Curriculum Vitae

Kostas G. Anagnostakis
Cryptography and Security Department
Institute for Infocomm Research
kostas@i2r.a-star.edu.sg
http://s3g.i2r.a-star.edu.sg/~kostas

Interests

Secure systems: design, performance analysis, and economics.

Education

University of Pennsylvania, USA

Ph.D. in Computer and Information Science, April 2005
Thesis: "*Exchange Mechanisms and Cooperative Distributed System Design*"
Advisor: Michael B. Greenwald

M.S.E. in Computer and Information Science, August 2000
Advisor: Jonathan M. Smith

University of Crete, Greece

Degree in Computer Science, September 1998

Employment summary

Institute for Infocomm Research, A-STAR, Singapore September 2005 – current
Research Fellow and Principal Investigator, heading the Software Systems Security Group (S3G).

University of Pennsylvania, USA September 1998 – May 2005
Research Assistant in the Distributed Systems Laboratory.

Institute of Computer Science, FORTH, Greece January 2002 – September 2005
Associate Researcher (part-time), working on network security.

Leiden University, Netherlands June 2002 – December 2002
Visiting Researcher, working on network processors.

TERENA, Netherlands June 2000 – June 2001
Project Development Officer, supporting European task-forces and projects.

NLANR, University of California San Diego, USA October 1997 – May 1998
Research Staff, member of the SQUID team of the NLANR Web Caching project.

Institute of Computer Science, FORTH, Greece October 1994 – September 1997
Undergraduate research trainee with the networking group.

Local Operations Center, University of Crete, Greece September 1993 – October 1994
System and network administrator.

Teaching Experience

Teaching Assistant, University of Pennsylvania, "CSE240: Introduction to Computer Architecture", Fall 2002

Teaching Assistant, University of Pennsylvania, "CIS502: Analysis of Algorithms", Summer 2001

Grader, University of Pennsylvania, "CIS501: Advanced Computer Architecture", Fall 2000

Honors and Awards

- NYU Stern School Network Economics Institute (NET Institute), Summer Grant, 2006
- Best student paper award, Performance 2002 Conference, 2002
- USENIX/Stichting NLnet Research Exchange Grant, 2002
- Best Presentation Award, INFORMS Technical Section on Telecommunications, 2001
- Graduate Research Fellowship, CIS Department, University of Pennsylvania, 1998-2005
- Ericsson Award for Excellence in Telecommunications (for undergraduate thesis), 1998

Publications

Journal Publications

10. V. T. Lam, S. Antonatos, P. Akritidis, K. G. Anagnostakis, **“Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure”**, to appear in *ACM Transactions on Information and Systems Security (TISSEC)*, 2007

9. S. Antonatos, P. Akritidis, E. Markatos, K. G. Anagnostakis, **“Defending against Hitlist Worms using Network Address Space Randomization”**, to appear in *Computer Networks Journal*, 2007

8. K. G. Anagnostakis, S. Ioannidis, A. D. Keromytis, M. B. Greenwald, **“Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation”**, to appear in *International Journal of Information Security (IJIS)*, 2007

7. M. Polychronakis, K. G. Anagnostakis, E. P. Markatos, **“Network-Level Polymorphic Shellcode Detection Using Emulation”**, to appear in *Journal in Computer Virology*, vol. 2, no. 4, pp. 257-274, February 2007

6. S. Ioannidis, S. M. Bellovin, J. Ioannidis, A. D. Keromytis, K. G. Anagnostakis, and J. M. Smith, **“Virtual Private Services: Coordinated Policy Enforcement for Distributed Applications”**, in the *International Journal of Network Security (IJNS)*, January 2007

5. K. G. Anagnostakis, M. B. Greenwald, S. Ioannidis, D. Li, J. M. Smith, “**Flexible Network Monitoring with FLAME**”, *Computer Networks Journal (Special Issue on Active Networks)*, Vol. 50 (14), pp. 2548-2563, October 2006

4. K. Xinidis, I. Charitakis, S. Antonatos, K. G. Anagnostakis, E. P. Markatos, **“An Active Splitter Architecture for Intrusion Detection and Prevention”**, in *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 1, pp. 31-44, January-March 2006

