A Scheme for Privacy-preserving Data Dissemination

by L Lilien, b Bhargava
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

[11] V. Scarlata, B. Levine, and C. Shields, "Responder anonymity and anonymous peer-to-peer file sharing," in *Proc. IEEE ICNP*, Riverside, CA, 2001, pp. 272–280.

[12] M. Waldman, A. D. Rubin, and L. F. Cranor, "Publius: A robust, tamper-evident, censorship-resistant, web publishing system," in *Proc. USENIX Security Symp.*, 2000, pp. 59–72.

[13] L. Xiao, Z. Xu, and X. Zhang, "Low-cost and reliable mutual anonymity protocols in peer-to-peer networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 14, no. 9, pp. 829–840, Sep. 2003.

[14] I. Clarke, O. Sandberg, B. Wiley, and T. Hong, "Freenet: A distributed anonymous information storage and retrieval system," in *Proc. Workshop Design Issues Anonymity and Unobservability*, Berkeley, CA, 2000, pp. 45–66.

[15] I. Clarke, S. Miller, T. Hong, O. Sandberg, and B. Wiley, "Protecting free expression online with freenet," *IEEE Internet Comput.*, vol. 6, no. 1, pp. 40–49, Jan. 2002.

[16] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web transactions," *ACM Trans. Inf. Syst. Secur.*, vol. 1, no. 1, pp. 66–92, 1998.

[17] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," *Commun. ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[18] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE J. Sel. Areas Commun.—Special Issue on Copyright and Privacy Protection*, vol. 16, no. 4, pp. 482–494, May 1998.

[19] J. Bailes and G. Templeton, "Managing P2P security," *Commun. ACM*, vol. 47, no. 9, pp. 95–98, Sep. 2004.

[20] M. Agarwal, *Security Issues in P2P Systems*. (2002). [Online]. Available: www.ece.rutgers.edu/ parashar/Classes/01-02/ece579/slides/security.pdf

[21] J. Kong and X. Hong, "ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *Proc. 4th ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Annapolis, MD, Jun. 2003, pp. 291–302.

[22] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, "Geographic routing without location information," in *Proc. ACM Int. Conf. Mobile Computing and Networking*, San Diego, CA, Sep. 2003, pp. 96–108.

[23] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from mere connectivity," in *Proc. 4th ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Annapolis, MD, Jun. 2003, pp. 201–212.

[24] S. Buchegger and J. L. Boudec, "Cooperation of nodes," extended abstract in L. Buttyàn and Hubaux (eds.), "Report on a working session on security in wireless ad hoc networks", *ACM Mobile Comput. Commun. Rev. (MC2R)*, vol. 7, no. 1, pp. 74–94, 2003.

[25] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proc. 1st IEEE/ACM MobiHOC*, Boston, MA, Aug. 2000, pp. 87–96.

[26] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "p^5: A protocol for scalable anonymous communication," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, May 2002, pp. 58–70.

[27] S. Goel, M. Robson, M. Polte, and E. Sirer, "Herbivore: A scalable and efficient protocol for anonymous communication," Dept. Comput. Inform. Sci., Cornell Univ., Ithaca, NY, CIS Tech. Rep. TR2003-1890, Feb. 2003.

[28] B. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, Jul. 1970.

[29] R. Kalman, "A new approach to linear filtering and prediction problems," *Trans. ASME J. Basic Eng.*, ser. D, vol. 82, pp. 35–45, 1960.

[30] Y. Zhong, "Formalization of dynamic trust and uncertain evidence for user authorization," Ph.D dissertation, Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, 2005.

[31] N. Li, W. H. Winsborough, and J. C. Mitchell, "Distributed credential chain discovery in trust management," *J. Comput. Secur.*, vol. 11, no. 1, pp. 35–86, Feb. 2003.

