Final Project Report

To: technicalreports@afosr.af.mil
Subject: Annual Progress Statement to Dr. Robert L. Herklotz

Contract/Grant Title: Intrusion Detection and Forensics for Self-defending Wireless Networks
Contract/Grant #: FA9550-07-1-0074
Reporting Period: 1 December 2006 to 30 November 2010

Accomplishments: Our proposed self-defending wireless networks have three components: 1) automatic detection and signature generation for zero-day polymorphic worms; 2) situational-aware analysis and forensics for botnet scan, and 3) vulnerability analysis of wireless network protocols. We are able to complete the tasks and even exceed what we planned to achieve.

In the first year, we finished the first component, automatic detection and signature generation for zero-day polymorphic worms, and started to work on the second component of intrusion forensics for botnet scan. Through evaluation with real-world polymorphic worms and real network traffic, we demonstrate that our approach significantly outperforms existing approaches such as Polygraph in terms of efficiency, accuracy, and attack resilience. We also started the collaboration with AFRL researchers such as Dr. Keesook Han on the detection and forensics of botnet.

In the second year, we finished the second component, situational-aware analysis and forensics for botnet scan, and we've started to work on the third component of vulnerability analysis of wireless network protocols. Our analysis draws upon extensive honeynet data to explore the prevalence of different types of scanning, including properties, such as trend, uniformity, coordination, and darknet avoidance. In addition, we design schemes to extrapolate the global properties of scanning events (e.g., total population and target scope) as inferred from the limited local view of a honeynet. Cross-validating with data from DShield shows that our inferences exhibit promising accuracy. We have collaborated with AFRL researcher Dr. Keesook Han on the detection and forensics of botnet. We have a joint paper in IEEE COMPSAC 2008 conference as shown below.

In the third and extended forth year, we focus on the last component. We identified a practical way to launch DoS attacks on security protocols by triggering exceptions. Through experiments, we show that even the latest strongly authenticated protocols such as PEAP, EAP-TLS and EAP-TTLS are vulnerable to these attacks. Real attacks have been implemented and tested against TLS-based EAP protocols, the major family of security protocols for Wireless LAN, as well as the Return Routability of Mobile IPv6, an emerging lightweight security protocol in new IPv6 infrastructure. Countermeasures for detection of such attacks and improvements of the protocols to overcome these types of DoS attacks are also proposed and verified experimentally.

Archival publications (conference/journal papers and book chapters published) during reporting period:
15. Yao Zhao, Sagar Vemuri, Jiazhen Chen, Yan Chen, Hai Zhou and Zhi (Judy) Fu, Exception Triggered DoS Attacks on Wireless Networks, in the Proc. of the 39th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-DCCS), 2009


17. Yao Zhao, Zhaosheng Zhu, Yan Chen, Dan Pei, and Jia Wang, Towards Efficient Large-Scale VPN Monitoring and Diagnosis under Operational Constraints, IEEE INFOCOM (main conference), 2009


Patens filed:


Software/data release and impact to the community:

In 2006, we released our polymorphic worm signature generator Hamsa and its related test polymorphic worms~\cite{monitor-intrusion-detection}. They have been used by various institutes such as Columbia University, UT Austin, Purdue, Georgia Tech, UC Davis, /etc. In 2010, we release the NetShield system, a network-based Intrusion Detection and Prevention System using massive vulnerability signatures~\cite{nshield}. So far, it has been downloaded by dozens of institutes/companies from seven countries in the world (USA, China, Canada, India, Iran, Sri Lanka, and Algeria), including well-known institutes such as UIUC and University of Toronto.
In this YIP project, we proposed self-defending wireless networks have three components: 1) automatic detection and signature generation for zero-day polymorphic worms; 2) situational-aware analysis and forensics for botnet scan, and 3) vulnerability analysis of wireless network protocols. In summary, we fulfill the task completely and have achieved significant results as follows: (1) 20 peer-reviewed conference papers and 9 journal papers in top venues such as ACM SIGCOMM, ACM/USENIX NSDI, NDSS, and ACM Transaction in Networking (ToN), (2) 4 book chapters, (3) 3 pending patents, and (4) numerous articles that are currently under review. Furthermore, my YIP research was featured in the article entitled "AFOSR-Supported YIP Research Leads to Algorithms That Deflect Network Attackers", in Air Force Print News, October 18, 2010.