Research Projects

Table of Contents

- Trust Management
  - RT: A Family of Role-based Trust-management Languages
  - Distributed Credential Chain Discovery
  - Constraint Datalog as a Foundation for Trust-Management Languages
  - Security Analysis in Trust Management
  - Delegation Logic
  - Analyzing SDSI's Linked Local Name Spaces
- Automated Trust Negotiation
- Applied Cryptography
  - Oblivious Signature-Based Envelope
- Trust-Management Applications
  - August: A Distributed Calendar Program
  - Digital U-STOR-IT: Secure Web-based File Sharing
- Other Projects
  - Certificate Revocation in Public Key Infrastructure
  - Securing Proxy-based Distributed Systems

Trust Management

One main goal of computer security is to ensure that access to resources is restricted to parties with legitimate access permissions. Access control in decentralized, open, and distributed systems is different from access control in the traditional setting of operating systems and database systems. The main difference is that the resource owner and the requester are often unknown to one another. The term *trust management* was coined in Blaze, Feigenbaum, and Lacy 1996 to describe an approach to distributed access control where decisions are based on policy statements that encode trust and delegation relationships among parties. Policy statements are made by multiple principals. Some statements may be digitally signed to ensure their authenticity and integrity; these are called credentials. Some statements may be stored in local trusted storage and do not need to be signed. A trust-management (TM) language has a syntax for specifying policy statements and queries and a semantic relation for determining whether a query is true for a given set of policy statements.

- RT: A Family of Role-based Trust-management Languages

  Together with John Mitchell and Will Winsborough, we developed the RT family of Role-based Trust-management languages. RT combines the strengths of role-based access control and previous trust-management systems such as Delegation Logic and SDSI (Rivest and Lampson).


- Distributed Credential Chain Discovery

  Credentials in trust management may be issued and stored in a distributed manner. In an Internet-scale system, there are potentially millions of credentials. One needs a mechanism that can answer queries by retrieving only the relevant
credentials and a way to guarantee that relevant credentials can be found when needed. Together with Will Winsborough and John Mitchell, we developed goal-directed algorithms to do distributed credential chain discovery for RT0, the most basic component in the RT framework. We also introduced a storage-typing scheme, which guarantees well-typed credential chains can be discovered, and helps make the discovery process more efficient. These algorithms are implemented in a TM engine for RT0. The engine is used in demonstration applications in our Agile Management of Dynamic Collaboration project and the Attribute Based Access Control project at NAI Laboratories.


**Constraint Datalog as a Foundation for Trust-Management Languages**

Trust-management (TM) languages need a declarative and formal foundation. Although Datalog was used in several TM languages and has been the best logical foundation for TM languages to date, Datalog does not meet the practical need for policies about common structured resources, such as file hierarchies. By using ideas from the field of constraint databases, we showed that Datalog extended with constraints is a promising and expressive alternative that eliminates some deficiencies of Datalog without sacrificing any of the attractive features that make Datalog appealing for trust management. This is joint work with John Mitchell.


**Security Analysis in Trust Management**

Trust management has delegation as its key power. Because one organization may delegate partial control to another organization, it is natural to ask what permissions may be granted as the result of policy changes by other organizations. Together with John Mitchell and Will Winsborough, we studied security properties such as safety and availability in the RT framework using a trust-management model. We showed that many properties can be determined efficiently using logic programs, and proved that the most complicated cases are decidable but intractable. These results are somewhat surprising. In *Harrison, Ruzzo, and Ullman 1976*, it was shown that a basic form of safety analysis in the context of the well-known access matrix model is undecidable. Our trust-management model is more powerful in certain ways than the HRU access matrix model, and the security properties we considered are more than simple safety. In our paper, we explained the differences between the HRU model and our TM model.


**Delegation Logic**

In my PhD research, together with Joan Feigenbaum and Benjamin Grosof, I developed Delegation Logic (DL), a logic-based TM language. DL extends the logic-programming language Datalog with expressive delegation constructs that feature delegation depth and a wide variety of principal structures (including, but not limited to, k-out-of-n thresholds). The approach of designing TM languages by extending Datalog is later used in RT, SD3 and Binder. The monotonic subset of DL, called D1LP, has been implemented using XSB.


