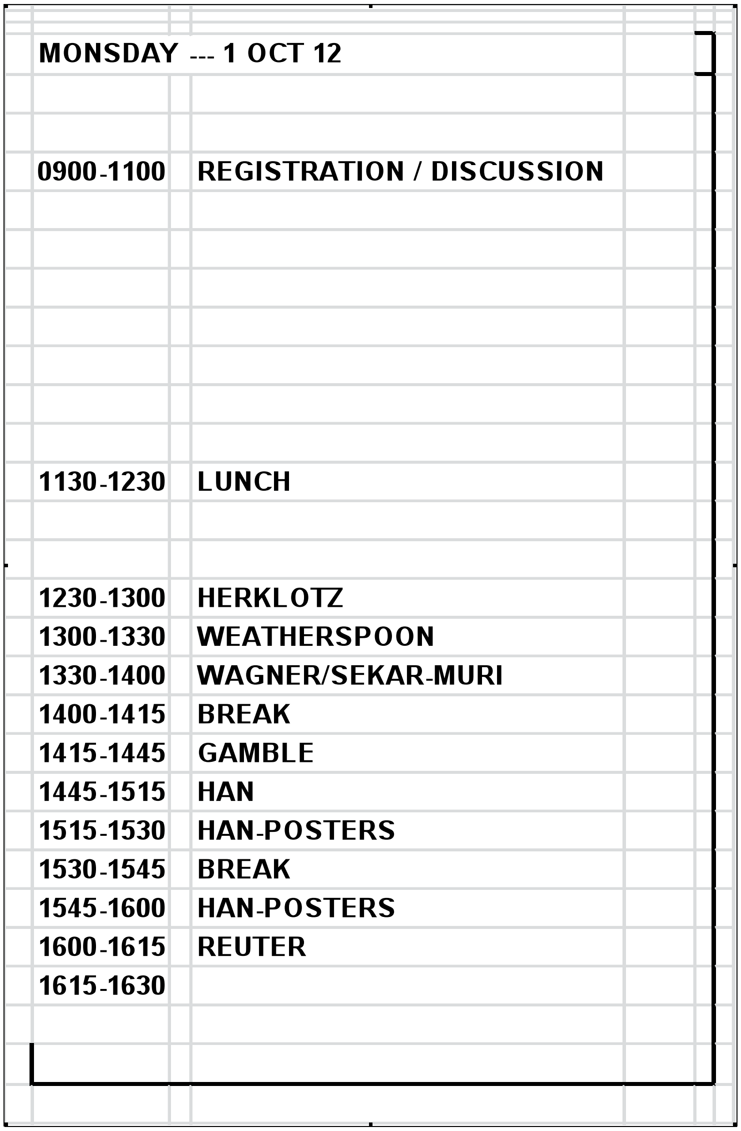
HERKLOTZ: 1012 INFORMATION OPERATIONS AND SECURITY PI MEETING ABSTRACTS



MONSDAY --- 1 OCT 12	
0900-1100	REGISTRATION / DISCUSSION
1130-1230	LUNCH
1230-1300	HERKLOTZ
1300-1330	WEATHERSPOON
1330-1400	WAGNER/SEKAR-MURI
1400-1415	BREAK
1415-1445	GAMBLE
1445-1515	HAN
1515-1530	HAN-POSTERS
1530-1545	BREAK
1545-1600	HAN-POSTERS
1600-1615	REUTER
1615-1630	

David Wagner, UCB
DHOSA: Defending Against Hostile Operating Systems

Continuing advances in sophisticated and stealthy rootkits warrant a reexamination of a fundamental assumption made in application security, namely, that the underlying operating system is trustworthy. The conventional wisdom beneath this assumption is that it is impractical, if not impossible, to build security mechanisms without support from the operating system and hardware. The DHOSA project challenges this conventional wisdom, and seeks to develop an integrated suite of techniques that limit the harm that a hostile OS can inflict on an application. We are pursuing basic research on a wide range of topics, including virtualization and binary translation techniques to build security mechanisms over untrustworthy software components, new approaches that minimize the impact of vulnerabilities in operating systems, architectures and algorithms for building secure distributed systems, and formal methods to increase confidence in hypervisors, virtual machine monitors, binary translators, binary emulators, assemblers, compilers, and other critical trusted components.