[32] Trust-Enhanced Role Assignment (TERA) Prototype. (2004). http:// raidlab.cs.purdue.edu/zhong/NSFTrust/

A Scheme for Privacy-Preserving Data Dissemination

Leszek Lilien, *Senior Member, IEEE*, and
Bharat Bhargava, *Fellow, IEEE*

***Abstract*—An adequate level of trust must be established between prospective partners before an interaction can begin. In asymmetric trust relationships, one of the interacting partners is stronger. The weaker partner can gain a higher level of trust by disclosing private information. Dissemination of sensitive data owned by the weaker partner starts at this moment. The stronger partner can propagate data to others, who may then choose to spread data further. The proposed scheme for privacy-preserving data dissemination enables control of data by their owner (such as a weaker partner). It relies on the ideas of bundling sensitive data with metadata, an apoptosis of endangered bundles, and an adaptive evaporation of bundles in suspect environments. Possible applications include interactions among patients and healthcare providers, customers and businesses, researchers, and suppliers of their raw data. They will contribute to providing privacy guarantees, which are indispensable for the realization of the promise of pervasive computing.**

***Index Terms*—Data dissemination, data privacy protection, privacy, trust.**

I. Introduction

Any interaction, from a simple transaction to a complex collaboration, can start only after an adequate level of trust exists between interacting entities. *Trust* is defined as "reliance on the integrity, ability, or character of a person or thing" [1].

Use of trust is often implicit. Quite frequently, it is gained offline [6]. A user who downloads a file from an unfamiliar Web site trusts it implicitly by not even considering trust in a conscious way. A user who decides to buy an Internet service from an Internet service provider may build her trust offline by asking her friends for recommendations.

Privacy and trust are as closely related in computing environments as they are in social systems [6]. We define *privacy* as an entity's ability to control the availability and exposure of information about itself. This definition extends the scope of privacy from a *person* in the original definition [13] to an *entity*, including an organization or software. The extension is consistent with the use of the notion of "trust" also in relationship to artifacts [1], and with the common practice of antropomorphization of intelligent system components (such as objects and agents) in computer science.

An entity can choose to trade its privacy for a corresponding gain in its partner's trust in it [25]. The scope of a privacy disclosure should be proportional to the expected benefits—a customer applying for a mortgage must reveal much more personal data than one buying a book.

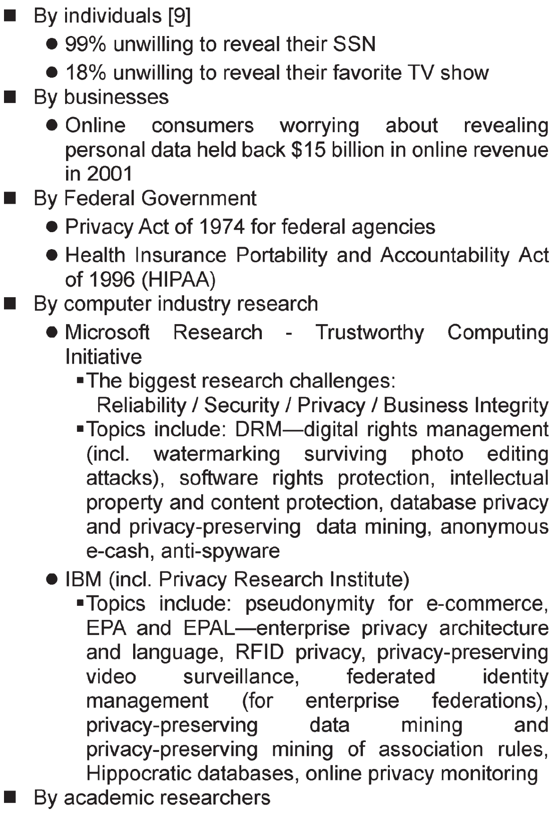
A mere perception of a threat to users' privacy from a collaborator may result in the substantial lowering of trust. This impedes the sharing

Manuscript received January 24, 2005; revised September 14, 2005. This work was supported in part by the National Science Foundation under Grants IIS-0209059 and IIS-0242840, in part by grants from the Defense Advanced Research Projects Agency (DARPA), IBM, and Cisco University Research Program (URP), and in part by a seed Grant from the Regenstrief Center for Healthcare Engineering (RCHE) at Purdue University. This paper was recommended by Guest Editors H. R. Rao and S. J. Upadhyaya.

