Communication in the Software Vulnerability Reporting Process

Tiina Havana, Juha Röning, Oulu University Secure Programming Group (OUSPG), Computer Engineering Laboratory,
PL 4500, FIN-90014 University of Oulu, Finland.
{thavana, jjr}@ee.oulu.fi

Abstract

Reporting software vulnerabilities to vendors is an essential part of the vulnerability life-cycle and central to software quality development. The present article is based on a study that aimed to interpret the communication network related to security vulnerability reporting and handling process. The organizing of software vulnerability reporting is analyzed, and the differences of opinions between reporters and receivers of the reports are compared. The communication process in a software vulnerability reporting network is described. Knowledge production, mediation, and application in the network are analyzed. Publicity, crisis, and risk management as well as professional ethics, trust, and corporate social responsibility in the network are discussed. The study was based on a quantitative survey that was completed during summer 2002. Snowball sampling was used to reach potential respondents. Altogether 157 valid answers were received, of which 60 were from receivers and 97 from reporters. It was concluded that communication in the software vulnerability reporting process seems often to be one-way, although two-way symmetrical communication could in many cases make the knowledge application easier. It was discerned that especially procedural knowledge, i.e., know-how and know-who, in the reporting process requires development. It was also detected that the combination of information with existing knowledge assets is essential in the receiving organizations. A lack of codification is often typical to the communication process, which may, among other things, have an effect on the development of trust between the communication participants. Also the opinions about the publicity and extent of the disclosures were determined. Overall, both the receivers and reporters agreed on publishing some part of the information after a pre-defined time.

1 Introduction

Due to growth in the usage of information technology, our society has become increasingly dependent on computer security. Attention in the research field of secure computing has most recently focused on pure technical aspects. The challenges in the communication process have been discussed widely, for example, on different mailing lists during the past few years[1]. Many difficulties may occur in the vulnerability reporting process. No consensus exists between groups that take part in the reporting process about the ethically correct disclosure. However, to our knowledge, the communication related to the disclosure of the vulnerabilities has not been studied before.

Creating complex information and communication systems is demanding work. At the moment software products typically contain a large number of different flaws or bugs. Reasons for the emergence of these flaws include human errors, carelessness and ignorance in the design, implementation and management states of the software development process (Arbaugh, Fitchen & McHugh 2000, 52). Some of these flaws lead to software security vulnerabilities. According to the NSA Glossary of Terms Used in Security and Intrusion Detection a vulnerability is "a hardware, firmware, or software flaw that leaves an automated

[1] Several examples of these discussions can be found for example from the Vulnerability disclosure publications and discussion tracking list that is maintained by OUSPG and is available at: http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/.

information system open for potential exploitation". (Stocksdale 1998.) Arbaugh et al. (2000, 53) defines the vulnerability life-cycle as the whole process from the finding of a vulnerability to its repair.

One essential part of the vulnerability life-cycle is its reporting process or disclosure. The bug reporting process refers to the communication process during which the knowledge of a vulnerability is transmitted to persons or organizations that are responsible for fixing the vulnerability or distributing the knowledge about the vulnerability further to other relevant parties, such as software vendors. Software vulnerabilities are disclosed in many ways, e.g. public disclosures, security advisories and security bulletins from vendors. Reporting channels for vulnerabilities can include full disclosure mailing lists, various distribution lists, and sometimes even mainstream media. New vulnerabilities are found by the vendors, by private persons (customers of the vendors or other interested parties), and independent organizations. Vulnerabilities are found during security reviews, quality assurance and normal system operation, and sometimes in more thorough penetration testing. (Laakso, Takanen & Röning 1999, 2.)

The purpose of this article is to describe the main results of a study of the communication process related to software security vulnerability reporting. The aim of the study was to interpret the communication network related to security vulnerability reporting process. We focused on how the information of a vulnerability is received and processed and how the information is managed after the reception. Interesting aspects of this particular communication process include, how people communicate in a crisis situation and how trust is developed in the communication process.

2 The theoretical background of the research

2.1 Disclosing software vulnerabilities

There are three different possibilities for disclosure: 1) full-disclosure, 2) partial-disclosure, and 3) no-disclosure. The publicity for the disclosure may be a) wide public, b) limited public (for example one organization) or c) totally limited public (for example an internal testing team in an organization). The source of a vulnerability report may be a white-hat hacker, a security professional, a vendor, a coordinator or an internal group in a company. Publishing a full report to as wide a public audience as possible has been justified by saying that system security administrators are able to decide what actions need to be taken if they are aware of all aspects of the issue. It has also been suggested that publicity is a way to force the vendors to make patches as soon as possible. (Gordon & Ford 2000, 6.) According to those who support partial and public disclosure or full disclosure with limited publicity, full- and public-disclosures are more harmful than useful, since they may be exploited by criminals. Partial disclosure seems to solve the problems in a no-disclosure policy without giving away the benefits of full-disclosure. However, problems arise because patches are often not ready on the publication day. Even conveying which software system is vulnerable may expose it to attacks. (Gordon & Ford 2000, 6.)