Dr. Keesook J. Han, AFRL/RIGA
CyberBAT: High Performance Cloud Auditing and Applications

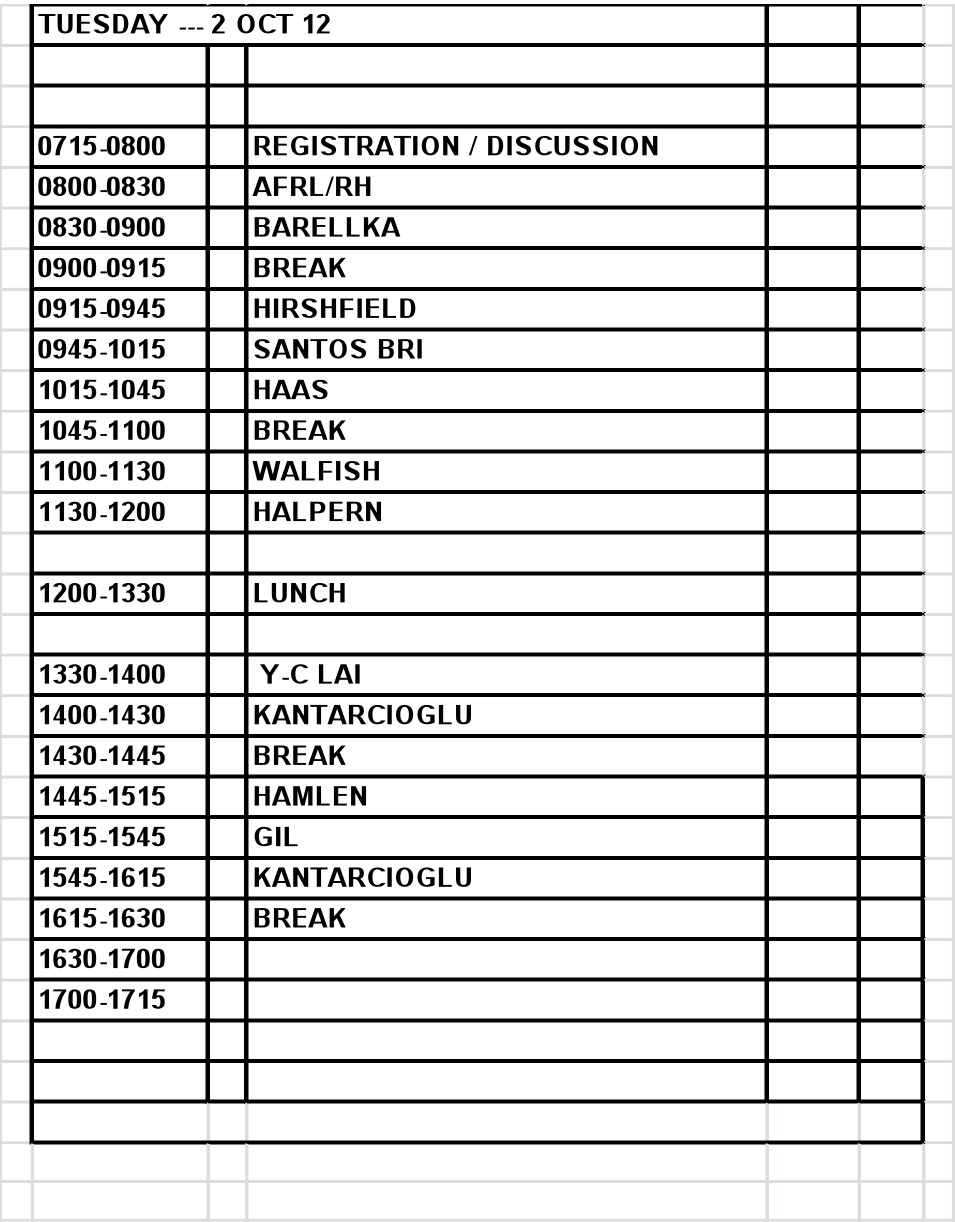
Cloud computing represents one of the most significant shifts in information technology due to its scalable, flexible, and cost-efficient access to computing resources. There are persistent concerns about security, availability and performance of cloud services. Cloud auditing is an urgent cloud computing research topic to resolve these concerns. The main objective of this research is to present the concepts, algorithms, techniques and components of high performance cloud auditing systems in order to reduce cloud security risks, and increase availability and the performance of cloud computing for surviving in a contested network environment. CyberBAT team's cloud research focuses on the emerging cloud auditing challenges and issues to manipulate massive and multimodal data management and access control for rapid response in heterogeneous and hybrid cloud computing environments including Android smartphone cloud auditing.
This presentation briefly introduces the CyberBAT team's cloud research areas as follows:

