CS&IIR Workshop 2006 Overview and Agenda

*The **actual schedule is slightly modified from the times indicated below** as follows. Wednesday's Keynote has been moved to the first talk after lunch. All presenters up to that time are moved ahead to accommodate this change.*

Wednesday, May 10, 2006 **Building 5200, Visitor Center**

07:30am – 08:00am Registration and Badging

Building 5100, Auditorium (Room 128)

08:00am – 08:30am Refreshment Delta Crown Room, Room 140

08:00am – 08:10am Welcome & Overview Joseph P. Trien/Brian Worley

08:15am – 09:00am Thomas Longstaff Keynote Address

Thomas Longstaff is the Deputy Director for Technology in the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI). Longstaff has spent the past 12 years managing and initiating many of the CERT/CCs projects and initiatives such as the CERT Analysis Center, CERT Research Center, many survivability projects, and most recently Network Situational Awareness. His current scope of work includes evaluating technology across the entire NSS program to assure continued quality and innovation of all the work at CERT. Longstaff is responsible for strategic planning for the NSS program, technology scouting for promising avenues to address security problems, and operating as a point of contact between research projects at Carnegie Mellon University and the NSS program. Prior to coming to the Software Engineering Institute, Longstaff was the technical director at the Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory in Livermore, California. Longstaff obtained his M.S. in 1986 and Ph.D. from the University of California, Davis in 1992 in software environments, and his B.A. from Boston University in 1983 in Physics and Mathematics. Longstaff's publications span topics such as security policy, information survivability, insider threat, intruder modeling, and intrusion detection. His awards include Best Paper in 1995 at the NCSC Conference and the Carnegie Mellon University Andy Award for Outstanding Innovation in 2000.

09:05am – 09:35am Lee Hively, ORNL New Paradigm for Cyber Security

Next-generation information infrastructure must robustly provide pervasive, end-to-end connectivity among computers, mobile devices, wireless sensors, instruments, etc. Cyber-security is an essential component of information and telecommunications, which impacts all of the other critical US infrastructures (agriculture, food, water, public health, emergency services, government, defense industrial base, energy, transportation, banking and finance, chemicals and hazardous materials, postal and shipping) [NSHS 2002, NSPPCI 2003]. However, traditional cyber-security methods involve a never-ending cycle of detection and response to new vulnerabilities and threats. We submit that this patches-on-patches approach attests to the failure of the present cyber-security paradigm, and points to the need for a new and bold approach, which is the focus of this white paper. This proposal addresses an infrastructure project to design and develop cyber-security for the next-generation Internet with pervasive, trust-based computing as an integral part of the network technology. Indeed, any new cyber-security approach must address several essential features. Computers and information devices must be secured from malicious attacks. Malicious users must be held accountable for their actions. Trust-based interactions must enable sufficiently secure interactions among our society's other critical infrastructures, which are vital to our economic well-being, growth, and quality of life. The paradigm must enable continuing innovations in the information infrastructure (e.g., global computing, storage, massive databases, and data mining) and knowledge-age technology (e.g., new services, business, and education). The proposed work satisfies these needs.

09:40am – 10:10am Axel Krings, U of Idaho Fault-Models in Wireless Communication: Towards Survivable Ad-Hoc Networks

Ad hoc networks are among the most recent wireless applications. They operate in environments where the restrictions on nodes with respect to their computation and communication capabilities vary greatly. The characteristic property of these networks is the dynamic nature of computation and communication, may it be as the result of limited battery power of the nodes or due to their physical movement, to name a few. The reliability of ad hoc networks has been addressed primarily in the context of quality of service (QoS) and the main considerations have been routing and the overhead resulting from dealing with disruptions of the communication paths. However, due to the nature of wireless communication, the network model also raises many security related concerns. Nevertheless, the same features, i.e. wireless broadcast, which create security problems, can also be part of the solution in addressing diverse faults. This presentation introduces a new approach to modeling ad hoc network reliability under diverse fault assumptions. It allows for quantifying reliability and offers potential for modeling

survivability. The general model is presented and an example of its use is given. Specifically, we consider benign and omission faults and utilizes primary-backup and backup-backup link scheduling as fault tolerant mechanisms.

