Computer Network Security:

Report from MMM–ACNS

Nicolas Sklavos
University of Patras, Greece

Nikolay Moldovyan
St. Petersburg Electrical Engineering University

Vladimir Gorodetsky
St. Petersburg Institute for Informatics and Automation

Odysseas Koufopavlou
University of Patras, Greece

The Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Networks (MMM–ACNS 2003; http://space.iias.spb.su/mmm-acns03/index.jsp) took place 21–23 September 2003 in St. Petersburg, Russia. The European Office of Aerospace Research and Development, the Russian Foundation of Fundamental Research and Office of Naval Research International Field Office, the Russian Foundation for Basic Research, and the Ministry, Technical Policy, and Science of the Russian Foundation sponsored the event.

The workshop had more than 100 registered attendees from academia and industry. There were six invited talks and 29 accepted papers. Here, we summarize the invited talks and the workshop sessions.

Invited talks

The invited speakers focused on important security topics such as computational complexity, calculus and higher-order logic, behavior-based security, network forensics, and inside intruder attacks. Workshop attendees agreed that all the talks addressed issues of great interest. The "Invited talks" sidebar on p. 50 lists the papers' topics.

Computational complexity

Anatol' O. Slissenko at the University Paris and the Russian Academy of Sciences spoke about security problems' computational complexity. Complexity analysis is helpful in determining any information system's efficiency, particularly computer network security components. The complexity approach relates to cryptology, steganography, watermarking, verification, recognition, virus detection, intrusion detection, and cryptographic protocols, and determines an information system's efficiency. Slissenko pointed out that researchers can use complexity to compare various security-related algorithms and to craft appropriate theories. He argued that proofs of the negative algorithmic results, such as algorithmic not decidability or high lower-bound complexity are not relevant to practical systems analysis and, thus, should not discourage further work on theory development. Using some properties of realistic systems could provide more adequate complexity results. His presentation focused on the access problem, with examples of cryptography, protocols, and network vulnerability. Slissenko concluded that complexity analysis is feasible and useful, and underlined that cryptography practice and theory underlie security's foundations.

Calculus and higher-order logic

Shiu-Kai Chin, from Syracuse University, talked about three aspects of establishing, maintaining, and assessing trust and trustworthiness in distributed systems: the common object request broker architecture (Corba) and common secure interoperability v2 (CSIv2) protocols for secured brokered services, a specialized calculus for reasoning about access-control decisions, delegations, identities, and authorizations, and theorem proofs that formally verify security claims. Chin described the CSIv2 protocol and the access-control calculus syntax and semantics defined in the Cambridge, higher-order logic environment theorem proofs. Descriptions of the CSIv2 protocol by the access-control calculus provide a formal and consistent interpretation of the protocol. He claimed that HOL could verify the calculus and protocol properties.

Behavior-based security

Salvatore J. Stolfo from Columbia University discussed behavior-based security, the general approach of anomaly detection for intrusion detection applications. Behavior-based security tools defend and protect systems not only by attempting to identify known attacks using signatures or rules, but also by detecting deviations from a system's nor-

Invited talks

Anatol' O. Slissenko, "Complexity Problems in the Analysis of Information Systems Security."
Shiu-Kai Chin, "Implementing a Calculus for Distributed Access Control in Higher Order Logic and HOL."
Salvatore J. Stolfo, "Behavior-Based Computer Security."
Nasir Memon, "ForNet: A Distributed Network Forensics Systems."
Shambhu Upadhyaya, "Real-Time Intrusion Detection with Emphasis on Insider Attacks."

Workshop sessions

Peter D. Zegzhda, Dmitry Zegzhda, and Maxim Kalinin, "Logical Resolving for Security Evaluation."
Antonio Lain and Viacheslav Borisov, "Key History Tree: Efficient Group Key Management with Off-line Members."
John Bigham, David Gamez, and Ning Lu, "Safeguarding SCADA Systems with Anomaly Detection."
Youngdai Ko, Deukjo Hong, Seokhie Hong, Sangjin Lee, and Jongin Lim, "Linear Cryptanalysis on Spectr–H64 with Higher Order Differential Property."
Shuozhong Wang, Xinpen Zhang, and Kaiwen Zhang, "Data Hiding in Digital Audio by Frequency Domain Dithering."

mal behavior. The anomaly-detection algorithms are applicable to many detection tasks, including anomalous Windows registry accesses, file-system anomalies, malicious email, and stealthy reconnaissance. The talk focused on email analysis and statistical methods of profiling user behaviors implemented in Columbia's Email Mining Toolkit. The EMT computes statistical models that detect the early onset of viral propagations, spam, and policy violations. Interestingly, the technique detects deviations from a typical user's behavior rather than applying text-content analysis. For example, viruses propagate by violating a user's typical communication with their social cliques. Stolfo presented results for experiments using thousands of emails from 15 users. The process showed detection rates from 99 to 100 percent with false positive rates of less than 1 percent.

