Application Service Security Session

Evaluation of Survivable Service-Oriented Systems Through Collaborative Red Teaming

1569612281

An increasing number of military systems are being developed using Service Oriented Architecture (SOA). Some of the features that make SOA appealing, like loose coupling, dynamism and composition-oriented system construction, make securing service-based systems more complicated. We have been developing Advanced Protected Services (APS) technologies for improving the resilience and survival of SOA services under cyber attack. These technologies introduce a layer to absorb, contain, and adapt to cyber attacks prior to the attacks reaching critical services. This paper describes an evaluation of these advanced protection technologies using a set of cooperative red team exercises. In these exercises, an independent red team launched attacks on a protected enclave in order to evaluate the efficacy and efficiency of the prototype protection technologies. The red team was provided full knowledge of the system under test and its protections, was given escalating levels of access to the system, and operated within agreed upon rules of engagement designed to scope the testing on useful evaluation results. We also describe the evaluation results and the use of cooperative red teaming as an effective means of evaluating cyber security.

Partha Pal
BBN Technologies, USA

Sources of Misinformation in Online Social Networks: Who to suspect?

1569612359

Online Social Networks (OSNs) have recently emerged as one of the most effective channels for information sharing and discovery due to their ability of allowing users to simultaneously consume and produce new content. While this advantage provides users more rooms to decide which content to follow, it also makes OSNs fertile grounds for the wide spread of misinformation which can lead to undesirable consequences. In order to guarantee the trustworthiness of content sharing in OSNs, it is thus essential to have a strategic investigation on the first and foremost concern: the sources of misinformation.

In this paper, we study k Suspector problem which aims to identify the top k most suspected sources of misinformation. We propose two effective approaches namely ranking-based and optimization-based algorithms. We further extend our solutions to cope with the incompleteness of collected data as well as multiple attacks, which mostly occur in reality. Experimental results on real-world datasets show that our approaches achieve competitive detection ratios in a timely manner in comparison with available methods.

Dung Nguyen
University of Florida, USA

Security and Provenance in M3GS for Cross-Domain Information Sharing

1569612381

Modern military activities involve significant data sharing across security domains. We present the concepts and architecture of a Mission-oriented Multi-domain Multi-level security Graphics Server (M3GS) in the environment of GIG 2.0 and cloud computing. M3GS aims at providing information support for a dynamic team collaborating on a mission of...
warfighting, intelligence, anti-terrorism, or rescue and disaster relief; information providers input data (with various security labels in different security domains) into M3GS, and through M3GS, those data are displayed with proper widgets on the screens of information clients permitted to access; what data can flow to which screen is governed by security policies. While the Bell-LaPadula model is used to enforce traditional mandatory access control, a new challenge is that the data shared have different owners from different security domains, and are subject to their own security policies. We address this problem by using dynamic provenance-dependent attribute-based policies.

Jingwei Huang
University of Illinois at Urbana-Champaign, USA

Network Performance Impact of Access Control Policies in Tactical Wireless Networks

1569612789

Tactical Wireless Networks (TWN) are a cornerstone of military communications in deployed environments. In TWNs bandwidth and network resources are extremely limited; efficient security mechanisms must be considered as networks become exposed to multinational access, influence and composition as well as increasingly complex security protocols. The communication burden of the WSN Authorization Specification Language (WASL) access control policies on an Enhanced Position Location Reporting Service is analyzed for three needlines: Carrier Sense Multiple Access (CSMA), Dynamically Allocated Permanent Virtual Circuits (DAP), and Multiple Source Group (MSG). Results determined that CSMA needlines quickly exhausted resources as nodes vied for transmission time; shorter delay times were experienced but suffered greater packet losses. The DAP needlines generally performed very well. The virtual circuits allowed data to be transmitted reliably resulting in a high completion rate with moderate to extreme delay times depending on resource contention. In small networks or networks with few sources, multiple MSG shares could be used to increase guaranteed bandwidth. The traffic model applied to the MSG network was well suited for this and had high completion rates for messages. However, as the number available of shares dwindled, delay and communication loss increased dramatically.

William Stout
Air Force Institute of Technology, USA

NextVC2 - A Next Generation Virtual World Command and Control

1569612839

In this paper we introduce a new approach to Virtual World-based Command and Control environments for multi-domain mission critical operations. Our target scenario is a military coalition operation in common operation setting. All coalition partners participate in a common virtual command and control environment while different operational contexts take place simultaneously, at different levels of information release. Context-dependent information release is regulated through policies and seamlessly enforced by the command and control framework without explicit participation of users. A prototype of the proposed capability was implemented and demonstrated in open source software. In this paper, we describe our approach, some details of our prototype implementation, and our preliminary capability demonstrations.

Marco Carvalho
Florida Institute of Technology, USA
GPS Security Session

**GPU Accelerated Differential Power Analysis**

1569591375

Differential Power Analysis (DPA) is a powerful technique that has proven devastatingly effective against various encryption algorithms such as AES, Triple-DES and RSA. DPA has been able to successfully extract the secret key from these algorithms during the process of decrypting ciphertext information. Even in implementations with countermeasures, DPA can still be effective with additional traces, however at the cost of a corresponding increase in processing times. Hundreds of thousands to millions of traces may be necessary to defeat counter-measures; even high-end workstations can take days to process such large data sets. Graphics Processing Units (GPUs), available in most desktops as graphics cards on the other hand, have been effectively used in many parallel processing tasks. We use the GPU to accelerate DPA analysis and find a speedup of more than 200 times over workstation processing time. Using this method, we reduce computation time for a particular attack from 41 minutes to 12.24 seconds including the time for data transfer between the GPU and CPU.

Hiren Patel
Air Force Institute of Technology, USA

**GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design**

1569596789

In this paper, we introduce a GPS spoofing attack on the time synchronization in wireless networks. As a case study, the frequency hopping code division multiple access (FH-CDMA) based ad hoc network relying on the GPS signal is investigated. The GPS spoofing attack, which could be more malicious than other attacks such as jamming, could lead to the loss of network-wide synchronization as well as the loss of synchronization in FH code. The performance in terms of symbol error rate (SER) of the FH-CDMA based ad hoc network under such an attack is evaluated. Then we propose a CUSUM testing scheme to detect the spoofing attack by observing the dynamic range of the successful detection rate. Simulation results show that our proposed CUSUM scheme is an effective method to detect the GPS spoofing attack.