L. Lilien is with the Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008 USA and affiliated with the Center for Education and Research in Information Assurance and Security (CERIAS) and the Regenstrief Center for Healthcare Engineering (RCHE), Purdue University, West Lafayette, IN 47907 USA (e-mail: llilien@cs.wmich.edu).

B. Bhargava is with the Department of Computer Sciences, CERIAS and RCHE, Purdue University, West Lafayette, IN 47907 USA (e-mail: bb@cs.purdue.edu).

Digital Object Identifier 10.1109/TSMCA.2006.871655



- By individuals [9]
  - 99% unwilling to reveal their SSN
  - 18% unwilling to reveal their favorite TV show
- By businesses
  - Online consumers worrying about revealing personal data held back $15 billion in online revenue in 2001
- By Federal Government
  - Privacy Act of 1974 for federal agencies
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- By computer industry research
  - Microsoft Research - Trustworthy Computing Initiative
    - The biggest research challenges: Reliability / Security / Privacy / Business Integrity
    - Topics include: DRM—digital rights management (incl. watermarking surviving photo editing attacks), software rights protection, intellectual property and content protection, database privacy and privacy-preserving data mining, anonymous e-cash, anti-spyware
  - IBM (incl. Privacy Research Institute)
    - Topics include: pseudonymity for e-commerce, EPA and EPAL—enterprise privacy architecture and language, RFID privacy, privacy-preserving video surveillance, federated identity management (for enterprise federations), privacy-preserving data mining and privacy-preserving mining of association rules, Hippocratic databases, online privacy monitoring
- By academic researchers

Fig. 1. Recognition of the need for privacy guarantees by different entities.

of sensitive data among interacting entities, and can result in a complete rejection of collaboration between prospective partners.

As Fig. 1 shows, the growing recognition of the importance of privacy is motivated not only by users' sensitivity about their personal data. Other factors include business losses due to privacy violations, and enactments of federal and state privacy laws.

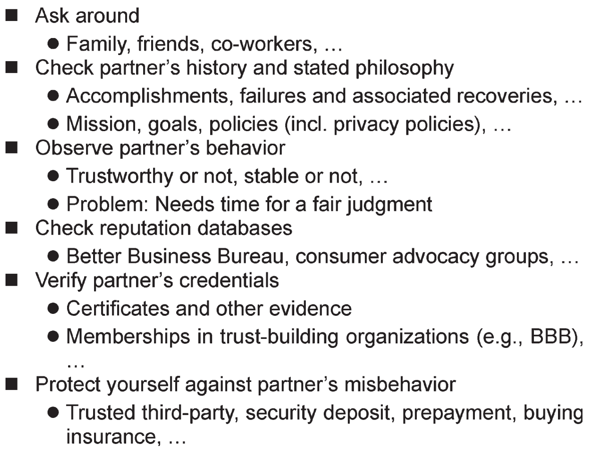
The main contribution of this paper—a scheme for privacy-preserving data dissemination—is presented in Section III. It is preceded by a discussion of the context in which it is to function. The trust and privacy backgrounds are presented in Section II. Section IV concludes the paper.

II. Trading Privacy for Trust in Asymmetric Trust Relationships

Trust relationships can be symmetric, which occurs between partners of similar stature, or asymmetric, which occurs when one partner's position is stronger vis-à-vis the other's. The *strength* of a party is defined by its capability to demand private information from the other party, and its means available in case when the other party refuses to comply. As a simple example, a bank is stronger than a customer requesting a mortgage loan.

