Security and Privacy Metrics Foundations for Services Cost Models

COST 605, Limassol, February 2 - 4, 2009

Denis Trček
Laboratory of E-media
Faculty of computer and information science
University of Ljubljana
denis.trcek@fri.uni-lj.si

Introduction

- Security is among top priorities in IS for more than a decade.
- Despite its importance, it is interesting to note that the area still lacks (completeness) of related metrics.
- The importance for risk management:
  - for business decisions ranging from economical justifications of new security implementations to customized services with appropriate security costs calculations;
  - new business models…

Introduction

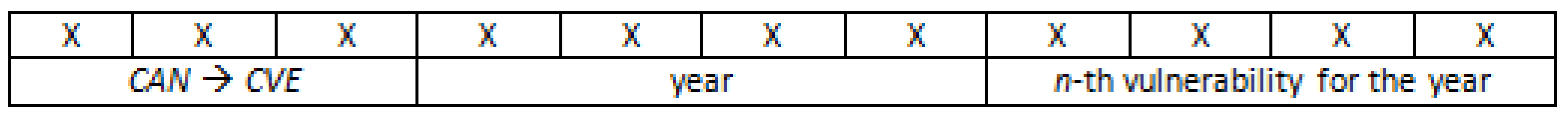
- Our research (this presentation) gives:
  - overview of up-to-date situation in this field by analyzing of existing metrics that could serve for the above mentioned purpose;
  - presentation of a generic risk management model based on system dynamics;
  - short analysis of possibilities for application of these existing metrics to the model.

Risk management and metrics overview

- Among the most important endeavors the following two databases have to be mentioned:
  - MITRE Corporation Common Vulnerabilities and Exposures and
  - US National Vulnerability Database
  - (a useful complementary effort that should also be mentioned is Open Web Application Security Project, OWASP, which is focused on web applications security flaws).

Risk management and metrics overview

- MITRE Corporation Common Vulnerabilities & Exposures Database.
  - Vulnerabilities can be in one of two states:
    - publicly known, with no patch available from the vendor, or
    - publicly known, with a patch available from the vendor.
- All vulnerabilities have an ID which is an eleven digit unique number with its syntax as given in the table below:



X	X	X	X	X	X	X	X	X	X	X
CAN → CVE			year				*n*-th vulnerability for the year			

Risk management and metrics overview

- Using this database as a foundation, Jones suggests metric called DVE (daily vulnerability exposure) [Jones]:
  - DVE is a sum of num. of publicly known vulnerabilities for a system *s* without corresponding patch on each day of the year:

$$DVE_s(date) = \sum_{vuln\ s} (date_{known} < date) \wedge (date_{patched} > date)$$

  - DVE expresses for any given day the exposure (number of exposures) of a system to those vulnerabilities that were publicly disclosed prior to that day, but patches were not available until after that day.

Risk management and metrics overview

- Jaquith suggests a simple metric called BAR (business adapted risk) [Jaquith]:
  - Security defects should be classified by vulnerability type, degree of risk, and potential business impact - a score is calculated as

$$BAR = BI * RoE$$

  - where *BI* stands for business impact (its values are taken from the interval [1,5]) *RoE* stands for risk of exploit (these values are taken from the interval [1,5]), and *BAR* stands for business adjusted risk (with values from the interval [1,25]).