Qi Zeng
The University of Tennessee, USA

**Cooperative Jammer Design in Cellular Network with Internal Eavesdroppers**

1569599143

In this paper, we consider a cooperative jammer to improve a secrecy of the wireless transmission in a cellular downlink network. The private message intended for a single user should be kept from the remainder of the users who are regarded as internal eavesdroppers. To improve the secrecy of the intended user, we propose an employment of a helper with multiple antennas and design its optimal transmit beamforming vector. Specifically, the helper node generates the artificial interference to the internal eavesdroppers and so enhance the security by increasing the ambiguity at the eavesdroppers. Based on a framework of power gain region in [1], we optimizes the transmission strategy for the helper which maximizes the secrecy capacity of the intended user. The analytical and simulation results show that the proposed scheme enhances the secrecy capacity. In addition, all users can achieve the positive secrecy rate by the proposed scheme whose secrecy rates are zero with no helper's cooperation.

Seongah Jeong
Korea Advanced Institute of Science, Korea
Quickest Detection of GPS Spoofing Attack

1569610201

GPS is being increasingly used in critical infrastructures in modern society. Therefore, the reliability of GPS is extremely important. Recently, the vulnerability of GPS to a spoofing attack has been discussed in the literature. A malicious attacker may spoof a GPS receiver, causing it to provide incorrect navigation and timing information, which may lead to serious damage. Therefore, it is extremely important to detect spoofing attacks as quickly as possible. In this paper, we propose a quickest spoofing detection algorithm to combat GPS spoofing attacks. The experimental results demonstrate that the proposed algorithm can effectively detect the spoofing attack quickly after it occurs.

Zhenghao Zhang
The University of Tennessee, USA
MANET Security Session

A Game Theoretic Approach for Security and Quality of Service (QoS) Co-Design in MANETs with Cooperative Communications

1569554377

Cooperative communication is proposed to form a virtual MIMO system through strategic relay selection to improve communication quality in wireless networks, including mobile ad hoc networks (MANETs). Due to their unorganized and decentralized infrastructure, MANETs with cooperative communications (CO-MANETs) are vulnerable to attacks initiated on relays. Although encryption and authentication protocols may prevent compromised data transmission when a selected relay is attacked, their cost is high. In this paper, we propose a game theoretic approach to quantitatively analyze the attack strategies of the attacker so as to make rational decision on relay selection and the authentication parameter adaptation to reach the trade-off between security and Quality of Service (QoS) in CO-MANETs. Simulation results show the effectiveness of the proposed approach for security and QoS co-design in CO-MANETs.

Du Zheng
Carleton University, Canada

On Effective Sampling Techniques for Host-based Intrusion Detection in MANET

1569590187

Tactical Mobile Ad Hoc Network (MANET) demands a robust, diverse, and resilient protected communication and computing environment enabling network-centric operation with minimal downtime. Nevertheless, the nature of MANET causes security risks because mobile nodes are deployed in the open field and wireless communication makes the information accessible by anyone. Conducting cyber attack monitoring and detection in a tactical MANET becomes challenging because of limited resources and its infrastructureless network environment. To address these issue, we first study the host-based detection architecture to monitor and detect cyber attacks and then develop sampling techniques to balance the tradeoff between detection accuracy and bandwidth overhead. We derive the closed formulae to investigate the impact of detection accuracy vs. sampling techniques and parameters. We conduct real-world experiments to evaluate the effectiveness of sampling techniques and our empirical evaluation validate our theoretical findings well. We also investigate the impact of host-based attack detection on MANET.

Linqiang Ge
Computer and Information Sciences, Towson University, USA
LAA: Link-Layer Anonymous Access for Tactical MANETs

1569610217

Link layer security has been widely researched in the last decade as a means of protecting wireless networks (e.g., WEP, RSN, WPA, WPA2). However, there is little research in this area for Mobile Ad Hoc Networks (MANETs), especially for tactical MANETs. Although RSN can be used for MANETs as described in the IEEE 802.11i standard, it fails to meet some requirements of tactical MANETs, such as strong security, anonymity, and quick connectivity. In this paper, we propose a link layer anonymous access protocol (LAA) in order to provide strong security and anonymity protection for tactical MANETs. The protocol uses dynamic pseudonyms as network and node identities for network access authentication to prevent tracking, tracing, and other common attacks. It uses a localized key management mechanism for local shared key and broadcast key establishment that outperforms the connectivity and efficiency of key management in RSN and other link layer security technologies such as SEAMAN. Simulations show that the protocol has only a small effect on end-to-end delay and no effect on packet delivery ratio relative to the standard MAC, meanwhile providing anonymous communication, better protection and improved connectivity performance in the link layer for tactical MANETs.

Ronggong Song
DRDC-Ottawa, Canada

IPsec Tunnels vs. Identity-Only Obfuscation Techniques for Moving Target Networks

1569611293

There has been recent interest in applying moving target approaches to computer networks. The ability to obfuscate the adversary's view of an organization's internal network is thought to confound the adversary's network reconnaissance steps, causing certain inefficiencies in nation state actors' attack processes. Novel Moving Target Network (MTN) techniques have been proposed specifically to hide communicating endpoint identities, blinding the adversary's view of the nodes in the network. To date, however, no published work has evaluated identity-only obfuscation approaches against using IPsec ESP tunnels as a way of hiding endpoint identities. The question is, are there some network configurations where identity-only obfuscation techniques work better than IPsec ESP tunnels? We present arguments that low-overhead MTN identity-only obfuscation approaches may work more efficiently on wireless mobile, tactical, peer-to-peer networks where processing energies and transmission bandwidth are constrained and we also discuss features of metrics for measuring the success of moving target network approaches, helping to guide future research in this area.

Russell Fink
Johns Hopkins University Applied Physics Laboratory, USA

Best-Effort Data Leakage Prevention in Inter-Organizational Tactical MANETs

1569611947

Reconfigurable Radio Systems (RRS), based on technologies such as Software Defined Radio (SDR) and Mobile Ad-hoc Networks (MANETs) offer considerable advantages for military operations, such as increased network survivability and interoperability. The RRS-based Common Tactical Radio System (GTRS), currently in development by the Swedish Armed Forces, is designed for use in diverse geographical settings and for purposes varying from international combat missions to national contingency operations. However, protecting these networks from attacks and safeguarding the carried information against leaks is an ongoing research challenge, especially in combined scenarios where tactical data may flow across organizational boundaries.

This paper presents a best-effort approach to Data Leakage Prevention (DLP) for inter-organizational RRS-based networks. The proposed architecture makes use of data mining techniques and an efficient n-dimensional clustering algorithm which has previously been successfully used for real-time anomaly detection in critical infrastructure protection. The DLP architecture is developed as an extension to the GTRS system, modeled and simulated in OPNET™ Modeler.
Our results show that common data leaks can be efficiently identified by the proposed scheme, while keeping the important false positive rate at a very low level.

