Oulu University Secure Programming Group

Communication in the Software Vulnerability Reporting Process

Oulu

Communication in the Software Vulnerability Reporting Process

Index

Oulu University Secure Programming Group (OUSPG) 2003

ISBN 951-42-7072-X

Professor Juha Röning
University of Oulu
Department of Electrical and
Information Engineering

Foreword

Modern society is inevitably dependent upon undisturbed information flow. In every level of our society, communication forms the basis of working interactions. Failure to communicate is a major factor in creating or exacerbating problems in the workplace. In a crisis situation, poor communication will have an amplifying effect. In the minimum it will cause "bad will" within the company; in the extreme it can threaten its entire future.

This report deals with communication of vulnerabilities in software systems. Reporting software vulnerabilities to vendors is an essential part of the vulnerability life-cycle and central to quality software development. The hard fact is that software vulnerabilities will be discovered, disclosed and abused. Bruce Schneier has said: "Security is a process, not a product". It is crucial that this part of the process is handled properly.

1. Introduction

"Fragile and insecure software continues to be a major threat to a society increasingly reliant on complex software systems."

- Anup Ghosh
[Risks Digest 21.30]

Due to growth in the usage of information technology, our society has become increasingly dependent on computer security. At the moment software products typically contain a large number of different flaws that have arisen due to human errors, carelessness and ignorance in the software development process. Some of these flaws lead to software security vulnerabilities. Reporting software vulnerabilities to vendors is an essential part of the vulnerability life-cycle and central to software quality improvement.

The vulnerability reporting process refers to the communication in which the knowledge of a vulnerability is transmitted to the persons or organizations whom are responsible for fixing the vulnerability or distributing the knowledge of the vulnerability to other relevant parties, such as the coordinators of the reporting process. 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.)

This brochure presents the main results of a quantitative survey on the vulnerability reporting process that was conducted during summer 2002. It includes several examples of issues related to the vulnerability handling process, and aims to illustrate the whole process of vulnerability handling. The organizing of software vulnerability reporting is analyzed, and the opinions of reporters and the report recipients are compared. One of our aims in this brochure is to emphasize the essentiality of effective and fluent communication. Communication is by no means easy. Various factors affect it, especially knowledge, publicity, and crisis management. These are important factors to be taken into consideration when the vulnerability handling process is developed. According to the results of the survey a more codified reporting approach could bring benefits in many cases. More emphasis should be put on knowledge, publicity, and crisis management in organizations that take part in the process.

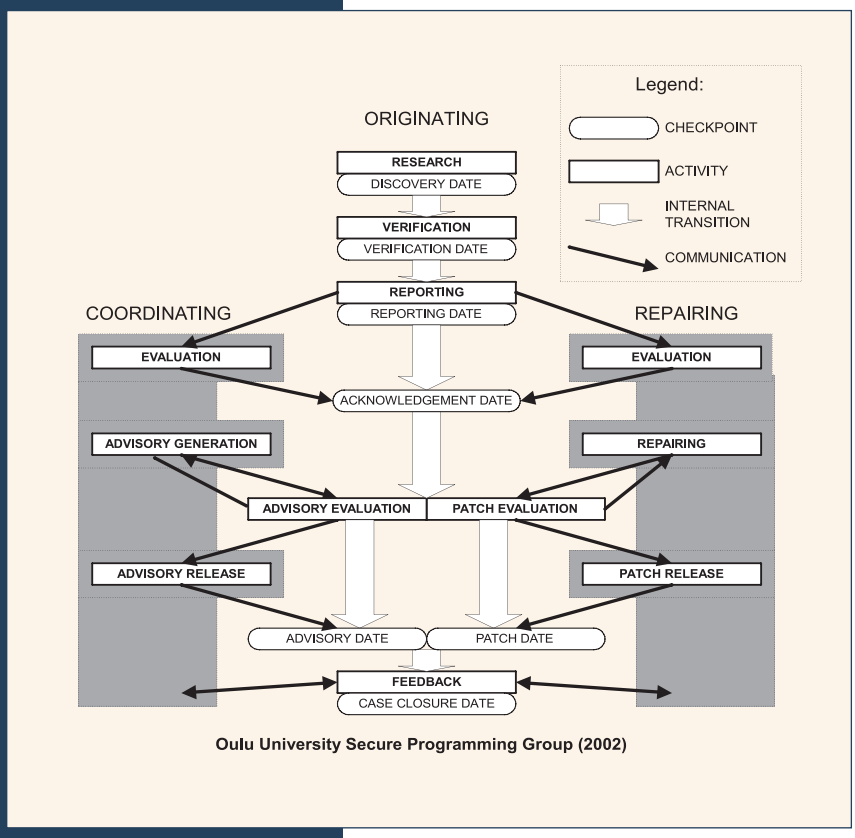


Figure 1: Model of a vulnerability life-cycle

2. The survey

The purpose of the research was to investigate how the communication of the vulnerabilities is organized in practice, what kind of views people participating in the software vulnerability reporting process have about different aspects of it, and what differences there are in the way reporters and report recipients see the process. The focus is on the respondents' opinions about how the reporting should be handled. During summer 2002 a quantitative survey was conducted. The survey covered issues such as which channels are used to transfer information, how the right contact persons are found, and who is informed about the vulnerability. The opinions of the respondents regarding the vulnerability reporting process was also described. The aim of the work was to analyze what kind of knowledge relates to the vulnerability reporting process, how this knowledge is transmitted in the communication network and how public this knowledge should be.

2.1 The research methods

To answer the research questions of this study, a quantitative survey. Two questionnaires, one for the reporters and one for the report recipients, were developed with the help of a qualitative group discussion with the professionals at the OUSPG (Oulu University Secure Programming Group). At the end the results of the survey was analyzed with quantitative methods.

Snowball sampling technique was used to reach the potential respondents. The survey was advertised to the two CERTs, AusCERT and CERT/CC, and on three public disclosure mailing lists that reach many professionals in the field. In the advertisement readers were asked to either fill in the questionnaire, if they belong to the population in question, or to send the advertisement to their contacts that deal with these issues and for that reason belong to the population in question. The survey was conducted through the Internet.

