DEPARTMENT OF COMPUTER SCIENCE | LUND UNIVERSITY | PRESENTED 2020-06-11

MASTER'S THESIS Sharing is caring: Communicating recipient tailored OSS vulnerability information on an online platform
STUDENTS Emmy Dahl, Michaela Karlsson
SUPERVISOR Martin Hell (LTH)
EXAMINER Martin Höst (LTH)

Sharing is caring

POPULAR SCIENCE PAPER **Emmy Dahl, Michaela Karlsson**

To tackle the increasing number of vulnerabilities in open source software, more and more extensive vulnerability management is needed. Proactive sharing of vulnerability information has never been more important, thus it is of essence for organisations to establish a structured way of communicating vulnerabilities.

Introduction

With IoT and digitisation in general comes initiatives for malicious actors to exploit possible vulnerabilities in the software used. Both the usage of open source software and detected vulnerabilities have increased in the last decade and it is becoming important for companies to know what weaknesses they have in their software systems, to enable secure products. The total cybersecurity of a product often depends on cooperation between several actors. Presently the communication regarding vulnerabilities in organisations is done reactively instead of proactively. This even though research has shown that sensitive information sharing increases the performance of the actors in a network. This insinuates an industrial need for structured communication between organisations regarding software vulnerability management.

As stated above, it exists an industrial need for structured communication between organisations regarding software vulnerability management. An investigative case study into the area can render a differentiation of information recipient groups within companies, as well as suggestions on how communication can be handled and in what way suggested information can be presented to various professional roles. Companies often consist of several employees that contribute to the organisational activities in different ways, depending on what their professional roles are. Different professional roles imply varying employee knowledge of software, vulnerabilities and their importance for the companies, therefore each recipient group needs specific vulnerability information. A possible solution that can improve vulnerability management between industry actors is illustrated in Figure 1.

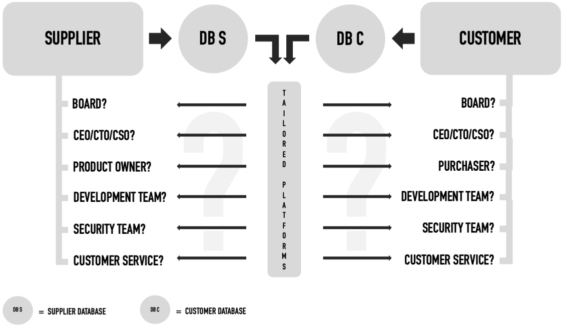

Figure 1: Illustration of the problem formulation.

The Study

The study was conducted as a qualitative case study, consisting of twelve interviews with people that come across vulnerabilities in their everyday work. The interview results were compared to existing theoretical frameworks, to be able to derive prototype views for the online platform. To make the prototype views as accurate and suitable as possible, feedback was collected from the interviewees to verify that the correctness of the information.

The Vulnerability Information Recipient Groups

From the interview results it is clear that the type of professional roles that are mentioned as partakers in the handling of vulnerabilities vary greatly between the different companies. 72% of the mentioned roles are in fact only mentioned by one company. This result is not completely unexpected, since the theory shows that the ways of organising and structuring software development are almost endless. The above leads to the conclusion that trying to identify individual professional roles to design platform views to is difficult and some kind of grouping of recipients is necessary to conduct a feasible solution. The analysis of the interview results show that some recipients are possible to identify as needing certain information. Through this analysis it is therefore possible to group the different professional roles into more prominent recipient groups, that are deemed appropriate for tailoring platform views to. These recipient groups are presented in Table 1.

Table 1: Summary of final recipient groups.

Recipient group	**Information**
Communication function	Less technically detailed information, but enough details to redirect information to the appropriate recipients.
Support function	Less technically detailed information, should be suitable for communication with customers.
Management and Board	Less technically detailed information, more focus on relating vulnerabilities to a business context.
Triage responsible	Technically detailed information, product knowledge and severity scoring to be used as basis for reevaluation.
Development team	Technically detailed information, more focus on remedies than actual triage.
Customer	Not too technically detailed information, straight forward instructions on how to address the issue.

The Vulnerability Information Recipient Onion Model

In an attempt to illustrate the recipient groups' different information needs, a Vulnerability Information Recipient Onion Model (VIROM) is derived from the analysis. VIROM is constructed as follows: The more technically detailed information related to vulnerabilities the recipients need in order to carry out their work duties, the further into to the core of the onion the recipients belongs. Moving towards the outer layers of the onion, the degree of necessary software security knowledge for interpreting and making use of the information declines. Such segmentation of recipients based on their knowledge in software security and need of technical information creates a way of sorting them in a information hierarchical way. As a suggestion VIROM consists of three main layers for a company handling vulnerabilities: The Technical layer, the Organisation layer and the Client layer. To the Technical layer belong recipients of vulnerability information within the company that are heavily involved with the technical aspects of development and vulnerabili-

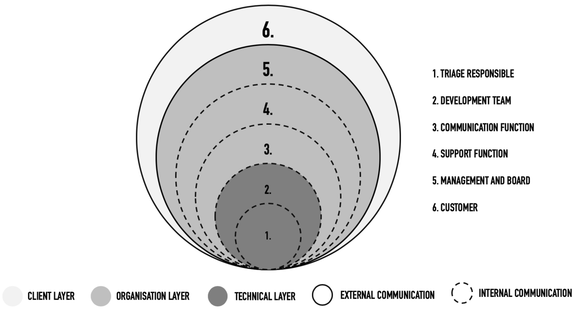

Figure 2: Illustration of final recipient groups sorted according to VIROM.

ties, i.e. triage responsible and development team. To the Organisation layer belong recipients of vulnerability information within the company that have responsibilities within business, communication and customer relations, i.e. management and board, communication function and support function. Finally, external recipients of vulnerability information, i.e. customer, belongs to the Client layer. A graphic presentation of VIROM with the recipient groups is depicted in Figure 2.