Johan Sigholm  
Swedish National Defence College, Sweden

Survivability Prediction of Ad Hoc Networks Under Attack

Survivability analysis focuses on the ability of network entities to function during incidents such as attacks. Currently, testing survivability of ad hoc networks consists of running scenarios with several configurations, often thousands, to obtain an understanding of the impacts of an attack. This process is very latent, choice of configurations are subjective or random, and results do not generalize to different scenarios. Focusing on these problems, in this paper, we introduce a novel method for efficient survivability analysis that uses machine learning and an attacker-focused network representation. We have collected a dataset and use it to build a classifier that accurately (above 97% true positive rate) predicts flow loss due to spoofing and data forwarding attacks.

Jaime Acosta  
US Army Research Laboratory, USA
Physical-Layer Security Session

Certification Codes for Maliciousness Detection in Physical-layer Network Coding

1569612339

The problem of two sources wanting to share information through a potentially untrustworthy relay node is considered. The two sources transmit symbols simultaneously, and the relay node employs physical-layer network coding (PNC) to forward information back to the two sources in order to increase throughput. In such a system using PNC, the relay node can easily fool the source nodes by manipulating the PNC output symbols. To enable relay maliciousness detection, a class of variable-rate codes, called certification codes, is introduced. In a certification code, redundancy is added to the source message to act as a certificate, using which a node can check against any malicious action by the relay. A simple binary certification code is designed and analyzed to demonstrate the proposed approach.

Eric Graves
University of Florida, USA

An RF-DNA Verification Process for ZigBee Networks

1569612583

Impersonation of authorized network devices is a serious concern in applications involving monitoring and control of battlefield operations and military installation infrastructure—ZigBee is among the ad hoc network alternatives used for such purposes. There are considerable security concerns given the availability of ZigBee "hacking" tools that have evolved from methods used for IEEE 802.11 Wi-Fi and IEEE 802.15.1 Bluetooth attacks. To mitigate the effectiveness of these bit-level attacks, RF waveform features within the OSI physical (PHY) layer are used to augment bit-level security mechanisms within the OSI Medium Access Control (MAC) layer. The evolution of RF 'Distinct Native Attribute' (RF-DNA) fingerprinting continues here with a goal toward improving defensive RF Intelligence (RFINT) measures and enhancing rogue device detection.

Demonstrations here involve ZigBee burst collection and RF-DNA fingerprint generation using experimentally collected emissions from like-model CC2420 ZigBee devices operating at 2.4 GHz. RF-DNA fingerprints from 7 authorized devices are used for Multiple Discriminant Analysis (MDA) training and authorized device classification performance assessed, i.e. answering: "Is the device 1 of M authorized devices?" Additional devices are introduced as impersonating rogue devices attempting to gain unauthorized network access by presenting false bit-level credentials for one of the M authorized devices. Granting or rejecting rogue network access is addressed using a claimed identity verification process, i.e. answering: "Does the device’s current RF-DNA match its claimed bit-level identity?" For authorized devices, arbitrary classification and verification benchmarks of %C > 90% and %V > 90% are achieved at SNR ≈ 10.0 dB using a test statistic based on assumed Multivariate Gaussian (MVG) likelihood values. Overall, rogue device rejection capability is promising using the same verification test statistic, with %V < 10% (90% or better rejection) achieved for 11 of 14 rogue trials. One case yielded near 85% rogue verification (unauthorized access) and security cannot be a matter of chance—work continues to find a more robust test statistic and improve the proposed process.

Clay Dubendorfer
Air Force Institute of Technology, USA
Limitations of Quorum-Based Rendezvous and Key Establishment Schemes Against Sophisticated Jamming Attacks

1569612653

Recently Quorum-based frequency hopping schemes have been studied to increase the rendezvous probability and to provide fast key establishment techniques in RF communication under jamming attacks. However, these schemes are still vulnerable to the sophisticated jamming attack in which a jammer has the capability of listening and jamming multiple frequencies. In this paper, we present the sophisticated jamming attack and particularly evaluate its effectiveness on Frequency Quorum-based Rendezvous (FQR) schemes [6]. The sophisticated jammer can find the sender's quorum set within the second frame (i.e., 2k time slots) in FQR system when it has the capability of listening on k frequencies from the minimal (N; k) difference sets. The jammer can completely jam the sender after 2k time slots using an average of \( \frac{k+1/2}{k} \) and a maximum of k frequencies. To remedy this jamming problem, we revisit the role-based rendezvous scheme and extend it to Role-based Frequency Rendezvous (RFR) scheme. Our simulation results demonstrate that the rendezvous probability of FQR system under the sophisticated jamming attack is dramatically decreased as the number of available channel N increases (e.g., 20% for N = 100 in k2 time slots). On the other hand, the rendezvous probability of our RFR scheme is almost steady for all available frequencies N (e.g., 95% for N = 100). Therefore, RFR scheme can be an effective, efficient and robust rendezvous and key establishment scheme against sophisticated jamming attacks.

Young-Hyun Oh
North Carolina State University, USA

Securing Wireless Network Coding Against Pollution Attack at the Physical Layer

1569612943

We take a physical layer perspective in detecting the falsely injected vector (pollution attack) and removing it from the polluted packet to restore the true coded packet in wireless network coding system. The proposed scheme builds on the maximum likelihood detection principle which is optimal in the sense of minimizing the probability of detection error. It discards only the faulty information and keeps the true coded packet, thereby making the retransmission of new coded packets unnecessary. This allows uninterrupted communication even under the attack. The proposed scheme is shown to provide a significant throughput and reliability gain over the current cryptographic solutions.

Sang Kim
Iowa State University, USA
Information-Guided Randomization for Wireless Physical Layer Secure Transmission

1569612525

Security capacity improvement is always the implementation goal of physical layer security, which can be achieved by deliberate randomization based on differentia and uniqueness of wireless channels through signal processing method. An information-guided randomization secure transmission scheme is proposed combined with a spatial modulation system in which information can be carried by receiving antennas index but actually by channel differentia. Randomization is generated along with channel modulation procedure realized by corresponding preprocessing to transmitting signals. We provide three approaches for designing preprocessing weights under different constraint conditions. The former two can only be used when the number of receiving antennas is less than transmitting and have a tradeoff with varying degrees between receiving performance and security. The third one then relaxes the limits via generalized spatial modulation and can be used for arbitrary antennas configuration but with a receiving performance compromise. Lastly, results of performance analysis and numerical evaluation show that the proposed secure scheme is effective to prohibit the eavesdropper from intercepting information.