Altogether 164 responses were received from the survey. 102 of them were from reporters, 62 answers were from report recipients. After the invalid answers, i.e. obviously incomplete forms, were removed, there were 97 reporters' answers and 60 receivers' answers left, a total of 157 valid answers. The statistical analysis of the results was conducted with the help of factor analysis, ^{2}-tests, and Mann-Whitney U-tests.

2.2 The respondents

Most of the respondents were young, male, and from western countries.

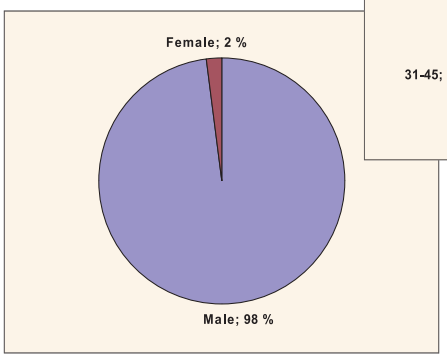


Figure 3: Gender of the respondents

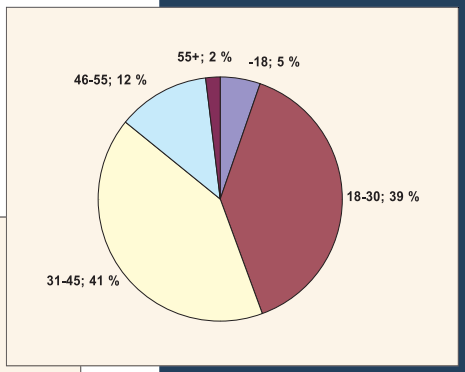


Figure 2: Age of the respondents

The education level of the respondents was relatively high. Nearly all of the respondents had at least some academic education. On the other hand, only 16 % of the respondents had a higher level academic degree.

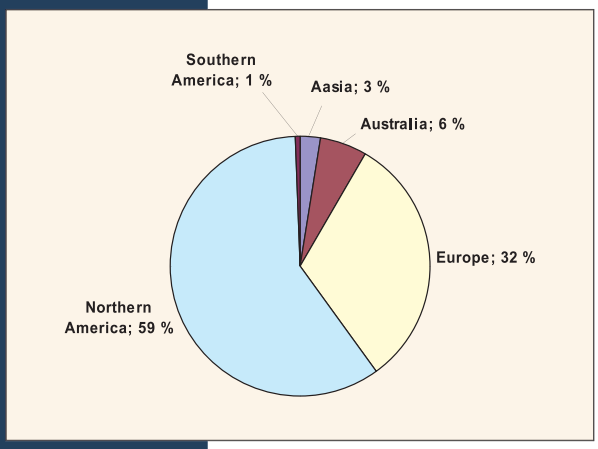


Figure 4: Locations of the respondents' organizations

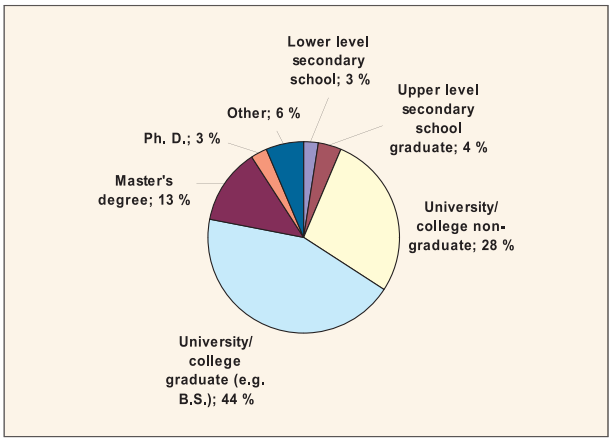


Figure 5: Respondents' education level

The respondents came from both private and public sector organizations. Approximately half of the respondents' organizations operated in ICT-business.

More than half of the respondents worked in organizations that had less than 100 employees, although there was also responses from employees of very large companies.

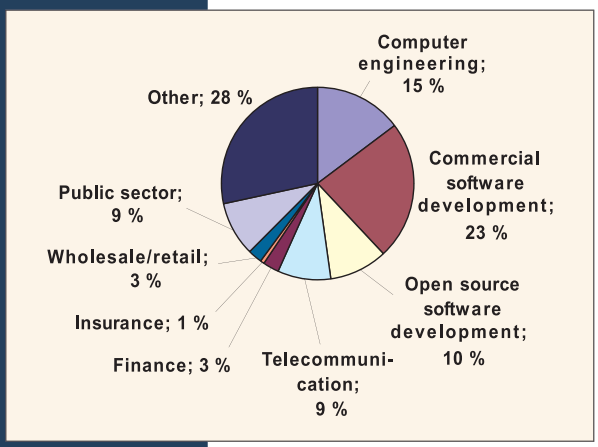


Figure 6: The industries of the respondents' organizations

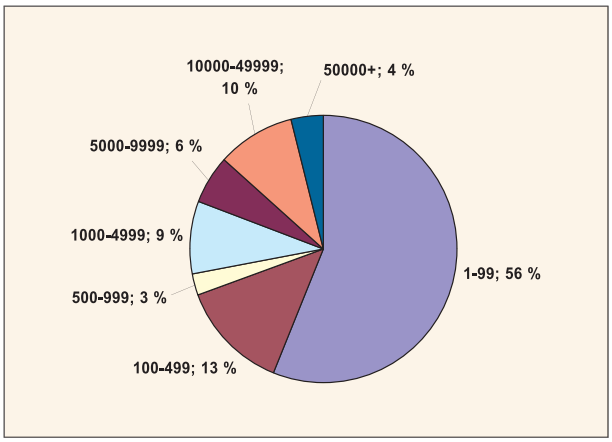


Figure 7: Number of employees in the respondents' organizations

3. Communication network

– *Sources and channels of vulnerability information*

Communication is a process in which a state of issues is interpreted and this interpretation is published (i.e. brought into others' knowledge) through interaction in a network. In the vulnerability handling process the communication network consists of the originators of the information (i.e. the reporters), the coordinators and the repairers (i.e. the receivers). Communication channels and information flows are essential parts of the vulnerability reporting network. In the survey, values and beliefs of the respondents concerning transmission of vulnerability information as investigated. Values and beliefs about the procedure affect the communication remarkably.