10:15am – 10:40am	James Caverlee, Ga Tech Mudhakar Srivatsa, Ga Tech Ling Liu, Ga Tech	Countering Web Spam Using Link-Based Analysis

Web spam refers to e□orts by malicious adversaries to manipulate how users view and interact with the World Wide Web, often to drive tra□c to particular spammed Web pages, regardless of the merits of those pages. As the Web has grown and increasingly become the primary platform for information sharing and electronic commerce, there has been a rise in targeted Web spam that is designed to degrade the quality of legitimate Web sites (and the services they o□er) and to manipulate the user experience for the advantage of the Web spammer. Our targeted countermeasures are designed to significantly raise the costs of link-based manipulation, so that Web spammers wield only a limited ability to impact link-based algorithms and to continue the arms race cycle. One such countermeasure we have developed relies on a notion of *hijack-resistant influence flow* to selectively throttle the influence of Web spammers. The countermeasure limits the impact of hijacked pages from sources outside of the complete control of the Web spammer, so that it is more di□cult for spammers to capture endorsements from reputable pages.

10:45am – 11:15am	Lori Delooze, USNA	Applying Soft Computing Techniques to Intrusion Detection

As more computers are integrated into the Internet, the threat of computer crimes increases and it becomes much more difficult and challenging to predict and prevent computer attacks and malicious intrusions. We apply soft computing techniques of artificial neural networks, evolutionary computing and fuzzy logic to produce an effective Intrusion Detection System to classify attacks by type and characterize the connection according to its behavior…..

Building 5200, Cafeteria

11:20pm – 12:20pm		Break for Lunch

Building 5100, Auditorium (Room 128)

12:30pm – 13:00pm	Jugal Kalita, U of Colo William Wilson, U of Colo	Combining Incremental Clustering and Signature Creation for Intrusion Detection

Anomaly based intrusion detection systems are able to discover many new attacks, but not all hosts and networks have the resources required for anomaly based detection. The false positive rate in anomalous sensors is also a source of concern. To overcome the limitation and requirements of anomaly sensors, the data captured by those sensors must be normalized and validated. We have developed a proof of concept implementation, based on a detailed design for a system where incremental clustering is combined with signature creation for intrusion detection……

13:05pm – 13:35pm	Itamar Elhanany, UTK Ortal Arazi, UTK Benjamin Arazi, UTK Derek Rose, UTK Hairong Qi, UTK	Self Certified Public Key Cryptography

The resource-constrained characteristics of sensor nodes, the ad-hoc nature of their deployment, and the vulnerability of wireless communications in general pose a need for unique solutions. A fundamental requisite for achieving security is the ability to encrypt and decrypt confidential data among arbitrary sensor nodes, necessitating the generation of joint private keys. Elliptic Curve Cryptography (ECC) has emerged as a suitable public key cryptographic foundation in constrained environments, providing high security for relatively small key sizes…….

13:40pm – 14:10pm	Richard Brooks, Clemson	Percolation Theory and Random Key Pre-distribution to Counter Cloning, Sybil, and Byzantine Attacks in Networks of Embedded Systems

This work considers security issues in networks of embedded systems. The applications that we consider are large systems consisting of hundreds, if not thousands, of nodes. We are particularly interested in problems associated with networks placed in unprotected environments. Individual network nodes that are discovered by adversaries can easily be tampered with and subverted. Since security approaches are traditionally based on the existence of a trusted computing base and secrets kept from the adversary, most existing techniques are not applicable to this problem domain.