Qiaolong Li
National Digital Switch System Engineering Technology Research Center, P.R. China

A Forensic Hypervisor for Process Tracking and Exploit Discovery

1569612695

Complete forensic reconstruction of a processes memory and interaction history is impractical in modern computing environments because the volume of data processed on a typical server is immense. In addition, the system under observation cannot be trusted to record accurate results after it is infected with a virus. When an anomalous event is detected, there is subsequently no way to attest which, if any, processes were related to the initial event after time has passed, hampering recovery or data verification efforts. However, correlation between processes would provide clues in the search for zero-day attacks during incident investigation and restoration of a server. To address these problems, we describe a novel micro-hypervisor design that enables coarse-grained process tracking using custom forensic introspection techniques. This paper presents a detailed analysis of the steps necessary to perform forensic analysis on the Intel platform and our results of the performance impact caused by the inclusion of the forensic code.

Stephen Kuhn
Dartmouth College, USA
Security Key Management Session

Robust Wireless Channel Based Secret Key Extraction

1569580621

Prior work in channel based key extraction has assumed that the adversary has negligible knowledge/control of the wireless channel. Recent analysis, however, has shown that this assumption is not necessarily valid. Gaining a better understanding of the implications of this assumption is crucial as the wireless channel plays a critical role in the security of this type of key extraction system. In this paper, we discuss why we feel this assumption oversimplifies the problem and present a formal adversary model which takes into account an adversary's knowledge/control of the wireless channel. We present impossibility results learned from our formal model and discuss why previously proposed systems fail to defend against our adversary. We propose the first secret key extraction system which thwarts this adversary and give a generic implementation of our system.

Michael Clark
Air Force Research Laboratory, USA

Differential Power Analysis Using Wavelet Decomposition

1569591377

Differential Power Analysis (DPA) has been successfully used against cryptographic hardware to extract the secret key in a non-invasive manner. However, the great success of DPA requires a large number of traces to overcome system noise or countermeasures, which equates to increased processing times and computing hardware requirements. We investigate wavelet decomposition of a DPA trace data set as a means to reducing the number of traces. By decomposing the signal into various wavelet coefficient levels, we identify those that reduce DPA performance and mitigate their impact. We achieve an 11.53% increase in correct key correlation value vs traditional DPA and exceed traditional DPA with as little as 30 traces. This method significantly reduces the number of traces needed to overcome system noise and countermeasures which introduce random operations.

Hiren Patel
Air Force Institute of Technology, USA

ARQ-Based Key Scheduling Algorithm over Correlated Erasure Channels

1569600187

This paper focuses on the problem of sharing secret keys using the Automatic Repeat reQuest (ARQ) protocol. We first model the forward and feedback channels as erasure channels for both legitimate receiver (Bob) and an eavesdropper (Eve). In prior works, wiretap channel is modeled as statistically independent packet erasure channels for Bob and Eve. In this paper, we go beyond the state-of-the-art by addressing correlated erasure events across the wiretap channel. The created randomness is shared between two legitimate parties through ARQ transmission that will be mapped into a destination set using the first order digital filter with feedback. Then, we characterize Eve's information loss about this shared destination set, due to inevitable transmission errors that will be manipulated by privacy amplification to generate a series of secret keys about which Eve's knowledge remains negligible. We define two metrics to measure secrecy enhancement: outage probability and secret key rate. The resulting secrecy improvement is presented as a function of the correlation coefficients and the erasure probabilities for both channels. It is shown that secrecy improvement is achievable even when Eve has a better channel than the legitimate receiver, and her channel condition is unknown.

Yahya Khiabani
Louisiana State University, USA
The Glowworm Hash: Increased Speed and Security for BBC Unkeyed Jam Resistance

1569611227

Jam resistance for omnidirectional wireless networks is an important problem. There is currently only one system for achieving it without any shared secret: BBC coding. This algorithm requires the use of a hash function that is fast and secure, but "secure" in a different sense than for standard cryptographic hashes.

Last year at MILCOM, the Inchworm hash was presented, which is 300 times faster than SHA-1 for this application, and had no security flaws yet known. A variant of it, Inchworm-S, was also presented, that was intended to be more secure.

We present an academic break of both Inchworm and Inchworm-S, and a practical break of the former. The advantage to the attacker is very small, but it is definitely nonzero.

We also present a new hash algorithm: Glowworm. Glowworm is simpler than Inchworm, and the same speed as Inchworm-S, while being more secure. We mathematically prove that it is immune to the theoretical attack we show for Inchworm and Inchworm-S. We also show empirically that it is immune to our empirical attack on Inchworm, even when the attack algorithm is run for much longer periods. In fact, we show that for our best attack software, it is indistinguishable from SHA-1, MD5, and all five SHA-3 candidates. We also mathematically prove that it has avalanche properties that prevent many other type of internal-state collisions and related attacks.

We give an optimized, portable, C implementation of Glowworm. For incremental hashes as used in BBC codes, it can hash a string of arbitrary length in 11 clock cycles. That is not 11 cycles per bit or 11 cycles per byte. That is 11 cycles to hash the entire string, given that the current string being hashed differs from the last in only an addition or deletion of its last bit.

Finally, we discuss our implementation of Glowworm in a Field Programmable Gate Array (FPGA), where it runs in just one clock cycle per string, using modest amounts of resources.

Leemon Baird
US Air Force Academy, USA

Hamming Masks: Toward Defending Constrained Networked Systems

1569612543

The ability of intrusion detection systems to identify anomalous behavior successfully has lagged behind their ability to recognize activity based on signatures. Anomaly detection techniques for enterprises typically use statistical traffic models to accommodate varying network traffic profiles and limit the volume of false alerts. We offer a set of characteristics to identify constrained networked systems in which we hypothesize that anomaly detection techniques are well suited and useful. We offer a specific, concrete approach, Hamming Masks, for identifying expected behavior in a constrained networked system and recognizing previously unknown behavior. We demonstrate the applicability of Hamming Masks for two different data sets and find that the distinctions between the enterprise data set and the constrained networked system data set are large.

Andrew Jurik
Johns Hopkins University Applied Physics Laboratory, USA
Lightweight Key Management in Distributed Multi-Channel Cognitive Radio Networks

1569614071

In this paper, lightweight identity-based and certificate-based distributed key management algorithms are proposed for self-organized multi-channel cognitive radio networks. Both key management schemes use threshold secret sharing. In identity-based scheme, after system initialization, each CR sends its channel key request to distributed private key generators. Then, it can construct the channel key based on its received shares. In certificate-based scheme channel certificate can be constructed by receiving certificate authority shares at the CR. Simulation results show that the proposed identity-based and certificate-based schemes significantly increase the average battery life of CRs and decrease the traffic overhead in multi-channel cognitive radio networks.