- Surveys and Future Issues: Cloud Computing, Cloud Security, Cloud Auditing
- Cloud Management: QoS, Service Level Agreements at Different Levels, Service Level Management, Availability Management, Capacity Management, Semantic Cloud Computing, Data Sharing and Management
- Cloud Auditing: Cloud Audit Data Collection Techniques, Monitoring and Characterization, Emerging Cloud Threat Analysis, Information Theoretic Data Analytics and Visualization for Cloud Auditing, Information Metrics for Decision Making, Heavy-Tailed Distribution Analysis, Inference Theory, Information Fusion, Android Smartphone Security
- High Performance Computing and Communication for Cloud Auditing: GP-GPU Computing, Hadoop based Distributed Computing, MapReduce, I/O virtualization for Storage/Network/Accelerators, Storage and network I/O subsystems in Hybrid Cloud Environments, Fast and Reliable Data Transfer
- Assured Cloud Auditing Architecture, Cross-Sites Auditing Mechanism (server/router/clients), Reliability, Fault-Tolerance, Privacy Protection and Security, Cloud Audit Data Storage, and Secure and Efficient Sharing for Rapid Response

Shouhuai Xu

Stochastic Cyber Attack Processes: Concept, Statistical Analysis Framework and Case Study

Rigorously characterizing cyber attacks is an important aspect of cyber security research. The importance can be appreciated not only from a theoretic perspective (the characterizations are a necessary step before we can build faithful cyber security models), but also from a practical perspective (the characterizations can lead to insights for proactive adaptive defense). This motivates us to introduce the novel concept of stochastic cyber attack processes, a new kind of mathematical objects for describing cyber attacks. We also present a statistical framework for analyzing the properties of stochastic cyber attack processes. To demonstrate the usefulness of the new concept and the statistical framework, we conduct a case study based on some cyber attack data collected by honeypots. One particular finding is that the stochastic cyber attack processes exhibit the so-called Long-Range Dependence (LRD), a phenomenon that was not known to be relevant in the cyber security domain until now. We show that knowing the presence of LRD facilitates “Gray-Box” model fitting and attack prediction, which are significantly more accurate than “Black-box” fitting and prediction.



TUESDAY --- 2 OCT 12				
0715-0800		REGISTRATION / DISCUSSION		
0800-0830		AFRL/RH		
0830-0900		BARELLKA		
0900-0915		BREAK		
0915-0945		HIRSHFIELD		
0945-1015		SANTOS BRI		
1015-1045		HAAS		
1045-1100		BREAK		
1100-1130		WALFISH		
1130-1200		HALPERN		
1200-1330		LUNCH		
1330-1400		Y-C LAI		
1400-1430		KANTARCIOGLU		
1430-1445		BREAK		
1445-1515		HAMLEN		
1515-1545		GIL		
1545-1615		KANTARCIOGLU		
1615-1630		BREAK		
1630-1700				
1700-1715				

Michael Walfish, UT
Using computational resources without assuming their correctness

We are investigating how clients can use computer resources without having to trust (meaning assume) that those resources operate correctly. For example: Can we outsource computation to servers if the servers are not guaranteed to return the right answer? Can we build a distributed storage system that works even if _all_ of the machines misbehave? Can we build a network if we cannot trust that the routers will forward properly? These are critical questions in high-assurance regimes.

