Communication in the Software Vulnerability Reporting Process

Tiina Havana, University of Oulu, Finland
ouspg@ee.oulu.fi
http://www.ee.oulu.fi/research/ouspg/

Wiio's laws

- Communication usually fails, except by accident
- If communication can fail, it will
- If communication cannot fail, it still most usually fails
- If a message can be interpreted in several ways, it will be interpreted in a manner that maximizes damages
- The more we communicate, the worse communication succeeds

(Wiio 1978)

Presentation contents

- Basic concepts
  - Software vulnerability reporting
  - Communication in a network
  - Knowledge management and organizational learning
  - Risk, crisis, and publicity management
- Methods
- Results
  - Characteristics of the software vulnerability communication process
  - The right way to do the reporting?
  - Values and beliefs that lie behind
- Conclusions

Software vulnerability reporting

- Information society
  - Dependence on the computer security
- A Software vulnerability:
  - A hardware, firmware, or software flaw that leaves an automated information system open for potential exploitation
- Problems in the reporting process exist

Level of the publicity	*Widely public*	*Limited publicity*	*Private*
Extent of the disclosure			
full	White-hat hackers (1)	Professional vulnerability testers (3)	Internal testing teams (4)
partial	Vendors (2), Coordinators (2)		Internal bulletins inside the organizations (5)
no			Non-public bulletin inside the internal testing team (6)

Communication process

- Communication:
  - A process in which a state of issues is interpreted and this interpretation is published through interaction in a network
- Communication network architecture
- Information transmission
  - = knowledge creation + transmission + interpretation

Knowledge management and organizational learning

- Content knowledge
  - Facts or information (know-what)
  - Principles that explain (know-why)
- Procedural knowledge
  - Competence and skills (know-how)
  - Knowledge of the source of information (know-who)
- Knowledge creation
  - An iterative process between knowledge production, mediation and application
  - SECI theory (Nonaka & Takeuchi, 1995)
    - Tacit knowledge to explicit knowledge and back to tacit knowledge
    - Socialization, Externalization, Combination, Internalization

Publicity management

- Effective publicity management requires that the organization has
  - An articulated, proactive publicity strategy
  - Knowledge of how the publicity works
  - Trustworthy PR personnel
  - Direct contacts to media
- The organization has to
  - Take care of its relationships to its stakeholders
  - Take responsibility of its actions
  - Follow the changes of its stakeholders' values and expectations, as well as public discussions

Reacting to a crisis situation

- Fitzpatrick's and Rubin's (1995) grouping
  - The traditional public relations strategy
  - The traditional legal strategy
  - The mixed strategy
  - The diversionary strategy
- The most common strategies in the vulnerability scene
  - The mixed strategy and the traditional public relations strategy

