Final Report for Period: 08/2007 - 07/2008
Submitted on: 06/24/2009
Principal Investigator: Lee, Wenke .
Award ID: 0133629
Organization: GA Tech Res Corp - GIT
Submitted By:
Lee, Wenke - Principal Investigator
Title:
CAREER: Adaptive Intrusion Detection Systems

Project Participants

Senior Personnel

Name: Lee, Wenke
Worked for more than 160 Hours: Yes
Contribution to Project:
Wenke advises 7 Ph.D. students, 2 MS thesis students, and 3 undergraduate senior design projects. In addition, Wenke teaches an undergraduate 'Computer and Network Security' course and a graduate Network Security course each year.

Both of these courses were created as part of the teaching plan of the CAREER project. Wenke receives excellent feedback/evaluation on these courses and continues to make improvements. The course materials (PowerPoint lecture slides and homework/projects) are made available on the Web. Several colleagues from other universities, e.g., Peng Ning of the Computer Science Department at NC State, have been using these materials to develop their courses.

The research plan of is CAREER project has three main thrusts.

In anomaly detection, Wenke directs Ph.D. students Prahlad and Oleg to work on an information-theoretic based framework for constructing features and models for anomaly detection, and dynamic and static analysis approaches to generate anomaly detection models for program executions.

In alert correlation, Wenke directs Ph.D. student Xinzhou to develop algorithms for finding new attack step relationships and discovering stealth attack plans.

In real-time IDS architecture and performance optimization, Wenke directs MS student Mohamed and undergraduate students Brian Lee and Craig Wampler to work on a network processor based network node IDS (NNIDS). We have developed the first NNIDS that runs on Intel IXP 1200.

Post-doc

Graduate Student

Name: Fogla, Prahlad
Worked for more than 160 Hours: Yes
Contribution to Project:
Prahlad works on anomaly detection. He studied information-theoretic measures for anomaly detection. He also worked on dynamic analysis approach to generate anomaly detection models of program execution. He is currently working on optimizing the efficiency of real-time anomaly detector. More specifically, he has developed a tree data structure for storing normal patterns and efficient algorithms for variable-length substring matching.

Prahlad was a main contributor to the following paper:

'Anomaly Detection Using Call Stack Information.'
Henry H. Feng, Oleg Kolesnikov, Prahlad Fogla, Wenke Lee, and Weibo Gong
In Proceedings of The 2003 IEEE Symposium on Security and Privacy, Oakland, CA, May 2003.

Name: Qin, Xinzhou

Worked for more than 160 Hours: Yes

Contribution to Project:

Xinzhou works on alert correlation, which is his thesis topic. Xinzhou has developed a framework for alert clustering/aggregation, prioritization, and correlation. His main constribution was a method for discovering new attack step relationships using very weak domain knowledge. This is a significant advance because the existing alert correlationships rely on hard-coded patterns.

Xinzhou is entering his fifth year of the Ph.D. program and is expected to graduate in a year. His main publications are:

'Discovering Novel Attack Strategies from INFOSEC Alerts'.
Xinzhou Qin and Wenke Lee.
In Proceedings of The 9th European Symposium on Research in Computer Security (ESORICS 2004) , French Riviera, France, September 2004 (to appear).

'Statistical Causality Analysis of INFOSEC Alert Data'.
Xinzhou Qin and Wenke Lee
In Proceedings of The 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003), Pittsburgh, PA, September 2003.

Name: Kone, Mohamed

Worked for more than 160 Hours: Yes

Contribution to Project:

Mohamed works in real-time IDS architecture and performance optimization, his MS Thesis topic area. Mohamed has developed the first NNIDS that runs on Intel IXP 1200. The NNIDS is based on the open-source IDS Snort but with significant changes. These include splitting several Snort modules into smaller components to take advantage of IXP's pipelined processors, and moving detection as early in the pipeline as possible to improve throughput.