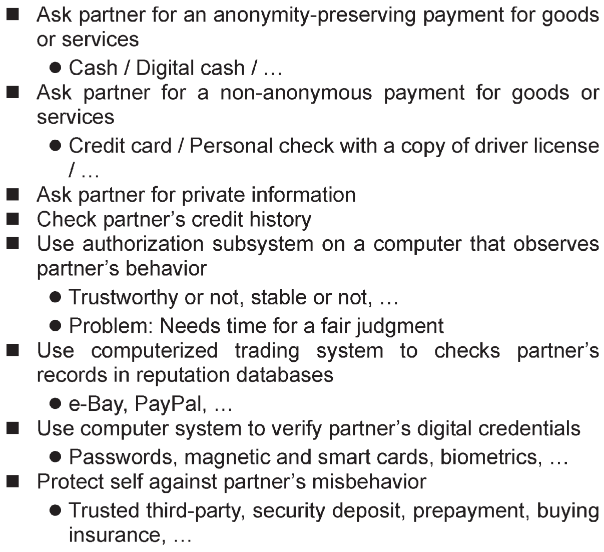
This paper concentrates on asymmetric relationships, so we interchangeably use the terms: "a weaker partner" and "a customer," as well as "a stronger partner" and "a company."

A customer's major weapon is information on a company's reputation, and some of its sources are shown in Fig. 2. Information also assists a company in its fight against customer fraud, as shown in Fig. 3. With the exception of the first item listed in Fig. 3, all others compromise the customer's anonymity and result in disclosing private information. In general, a weaker party must trade its privacy loss for a trust gain, which is required to start interactions with the stronger party.



- Ask around
  - Family, friends, co-workers, …
- Check partner's history and stated philosophy
  - Accomplishments, failures and associated recoveries, …
  - Mission, goals, policies (incl. privacy policies), …
- Observe partner's behavior
  - Trustworthy or not, stable or not, …
  - Problem: Needs time for a fair judgment
- Check reputation databases
  - Better Business Bureau, consumer advocacy groups, …
- Verify partner's credentials
  - Certificates and other evidence
  - Memberships in trust-building organizations (e.g., BBB), …
- Protect yourself against partner's misbehavior
  - Trusted third-party, security deposit, prepayment, buying insurance, …

Fig. 2. Means of building trust by a weaker partner in his stronger partner for business transactions.



- Ask partner for an anonymity-preserving payment for goods or services
  - Cash / Digital cash / …
- Ask partner for a non-anonymous payment for goods or services
  - Credit card / Personal check with a copy of driver license / …
- Ask partner for private information
- Check partner's credit history
- Use authorization subsystem on a computer that observes partner's behavior
  - Trustworthy or not, stable or not, …
  - Problem: Needs time for a fair judgment
- Use computerized trading system to checks partner's records in reputation databases
  - e-Bay, PayPal, …
- Use computer system to verify partner's digital credentials
  - Passwords, magnetic and smart cards, biometrics, …
- Protect self against partner's misbehavior
  - Trusted third-party, security deposit, prepayment, buying insurance, …

Fig. 3. Means of building trust by a stronger partner in her weaker partner for business transactions.

Privacy guarantees for dissemination of private data are necessary. Without them, many interaction opportunities are lost. Examples are patients' symptoms hidden from doctors, given up business transactions, lost research collaborations, and rejected social contacts. Perhaps most importantly, without privacy guarantees, the promise of pervasive computing will not be realized.

The careful dissemination of sensitive data, and protecting the weaker partner's privacy rights, are critical not only for both parties involved but also for the society in general. Still, protecting data privacy and providing appropriate mechanisms is mainly a responsibility of the stronger partner.

Privacy can be traded for trust in many application areas—including health care delivery, e-commerce, and location-based networking services. A highly trusted customer can get more benefits, such as discounts and better services, from a trusting business. To gain trust, she can trade in private digital credentials—certificates, recommendations, or past interaction histories.