2.2 Communication theoretical aspects

In the present article communication is seen as a process where a state of issues is interpreted and this interpretation is published (i.e. brought into others' knowledge) through interaction in a network. Thus, communication is analyzed from the process school of communication point of view. The central issue is how the messages are transferred – the focus is on communication acts.

Specifically, this article handles organizational communication, i.e. communication between and inside organizations. Juholin (1999, 57-59) has formed a categorization of paradigms that influence organizational communication. The functional paradigm dominates in an organization that sees communication as a management tool and resource, and is prevalent in traditional and hierarchical organizations. According to the functional paradigm, communication is organized and systematic. Conversely the dissipative paradigm describes communication that is dynamic, non-linear and creative. The dissipative paradigm is based on the chaos theory of communication. Dissipative communication may be effective, but predicting the nature and outcome of it is difficult. Juholin (1999, 57) identifies a third paradigm: the dialogic paradigm of communication. A characteristic of organizations, in which the dialogic paradigm dominates is that every member of the organization is active in communication and takes part in it both as a receiver and a sender of messages. Typical of these organizations is a strong communality and that members take responsibility of the organization. (Juholin 1999, 57-59.)

Dozier, Grunig & Grunig (1995, 13) have presented four models of communication. The models can be divided into one-way and two-way models. The one-way communication models emphasize the flow of information from organization to the public. In these cases there are no channels of information from the public back into the organization. When using the two-way asymmetrical model, the organization gathers information about the public, which helps the communicators to develop messages that are most likely to persuade the public to behave as the organization wants. Two-way symmetrical communication seeks to manage conflict and to promote mutual understanding with key public groups. According to Dozier et al. (1995, 13), in this model communicators seek to negotiate solutions to conflicts between their organizations and those groups. The aim is to seek "win-win" solutions to conflicts with the public.

Information transmission and knowledge creation, organizational learning, risk, crisis, and publicity management must be examined in order to analyze the communication in the network. These are handled in more detail in the next chapters.

2.2.1 Knowledge management

Knowledge can be classified as 1) facts or information (know-what), 2) principles that explain (know-why), 3) competence and skills (know-how), and 4) knowledge of the source of the information (know-who) (Lundvall 2000, 14). The central question in the bug reporting process, as well as in many other situations in the world today, is whether knowledge should be private or public and should some of these knowledge types be more public than others. According to Greene and Geddes (1993, 26-49) individuals have two kinds of knowledge: content knowledge and procedural knowledge. This means that people have both intellectual knowledge about things as well as know-how to do things.

Hargreaves (2000, 39) states that information transmission consists of knowledge creation, transmission and interpretation. A closer look reveals that there are actually seven different stages in this process: production, validation, collation, dissemination, adaptation, implementation and institutionalization of the information. In practice these stages do not proceed sequentially since there is feedback from one stage to another. This suggests that the model should be interactive, and therefore process is iterative between knowledge production, mediation, and application. (Hargreaves 2000, 41.)

2.2.2 Organizational learning

Organizational learning is the procedure in which the knowledge is interpreted and used in an organization. Nonaka and Takeuchi (1995, 56-90) have developed a theory of organizational knowledge creation that is based on knowledge conversion, which means the interaction between tacit and explicit knowledge. This conversion happens in four stages: socialization, externalization, combination, and internalization. The theory has been named according to these stages, and is thus called the SECI theory. In the socialization phase the knowledge is tacit and is transmitted in a tacit form. The members of the communication process share their experiences and may transmit know-how (Nonaka & Takeuchi 1995, 62-64). In the externalization phase the tacit knowledge is articulated in an explicit form. This requires that the organization members create concepts, metaphors, analogies, hypotheses or models (Nonaka & Takeuchi 1995, 64). In the third phase, the new explicit knowledge is combined with pre-existing explicit knowledge. The concepts are systematized into a knowledge system (Nonaka & Takeuchi 1995, 67). Finally the explicit knowledge is embodied into tacit knowledge (Nonaka & Takeuchi 1995, 69). Lundvall (2000, 18-19) notes that the transferability of knowledge particularly depends on the extent to which it is tacit. Knowledge is more easily shared if it is codified, but, on the other hand, the impact of codification depends on whether codes are made explicit and hence widely usable.

