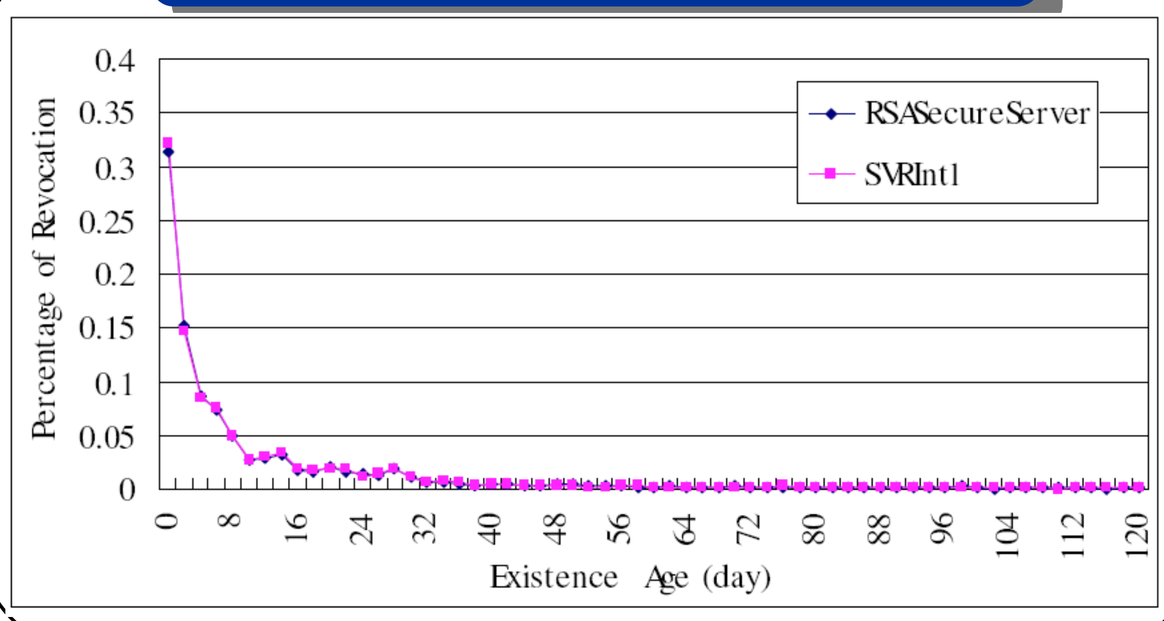
Data Application Security

SMU SINGAPORE MANAGEMENT UNIVERSITY
School of Information Systems

Associate Professor Yingjiu Li

DISTRIBUTION OF CERTIFICATE REVOCATION



CENTRAL CONCERNS & QUESTIONS

The major concern in data application security is to specify the security requirements for data-centric applications, and design information systems that meet the security requirements.

EMERGING IDEAS & INITIATIVES

An emerging idea in our research is to conduct empirical analysis on real-world data for better prediction or management of information security technology. Another idea is to embed user identification information into data for ownership protection or tamper detection.