3. H. Bos, B. Samwel, M. Cristea, K. G. Anagnostakis, **“Safe Execution of Untrusted Code on Embedded Network Processors”**, to appear in *International Journal on Embedded Systems*, (Ed Deprettere, et al.; Eds), 2006

2. K. G. Anagnostakis, M. B. Greenwald, **“Direct Measurement versus Indirect Inference for Determining Network-internal Delays”**, *Performance Evaluation*, Elsevier Science, vol.49/1-4, pp. 165-176, September 2002

1. P. B. Menage, D.S. Alexander, W. A. Arbaugh, A. D. Keromytis, K. G. Anagnostakis, J. M. Smith, “**The Price of Safety in an Active Network**”, *IEEE/KICS Journal of Communications and Networks*, vol.3, no.1, pp. 4-18, March 2001

Conference and Workshop Publications

41. S. Antonatos, E. Markatos, K. G. Anagnostakis, **“Honey-at-home: A New Approach to Large-Scale Attack Detection”**, to appear in *Proceedings of ACM WORM’07*, October 2007

40. P. Akritidis, W.Y. Chin, V.T. Lam, S. Sidiroglou, K.G. Anagnostakis, **"Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks"**, to appear in *Proceedings of the 16th Annual USENIX Security Symposium*, August 2007

39. M. Polychronakis, K. G. Anagnostakis, and E. P. Markatos, **"Emulation-based Detection of Non-self-contained Polymorphic Shellcode"**, to appear in *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID)*, September 2007

38. E. Athanasopoulos, M. Roussopoulos, K. G. Anagnostakis, E. P. Markatos, **"GAS: Overloading a File Sharing Network as an Anonymous System"**, to appear in *Proceedings of the International Workshop on Security (IWSEC 2007)*, October 2007

37. M. Zghaibeh, K. G. Anagnostakis, **"On the Impact of P2P Incentive Mechanisms on User Behavior"**, to appear in *Proceedings of the ACM Joint Workshop on The Economics of Networked Systems and Incentive-Based Computing (NETECON+IBC'07), in conjunction with the 2007 ACM Conference on Electronic Commerce (EC'07)*, June 2007

36. V. T. Lam, S. Antonatos, P. Akritidis, K. G. Anagnostakis, **"Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure"**, in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*, pp. 221-234, November 2006

35. S. Antonatos, K. G. Anagnostakis, **"TAO: Protecting against Hitlist Worms using Transparent Address Obfuscation"**, in *Proceedings of the 10th IFIP Open Conference on Communications and Multimedia Security (CMS 2006)*, pp. 12-21, October 2006

34. D. Koukis, S. Antonatos, K. G. Anagnostakis, **"On the Privacy Risks of Publishing Anonymized IP Network Traces"**, in *Proceedings of the 10th IFIP Open Conference on Communications and Multimedia Security (CMS 2006)*, pp. 22-32, October 2006

33. K. G. Anagnostakis, S. Ioannidis, A. D. Keromytis, M. B. Greenwald, **"Robust Reactions to Potential Day-Zero Worms through Cooperation and Validation"**, in *Proceedings of the 9th Information Security Conference (ISC'2006)*, pp. 427-442, September 2006

32. M. Polychronakis, K. G. Anagnostakis, E. P. Markatos, **"Network-Level Polymorphic Shellcode Detection Using Emulation"**, in *Proceedings of Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA) 2006 Conference*, Berlin, Germany, pp 54-73, July 2006

31. E. Athanasopoulos, K. G. Anagnostakis, E. P. Markatos, **"Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network that Never Forgets"**, in *P*roceedings of the 4th International Conference on Applied Cryptography and Network Security (ACNS'06), pp. 130-145, Singapore, June 2006

30. S. Antonatos, P. Akritidis, E. Markatos, K. G. Anagnostakis, **"Defending against Hitlist Worms using Network Address Space Randomization"**, in *Proceedings of the 3rd ACM Workshop on Rapid Malcode (WORM'05), in conjunction with the 12th ACM Conference on Computer and Communications Security (CCS)*, November 2005

