COST 605

Econ@Tel

A Telecommunications Economics COST Network

cost

Security and Privacy Related Risk Management Specifics in SOAs

COST 605, Sevilla April 2-4, 2008

Denis Trček

Laboratory of E-media

Faculty of computer and information science

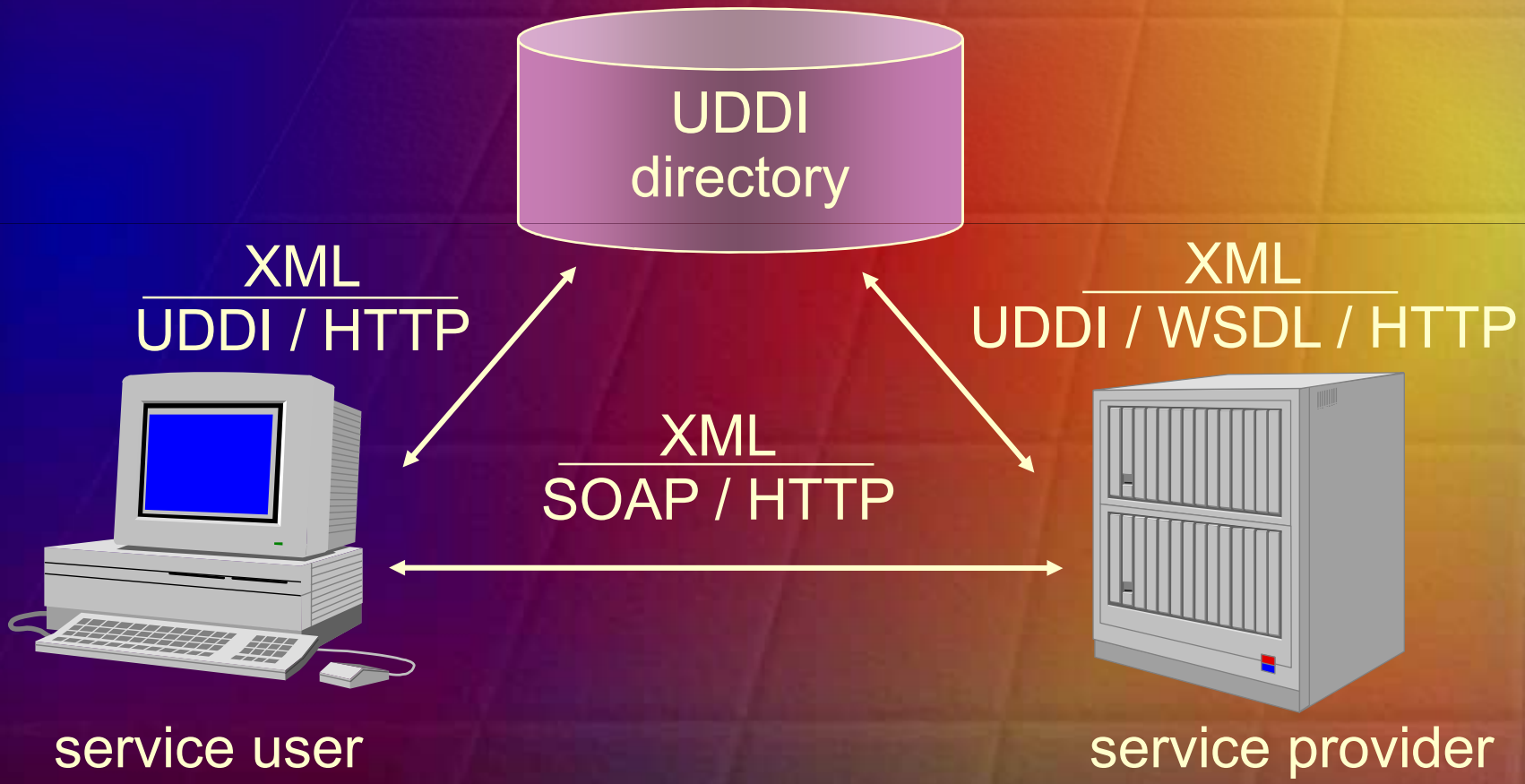
University of Ljubljana

denis.trcek@fri.uni-lj.si

Introduction

- Services oriented architectures (SOAs) are the core paradigm in contemporary user focused IT environments.
- The main standards are SOAP, UDDI and WSDL on top of XML.
- SOAs integrate (through choreography and / or orchestration) services from various administrative domains.