Methods

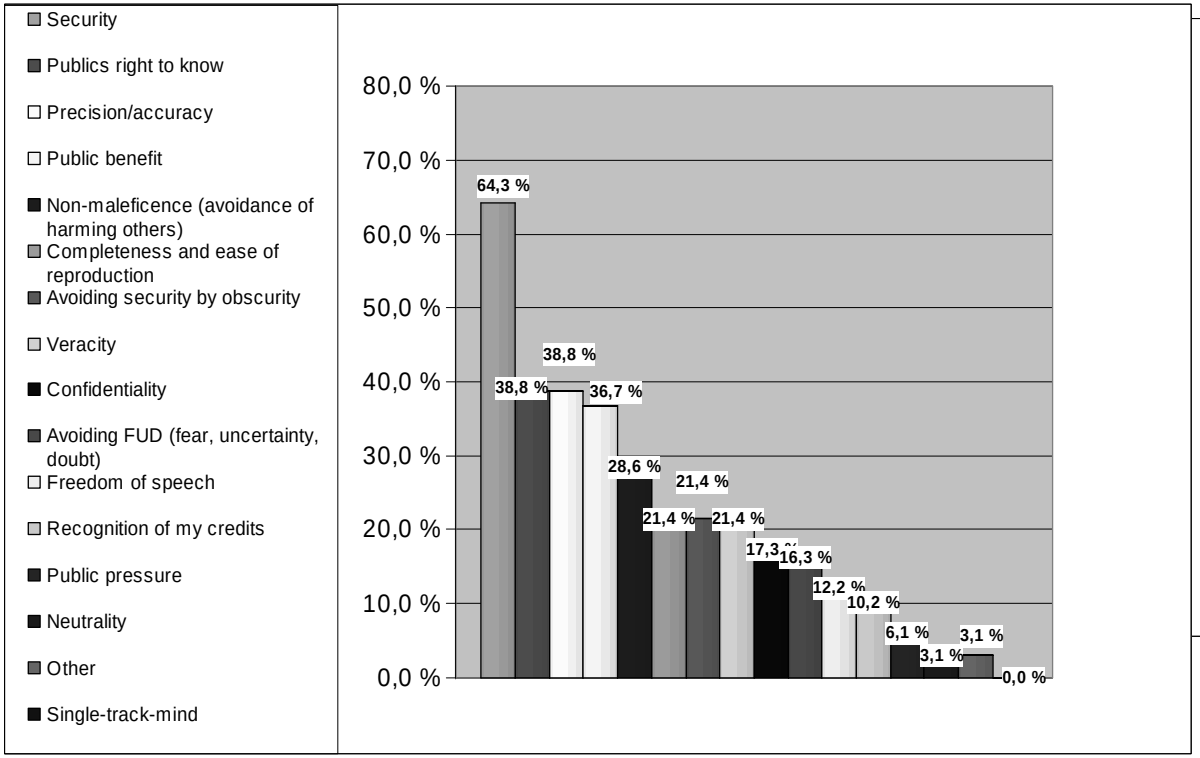
- Internet-based survey in summer 2002
  - Two questionnaires, one for the reporters and one for the receivers of the reports
  - Snowball sampling
    - Advertising the survey on mailing lists, and by AusCERT and CERT/CC
  - 157 valid answers (60 from receivers, 97 from reporters)
- Quantitative data analysis
  - Statistical methods to compare the two groups: Chi-square tests, Mann-Whitney U-tests, Factor analysis
  - Presenting data as simple percentage and mean values

General observations

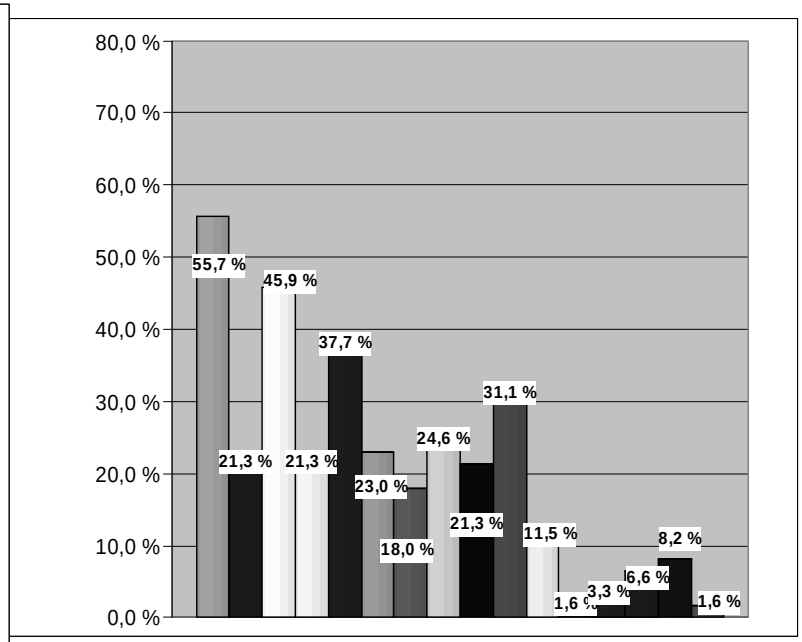
- The two groups' opinions about their trust and dependence on the communication network differ from each other
  - The receivers have more trust
  - The receivers think that they contact the reporters more often than the reporters think that they are contacted
- The values that guide the respondents communication actions differ between the two groups

