure that policies are well founded in the organization. The problem with OSS bugs is not exclusive to the public sector and research, on this subject, into the private sector is just as interesting.

Acknowledgement. The authors would like to thank Katinka Ruda and Armina Arazm for their assistance in this study and doctoral candidate Vasileios Gkioulos for his comments and suggestions.

A Appendix

Annex I: Interview Questions (Swedish)

- På en skala från 1–10 hur beroende är ni av OSS? (Ethical, Managerial)
- Hur många kritiska applikationer har OSS i er organisation? (Managerial, Technical)
- Hur hanterar ni uppdateringar av OSS? (Ex. vilka som ska göras, när, av em)…vem meddelar om uppdateringar? (Managerial, Operational, Technical)
- Hur vet ni när ni ska göra uppdateringar? (Ethic, Operational)
- Gör ni alla uppdateringar? (Ethic, Operational)
- Har alla tillgång till social media på arbetsplatsen? (Ethic, Operational)
- Hur används social media generellt i kommunen? (Ethic, Operational)
- Varför använder ni OSS? (Ethic, Managerial)
- Görs det en riskanalys av säkerhetsläget på kommunen varje år? Har risken med OSS inkluderats i analysen? (Managerial)
- Behövde ni gå ut med information till användarna av systemen som drabbats av Heartbleed I samband med incidenten? (Managerial, Operational)
- Finns det några politiska eller lagstadgade påtryckningar för användningen av OSS? (Legal)
- Hur hanterar ni IT? (Internt, outsourcing, annan lösning) (Managerial)
- Hur ser organisationen ut? (Vem rapporterar IT-ansvarig/du till? Taktisk/Operationell)
- Hur skulle du placera dig själv i en Strategisk, taktisk och operationell modell?
- Vad hände vid Heartbleed-incidenten? (Ethic, Managerial, Operational)
- Hur får ni den informationen of Heartbleed? (Operational)
- Använder ni sociala medier för att få information lite snabbare? (Ethic, Operational)
- Var det någon specifik sida ni var inne på under Heartbleed-incidenten? (Ethic, Operational)
- Skulle du se någon fördel med att ha örat mot sociala medier också? (Ethic, Managerial, Operational)
- Ändrade ni eller skapade nya rutiner/policies efter Heartbleed-incidenten? (Managerial)
- Har ni några speciella regler eller policys som bara rör OSS och inte proprietär mjukvara? Vilka? Vet ni hur andra kommuner hanterar IT? (Legal, Managerial)
- Använder ni några varningssystem för säkerhetsincidenter? (Technical)
- Tycker ni att det är lätt att hitta information om öppen källkod och dess brister? (Ethic, Operational)
- Om man jämför med proprietär mjukvara? (Ethic, Operational)
- Känns det som att det är svårare att få ansvarstagande från OSS-leverantörerna? (Ethic, Operational)

Annex II: Interview Questions (English)

- On a scale from 1–10 how dependent are you on OSS? (Ethical, Managerial)
- How many critical applications has OSS in your organization? (Managerial, Technical)
- How do you handle updates of the OSS? (e.g. What should be done, when, by whom) (Managerial, Operational, Technical)
- How do you know when to make updates? (Ethic, Operational)
- Do you perform all updates? (Ethic, Operational)
- Can anyone use social media at your office? (Ethic, Operational)
- How do you use social media in general in the municipality? (Ethic, Operational)
- Why do you use OSS? (Ethic, Managerial)
- Is there a risk analysis of the system security in the municipality every year? Has the risk of OSS included in the analysis? (Managerial)
- Which information did you give the users of your systems in connection to Heartbleed? (Managerial, Operational)
- Is there any political or legal influence to use OSS? (Legal)
- How do you manage IT? (Internally, outsourcing, another solution) (Managerial)
- How does the organization look like? (Managerial)
- How would you place yourself in a strategically, tactical or an operational model? (Managerial)
- What happened during the Heartbleed incident? (Ethic, Managerial, Operational)
- How do you receive the information about Heartbleed bug? (Operational)
- Do you use social media to obtain information more quickly? (Ethic, Operational)
- Was there any specific page you visited during the Heartbleed incident? (Ethic, Operational)
- Can you see any advantages with keeping an eye on social media too? (Ethic, Managerial, Operational)
- Did you create or change any new routines/policies after the Heartbleed incident? (Managerial)
- Do you have any special rules or policies that concern OSS, not proprietary software? Do you know how other municipalities manage IT? (Legal, Managerial)
- Do you have any warning systems for security incidents? (Technical)
- Do you think it is easy to find information about open source and its deficiencies? (Ethic, Operational)
- If compared with proprietary software? (Ethic, Operational)
- Do you feel that it is harder to get accountability from OSS suppliers? (Ethic, Operational)

References

1. Al Sabbagh, B., Kowalski, S.: A socio-technical framework for threat modeling a software supply chain. In: The 2013 Dewald Roode Workshop on Information Systems Security Research, 4–5 October 2013, Niagara Falls, New York, USA. International Federation for Information Processing (2013)