Behzad Kasiri
University of Manitoba, Canada
Detection of Global Metamorphic Malware Variants Using Control and Data Flow Analysis

1569574345
11/1/2012 9:30

Current malware detection and classification tools fail to adequately address variants that are generated automatically using a new breed of polymorphic and metamorphic transformation engines, which can produce variants that bear no resemblance to one another. Present approaches partially address this problem by employing syntactic signatures that mimic the underlying control structures such as call- and flow-graphs. These techniques, however, are easily defeated using new program diversification techniques. This hampers our ability to defend against zero day attacks perpetrated by such auto "replicating", rapidly spreading malware variants. In this paper, we present a new form of abstract malware signature generation that is based on extracting a semantic summary of the malware code, which is immune to most polymorphic and metamorphic transformations, and present results of our preliminary evaluation of the same.

Hira Agrawal
Applied Communication Sciences, USA

CD-PHY: Physical Layer Security in Wireless Networks through Constellation Diversity

1569598443

A common approach for introducing security at the physical layer is to rely on the channel variations of the wireless environment. This type of approach is not always suitable for wireless networks where the channel remains static for most of the network lifetime. For these scenarios, a channel independent physical layer security measure is more appropriate which will rely on a secret known to the sender and the receiver but not to the eavesdropper. In this paper, we propose CD-PHY, a physical layer security technique that exploits the constellation diversity of wireless networks which is independent of the channel variations. The sender and the receiver use a custom bit sequence to constellation symbol mapping to secure the physical layer communication which is not known a priori to the eavesdropper. Through theoretical modeling and experimental simulation, we show that this information theoretic construct can achieve Shannon secrecy and any brute force attack from the eavesdropper incurs high overhead and has minuscule probability of success. Our results also show that the high bit error rate also makes decoding practically infeasible for the eavesdropper, thus securing the communication between the sender and receiver.

Mohammad Husain
(University at Buffalo, USA

Adaptive Algorithms for Detecting Critical Links and Nodes in Dynamic Networks

1569598521

The assessment of network vulnerability is of great importance in the presence of unexpected disruptive events or adversarial attacks targeting on critical network links and nodes. However, it is extremely challenging to seek and safeguard against most destructive scenarios in dynamic networks where changes to their topologies are frequently introduced. In this paper, we propose CLA and CNA algorithms, to adaptively detect critical links and nodes in a dynamic network whose removals maximally destroy the network's functions, without recomputing from scratch. The effectiveness of our solutions is validated on various types of networks with different topology structures.

Yilin Shen
University of Florida, USA
Distributed Detection in Wireless Sensor Networks in the Presence of Misbehaving Nodes

Erfan Soltanmohammadi
Louisiana State University, USA

Using Covert Timing Channels for Attack Detection in MANETs

Jonathan Edwards
Carleton University, Canada

The Trust Engineering Framework: Architecting Native Security to Defend Against the Next Generation Threats

Bassam Farroha
US Department of Defense, USA
Performance Analysis of Wireless Intruder Geolocation in Campus Wireless Networks

Wireless intruder geolocation techniques using received signal strength (RSS) measurements from an array of sensors are very attractive for campus wireless network security because of their low cost implementation and simplicity. Both precision in RSS measurements and the relative geometry between RF sensors and the wireless intruder can affect the geolocation accuracy. This paper presents a comparative performance analysis of three RSS-based geolocation algorithms for non-cooperative wireless intruders in terms of their root mean square errors in wireless campus networks. A comparison study is established in a RF sensor grid and circular sensor geometries to fit general campus topology. Geolocation algorithm accuracy is examined for these particular geometric configurations of RF sensors with respect to various wireless intruder locations in and around a campus area. The results show that certain geolocation algorithms perform much better than others when wireless intruders are inside a campus wireless network, whereas the performance of the same geolocation algorithms is turned around when wireless intruders are outside a campus wireless network. As a result, a high accuracy solution to wireless intruder geolocation in campus wireless networks is discovered and proposed. MATLAB-based numerical simulations were used to evaluate the performance of these algorithms for various scenarios and parameters.

Shanzeng Guo
DRDC Ottawa, Canada
Distributed Compromised Nodes Detection Scheme at First Stage for SurvSec Security Architecture

1569612165

SurvSec is a novel security architecture for reliable network recovery from base station BS failure of surveillance Wireless Sensor Network WSN in hostile environment. Compromised nodes detection is a very important security mechanism in surveillance WSN to detect compromised nodes before they destroy the security of the WSN. Node compromise attack is a multi-stage attack which consists of three stages: physically capturing and compromising sensor nodes; redeploying the compromised nodes back to network and compromised nodes rejoining the network. Only two protocols detect compromised nodes at first stage. The first protocol can be easily broken by targeting couple of nodes at the same time and the second protocol has high overheads and it is based on the distribution of one key list for all nodes which is not secure if one node is compromised. In this paper, we proposed a new compromised nodes detection algorithm that detects compromised nodes at first stage for SurvSec security architecture. Our proposed scheme is based on four algorithms. First algorithm provides the network with key management. Second algorithm provides the network with secure localization. Third algorithm provides the network with secure clustering. Fourth algorithm builds overlapped groups from clusters. Each cluster has a security manager SM and backup security manager BKSM to manage security issues. From the locations of nodes in the cluster, the nodes can form a group by sending and receiving from their right and left neighbours in the cluster. Each group forms overlapped group with its neighbour groups. The groups resemble interconnected rings in a chain and if attackers capture one group in the chain, the chain will be cut and its overlapped groups will discover the compromised group. Each node in the cluster sends an encrypted "Hello" message to its neighbours in the cluster every 15 seconds. If a node does not respond to the "Hello" message, this means it is compromised and its neighbours will send to the SM that the node is compromised and if the SM is compromised, its neighbours will send to the BKSM that the SM is compromised then to BS. Our protocol is designed to be resistant against large number of compromised nodes by collaborative work of attackers. Extensive simulation results are given to demonstrate the high detection rate of the proposed scheme besides the low overheads with high security level for the protocol.

