Center for Education and Research
in Information Assurance and Security

Greetings from CERIAS at Purdue University!

Our first newsletter generated some very positive responses – thank you! So, here's issue #2, two months later. We'll keep this at two-month intervals for now, and try to feature a few highlights each issue. Of course, we continue to add new content to the CERIAS WWW site, so in between newsletters that is a good source of additional information.

If, at any time, you want to *unsubscribe* from this newsletter mailing list, send email to <newsl-request@cerias.purdue.edu> with a message body of only the word "unsubscribe". If you know other people who would like to *subscribe*, have them send an email to the same address with "subscribe" as the message.

Please mark your calendars for March 19 & 20, 2008. Those are the dates for our 9th annual security symposium. We'll have more details in the next newsletter, and we'll post registration details and schedule on the CERIAS WWW site sometime around then (early February). So stay tuned, and mark the dates!

If you missed the first issue of this newsletter, you can download it as <http://spaf.cerias.purdue.edu/trans/newsl1.pdf>

If you have any comments, send them to <info@cerias.purdue.edu>.

Until issue #3,

-- gene spafford
CERIAS Executive Director

Purdue University CERIAS 656 Oval Drive
Recitation Building West Lafayette, IN 47907-2086 **T** 765-494-7841 **F** 765-496-3181 info@cerias.purdue.edu http://www.cerias.purdue.edu

Where do they go?

In the last newsletter we mentioned that by the end of this academic year CERIAS will have graduated over 100 PhD students from our affiliated departments. One question that was asked by several people was where some of those people went – did they go primarily to industry or academia? Although we don't have complete data, about 55% seem to go on to academic positions: as regular faculty, research faculty, or post-doc researchers.

Based on our database, here's a list of all the institutions of higher education where our PhD graduates and (about a half-dozen) post-docs have gone after leaving Purdue.

> Air Force Institute of Technology; Cairo University (Egypt); California State University, Long Beach; Carnegie Mellon University; Case Western Reserve University; College of Aeronautical Engineering, PAF Academy, Risalpur Pakistan; Colorado State University; George Mason University; Helsinki University of Technology (Finland); Hong Kong University of Science & Technology; Illinois Wesleyan University; Indiana University-Purdue University Indianapolis; Iowa State University; James Madison University; Kansas State University; Marquette University; Miami University of Ohio; Oberlin College; Penn State University; Purdue University; Rutgers University; Simon Fraser University; Southwest Normal University (China); SUNY Oswego; SUNY Stony Brook; Syracuse University; University of Calgary; University of California, Berkeley; University of Cincinnati; University of Dayton; University of Denver; University of Kansas; University of Minnesota; University of Mississippi; University of New Mexico; University of North Carolina, Charlotte; University of Notre Dame; University of Ohio; University of Pittsburgh; University of Texas, Dallas; University of Texas, San Antonio; University of Zurich; Virginia Tech; Washburn University; and Western Michigan University.

We're quite proud of the continuing impact we've been able to have on the field by helping to educate all of these people!

Of Special Note

Speaking of making an impact, here are notes on a few of the people associated with CERIAS:

- Professor Victor Raskin was recently named as a Purdue University Distinguished Professor. This is the highest rank for faculty at Purdue, and represents a rare (and well-deserved) honor – only about 3% of faculty have this designation.
- Kurt Erik Ackermann, a senior majoring in Computer Science, was recently selected for Honorable Mention in the Computing Research Association's Outstanding Undergraduate Award competition for 2008. CRA's Outstanding Undergraduate Awards program recognizes undergraduate students in North American universities who show outstanding research potential in an area of computing research. Kurt has been working with Prof. Cristina Nita-Rotaru on wireless network security.
- Professor Mike Atallah (also a Distinguished Professor) was recently named as a Distinguished Alumnus of the American University, Beruit.