29. K. G. Anagnostakis, A. D. Keromytis, **"Action Amplification: A New Approach To Scalable Administration"**, in *Proceedings of the IEEE-MICC International Conference on Networks (ICON 2005)*, Kuala Lumpur, Malaysia, November 2005

28. K. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos, A. Keromytis, **"Detecting Targeted Attacks Using Shadow Honeypots"**, in *Proceedings of the 14th Annual USENIX Security Symposium*, pp. 129-144, August 2005

27. P. Akritidis, M. Polychronakis, K. G. Anagnostakis, E. Markatos, **"STRIDE: Detecting Polymorphic**

Worms through Instruction Sequence Analysis", in *Proceedings of the 20th IFIP International Information Security Conference (SEC 2005)*, pp. 375-391, June 2005

26. S. Antonatos, M. Polychronakis, P. Akritidis, K. G. Anagnostakis, E. P. Markatos, **"Piranha: Memory-efficient String Matching for Intrusion Detection"**, in *Proceedings of the 20th IFIP International Information Security Conference (SEC 2005)*, pp. 392-408, June 2005

25. K. Xinidis, K. G. Anagnostakis, E. P. Markatos, **"Design and Implementation of a High-Performance Intrusion Prevention System"**, in *Proceedings of the 20th IFIP International Information Security Conference (SEC 2005)*, pp. 359-374, June 2005

24. P. Akritidis, K. Anagnostakis, E. P. Markatos, **"Efficient Content-based Worm Fingerprinting"**, in *Proceedings of the 40th IEEE International Conference on Communications (ICC 2005)*, May 2005

23. K. G. Anagnostakis, M. B. Greenwald, **"A Hybrid Direct-Indirect Estimator of Internal Network Queuing Delays"**, **short paper** in *Proceedings of ACM SIGMETRICS/Performance'04*, pp. 426-427, New York, USA, June 2004

22. K. G. Anagnostakis, M. B. Greenwald, **"Exchange-based Incentive Mechanisms for Peer-to-Peer File Sharing"**, in *Proceedings of the 24th IEEE International Conference on Distributed Computing Systems (ICDCS 2004)*, pp. 524-533, Tokyo, Japan, March 2004

21. M. Polychronakis, K. G. Anagnostakis, A. Oslebo, E. P. Markatos, **"Design of an Application Programming Interface for IP Network Monitoring"**, in *Proceedings of the 9th IEEE/IFIP Network Operations and Management Symposium (NOMS'04)*, pp. 483-496, Seoul, S. Korea, April 2004

20. S. Antonatos, K. G. Anagnostakis, E. P. Markatos, **"Generating Realistic Workloads for Intrusion Detection Systems"**, in *Proceedings of the 4th ACM SIGSOFT/SIGMETRICS International Workshop on Software and Performance (WOSP 2004)*, pp. 207-215, San Francisco, USA, January 2004

19. S. Antonatos, K. G. Anagnostakis, E. P. Markatos, M. Polychronakis, **"Performance Analysis of Content Matching Intrusion Detection Systems"**, in *Proceedings of the 4th IEEE/IPSJ Symposium on Applications and the Internet (SAINT 2004)*, Tokyo, Japan, January 2004

18. A. D. Keromytis, K. Anagnostakis, S. Ioannidis, M. Greenwald, J. M. Smith, **"Managing Access Control in Large Scale Heterogeneous Networks"**, in *Proceedings of the NATO C3 Symposium on Interoperable Networks for Secure Communications (INSC 2003)*, The Hague, Netherlands, November 2003

17. K. G. Anagnostakis, M. B. Greenwald, S. Ioannidis, A. D. Keromytis, D. Li, **"A Cooperative Immunization System for an Untrusting Internet"**, in *Proceedings of the 11th IEEE International Conference on Networks (ICON'03)*, pp. 403-408, Sydney, Australia, October 2003