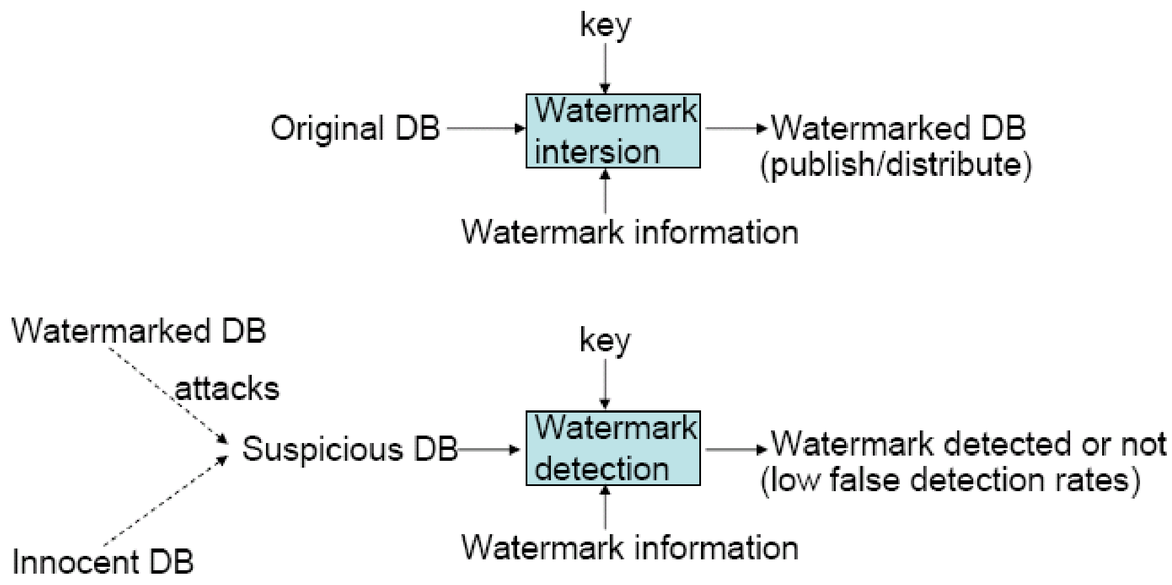
RESEARCH HIGHLIGHTS

➢Empirical analysis on market data of adopting information security technology such as trusted computing shows that traditional two-factor diffusion model based on influentials and imitators should be extended to include the effect of opponents as the third factor for better prediction of technology diffusions.

➢Based on the distribution of public key certificate revocations discovered from real data, optimal strategies are devised for certificate authorities to manage certificate revocation lists in a cost-effective manner.

➢A series of rights management techniques are designed for protecting numerical (non-multimedia) data sets. These techniques include robust watermarking, fragile watermarking, public watermarking, multiple watermarking, and collusion resistant fingerprinting, while the date sets being protected include relational data, categorical data, data cubes, and data streams. These techniques can be effectively used for ownership proving and traitor tracing in data distributions in the presence of attacks such as tuple/attribute insertion/deletion, random/selective value modification, data frame-up, and additional watermark/fingerprint insertion.

DATABASE WATERMARKING



FUNDING AND PEOPLE

• FUNDING: Flexible and efficient access control in collaborative environment. SMU Office of Research, Mar 2011 - Feb2012. .

• FUNDING: On the Safety of Next Generation of Access Control. SMU Office of Research, Oct 2004-Oct 2005.

•FUNDING: Techniques against Database Piracy. Wharton-SMU Research Center. Nov 2003-Oct 3004.

•FACULTY / RESEARCH STUDENTS / RESEARCH STAFF: Yingjiu Li, Robert Deng, Dan Ma, Ge Fu, Jie Guo, Divya Nalla, Chengyu Ma, Jianhui Huang

• EXTERNAL COLLABORATORS: Sushil Jajodia, Vipin Swarup, Huiping Guo, Nan Hu, Giri K. Tayi, Xinwen Zhang, Shouhuai Xu, Sean X. Wang, Ningning Wu

SELECTED PUBLICATIONS

1. Hasan Cavusoglu, Nan Hu, Yingjiu Li, Dan Ma: Information Technology Diffusion with Influentials, Imitators, and Opponents: Model and Preliminary Evidence. Journal of Management Information Systems (JMIS), 27(2), pages 305-334, 2010.
2. Chengyu Ma, Nan Hu, Yingjiu Li: On the Release of CRLs in Public Key Infrastructure. 15th USENIX Security Symposium (USENIX Security 2006), pages 17-28, Vancouver, Canada, July 31-August 4, 2006.
3. Yingjiu Li, Robert Deng: Publicly Verifiable Ownership Protection for Relational Databases. ACM Symposium on InformAtion, Computer, and Communication Security (ASIACCS), pages 78-89, Taipei, Taiwan, March 21-24, 2006.
4. Yingjiu Li, Vipin Swarup, Sushil Jajodia: Fingerprinting Relational Databases: Schemes and Specialties. IEEE Transactions on Dependable and Secure Computing (TDSC), 2(1): 34-45, 2005.