2.2.3 Risk, crisis, and publicity management

Currently vulnerability disclosure is often a crisis for the vendor. It is a sudden and unexpected notification about weaknesses in products. Lehtonen (1999, 67) has listed things to be done in order to avoid crises. An organization must recognize and list possible risks, imagine what could happen if some of those came true, develop operational models of how to act in the crisis situations, make a communication plan, and finally test that everything works. Fitzpatrick and Rubin (1995, 22-23) describe four possible ways to react to a crisis situation. They based their model on a comparison of the candid public relation strategy and a strategy that they called the legal strategy. The four possible ways according to them are 1) traditional public relations strategy, 2) traditional legal strategy, 3) mixed strategy, and 4) diversionary strategy. By the traditional public relations strategy Fitzpatrick and Rubin refer to the way that traditional public relations advise the companies to react. These include stating the company policy on the issue, investigating the allegations, being candid, voluntarily admitting that the problem exists, if true, and finally announcing and implementing corrective measures as quickly as possible. However, because there is a possibility that any admission of guilt could be used against the organization in a lawsuit, a traditional legal strategy may be used. This includes saying nothing or as little as possible, releasing information as quietly as possible, citing privacy laws, company policies or sensitivity, denying guilt, acting indignant that such charges could have been made, and shifting the blame. In this case the organization understands the meaning of the publicity but thinks that it is a threat to the company's functions. In the mixed strategy the company may also deny fault while at the same time expressing remorse that a problem has occurred. A diversionary strategy means a procedure, in which media and public attention were attempted to be diverted away from the accusations, the media was told that the organization is outraged at the situation, while taking little or no substantive action, and/or the problem was claimed to be solved. The organization tries to manipulate the public’s opinions. (Fitzpatrick & Rubin 1995, 22-23.)

Ikävalko (1996) developed a model of the qualities that affect how an organization can handle publicity. Above all an organization needs an articulated, proactive publicity strategy, knowledge about how publicity works, trustworthy PR-personnel, and direct contacts to media. Thus, it is essential that the organization aims at managing its publicity, not only at benefiting from it. (Ikävalko 1996, 190.) According to Lehtonen (2002, 6) an organization has to integrate three tasks to be successful in publicity management. It has to take care of its relationships to those stakeholders of which it is dependent on, it has to show to its environment that it takes responsibility for its actions, and it has to follow the changes of its stakeholders’ values and expectations, as well as public discussions. Effective publicity management include reputation management, stakeholder strategy, and corporate social responsibility, and reduces the risk of a publicity crisis. (Lehtonen 2002, 38.)

3 Methods

The study was based on a quantitative data analysis of the results of a survey that was conducted during the summer 2002. The participants in the survey were reporters and receivers of the vulnerability information. The total amount of the respondents was 164. 102 of them were from reporters and 62 answers were from receivers of the report. After the invalid answers, i.e. obviously incomplete forms, were removed, there were 60 receivers' answers and 97 reporters' answers left. Altogether there were 157 valid answers.

A quantitative survey is based on information gathered with a questionnaire, which is a self-report measure. The respondents are asked what they think their attitudes, opinions and beliefs about an issue are. The focus is not on behavior, but on how people think they would behave in a certain situation. Thus, questionnaires can measure the subjects' perceptions of a concept, not the concept itself. Finding out people's own ideas of their beliefs and attitudes, as well as behaviors of the related parties, forms the core purpose of the questionnaire. (Black 1999, 36-37.) Two questionnaires, one for the reporters and one for the receivers of the reports, were developed with the help of qualitative group discussion with experts in the field of computer security, working at the Oulu University Secure Programming Group, whom have experience in the reporting process. In this way the validity of the questions were also evaluated. The questionnaire was grouped into four parts. In the first questionnaire, which was for reporters, the first part included questions about the background of the respondents, the second part handled general issues related to the actual reporting process, the third part covered the concrete reporting handling process, and the last section concentrated on specialties in the communication process. The second questionnaire was for receivers of the reports. In this version the same things asked from the reporters were asked, but from the receiver point of view.

Snowball sampling was used to reach the potential respondents. For this reason the respondents form a purposive sample of the population. Snowball sampling is a technique in which subjects with desired traits propose further potential respondents to be contacted. Snowball sampling is an effective sampling method in cases where no lists of population members are available. (Black 1999, 125.) The survey was conducted through the Internet, being the most efficient and inexpensive way to gather the answers from people over a wide geographic area. The survey was advertised to the two CERTs, AusCERT and CERT/CC, and on three mailing lists that reach many professionals in the field. In the advertisement the receivers were asked either to fill in the questionnaire if they belong to the population in question or to send the advertisement to their contacts that are dealing with these issues and for that reason belong to the population in question.

At the end the results of the survey were analyzed with quantitative methods. The statistical analysis of the research was conducted with factor analyses, Mann-Whitney U-tests and χ^2-tests. Some part of the data was simply presented with percentage and mean values.

4 Results and discussion

4.1 The software vulnerability communication network

Figure 1 presents vulnerability information flows and their directions in the communication network. It includes the percentages calculated from the reporters' and receivers' answers about the sources and communication partners that they use in the reporting process. The majority of both the receivers and reporters communicate about vulnerabilities inside their own working group. 38,8% of the reporters send information about vulnerabilities directly to the vendor company. 39,9% of these reporters answered that they talk directly with security experts in the vendor company. 24,5% of the reporters who send information directly to the vendor company are in contact with other professionals of the vendor company who have been instructed about the issue but are not security experts. 12,2% of the reporters who send information directly to the vendor company communicate with people who have no previous knowledge about vulnerabilities. 22% of the receivers answered that in some cases they receive information about the vulnerabilities directly from the reporter. The most common source of vulnerability information for the receivers were coordinators. The answers to the question "whether the respondents talked about the vulnerabilities with their spouse and/or some friends" were compared with an χ^2-test. The statistically significant result was that reporters talk about these issues more often with their spouse and/or some friends.

