COST 605

Econ@Tel

A Telecommunications Economics COST Network

cost

A Survey of Security and Privacy Metrics for IT Services

COST 605 WG4, Vienna, May 5, 2008

Denis Trček

Laboratory of E-media

Faculty of computer and information science

University of Ljubljana

denis.trcek@fri.uni-lj.si

Our history… and intentions

- Public key infrastructure – CA Browsing System.
- Supporting trust management (trusGuard application).
- Supporting security and provacy related analysis / charging for costs induced by related services.

Introduction

- Providing security and assuring privacy induces certain costs.
- Although these costs are tangible, there exist very few metrics to quantify ANY issues related to security and privacy.
- There is no mapping all the way from the technological domain to economics domain (at least not known to me).

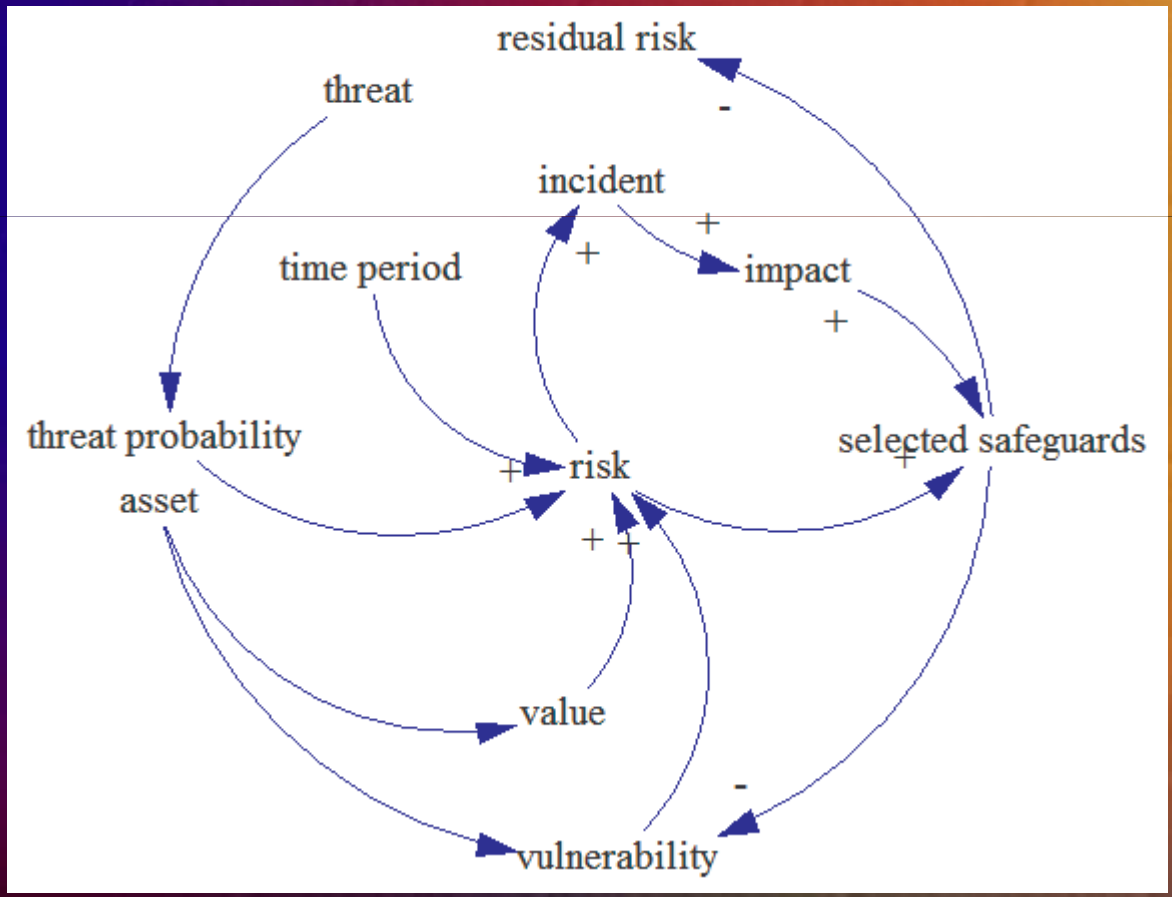
Economics of security and privacy

- The first basic problem related to security and privacy in IT environments is the question of risk management.
- The second problem is the problem of non-existence of appropriate metrics in the field of security & privacy.
- The third problem is related to (lack of standardized) charging mechanisms and appropriate business models.

Risk management issues

(D. Trček, Managing IS Security and Privacy, Springer, 2006)

- The generic risk-management model.



Security and privacy related metrics

- Attacks treshold metrics.
  - A cost/benefit economyof a cybercrime requires the following eq. to be fulfilled:

$$M_b + P_b > O_{cp} + O_{cm} * P_a * P_c$$

  - where *Mb* denotes monetary benefits of the crime, *Pb* denotes psychological benefits of committing the crime, *Ocm* denotes the monetary opportunity costs of conviction, *Ocp* denotes the psychological costs of committing the crime, *Pa* denotes the probability of arrest, and *Pc* denotes the probability of conviction (the term *Ocm*Pa*Pc* is the *expected penalty effect*).

Security and privacy related metrics

- Vulnerability metric.
  - To calculate the complete impact factor for the network, component impact factor (*CIF*) has to be calculated first.
  - For example, assume a router and a given attack scenario (A_k). Due to attack, the normal data transfer rate is decreased and the difference is compared to the difference between normal data transfer rate and minimal operational data transfer rate:

$$CIF(A_k) = \frac{|TR_{norm} - TR_{attack}|}{|TR_{norm} - TR_{min}|}$$

Security and privacy related metrics

- Vulnerability metric.
  - System impact factor (*SIF*) can now be computed as the weighted impact factors of all components (the percentage of components in vulnerable state in relation to the total # of components is determined):

$$SIF(A_k) = \frac{\sum_{\forall i, CIF_i > d} COS_i}{total\_number\_components}$$

  - *COS* (component operation state) is a binary variable that equals 1 when a component operates in abnormal state, i.e. when $CIF_i > d$ (d denotes the upper threshold for normal operating conditions), and 0 otherwise ($CIF_i < d$).

Conclusions

- Further work:
  - The analysis of appropriate metrics for elements in line with the generic risk management model.
  - Bridging the gap…

References

- Kshetri N., The Simple Economics of Cybercrime, IEEE Security & Privacy, Vol. X. No 1., pp. 33 – 39, IEEE Press, 2006
- S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, Impact Analysis of Faults and Attacks in Large-Scale Networks, IEEE Security & Privacy, Vol. X, No. 5, pp. 49-54, IEEE, 2003.