- Professor Arif Ghafoor was recently present with an Outstanding Achievement Award from the IEEE Bioinformatics and Bioengineering 2007 Conference and the IEEE Society on System, Man and Cybernetics.
- Keith Watson, CERIAS Research Engineer, recently was accredited as a Certified Information Systems Auditor (CISA) to accompany his CISSP certification.
- Gene Spafford was reappointed by the CERIAS Policy Board to another 3 year term as CERIAS Executive Director.

Upcoming Special Event

CERIAS, along with the College of Technology Computer & Information Technology Cyber Forensic Lab will be sponsoring a new conference. **Mobile Forensics World** is specifically dedicated to federal, state and local law enforcement forensic specialists, corporate and private forensic examiners, industry leaders, and academic researchers performing mobile device forensics. This includes forensics for cell phones, PDAs, SAT phones, GPS units, and more. The conference will be held May 8-10 in Chicago. For more details, see the conference WWW site <http://www.MobileForensicsWorld.com>.

Research Snapshots

One request as a result of the first newsletter was that we provide some information on current research at CERIAS. We have upwards of 50 active projects being conducted by faculty affiliated with the center at any one time. We try to keep information about these up-to-date on the WWW site, although that is highly dependent on the willingness of those faculty to provide us with the information.

For this newsletter, we asked faculty members for no more than 100 words on a current project. The following were the snapshots we received. If you'd like more information, contact the listed personnel, or send us a note at <info@cerias.purdue.edu>.

A Testbed for Research and Development of Secure IP Multimedia Communication Services

- Sonia Fahmy and Elisa Bertino, funded by NSF

Internet multimedia services such as Voice over IP (VoIP) and IP Television (IPTV) have increased the flexibility and reduced the cost of multimedia communication. These new services, however, have introduced new risks. Fraudulent use of network resources and Denial of Service (DoS) attacks against multimedia services can disrupt communication. We have constructed and configured a multi-university testbed that includes a variety of VoIP phones and video phones, and several traffic generation and monitoring tools. We are utilizing the testbed to study attacks against emergency 911 services, defenses against VoIP spam, and defenses against multimedia DoS attacks.

On-line Information Auctions

- Karthik Kannin

The goal of this research project is to develop an understanding of auctions employed in information systems settings. People are quite familiar with consumer auction settings such as eBay, where physical products are transacted; also, researchers have extensively investigated such contexts. However, there are many other markets where auctions have been used, yet little research has been pursued. My interest has particularly been on markets typically characterized by goods with zero marginal cost of production (or where the goods are not exclusive). An excellent example would be auctions in wslabi.com for vulnerability information. In such markets, the information good characteristics lead to interesting tradeoffs.

On the Accuracy of Decentralized Virtual Coordinate Systems in Adversarial Networks

- David Zage and Cristina Nita-Rotaru

(This work was presented at ACM CCS 2007.) Virtual coordinate systems provide an accurate and efficient service that allows hosts on the Internet to determine the latency to arbitrary hosts without actively monitoring all nodes in the network. Many of the proposed virtual coordinate systems were designed with the assumption that all of the nodes in the system are altruistic. However, this assumption may be violated by compromised nodes acting maliciously to degrade the accuracy of the coordinate system. As numerous peer-to-peer applications rely on virtual coordinate systems to achieve good performance, it is critical to address the security of such systems.

In this work, we demonstrate the vulnerability of decentralized virtual coordinate systems to insider (or Byzantine) attacks. We propose techniques to make the coordinate assignment robust to malicious attackers without increasing the communication cost. We demonstrate the attacks and mitigation techniques in the context of a well-known distributed virtual coordinate system using simulations based on three representative, real-life Internet topologies of hosts and corresponding round trip times (RTT).

Process Coloring: Information Flow-Preserving Approach to Malware Investigation and Warning

- Dongyan Xu, Eugene H. Spafford, Ryan Riley, and Xuxian Jiang (George Mason U.) funded by DTO

Process coloring is a malware detection technique based on tracking information flows through an operating system. Potential malware entry points, such as a web browser, are given a unique "color" that is propagated to data objects and other processes based information flowing through a colored item. For example, if an infection occurs through a web browser colored "red" then the installed malware and all files it writes will also be colored "red." This gives us a number of unique opportunities including quickly determining a malware break-in point as well as detecting system anomalies based on abnormal color interactions.