16. I. Charitakis, K. G. Anagnostakis, E. P. Markatos, **"An Active Splitter Architecture for Intrusion Detection"**, **short paper** in *Proceedings of the 10th IEEE/ACM Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS 2003)*, pp. 238-241, Orlando, USA, October 2003

15. I. Charitakis, D. Pnevmatikatos, E. Markatos, K. G. Anagnostakis, **"Code Generation for Packet Header Intrusion Analysis on the IXP1200 Network Processor"**, in *Proceedings of the 7th International Workshop on Software and Compilers for Embedded Systems (SCOPES 2003)*, pp. 226-239, Vienna, Austria, September 2003

14. K. G. Anagnostakis, S. Antonatos, E. P. Markatos, M. Polychronakis, **"E^{2}xB: A Domain-Specific String Matching Algorithm for Intrusion Detection"**, in *Proceedings of the 18th IFIP International Information Security Conference (SEC 2003)*, pp. 217-228, Athens, Greece, May 2003

13. K. G. Anagnostakis, M. B. Greenwald, R. S. Ryger, **"cing: Measuring Network-Internal Delays using only Existing Infrastructure"**, in *Proceedings of the 22nd Annual Joint Conference of IEEE Computer and Communication Societies (INFOCOM 2003)*, San Francisco, USA, April 2003

12. K. G. Anagnostakis, M. Greenwald, S. Ioannidis, S. Miltchev, **"Open Packet Monitoring on FLAME: Safety, Performance and Applications"** , in *Proceedings of the 4th IFIP Int'l Working Conference on Active Networks (IWAN 2002)*, pp. 120-131, Zurich, Switzerland, December 2002

11. E. P. Markatos, S. Antonatos, M. Polychronakis, K. G. Anagnostakis, **"Exclusion-based Signature Matching for Intrusion Detection"**, in *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN 2002)*, pp. 146-152, Cambridge, USA, November 2002

10. K. G. Anagnostakis, M. B. Greenwald, R. S. Ryger, **"On the Sensitivity of Network Simulation to Topology"**, in *Proceedings of the 10th IEEE/ACM Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS 2002)*, pp. 117-126, Fort Worth, Texas, USA, October 2002

9. K. G. Anagnostakis, M. B. Greenwald, **"Direct Measurement versus Indirect Inference for Determining Network-internal Delays"**, in *Proceedings of IFIP Performance 2002*, published in Performance Evaluation, Elsevier Science, vol.49/1-4, pp. 165-176, Rome, Italy, September 2002 (***best student paper award***)

8. S. Ioannidis, K. G. Anagnostakis, J. Ioannidis, A. D. Keromytis, "**xPF: Packet Filtering for Low-Cost Network Monitoring**", in *Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR)*, pp. 121-126. Kobe, Japan, May 2002

7. K. G. Anagnostakis, S. Ioannidis, S. Miltchev, J. Ioannidis, M. Greenwald, J. M. Smith, "**Efficient Packet Monitoring for Network Management**" , in *Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS 2002)*, pp. 423-436. Florence, Italy, April 2002

6. K. G. Anagnostakis, S. Ioannidis, S. Miltchev, J. M. Smith, "**Practical Network Applications on a Lightweight Active Management Environment**", in *Proceedings of the 3rd IFIP International Working Conference on Active Networks (IWAN 2001)*, pp. 101 - 115. Philadelphia, USA, October 2001

5. A. V. Vasilakos, K. G. Anagnostakis, W. Pedrycz, **"Application of Computational Intelligence Techniques in Active Networks"**, in *Proceedings of the 16th ACM Symposium on Applied Computing (SAC'01)*, pp. 448-455, Las Vegas, USA, March 2001

4. K. G. Anagnostakis, M. W. Hicks, S. Ioannidis, A. D. Keromytis, J. M. Smith, "**Scalable Resource Control in Active Networks**" , in *Proceedings of the 2nd IFIP International Working Conference on Active Networks (IWAN 2000)*, pp. 343 - 357. Tokyo, Japan, October 2000

