

Konstantinos Xinidis

Education

- October 2004 **M.Sc.** in Computer Science, University of Crete, Greece (GPA 8.9/10.0)
Thesis: Network Intrusion Prevention on Multilevel Processing Architectures
Advisor: Evangelos P. Markatos, Associate Professor
Co-Advisor: Kostas G. Anagnostakis, Researcher
- June 2002 **B.Sc.** in Computer Science, University of Crete, Greece (GPA 7.9/10.0)
Thesis: Discovery of the Topology of Gnutella Network and Study of its Performance
Advisor: Evangelos P. Markatos, Associate Professor

Employment History

- February 2007 - present Security Engineer, Virtual Trip Ltd, Greece.
Research and Technological Development Department (RTD).
- October 2006 - April 2007 Network Systems Engineer, Systems and Security Department (SSD), Institute for Infocomm
Research (I2R), Singapore.
Software Systems Security Group (S3G).
- November 2005 - July 2006 National Military Service.
Sergeant, Arm of Infantry, Hellenic Armed Forces.
- November 2004 - October 2005 Network Systems Engineer, Institute of Computer Science (ICS), Foundation for Research and
Technology - Hellas (FORTH), Greece.
Computer Architecture and VLSI Systems Lab (CARV).
- October 2002 - October 2004 Graduate Research Assistant, ICS-FORTH, Greece.
Advanced Computing Systems group, Computer Architecture and VLSI Systems Lab (CARV).
- June 2001 - September 2002 Undergraduate Trainee, ICS-FORTH, Greece.
Advanced Computing Systems group, Computer Architecture and VLSI Systems Lab (CARV).

Honors and Awards

- Graduate Research Fellowship, ICS-FORTH, Greece, 2002-2004
- Ericsson Award for Excellence in Telecommunications (for my undergraduate thesis), Zappeion, Athens, May 2003
- Undergraduate Research Fellowship, ICS-FORTH, Greece, 2001-2002

Certificates

- Information Security Management Systems Auditing (According to EN ISO 27001:2005). Cert-No. 08.108.097.03/03, TUV AUSTRIA Academy.

Publications and Reports

1. K. Xinidis. **Wireless (In-)Security: Emerging Threats in Metropolitan Wireless Networks (Part II)**. In *Communication Solutions*, Vo. 51, September-October 2007
2. K. Xinidis. **Wireless (In-)Security: Emerging Threats in Metropolitan Wireless Networks (Part I)**. In *Communication Solutions*, Vo. 50, Pg. 4-13, July-August 2007
3. M. Marazakis, K. Xinidis, V. Papaefstathiou, and A. Bilas. **Efficient Remote Block-level I/O over an RDMA-capable NIC**. In *The 20th ACM International Conference on Supercomputing*, July 2006
4. K. Xinidis, I. Charitakis, S. Antonatos, K. G. Anagnostakis, and E. P. Markatos. **An Active Splitter Architecture for Intrusion Detection and Prevention**. In *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 1, January-March 2006
5. K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. P. Markatos and A. D. Keromytis. **Detecting Targeted Attacks Using Shadow Honeypots**. In *Proceedings of the 14th USENIX Security Symposium*, August 2005
6. K. Xinidis, K. G. Anagnostakis and E. P. Markatos. **Design and Implementation of a High-Performance Network Intrusion Prevention System**. In *Proceedings of the 20th International Information Security Conference (SEC 2005)*, June 2005
7. K. Xinidis and E. P. Markatos. **Network Intrusion Prevention on Multilevel Processing Architectures**. Masters of Science (M.Sc.) Thesis, Dept. of Computer Science, University of Crete, October 2004
8. K. Xinidis and E. P. Markatos. **Discovery of the Topology of Gnutella Network and Study of its Performance**. Diploma Thesis, Dept. of Computer Science, University of Crete, July 2002