Introduction



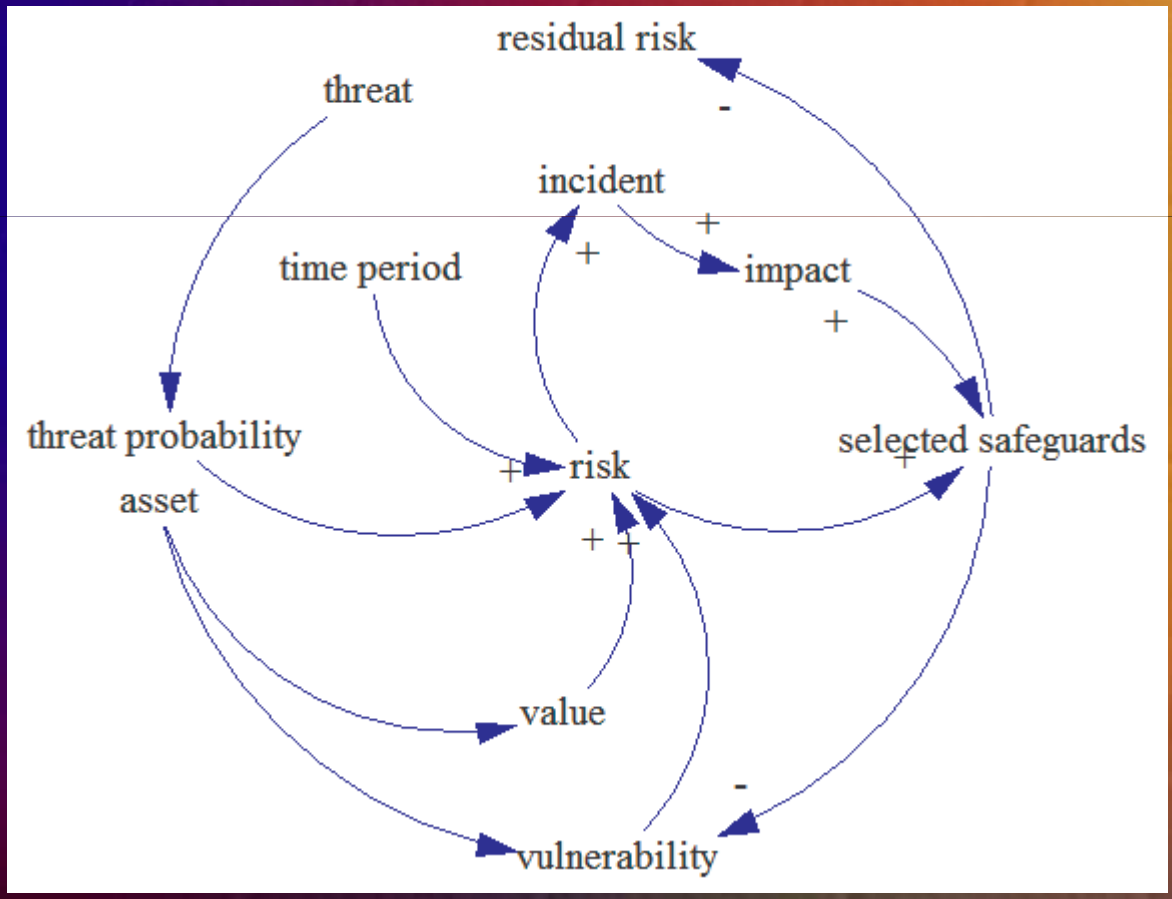
Economics of security and privacy

- 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)

- Risk-management elements and their relationships.



Risk management issues

- Risk management in main standards:
  - ISO 27003 / BS 7799-3, Information security management systems – Guidelines for information security risk management, London / Geneva, 2005.
  - NIST, Managing Risk from Information Systems, NIST SP 800-39 Draft, US Dept. Of Commerce, Washington D.C., 2007.
  - HIPAA, Basics of Risk Analysis and Risk Management, US Dept. Of Health & Human Services, Washington D.C., 2005.

Risk management in SOAs

- Risk management in ISO 27003.
- Risk management in NIST SP 800-30 and 800-39.

SC inf. system = {(*confidentiality*, *impact*), (*integrity, impact*), (*availability, impact*)}, where the acceptable values for potential impact are low, moderate, or high, and SC stands for security category.

threat description	level of threat	Low			medium			high		
	vulnerability level	L	M	H	L	M	H	L	M	H
level of asset value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Risk management in SOAs