Mohamed Megahed
University of Ottawa, Egypt

Detecting Communication Anomalies in Tactical Networks via Graph Learning

1569612167

A widely practiced approach for detecting suspicious communications in a network is to formulate the problem as statistical anomaly detection. However, communication patterns, especially, those observed in mission-oriented tactical networks are highly variable and have a much richer structure than incorporated by existing anomaly detection methods. For instance, the legitimacy of a communication may depend on who sends the message to who and when. Existing anomaly detection methods insensitively aggregate the data and thereby lose critical contextual information about the structure of communication and as a consequence, they either fail to detect suspicious communication or produce excessive amount of false positives. We have developed an extended graph based anomaly detection method that allows us to incorporate the context and rich structure of communication in a mission-oriented tactical network to model and detect suspicious patterns. We use a vector-weighted multidigraph representation to model communications in a network and use a given data to learn the graph, i.e., to determine the nodes, the edges, and their statistical attributes corresponding to normal communication. We then use deviations from the normal graph attributes to detect suspicious communications. We have applied to the proposed approach to detect suspicious communication in a MANET comprising of USRP2 radio nodes and successfully demonstrated the approach in a TRL-6 demonstration at Fort Dix. While our proposed approach is very general, only a part of it applies to the MANET under consideration and we used it to successfully detect various types of illegal messages, congestion, and the DDoS attack.

Akshay Vashist
Applied Communication Sciences, USA
Clustering of Snort Alerts to Identify Patterns and Reduce Analyst Workload

1569612329

Pattern-matching intrusion detection system (IDS) tools such as Snort are known to generate an extremely large number of alerts. To address this problem, we present a greedy aggregation algorithm that efficiently reduces multiple alerts by grouping the raw output of IDS tools into 'meta-alerts' that contain common information. In contrast to the current thrust of alert aggregation efforts, our approach does not require developing elaborate semantic structures for capturing information, nor creating and maintaining an external database containing information on attack vectors, network topologies, and cause-and-effect relationships. We apply our method to 30 days of Snort alerts, grouped by hour, and observe that we can reduce the number of analyst-visible Snort alerts by up to 99.5%, with an average reduction of approximately 83.2%.

Richard Harang
ICF International, USA

An Efficient Common Substrings Algorithm for On-the-Fly Behavior-Based Malware Detection and Analysis

1569612723

It is well known that malware (worms, botnets, etc...) thrive on communication systems. The process of detecting and analyzing malware is very latent and not well-suited for real-time application, which is critical especially for propagating malware. For this reason, recent methods identify similarities among malware dynamic trace logs to extract malicious behavior snippets. These snippets can then be tagged by a human analyst and be used to identify malware on-the-fly. A major problem with these methods is that they require large processing resources. This is especially due to the large amount of malware released each year (upwards of 17 million new instances in 2011). In this paper, we present an efficient algorithm for identifying common substrings in dynamic trace events of malware collections. The algorithm finds common substrings between malware pairs in theoretical linear time by using parallel processing. The algorithm is implemented in the CUDA and results show a performance increase of up to 8 times compared to previous implementations.

Jaime Acosta
US Army Research Laboratory, USA

A Case for Trusted Sensors: Encryptors with Deep Packet Inspection Capabilities

1569607731

In today's classified networks, the health and availability of the network are crucial to support the mission needs of US Government. Inclusion of sensing appliances into these sensitive networks has been a priority for several years to achieve the situational awareness of the network. The purpose of this paper is to see how an encryptor at the network boundaries with Deep Packet Inspection sensing can aid and enhance in understanding the network's health. We will show that these encryptors and their unique place within the network architecture provide valuable insight in the present operation of the network. General Dynamics has investigated advantages and methods for high speed content monitoring within future enhanced sensing encryptors.

David King
General Dynamics, USA
Security Protection - 3 Session

Evaluating Network Cyber Resiliency Methods using Cyber Threat, Vulnerability and Defense Modeling and Simulation

1569565061

This paper describes a Cyber Cyber Threat, Vulnerability and Defense Modeling and Simulation tool kit used for evaluation of networks to improve cyber resiliency. This capability was used to help increase the resiliency of networks at various stages of their lifecycle, from initial design and architecture through the operation of deployed systems and networks.

Resiliency of computer systems and networks to cyber threats is facilitated by the modeling of agile and resilient defenses versus threats and running multiple simulations evaluated against resiliency metrics. This helps network designers, cyber analysis and SOC personnel to perform trades using what-if scenarios to select resiliency capabilities and optimally design and configure cyber resiliency capabilities for their networks.

Raytheon Corporation, USA

On the Use of Distributed Relays to Increase Base Station Anonymity in Wireless Sensor Networks

1569569757

In recent years, Wireless Sensor Networks (WSNs) have become valuable assets to both the commercial and military communities with applications ranging from industrial control on a factory floor to reconnaissance of a hostile border. In both applications, the sensors act as data sources and forward information to a central sink or base station (BS). The unique role of the BS makes it a natural target for an adversary that desires to achieve the most impactful attack possible against a WSN with the least amount of effort. An adversary may employ traffic analysis techniques to identify the BS based on network traffic flow even when the WSN implements conventional security mechanisms. This motivates a significant need for improved BS anonymity to protect the identity, role, and location of the BS. In this paper we propose a strategy to increase BS anonymity in a WSN by utilizing multiple relays at each hop. Each relay retransmits received messages at an increased power level to increase the number of candidate receivers included in the adversary's analysis. We examine the effect of the distributed relay technique on improving BS anonymity using evidence theory and demonstrate the effectiveness of this approach through simulation.

Jon Ward
The Johns Hopkins University, USA

Guest-Transparent Instruction Authentication for Self-Patching Kernels

1569577109
10/31/2012 15:10

Kernel rootkits have the ability to create and execute malicious code with kernel-level privileges. Security mechanisms have been created to prevent kernel rootkit implantation by relocating the vulnerable physical system to a guest virtual machine and enforcing a W XOR KX memory access control policy from the host virtual machine monitor. Such systems must also be able to identify and authorize the introduction of known good kernel code. Previous works use digital signatures to verify the integrity of kernel code at load-time. The signature creation and verification procedure depends on immutable kernel code. However, many modern kernels are "self-modifying;" they may dynamically overwrite executable instructions in memory after load-time. Such dynamic patching may occur for a variety of reason including: CPU optimizations, multiprocessor compatibility adjustments, and advanced debugging. The previous signature verification procedure cannot handle such modifications. We describe the design and implementation of a procedure that verifies the
integrity of each modified instruction as it is introduced into the guest kernel. Our experiments with a self-modifying Linux guest kernel show that our system can correctly detect and verify all valid instruction modifications and reject all invalid ones. In most cases our instruction verification procedure incurs only nominal performance impact.