Mohamed was a main contributor to a paper describing our NNIDS:

'A Hardware Platform for Network Intrusion Detection and Prevention'.
Chris Clark, Wenke Lee, David Schimmel, Didier Contis, Mohamed Kone, and Ashley Thomas
In Proceedings of The 3rd Workshop on Network Processors and Applications (NP3), Madrid, Spain, February 2004.

Name: Gu, Guofei

Worked for more than 160 Hours: Yes

Contribution to Project:

Guofei participated in the work on adaptive real-time intrusion detection systems. He is supported in part by this grant. In particular, his trip to the IEEE Symposium on Security and Privacy is supported by this grant.

Name: Dagon, David

Worked for more than 160 Hours: Yes

Contribution to Project:

David worked on analysis techniques for constructing anomaly detection models for programs. He is supported in part by this grant. In particular, his trip to the IEEE Symposium on Security and Privacy is supported by this grant.

Name: Sharif, Monirul

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Singh, Kapil

Worked for more than 160 Hours: Yes

Contribution to Project:

Name: Royal, Paul

Worked for more than 160 Hours: Yes

Contribution to Project:

Undergraduate Student

Technician, Programmer

Other Participant

Name: Cabrera, Joao

Worked for more than 160 Hours: No

Contribution to Project:

Joao is an expert in control and optimization. His current reserach interests are mainly in real-time IDS performance optimization. We collaborated on research in real-time IDS architecture. We co-authored several papers on this topic. In addition, we teamed up for several funded Army research projects on IDS implementation and anomaly detection.

Joao was a main contributor of the paper:

'Performance Adaptation in Real-Time Intrusion Detection Systems.'
Wenke Lee, Joao B. D. Cabrera, Ashley Thomas, Niranjan Balwalli, Sunmeet Saluja, and Yi Zhang
In Proceedings of The 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002), Zurich, Switzerland, October 2002.

Name: Giffin, Jon

Worked for more than 160 Hours: Yes

Contribution to Project:

Jon (Ph.D. student at University of Wisconsin at Madison) worked with David on analysis techniques for building anomaly detection models for programs. He is not supported by this grant.

Name: Jha, Somesh

Worked for more than 160 Hours: Yes

Contribution to Project:

Somesh (Assistant Professor at University of Wisconsin at Madison) worked with Jon and David on analysis techniques for building anomaly detection models for programs. He is not supported by this grant.

Research Experience for Undergraduates

Organizational Partners

Other Collaborators or Contacts

The PI has worked with Dr. Joao Cabrera of Scientific Systems Company Inc. and Prof. Weibo Gong of UMASS at Amhurst. The PI collaborated with Dr. Cabrera on IDS architecture and performance optimization, and Prof. Gong on anomaly detection. We have co-authored papers. In addition, the PI has several funded projects with Dr. Cabrera and one project with Professor Gong.

Activities and Findings

Research and Education Activities: (See PDF version submitted by PI at the end of the report)

Findings: (See PDF version submitted by PI at the end of the report)

Training and Development:

This project has given the PI the opportunity to collaborate with researchers in other institutions, often at the PI's initiatives. The PI also gained experience in guiding Ph.D. students.

More specifically, with the support of this grant, the PI is able to tackle some very hard problems instead of the 'low-hanging fruits'. In anomaly detection, we are developing a framework, based on information-theoretic measures, that provides the general understanding and guidelines for constructing features and models that are both accurate and efficient. In alert correlation, we focus on detecting 'new' attack step relaionship and 'stealth' attack plans.

By working on these hard problems, the PI has gained a better and deeper understanding of computer security and has improved research productivity and impact.

More importantly, the Ph.D. students are developing their skills in reserach and learn to select good research problems. All students involved in this project have published papers in top security conferences in the past two years.

Outreach Activities:

Our work in alert correlation has attracted commercial interests. We are woking with SecureWorks (a IDS/IPS vendor and managed security service provider) to test our algorithms using live alert data from customers' netowrks.