2. Alsabbagh, B., Kowalski, S.: A cultural adaption model for global cyber security warning systems. In: 5th International Conference on Communications, Networking and Information Technology Dubai, UAE (2011)
3. Andersson, C.: Öppen källkod inom kommuner-Analys av risker och möjligheter. Bachelor. Skövde Högskola, Sweden (2014)
4. Bider, I., Kowalski, S.: A framework for synchronizing human behavior, processes and support systems using a socio-technical approach. In: Bider, I., Gaaloul, K., Krogstie, J., Nurcan, S., Proper, H.A., Schmidt, R., Soffer, P. (eds.) BPMDS/EMMSAD-2014. LNBIP, vol. 175, pp. 109–123. Springer, Heidelberg (2014). doi:10.1007/978-3-662-43745-2_8
5. Bryman, A., Bell, E.: Business Research Methods. Oxford University Press, New York (2015)
6. CERT-SE: BM14-001 - Allvarlig sårbarhet i bash. Blixtmeddelande. 25 September 2014. https://www.cert.se/2014/09/bm14-001-allvarlig-sarbarhet-i-bash
7. CERT-SE: CERT-SE's newsletter v. 17. CERT-SE, 25 April 2014. https://www.cert.se/2014/04/cert-se-s-veckobrev-v-17
8. Datatracker: TLS and DTLS Heartbeat Extension. Datatracker, February 2012. https://datatracker.ietf.org/doc/rfc6520/
9. Denscombe, M.: The Good Research Guide for Small-Scale Research Project, 4th edn. Open University Press, Maidenhead (2010)
10. Dickson, Å.: Buggen visar allt du vill skydda utan att det märks. SVT, 10 April 2014. http://www.svt.se/nyheter/buggen-visar-allt-du-vill-skydda-utan-att-det-marks
11. Drevfjäll, L.: Information från din e-port kan läcka ut. Expressen, 8 April 2014. http://www.expressen.se/nyheter/information-fran-din-e-post-kan-lacka-ut/
12. Durumeric, Z., Kasten, J., Adrian, D., Halderman, J.A., Bailey, M., Li, F., Weaver, N., Amann, J., Beekman, J., Payer, M.: The matter of Heartbleed. In: Proceedings of the 2014 Conference on Internet Measurement Conference. ACM (2014)
13. Eriksson, G.: Nätets "största säkerhetsläcka någonsin" upptäckt. Metro, 8 April 2014. http://www.metro.se/teknik/natets-storsta-sakerhetslacka-nagonsin-upptackt/EVHndh!Wcv38F6U6n8Es/
14. Github: OpenSSL heartbeat PoC. gist.github.com (2014). https://gist.github.com/takeshixx/10107280
15. Graziano, J.: Spam Campaign Spreading Malware Disguised as HeartBleed Bug Virus Removal Tool. Symantec Official Blog, 27 May 2014. http://www.symantec.com/connect/blogs/spam-campaign-spreading-malware-disguised-heartbleed-bug-virus-removal-tool
16. Grubb, B.: Heartbleed disclosure timeline: who knew what and when. Sydney Morning Herald, 15 April 2014. http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140414-zqurk.html
17. Heartbleed: The Heartbleed bug (2014). http://heartbleed.com/
18. Jackson, W.: Sonatype Open Source Development and Application Security Survey. Electronic document (2014). http://img.en25.com/Web/SonatypeInc/%7B138a2551-edac-46a3-bfcb-240352a42fed%7D_2014SurveyResults_july-14-14.pdf
19. Karokola, G., Kowalski, S., Yngstrom, L.: Secure e-government services: towards a framework for integrating it security services into e-government maturity models. In: Information Security South Africa (ISSA). IEEE (2011)
20. Karokola, G., Kowalski, S., Yngström, L.: Towards an information security maturity model for secure e-government services: a stakeholders view. In: HAISA (2011)
21. Karokola, G.R., Kowalski, S., Mwakalinga, G.J., Rukiza, V.: Secure e-government adoption: a case study of Tanzania. In: European Security Conference (2011)
22. Kihlström, S.: Bugg öppnade hål i Krypteringsprogram. Dagens Nyheter, 8 April 2014. http://www.dn.se/ekonomi/bugg-oppnade-hal-i-krypteringsprogram/