3. A. V. Vasilakos, K. G. Anagnostakis, C. Ricudis, W. Pedrycz, A. Pitsillides, "**Evolutionary-Fuzzy Prediction for Strategic QoS Routing in ATM/SDH Networks**" in *Proceedings of the 16th IEEE World Conference on Computational Intelligence (WCCI'98)*, Anchorage, USA, May 1998

2. K. G. Anagnostakis, S. Sartzetakis, "**Web-based, CORBA-controlled Advanced Telecommunication Services for Medical Tele-Education**" in *Proceedings of the 2nd European Workshop on Multimedia Technology in Medical Tele-training (W2MT)*, Aachen, Germany, September 1997

1. K. G. Anagnostakis, F. C. Harmantzis, "**Simple, Usage-Based Charging for Web Cache Services**", *2nd International Web Caching Workshop (IWCW'97)*, Boulder, USA, June 1997

Patents

4. "**Methods for Preventing Spoofing Attacks in WiFi Networks**" (with P. Akritidis), US Provisional Patent Application, July 2007

3. "**SIGVAL: Architecture and Algorithm for Signature Validation in Intrusion Detection and Prevention Systems**" (with S. Antonatos), US Provisional Patent Application, March 2007

2. "**Detecting Targeted Attacks using Shadow Honeypots**" (with S. Sidiroglou, A. D. Keromytis), US Patent Application, February 2007

1. "**ACTs: Protecting against Puppetnet DDoS attacks using Access Control Tokens**" (with S. Antonatos), US Provisional Patent Application, October 2006

Unrefereed papers and works in progress

11. W.Y.Chin, K.G. Anagnostakis, "**Estimating the Risk of Potential Wireless-Phishing and Worm Attacks in Singapore**", *working paper*, November 2006

10. M. Zghaibeh, K. G. Anagnostakis, **"On the Impact of P2P Incentive Mechanisms on User Behavior"**, working paper, SSRN Economics of Networks Working Papers Series, Vol. 3, No. 27, November 2006

9. K.G. Anagnostakis, E.P. Markatos, **"Real-time Monitoring and Detection of Cyberattacks"**, ENISA Quarterly Newsletter, Vol. 3, No. 1, Jan-Mar 2007

8. S. Antonatos, K. G. Anagnostakis, E.P. Markatos, **"A European Platform for Detection and Containment of Attacks on the Internet"**, The Economist (Greek Edition), April 2006

7. S. Sidiroglou, S. Nagpal, K. G. Anagnostakis, A. D. Keromytis, **"Cassandra: A Mechanism for Search Query Concealment"**, *submitted*, February 2007

6. K.G. Anagnostakis, E.P. Markatos, **"Towards a European Malware Containment Infrastructure"**, in ERCIM News No. 63, October 2005

5. K. G. Anagnostakis, M. B. Greenwald, **"cing+: Using Queuing-delay Distributions to Identify Network Chokepoints"**, *submitted*, July 2005

4. K. G. Anagnostakis, M. B. Greenwald, **"On the Feasibility of Network Delay Tomography without Infrastructure Support"** , UPENN TR MS-CIS-01-35, December 2001

3. K. G. Anagnostakis, **"Congestion Control in Packet-Switching Internetworks"**, Written Preliminary Examination II, University of Pennsylvania, April 2001

2. K. G. Anagnostakis, **"Design of an Environment for the Rapid Development of Experimental Telecom. Applications"**, Diploma Thesis, University of Crete, October 1997

Other Publicity

1. CommunicAsia press release, June 2006
2. Thorsten Holz's honeyblog feature of the week: Puppetnets, March 2007
3. digg.com weekly top-10 most popular, "A Batch of Interesting Papers", October 2006
4. F-Secure CTO blog: "A Batch of Interesting Papers", October 2006
5. wormblog feature: Cooperative Immunization for an Untrusting Internet, November 2006
6. "SINSHIELD Goes to War on Cyber Attacks", A-STAR@work Newsletter, August 2006
7. "Move Over, Malware", I2R K-Batsu Newsletter, March 2006
8. Wormblog feature: Network Address Space Randomization, February 2006

Major Projects

UN0WN – *Mobile Device Security* 2006-current

Our project aims to carry out a rigorous threat assessment study and develop advanced defenses against current and emerging security threats to mobile devices and wireless networks. The network technologies to be investigated are primarily GSM and, if the need arises, WiFi (in terms of communications technologies). The devices to be investigated are to be chosen among Pocket PC, smartphones, blackberries, and, if necessary, other mobile devices. The operating systems to be investigated are to be chosen among WM2003/WM2005 and Symbian (in terms of computing platforms).