Network forensics

Nasir Memon from Polytechnic University Brooklyn, said that owing to the security community's extensive research, networks currently have ample defensive mechanisms against cyber attacks. However, we lack track-and-trace mechanisms, which could help professionals follow the attackers to their source. Most defensive measures are fail–open by design. Thus, when they fail, the attackers can attack and leave the crime scene without any evidence. To track down the perpetrators, we need better digital forensic tools. Memon presented the design of a distributed network forensics system called ForNet, which is a collection of appliances called SynApps that create and store intelligent summaries of the network traffic they monitor. SynApps in a network domain connect to a forensics server, which answers queries about network events within its domain. The forensics servers connect via a peer-to-peer system to provide a network-wide forensics system.

Inside intruder attacks

Shambhu Upadhyaya from the University at Buffalo covered real-time intrusion detection (ID) problems, focusing on insider attacks and the difficulty of closing all loopholes. Currently, there are more than 100 consumer products and prototypes that could be classified as misuse detection or anomaly detection systems. These detection approaches rely on audit trails or large samples of data. Moreover, they are mostly offline in terms of strong attack deterrence. The presentation examined ID tools and techniques from a taxonomical viewpoint, studying their real-time properties, shortcomings, and applicability to real systems. Upadhyaya proposed a reasoning framework that performs decision-making on a more informed basis and develops as a stochastic process based on a user's profile and intent at a session's start. Each user's unique activity samples help identify and halt attempts by an intruder who might be masquerading as an authentic user or who might be a malicious insider trying to abuse internal resources. Upadhyaya's discussion identified the need for testing this new reasoning framework and highlighted ongoing efforts to build a prototype system.

Workshop sessions

Five technical sessions covered Mathematical Models and Architectures for Security, Public Key Distribution, Authentication, and Access Control, Intrusion Detection, Cryptography, and Steganography. Here, we highlight representative presentations from each workshop session. The "Workshop sessions" sidebar lists the session titles.

Models and architectures for security

Peter D. Zegzhda, Dmitry Zegzhda, and Maxim Kalinin from Polytechnical University, St. Petersburg, Russia discussed an approach for testing security policies' enforcement abilities and weaknesses in enterprise implementations. Zeghda claimed that it is possible to examine the vulnerabilities of thousands of security-related objects in a multiuser system and identify security risks. By acting on this information, a security officer or system administrator could significantly reduce a system's security exposure. This session also examined theoretical foundations for the design of a safety evaluation toolkit. The presenters also described the integrated evaluation workshop's functional structure based on a security-analyzing kernel.

Public key variations

Antonio Lain and Viacheslav Borisov of HP Labs, Bristol presented a new approach for offline members of a secure dynamic group, who share a secret key that continuously changes to match current membership. Instead of renegotiating keys when members go offline or forcing direct interaction with a key manager, the speakers proposed a safe caching mechanism particularly suited for logical key hierarchy schemes. The basis of the approach is that in many applications, members coming back online only need to know the current key and not all the intermediate keys negotiated while they were offline. The speakers also proposed a compact representation for that purpose—called a key history tree. A KHT's operation is transparent to clients and key managers, contains only publicly available information, and can be replicated safely over a network.

Intrusion detection

John Bigham, David Gamez, and Ning Lu of Queen Mary, University of London showed how to improve supervisory control and data acquisition (SCADA) systems' accuracy and security by using anomaly detection to identify suspect values caused by attacks and faults. Their presentation compared invariant induction and n-gram anomaly-detector performance and outlined plans for taking this work further by integrating the output from several anomaly-detecting techniques using Bayesian networks. They discussed n-gram, an approach of modeling SCADA data from an electrical network. This method treats the data as text and learns the normal patterns in this text. Although they illustrated their methods using data from an electrical network, this research springs from a more general attempt to improve SCADA systems security and dependability using anomaly detection.

Cryptography

Youngdai Ko, Deukjo Hong, Seokhie Hong, Sangjin Lee, and Jongin Lim from Korea University, studied Spectr–H64 linear equations using the property of controlled permutation boxes. They created a fourth-order differential structure using the property that the algebraic degree of function *G* is 3, which is the only non-linear part of Spectr–H64. These linear equations and structures enable us to attack the reduced sixth-round Spectr–H64. So, the authors showed how they managed to recover the sixth-round subkey with about 2^{44} chosen plaintexts and $2^{229.6}$ steps, which are lower than the 2^{256} exhaustive search.

