# 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 compoent. 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:

1. Zhichun Li, Anup Goyal, and Yan Chen, "Honeynet-based Botnet Scan Traffic Analysis", invited book chapter for Botnet Detection: Countering the Largest Security Threat, Springer, 2007.
2. R. Schweller, Z. Li, Y. Chen, Y. Gao, A. Gupta, E. Pearson, Y. Zhang, P. Dinda, M. Kao, and G. Memik, Reversible Sketches: Enabling Monitoring and Analysis over High-speed Data Streams, in ACM/IEEE Transaction on Networking, Volume 15, Issue 5, Oct. 2007.
3. Y. Chen, D. Bindel, H. Song, B. Chavez, and R. H. Katz, An Algebraic Approach for Scalable Overlay Network Monitoring: Algorithms, Evaluation, and Applications, in ACM/IEEE Transaction on Networking, Volume 15, Issue 5, Oct. 2007.
4. Zhichun Li, Lanjia Wang, Yan Chen and Zhi Fu, Network-based and Attack-resilient Length Signature Generation for Zero-day Polymorphic Worms, in the Proc. of *the 15th IEEE International Conference on Network Protocols (ICNP),* Nov. 2007.
5. Yao Zhao, Yan Chen, Bo Li, and Qian Zhang, Hop ID: A Virtual Coordinate based Routing for Sparse Mobile Ad Hoc Networks, in IEEE Transaction on Mobile Computing, Volume 6, Number 9, September 2007.
6. Ehab Al-Shaer and Yan Chen, Integrated Fault and Security Management, invited book chapter for Information Assurance: Dependability and Security in Networked Systems, Morgan Kaufmann Publishers, 2007.
7. Yan Gao, Yao Zhao, Robert Schweller, Shobha Venkataraman, Yan Chen, Dawn Song, and Ming-Yang Kao, "Detecting Stealthy Spreaders Using Online Outdegree Histograms", in the Proc. of *the 15th IEEE International Workshop on Quality of Service (IWQoS),* June 2007.
8. Yao Zhao and Yan Chen, A Suite of Schemes for User-level Network Diagnosis without Infrastructure, in the Proc. of *IEEE INFOCOM*, April 2007.
9. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, Chi Yin Cheung and Xing Li, End-to-end Inference of Router Packet Forwarding Priority, in the Proc. of *IEEE INFOCOM*, April 2007.
10. Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, and Keesook Han, "Botnet Research Survey", 32nd Annual IEEE International Computer Software and Applications Conference (COMPSAC), 2008.
11. Chengchen Hu, Sheng Wang, Jia Tian, Bin Liu, Yu Cheng, and Yan Chen, Accurate and Efficient Traffic Monitoring Using Adaptive Non-linear Sampling Method, in the Proc. of *IEEE INFOCOM, 2008*
12. Leiwen Deng, Yan Gao, Yan Chen, and Alexsander Kuzmanovic, Pollution Attacks and Defenses for Internet Caching Systems, in Journal of Computer Networks, Volume 52, Issue 5, 2008.
13. Yao Zhao, Yan Chen, and Sylvia Ratnasamy, Load balanced and Efficient Hierarchical Data-Centric Storage in Sensor Networks, in the Proc. of *the fifth IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2008* (64/300=21.3%).
14. Yan Chen, Dynamic, Scalable, and Efficient Content Replication Techniques, invited book chapter for Content Delivery Networks: Principles and Paradigms, Springer, 2008.

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
16. Zhichun Li, Anup Goyal, Yan Chen, and Vern Paxson, Automating Analysis of Large-Scale Botnet Probing Events, in the Proc. of ACM Symposium on Information, Computer and Communications Security (ASIACCS), 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
18. Yao Zhao, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Chen, and Eliot Gillum, BotGraph: Large Scale Spamming Botnet Detection, in the Proc. of the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI) 2009.
19. Yao Zhao and Yan Chen, "Algebraic Approaches for Scalable End-to-End Monitoring and Diagnosis", invited book chapter for Algorithms for Next Generation Network Architecture, Springer, 2009. ISBN: 978-1-84882-764-6
20. Yao Zhao and Yan Chen, "FAD and SPA: End-to-end Link-level Loss Rate Inference without Infrastructure", in the Journal of Computer Networks, 53(9): 1303-1318, 2009.
21. Yao Zhao, Yan Chen, and David Bindel, "Towards Unbiased End-to-End Network Diagnosis", in ACM/IEEE Transaction on Networking (ToN), Volume 17, Number 6, Dec. 2009.
22. Kai Chen, David R. Choffnes, Rahul Potharaju, Yan Chen, Fabian E. Bustamante, Dan Pei, and Yao Zhao, Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes From P2P Users, in the Proc. of the Fifth ACM International Conference on emerging Networking Experiments and Technologies (CoNEXT), 2009.
23. Zhaosheng Zhu, Vinod Yegneswaran, and Yan Chen, Using Failure Information Analysis to Detect Enterprise Zombies, full paper, in the Proc. of the 5th International Conference on Security and Privacy in Communication Networks (SecureComm), 2009.
24. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y. Zhao, Detecting and Characterizing Social Spam Campaigns, in the Proc. of ACM SIGCOMM IMC 2010.
25. Zhichun Li, Gao Xia, Hongyu Gao, Tang Yi, Yan Chen, Bin Liu, Junchen Jiang, and Yuezhou Lv, NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks, in the Proc. of ACM SIGCOMM 2010.
26. Kai Chen, Chuanxiong Guo, Haitao Wu, Jing Yuan, Zhenqian Feng, Yan Chen, Songwu Lu, Wenfei Wu, Generic and Automatic Address Configuration for Data Center Networks, in the Proc. of ACM SIGCOMM 2010.
27. Zhichun Li, Yan Gao, and Yan Chen, HiFIND: A high-speed flow-level intrusion detection approach with DoS resiliency, Journal of Computer Networks, Volume 54, Issue 8, June 2010.