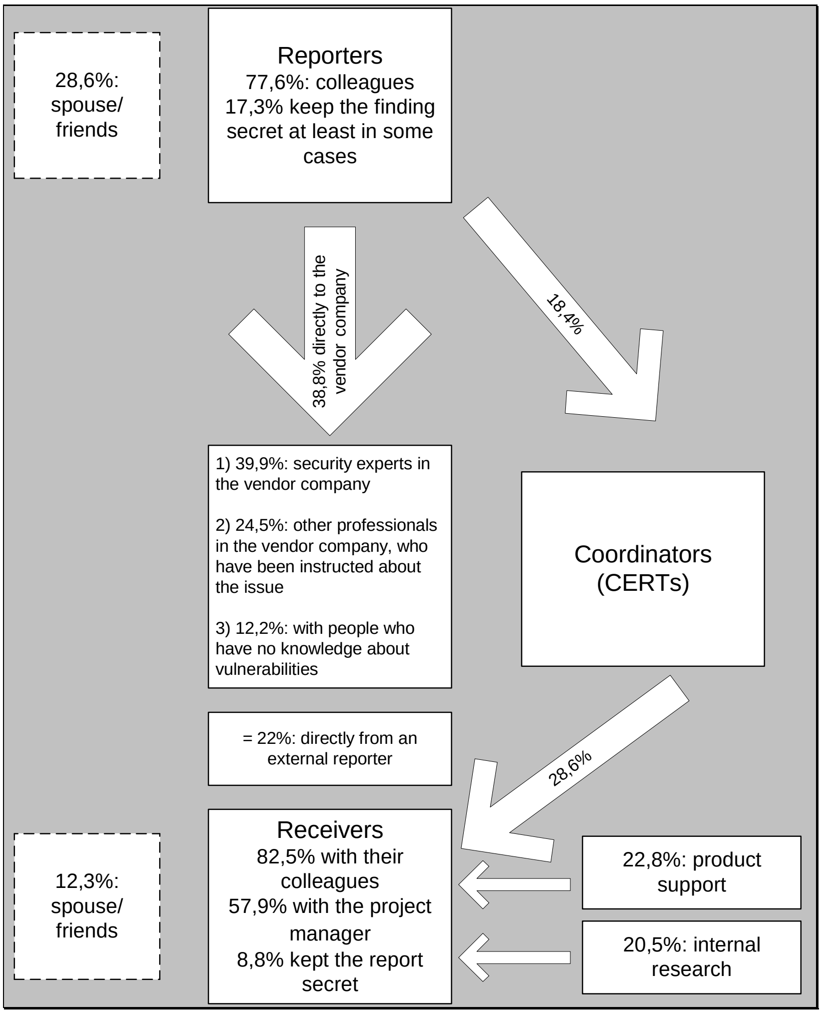
28,6%: spouse/ friends
Reporters
77,6%: colleagues
17,3% keep the finding secret at least in some cases
38,8% directly to the vendor company
18,4%
1) 39,9%: security experts in the vendor company
2) 24,5%: other professionals in the vendor company, who have been instructed about the issue
3) 12,2%: with people who have no knowledge about vulnerabilities
Coordinators (CERTs)
= 22%: directly from an external reporter
28,6%
12,3%: spouse/ friends
Receivers
82,5% with their colleagues
57,9% with the project manager
8,8% kept the report secret
22,8%: product support
20,5%: internal research

FIGURE 1: The vulnerability information flows and their directions

Seven questions in the questionnaire were designed to analyze the respondents' opinions about the communication network. The analysis of these responses was conducted with a factor analysis and three new factors were identified. The new factors were called 1) restricted information transmission in the network, 2) open information transmission in the network, and 3) the amount of network dependence/trust in the network. The comparison between the answers of the two groups, the receivers and the reporters, to these new factors was made with a Mann-Whitney U-test. It was detected that the most significant difference between the groups is in the third factor, i.e. in how the respondents' see trust and dependence on the communication network. The p-value of this result indicates that the result is statistically very significant. Also the answers that were given to questions which form the first factor differ between groups however the result is only marginally significant. On the basis of this analysis it was concluded that the opinions of the two groups about network dependence and trust differ significantly from each other: the receivers trust more in the communication network. They see CERTs more useful than the reporters and believe that their organization is dependent on its contacts to other organizations in the network.