Most of those reporting vulnerabilities, learn of them during their own work or by accident. Internal testing groups are also relatively common sources of information, but other sources are clearly less common.

The statistics on information sources and communication channels are frequencies of the reported answers. Despite there being only 157 respondents, the total number of answers to the same question may be nearly 200, as the respondents were able to give more than one answer to each of these questions.

Email is the most common reporting channel. Both encrypted and non-encrypted emails are used. The recipients of vulnerability reports indicated that they receive the information about vulnerabilities through web-based reporting forms and media more often than the reporters indicated that they send the information through these channels.

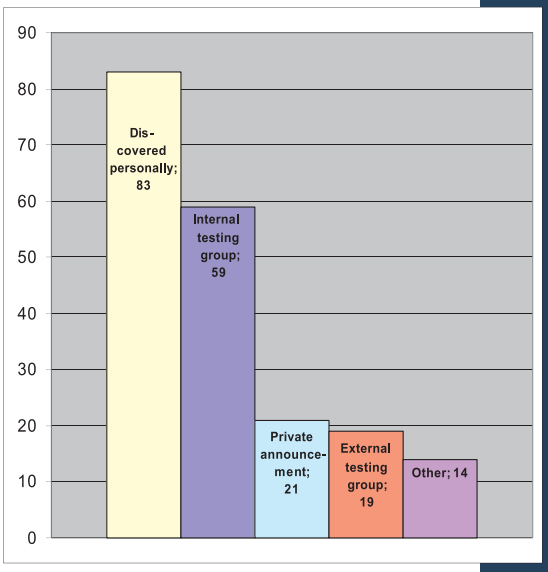


Figure 8: Reporters' information sources

Case	Number of emails	Case	Number of emails
1	*4*	*11*	*9*
2	*2*	*12*	*24*
3	*8*	*13*	*3*
4	*5*	*14*	*19*
5	*0*	*15*	*37*
6	*0*	*16*	*12*
7	*3*	*17*	*26*
8	*0*	*18*	*489*
9	*1*	*19*	*14*
10	*3*	*20*	*19*

Table 1: Examples of number of emails per reported vulnerability at OUSPG.

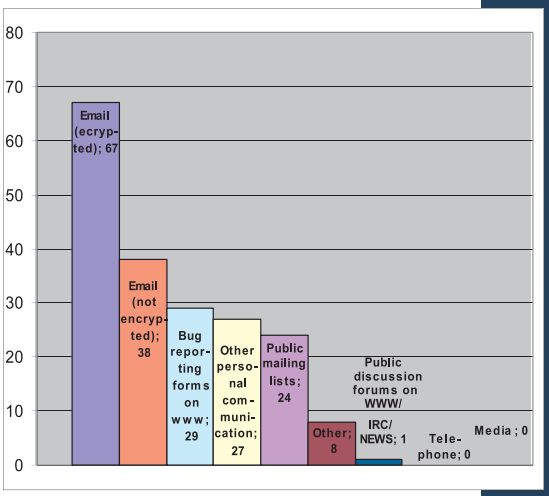


Figure 9: Reporting channels

Year	1995	1996	1997	1998	1999	2000	2001	2002
Vulnerabilities	171	345	311	262	417	1090	2437	4129

Table 2: Vulnerabilities reported, CERT/CC (http://www.cert.org/stats/cert_stats.html)

The report recipients' most common information source was a national CERT or alike. Other sources were product support, external reporters and internal research, which all were relatively common as well.

The communication network is presented in Figure 12. It shows the information flows related to the vulnerability reporting, and the directions of these flows. The percent values in the figure represent the amount of the respondents that indicated that they handle the communication through the channel in question. The values were calculated from the reporters' and recipients' responses regarding the sources and communication partners that they use in the reporting process. For example nearly 1/3 of the reporters but only 12,3% of the recipients reported that they discuss the issues with their spouse or friends.

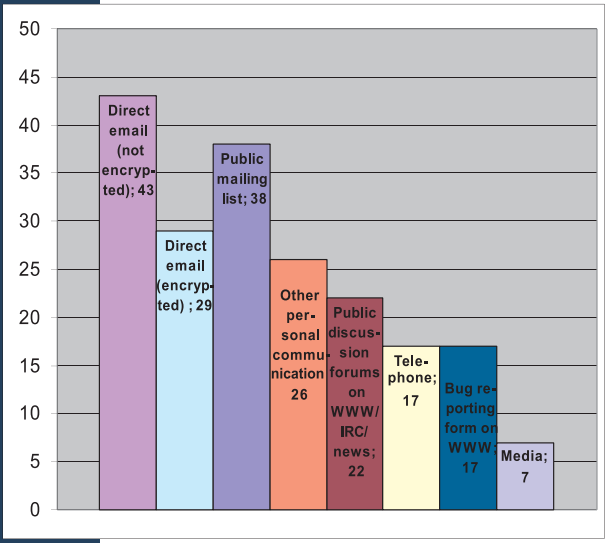


Figure 10: Receivers communication channels

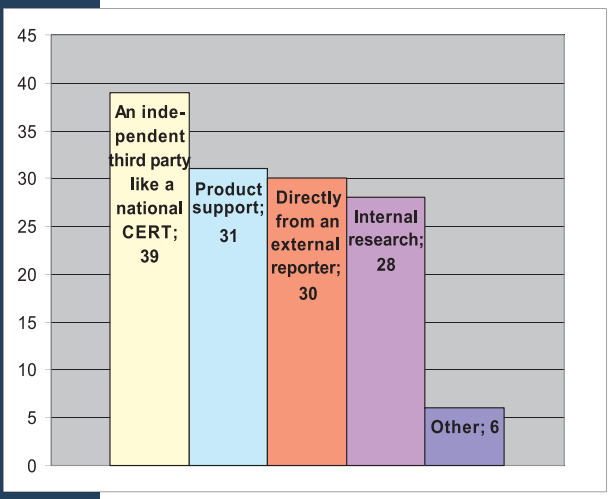


Figure 11: Receivers' information sources

The majority of both the reporters and the recipients discuss the vulnerabilities inside their own working group. 38,8% of the reporters send information about the vulnerabilities directly to the vendor company. 22% of the report recipients indicated that at least in some cases they receive information about the vulnerabilities directly from the reporter. The most common source of vulnerability information for the recipients were the coordinators.