23. Kiss, B., Kosmatov, N., Pariente, D., Puccetti, A.: Combining static and dynamic analyses for vulnerability detection: illustration on heartbleed. In: Piterman, N. (ed.) HVC 2015. LNCS, vol. 9434, pp. 39–50. Springer, Cham (2015). doi:10.1007/978-3-319-26287-1_3
24. Kowalski, S.: IT insecurity: a multi-discipline inquiry. Ph.D. thesis, Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden (1994). ISBN: 91-7153-207-2
25. Kupsch, J.A., Miller, B.P.: Why do software assurance tools have problems finding bugs like heartbleed? Continuous Software Assurance Marketplace, 22 April 2014
26. Langley, A.: Time to update all OpenSSL 1.0.1 to 1.0.1g to fix CVE-2014-0160. Twitter, 7 April 2014. https://twitter.com/agl__/status/453235260520542208
27. Lee, C., Yi, L., Tan, L.-H., Goh, W., Lee, B.-S., Yeo, C.-K.: A wavelet entropy-based change point detection on network traffic: a case study of heartbleed vulnerability. In: 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE (2014)
28. Lundell, B., Lings, B., Lindqvist, E.: Open source in Swedish companies: where are we? Inf. Syst. J. **20**(6), 519–535 (2010)
29. Lyne, J.: Heartbleed Roundup: Hacking Made Easy, First Victims Come to Light and Heartbleed Hacker Arrested. forbes.com, 17 April 2014. http://www.forbes.com/sites/jameslyne/2014/04/17/heartbleed-roundup-hacking-made-easy-first-victims-come-to-light-and-heartbleed-hacker-arrested/#3f8fe3e01fe6
30. May, T.: Social Research. Open University Press, Buckingham (2011)
31. MSB: Att lära stort från små incidenter, July 2012. https://www.msb.se/RibData/Filer/pdf/26272.pdf
32. Myers, M.D.: Qualitative Research in Business and Management. SAGE, Thousand Oaks (2013)
33. NIST: Vulnerability Summary for CVE-2014-0160. NVD, 7 April 2014. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
34. O'Reilly, T.: Ten Myths About Open Source Software (1999). http://archive.oreilly.com/lpt/a/2019
35. Persson, I.: Skatteuppgifter stulna i Kanada efter Heartbleed. Omni, 15 April 2014. http://www.aftonbladet.se/nyheter/article18688985.ab
36. Project, O.: OpenSSL Security Advisory. Mail-Archive, 7 April 2014. http://www.mail-archive.com/openssl-users@openssl.org/msg73408.html
37. Project, O.: OpenSSL Version 1.0.1g Released. Mail-Archive, 7 April 2014. http://www.mail-archive.com/openssl-users@openssl.org/msg73407.html
38. Ramanathan, L., Iyer, S.K.: A qualitative study on the adoption of open source software in information technology outsourcing organizations. In: Damiani, E., Frati, F., Riehle, D., Wasserman, Anthony I. (eds.) OSS 2015. IAICT, vol. 451, pp. 103–113. Springer, Cham (2015). doi:10.1007/978-3-319-17837-0_10
39. Regeringen: Från IT-politik för samhället till politik för IT-samhället. Digital document (2004). http://www.regeringen.se/rattsdokument/proposition/2005/07/prop.-200405175/
40. Riksrevisionen: NIS-direktivet. NIS-direktivet (2013). http://www.riksdagen.se/sv/Dokument-Lagar/EU/Fakta-PM-om-EU-forslag/NIS-direktivet_H006FPM68/
41. Riksrevisionen: Riksrevisionens rapport om informationssäkerhet i den civila statsförvaltningen, March 2015. https://data.riksdagen.se/fil/BE7AD878-9C78-4756-95B0-F1617EAB2241
42. Sambrk: Municipalities for Joint Development of e-Services. http://www.sambruk.se/ovrigt/inenglish.4.72ebdc8412fd172bb7480001338.html
43. SKL: Kommuner och Landsting. http://skl.se/tjanster/kommunerlandsting.431.html

44. Torres, G., Liu, C.: Can data-only exploits be detected at runtime using hardware events? A case study of the Heartbleed vulnerability. In: Proceedings of the Hardware and Architectural Support for Security and Privacy 2016. ACM (2016)
45. Tosi, D., Lavazza, L., Morasca, S., Chiappa, M.: Surveying the adoption of FLOSS by public administration local organizations. In: Damiani, E., Frati, F., Riehle, D., Wasserman, Anthony I. (eds.) OSS 2015. IAICT, vol. 451, pp. 114–123. Springer, Cham (2015). doi:10.1007/978-3-319-17837-0_11
46. Wikipedia: Heartbleed. CERT-SE, 25 April 2014. https://en.wikipedia.org/wiki/Heartbleed
47. Williams, C.: Anatomy of OpenSSL's Heartbleed: just four bytes trigger horror bug. TheRegister, 9 April 2014. http://www.theregister.co.uk/2014/04/09/heartbleed_explained/
48. Winter, J.S.: Upphandlare missar inlåsningseffekter. Upphandling24, 18 June 2014. http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5834048
49. Wu, H.: Heartbleed OpenSSL vulnerability: a Forensic Case Study at Medical School. NJMS Advancing Research IT, May 2014. http://research.njms.rutgers.edu/m/it/Publications/docs/Heartbleed_OpenSSL_Vulnerability_a_Forensic_Case_Study_at_Medical_School.pdf
50. Zhang, L., Choffnes, D., Levin, D., Dumitras, T., Mislove, A., Schulman, A., Wilson, C.: Analysis of SSL certificate reissues and revocations in the wake of Heartbleed. In: Proceedings of the 2014 Conference on Internet Measurement Conference. ACM (2014)