14:10pm – 14:30pm	BREAK	Delta Crown Room, Room 140

14:35pm – 15:05pm | Phillip Bradford, U of Ala
Xiaoyan Hong, U of Ala | Proactive Computer-system Forensics

Proactive computer-system forensics is the design, construction and configuring of systems to make them most amenable to future digital forensics analyses. The objective of this research is to strengthen system security through better understanding of insider's illicit behavior. This research involves designing and developing three complimentary digital forensics systems. These systems are being built concurrently as practical and theoretical foundations are developed and refined. A hypothesis of this work is insider security risks are inevitable. Thus, we should be prepared to use computer resources to monitor these risks and focus resources on more risky insiders.

15:10pm – 15:40pm | Aditya Mathur, Purdue
KR Jayaram, Purdue
Arif Ghafoor, Purdue
Ammar Masood, Purdue | Model Based Testing of Implementations of Authentication and Access Control

Our focus is on testing implementations of authentication and access control mechanisms in embedded components and in integrated distributed systems that are collections of embedded components. Such mechanisms are the basis of secure operation of online business applications that form the foundation of tomorrow's cyber-centric economy as well as the nation's security. Our research focuses on the following two distinct research and development tasks: (i) Automation and evaluation of test generation techniques using dynamic formal models; (ii) Development and evaluation of (a) models for access control in the presence of timing constraints and (b) automated test generation techniques…..

15:45pm – 16:15pm | Andrew Walenstein, LSU
Arun Lakhotia, LSU | Direction for Research on Hardening Software Analysis Against Adversarial Code

Malicious code is commonly adversarial towards analysis, i.e., seeks to defeat mechanisms that could detect, identify, or thwart its malicious intents. This is just another way of saying that malware attacks the science and engineering foundation supports current practice. This presentation will discuss directions for hardening software analysis techniques……

16:20pm – 16:50pm | Sandip Patel, U of Louisville | Secure Communication Protocol for SCADA

SCADA networks can be easy targets for unauthorized intrusions that can result in devastating consequences to public health and safety. This presentation will discuss the research proposing a new set of Distributed Network Protocol Version 3 (DNP3) based protocols that are inherently secure and provide end-to-end security to SCADA-communications. DNP3 protocol is the most widely used SCADA protocols in the United States and many other countries. The proposed protocols use cryptographic security models not previously evaluated for SCADA applications. Additionally, various alternative methods of securing SCADA communication are proposed and evaluated in this research including using Secure Socket Layer/ Transport Layer Security (SSL/TLS), Secure IP (IPsec), and object security.

16:55 – 17:25 | Mark Burmester, FSU
Breno de Medeiros, FSU
Alec Yasinsac, FSU
Tri le Van, FSU | Ubiquitous Security Initiative at Florida State University

Network security measures such as traditional firewalls and intrusion detection systems rely on the establishment and enforcement of boundaries. By analogy with security and integrity measures by biological and political systems, having protected boundaries is an important, but not the only form of security. Biological systems use lock-and-key protein-matching approaches to recognize self from other. Security systems have an equivalent: The use of cryptographic keys, passwords, and other authentication mechanisms. While cryptography cannot provide solutions for all (and even most) types of security problems, poor utilization of cryptographic techniques remains a factor behind security failures. System administrators find it di□cult to apply cryptography e□ectively. Part of the problem is that cryptographers' description of Alice-and-Bob cryptographic protocols is often far distanced from real-world utilization scenarios. On this front, there is an improving perspective. Recent cryptographic approaches (such as universal composability and reactive systems) merge cryptographic analysis and formal methods techniques and may finally give security researchers appropriate tools to apply rigorous (i.e., provable) approaches to the design of real, useful security systems. In this talk, I will present current e□orts at Florida State University's Security and Assurance in Information Technology Lab to further the research into universally compos-able security mechanisms for practical security in the ubiquitous computing environment.