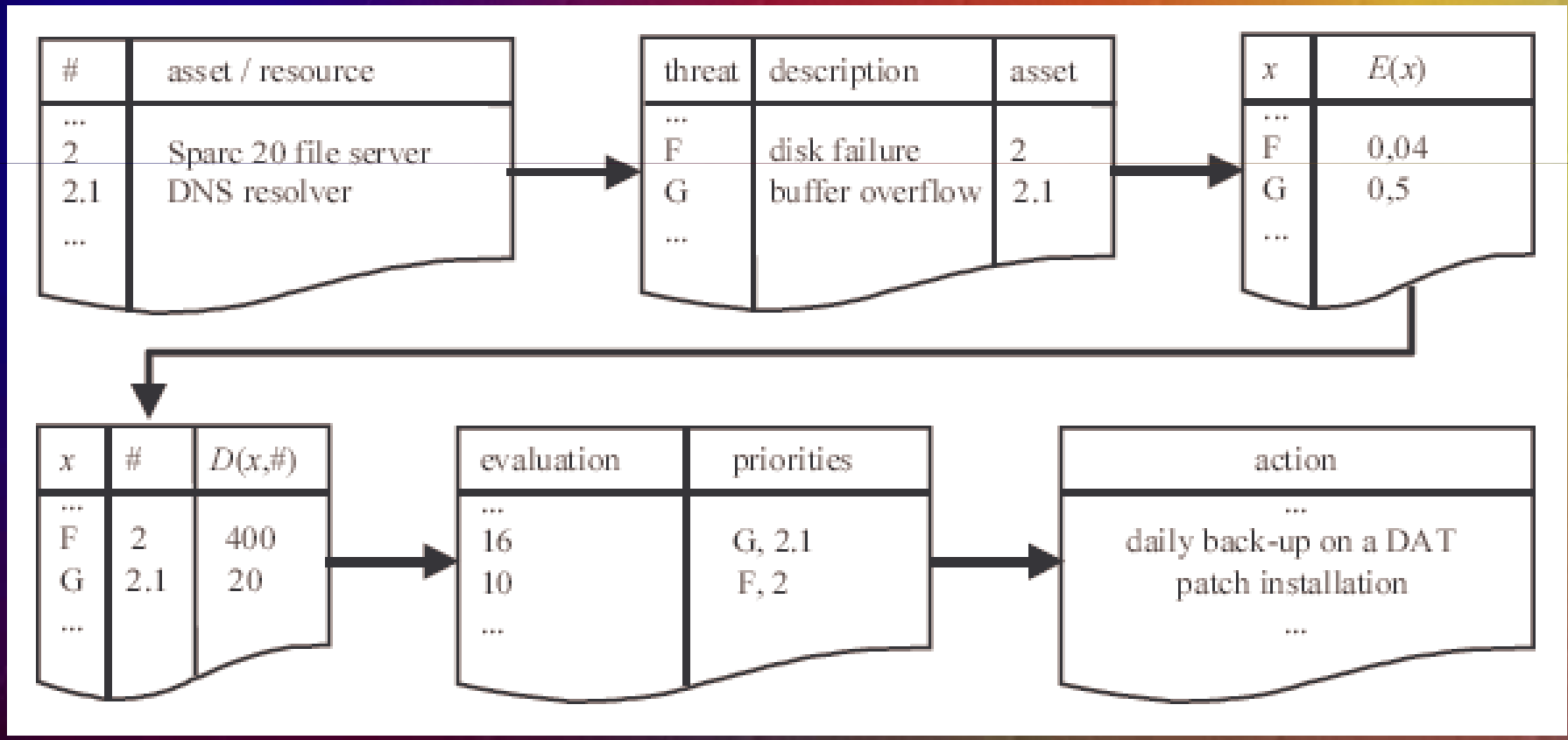
- Risk management in HIPAA.
  - QUALITATIVE METHOD
    - The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high,medium or low scale.

Risk management in SOAs

- Risk management in HIPAA.
  - QUANTITATIVE METHOD
    - In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

Risk management in SOAs

- Risk management - quantitative approach.



Risk management in SOAs

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

- Risk management - quantitative approach.

For example, having D = US$ 1,000 and E = 0.5 per annum, the first mitigation option with $M_1(x)$ = 0.5 results in expected annual loss of US$ 250 ($1,000 * 0.5 * 0.5). With mitigation option $M_2(x)$ = 0.1 the expected annual loss is US$ 50 ($1,000 * 0.5 * 0.1). Assume the cost of the first solution is US$ 100, and of the second solution US$ 300. The return on investment (ROI), which is obtained by dividing annual benefit by the investment amount, is calculated as follows. Firstly, savings minus mitigation costs are calculated, where savings are the difference between expected annual loss and modified annual loss [28]. Thus in the first case the savings are US$ 500 - US$ 250 = US$ 250 and, in the second US$ 500 - US$ 50 = US$ 450. Secondly, savings are evaluated relatively to required input, which results in the ROI for the first case to be US$ 250/US$ 100 = 2.5 and, for the second, US$ 450/US$ 300 = 1.5. This clearly identifies the winning safeguard.

Risk management in SOAs

- Structural view on security (and privacy) related costs:
  1. risk analysis,
  2. safeguards implementation and improvements (safeguards have to be treated from technical, organizational and legal point of view),
  3. safeguards operation,
  4. safeguards monitoring (go to 1 or 2).
- The key part is bullet 1, while the majority of costs comes from bullets 2 and 3.

Risk management in SOAs

- Our current research in the area of technology – metrics for lightweight protocols:
  - Emerging RFID based solutions – enormous potential and serious securtiy and privacy issues.
  - Costs viewed only from the perspective of chip implementation.
  - Our metrics enables quantitative valuation of RFID tags security and privacy implementation costs.

Conclusions

- Central problems related to RM and costs of security and privacy in SOAs:
  - Risk management remains largely treated by qualitative methods.
  - In many areas appropriate (quantitative) metrics is needed (e.g. what is the cost of implementation of a lightweight protocol).
  - SOAs lack standardized mechanisms for acquiring and exchange of costs related data (charging and biz-models issues).
- This defines our incentives for research within COST ECONOTEL.