Other Activities

1. K. Xinidis. **Emerging Ways to Protect your Network - From Vulnerability Scanning to Real-Time Detection of Cyber-Attacks.** In *3rd Regional Electronic Security Forum: Telecommunications Networks and Systems Security, Thessaloniki, 11-12 October 2007*
2. K. Xinidis. **A Solution that Integrates the Most Popular Internet Services and a Private Branch Exchange - SOLO.** In *i-techpartner Academy, Macedonia Palace, Thessaloniki, 8 June 2007*
3. M. Marazakis, K. Xinidis, V. Papaefstathiou, and A. Bilas. **Efficient Remote Block-level I/O over an RDMA-capable NIC.** In *2006 Workshop on On- and Off-Chip Interconnection Networks for Multicore Systems, December 2006*

Projects

Feb 2007 - present

i) Network Security Tools. Implementing a tool that parses the data that are collected by a honeypot and populates a MySQL database. Also, a web application (based on Ruby on Rails web framework) that eases the installation and management of a network of honeypots was implemented. **ii) Secure Mobile Applications using Web Services.** Implementing mobile phone applications using J2ME Connected Device Configuration (CDC) and Connected Limited Device Configuration (CLDC) profiles, the Apache Axis2 web service engine and the Rampart (WS-Security) module. **iii) VOIP Configuration Tool.** Implementing a tool based on Python for automatic configuration of Asterisk VoIP server.

Aug 2006 - Jan 2007

Wireless Intrusion Prevention System. Designing and implementing a wireless intrusion prevention system. With the explosive adoption of wireless networking, wireless security became an issue of paramount importance. With the physical medium (air) providing no restriction to unauthorized users and encryption protocols failing to achieve their claimed security requirements, wireless security is a challenging research area. In this work, we examine in detail possible wireless security threats and countermeasures while focusing on phishing attacks and internet worms. We have implemented a prototype using low-cost, off-the-self technology: a PC and commodity wireless access points. The PC acts as a controller that inspects all the traffic that is received from the access points. Our prototype is capable of preventing DNS spoofing attacks and effectively blocking novel worms that exploit unknown vulnerabilities.

2004 - 2005

Scalable Storage Systems. Designing and implementing a low-level, scalable communication infrastructure for networked storage systems. Modern storage systems are required to scale to large storage capacities and I/O throughput in a cost effective manner. For this reason, they are increasingly being built out of commodity components, mainly PCs equipped with large numbers of disks and interconnected of high-performance system area networks. A main issue in these efforts is to achieve high I/O throughput over commodity, low-cost system area networks and commodity operating systems. In this work, we examine in detail the performance of remote block-level storage I/O over commodity, RDMA-capable network interfaces and networks. We examine the support that is required from the network interface for achieving high throughput. We also examine in detail the overheads associated in kernel-level protocols for networked storage access. We find that base system performance is limited by (a) interrupt cost, (b) request size, and (c) protocol message size. We examine the impact of techniques to alleviate (a) and (b) and find that our techniques each can improve throughput by up to 50% over the unoptimized version. Our current prototype is able to achieve a throughput of about 200 MBytes/s over a network that is capable of delivering about 500 MBytes/s and is mostly limited by small messages in the remote storage access protocol.

Projects (cont)