Finding contact persons was somewhat problematic to many of the vulnerability reporters. 20,6% answered that they rarely find the right contact persons without problem.

In software vulnerability communication the flow of information seems to relatively often be one-way. For example, the wide usage of one-way communication can be noted from the fact that getting a response to a report may be difficult. Even if the recipient would be willing to give a response to the reporter, a dialog between the two parties is not necessarily the standard procedure. Developing a dialogical relationship between the communication participants would be of benefit in the communication process.

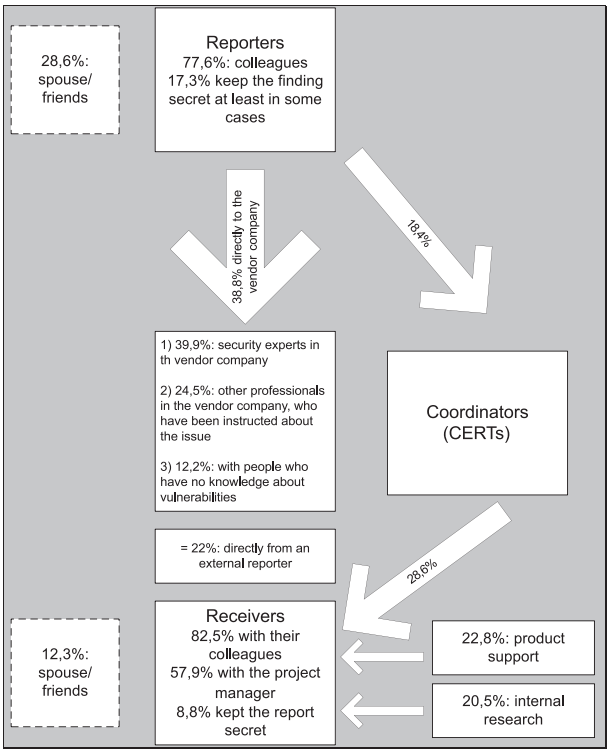


Figure 12: Information flows and their directions

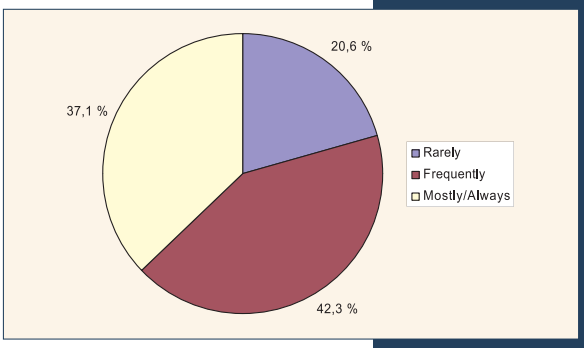


Figure 13: Finding the right contact persons without problems?

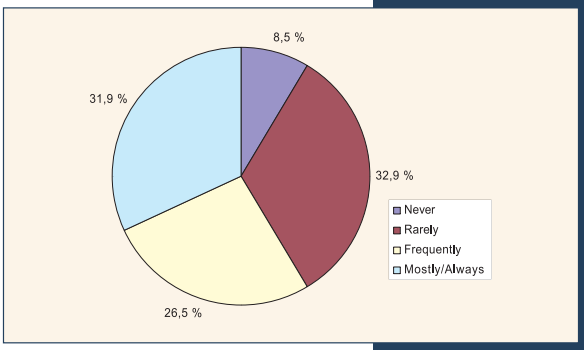


Figure 14: Our organization has been contacted by the receiver of the bug report after reporting...

Table 3: Communication statistics

Vulnerability handling: Communication

Test-suite	Failed products	Vendor responses	Advisory
wap-wsp-request	7 (7 tested)	5	n/a
wap-wmlc	10 (10 tested)	1	n/a
http-reply	5 (12 tested)	2	n/a
ldapv3	6 (8 tested)	10	CA-2001-18
snmpv1	12(12 tested)	~140	CA-2002-03

Table 4: Recent PROTOS Test-Suite: c06-snmpv1

Oulu University Secure Programming Group (2002)
Recent PROTOS Test-Suite: c06-snmpv1

• CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)

- http://www.cert.org/advisories/CA-2002-03.html
- Couple of man months to develop
- Several man months to coordinate
- As of May 2002:
  - over 200 vendors informed
  - ~140 vendors have responded publicly
  - ~100 vendors had affected (vulnerable) products
  - New vendor statements keep pouring into the advisory

"Mr. Hernan said that in "quite a number of cases", CERT went so far as to send letters to chief executives when other methods of making contact had been ignored. "I'm somewhat dissapointed in our ability to raise the attention of some of the companies", he said. "It was a very difficult problem in trying to raise the attention of the right people."

