Dynamic certificate lifetime calculation based on aggregated risk assessment

Alexander Beck, FIN, Otto-von-Guericke Universität Magdeburg

04.05.12
Motivation

- IT-Systems are protected nowadays by Public-Key-Infrastructures (PKI)
- PKI is based on digital certificates
- Certificate lifetime is fixed and ignores the actual risk of potential security breaches
Goal

• The calculation of the certificate lifetime shall depend on an aggregated risk calculation.

• This includes the following factors:
  • Security of the infrastructure
  • Security relevance of the sensitive informations
  • Vulnerability of the system
  • Further ones?
Trust = 1,0 * 0,8 * 0,6
or
Trust = (1,0 + 0,8 + 0,6) / 3
or ???

maxTime * Security of system

Lifetime = Security relevance of the sensitive informations
Related Work

• J. Huang and D. Nicol. A formal semantics based calculus of trust. In ITI Research Report, University of Illinois at Urbana-Champaign, 2008.
• J. Huang and D. Nicol. A Calculus of Trust and Its Application to PKI and Identity Management, University of Illinois at Urbana-Champaign, IDtrust '09 Proceedings of the 8th Symposium on Identity and Trust on the Internet, 2009.