SINSHIELD – *Defending against Evolving Malicious Software* 2006-current

In the ongoing software-security arms race, current defense capabilities have been shown to be weak against sophisticated zero-day and polymorphic attacks. At the same time, the increasing penetration of wireless networks and mobile devices alter the tradeoff space and call for new approaches to attack containment. Our work combines four complementary techniques: the use of instrumented honeypots for obtaining early samples of previously unknown worms; advanced filtering algorithms for containing not just current but also future variants of an attack; novel session hijack protection techniques to patch up a major wireless-specific attack vector; and migration of expensive security checks to a centralized emulated replica of subscribers' mobile devices, to protect mobile devices without affecting battery lifetime. In our early internal trials we have demonstrated instant reaction for 90% of all attacks, and 10-second reaction times for the remaining 10% of attacks.

COVERAGE – *Cooperative worm defense algorithms* 2002-2006

Worm detection and immunization systems that act completely independently are at a disadvantage against epidemic-like attacks. Cooperative defensive systems communicate and cooperate in their response to worm attacks, but determine the presence of a worm attack solely on local information. Distributed worm detection and immunization systems track suspicious behavior at multiple cooperating nodes to determine whether a worm attack is in progress. We have shown that cooperative, distributed worm immunization systems are practical, and evaluated the effectiveness of different system configurations in various simulations. Our results show that distributed algorithms are better able to balance effectiveness against viruses with reduced cost in computation and communication when faced with false alarms. Furthermore, cooperative, distributed systems seem more robust against malicious participants in the immunization system than earlier cooperative but non-distributed approaches.

EXCHANGE – *Robust incentives for cooperative distributed systems* 2003-2005

Enforcing cooperation in distributed systems is a difficult problem, as cash-, credit- and reputation-based proposals have seemed vulnerable to selfish-malicious users, and either too complex or not providing strong incentives for cooperation. As an alternative, we have investigated the use of exchange-based mechanisms, where peers give higher service priority to requests from peers that can provide a simultaneous and symmetric service in return. We have generalized this approach to n-way exchanges among rings of peers and developed efficient search mechanisms for locating such rings. Our analysis, simulation, and real-world measurements demonstrate that exchange-based mechanisms can provide strong incentives for cooperation without the security problems and complexity of previous proposals.

CING(+) – *Network-internal delay measurement* 2001-2005

We have developed a method and the first practical tool for measuring network-internal delays in the Internet. We have shown that the method is more accurate than previous indirect methods, and that it can be used without any additional infrastructure support. Using this tool, we conducted a large-scale measurement study on the Internet, showing that the fraction of paths that have multiple congestion points is not negligible, and thus the single-bottleneck barbell topology used in most congestion control studies is not representative of the Internet. We also designed a hybrid direct-indirect measurement technique that can measure delay distributions on almost any link on the Internet, and are currently exploring the use of our tools for detecting chokepoints and estimating per-link available capacity.

FLAME – *Extensible network monitoring for security and performance* 2000-2003

We have employed technology derived from active networking research to develop a series of network monitoring systems, but unlike most previous work, made application needs the priority over infrastructure properties. This choice has produced the following results: (1) the techniques for general infrastructure are both applicable and portable to specific applications such as network monitoring; (2) tradeoffs can benefit our applications while preserving considerable flexibility; and (3) careful engineering allows applications with open architectures to perform competitively with custom-built static implementations. These results are demonstrated via measurements of the Lightweight Active Measurement Environment (LAME), its successor, Flexible LAME (FLAME), and their application to monitoring for performance and security. We have also investigated enhancing FLAME technology with network processor support, and extensions to the Berkeley Packet Filter to allow more flexibility and higher performance.