Influence of the Privacy Bird User Agent on User Trust of Different Web Sites

- Robert Protctor, funded by NSF

With increasing growth of Internet commerce, online fraud accounts for as much as 20% of identity theft cases. We conducted a study that evaluated Privacy Bird, a computer program that warns users of privacy preference violations by displaying a colored bird. The influence of Privacy Bird on users' trust of, and willingness to give financial information to, web sites in three categories (financial, retail, and social networking) was examined. Privacy Bird improved participants' privacy practices, increasing their trust in and willingness to provide financial information to web sites that yielded green birds, reducing it for sites that yielded red birds, and inducing further consideration of policies for sites that yielded yellow birds.

VOIP IDS

- Saurabh Bagchi, funded by Avaya

Voice over IP (VoIP) systems are gaining in popularity. These systems are likely to be subjected to different kinds of intrusions, some of which are specific to VOIP, and some of which are shared with general-purpose data networks. There have been enormous strides made in the field of intrusion detection systems (IDS) for general-purpose data networks. However, intrusion detection systems and intrusion prevention systems (IPS) for VoIP systems have lagged far behind. VoIP systems pose several new challenges to IDS and IPS designers such as the delay sensitive nature of the traffic. Therefore launching a denial of service is easier than in conventional networks.

We have been developing a system for intrusion detection and intrusion prevention customized to VoIP systems, named SpaceDive. The system comprises multiple components, which are distributed among the end clients and the servers. SpaceDive provides fast matching of network packets at a host against a rulebase specified in a novel language, coordination among multiple components to detect attacks that manifest themselves at multiple points of the network, and mechanism for aborting an attack based on initial symptoms. At the next level of sophistication, SpaceDive is customized to learn to detect previously unknown attacks. It uses machine learning clustering to detect spam VoIP calls and build profiles of legitimate behavior.

Controlled Declassification with Transactional Memory

- Jan Vitek, funded by NSF

We intend to apply recent techniques in transactional computing to the problem of preventing unwanted declassification of secure information. Regulating the nature and amount of information that is declassified for complex software system is difficult; even when leaks are identified, suitably repairing the computation is usually not possible. This proposal will develop programming language techniques to support information flow security by using ideas inspired from language-centric transactional computing to encapsulate critical regions that (a) either cannot be analyzed effectively statically or (b) declassify some set of confidential data. Isolation and atomicity proper ties of transactional regions ensure the approach is safe even in a multi-

threaded environment. Controlled declassification is a significant problem in the area of information security. This proposal will examine open technical issues associated with declassification from an entirely new perspective – rather than attempting to prevent statically any leaks from occurring (an approach that has notable inherent limitations), we will devise and validate approaches that dynamically monitor when leaks occur, and transparently revert program state to an earlier safe context when leaks are identified.

Miscellaneous

We continue to podcast our seminar series, update our WWW site and papers archive, and post items to the CERIAS blog. All are available via our WWW site at no charge.

CERIAS runs a set of NTP servers at Tier I and Tier II that are available for general use. See <http://ntp.cerias.purdue.edu> for details.

With Gratitude

Our continuing thanks to our sponsors – a set of organizations with visionary interest in a safer cyber environment for everyone, and that have generously helped to sponsor CERIAS efforts.

Current sponsors of CERIAS are:

[Tier I]

- Sun Microsystems (founding sponsor)
- Hewlett Packard
- IBM
- Lockheed Martin
- Microsoft
- MITRE
- National Reconnaissance Office
- Northrop Grumman

[Tier II]

- Booz Allen Hamilton
- Motorola
- Symantec
-

Companies and agencies interested in the CERIAS sponsorship program should contact Joel Rasmus (jrasmus@cerias.purdue.edu).

Finally

From everyone at CERIAS, our wishes for a happy and safe holiday season to you all!