Our work in NNIDS on IXP 1200 has also attracted commercial interests. There have been several inquiries from start-ups. But we are not ready yet because we feel that we still need to make a lot of improvement on our current system.

In the past two years, the PI has worked with two companies on their SBIR proposals/projects. These companies are doing research and development work for DoD, and are looking to further develop our algorithms in anomaly detection and real-time adaptive intrusion detection.

In Spring 2006, the PI co-founded Damballa Inc. a company specialized in botnet detection. This start-up is based on our research in network-based and host-based anomaly detection.

We released a version of PolyUnpack to the research community. Several research groups are using this tool in the research in malware analysis.

Journal Publications

Prahlad Fogla and Wenke Lee, "q-Gram Matching Using Tree Models", IEEE Transactions on Knowledge and Data Engineering, p. 433, vol. 4, (2006). Published,

Books or Other One-time Publications

Henry H. Feng, Oleg Kolesnikov, Prahlad Fogla, Wenke Lee, and Weibo Gong
, "Anomaly Detection Using Call Stack Information
", (2003). Conference Proceedings, Published
Collection: Proceedings of The 2003 IEEE Symposium on Security and Privacy
Bibliography: In Proceedings of The 2003 IEEE Symposium on Security and Privacy, Oakland, CA, May 2003

Wenke Lee, Joao B. D. Cabrera, Ashley Thomas, Niranjan Balwalli, Sunmeet Saluja, and Yi Zhang
, "Performance Adaptation in Real-Time Intrusion Detection Systems", (2002). Conference Proceedings, Published
Collection: Proceedings of The 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002)
Bibliography: In Proceedings of The 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002), Zurich, Switzerland, October 2002

Henry H. Feng, Jonathon T. Giffin, Yong Huang, Somesh Jha, Wenke Lee, and Barton P. Miller
, "Formalizing Sensitivity in Static Analysis for Intrusion Detection", (2004). Conference Proceedings, Published
Collection: Proceedings of The 2004 IEEE Symposium on Security and Privacy
Bibliography: In Proceedings of The 2004 IEEE Symposium on Security and Privacy

Chris Clark, Wenke Lee, David Schimmel, Didier Contis, Mohamed Kone, and Ashley Thomas
, "A Hardware Platform for Network Intrusion Detection and Prevention", (2004). Conference Proceedings, Published
Collection: Proceedings of The 3rd Workshop on Network Processors and Applications (NP3)
Bibliography: In Proceedings of The 3rd Workshop on Network Processors and Applications (NP3)

David Dagon, Xinzhou Qin, Guofei Gu, Wenke Lee, Julian Grizzard, John Levin, and Henry Owen, "HoneyStat: Local Worm Detection Using Honeypots", (2004). Conference Proceedings, Accepted
Collection: Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004)
Bibliography: Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004)

Xinzhou Qin and Wenke Lee, "Discovering Novel Attack Strategies from INFOSEC Alerts", (2004). Conference Proceedings, Accepted
Collection: Proceedings of The 9th European Symposium on Research in Computer Security (ESORICS 2004)
Bibliography: Proceedings of The 9th European Symposium on Research in Computer Security (ESORICS 2004)

Xinzhou Qin and Wenke Lee, "Statistical Causality Analysis of INFOSEC Alert Data", (2003). Conference Proceedings, Published
Collection: Proceedings of The 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003)
Bibliography: Proceedings of The 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003)

Jon Giffin, David Dagon, Somesh Jha,
Wenke Lee, and Barton Miller, "Environment-Sensitive Intrusion
Detection", (2005). Conference Proceedings, Accepted
Collection: Proceedings of the International
Symposium on Recent Advances in
Intrusion Detection (RAID)
Bibliography: Jon Giffin, David Dagon, Somesh Jha,
Wenke Lee, and Barton Miller.
Environment-Sensitive Intrusion
Detection. In Proceedings of the
International Symposium on Recent
Adva