Risk management and metrics overview

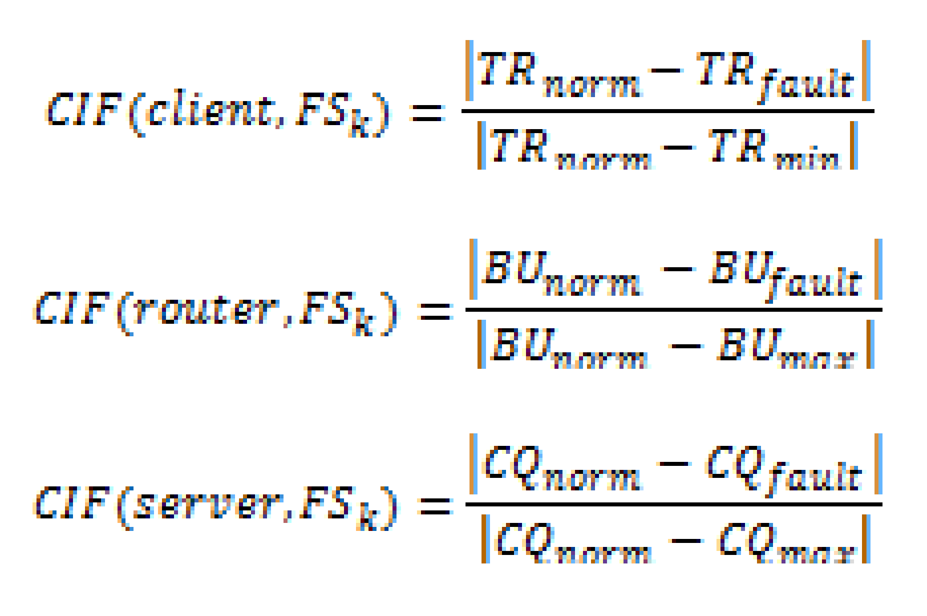
- Harriri et al. suggest vulnerability index (VI) [Harriri]:
  - This index is based on qualitative (categorical) assessment of a state of a system (be it a router, a server or a client), which can be normal, uncertain and vulnerable.
  - Each of the above devices has an auditing agent that measure the impact factors in real-time (they calculate the ratio between the changes of a normal and abnormal state). The vulnerability analysis engine statistically correlates the agent generated events to system impact metrics.

Risk management and metrics overview

- Harriri et al. suggest to use vulnerability index (VI) [Hariri]:
  - For each kind of a system a component impact factor (CIF) is calculated for a given fault scenario (FS).
  - CIF is the ratio between two differences – the first is the difference between the normal and faulty operation parameter value, and the second is the difference between the normal and acceptable threshold value of this operation parameter.

Risk management and metrics overview

- Vulnerability index (VI) [Hariri]:



$$CIF(client, FS_k) = \frac{|TR_{norm} - TR_{fault}|}{|TR_{norm} - TR_{min}|}$$

$$CIF(router, FS_k) = \frac{|BU_{norm} - BU_{fault}|}{|BU_{norm} - BU_{max}|}$$

$$CIF(server, FS_k) = \frac{|CQ_{norm} - CQ_{fault}|}{|CQ_{norm} - CQ_{max}|}$$

  – Now the system impact factor (SIF) can be obtained that identifies how a fault affects the whole (sub)network.

Risk management and metrics overview

- Vulnerability index (VI) [Harriri]:
  - For a given fault a SIF is obtained by evaluating the weighted IFs of all network components. This means the percentage of components in vulnerable states (i.e. where CIF exceeds normal op. thresholds *d*) in relation to the total num. of components:

$$SIF_{client}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ clients}$$

$$SIF_{router}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ routers}$$

$$SIF_{server}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ servers}$$

  - Component oper. state (COS) equals to 1 when the component operates in an abnormal state (that is, $CIF_i > d$), and 0 when it operates in a normal state ($CIF_i < d$).