Values and beliefs that guide the respondents choises

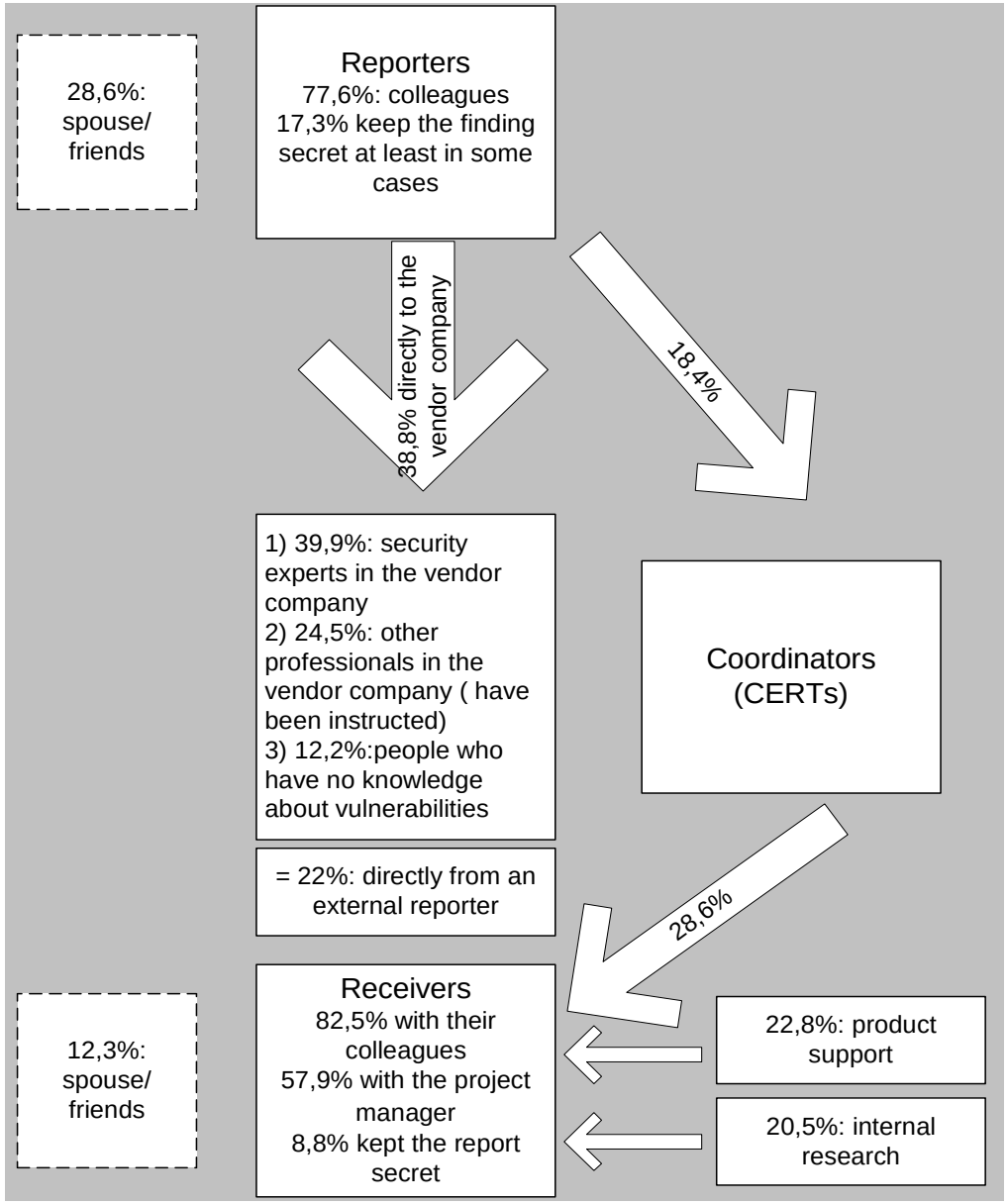
Reporters



Receivers



The vulnerability information flows and their directions



Knowledge management in the communication network

- Procedural knowledge seems to need development
- Routines are developed
- Codification of the knowledge is essential: policies
- Recognized or advertised point of contact more common in the receiving organizations

