Decision Support Systems
Available online 16 January 2013
In Press. Corrected Proof — Note to authors

Digital certificate management: Optimal pricing and CRL releasing strategies

Jie Zhang*, Nan Hu**, M.K. Raja***

* College of Business Administration, University of Texas, Arlington, TX, United States
** College of Business, University of Wisconsin at Eau Claire, Eau Claire WI, United States
*** College of Business, University of Wisconsin at Eau Claire, Eau Claire WI, United States

http://dx.doi.org/10.1016/j.dss.2012.12.043, How to Cite or Link Using DOI
Permissions & Reprints

View full text

Purchase $39.95

Abstract

The fast growth of e-commerce and online activities places increasing needs for authentication and secure communication to enable information exchange and online transactions. The public key infrastructure (PKI) provides a promising foundation for meeting such demand, in which certificate authorities (CAs) provide digital certificates. In practice, it is critical to understand consumer purchasing and revocation behaviors so that CAs can better manage the digital certificates and its CRL releasing process. To address this problem, we analytically model a CA’s pricing and revocation releasing strategies taking into consideration the users’ rational decisions. The model provides solutions to two main research questions: (1) How should the CA price the digital certificates? The price of the digital certificate should be determined by the expected losses of the user’s IT system, and the number of certificate revocations per period is expected to decrease over time during the lifecycle of the certificate. This result is supported by the empirical data from VeriSign. (2) How should the CA further propose a dynamic CRL releasing policy that suggests that the optimal releasing intervals within the lifecycle of a certificate should increase over time.

Keywords

Security management; Key Infrastructure (PKI); Certificate Authority (CA); Certificate Revocation List (CRL); Dynamic programming algorithm

Figures and tables from this article:

Fig. 1. Life cycle of a certificate.