Users are interested in answers to privacy and trust questions such as: 1) How much privacy is lost by disclosing given data? 2) How much does a user benefit by a certain trust gain? 3) How much privacy should a user be willing to sacrifice for a certain amount of trust gain?

Our solution proposed in [25] includes: a formalization of the privacy-for-trust trade, algorithms and metrics for estimating a privacy loss and a trust gain for a given credential set, and algorithms minimizing the privacy loss necessary for a required trust gain.

III. Privacy-Preserving Data Dissemination

A. Problem Statement and Challenges

Private data have their owner—an individual, a system, or an institution that they describe. A *guardian* is an entity entrusted by the owner of private data with their collection, processing, storage, and dissemination. We distinguish *primary guardians* (PGs), who interact directly with data owners, and subsequent or higher level guardians.

A guardian is allowed to share private data upon the owner's explicit consent. Any guardian may pass private data to a subsequent guardian, starting a *data-dissemination chain* (actually, this may be a cyclic graph). Risks of privacy violations grow with the chain length, and with the fallibility and vulnerabilities in its milieu. Under some circumstances, a guardian is required by the law to disclose data without the owner's consent—for instance, for public health reasons, by a court order, etc.

We state the research problem as follows: *The problem of privacy-preserving data dissemination* is defined as: assuring the privacy of sensitive data entrusted by their owner to a primary guardian for the entire data lifetime, which includes data collection, processing, storage, and dissemination to subsequent guardians, who in turn collect, process, store, and disseminate data.

B. Related Work

The Platform for Privacy Preferences (P3P) is a well-known protocol and tool suite for specifying privacy policies of Web sites and users' privacy preferences [10]. However, P3P is not a comprehensive privacy solution [23]. AT&T Privacy Bird is an implementation of P3P [2].

Privacy solutions for the Web (notably P3P) would be better utilized if they were a part of the data they are supposed to protect, not only for Web privacy but also for the entire information technology area [18]. In this way, they would become a part of metadata.

Metadata can be defined as data used for self-descriptiveness [16]. Examples of using self-descriptiveness in different contexts include name–value pairs [3], a metadata model [7], the Knowledge Interchange Format (KIF) language for knowledge bases [11], components in a context-aware mobile infrastructure [17], flexible data types for distributed systems [20], and a model for meta schema in federated databases [24].

Disseminated data need protection from illegitimate disclosures. We proposed the idea of coupling privacy-protection mechanisms with data [5] independently of the similar research direction suggested in the conclusions of an earlier survey paper [18]. Other approaches to protecting software clients or agents from a malicious host include [8]: 1) obfuscation; 2) tamper-proofing; and 3) watermarking or fingerprinting.

The self-destruction analogy is employed to secure mobile objects. In biology, there are two cell-destruction mechanisms: the chaotic destruction process of *necrosis* due to an injury, and an orderly self-destruction process of *apoptosis* [21]. In contrast to the former, the latter is "clean," i.e., no toxic waste is leaked to the cell's environment, so no inflammation is induced.

Mobile objects or agents, susceptible to many types of host attacks [4], [19], are commonly secured by running only on dedicated and tamper-resistant platforms—for example, on secure coprocessors [22]. In contrast, the Terra virtual machine-based platform [12] provides security on commodity hardware, by partitioning a hardware platform into isolated virtual "closed boxes."

C. Trust Model

An owner can build his trust in the PG in ways available to the weaker partner (cf., Fig. 2). Trusting the PG means trusting the integrity of the PG's data-sharing policies and practices and "transitively" trusting data-sharing partners of the PG. Transitive trust can be achieved in one of the following ways: 1) the PG provides a private data owner with an *a priori* list of subsequent guardians for data sharing; 2) the PG requests the owner's permission before each new dissemination of data; or 3) the PG uses a hybrid approach, combining the previous two—each for a fraction of higher level guardians.