David Dagon, Wenke Lee, and Richard
Lipton., "Protecting Secret Data from Insider
Attacks", (2005). Conference Proceedings, Published
Collection: Proceedings of The Ninth International
Conference on Financial Cryptography
and Data Security (FC'05)
Bibliography: David Dagon, Wenke Lee, and Richard
Lipton. Protecting Secret Data from
Insider Attacks. In Proceedings of The
Ninth International Conference on
Financial Cryptography and

Guofei Gu, David Dagon, Xinzhou Qin,
Monirul I. Sharif, Wenke Lee, and
George F. Riley, "Worm Detection, Early Warning, and
Response Based on Local Victim
Information", (2004). Conference Proceedings, Published
Collection: Proceedings of the 20th Annual
Computer Security Applications
Conference (ACSAC 2004)
Bibliography: G. Gu, D. Dagon, X. Qin, M. I. Sharif,
W. Lee, and G. F. Riley. Worm
Detection, Early Warning, and
Response Based on Local Victim

Information. In Proceedings of ACSAC
20

Xinzhou Qin and Wenke Lee, "Attack Plan Recognition and Prediction Using Causal Networks", (2004). Conference Proceedings, Published
Collection: In Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC 2004)
Bibliography: Xinzhou Qin and Wenke Lee. Attack Plan Recognition and Prediction Using Causal Networks. In Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC

Joao B.D. Cabrera, Jaykumar Gosar, Wenke Lee, and Raman K. Mehra, "On the Statistical Distribution of Processing Times in Network Intrusion Detection", (2004). Conference Proceedings, Published
Collection: Proceedings of the 43rd IEEE Conference on Decision and Control (CDC 2004)
Bibliography: J. B.D. Cabrera, J. Gosar, W. Lee, and R. K. Mehra. On the Statistical Distribution of Processing Times in Network Intrusion Detection. In Proceedings CDC 2004, Decembe

George F. Riley, Monirul I. Sharif, and Wenke Lee, "Simulating Internet Worms", (2004). Conference Proceedings, Published
Collection: Proceedings of the 12th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)
Bibliography: George F. Riley, Monirul I. Sharif, and Wenke Lee. Simulating Internet Worms. In Proceedings of MASCOTS, Volendam, The Netherlands, October 2004

Prahlad Fogla, Monirul Sharif, Roberto Perdisci, Oleg Kolesnikov, and Wenke Lee., "Polymorphic Blending Attacks.", (2006). Conference Proceedings, Accepted
Collection: Proceedings of The 15th USENIX Security Symposium (SECURITY '06)
Bibliography: 2. Prahlad Fogla, Monirul Sharif, Roberto Perdisci, Oleg Kolesnikov, and Wenke Lee. Polymorphic Blending Attacks. In Proceedings of The 15th USENIX Security Symposium (SECU

Collin Mulliner, Giovanni Vigna, David Dagon, and Wenke Lee., "Using Labeling to Prevent Cross-Service Attacks Against Smart Phones.", (2006). Book, Accepted
Collection: Proceedings of The 3rd Conference on Detection of Intrusions & Malware, and

Vulnerability Assessment (DIMVA 2006)
Bibliography: C. Mulliner, G. Vigna, D. Dagon, and
W. Lee. Using Labeling to Prevent
Cross-Service Attacks Against Smart
Phones. In Proceedings of The 3rd
Conference on Detection of
In

Guofei Gu, Prahlad Fogla, Wenke Lee,
and Douglas Blough., "DSO: Dependable Signing Overlay.", (2006). Conference Proceedings, Published
Collection: Proceedings of The 4th International
Conference on Applied Cryptography and
Network Security (ACNS '06).
Bibliography: Guofei Gu, Prahlad Fogla, Wenke Lee,
and Douglas Blough. DSO:
Dependable Signing Overlay. In
Proceedings of The 4th International
Conference on Applied Cryptography
and