High-performance IDS –*Algorithms and system architectures* 2002-2004

Increasing network speeds, the high cost of current-generation rule-based intrusion detection systems, along with the growing need for new anomaly-based heuristics for detecting previously unknown attacks, requires the development of efficient algorithms and system architectures for intrusion detection. In this research, we have designed efficient hash-based string matching algorithms and network-processor based system architectures for scaling up rule-based IDSes such as snort for high speed networks. The E^2xB algorithm we developed is currently the fastest known IDS string matching algorithm, while the network processor software architecture improves IDS throughput by 45%-95% compared to state-of-the-art designs.

BOP and SPYCElab – *Market mechanisms in active networks* 1998-2001

We investigated the use of market mechanisms and trading amongst nodes and programs with varying degrees of competition and cooperation to provide a scalable approach to managing active network resources. In the SPYCElab system, we used a trust-management architecture to ensure that the participants in the resource management marketplace have a policy-driven "rule of law" in which marketplace decisions can be made and relied upon. We have also investigated the use of application-specific congestion control policies in the "Bourse of Packets (BOP)" experiment, where active packets make decisions based on storage and forwarding prices on each node.

Invited Talks

1. **"Metro Wifi Threats: Wildfire Worms, Wireless Phishing and Citizen Tracknets"**, AIST, Japan, May 2007

2. **"Metro Wifi Threats: Wildfire Worms, Wireless Phishing and Citizen Tracknets"**, Computer Laboratory, University of Cambridge, March 2007

3. **"New Approaches to WiFi Security"**, Singapore GovernmentWare'06, November 2006

4. **"Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure"**, Bell Labs, Lucent Technologies, November 2006

5. **"Metro Wifi Threats: Wildfire Worms, Wireless Phishing and Citizen Tracknets"**, University of Pennsylvania, November 2006

6. **"Understanding the Threat of Mobile Worms in WiFi Environments"**, Euro-Southeast Asia ICT Forum 2006 (EUSEA 2006), June 2006

7. **"Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure"**, Computer Science Lab, SRI International, USA, April 2006

8. **"Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure"**, State Key Information Security Laboratory, Chinese Academy of Sciences, Beijing, March 2006
9. **"Where is Spyware Heading?"** (Panel Moderator), Asian Internet Security Summit, Singapore, November 2005
10. **"Attack-defense co-evolution: the case of Spyware"**, Asian Internet Security Summit, Singapore, November 2005
11. **"Worm Defenses: Network-level Detection and Beyond"**, Institute for Infocomm Research, Singapore, May 2005
12. **"Worm Detection: Network-internal Mechanisms and Infrastructure"**, NORDUnet 2005 Conference, April 2005
13. **"Some Thoughts on the Threat of Internet Worms"**, European Commission Internet Security Panel, January 2005
14. **"Network Monitoring for Security and Performance"**, Europe-China Bridge Symposium, December 2004
15. **"On the Sensitivity of Network Simulation to Topology"**, ONR SPYCE Project Annual Review Board, June 2002
16. **"A Bourse of Packets Approach to Internetwork Resource Control"**, INFORMS Meeting, November 2001
17. **"BOP: A Bourse of Packets Approach to Internetwork Resource Control"**, KPN Research - Twente, April 2001

Thesis Committee Service

1. External PhD committee member for Manaf Zghaibeh (Stevens Institute for Technology, School of Technology Management), September 2007

Student and Staff Supervision

1. Rahul Shetty, MSE student at Penn, working on `cing+`
2. Steve Zhao, MSE student at Penn, working on `cing+`
3. Frey Kuo, PhD student at Penn, working on `FLAME`
4. Dekai Li, PhD student at Penn, working on `FLAME`
5. Spyros Antonatos, MSc student at ICS-FORTH, working on IDS benchmarking and string matching
6. Kostas Xinidis, MSc student at ICS-FORTH, working on system architectures for high-performance IDS
7. Periklis Akritidis, PhD intern, Cambridge, working on worm defenses and shadow honeypots
8. Dimitris Koukis, BSc student at ICS-FORTH, working on privacy in network monitoring
9. Manaf Zgaibeh, PhD student at Stevens Tech, working on incentive mechanisms
10. Lam Vinh The, research engineer at I^2R, working on botnets
11. Chin Wee Yung, research engineer at I^2R, working on honeynets