D. Approach

The following scenario describes the operation of the proposed scheme in a healthcare environment. Suppose that a patient (a data owner) provides his health information to a nurse via an *electronic health record* (EHR) application (the PG). The EHR application obtains the patient's privacy preferences, and immediately creates an atomic *bundle*, which couples data and metadata, including the patient's preferences and hospitals' policies. Any subsequent data transmission must include complete bundles.

The atomicity of bundles prevents the nurse's EHR application from transmitting an incomplete bundle—such as a bundle missing the patient's privacy preferences—to an insurer's application (a secondary guardian). Whenever a delivery of a complete bundle fails, the insurer can recover it by asking for retransmission. Passing the bundle to a subsequent guardian can be repeated as long as it is allowed by the owner's preferences and the guardians' policies. This solves the problem of preserving privacy in the data dissemination for secure and reliable environments.

The scheme is extended to embrace malicious and unfamiliar environments. First, the *transmission atomicity* for the bundle is assured on the application or middleware level (using commitment protocols well known in database management systems). Second, we need atomic *apoptosis*, or clean self-destruction, of a bundle whenever it feels threatened. Third, we propose bundle *evaporation* when its private data and related metadata are not destroyed all at once but evaporate gradually. The active capabilities required of bundles—especially for apoptosis and evaporation—may require their implementation as intelligent agents or objects.

We now address in turn the three components of the proposed scheme.

1) Self-Descriptiveness and Metadata: Sensitive data are accompanied within the self-descriptive bundles by their metadata. Comprehensive metadata should include the following.

— *Owner's privacy preferences:* Read and write access circumstances. They include who or what, how, when, etc., is allowed to read or write private data.

— *Owner's contact information:* How to request owner's access permissions, or notify the owner of any accesses to his private data.

— *Guardians' privacy policies:* Privacy policies of primary and subsequent data guardians.

— *Metadata access conditions:* Verification and modification circumstances for metadata.

— *Enforcement specifications:* Describe allowed and/or prohibited access actions.

— *Data provenance:* Who created, modified, destroyed, or read any portion of the data.

— *Application-dependent and other components:* These may include the owner's trust levels for different contexts, and application-specific elements.

Self-descriptive bundles simplify *notifying* or *requesting permissions* from their owners, since contact information is within the metadata. If permission for a given request is granted in the metadata, the owner is only notified of an access to her private data. Otherwise, whenever her data are to be accessed in a way that is not allowed by the owner's preferences (or by a guardian's policy if accepted by the owner), she must be asked for a consent [14], [15], [23]. For very sensitive data, no default access permissions should be granted—each request requires an explicit permission. Requests and notifications are sent to owners immediately, periodically, or on demand. Communication channels include pagers, short message service (SMS), e-mail, or conventional mail.

2) Apoptosis: A bundle about to be compromised chooses apoptosis over risking a privacy disclosure. Apoptosis destroys both data and metadata to prevent inferences from metadata.

The apoptosis mechanism within a bundle can be implemented as a set of detectors setting off the associated apoptosis code. The code is activated when detectors determine a credible threat of a successful attack on the bundle by any host, including the destination guardian of a bundle being transmitted.

The detectors find the bundle's trust level for a host based on trust information from multiple sources—including the sending guardian, its neighbors, and reputation databases. Reputation databases collect information on behaviors of all hosts within the scope of their watch. A detector in a bundle scheduled to arrive at a host with a trust level below a certain threshold will discover danger and will trigger apoptosis. We have to deal with false-negative and false-positive indications of detectors.

We have different apoptosis threshold levels for hosts with different access permissions to private data. For example, higher trust levels are usually expected of the patient's home clinic than from a clinic visited by the vacationing patient.

The composite trust level is calculated, following our methods [26], from different pieces of evidence—including the source guardian's first-hand experience, its second-hand opinions from neighbors, and reputations obtained from databases.