Roberto Perdisci, David Dagon, Wenke
Lee, Prahlad Fogla, and Monirul Sharif., "Misleading Worm Signature Generators
Using Deliberate Noise Injection.", (2006). Conference Proceedings, Published
Collection: Proceedings of The 2006 IEEE
Symposium on Security and Privacy.
Bibliography: R. Perdisci, D. Dagon, W. Lee, P. Fogla,
and M. Sharif. Misleading Worm
Signature Generators Using Deliberate
Noise Injection. In Proceedings of The
2006 IEEE Symposium on

David Dagon, Cliff Zou, and Wenke Lee., "Modeling Botnet Propagation Using Time
Zones.", (2006). Book, Published
Collection: Proceedings of The 13th Annual Network
and Distributed System Security
Symposium (NDSS 2006)
Bibliography: 7. David Dagon, Cliff Zou, and
Wenke Lee. ?
Modeling Botnet Propagation Using
Time Zones. ?
In Proceedings of The 13th Annual
Network and Distributed System
Security Sym

Monirul Sharif, Kapil Singh, Jon Giffin,
andWenke Lee., "Understanding Precision in Host Based
Intrusion Detection: Formal Analysis and
Practical Models.", (2007). Conference Proceedings, Accepted
Bibliography: M. Sharif, K. Singh, J. Giffin,
and W. Lee. Understanding
Precision in Host Based Intrusion
Detection: Formal Analysis and
Practical Models. In Proceedings of
RAID 2007,

David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard Lipton, and Shabsi Walfish., "Intrusion-Resilient Key Exchange in the Bounded Retrevial Model.", (2007). Conference Proceedings, Published
Bibliography: 2. David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard Lipton, and Shabsi Walfish. Intrusion-Resilient Key Exchange in the Bounded Retrevial Model. In Proceedings

Roberto Perdisci, Guoei Gu, and Wenke Lee., "Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems,", (2006). Conference Proceedings, Published
Bibliography: Roberto Perdisci, Guoei Gu, and Wenke Lee. Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems. In Proceedings of ICDM '06, Hon

Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee., "PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware.", (2006). Conference Proceedings, Published
Bibliography: Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In Proceedings of ACSAC

Prahlad Fogla and Wenke Lee., "Evading Network Anomaly Detection Systems: Formal Reasoning and Practical Techniques.", (2006). Conference Proceedings, Published
Bibliography: 5. Prahlad Fogla and Wenke Lee. Evading Network Anomaly Detection Systems: Formal Reasoning and Practical Techniques. In Proceedings of CCS 2006, Alexandria, VA, October

Web/Internet Site

Other Specific Products

Contributions

Contributions within Discipline:

We have made important contributions.

In anomaly detection, we developed a the VtPath dynamic analysis approach to generating models of program execution. This work has generated several follow-up work by other researchers. We also developed a static analysis approach to generating program execution models. Compared with previous approaches that use non-deterministic pushdown automaton models, our approach uses call stack information to generate the much more efficient deterministic pushdown automaton models. Our work shows that it may now be practical to run such anomaly detection models because they slow down

program executions by 1% to 135%. In our work on constructing 'environment-sensitive' anomaly detection models of programs, we showed that our analysis techniques improved argument recovery by 55% to 99% in our experiments. Using the average reachability measure, we demonstrated that the value of whole-program data-flow analysis and
environment-sensitive models. On four test programs, we improved the precision of context-sensitive models from 77% to 100%.

In alert correlation, we developed a statistical causality analysis algorithm. This is the first approach that does not rely on prior knowledge of attack step relationship.

In real-time IDS architecture, we developed the principles and techniques for performance adaptation, a first in IDS research. We designed and implemented the first IDS on a programmable network processor. In our work on characterizing the performance of real-
time intrusion detection systems. we found that: rule checking accounts for about 75% of the total processing time; 2) the distribution of rule checking times is remarkably bimodal; 3) header processing times have a small variance and small correlation coefficients; 4) in contrast, the distribution of payload processing times displays high variance, in a form that can be generally characterized as 'slightly heavy-tailed'. Explicitly, payload
processing times have a Lognormal upper tail, clipped at the top 1%. This extreme 1% upper tail is better fit by the Exponential distribution.