(The New York Times, February 13, 2002: Computer Security Experts Warn of Internet Vulnerability)

Values and beliefs guiding the communication

The respondents were asked to evaluate the values and beliefs that guide their decisions related to vulnerabilities. A great deal of the recipients of vulnerability reports indicated that security is the most important value to them. On the other hand they did not see public benefit and the public's right to know about vulnerabilities to be very important. The recipients valued more precision and accuracy as well as non-maleficence. This indicates that the recipients are interested in security, but for other reasons than the reporters. The attitudes toward software vulnerabilities can be seen to be somewhat different. Presenting the idea in a pointed way, it could be argued that the report recipients seek to fulfill the expectations that their stakeholders have towards their products, whilst the vulnerability reporters seek to gain security that is the best possible for the benefit of the public. Thus, the two groups accumulate and organize information about vulnerabilities in a somewhat different way and see the information as negative in different contexts. These attitudes may change as new learning occurs, potentially as a result of new insights into the requirements of the various involved parties. For example, the vendors may learn that the customers demand better security, and change their attitudes. The belief system concerning the vulnerabilities could be analyzed in more detail in future research.

"I am disappointed in X for not even testing for these vulnerabilities until pressure was put on them through resellers and for not publically announcing it so that administrators are made aware."

(Anonymous vendor comment)

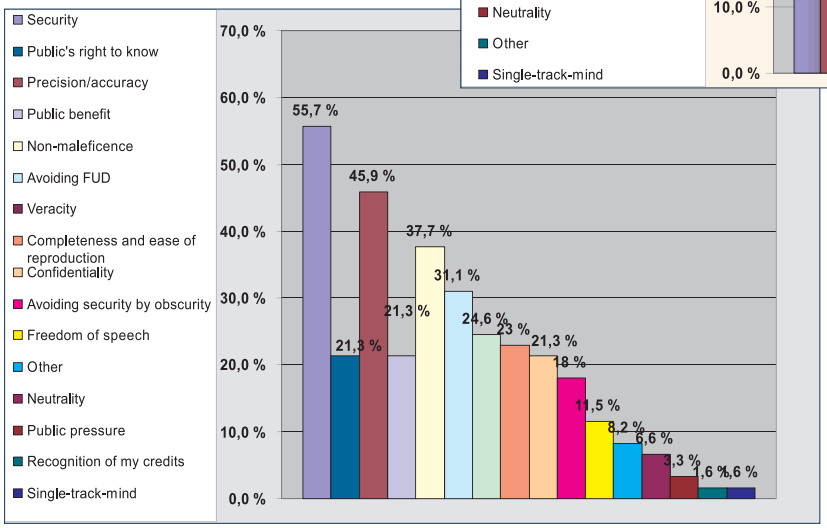


Figure 15: Receivers' values and beliefs

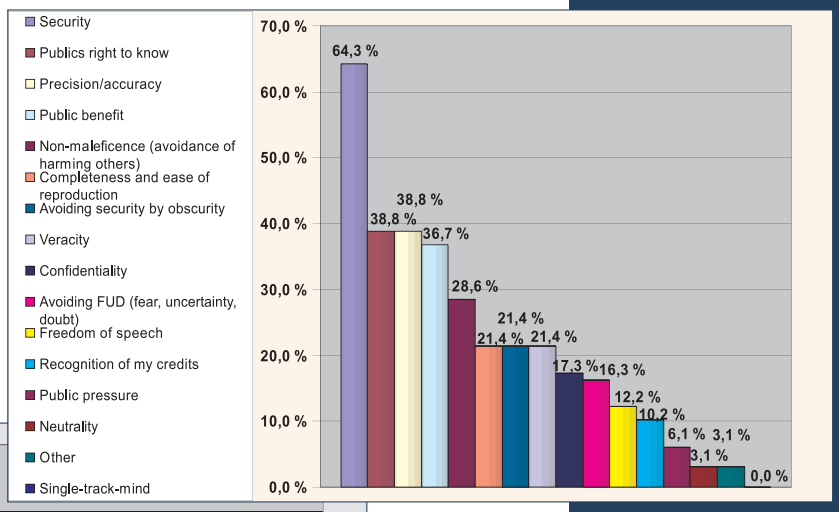


Figure 16: Reporters' values and beliefs

"Who is to blame for this? Patches are not installed because system administrators are not taught the importance of it."

(Steve Manzuik, 2001, Vuln-dev)

4. Knowledge management

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. Knowledge management means that information transmission in all its phases from knowledge creation through knowledge transmission to knowledge interpretation is well planned and reasonably organized.

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). 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. Procedural knowledge and content 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.

Experience in vulnerability reporting will probably make the communication easier.

Disclosure policies and Guidelines
(http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/)

Russ Cooper. (1999). "NTBugtraq Disclosure Policy". NTBugtraq.
Cisco PSIRT. (1999). "Cisco Product Security Incident Response". Cisco Technical tips.
Simple Nomad. (1999). "Nomad Mobile Research Centre - A N N O U N C E M E N T.
Microsoft. (2000). "Acknowledgment Policy for Microsoft Security Bulletins". Microsoft TechNet.
Rain Forest Puppy. (2000). "Full Disclosure Policy (RFPolicy) v2.0".
@stake. (2000). "@stake Security Advisory Disclosure Policy".
CERT/CC. (2000). "The CERT Coordination Center Vulnerability Disclosure Policy". CERT/CC.
Microsoft. (2000). "Microsoft Corporation Product and Service Security Policy". Microsoft TechNet.
anonymous. (2001). "Anti security "policy" v0.9 - Save the bugs!".
SGI. (2001). "SGI - Services & Support: Security: Response and Procedures".
ACROS Security. (2001). "ASPR Notification and Publishing Policy".
The Mozilla Organization. (2001). "Handling Mozilla Security Bugs v1.0".
Steve Christey and Chris Wysopal. (2002). "Responsible Vulnerability Disclosure Process". IETF DRAFT.
Steven M. Bellovin and Randy Bush. (2002). "Security Through Obscurity Considered Dangerous". IETF DRAFT.
Organization for Internet Safety. (2003). "Draft SecurityVulnerability Reporting and Responding Process".

Table 5: Disclosure policies and Guidelines

In the software vulnerability reporting process procedural knowledge, know-how and know-who, seems to especially need development. For example, this can be seen from the fact that 37,7% of the reporters indicated that they infrequently find the right contact persons without problems. Thus, the know-who -knowledge is not very good. In the survey only 8,2% of the reporters indicated that they use an independent third party, like a national CERT, for finding the right contact persons. Actors, such as CERT, could provide the potential to be utilized more efficiently in the communication network.