3) Adaptive Evaporation: Perfect passing of bundles is not always desirable. If bundles can be captured by attackers, their owners want to see their data evaporated partially (e.g., have them deidentified) before they are disclosed. More hostile environments are "hotter" for bundles, inducing faster evaporation. To prevent inferences from metadata, all metadata evaporate in step with the associated data and in a manner that does not compromise data privacy in any other way. For instance, the owner's preferences for owner's data never evaporate earlier than data they protect.

We considered a number of different metrics for adaptive control of the degree of evaporation. First, the trust level can be obtained—as discussed for apoptosis—and used to control the required degree of evaporation. Second, in some environments trust is directly proportional to the *physical distance* from the data owner. Third, distance can be defined in a more sophisticated way, such as in terms of *data-dissemination hops* or *business-type similarity*. The latter metric would be useful in situations when an entity's trust is related not just to individual institutions but to a type of business (e.g., trusting a clinic more than an insurance company). Fourth, multidimensional composite metrics—including measures of trust, reliability, and security—are an option.

Instances of data evaporation include replacing exact data with approximate data, or up-to-date values with outdated values. Evaporation can be applied to images as well. For example, a close-up photo of a person's face can be replaced with a distant whole-body photo.

Apoptosis can be seen as a special case of evaporation, which follows a step function with a constant minimum value (no evaporation) initially, and the maximum value (complete evaporation) above a certain threshold.

IV. Conclusion and Future Work

We presented a novel scheme for privacy-preserving dissemination of sensitive data. The scheme relies on the ideas of creating *bundles* with data and metadata, *apoptosis* of attacked bundles, and adaptive *evaporation* of bundles in unfriendly environments. We placed the scheme in the context of trading privacy by a weaker interaction partner for gaining trust of a stronger partner.

We believe that the scheme can be extended to cover diverse confidential data, such as intellectual property, proprietary data, and trade, diplomatic, or military secrets. An efficient implementation will contribute to facilitating data-sharing collaborations in many areas, including business, education, government, health care, the military, and research.

Acknowledgment

The authors thank unanimous reviewers for their excellent feedback. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors.

References

[1] *The American Heritage Dictionary of the English Language*, 4th ed. Boston, MA: Houghton Mifflin, 2000.

[2] *AT&T Privacy Bird Tour*, Feb. 2004. [Online]. Available: http://privacybird.com/tour/1_2 beta/tour.html

[3] J. Bentley, "Programming pearls," *Commun. ACM*, vol. 30, no. 6, pp. 479–483, Jun. 1987.

[4] F. Bergadano, A. Giallombardo, A. Puliafito, G. Ruffo, and L. Vita, "Security agents for information retrieval in distributed systems," *Parallel Comput.*, vol. 22, no. 13, pp. 1719–1731, Feb. 1997.

[5] B. Bhargava, L. Lilien, and D. Xu, "Private and trusted interactions," presented at the 5th Annu. Information Security Symp. "Energizing the Enterprise: Cyber Security in Context," CERIAS, Purdue Univ., West Lafayette, IN. Mar. 2004. Slides. [Online]. Available: http://www.cerias.purdue.edu/news_and_events/events/symposium/2004/presentations/bharat_leszek_lilien.pdf

[6] B. Bhargava, L. Lilien, A. Rosenthal, and M. Winslett, "Pervasive trust," *IEEE Intell. Syst.*, vol. 19, no. 5, pp. 74–77, Sep./Oct. 2004.

[7] S. Bowers and L. Delcambre, "The uni-level description: A uniform framework for representing information in multiple data models," in *Proc. Int. Conf. Conceptual Modeling (ER)*, Chicago, IL, Oct. 2003, pp. 45–58.

[8] C. Collberg and C. Thomborson, "Watermarking, tamper-proofing, and obfuscation—Tools for software protection," Dept. Comput. Sci., Univ. Arizona, Tucson, Tech. Rep. 2000-03, 2000.

[9] L. F. Cranor, J. Reagle, and M. S. Ackerman, "Beyond concern: Understanding net users' attitudes about online privacy," AT&T Labs Res., Florham Park, NJ, Tech. Rep. TR 99.4.3, Apr. 1999.