Dannie Stanley
Purdue University, USA

**Lightweight One-Time Signature for Multicast Authentication**

1569612683

Authentication is a security requirement with high priority in many multicast applications. One-Time Signature (OTS) is a promising solution to the multicast authentication problem. However, it often suffers from large signature sizes and frequent distributions of the public keys. In this paper, we propose a lightweight OTS scheme to combat these drawbacks. Our approach integrates the signature amortization technique and one-way hash chains, which markedly reduce the average communication overhead and relax the key renewal requirements. We also introduce a partial key renewal mechanism to provide a convenient means of renewing key pairs. In addition, our scheme is highly secure against signature forge and is resistant to packet losses. Numerical results show that our scheme achieves better performance than a former scheme under DoS attacks.

Pan Deng
Colorado State University, USA

**An Efficient Spectral Bound for Link Vulnerability Assessment in Large-scale Networks**

1569612951

Simultaneous attacks can cause devastating damage, breaking down communication networks into small fragments. To mitigate the risk and develop proactive responses, it is essential to assess the robustness of network in the worst-case scenarios. In this paper, we propose a novel lower bound on the number of removed links to incur a certain level of disruption in terms of pairwise connectivity. Our lower bound explores the latent structural information in the network spectrum, the set of eigenvalues of the Laplacian matrix, to provide guarantees on the robustness of the network against intentional attacks. Such guarantees often cannot be found in heuristic methods for identifying critical infrastructures. For the first time, the attack-resistant proofs of large scale communication networks against link attacks are presented.

Thang Dinh
University of Florida, USA
Software Updates as a Security Metric Passive Identification of Update Trends and Effect on Machine Infection

1569613713

Botnets have become a vital part of underground economy and botherders are actively looking for new recruits to join their bot army. A lapse by an end user or an administrator in terms of not updating their software enables the botherder to achieve this objective. In this paper we will investigate the phenomenon of a machine infection from the perspective of a user update behavior. We also present type of attacks that are launched by hackers to compromise machine and the vulnerabilities that lead to such attacks as a result of update behavior. We will also characterize the user update behavior on the test network of study. Finally we will compare the update behavior of machines that were infected with the ones that were not infected. The objective of this investigation is to see if update behavior could be used as an effective security metric, our trends show that there is a very clear correlation between the machines that were infected and the machines that were not updated.

Moazzam Khan
Georgia Institute of Technology, USA

Identity-Based Internet Protocol Networking

1569565313
10/31/2012 14:30

The Identity-Based Internet Protocol (IBIP) Networking project is experimenting with a new enterprise oriented network architecture using standard IP version 6 protocol to encode user and host identity (ID) information into the IP address. Our current implementation plan uses credentials from the Common Access Card (CAC) to establish a 40-bit user ID and credentials stored on the computer’s Trusted Platform Module (TPM) to establish a 40-bit host ID. The remaining part of the IP address can be a standard (/48) network prefix or support a (/32) prefix and a 16-bit group tag. A registration process (built on top of an 802.1x security framework) then occurs between the host and a registration server (which is currently an enhanced RADIUS server). The IBIP registration server then validates the credentials and automatically configures the edge router, fronting the host, with appropriate access privileges so that no IP address spoofing (or impersonation) is permitted. Access control policies are performed on a per packet basis and continue to monitor the admission of each packet after the initial authentication and admission process. Ingress and egress filters can be implemented and access policies based on a combination of host, user, or group values are possible. Hosts that are client machines do not have their IP addresses advertised across the network - basically making them unreachable or hidden from reconnaissance initiated by other clients. Servers have their IP addresses advertised in the normal sense using standard routing protocols on commercially available routers. A unique IPv6 extension header was conceived to permit servers to return traffic to hidden clients. This approach will also provide support for approved peer-to-peer applications which may have hidden clients at both ends (voice-over-IP phones, for example). All infrastructure devices (routers, switches, DNS, DHCP, and other designated servers) are also not directly accessible by end user machines. For servers, the user ID is replaced with a service ID which can be used to identify and enforce policies on what the server is permitted to do. For example, if the server policy is to function only as a web server and not allow other applications onto the network, access control implemented on the edge router in front of that server would only permit web transactions from entering the network. Attempts to use other non-approved applications such as telnet can be explicitly blocked or monitored and reported. These access controls are created and deployed from the IBIP registration server without human intervention, reducing the likelihood of human error while simplifying configuration and training. All policy violations are also reported via syslog messaging (using existing infrastructure devices) which enhances situational awareness. In summary, this network architecture hides a majority of the machines and infrastructure devices from unapproved access, enforces strong ubiquitous authentication for both host and user, enables enforceable authorization policies, simplifies the configuration of routers, and provides improved situational awareness.

Shu Nakamoto
MITRE Corporation, USA
Unexpected occurrences of large-area cascading failures due to small disturbances in worldwide electricity grids serve as evidence of their intrinsic instability. As the grid is the most fundamental critical infrastructure in any modern society, detection and mitigation of such cascading failures due to accidental failures or malicious attacks are of vital importance to both civilian and military applications. However, due to the unique physical properties of electricity, such as its travel speed, systems must be able to react within a fraction of a second in order to detect and prevent occurrences of cascading failures. In this paper, by modeling the grid as a cyber-physical system, we propose a decentralized, hierarchical framework to develop and implement a wide-area actionable system, capable of detecting and mitigating potential cascading failures. The states of the grid and physical constraints are modeled as manifolds, and evolution of the grid becomes a path on the manifold. By decomposing the grid into resilience zones with minimal power flow between them, we utilize precomputed scenarios in each resilience zone to develop a parametrized model. During deployment, online phasor measurements will be used to estimate the stability within each zone and interactions among them. The detection of cascading failures will be based on the detection of cascading failing paths among the K hop trees built for each zone. We illustrate the effectiveness of the proposed approach using the 2003 Italy blackout scenarios, and we discuss practical requirements in order to deploy such a system.

Josef Allen
Oak Ridge National Laboratory, USA
Supervisory Command and Data Acquisition (SCADA) System Cyber Security Analysis Using a Live, Virtual, and Constructive (LVC) Testbed

1569612717

Modern critical infrastructure systems are built on a hodgepodge of complex, interconnected information systems for control and management. For electrical power distribution, the critical infrastructure includes the physical system; comprised of power generation and power distribution capability. The control of the physical system is accomplished via Supervisory Command and Data Acquisition (SCADA) system. The SCADA systems employ legacy systems along with many of the same information system devices as traditional business information systems. SCADA system networks, just as business information systems, are connected to external networks including the Internet. Thus SCADA systems are vulnerable to the same classes of threats as other networked computer system in addition to threats associated with their legacy systems. Many of these systems have been put in place for decades and often have an unknown security posture. Cyber security analysis of the systems remains a significant challenge. Traditional techniques such as red-teaming, vulnerability assessments, and penetration testing are often unsatisfactory and limited in scope because power plants do not want to risk taking the system off-line or degrading or damaging the expensive equipment. The consequence is that the effects of a cyber-attack on a SCADA system are often unknown.

