Adrian Perrig
Associate Professor
Cybersecurity Laboratory, SCS
4 September 2007

Research Topic
Network Trust Domain

Research Problem
How do you maintain computer security from network attacks emanating internal to the trust domain?

Problem Statement
Given a network trust domain and malicious code, construct attestation that enables a verifier to obtain assurance of what code is being executed on nodes inside the network.

Problem Description
Nodes in a computer network may execute a malicious code on the network. If the malicious node is external to our trust domain, many attacks can be avoided through authentication and encryption. Attacks emanating internal to the trust domain, however creates a greater challenge. Code attestation enables a verifier to obtain assurance of what code an un-trusted node is executing. Programs running on a remote system store hash codes on a PCR register that can be securely transmitted to a verifier. Unfortunately, there are still weaknesses in this system. The goal of research is to improve security internal to the trust domain.

Computer Science Perspective
This research is focused on improving the internal security of a network. This is important for maintaining a network and guarding against an attack for a variety of applications.

Disciplines Actively Involved
Mathematics

Other Discipline Involved
Cryptography is widely used in this research. Cryptography is an application of abstract algebra (mathematics) that studies message secrecy. Issues in complexity theory and information theory are also used in this research.

Actively Involved Discipline is defined as a discipline associated with an investigator working on the research problem.

References

- Kuo, Cynthia, Mark Luk, Rohit Negi, Adrian Perrig. "Message-In-a-Bottle: User-Friendly and Secure Key Deployment for Sensor Nodes" In *Proceedings of the ACM*

Conference on Embedded Networked Sensor System (SenSys 2007), Sydney, Austrialia. November, 2007.

- Franklin, Jason, Vern Paxson, Adrian Perrig, and Stefan Savage. "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants" In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007), A*lexandria, Virginia, October 29 - November 2, 2007, November, 2007.

- Studer, Ahren, Mark Luk, and Adrian Perrig. "Efficient Mechanisms to Provide Convoy Member and Vehicle Sequence Authentication in VANETs." In *Proceedings of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm'07)*, September, 2007.

- Han, Jun, Abhishek Jain, Mark Luk, and Adrian Perrig. "Don't Sweat Your Privacy: Using Humidity to Detect Human Presence." In *Proceedings of 5th International Workshop on Privacy in UbiComp (UbiPriv'07)*, September, 2007.

By imccullo
Updated imccullo