Our funded research over the last few years has established, over several inquiries, that these questions have affirmative answers. This talk will cover several of these inquiries.
First, I will describe a system for _verified computation_: one machine specifies a computation to another one and then, without executing the computation, checks that the other machine carried it out correctly. It has long been known that (1) probabilistically checkable proofs (PCPs) offer highly principled and powerful solutions in theory; and (2) these solutions are wildly impractical (trillions of CPU-years or more to verify simple computations). Yet, we have challenged (2). We have done new theoretical work to improve performance by over 20 orders of magnitude and to verify arbitrary computations expressed in a high-level language. We have a parallel GPU-based implementation of the system and a compiler to go from computations in a high-level language to executables that implement the protocol entities. The resulting system is not quite ready for the big leagues, but it is close, and it suggests that in the near future, PCPs could be a real tool for building secure systems. Since PCPs offer unconditional (and hence extremely principled and strong) guarantees, this is a very exciting development.
Second, I will describe a cloud storage system that tolerates buggy or malicious behavior by any number of clients or servers, yet it provides guarantees to correct clients. Put differently, this system assumes radically less than any prior system about the correctness of participating hosts.
Third, and time permitting, I will describe a new networking primitive, called a Path Verification Mechanism (PVM). The purpose of a PVM is to enforce the network policies of the entities along a communication path. For instance, users may want to choose providers whom they trust to be discreet, or a receiver may want traffic destined to it to travel through an intrusion detection service; the PVM enforces these considerations even if the forwarders in the network misbehave.

Ying-Cheng Lai, Arizona State University
Controllability of Complex Networks

Controlling complex networks is relevant to many areas of science and engineering, and has the potential to generate technological breakthroughs. The aim of the talk is to discuss recent results from AFOSR sponsored research on complex networks at Arizona State University: (1) optimization of network controllability and (2) energy required for controlling complex networks.
For the first problem, optimal control is referred to as the situation where a large, complex networked dynamical system is driven toward some desired state using as few external control signals as possible. In the past year, we proposed a general approach to optimizing the network controllability by judiciously perturbing the structure of the network. The principle of our perturbation method was validated theoretically and demonstrated numerically for homogeneous and heterogeneous random networks and for different types of real networks as well. The applicability of the method was addressed with respect to the relative costs of establishing links and imposing external controllers. The implementation of our method elucidates, interestingly, some intricate relationship between certain structural properties of the network and its controllability.
For the second problem, we addressed the physically important issue of the energy required for achieving control by deriving and validating scaling laws for the lower and upper energy bounds. These bounds represent a reasonable estimate of the energy cost associated with control, and provide a step forward from the current research on controllability toward ultimate control of complex networked systems.

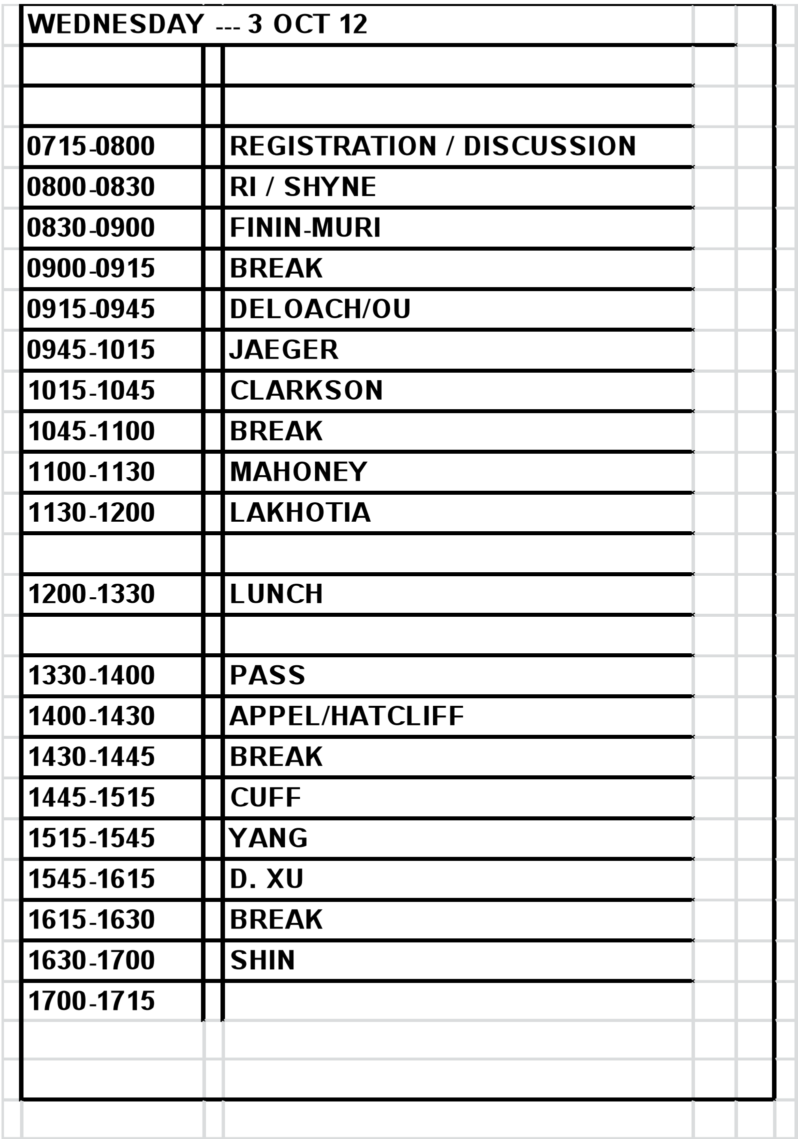
References:

1. W.-X. Wang, X. Ni, Y.-C. Lai, and C. Grebogi, “Optimizing controllability of complex networks by small structural perturbations,” Physical Review E 85, 026115 (2012).

2. G. Yan, J. Ren, Y.-C. Lai, C. H. Lai, and B. Li, “Controlling complex networks - how much energy is needed?” Physical Review Letters 108, 218703 (2012).

Gil, Yolanda – University of Southern California
“Cybersecurity through Nimble Task Allocation: Workflow Reasoning for Mission-Centered Network Models”

Traditional cybersecurity has focused on techniques to analyze and eliminate vulnerabilities in a network, often in response to actual security breaches of previously unknown weaknesses. Recognizing that in practice network operations can never be fully secure, a major focus of recent research is on intrusions that are assumed to be ongoing in the network by one or more malicious parties. In this new view on cybersecurity, a key desired capability is to be able to accomplish a mission even while the network is compromised and subject to deception. However, traditional network models lack a representation of the mission and of how network resources are utilized to accomplish various aspects of the mission. In this project, we will investigate a new approach to develop a general framework for representing models of mission goals and tasks, and to exploit those models to make a mission more robust to deception operations co-occurring in the network. These mission-centered network models (MCNMs) will build on and extend current two-layered (logical/physical) network models by integrating a new layer of task-level representations of the mission into those models. In this new task-oriented layer, a mission can be characterized as a set of goals, each accomplished by a set of interdependent tasks that place requirements on the network resources. The system can then dynamically control the mappings of those tasks onto network resources using a variety of algorithms that take into account which resources are currently compromised. As a result, a mission can be protected from ongoing intrusion and deception activities by dynamically reallocating resources as they become compromised and by examining provenance records of task outcomes to determine their reliance on compromised resources. MCNMs can be used to determine which resources are critical for any given mission, to prioritize the use of uncompromised resources, to accomplish and estimate the trust on mission tasks when resources are compromised, and to determine the practical impact on the mission of deception activities. MCNMs will enable a new approach to cybersecurity in network-based operations.



WEDNESDAY --- 3 OCT 12

0715-0800	REGISTRATION / DISCUSSION
0800-0830	RI / SHYNE
0830-0900	FININ-MURI
0900-0915	BREAK
0915-0945	DELOACH/OU
0945-1015	JAEGER
1015-1045	CLARKSON
1045-1100	BREAK
1100-1130	MAHONEY
1130-1200	LAKHOTIA
1200-1330	LUNCH
1330-1400	PASS
1400-1430	APPEL/HATCLIFF
1430-1445	BREAK
1445-1515	CUFF
1515-1545	YANG
1545-1615	D. XU
1615-1630	BREAK
1630-1700	SHIN
1700-1715	

Trent Jaeger, Vinod Ganapathy, Somesh Jha, Penn State University
Information Flow Integrity for Systems of Independently-Developed Components