[10] L. Cranor, "P3P: Making privacy policies more useful," *IEEE Secur. Priv.*, vol. 1, no. 6, pp. 50–55, Nov./Dec. 2003.

[11] M. Gensereth and R. Fikes, "Knowledge Interchange Format," Stanford Univ., Stanford, CA, Tech. Rep. Logic-92-1, 1992.

[12] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in *Proc. ACM Symp. Operating System Principles*, Bolton Landing, NY, Oct. 2003, pp. 193–206.

[13] The Internet Society, *Internet Security Glossary*, Aug. 2004. [Online]. Available: www.faqs.org/rfcs/rfc2828.html

[14] M. Langheinrich, "Privacy by design—Principles for privacy-aware ubiquitous systems," in *Proc. UbiComp*, vol. 2201, *Lecture Notes in*

Computer Science, G. D. Abowd, B. Brumitt, S. Shafer, Eds. Berlin, Germany:Springer-Verlag Oct. 2001, pp. 273–291. [Online]. Available: http://www.inf.ethz.ch/vs/publ/papers/privacy-principles.pdf

[15] D. M. Martin, Jr., R. M. Smith, M. Brittain, I. Fetch, and H. Wu, "The privacy practices of Web browser extensions," *Commun. ACM*, vol. 44, no. 2, pp. 45–50, Feb. 2001.

[16] R. McClatchey, Z. Kovacs, F. Estrella, J.-M. Le Goff, L. Varga, and M. Zsenei, "The role of meta-objects and self-description in an engineering data warehouse," in *Proc. IDEAS*, Montreal, QC, Canada, Aug. 1999, pp. 342–350.

[17] A. Rakotonirainy, "Trends and future of mobile computing," in *Proc. 10th Int. Workshop Database and Expert Systems Applications*, Florence, Italy, Sep. 1999, pp. 136–140.

[18] A. Rezgui, A. Bouguettaya, and M. Eltoweissy, "Privacy on the Web: Facts, challenges, and solutions," *IEEE Secur. Priv.*, vol. 1, no. 6, pp. 40–49, Nov./Dec. 2003.

[19] M. Saeb, M. Hamza, and A. Soliman, "Protecting mobile agents against malicious host attacks using threat diagnostic AND/OR tree," in *Proc. Smart Objects Conf.,* Grenoble, France, May 2003. [Online]. Available: http://www.grenoble-soc.com/proceedings03/Pdf/2-Saeb.pdf

[20] M. Spreitzer and A. Begel, "More flexible data types," in *Proc. IEEE 8th WETICE*, Stanford, CA, Jun. 1999, pp. 319–324.

[21] C. Tschudin, "Apoptosis—The programmed death of distributed services," in *Secure Internet Programming*, J. Vitek and C. Jensen, Eds. New York: Springer-Verlag, 1999.

[22] J. D. Tygar and B. Yee, "Dyad: A system for using physically secure coprocessors," in *Proc. Joint Harvard-MIT Workshop on Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment,* Cambridge, MA, Apr. 1993. [Online]. Available: http://www.cni.org/docs/ima.ip-workshop/Tygar.Yee.html

[23] U.S. Federal Trade Commission, *Privacy Online: A Report to Congress*, Jun. 1998.

[24] S. Urban and T. B. Abdellatif, "An object-oriented query language interface to relational databases in a multidatabase database environment," in *Proc. ICDCS*, Poznan, Poland, Jun. 1994, pp. 387–394.

[25] Y. Zhong and B. Bhargava, "Using entropy to trade privacy for trust," presented at the Workshop on Secure Knowledge Management (SKM 2004), Amherst, NY, Sep. 2004.

[26] Y. Zhong, B. Bhargava, Y. Lu, and L. Lilien, *A Computational Dynamic Trust Model for User Authorization*. submitted for publication.