Presentation of Vulnerability Information

The results from the analysis of recipient groups and what information they need, resulted in six different prototype views with suggestions of how vulnerability information can be presented on an online platform.

Triage View Since the triage responsible recipient group is heavily involved with the technology aspects of handling vulnerabilities, i.e. making evaluations and assessments of vulnerabilities based on factors such as CVSS details and technical product knowledge, the Triage view concept mirrors this in its layout.

Development View The layout and content of the Development view pages are similar to those of the Triage view. The biggest difference between these views is less focus on evaluation and more on creation of the recommended remedy. Another suggested content difference from the corresponding Triage view is that development teams are not able to make communication requests, as this is restricted to the triage responsible in order for the development teams to solely focus on carrying out the decided measures. Both models emphasise that development teams should not waste valuable time on other tasks than writing and developing code. As much else, this kind of division of duties does of course depends on the requirements and work policies of the company in question. For some companies, some type of two-way communication between development teams and triage responsible carried out from this view is likely of interest.

Comunication Function View The purpose of this view is to address the need of filtering and forwarding vulnerability information, so it is appropriately communicated both internally and externally. This by adding the function of sending communication requests within the organisation. Depending on organisation structure, e.g. who it is that evaluates and fixes vulnerabilities, the originator of the request is likely a development team or the triage responsible, as is shown in this view. By requesting the communication, describing what information should be sent out and who the recipients should be, the information is adjusted and formulated by the receiver of the request and passed on. Receiver of the request is likely PR or technical writers. Requests are sent from company internal stakeholders, but the communication that is requested might also be intended for both internal and external stakeholders, e.g. emails for customers or publications on the website.

Support Function View This view shows information that support functions such as customer support or key account managers should know in order to assist customers that contacts them regarding vulnerability related events.

Management and Board View The purpose of this view is to give management and board an overview of vulnerabilities on a product or product group level, since the interview results shows that this recipient group often do not need to know so much technical details and only want to be made aware of severe incidents. As mentioned before, this varies of course depending on the organisation structure and division of responsibilities between different companies. If the management or board of a specific company is interested in being informed of more technical details, such view pages are adapted for these recipient groups from perhaps the Triage and Development views.

Customer View This view is the only view intended for a company external recipient, a customer. The interview results shows that customers in general want as straight forward information as possible, only be given brief information about what has occurred and what they need to do to fix it. Notice that customers often also are suppliers to other companies, meaning that they might have internal views such as the other described prototype views. One idea is that the type of information shown in this view can perhaps appear when the customer enters their equivalent to the page Information sources from the Triage view and choosing to enter one of their suppliers information flows. According to the analysis, it is likely that the first to receive this kind of information at the customer company are the recipient groups Triage responsible and Development team.

Conclusion

The most prominent recipient groups that are identified are triage responsible, development team, communication function, support function, management and board and finally customer. The recipient groups triage responsible and development team need more technically detailed information, because of their deep involvement with the technical aspects of handling vulnerabilities. Communication function, support function and management and board need vulnerability information that is related to their more business, communication and customer inclined responsibilities. Customer needs information that is as straight forward and solution oriented as possible. Finally, prototype views are designed for each prominent recipient group. These views are called the Triage view, the Development view, the Communication function view, the Support function view, the Management and Board view and finally the Customer view. The final answer to the initial problem formulation is presented in Figure 3.

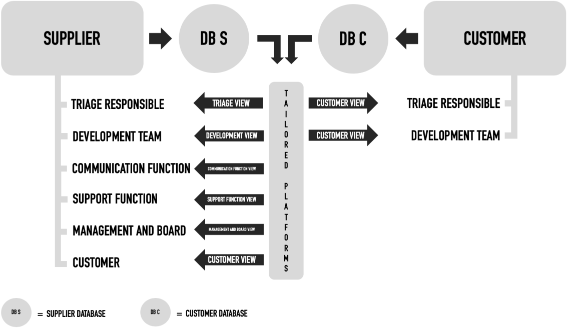

Figure 3: Addressing the problem formulation with answers to the research questions.

Acknowledgment

The authors would like to express their sincere gratitude towards the participating interviewees, for devoting their time and sharing valuable insights to our work. We want to thank Vinnova and the HATCH project for providing a great foundation for our research to be carried out. We also want to thank Debricked for giving us the opportunity to conduct our thesis in collaboration with them and last but not least we would like to thank or supervisor Martin Hell and our examiner Martin Höst for their invaluable support and input. Thank you.