We were the first to study 'mimicry attacks' against network anomaly detection systems. It shows that we need to develop more sophisticated anomaly detection systems by incorporating more semantic information in the models. We also provided the first formal
treatment of the PBA, and more generally, mimicry attacks.

We were the first to show that for worm signature generation, the first order of business is to get a very 'cleaner' set of anomalous flows because otherwise the attackers can inject 'fake anomalous flows' such that the signature generator cannot produce effective
signatures.

In our work on botnet propagation modeling, we discovered botnet propagation exhibits a diurnal model because of the activity rhythms of the computer owners, e.g., turning off the computers at nights. We show that the diurnal behavior characteristics can be used to
determine the optimal botnet 'release' time and location (timezone). As a defender, we can determine which botnet is likely to propagate faster or more widespread.

In our work on a formal model for reasoning and comparing the precision of host-based anomaly detection models, we showed that for any system-call sequence model, under the same (static or dynamic) program analysis technique, there always exists a more precise
control-flow sequence based model. We also showed that the hybridization of these two techniques brings no advantage. This work represents a very important contribution to the intrusion detection research community because it provides a clear understanding, with
the rigor of formal analysis, of the precision (or detection power) of the various models proposed thus far.

We released a version of PolyUnpack, a tool for automatic unpacking malware, to the research community.

Contributions to Other Disciplines:

Contributions to Human Resource Development:

Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:

Conference Proceedings

Categories for which nothing is reported:

Organizational Partners
Any Web/Internet Site
Any Product
Contributions: To Any Other Disciplines

Contributions: To Any Human Resource Development
Contributions: To Any Resources for Research and Education
Contributions: To Any Beyond Science and Engineering
Any Conference

1. Anomaly detection:

In our work of using call stack information to generate system call based anomaly detection models, we showed that our models are pushdown automatons, thus making our models significantly more efficient than previous nondeterministic pushdown automaton models. Experiments showed that our models slow execution of programs by 1% to 135%. No anomaly detection model of program execution has been widely deployed yet because of false alarms and/or high performance overhead. Our static analysis approach generates models with no false alarms and relatively low overhead. Our research thus demonstrates the feasibility of producing usable (deployable) anomaly detection models.

In our work on constructing "environment-sensitive" anomaly detection models of programs, we showed that our analysis techniques improved argument recovery by 55% to 99% in our experiments. Using the average reachability measure, we demonstrated that the value of whole-program data-flow analysis and environment-sensitive models. On four test programs, we improved the precision of context-sensitive models from 77% to 100%.

In our work on evading payload-based network anomaly detection systems, we studied how an attacker can learn the normal profile used by the detection system, and generate polymorphic attack packets that purposely match the normal profile so that the attack can go undetected. We showed that while the problem of finding a transformation from attack payload to a "normal" payload can be NP-complete, with heuristics-based solutions, such "polymorphic blending attacks" are actually quite easy to implement against a host of simple payload (content) -based network anomaly detection systems. This is the first work in "mimicry attacks" against network anomaly detection systems. It shows that we need to develop more sophisticated anomaly detection systems by incorporating more semantic information in the models.

We also studied the general and theoretical problem: given an anomaly detection system and an attack, can one automatically generate its PBA instances. We also studied how the anomaly detection system can be automatically improved to detect the known PBA instances. We showed that in general, generating a PBA that optimally matches the normal traffic profile is a hard problem (NP-complete). However, the problem of finding a PBA can be reduced to the SAT or ILP problems so that solvers available in those domains can be used to find a near-optimal solution. Further, heuristics such as hill-climbing can also be used to find an approximate solution. Our work represents the first formal treatment of the PBA, and more generally, mimicry attacks. In our work on building a machine-learning based anomaly detector, we showed that by combining multiple one-class SVM classifiers, the resulting classifier (anomaly detector) is very accurate and hard to evade even when polymorphic blending attacks are used.