XD1LP: An XSB implementation of D1LP

- Analyzing SDSI's Linked Local Name Spaces

SPKI/SDSI 2.0 (RFC 2793) is the merged effort of SPKI (Ellison et al.) and SDSI (Rivest and Lampson). Its feature of linked local names has generated a lot of interests in the security research community. By interpreting local names as distributed groups, I developed a simple logic program for SPKI/SDSI's linked local-name scheme and proved that it is equivalent to the name-resolution procedure in SDSI 1.1 and the 4-tuple-reduction mechanism in SPKI/SDSI 2.0.


Automated Trust Negotiation

Trust management uses digital credentials that document attributes of principals. Credentials may contain sensitive information and need protection. Automated Trust Negotiation (ATN) is an approach to regulate the exchange of sensitive credentials by using access-control policies.

- Automated Trust Negotiation in Attribute-Based Access Control

Together with Will Winsborough, we introduced the notion of attribute acknowledgment policies (Ack policies), which protects against unauthorized leakage of information that one has certain attributes, in addition to protecting the transmission of credentials. We also introduced the trust target graph (TTG) protocol, which supports a credential language that has delegation, Ack policies, and distributed storage of credentials.


Applied Cryptography

- Oblivious Signature-Based Envelope

Previous work on Automated Trust Negotiation based on access-control techniques cannot handle cyclic policy interdependency. Suppose user A wants to convince user B that she has a certain credential and user B wants to do the same for A, but neither one wants to reveal their credentials first, access-control-based ATN protocols had to conclude negotiation failure. Together with Dan Boneh and Wenliang Du, we introduced a cryptographic primitive called oblivious signature-based envelope (OSBE), which can break cyclic policy interdependency in ATN and can be applied to other privacy sensitive scenarios. We developed an efficient and provably secure OSBE protocol for credentials signed using RSA signatures and built one-round OSBE for Rabin and BLS signatures from recent constructions for identity-based encryption.
Trust-Management Applications

Two demonstration applications were developed under the Agile Management of Dynamic Collaboration project to experiment with policy development and requirement and to demonstrate the RT framework. They both use the RT0 inference engine I developed.

- **August: A Distributed Calendar Program**
  
  With help from John Mitchell, Ajay Chander, and Raghuram Sivalanka, I implemented August; it is a calendar program written in Java. It can be used as a single-user calendar program or a distributed calendar program for a group of users. In August, each user has a calendar and can specify policy. Policy determines who is allowed to view which part of the user's calendar and who is allowed to add an activity of a certain kind at a certain time. Each August user declares different roles (or groups), e.g., friends, family members, colleagues, etc., and defines the members of these roles. Users may use delegation in defining role members. For example a user may specify that "my family members' friends are also friends". This adds many users to a role, using a single policy statement.

  - Instructions for installing and using August

- **Digital U-STOR-IT: Secure Web-based File Sharing**
  
  Together with John Mitchell and several undergraduate students at Stanford University, we developed U-STOR-IT, a web-based file sharing system. A user connects to U-STOR-IT using a browser. User authentication is done using client-side certificates, generated by the U-STOR-IT Certification Authority site. Users control access to their lockers and files by specifying policy statements, which may refer to other users' group-definition statements. U-STOR-IT also provides collaboration tools such as basic version control, per-file bulletin board, and in-system messaging.

  - Instructions for accessing U-STOR-IT

Other Projects

- **Certificate Revocation in Public Key Infrastructure**
  
  In this work, we considered certificate revocation from three high-level perspectives: temporal nonmonotonicity, user interfaces, and risk management. We argued that flawed understanding of these three aspects of revocation schemes has caused these schemes to be unnecessarily costly, complex, and confusing. This is joint work with Joan Feigenbaum.


- **Securing Proxy-based Distributed Systems**
  
  In proxy-based distributed systems such as Jini and RMI-based systems, services register their proxies in directories, and client programs look up proxies in directories and use proxies as if they are local services. Such systems are subject to various kinds of attacks. Together with John Mitchell and Derrick Tong, we studied these attacks, proposed an architecture to defend against them, and implemented a toolkit that helps others to write applications using the architecture. We are currently working on applying the toolkit to sample applications and performance study. This work will be reported in near future.