Lundvall (2000, 18-19) notes that the transferability of knowledge depends particularly 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 relies on whether codes are made explicit and hence widely usable. Tacit knowledge is more difficult to distribute forward inside the organization. This has also been noticed in the responding organizations. Up to 76% of the organizations reporting vulnerabilities and 71,9% of the recipient organizations keep a record of vulnerabilities and their patches. Policies can be seen as a way of codifying information, and this should be taken into account in the organizations that take part in the reporting process. Currently policies are more common in organizations receiving vulnerability reports. Policies are also a way to improve procedural knowledge in the organization.

The participants in the vulnerability reporting process can prepare by developing a policy for the situation. Surprisingly few of the participants have a crisis or risk management plan, such as a reporting policy. In the survey it was detected that nearly half of the recipient organizations, but only one third of the reporting organizations, had some kind of a reporting policy.

According to our results the recipients have a more standardized procedure. More often they at least have an internal reporting policy. The reporters do not have a standardized policy as often, and even if they have it is a non-written or internal one and thus not available to people who are not members of the organization in question.

"Very interesting. We were extremely careful, but there was a deeply embedded support routine that was not doing proper bounds checking on the host portion of the URL."

(Anonymous vendor comment)

	We have a public reporting policy	We have an internal reporting policy	We have a non-written reporting policy	There is no standard way - depends on the situation	It is up to the reporter to determine the best way	Other	Total
receivers	10	15	2	20	7	4	***58***
reporters	6	10	15	32	27	7	***97***
Total	***16***	***25***	***17***	***52***	***34***	***11***	***155***

Table 6: The comparison of the usage of different reporting policies in the organizations (cross-tabulation)

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).

In the software vulnerability reporting process these stages can also be noticed, and in this case the learning process is described as interorganizational learning. The socialization stage is the stage in which knowledge is still tacit. This refers to the phase when the communication participants figure out what the issue is all about inside their own working group. 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. 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 results made it clear that the combination stage inside the organizations receiving reports is essential. More than half of the respondents (51,8%) told 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 recipient organizations learning process and knowledge management. On the other hand this fact raises the question of a more intensive dialog between the reporters and the recipients. 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. The conclusion was 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.

5. Publicity and crisis management

"It is impossible to discuss a vulnerability without giving enough information that would allow someone else to re-discover the problem and use it."

(Steve Manzuik, 2001, Vuln-dev)

One of the central issues related to the vulnerability reporting process is the extent of publicity related to discovered vulnerabilities. Publicity and crisis management are closely linked together, and with careful publicity management a crisis situation may be avoided. On the other hand there are different views about the ethically correct amount of publicity related to software vulnerabilities.

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 includes reputation management, stakeholder strategy, and corporate social responsibility, and reduces the risk of a publicity crisis. (Lehtonen 2002, 38.)

To manage its publicity, 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.)

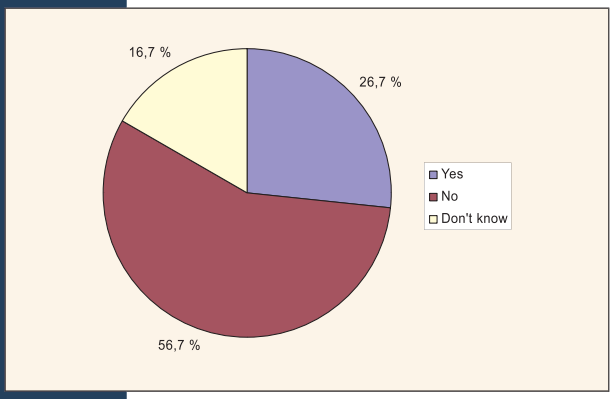


Figure 17: Do the receiving organizations have a proactive publicity strategy for these kind of crisis situations?

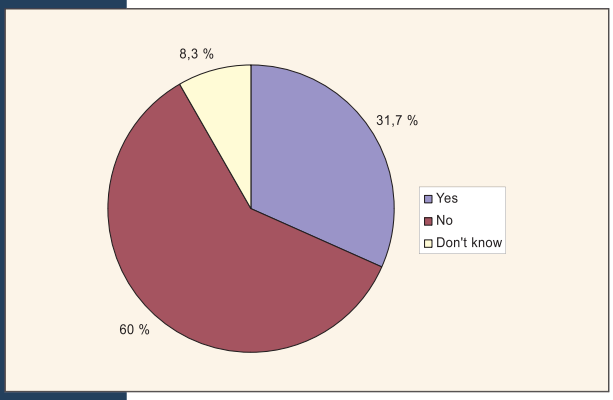


Figure 18: Do the organizations have a PR-personnel who is familiar with the vulnerability issues and has direct contacts to media?

Approximately one third of the organizations receiving reports answered that they have PR-personnel who are familiar with vulnerability issues and have direct contacts to the media. This seems to indicate that one third of the organizations have prepared for publicity management related to vulnerability reports.

In the survey it was discovered that both the receivers and the reporters see publicity in most cases to be primarily positive. Typically, the communication with publicity is not dialogical. Most of the organizations seek to inform the media actively. However, also seeing the media as an important and equal discussion partner is relatively common. This was concluded from the basis of the last question in the survey. In the question it was inquired as to which of the four possible ways of reacting to publicity in a crisis situation the respondents would most probably use, and thus, what kind of attitudes the respondents have towards publicity. It was noticed that in the vulnerability scene the most common strategies are comparable to Fitzpatrick's and Rubin's mixed strategy and traditional public relations strategy.

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 are attempted to be diverted away from the accusations, the media told that the organization is outraged at the situation, whilst the company takes little or no substantive action, and/or the problem is claimed to be solved. The organization tries to manipulate the public's opinions. (Fitzpatrick & Rubin 1995, 22-23.)