In our work on worm signature generation, we showed that it is quite easy for an attacker to inject noise, in particular, the "fake anomalous flows", to the traffic analyzed by a syntax-based worm signature generator so that it cannot learn and produce effective signatures. This work shows for worm signature generation, the first order of business is to get a very "cleaner" set of anomalous flows. There are several approaches to achieve this, including using both host-based and network-based detectors and correlate the

observations. This work also demonstrates that any machine learning based approach needs to be concerned about the threat of attackers "poisoning" training data.

In our work on PolyUnpack, we showed that by observing the execution of a binary and compared the instructions being executed with the set of instructions in the binary as determined via static analysis, we can detect the unpack-and-execute behavior of a binary and determine the unpacked (i.e., previously hidden) code segment. Our experiments showed that PolyUnpack outperforms other analysis tools and can successfully unpack the vast majority of the packed malware seen to date. We have released a version of PolyUnpack to the research community.

In our work on a formal model for reasoning and comparing the precision of host-based anomaly detection models, we showed that for any system-call sequence model, under the same (static or dynamic) program analysis technique, there always exists a more precise control-flow sequence based model. We also showed that the hybridization of these two techniques brings no advantage. We also implemented a detection system and showed that external control-flow monitoring allows performances similar to the ones of previous system call based approaches. This work represents a very important contribution to the intrusion detection research community because it provides a clear understanding, with the rigor of formal analysis, of the precision (or detection power) of the various models proposed thus far.

2. Efficiency:

In our work on characterizing the performance of real-time intrusion detection systems, we found that: rule checking accounts for about 75% of the total processing time; 2) the distribution of rule checking times is remarkably bimodal; 3) header processing times have a small variance and small correlation coefficients; 4) in contrast, the distribution of payload processing times displays high variance, in a form that can be generally characterized as "slightly heavy-tailed". Explicitly, payload processing times have a Lognormal upper tail, clipped at the top 1%. This extreme 1% upper tail is better fit by the Exponential distribution.

Our experience on building an IDS on network processors showed that general-purpose network processors such as the Intel IXP are capable of running all IDS functions. However, FPGA is more suitable for fast pattern-matching required by IDS. We showed that by connecting FPGA with a network processor, we can partition the IDS functions: pattern-maching to FPGA and the rest to the network processor, and achieve very high overall performance.

Project activities

1. Summary:

The project focuses on building adaptive intrusion detection systems (IDSs). There are two main research themes. The first is anomaly detection. An IDS with anomaly detection abilities can learn the profiles of normal operations, and detect new intrusions as anomalies. Therefore anomaly detection is the fundamental way an IDS can adapt to new attacks. In this CAREER project, I have studied the general principles and techniques for analyzing normal audit data and constructing anomaly detection models. I have also studied in-depth the important problem of modeling and monitoring program execution. In particular, I studied how to improve both detection rate and efficiency over previous approaches by systematically including more observable run-time information.

The second research theme is real-time performance adaption. A real-time intrusion detection system has several performance objectives: good detection coverage, economy in resource usage, resilience to stress, and resistance to attacks upon itself. These objectives are trade-offs that must be considered not only in IDS design and implementation, but also in deployment and in an adaptive manner. Otherwise, an attacker can create traffic conditions to overload an IDS and launch attacks that can evade detection. In this CAREER project, I have explored a modeling approach that considers the trade-offs of IDS performance objectives in terms of cost and value. Performance optimization is then the problem of computing an IDS configuration that provides the best value under cost constraints. Performance adaptation is the problem of recomputing the optimal configuration when run-time conditions change. I have also explored an IDS architecture that consists of network-node IDS (NNIDS) sensors each running on the network interface of a network node. This approach has the ability to scale with networking technologies because each NNIDS only needs to deal with traffic to a node(s) and can even throttle the traffic if the NNIDS cannot keep up.

This project resulted in many papers including four in IEEE Symposium of Security and Privacy (2001, 2003, 2004, and 2006), four in RAID (2002, 2004, 2005, and 2007), one in USENIX Security (2006) and one in ACM CCS (2006.