The answers to the question in which the respondents were asked to "name the three values or beliefs that guide one's decisions about security vulnerability information" were analyzed with an χ^2-test. A statistically significant difference in how the two groups see public benefit and the public's right to know was discovered, and they were listed as the three most important values by the reporters more often than by the receivers. The views of valuing recognition of the respondents' own credits also differ between the two groups. The difference is marginally significant. The reporters value recognition of their own credits more that the receivers, even though this was not specifically common for them either. 10 of the 97 reporters said that this issue is one of the three most important values to them, but only one receiver agreed with the statement. Avoiding fear, uncertainty and doubt was more important to the receivers than the reporters. In other cases the two groups were in agreement with each other regarding which things are important. Above all these included security, precision and accuracy, and non-maleficence.

There was a statistically significant difference between the receivers' and reporters' conception about how often receivers contact reporters after having received a vulnerability report. The receivers think that they contact the reporters significantly more often than the reporters think that they are contacted. The result was obtained by comparing the two questions with an χ^2-test. The receivers and reporters agreed with each other that the minimum level of response to the reporter is that the receiver informs the reporter about the priorisation of the report inside the receiver organization. Many of both the receivers and reporters also thought that a simple acknowledgement that the report has been received would be enough.

4.2 Knowledge management in the communication network

In the previous section it was concluded that the knowledge creation process is iterative between knowledge production, mediation and application. This is also the case in the vulnerability reporting process in which the reporters produce knowledge about the vulnerabilities, and mediate it to the vendors, who apply the knowledge in the way they find most appropriate. All the parts of this iterative process are essential to the effective distribution of vulnerability information.

The different knowledge types were classified into four groups: know-what, know-why, know-how and know-who. The first two of these are content knowledge, and the next two procedural knowledge. In the software vulnerability reporting process especially procedural knowledge, know-how and know-who, needs development. For example, this can be seen from the fact that less than half of the reporters indicated that they could not find the right contact persons without problems in most cases. Thus, the know-who -knowledge is not very good. In the survey only 8,2% of the reporters indicated that for finding the right contact persons they use an independent third party, like a national CERT. Actors, such as CERT, could provide the potential to be utilized more efficiently in the communication network.

Content and procedural knowledge help people to act in the right way in a specific context. Routines are developed when a person learns the procedure that helps them to act correctly. A comparison of the working years and the time used per vulnerability by the receivers can be seen as indications about the learning process. In the analysis it was noticed that there is a statistical interdependence between these factors. The experience of the organizations and the respondents in the reporting process were compared with χ^2-tests. The conclusion was that the receivers who answered to the survey, and also their organizations, were more experienced than the reporters or their organization. According to the χ^2-tests the difference between both the experience of the organizations and the experiences of the respondents were statistically significant. This also indicates that in the software vulnerability reporting process some routines are developed.

An important thing to be taken into consideration is that knowledge is more easily shared if it is codified. Tacit knowledge is more difficult to distribute forward inside the organization. This has also been recognized by the organizations with up to 76% of the reporting organizations and 71,9% of the receiving organizations keeping a record of vulnerabilities and their patches. Policies can also be seen as a way of codifying information, and whilst more common in receiving organizations than in reporting organizations, more attention should be focused on them in the organizations that take part in the reporting process. Policies are also a way to improve procedural knowledge in the organization. According to the results the receivers have a more standardized procedure than the reporters do, having more often at least an internal reporting policy. The reporters have a standardized policy less often, and even if they have it is a non-written or internal one and thus is not available to people who are not members of the organization in question.

It is more common for receivers of the reports to have a recognized or advertised point of contact for vulnerability issues than it is for reporters. Approximately two thirds of the receiving organizations and half of the reporting organizations indicated having one, however the difference was marginally significant. This also indicates that the organization has understood the meaning of codifying the information. It also improves procedural knowledge of the people participating in the communication process.

4.3 Organizational learning in the vulnerability reporting network

In the software vulnerability reporting process the stages of Nonaka's and Takeuchi's SECI theory of organizational learning can be observed. In this case the learning process is described as interorganizational learning. The socialization stage refers to the phase when the reporters evaluate the vulnerability inside their own working group, and, if seen necessary, bring the information to others' knowledge. The externalization phase is the stage during which the information is distributed to the vendor. The combination phase is the evaluation phase in the vendor company where the information is compared to the knowledge the vendor has about its products and its significance is evaluated. In the internalization phase the information is embodied in the tacit knowledge, which means in practice the distribution of the knowledge to the software developers in the vendor company.

The survey made it clear that the combination stage inside the receiving organizations is essential. More than half of the respondents (51,8%) indicated that of all the reports their organization had received during the last 12 months less than 20% were valid. This underlines the essentiality of the receiving organizations learning process and knowledge management. On the other hand this raises the question of a more intensive dialog between the reporters and the receivers. There is an obvious need for a dialogical connection between the potential participants for the development of the communication process. The internalization of the information was also evaluated in the survey with the conclusion that little over half (55%) of the receivers pass the information about discovered bugs to their software developers in order to prevent similar vulnerabilities in the future. 15% of the respondents pass the information to their software developers, but this information does not have an essential part in the software development process. Thus, in these organizations, the information is not internalized to create new knowledge.