Modern commodity systems now have several security enforcement mechanisms to limit adversary access to processes, yet security practitioners still work reactively, responding to vulnerabilities as adversaries identify them. A problem is that these available security enforcement mechanisms are deployed independently of one another, so adversaries take advantage of inconsistencies and invalid assumption to further attacks. To address this problem, we are developing a theory of integrity safety that enables reasoning about adversary access across security mechanisms. Using this theory, we will

aim to develop methods that evaluate whether a program can be safely deployed in particular deployments relative to integrity safety.
In this talk, I will discuss our progress thusfar on identifying candidate integrity safety properties in systems and programs and in applying them to protect process integrity. First, I will describe our experiences evaluating the integrity of running code, which will highlight several integrity safety properties. One specific topic will be our recent work in detecting name resolution vulnerabilities in programs. Second, I will outline how we envision using such integrity safety properties to protect process integrity. For example, I will show how to use security policies and runtime analysis to compute program attack surfaces, which identify the individual program system calls accessible to adversaries. Using this knowledge, information flow models of programs can be constructed to evaluate program integrity safety, but the challenge is to deal with adversary access (i.e., choose endorsers and where to place them). We will discuss possible program integrity safety properties to limit adversary access in programs, with the goal of maintaining integrity safety for system objects. The resulting combination system and program integrity safety enforcement enables end-to-end evaluation of integrity protection using commodity system policies and legacy code.

Rafael Pass, Cornell University
On the (Im)Possibility of Tamper-Resilient Cryptography

We initiate a study of the security of cryptographic primitives in the presence of efficient tampering attacks to the randomness of honest parties. More precisely, we consider p-tampering attackers that may tamper with each bit of the honest parties' random tape with probability p, but have to do so in an "online" fashion. We present both positive and negative results:
* Any secure encryption scheme, bit commitment scheme, or zero- knowledge protocol can be ^{3}broken^{2} with probability p by a p-tampering attacker. The core of this result is a new Fourier analytic technique for biasing the output of bounded-value functions, which may be of independent interest (and provides an alternative, and in our eyes simpler, proof of the classic Santha-Vazirani theorem).
* Assuming the existence of one-way functions, cryptographic primitives such as signatures, identification protocols can be made resilient to p-tampering attacks for any p = 1/n^{\alpha}, where \alpha > 0 and n is the security parameter.

Junfeng Yang, Columbia University
Concurrency Attacks and Defenses

Just as errors in sequential programs can lead to security exploits, errors in concurrent programs can lead to concurrency attacks. Questions such as whether these attacks are feasible and what characteristics they have remain largely unknown. In this talk, I will present a preliminary study of concurrency attacks and the security implications of real world concurrency errors. Our study shows that concurrency attacks are indeed real and can be practiced by attackers to violate confidentiality, integrity, and availability of critical systems. Based on our study, we propose new research directions for accurately Detecting, Avoiding, Surviving, and Healing concurrency errors. If successful, our research will result in a novel approach and a system called DASH for improving software security and reliability, benefiting the Nation's cyber security; the Military can also gain new competitive means in cyber warfare by running DASH to identify concurrency vulnerabilities in the infrastructure of hostile nations.

Kang G. Shin, The University of Michigan
Protection of Mission-Critical Applications from Untrusted Execution Environments

Computing environment has changed significantly in the past few years. Instead of relying on a local physical host for computing tasks, companies, government organizations and personal users have all begun to take advantage of the emerging cloud computing infrastructure to improve their computing performance and experiences. How to provide a secure and fault-resilient environment in this new cloud era become a great challenge for computer science researchers and practitioners from both academia and industry.

We have been taking a two-pronged approach. First, we extend our SP3 protection system to better support recent computer architectures so that the secrecy and integrity of user applications data are protected against potentially compromised operating systems running on either users' local physical hosts or cloud computing facilities, or both. Second, we find that cloud management stacks have significant impact, not only on the performance and functionality of the cloud environment, but also on the security and fault-resilience of the cloud as well. To meet this challenge, we have designed and implemented a prototype diagnostic tool utilizing a new logging framework of OpenStack—a popular open-source cloud management stack, and demonstrate its usefulness via bug/fault detection in some virtual machine provisioning scenarios. Combining local physical host protection with high-level cloud management stack hardening techniques, we are working toward the construction of a more secure and fault-resilient computing environment.

THURSDAY---4 OCT 12		
0715-0800		REGISTRATION / DISCUSSION
0800-0830		AFRL/RY
0830-0900		FRIDRICH
0900-0915		BREAK
0915-0945		CRAVER??
0945-1015		PADOS
1015-1045		
1045-1100		BREAK
1100-1130		DEBRAY
1130-1200		KIYAVASH
1200-1330		LUNCH
1330-1400		BROOKS
1400-1430		
1430-1445		BREAK
1445-1515		STOLFO
1515-1545		SKORMIN
1545-1600		BREAK
1600-1630		ZUO
1630-1700		B. CHEN
1700-1715		
1715-1730		

Negar Kiyavash, University Illinois
Timing-based Inference: The Good, the Bad, and the Ugly

Timing can provide a new degree of freedom for communication and causal inference, but it may also be exploited to learn or leak information by adversaries. We investigate the power of timing analysis in three scenarios. First, we quantify the amount of information leakage in timing side channels and provide some counter measures. Second, we present robust and transparent steganographic timing codes. Finally, we introduce efficient algorithms for causal inference in networks.