2. Anomaly detection:

We developed a method based on information-theoretic measures (entropy, conditional entropy, and relative entropy) to characterize the intrinsic “regularity” of normal audit data and to use such measures to determine how to build the “best” anomaly detection model given *only* the normal data. For example, for modeling process execution using its system call sequences, this approach can be used to determine what the best sequence length is for detection performance when only the normal sequences are available. This work was published in the 2001 IEEE Symposium of Security and Privacy

We developed a dynamic analysis approach to generate anomaly detection models of programs. Compared with previous work, this approach utilizes additional observable program data such as the call stack to make it much harder for attacks to evade detection. For example, our approach can detect several attacks, including an “impossible path”

attack, that evade previous approaches. Continuing this line of work of using call stack information, we then developed a static analysis approach to generate anomaly detection models that are much more efficient than previous work, and development of a theoretical framework to evaluate the sensitivity and efficiency of static analysis. From a theoretical point of view, our static analysis approach utilizes call stack information to achieve determinism in the pushdown automaton models, thus making our models significantly more efficient than previous nondeterministic pushdown automaton models. Experiments showed that our models slow execution of programs by 1% to 135%. This work was published in the 2003 and 2004 IEEE Symposiums of Security and Privacy.

We also developed an analysis technique that uses "environment-sensitive" information to construct more accurate models of system call arguments. This work will be published in the International Symposium on Recent Advances in Intrusion Detection (RAID), September 2005. We also introduced a new kind of attacks, "evasion by blending in with normal traffic", on network anomaly detection systems, and are developing a theoretical framework to evaluate the "hardness of evasion" of an anomaly detection system.

We studied how to efficiently store and match a large amount of patterns of normal activities. We developed very efficient tree models and algorithms. This work was published in IEEE TKDE 18(4).

We studied the problem of how to evade a payload-based network anomaly detection system. We defined a new attack called "polymorphic blending attack" (PBA) where attack packets are morphed to evade detection by a payload-based network anomaly detection system. Using several IDSs as examples, we showed that while in theory it is difficult to carry out the attack, in practice, it is quite easy. This work was published in USENIX Security 2006. We then studied the more general and theoretical problem: given an anomaly detection system and an attack, can one automatically generate its PBA instances. This work was published in the ACM CCS 2006. We also studied how the anomaly detection system can be automatically improved to detect the known PBA instances. We also proposed a machine-learning based approach to produce payload-based anomaly detection that makes PBAs very difficult to realize. This work was published in ICDM 2006 (IEEE International Conference on Data Mining).

We studied the problem of worm signature generation. We developed noise injection techniques to show that attackers can inject carefully crafted noise to traffic mislead worm signature generator. This work was published in the 2006 IEEE Symposium on Security and Privacy.

We studied the problem of automatically unpacking packed (obfuscated) malware, and developed an automatic unpacking system, PolyUnpack, and made it available to researchers. This work was published in ACSAC 2006.

We developed a formal model for reasoning and analyzing the precision of various host-based anomaly detection models, in particular, those based on system call and control-flow events. This work is to appear in RAID 2007.

3. Efficiency:

We studied cost-based modeling of intrusion detection performance. We defined the cost factors (compute cost, and cost of damage, false positive, and misclassified hit) and developed models for expressing the total value of an IDS. We developed the principles and techniques for IDS run-time performance optimization and adaptation, and implemented prototype adaptive IDSs. This work was published in RAID 2002.

We studied the performance characteristics of real-time intrusion detection systems, and developed theoretical models, which can then provide guides for building adaptive real-time intrusion detection systems. This work was published in the 43rd IEEE Conference on Decision and Control (CDC 2004), December 2004.

We designed and implemented a high-speed network-node IDS (NNIDS) using Intel IXP network processors. This NNIDS is intended for desktop computers and can keep up with several hundreds of Mbps traffic. This was the first IDS on a programmable network processor.