4.4 Publicity, risk, and crisis management in the communication network

The questionnaire included four statements regarding the receivers' and reporters' opinions about the extent of the disclosure. These were: "All information should be public after a pre-determined time", "All information should be public immediately", "Some part of the information should be public immediately" and "Some part of the information should be public after a pre-determined time". The respondents were asked to give their opinion on the Likert scale, and the answers were analyzed with Mann-Whitney U-tests. A statistically significant difference between the two groups was detected. According to the reporters all information related to software vulnerabilities should be public at least after a predefined time, and they believe more often than receivers that all information should be public immediately, even though they were also pretty skeptic towards this issue. The receivers disagreed with both of these statements. The p-values calculated with the Mann-Whitney U-test indicated statistical significance for both statements that concern publishing all known information, but otherwise the two groups were in agreement with each other about the right procedure. Thus, both the receivers and the reporters thought that some part of the information could, at least in some cases, be published after a pre-determined time. The reporters appear to regard the issue more positively than the receivers, although the difference between the opinions was not statistically significant. Both the receivers and the reporters had a pretty neutral view towards the statement that some part of the information should be public immediately. This refers to agreement about the necessity of publishing some part of the information at least in some cases. Partial disclosure is seen to be the ethically correct way to handle vulnerabilities.

In the questionnaire it was also asked "How, in your opinion, does your organization view publicity related to software vulnerabilities?". It was noticed that the receivers' and the reporters' conceptions about their organizations' relationship with publicity do not differ from each other significantly. Both the receivers and the reporters of the reports see publicity to be important and think that the organization has to inform the media actively. It was discovered that both the receivers and the reporters see publicity in most cases to be primarily positive. Typically, the communication with the media is not dialogical, and most of the organizations seek to inform them actively. However, also seeing the media as an important and equal discussion partner is relatively common. This question was analyzed by determining which ways to react to publicity in a crisis situation the respondents would most probably use, thus, what kind of attitudes the respondents have towards publicity. It was noticed that when related to Fitzpatrick's and Rubin's grouping, the most common strategies are the mixed strategy and the traditional public relations strategy.

In the survey less than one third of the respondents from receiving organizations answered that they have a proactive publicity strategy for a case of publicity crisis concerning vulnerabilities. Nearly half of the receiving organizations but only one third of the reporting organizations had some kind of a reporting policy. Policies are more common in receiving organizations, but still more than half of them are not prepared for a vulnerability report. Approximately one third of the receivers indicated that their organization has PR-personnel who are familiar with vulnerability issues and have direct contacts to the media. This seems to indicate that one third of the receiving organizations are prepared for publicity management related to vulnerability reports. The communication policies can also be seen as preparation for a crisis situation. Surprisingly few of the participants have a crisis or risk management plan, such as a reporting policy. Lehtonen (2002, 12) states that if an organization is prepared for a crisis situation there is a bigger chance that the situations never goes so far. He (2002, 67) also notes that if an organization is prepared for any crisis situation, it is easier to act in a crisis situation that was not expected.

Often, the reporters can be seen as secondary stakeholders of the receivers in the present situation of the software vulnerability reporting process. They are interested in affecting the actions of the receiving organizations, but they do not have a concrete bond to them. Lehtonen (2002, 36) states that relationships to stakeholders can develop from a monolog, through dialog to participative co-operation. All these actions are alternatives for handling the stakeholder relationships. A participative stakeholder strategy is, however, uncommon. Organizations may think that listening to their stakeholders is a signal of weakness or it may think that co-operation could lead to juridical obligations. (Lehtonen 2002, 22.)

According to Lehtonen (2002, 6) in order to be successful in publicity management an organization has to take care of its stakeholder relationships, to show to its environment that it takes responsibility for its actions and to follow the changes of its stakeholders' values and expectations and the public discussions. In the vulnerability reporting process the receivers' most important stakeholders are reporters. The relationship to them could, in the author's opinion, be handled better. This conclusion is drawn from the results of the survey that indicates communication between the two groups is not especially open or conversational. Only one third of the receivers responded that they always contact the reporter after receiving the report. Of course the reporters could also promote communication with the receivers more, and thus they could also handle their stakeholder relationship to receivers better. As stated in the previous section, fast repair of the found vulnerabilities is essential if the company wants to manage its corporate social responsibility. Corporate social responsibility can be seen as a part of publicity management. In order to maintain the public image of the reporters, the reporters should above all handle the reporting in an ethical way. In the survey it was not asked how the respondents follow the changes of their stakeholders' values and expectations, and public discussions, and thus the last point of Lehtonen's statement can not be commented on in this context.