Nathaniel Boggs and Salvatore J Stolfo, Columbia University
Towards Practical Measures of Security

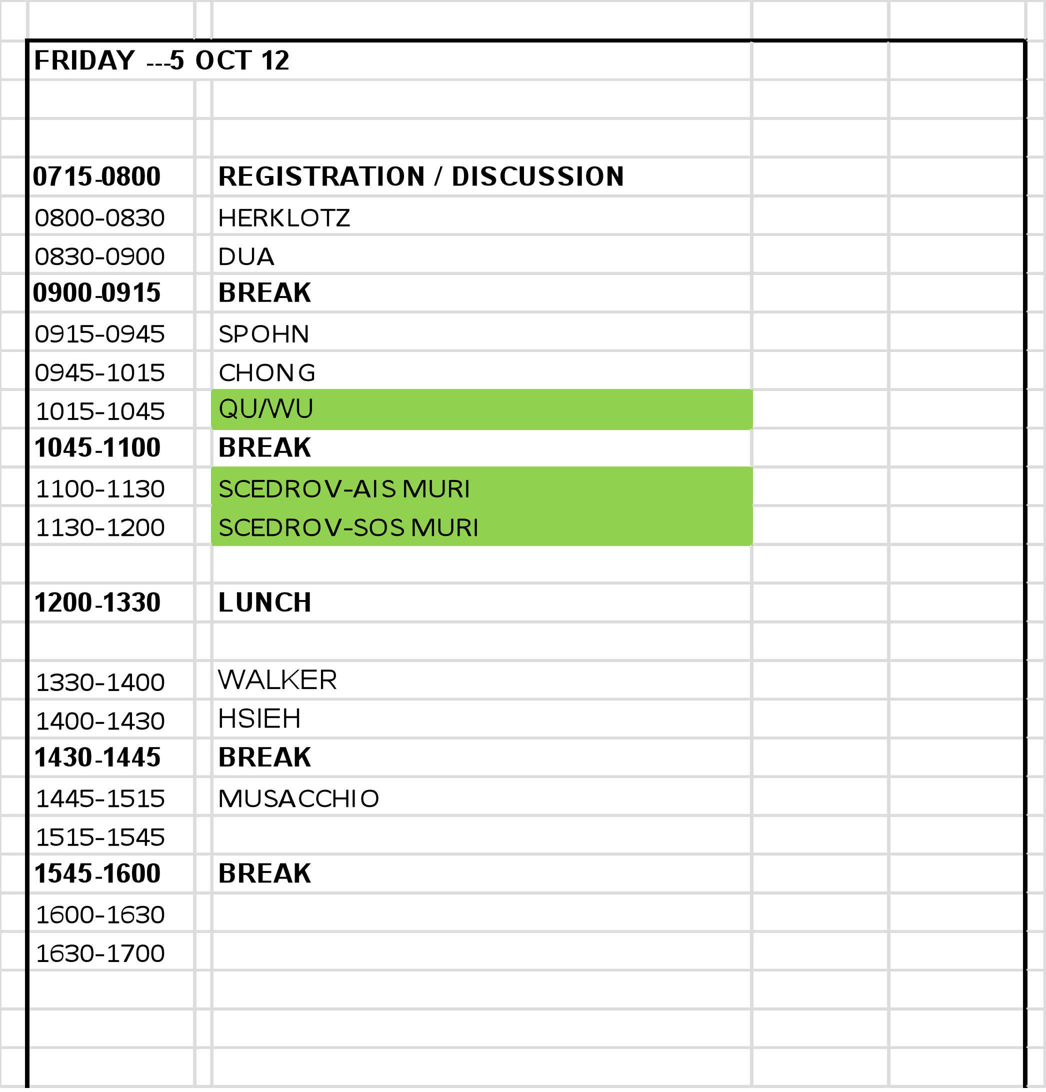
Organizations have little idea of how secure they are against varying degrees of attacks. Even after expensive penetration testing that may reveal vulnerabilities, an organization faces the difficult process of finding a security product that improves their security posture. We propose a novel scalable method for answering vital questions such as "How secure is an organization?" and "What is the most effective additional security product to purchase and deploy?" by empirical experiments. We acquired detailed attack information appropriate to represent a wide range of attacks seen in the wild. Each attack type is then tested against a large variety of security products each tested against the portion of the attack that it can parse. We then determine which attacks go undetected by a set of security products.
This test determines the overlap of security products and which additional product would best fill the gaps in any particular security setup.
This approach also may be used to measure the overall security posture of an organization. We conduct an experiment implementing the approach for the subclass of attacks known as drive-by downloads and the subclass of adversaries that send such attacks in non-targeted spam emails. We measure over 40 security products varying in detection techniques. By capturing in the wild attack data and testing against these products we identify in real time the particular attack vectors each is able to detect. These measurements reveal the redundant and complementary layers of defense against drive-by downloads confirming the need for defense in depth even against non-targeted attacks.
The technique is clearly extensible and may be implemented as a cloud-based service to amortize its cost by testing a number of (DoD) organization's network flows that subscribe to the service. This work is an initial practical step towards a Science of Security.