- 2003 - 2004 **Network Intrusion Detection.** Designing and implementing a high-performance network intrusion prevention system (for my master's thesis). Network intrusion prevention systems provide proactive defense against security threats by detecting and blocking attack-related traffic. This task can be highly complex, and therefore, software-based network intrusion prevention systems are not capable of handling high speed links. Our system, called Digenis, combines the use of software-based network intrusion prevention sensors and a network processor board. The network processor acts as a customized load balancing splitter that cooperates with a set of modified content-based network intrusion detection sensors in processing network traffic. We show that the components of such a system, if co-designed, can achieve high performance, while minimizing redundant processing and communication. We have implemented the system using low-cost, off-the-shelf technology: an IXP1200 network processor evaluation board and commodity PCs. Our evaluation shows that our enhancements can reduce sensor load considerably, resulting in a system that can handle a fully-loaded Gigabit Ethernet link using a small number of sensors.
- 2002 - 2003 **Monitoring Application Programming Interface.** Designing and implementing an expressive API for monitoring high-speed networks. We designed a novel general-purpose network traffic Monitoring Application Programming Interface (MAPI) for network monitoring applications. This work built on a generalized network flow model that is flexible enough to capture emerging application needs, and expressive enough to allow the system to exploit specialized monitoring hardware, where available. We implemented MAPI as a Linux Kernel module and a support user space library on top of a commodity Gigabit Ethernet adapter. Our results suggested that MAPI had more expressive power than competing approaches, while at the same time was able to achieve significant performance improvements.
- 2001 **Peer-to-Peer Systems.** Studing unstructured peer-to-peer networks (for my undergraduate project). Unstructured peer-to-peer networks such as Gnutella are attractive for certain applications because they require no precise control over network topology or data placement. However, the query algorithm used in Gnutella does not scale. Each query generates a large amount of traffic and large systems quickly become overwhelmed by the query-induced load. In this project we studied, through simulation, whether it is possible to achieve less traffic by keeping the classical routing algorithm of Gnutella and changing the network topology. Additionally, a portion of this project explored, through simulation, several alternatives to the query algorithm of Gnutella. We proposed a routing algorithm, which does not send messages to all the neighbors of a node but to some of them according to the number of hops that the messages have traveled.

Course Lab Projects

- 2000-2002 (1) Designed and implemented a RISC processor using verilog. (2) Implemented text detection using trained convolutional filters. The system consisted of a convolutional neural network designed to recognize strongly variable text patterns directly from pixel images with no preprocessing. (3) Implemented a morphological technique for text extraction from images. (4) Designed and implemented a compiler for a language similar to C. (5) Designed and implemented a highly-available, replicated data matrix.

Advanced Coursework

- 2002 Distributed Operating Systems, Parallel Systems and Grids
2001 Computer Architecture, Neural Networks, Digital Image Processing

Programming Skills

- | | |
|------------------------------|--|
| Programming Languages | C, Java, Python, Ruby, shell programming, assembly language of IXP1200/IXP2400 network processor, IXP1200/IXP2400 microC, Verilog, Xilinx Microblaze assembly language. |
| Linux Kernel Programming | Implementation of network and block device drivers, hacking of the network and block subsystems of the Linux Kernel. |
| Embedded Systems Programming | Porting of the Linux kernel on a Xilinx Virtex-II Pro evaluation board (contains a PowerPC 405 processor), IXP1200 Ethernet Evaluation board custom operating system implementation. |
| FPGA Programming | Xilinx EDK and ISE tools. |
| Web Applications Development | Ruby on Rails, Apache Axis2, Joomla, XHTML, CSS |

Security Tools Knowledge

Vulnerability Assessment	Nessus, nmap
Penetration Testing	Metasploit
Firewalls and Intrusion Detection	Snort, Bro, iptables/netfilter
Network Monitoring	tcpdump, ethereal/wireshark

Participation in EU Projects

Apr 2005 - Mar 2008	NOAH European Network of Affined Honeypots.
Feb 2006 - Jul 2008	PLASTIC Providing Lightweight and Adaptable Service Technology for Pervasive Information and Communication.
Jan 2004 - Dec 2005	SIVSS Scalable Intelligent Video Server System.
Apr 2002 - Sep 2004	SCAMPI A Scaleable Monitoring Platform for the Internet.

References

References available upon request

Personal

Name:	Konstantinos Xinidis
Date of Birth:	December 16, 1980
Place of Birth:	Komotini, Rodopi, Greece
Nationality:	Greek (EU citizen)
Foreign Languages:	English - Cambridge First Certificate
Marital Status:	Single
Military Obligations:	Fulfilled

Contact

Private Address (Greece):	Sokratous 6, 57001 Thermi, Thessaloniki, Greece
Tel:	(+30) 6976172167 (Mobile) (+30) 2310498294 (Work)
E-mail:	kxinidis@gmail.com
Web:	http://kxinidis.dyndns.org