In the context of vulnerability reporting an indication of corporate social responsibility is that the receiving organization seeks to eliminate the vulnerability as soon and effectively as possible. This is an expression to the environment that the receivers take responsibility for their actions. The survey evaluated this by asking the receivers how they react to the vulnerability reports. The conclusion was that only 13,3% of the receivers put the reports aside to wait for a suitable time to handle them. The rest of the respondents handle them in the priority order, interrupting other work immediately when they receive a report and concentrating on the repairing process, or have alternatively formed a specific schedule within which the reports are supposed to be handled. Thus, from the corporate social responsibility point of view, it can be argued that an attempt is made to handle vulnerability reports fast and effectively in most of the receiving organizations, and that corporate social responsibility is managed effectively. However, it must be taken into consideration that the answers may also be biased by pure reputation management.

5 Conclusions

In this study communication was seen as an information interpretation and publication process through interaction in a network. The various characteristics of this specific network were presented in this article.

The preconception, based on the Juholin's categorization as presented in Chapter 2, was that there might be a difference between the receiving and reporting organizations' communication paradigms. This seems to be the case, but the interpretation must be evaluated with care. The theoretical concepts of communication paradigms form an interesting view on the issue, but the conclusions about the paradigms in the vulnerability scene would need more thorough data. However, when this is taken into account, some tentative conclusions can be made. The receivers of the reports seem to have more faith in the reporting network, and be more dependent on it than the reporters. They also typically support restricted information transmission, more often have a reporting policy and more often think that only some part of the information should be published. These things indicate a functional communication paradigm. According to the receivers of the reports the information transmission should be codified and organized. On the other hand, the reporters seem to value a more dissipative paradigm of communication. Reporting policies are not as common as for the receivers, and the reporters seem more often to do the reporting without prior planning. They also discuss about the issues with outsiders more often than the receivers. Communication seems to be more dynamic and creative than for the receivers. Dynamics and creativeness are typical characteristics of a dissipative communication paradigm. Meanwhile, the dialogic paradigm of communication does not have a big part in the reporting process. The respondents think that the participants should have regular discussions about vulnerabilities, but this is quite seldom the case in reality. Even getting some kind of response to the report may be hard. Communality is not a characteristic for the vulnerability reporting process.

As noted previously, according to Dozier, Grunig & Grunig (1995, 13) a win-win relationship can be developed with symmetrical two-way communication. However, in software vulnerability communication the flow of information seems relatively often to be one-way, which can be noticed, for example, from the fact that getting a response to a report appears to be difficult. Even if the receiver would give a response to the reporter, a dialog between the two parties is not necessarily the standard procedure. In the author's opinion communication in the software vulnerability reporting process requires the usage of two-way symmetrical communication, because with two-way symmetrical communication organizational learning can be possible.

Argyris and Schön (1978, 18-26) describe organizational learning as taking place in two phases. According to them there can be single-loop learning, which means that the aim is to trace and fix an error within the scope of existing rules and norms. Double-loop learning happens when these existing rules are opened to question. One of the aims of the software vulnerability reporting process is to improve the quality of software systems, and this can be achieved if the developers learn to make software that is originally secure. This learning is possible if the existing norms of the software development process are re-estimated, thus double-loop learning is achieved.

The receivers and reporters seem to have a different view about the ethically correct way to view software vulnerability reporting. This is an interesting phenomenon, because it indicates that the two groups are not unanimous about professionalism in the field. The field is very new compared to many other professions, which may be one reason why the common rules for the right procedure have not yet been fully developed. There is a need for an international codification of the rules that could help the disclosure policies. Professionals posses and exercise legitimate authority to act in the way that their profession is entitled to, when they actually promote general benefit. In the survey it was observed that the reporters value general benefit (public benefit and the public's right to know) about the issues to be more important than the receivers of the reports. Thus, the reporters' attitudes toward general benefit are more positive. They see their work to be useful for the whole society. The receivers see the issue to be important first and foremost for their company, and the company's role is to promote general benefit – it is not primarily their personal task.

In the software vulnerability reporting process the reporters' and receivers' stakeholder relationship could be classified as being somewhere between a monolog and a dialog. This conclusion can be made on the basis of the survey, in which it was discovered that the participants rarely have regular communication with each other. However, in the factor analyses made about the participants' opinions of open information transmission in the network, it was noticed that both the receivers and the reporters agreed that communication between all the parties should be more intensive.

The vulnerability life-cycle was defined as the process from the finding of a vulnerability to its repair (Arbaugh et al. 2000, 53) However, it can be argued that the vulnerability life-cycle starts from the introduction of the vulnerability and ends with the elimination of it. This is a fundamental difference from the liability point of view. If it is seen that the vulnerability life-cycle starts at finding the vulnerability, the finder can be claimed to be responsible for it. If, however, the vulnerability life-cycle is seen to start at the point in which the vulnerability is created, the vendor is responsible for it. The liability issues also effect trust in the communication network.