28. Zhichun Li, Ming Zhang, Zhaosheng Zhu, Yan Chen, Albert Greenberg, and Yi-Min Wang, WebProphet: Automating Performance Prediction for Web Services, in the Proc. of ACM/USENIX NSDI 2010.
29. Chengchen Hu, Bin Liu, Hongbo Zhao, Kai Chen and Yan Chen, "DISCO: Memory Efficient and Accurate Flow Statistics for Network Measurement", in the Proc. of IEEE ICDCS, 2010.
30. Zhichun Li, Anup Goyal, Yan Chen, and Aleksandar Kuzmanovic, Measurement and Diagnosis of Address Misconfigured P2P Traffic, in the Proc. of IEEE INFOCOM (main conference), 2010.
31. Chengchen Hu, Kai Chen, Yan Chen and Bin Liu, Evaluating Potential Routing Diversity for Internet Failure Recovery, in the Proc. of IEEE INFOCOM (mini conference), 2010.
32. Lanjia Wang, Zhichun Li, Yan Chen, Zhi (Judy) Fu, and Xing Li, Thwarting Zero-Day Polymorphic Worms With Network-Level Length-Based Signature Generation, in ACM/IEEE Transaction on Networking (ToN), Volume 18, Issue 1, 2010.
33. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, and Xing Li, POPI: A User-level Tool for Inferring Router Packet Forwarding Priority, in ACM/IEEE Transaction on Networking (ToN), Volume 18, Issue 1, 2010.

Patens filed:

1. Zhichun Li, Lanjia Wang, Yan Chen, and Zhi Fu, "Method and Apparatus to Facilitate Generating Worm-Detection Signatures Using Data Packet Field Lengths", filed on December 18, 2007. U.S. Patent Application No. 11/985,760.
2. Jia Wang, Yan Chen, Dan Pei, Yao Zhao, and Zhaosheng Zhu, "Towards Efficient Large-Scale Network Monitoring and Diagnosis Under Operational Constraints", filed on January 2009. U.S. Patent Application No. 12/186,096.
3. Yan Chen, Zhichun Li, Gao Xia and Bin Liu, "Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense," filed on July 29, 2010, Patent Application No. 12/846,541.

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.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.**

| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 12-01-2012 | Final report | Dec. 2006 to Nov. 2010 |

**4. TITLE AND SUBTITLE**
(YIP-07) INTRUSION DETECTION AND FORENSICS FOR SELF-DEFENDING WIRELESS NETWORKS

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**
FA9550-07-1-0074

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Yan Chen

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Northwestern University
2145 Sheridan Rd,
Evanston, IL 60208

**8. PERFORMING ORGANIZATION REPORT NUMBER**
NU CUFS #: 0650-350-FF18

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
AFOSR
Suite 325, Room 3112
875 N. Randolph Street
Arlington, VA 22203-1768

**10. SPONSOR/MONITOR'S ACRONYM(S)**
AFOSR

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
FA9550-07-1-0074

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
Statement ean be publiely released.

AFRL-OSR-VA-TR-2012-0075

**13. SUPPLEMENTARY NOTES**

20120918152

**14. ABSTRACT**
In this YIP project, we proposed self-defending wireless networks have three components: 1) automatie detection and signature generation for zero-day polymorphie worms; 2) situational-aware analysis and forensies for botnet sean, and 3) vulnerability analysis of wireless network protoeols. In summary, we fulfill the task completely and have achieved significant results as follows: (1) 20 peer-reviewed conferenee papers and 9 journal papers in top venues suеh as ACM SIGCOMM, ACM/USENIX NSDI, NDSS, and ACM Transaction in Networking (ToN), (2) 4 book chapters, (3) 3 pending patents, and (4) numerous artieles that are eurrently under review. Furthermore, my YIP research was featured in the artiele entitled "AFOSR-Supported YIP Research Leads to Algorithms That Defleet Network Attaekers", in Air Force Print News, October 18, 2010.

**15. SUBJECT TERMS**
Self-defending, wireless networks, intrusion detection, zero-day, polymorphic worms, signature generation, situational-awareness, forensics, botnets, vulnerability analysis, network protocols.

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Yan Chen |
| U | U | U | UU | | 19b. TELEPHONE NUMBER *(Include area code)* 847-491-4946 |