Steganography

Shuozhong Wang, Xinpen Zhang, and Kaiwen Shuozhong Wang from Shanghai University, Shanghai, China proposed a technique that uses frequency-domain dithering to insert large amounts of data into short frames in a digital audio signal. Their proposed method allows storage of a large amount of data that is difficult to detect. Detection synchronization uses a two-step search process that accurately locates a pseudo noise sequence-based pilot signal attached to the data during embedding. This method treats the data as text and learns the normal patterns in this text. Except for a few system parameters, the receiver needs no information about the host signal or the embedded data. Experimental results show that the method is robust against attacks including active white Gaussian noise interference and MPEG-3 coding.

A panel discussion devoted to intrusion detection systems (IDS) problems closed the workshop. Discussion topics included maintenance (the cost of updates and staying current is growing), limited-coverage problems (IDS systems suffer from false negatives), data reduction (IDS are inherently noisy and chatty and suffer from false negatives), and insider attacks (the most serious threat is an insider, so host and LAN-based IDS now are more crucial than ever).

The discussion's primary outcome was identifying the latest trends and problems and how to address them. These included

- the need for research and development of behavior-based defensive approaches that would account for the temporal nature attacks and which would provide automated event analysis to reduce the time required to update and deploy defensive mechanisms, improve analyst–security staff productivity, and discover new attacks;
- a means to offload and load-balance detection tasks among separate specialized modules;
- providing correlation among distributed sites would provide new opportunities for real-time global detection (early warning) and attacker identification;
- using new knowledge-based models and frameworks, including (data mining, data and information fusion, neural networks, genetic algorithms, human-like immunology systems, multiagent technologies, failure-modeling technolo-

gies, self-adaptation techniques, malefactors' deception mechanisms, and so on) and applying a combination of signature-, anomaly-, and specification-based intrusion detection techniques.

We were pleased to attend a security workshop with such a wide variety of related topics and presentations with such technical depth. □

Nicolas Sklavos *is pursuing his PhD in the Electrical and Computer Engineering Dept, University of Patras, Greece. His research interests include VLSI and low-power design, cryptography implementations for wireless communications, and reconfigurable computing architectures. He holds an award for his PhD thesis on* VLSI Designs of Wireless Communications Security Systems, *from IFIP VLSI SOC 2003. He is a member of the IEEE. Contact him at VLSI Design Laboratory, Electrical and Computer Engineering Dept, University of Patras, Patras, Greece; nsklavos@ee.upatras.gr.*

Nikolay A. Moldovyan *is a chief researcher with the Specialized Center of Program Systems and professor with the St. Petersburg Electrical Engineering University, St. Petersburg, Russia. His research interests include computer security, cryptography, and developing the concept of variable transformations as a new direction in applied cryptography. He is an Honored Inventor of Russian Federation. He has a PhD in computer science from the Academy of Sciences of Moldova. He is a member of the International Association for Cryptologic Research. Contact him at SCPS SPECTR, Kantemirovskaya Str., 10, St. Petersburg, 197342, Russia; nmold@cobra.ru.*

Vladimir I. Gorodetsky *is a professor of computer science and head of the Intelligent Systems Laboratory of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science, St. Petersburg, Russia. His research interests include optimal control system theory, knowledge discovery from databases and data fusion, steganography, network security, intrusion detection, and multiagent systems. He has an MS in mechanical engineering from the Military Air Force Engineer Academy in St. Petersburg and an MS in mathematics from St. Petersburg State University. He is a member of IEEE, the International Society for Information Fusion, and the European and Russian Societies for Artificial Intelligence. Contact him at Intelligent Systems Laboratory of the St. Petersburg, Institute for Informatics and Automation, Russian Academy of Science; gor@iias.spb.su.*

Odysseas Koufopavlou *is an associate professor with the Department of Electrical and Computer Engineering, University of Patras, Greece. His research interests include VLSI, low-power design, VLSI cryptography systems, and high-performance communication subsystems' architecture and implementation. He has a PhD in Very Large Scale Integration (VLSI) Design for Digital Signal Processors, from the University of Patras, Greece. He is a member of the IEEE. Contact him at VLSI Design Laboratory, Electrical and Computer Engineering Dept, University of Patras, Patras, Greece; odysseas@ee.upatras.gr.*