In crisis communication theory it is traditionally recommended that a notification about the issue should be given to all people who are concerned with the issue in a short time frame. This is advised to be done even if all the necessary information about future actions is not available. The related parties should be told what is known at the moment and the necessary details should be given as soon as they are known. (Wilcox 2000, 181-182.) However, the vulnerability reporting process is a somewhat exceptional case. At the point in which the vulnerability is found, the most essential aspect is to get it repaired, and the situation has not yet escalated to a crisis. The escalation is possible if information about the vulnerability is made public too early. For this reason software security professionals often oppose a full and public report that is written immediately after the vulnerability has been found. The consensus is to first inform only the vendor, giving the vendor enough time to develop the patch and then publish the patch. After that it is possible to publish a full report if that is wanted. (Deline 2000.) In this way only a small circle of people knows about the vulnerability before it has been repaired.

Publicity management related to the vulnerability reporting process has many interesting specialties compared to typical publicity management of an organization. Keeping things secret at least to some point is seen to be the ethically correct way to handle the disclosure, which is not the way that publicity management is usually recommended to be handled. In this context it seems, however, to be the most secure and effective way. Trust and risk go hand in hand. The potentiality of a crisis situation affects on communication. At the moment trust between the two parties is developed separately in every reporting process, again and again. Trust is not something that fundamentally belongs to the nature of the relationships. The reason for this is at least partially the lack of codification in the communication process.

This research gives many possibilities for future studies. During the research it was noticed how many-sided communication in the software vulnerability reporting process actually is. Each of the diverse sides of communication give opportunities to look at the issue in more detail. Interesting viewpoints would be for example to conduct qualitative research by making a group/personal interview to get deeper understanding about the opinions of the participants of the reporting process. A comparison of existing company documents, for example existing reporting policies, would also give an interesting point of view to the issue. A wider perspective would be of great interest: how does the information or knowledge about computer security influence the behavior of computer users. Overall, while this research was based on a self-report measurement practice, the results must be related to the fact that they are people’s opinions about the issue. An observation about the vulnerability reporting process could give many new points of view to the analysis.

References

Arbaugh, W. A.; Fitchen, W. L. & McHugh, J. 2000. Windows of vulnerability. A Case Study Analysis. IEEE Computer. Vol. 33, No. 12.

Argyris, C. & Schön, D. A. 1978. Organizational learning. A theory of action perspective. Reading, Massachusetts: Addison-Wesley.

Black, T. R. 1999. Doing Quantitative Research in the Social Sciences. An Integrated Approach to Research Design, Measurement and Statistics. London: Sage Publications Ltd.

Deline, B. 2000. Full disclosure. SANS Institute - Information Security Reading Room. Available in www-form: http://www.sans.org/infosecFAQ/hackers/disclosure.htm.

Dozier, D. M., Grunig, L. A. & Grunig, J. E. 1995. Manager's guide to excellence in public relations and communication management. New Yersey: Lawrence Erlbaum Associates Inc.

Fitzpatrick, K. R. & Rubin, M. S. 1995. Public relations vs. legal strategies in organizational crisis decisions. Public Relations Review 21/1: 21-34.

Gordon, S. & Ford, R. 2000. When the worlds collide. Information sharing for the Security and Antivirus Communities. Brussels: EICAR 2000 Best Paper Proceedings, 1-20.

Greene, J. O. & Geddes, D. 1993. An Action Assembly Perspective on Social Skill. Communication Theory 3/1993: 26-49.

Hargreaves, D. 2000. The Production, Mediation, and Use of Knowledge in Different Sectors. In: Knowledge Management in the Learning Society. 2000, 37-66. Paris: OECD (Organization for Economic Co-operation and Development).

Ikävalko, E. 1996. Ylivoimapeli mediassa. Julkisuusmekanismit ja julkisuuden hallinta. Helsinki: Inforviestintä Oy.

Juholin, E. 1999. Paradise lost or regained? The meanings and perceptions of organizational communication of 1990's in Finnish work organizations. Helsinki: Inforviestintä Oy.

Laakso, M.; Takanen, A. & Röning, J. 1999. The Vulnerability Process: A Tiger Team Approach to Resolving Vulnerability Cases. In the proceedings of the 11th FIRST Conference on Computer Security Incident Handling and Response. Brisbane. 13th to 18th June 1999. Available in www-form: http://www.ee.oulu.fi/research/ouspg/protos/sota/FIRST1999-process/

Lehtonen, J. 2002. Julkisuuden riskit. Helsinki: Mainostajien liitto.

Lehtonen, J. 1999. Kriisiviestintä. Helsinki: Mainostajien liitto.

Lundvall, B. Å. 2000. Understanding the Role of Education in the Learning Economy. The Contribution of Economics. In: Knowledge Management in the Learning Society. 2000, 11-35. Paris: OECD (Organization for Economic Co-operation and Development).

Nonaka, I. & Takeuchi, H. 1995. The Knowledge-Creating Company. How Japanese Create the Dynamics of Innovation. Oxford: Oxford University Press.

Stocksdale, G. 1998. NSA Glossary of Terms Used in Security and Intrusion Detection. Available in www-form: http://www.sans.org/newlook/resources/glossary.htm.

Wilcox, D. L. 2000. Public relations. Strategies and tactics. New York: Addison-Wesley Educational Publishers Inc.