

Research Statement

Kazuhiro Minami

My research interest lies in security and privacy in a decentralized computing environment. In such an environment, which is common in mobile or pervasive computing, there exists no single trusted authority that manages all the resources and security policies. Therefore, I am particularly interested in studying techniques that reduce the trusted computing base necessary for sharing information across different administrative domains. My prime research agenda is to build a secure system that ensures security properties, such as confidentiality, and integrity, for information distributed across multiple domains. I primarily apply a logic-based approach to manage information and security policies in a flexible, manageable, and scalable way.

Previous and current research

In pervasive computing, many applications adapt their behavior based on the user's context (e.g., location and situation) in order to meet the user's requirements, which might be changing over the time. However, users have significant privacy concern, because the system that runs the context-aware applications could access the personal information of users. As part of my thesis research [4, 5], I examined the potential for authorization decisions to be based on the context of the user making the request. Such a context-sensitive authorization scheme is necessary to enable a mobile user whose identity is unknown to a system to access a resource in a flexible way.

My dissertation addresses the issue of protecting confidential information involved in an authorization process. Context information, such as the location of a user, could contain users' personal information or organizations' proprietary information. I took a logic-based approach, in which authorization policies and context information are expressed as logical statements, and built a distributed proof system that enables multiple hosts to make an authorization decision in a peer-to-peer way, while preserving each host's security policies. Our system eliminates the necessity for having a universally trusted central host that maintains all the policies and context information; the proof that derives the authorization decision is decomposed into subproofs produced by different hosts. Existing trust management systems and distributed authorization systems need to collect all the credentials issued by remote servers to a central server that makes an authorization decision.

The major contribution of my thesis is the design and analysis of a novel distributed, cryptographic algorithm that evaluates an authorization query in a decentralized way. The algorithm is based on a new security model for specifying trust in terms of integrity and confidentiality on authorization policies and facts. I prove the correctness (soundness) of the algorithm. I implemented the system by extending a Prolog engine and also developed a caching and revocation mechanism [6] that handles dynamic context information efficiently. Our experimental results show that the amortized performance of our system is scalable to dozens of servers in different domains.

I also have a strong interest in other security problems in pervasive computing. I studied an access-control mechanism [2] for protecting information in an event dissemination system, Solar, which was developed at Dartmouth. I mainly addressed the problem of automatically deriving an access-control policy on high-level context information from policies on lower-level information. There are numerous ways to derive context information from raw sensor data, and it is, therefore, infeasible to manually specify access-control policies on high-level information. I designed and implemented an access-control mechanism that automatically derives access-control policies for derived data and enforces those policies. I also conducted a detailed performance study of the access-control mechanism to show that it is scalable to a large number of users [3].

In a course project, I built an e-voting system [1] to demonstrate the advantage of using a secure coprocessor (IBM 4758) inside a web server to protect clients' sensitive information. Our approach significantly simplified complicated cryptographic protocols in existing e-voting systems.

Future directions

In the future, I would like to do research on secure and scalable information dissemination infrastructure for pervasive computing. Considering the amount of private information that is monitored with various sensing technologies, I think that user privacy will continue to be a central issue in pervasive computing. Since the users have different trust assumptions about the infrastructure of pervasive computing, such an infrastructure should be highly decentralized and consist of numerous servers that collaborate in a peer-to-peer way. I plan to study distributed algorithms that perform aggregation of information across different information sources that have different security policies. I am particularly interested in adopting techniques in the literature of secure multi-party computation and anonymization to protect the sources' privacy from the information receiver while developing other techniques that make the system scalable to large numbers of servers. I am also interested in reducing the complexity of managing policies in a decentralized environment. I plan to study techniques that enable administrators to understand the behavior of systems with complex policies by providing feedback while protecting confidential policies.

In the long term, I plan to pursue various system security problems in the wider context of distributed computing including grids, sensor networks, and ad-hoc networks, and to study other aspects of security properties such as availability and reliability.

References

- [1] Shan Jiang, Sean Smith, and Kazuhiro Minami. Securing Web Servers against Insider Attack. In *17th Annual Computer Security Applications Conference (ACSAC'01)*, pages 265–276, New Orleans, Louisiana, December 2001.
- [2] Kazuhiro Minami and David Kotz. Controlling access to pervasive information in the “Solar” system. Technical Report TR2002-422, February 2002.
- [3] Kazuhiro Minami and David Kotz. Controlling access to pervasive information. In *First International Conference on Mobile Systems, Applications, and Services (MobiSys'03) Poster Session*, May 2003.
- [4] Kazuhiro Minami and David Kotz. Secure context-sensitive authorization. In *Third IEEE International Conference on Pervasive Computing and Communications (PerCom'05)*, pages 257–268, Kauai, Hawaii, March 2005.
- [5] Kazuhiro Minami and David Kotz. Secure context-sensitive authorization. *Journal of Pervasive and Mobile Computing*, 1(1):123–156, March 2005.
- [6] Kazuhiro Minami and David Kotz. Scalability in a secure distributed proof system. In *Proceedings of the Fourth International Conference on Pervasive Computing (Pervasive'06)*, May 2006.