17:30pm | Day 1 Session Ends

Thursday, May 11, 2006 Building 5100, Auditorium (Room 128)

07:30am – 08:00am	Refreshment available	Delta Crown Room, Room 140
08:00am – 08:45am	Kimberly D. Rasar	Keynote Address

Kimberly D. Rasar is the Acting Senior Information Management Executive, Office of Science, U.S. Department of Energy. After serving on a 2-year detail assignment to the Department of Energy's (DOE) Office of Science (SC) to help launch the (SciDAC) Scientific Discovery Through Advanced Computing Program as well as to launch the Corporate R&D Portfolio Management Environment (ePME) Project, Ms. Rasar joined the DOE in November 2000 as the Deputy Manager for the SciDAC Program in the SC's Office of Advanced Scientific Computing. Ms. Rasar later moved to the SC's Office of Information Technology Management and served as the Manager for the ePME project. Thereafter, Ms. Rasar became the Principle Associate Senior Information Management Executive (SIME); built and resided over the Capital Planning and Investment Control and Enterprise Architecture (EA) Programs; and served as a member of the Department's Information Technology Council and EA Governance teams. Ms. Rasar now serves as the SC's Acting Senior Information Management Executive. Prior to joining the Department, Ms. Rasar was the Director of Collaborative Technologies Research in the Computer Science and Mathematics Division at Oak Ridge National Laboratory. Prior to that, Ms. Rasar was a staff researcher in Visual and Information Science. Ms. Rasar began her career in finance and business management and served in that capacity for five years prior to joining the Computer Science and Mathematics Division. Ms. Rasar's undergraduate work was completed at the Tennessee Technological University, and her graduate work was completed at the University of Tennessee.

08:50am – 09:20am	Jim Rome, ORNL	Enclaves and Collaborative Domains

A well-behaved policy forms the basis for implementing security and for determining if the policy is being enforced. Policies become more difficult to define when multiple sites are involved, or when resources are controlled by different people. By splitting the problem into local enclaves and collaborative domains, which define policy across enclave boundaries, it becomes easier to express policies and to resolve differing site policies…..

09:25am– 09:55am	Jung-Min Park, VA Tech	Ensuring Trust in Cognitive Radio Networks

Cognitive Radios (CRs) [7, 9] are seen as the enabling technology for OSS *Opportunistic Spectrum Sharing*. Unlike a conventional radio, a CR has the capability to sense and understand its environment and actively change its mode of operation. CRs are able to carry out *spectrum sensing* for the purpose of identifying vacant spectrum not used by primary users—i.e., identifying spectrum "white spaces". Once white spaces are identified, CRs "opportunistically" utilize these white spaces by transmitting in them without causing interference to primary users. Recently, the problem of spectrum sensing has attracted a lot of attention from the research community. In this research, we are primarily interested in the security problems related to spectrum sensing. In particular, we focus on the mechanism for ensuring trust in spectrum sensing. Security in spectrum sensing is an important problem that arises from the need to distinguish primary users from secondary users……

10:00am – 10:15am	BREAK	Delta Crown Room, Room 140
10:20am – 10:50am	Seong-Moo Yoo, U of Ala	Modeling and implementation of Insider Threats Based on Bayes Net and Snort IDS

To facilitate early and accurate detection of the insider threat, a number of new methods and ideas should be explored. First, there must be a technique to understand the behavior of information systems users and to be able to determine that a user's behavior is not normal. To overcome the limitations of current systems, we are proposing a multi-level, evidence based intrusion detection software module. This system will monitor the network at multiple levels and fuse the information utilizing Bayesian Networks……

10:55am – 11:25am	Alec Yasinsac, FSU	Non-Boolean Authentication

In theory, authentication is Boolean; either someone is who they say the are or they are not. We propose a model, architecture, and mechanisms that accommodate the reality that authentication is rarely Boolean. We rely on abstract notions of limited transitive trust with time-sensitive, information maturity and growth in our multi-level authentication model. Our architecture is a two-tiered structure that allows action categories that are offset by active responses as additional authentication information emerges. Our mechanisms focus on independent, cooperating identity sensors and state reversion…..