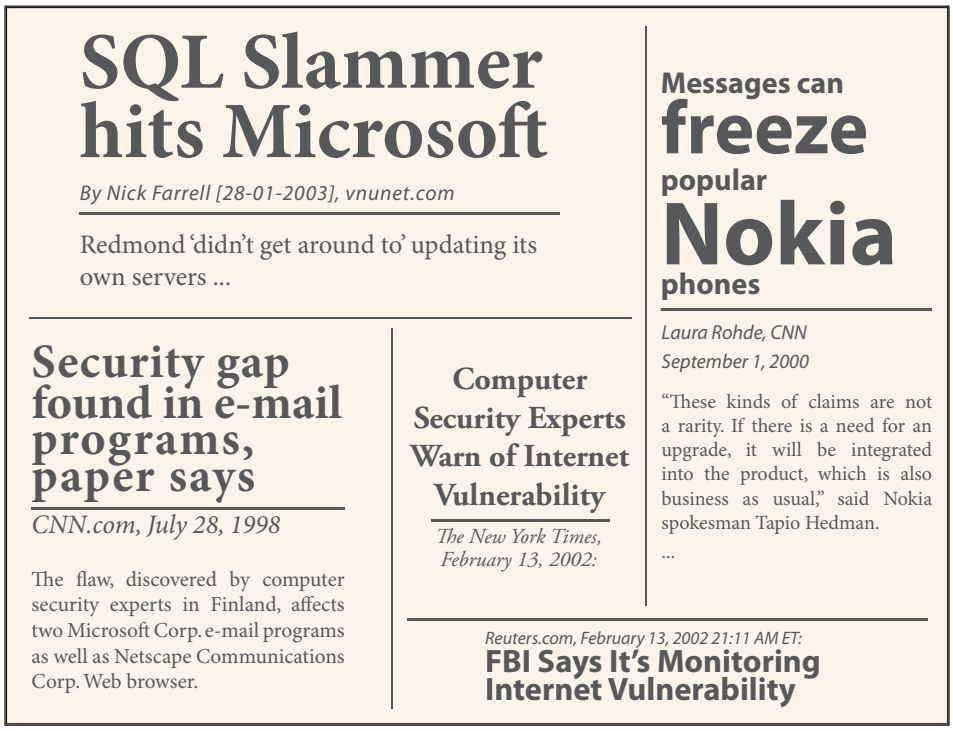


Figure 19: News headlines

"The full-disclosure movement appeared because companies were ignoring the problems with security holes or lying about them."

(Cesar Cerrudo, 2002, Bugtraq)

The opinions about publicity and the extent of the disclosures were also determined in the study. Overall, both the reporters and the recipients opposed immediate and full disclosure. However opinions differed between the choice of immediate full disclosure and that of only partial disclosure followed by full disclosure at a later time. The recipients opposed full disclosure more than the reporters in its every form. The two groups agreed on publishing some part of the information after a predefined time, thus partial disclosure is seen to be the ethically correct way to handle vulnerabilities.

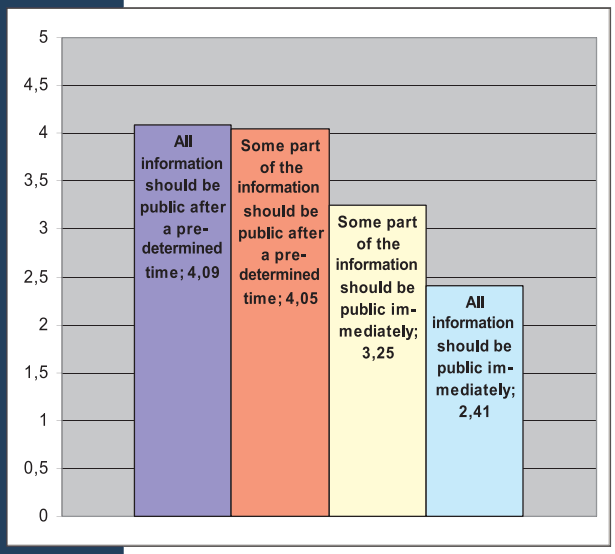


Figure 20: Vulnerability information handling (the reporters' opinions on the Likert scale: 1-5)

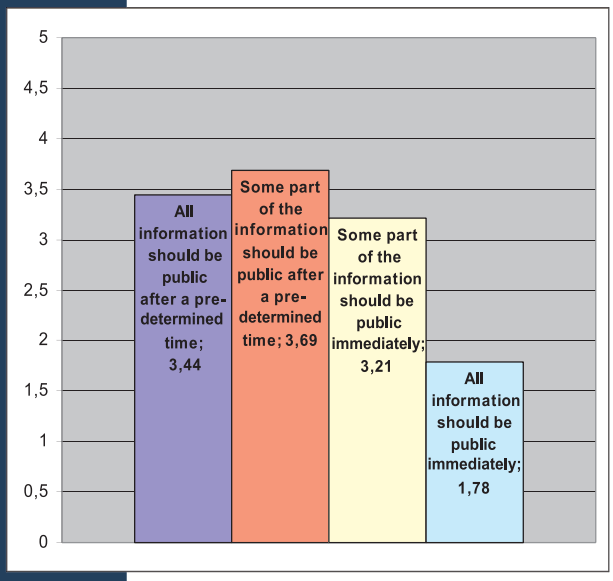


Figure 21: Vulnerability information handling (the receivers' opinions on the Likert scale: 1-5)

Currently vulnerability disclosure is often a crisis for the vendor. It is a sudden and unexpected notification about weaknesses in products. In crisis communication theory it is traditionally recommended that a notification about the issue should be given to all people concerned in a short time frame. This is advised 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 bug reporting process is a somewhat exceptional case. Keeping things secret, at least to some point, is seen to be the ethically correct way to handle the disclosure. At the point in which the vulnerability is found, the most essential thing 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 is found. The concensus is to first inform only the vendor, giving the vendor enough time to develop the patch. After this it is possible to publish a full report if that is wanted. (Deline 2000.)

