Project Title: Enforcing Access Control in Control Flow of Sensor Applications

Investigator: Qijun Gu

Department: Computer Science

Project Summary:

In this project, the PI studied several exploitation techniques by which an attacker can make self-propagating mal-packets to compromise sensors in a network. To counteract such attacks, the PI developed three defense schemes. Two schemes are based on existing defense techniques: S2Guard based on StackGuard, and S2Shuffle based on code space randomization. The third defense scheme is a novel self-healing scheme that enforces access control in the control flow of sensor applications and recovers the sensor application from compromised tasks when a control flow attack is captured. The scheme embeds randomized marks and access control code at particular locations to detect malicious control flow manipulation, then quickly removes a compromised task from the application and restore the sensor to a normal state. The three defense schemes have been implemented and tested in MICA2 sensors to verify their security and analyze their overhead.

The major achievement of the project includes (a) two conference papers accepted in ACM Conference on Wireless Network Security, 2008 and 2009, which is a highly competitive conference with an acceptance rate around 15%; (b) one journal paper submitted to Ad Hoc Networks Journal, Elsevier; (c) one submitted NSF CAREER proposal; (d) one invited research talk at University of Houston. The project also advanced the PI's research with undergraduates. Three undergraduates were involved in this project. Two students co-authored the papers. One student gave a poster talk on the Security Awareness Day at Texas State University-San Marcos.

In conclusion, the PI successfully completed the project. All the proposed tasks have been finished and all the proposed objectives have been achieved.

Publications: Q. Gu, C. Ferguson, R. Noorani, "Towards Self-propagating Mal-packets in Sensor

Networks: Attacks and Defenses", Ad Hoc Networks Journal, Elsevier. (in review)

C. Ferguson, Q. Gu, H. Shi. "Self-healing Control Flow Protection in Sensor Applications", IEEE Transaction on Secure and Dependable Computing, (to submit)

Presentations: C. Ferguson, Q. Gu, H. Shi. "Self-healing Control Flow Protection in Sensor Applications", Proceedings of ACM Conference on Wireless Network Security, 2009.

Q. Gu and R. Noorani, "Towards Self-propagate Mal-packets in Sensor Networks" Proceedings of ACM Conference on Wireless Network Security, 2008.

Perform Arts Activities:

Q. Gu, "Towards Self-propagate Mal-packets in Sensor Networks", Invited Research Talk at University of Houston, 2008.

C. Ferguson, "Sensor, Heal Thyself!", Poster on Security Awareness Day, Texas State University at San Marcos, 2008.

"How to Hack and Secure Sensor Applications", Demos and Software, http://www.cs.txstate.edu/~qg11/download.htm

O. Barrera, Q. Gu, "Heap Management in TinyOS", Technical Report, Texas State University at San Marcos, 2008.

External Grants Applied: Q. Gu, "CAREER: Software-based Defense in Networks of Embedded Systems", NSF CAREER, 2008.

Student Number: 3