Building 5200, Cafeteria

11:30am – 12:30pm	Break for Lunch

Building 5100, Auditorium (Room 128)

12:45pm – 13:15pm	Srivatsa Mudhakar, Ga Tech James Caverlee, Ga Tech Ling Liu, Ga Tech	Security Architectures and Algorithms for Publish-Subscribe Network Services

A large number of emerging Internet applications requires information dissemination across different organizational boundaries, heterogeneous platforms, and a large, dynamic population of publishers and subscribers. A publish-subscribe (pub-sub) network service is a wide-area communication infrastructure that enables information dissemination across geographically scattered and potentially unlimited number of publishers and subscribers…An important characteristic of pub-sub network services is the decoupling of publishers and subscribers combined with content-based routing protocols, enabling a many-to-many communication model. Such a model presents many inherent benefits as well as potential risks… We have developed SGuard − a security architecture and a set of algorithms to secure wide-area pub-sub network services. Our design has been guided by the following two principles: (i) Cryptographic techniques need to be adapted using application specific knowledge in order to secure an application without compromising on its performance and scalability metrics. (ii) Using intrinsic properties such as the structure of the pub-sub network and the semantics of the application leads to powerful and effective security algorithms……

13:20pm – 13:50pm	Carlton Pu, GA Tech Jinpeng Wei, GA Tech	Modeling, Finding, Analyzing and Taming Vulnerabilities in Unix-Style File Systems

TOCTTOU (Time-Of-Check-To-Time-Of-Use) is a well known security problem [1]. An illustrative example is sendmail, which used to check for a specific attribute of a mailbox file (e.g., it is not a symbolic link) before appending new messages. However, the checking and appending operations do not form an atomic unit. Consequently, if an attacker (the mailbox owner) is able to replace his mailbox file with a symbolic link to /etc/passwd between the checking and appending steps by sendmail, then he may trick sendmail into appending emails to /etc/passwd. As a result, an attack message consisting of a syntactically correct /etc/passwd entry with root access would give the attacker root access. TOCTTOU is a serious threat: ….
Although in general TOCTTOU problems are not limited to file access [6], in we have been focusing on file-related TOCTTOU problems. Our first contribution is an abstract model of such TOCTTOU problems (called STEM – **S**tateful **T**OCTTOU **E**numeration **M**odel) that captures all potential vulnerabilities…. Our second contribution is a mapping of the STEM model to concrete file systems, namely, POSIX and Linux. Applying the STEM model, we were able to enumerate all the exploitable TOCTTOU pairs (the ones that can be used by attacker to obtain some advantage such as privilege escalation) for POSIX (485 pairs) and Linux (224 pairs)…..

13:55pm – 14:25pm	Kevin G. Coleman	Combating Cyber-Crime and Terrorism

Combating the threat of cyber terrorism has become and endless task. Each day brings with it more sophisticated and complex attacks against the information assets within the United States. Here to fore the administrations attitude toward handling cyber terrorism could be described as mainly a hands-off approach. The primary responsibility for securing cyberspace has been handed off to individuals and corporations. Security researchers and ethical hackers who find these vulnerabilities need to realize that discretion is more important than ever. In 2005, software vulnerability exploitations were very successful because cyber criminals were able to detect vulnerabilities and capitalize on them or to create exploits faster than patches could be made available. Speed is the critical characteristic in these types of attacks. This presentation will examine the significance of this problem and the exposure the day-zero situations has created for business, government and industry. Our ability to combat cyber terrorism and the rampant growth in computer crime requires this issue to be solved now. Failure to address this issue will lead to a digital meltdown of our information infrastructure.

14:30pm - 16:00pm	Panel Discussion	"Roadmap for Research" Panelists: Richard Brooks (Clemson); Axel Krings (Univ of Idaho); Thomas Longstaff (CMU); Carlton Pu (GA Tech); Kimberly Rasar (DOE HQ)
17:00pm	CS&IIR Workshop 2006 Ends	

CS&IIR Workshop 2007 tentatively scheduled for April 26-27, 2007