Reputation Systems Security (Position Paper)

Roslan Ismail[1], Colin Boyd[1], Audun Josang[2], and Selywn Russell[1]

[1] Information Security Research Centre
Queensland University of Technology
Brisbane Qld 4001, Australia
{r.ismail,c.boyd,s.russell}@qut.edu.au
[2] Distributed Systems Technology Centre***
Queensland University of Technology
Brisbane Qld 4001, Australia
ajosang@dstc.edu.au

1 Abstract

The role of reputation systems is to record the behavior of participants in an e-commerce marketplace and then make information about each participants past behaviour available to potential transaction partners. Studies show that reputation systems have the potential of improving the quality of online markets. Unfortunately current reputation systems still suffer from various vulnerabilities. The information provided by reputation is intended for making decisions involving risk. It is therefore important to protect the completeness and integrity of the feedback and reputation information and to ensure that reputation systems are robust against deliberate malicious manipulation. Our work focuses on the security aspects of reputation systems with the aim of developing a security architecture for reputation systems. One problem is that participants are reluctant to give negative feedback even when it is appropriate for fear of retaliation. For this reason we have developed a solution for anonymity of feedback providers. This is important in order to allow participants to provide negative feedback when appropriate without fear of possible retaliation. Our solution [2] is based on cryptographic mechanisms; e-cash, designated verifier proof and knowledge proof. In some settings it is desirable for the reputation owner to control the distribution of his or her reputation information and to only disclose it to intended parties. We have developed a solution for this based on cryptographic certificates whereby the reputation owner can distribute his or her reputation information while not being able alter that information without detection. Again our solution is based on cryptographic mechanisms and digital certificates [2]. Apart from providing solutions for privacy we have also described security architectures that cover a combination of centralized and the distributed reputation systems [1]. Currently, we are working on solutions for off-line reputation systems and P2P reputation systems. For the former, we employ a proxy signature scheme and for the latter a ring signature scheme.

*** The work reported in this paper has been funded in part by the Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government's CRC Programme (Department of Industry, Science & Resources).

References

1. R. Ismail, C. Boyd, A. Josang, and S. Russell. A Security Architecture for Reputation Systems. *To appear at EC-WEB'03*, September 1-5, 2003.
2. R. Ismail, C. Boyd, A. Josang, and S. Russell. Strong Privacy in Reputation Systems. *To appear at WISA'03*, August 25-27, 2003.