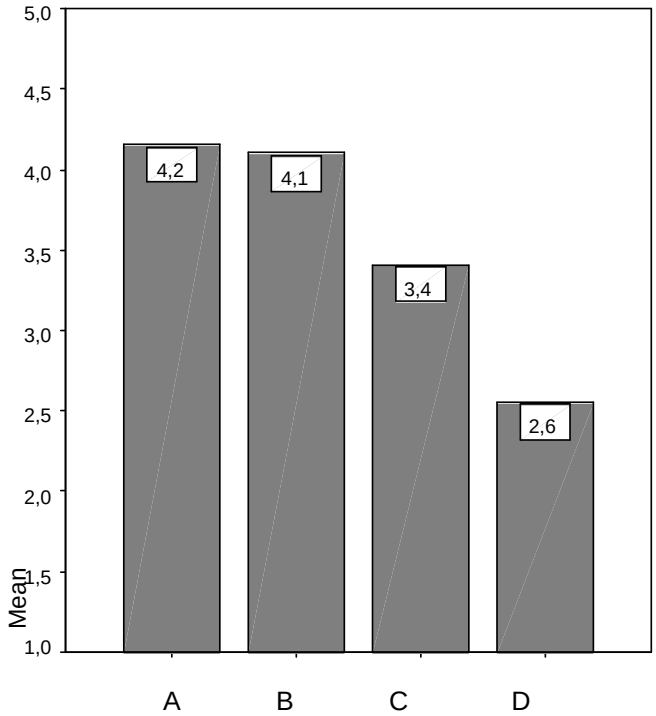
	A public reporting policy	An internal reporting policy	A non-written reporting policy	No standard way	The reporter decides	Other	Total
Receivers	10	15	2	20	7	4	58
Reporters	6	10	15	32	27	7	97
Total	16	25	17	52	34	11	155

Organizational learning

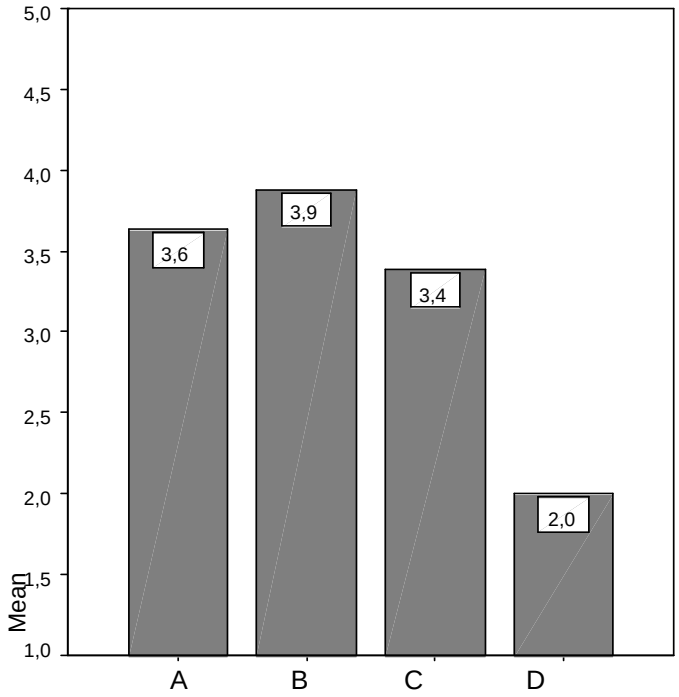
- SECI theory
  - Combination stage inside the receiving organizations is essential
    - need for a more intensive dialog between the reporters and the receivers
  - Internalization: 55% of the receivers pass the information about discovered bugs to their software developers
- Need for double-loop learning?

The correct vulnerability handling process?

Reporters



Receivers



A = All information should be public after a pre-determined time
B = Some part of the information should be public after a pre-determined time
C = Some part of the information should be public immediately
D = All information should be public immediately

Publicity

- 1/3 of the receiving organizations have a proactive publicity strategy for a case of publicity crisis concerning vulnerabilities.
- 1/3 of the receiving organizations have PR-personnel who are familiar with vulnerability issues and have direct contacts to the media

- In the vulnerability reporting process the receivers' most important stakeholders are the reporters
  - The relationship needs development
  - The communication between the two groups is not open or conversational

- Publicity management related to the vulnerability reporting process vs. typical/traditional publicity management of an organization
  - Keeping things secret at least to some point is seen to be ethically right

Corporate social responsibility

- 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 manage the public image of the reporters, the reporters should above all handle the reporting in an ethical way
  - Vulnerability reports are at least attempted to be handled fast and effectively in most of the receiving organizations

Crisis and risk management

- Surprisingly few of the participants have a crisis or risk management plan, such as a reporting policy
- 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.

Conclusions

- Functional vs. dissipative communication paradigm
- Communication seems quite often to be one-way, although two-way symmetrical communication could be needed
- Is bug reporting exceptional form of communication?
- A lack of vulnerability knowledge codification
- The concept of professionalism has not yet been fully developed

What there is to be done?

- Successful communication?
- Development of dialog between the different parties
- Mutual understanding
- Policies

Thank you for your attention!

Further information:

- Pro Gradu Thesis:
  http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/
  ouspg@ee.oulu.fi