ZUO, UNIVERSITY OF NORTH DAKOTA
"Towards a Proof-Carrying Approach for Survivability Specification and Verification"

This research aims to develop a logic-based framework for proof-carrying survivability: a system user publishes their survivability requirements, a system provider compiles and submits a proof-carrying code, and finally the user applies a simple and fast program to verify the proof. If the proof is validated, all the requirements are guaranteed to be satisfied. By shifting the responsibilities of the survivability proof from a user to a system provider, the user only needs a lightweight checker to verify that a system possesses a set of safety and security properties for system survivability. Any system that does not meet the user's requirements will be detected before the system is deployed, thus avoiding a situation where the user has to fix problems and recover the system after damages have already been caused.

Our work included two main thrusts. First, we developed the necessary approaches and algorithms for the user to quantify system survivability. Attack modeling and impact quantification allow the user to identify the critical system properties necessary for a system to survive malicious attacks. The survivability requirements are specified based on the qualitative analysis of system properties and modeling of attacks. We studied the inherent survivability properties of critical information systems in general and the distributed enterprise RFID system in particular.

In the second thrust, we developed the logic constructs for survivability proof-carrying. An application-specific logic was designed with sound formal properties. In particular, the logic framework facilitates constrained reasoning -- possibilistic uncertainty and survivability requirement constraints are effectively linked to a logical reasoning process. The framework makes it possible to express fuzzy pattern matching and arbitrary user-defined constraints in formal proofs.



FRIDAY ---5 OCT 12	
0715-0800	**REGISTRATION / DISCUSSION**
0800-0830	HERKLOTZ
0830-0900	DUA
0900-0915	**BREAK**
0915-0945	SPOHN
0945-1015	CHONG
1015-1045	QU/WU
1045-1100	**BREAK**
1100-1130	SCEDROV-AIS MURI
1130-1200	SCEDROV-SOS MURI
1200-1330	**LUNCH**
1330-1400	WALKER
1400-1430	HSIEH
1430-1445	**BREAK**
1445-1515	MUSACCHIO
1515-1545	
1545-1600	**BREAK**
1600-1630	
1630-1700	

Stephen Chong, Harvard University
Integrating Programming Language and Operating System Information Security Mechanisms

The interaction between language-based security mechanisms and operating system security mechanisms has remained largely unexamined, and unexploited. Language-based information security uses programming language abstractions and techniques to reason about and enforce information security, and can provide strong fine-grained application-specific information security guarantees. Operating system (OS) information security mechanisms use OS-level abstractions to provide isolation and protection for processes executing in a system; recent operating system mechanisms can provide fine-grained isolation and protection.

This project investigates interactions between language-based and OS mechanisms for information security, and aims to exploit these interactions both to improve the precision of security enforcement, and to provide greater assurance of information security. This talk will outline the proposed primary directions of research: Integration of language-level and OS mechanisms for provenance; Fine-grained information-flow control for scripting; and Automatic partitioning of applications to enforce information security with OS mechanisms.