6. Conclusions

Communicating software vulnerabilities is a challenge that defies the organizational practices over and over again. It is an issue that, at the first sight, seems rather secondary compared to other organizational management issues, but in fact has a big influence on security development. Currently the reporting process needs improvement. The reporters of vulnerabilities and recipients seem to have different views about the ethically correct way to view vulnerability reporting. This is an interesting phenomenon, as it indicates the two groups are not unanimous about professionalism in the field. There is an obvious need for an international codification of rules from the basis of which effective disclosure policies would be possible to be developed. In the future the significance of software vulnerabilities will call for the participation of governments, law makers, consumer advocacy groups and society at large. This uncontrolled growth will present many difficulties unless the communication framework significantly matures.

In the future, trust and liability issues in the reporting process need to be taken into consideration in more detail. The vulnerability life-cycle can be defined as the process from the discovery of a vulnerability to its repair. 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.

Effective communication demands trust in the communication partners. Trust and risk go hand in hand. Doney, Cannon and Mullen (1998) define trust as a willingness to rely on another party and to take action in circumstances where such action may make one vulnerable. They acknowledge that their definition incorporates the notion of risk as a precondition of trust, and that it includes both the belief and behavioral components of trust. Trusting in something means reducing complexity in the uncertain reality. The concept of trust includes also the orientation towards the future. (Mühlfelder, Klein, Simon & Luczak 1999, 350). Today, inside the vulnerability reporting network, trust is developed separately in every reporting case, 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. Reporting security problems in software is challenging but not impossible.

Tiina Havana, *Research Scientist*
OUPSG

"I've been watching the blame in computer security flow in circles for years. The flow looks like this:

- ***The hackers blame the sysadmins who leave their machines open***
- ***The sysadmins blame the vendors who write buggy insecure code***
- ***The vendors blame the customers who place a premium on features over quality"***

(Marcus J. Ranum, 2002, Fw-wiz)

"Consumers and Media should be listed as participants too, but I guess the Vendors figure Consumers and Media full under their purview."

(Russ Cooper, 2003, NTBugTraq)

References

- Doney, P.M., Cannon, J.P. & Mullen, M.R. 1998. Understanding the influence of national culture on the development of trust. Academy of Management Review, 23/3: 601-620.

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

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

- Ikävalko, E. 1996. Ylivoimapeli mediassa. Julkisuusmekanismit ja julkisuuden hallinta. Helsinki: Inforviestintä Oy. (Doctoral dissertation, in Finnish)

- 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/
[Accessed: 6th June 2003]

- Mühlfelder, M., Klein, U., Simon, S. & Luczak, H.1999. Teams without trust? Investigations in the influence of video-mediated communication in the origin of trust among cooperative persons. Behaviour & Information technology, 18, 349-360. London : Taylor & Francis.

- Lehtonen, J. 2002. Julkisuuden riskit. Helsinki: Mainostajien liitto. (Book, in Finnish)

- 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).

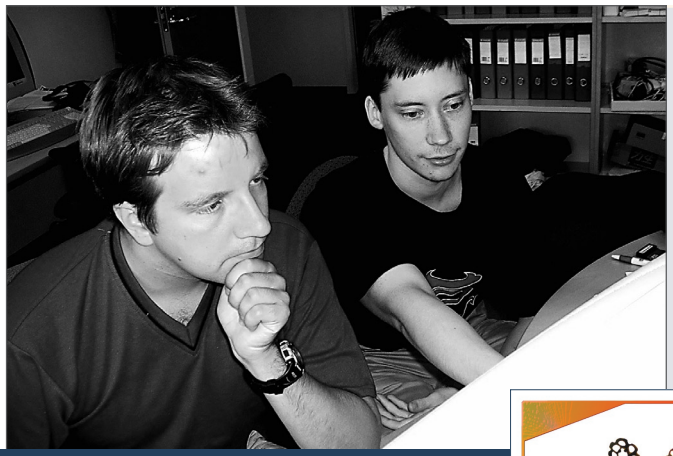
- Nonaka, I. & Takeuchi, H. 1995. The Knowledge-Creating Company. How Japanese Create the Dynamics of Innovation. Oxford: Oxford University Press.

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

Acknowledgement

We wish to express our gratitude to individuals and organisations who participated in our survey, their contribution made the difference. We are in debt to AusCERT, CERT/CC and CERT-FI for their valueable assistance with the survey and for all the support we have received while carrying out vulnerability work. Last, but not least, we are grateful to the vulnerability scene community at large for contribution to a field that certainly will have growing importance in the days to come.

OUSPG



Oulu University Secure Programming Group (OUSPG) is a research group of approximately 13 people interested in computer security issues. The purpose of OUSPG is to study, evaluate and develop methods of implementing and testing application and system software in order to prevent, discover and eliminate implementation level security vulnerabilities in a pro-active fashion. The focus of the research group is on implementation level security issues and software security testing.

OUSPG is active as an independent and academic research group in the Computer Engineering Laboratory of the University of Oulu since summer 1996. The University of Oulu is located in northern Finland. The research group is led by professor Juha Röning.

At the moment OUSPG is occupied with black-box testing for software vulnerabilities, vulnerability tracking and keeping a database of the internal disclosures, integrating secure programming in local curriculum, studying the vulnerability classifications and taxonomies, and studying the life-cycle of software vulnerabilities.

More information can be found at:
http://www.ee.oulu.fi/research/ouspg

The research group can be reached via email:
ouspg@ee.oulu.fi

PGP Key:
http://www.ee.oulu.fi/research/ouspg/ouspg-key.asc

Key fingerprint:
B2 F7 97 09 F5 4C 29 97 9A A8 2D FB 59 CA 10 C4

via fax:
+358 8 553 2612 [Attn: OUSPG]

or via mail:
Prof. Juha Röning
University of Oulu, Computer Engineering Laboratory
PL 4500
90014 University of Oulu
Finland

http://www.ee.oulu.fi/research/ouspg

www.mediakarhut.com

Oulu University Secure Programming Group

ISBN 951-42-7072-X