Risk management and metrics overview

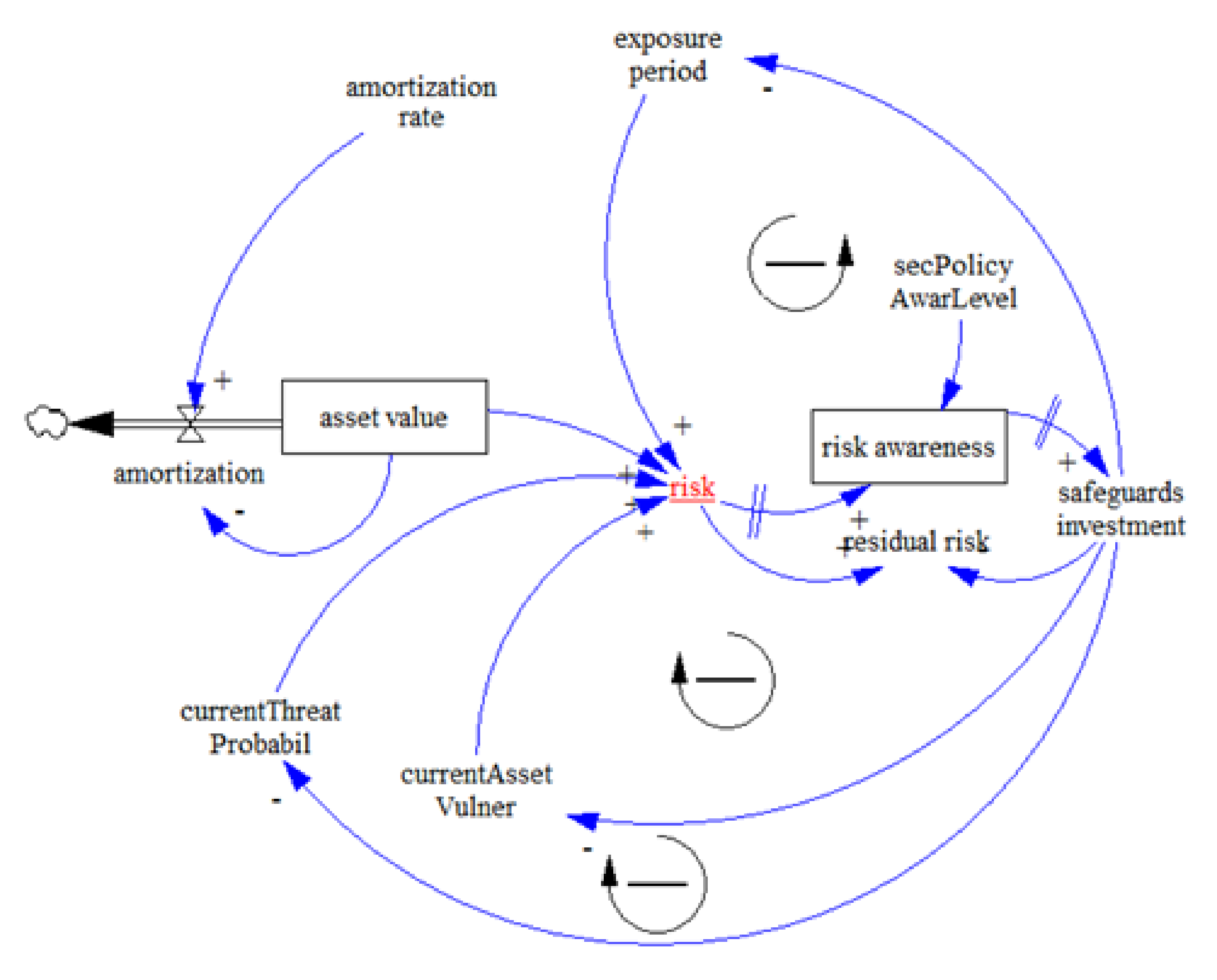
- Other metrics:
  - The first one is survivability analysis, where a fault is injected in systems specification and consequences are visualized by scenario graphs.
  - Graph methods are also used in graph-based network vulnerability analysis (where a database of common attacks is used and applied to a particular network configuration to identify the most probable attack paths), and attack trees (which are similar to former technique, but of a more general nature).

Generic IT Risk Management Model

- Generic IT risk manag. model [Trček]:
  - It is based on system dynamics.
  - It follows the main standards in this area:
    - Int. standards organization, Information security management systems – Guidelines for information security risk management, ISO 27003 / BS 7799-3, Geneva / London, 2005.
    - NIST, Managing Risk from Information Systems, NIST SP 800-39 Draft, US Dept. of Commerce, Washington D.C., 2007.
    - US Dept. of Health, Basics of Risk Analysis and Risk Management, US Dept. of Health & Human Services, Washington D.C., 2005.

© 2009 D. Trček
no. 14

Generic IT Risk Management Model



Conclusions

- Quite some metric can already be applied.
- Some elements are still missing, but…
- The complete automation of GIT- RM model has to be considered.
- Security metrics in IS security and privacy areas does get improved.
- How about pro-active approaches?

References

- [Jones] Jones J.R., Estimating Software Vulnerabilities, IEEE Security & Privacy, July and August, IEEE, 2007, pp. 28-32.
- [Hariri] Hariri S., Qu G., Dharmagadda T., Ramkishore M., Cauligi S., Raghavendra A. , Impact Analysis Of Faults And Attacks In Large-Scale Networks, IEEE Security & Privacy, September/October, IEEE, 2003, 49-54.

References

- [Jaquith] Jaquith A., Security Metrics: Replacing Fear, Uncertainty and Doubt, AW, Upper Saddle River, 2007.
- [Trček] Trček D., System Dynamics Based Risk Management for Distributed Information Systems, Proceedings of ICONS 09, IARIA / IEEE, Gosier, 2009 (forthcoming).