12. Zhao Zhigang, research engineer at I^{2}R, working on high-performance IPS
13. Lee Pern Chern, research engineer at I^{2}R, working on high-performance IPS
14. S.P.T. Krishnan, research engineer at I^{2}R, working on rapid attack response
15. Khu Kirk Jon, research engineer at I^{2}R, working on botnets
16. Ron Chew, undergraduate intern at I^{2}R, working on wifi security
17. Xu-Quian Yap, undergraduate intern at I^{2}R, working on wifi security
18. Vishwas Patil, PhD intern at I^{2}R, working on wifi security
19. Asia Slowinska, PhD intern at I^{2}R, working on application characterization

Research Funding

- 2007-2008, UN0WN: Security for Mobile Devices, CSIT/Singapore Ministry of Defence, 200kSGD (approx. 100kEUR)
- 2006, cyb.air.sec: Metro WiFi Security, through A*STAR/I2R DED(I) fund, 45kSGD (approx. 22kEUR)
- 2006-2008, SINSHIELD: Defending against Evolving Malicious Software, A*STAR Core Project Funding, 691kSGD (approx. 350kEUR)
- 2006, Understanding The Impact of Incentives in P2P Systems: A Case Study of BitTorrent and eMule, NET Institute Summer Research Award (with F. Harmantzis, M. Zghaibeh, S. Ioannidis), 3kUSD
- 2005-2006, ARMVEST: A Study of Honeypot Technology, Industry Collaboration Grant, 15kEUR
- 2005-2008, NoAH: A European Network of Affined Honeypots, EU IST, 389kEUR (with E. Markatos)
- 2005-2006, SecSPeer: Secure and Scalable peer-to-peer computing and communication systems, GSRT, 45kEUR (with E. Markatos)
- 2004-2006, LOBSTER: Large Scale Monitoring of Broadband Internet Infrastructure, EU IST, 364kEUR (with E. Markatos)
- 2002-2003, IXPMON, USENIX/Stichting NLnet Research Exchange Grant, 20kUSD (with H. Bos)
- 2001-2004, SCAMPI: A Scalable Monitoring Platform for the Internet, EU IST, 397kEUR (with E. Markatos)

Professional Activities

- Grant Proposal Reviewer, US Air Force Office of Scientific Research (AFOSR), 2007
- PC Co-Chair: 3rd European Conference on Computer Network Defense (EC2ND'07)
- PC Member: 5th ACM CCS Workshop on Recurring Malcode (WORM'07)
- PC Member: 16th USENIX Security Symposium (Security'07)
- PC Member: ACM SIGCOMM Workshop on Large Scale Attack Detection (LSAD 2007)
- PC Member: 27th International Conference on Distributed Computing Systems (ICDCS'07)
- PC Member: ESORICS Workshop on Automated Self-Healing (WASH 2006)

- PC Member: ACM SIGCOMM Workshop on Large Scale Attack Detection (LSAD 2006)
- PC Member: WWW 2006 Conference, Security, Privacy and Ethics track
- PC Member: ICDCS'06 Workshop on Incentive-Based Computing
- PC Member: SECURECOMM 2006 Workshop on the Value of Security through Collaboration (SECO-VAL)
- Session Chair: ACM Workshop on Rapid Malcode (WORM'05)
- External reviewer: Usenix Security, ACM SOSP, CCS, IEEE S&P, ISOC NDSS, IEEE/ACM Transactions on Networking, Computer Networks Journal, IEEE Comm. Letters, IJSN, IEE Security, Usenix ATC Freenix Track, IEEE INFOCOM, NOMS, MASCOTS, ISC, LCN, NPC, WISA, ICC, ISCC, HICSS, ICMLC, IFIP IWAN, IASTED CCN.
- Independent expert: European Network and Information Security Agency (ENISA) working groups.

References

Available upon request