In order to provide greater SCADA system security posture insight to service providers and administrators, security experts must perform security analysis. To overcome the problems with security analysis using either an exclusive hardware SCADA testbed or a simulation of a SCADA system, Sandia National Labs has developed a cyber-security analysis capability using physical hardware, extensive virtualization and emulated machines, and simulation to answer complex system questions about SCADA systems. In this paper we will discuss the methodology, several use-cases that were executed during the course of the study which leverage the methodology, the types of cyber-attacks that can be assessed and the class of questions security professionals can now ask and answer about cyber-attacks against SCADA systems.

Brian Van Leeuwen
Sandia National Laboratories, USA

Cyber Analysis System Toolkit A High-Fidelity, Virtual Cyber Test-Bed for Network Modeling and Experimentation

1569612823

There is a growing need to defend networked information systems from cyber-attacks. Cyber security analysis tools are key enablers in analyzing the attacks and developing defenses. In this paper, we present the Cyber Analysis Systems Tool-Kit (CAST), a high-fidelity, scalable, virtual test-bed for cyber systems modeling, experimentation and analysis. At the heart of CAST is the Common Open Research Emulator (CORE). CORE uses network emulation techniques that provide a high degree of modeling fidelity while maintaining network scalability. We use CAST to develop network emulations of a representative security model called Virtual Secure Enclaves (VSE). We evaluate different security model implementation options (including defense-in-depth concepts) for this illustrative example. The design options include combinations of firewalls and TLS VPNs, firewalls and IPSec VPNs, and defense-in-depth concepts that use multiple layers of these combinations. We use these models to analyze and quantify network performance metrics such as latency and throughput. For example, by adding two layers of TLS and IPSec VPNs, we see that latencies increase by ~400 msec for representative video traffic versus a network with no security. We have also investigated latencies for a variety of traffic types. Our main contribution is a real-time, high-fidelity model of a representative 100-node operational network with embedded security features.

Balaguruna Chidambaram
The Boeing Company, USA
System Security Session

**Chaining for Securing Data Provenance in Distributed Information Networks**

1569590969

Entities in an information communication network may use various types of collaborative networking for sharing information such as documents, sensing reports, datasets, etc. The derivation history (i.e., the provenance) of the information plays a very important role in such a networking environment. For example, provenance can be used for information trustworthiness assessment, copyright clearance, data reconciliation, and data replication. While substantial research efforts have focused on these usages of provenance, very limited work has focused on the security issues of the provenance, which is the prerequisite of any provenance-based information analysis systems. In this paper, we explore the security properties of provenance meta-data compared to other general user data in a distributed network environment. We introduce a "chain-structure" provenance scheme to provide security assurance for the provenance meta-data in three dimensions - confidentiality, integrity and availability. Our scheme outperforms the previously proposed "onion-structure" provenance security scheme in terms of the flexibility, protection capability as well as computational overhead.

Xinlei (Oscar) Wang
University of California, Davis, USA

**Architecting Dynamic Cyber Defense for a Secure Multi_Tenant Environment**

1569600271

This paper addresses the area of Architecting Dynamic Cyber Defense for a Secure Multi_Tenant Environment

Bassam Farroha
US Department of Defense, USA

**The Xenon Separation VMM: Secure Virtualization Infrastructure for Military Clouds**

1569600337

In conventional military computing, security separation is provided by cryptography, for data in motion and data at rest. Security separation for data under computation is provided by separate hardware. Cloud computing shares hardware for all data under computation, so a new approach to security separation is needed for military clouds. Cryptographic separation of data under computation is not practical with current technology, so the separation must be accomplished by software, i.e. the virtualization infrastructure. The strongest known means of software separation is the separation kernel. Separation kernels are special virtual machine monitors (VMMs) that are small enough and simple enough to be mathematically verified. Unfortunately, strict separation kernels cannot virtualize the complex modern commodity hardware and guest virtual machine (VM) operating systems that are essential to cloud computing. The best alternative to a strict separation kernel is a separation VMM. A separation VMM relaxes the strict size and simplicity goals of a separation kernel just far enough to be able to support commodity hardware and guest operating systems. Because they address all of the features of commodity hardware, separation VMMs are too large for formal mathematical verification. However, separation VMMs are small enough and simple enough to be completely specified by semi-formal means, i.e. they are smaller and simpler than conventional VMMs. A separation VMM has a complete systematic assurance argument that it isolates guest VMs from each other and strongly protects itself from tampering. A separation VMM provides the strongest separation of cloud VMs that is consistent with virtualizing complex commodity operating systems, on shared complex commodity hardware.

John McDermott
Naval Research Laboratory, USA
A High-assurance, Virtual Guard Architecture

1569600599

Although one senior security professional has emphasized that "it is unconscionable to use overly weak components" in a multilevel security (MLS) context, the majority of current transfer guards do exactly that. Basic guard technology is well-developed and has a long history, but most guards are built on low-assurance systems vulnerable to software subversion, and the lack of assurance limits the range of transfers. This paper describes a virtual guard architecture that leverages mature MLS technology previously certified and deployed across domains from TS/SCI to Unclassified. The architecture permits a single guard system to simultaneously and securely support many different transfer functions between many different domain pairs. Not only does this architecture substantially address software subversion, support adaptable information transfer policies, and have the potential to dramatically reduce (re)certification effort, the virtualized guard execution environment also promises to significantly enhance efficient and scalable use of resources.

Mark Heckman
Aesec Global Services, USA

MUSHI: Toward Multiple Level Security Cloud with Strong Hardware Level Isolation

1569606491

Multiple Level Security (MLS) has always been a center of focus since the usage of computers in military and intelligence systems. Extensive studies have been done on how to utilize virtualization technologies to provide multiple level secured execution in cloud, yet the general assumption is that all components in the cloud service provider are trusted. With the advanced persistent threats currently faced by the military and intelligence community, it is unrealistic to assume complex information systems can remain trustworthy all the time. In this work, we present MUltiple level Security cloud with strong Hardware level Isolation (MUSHI), a novel framework that can provide hardware level isolation and protection to individual guest virtual machine (VM) execution. With MUSHI, user can maintain confidentiality and integrity of her VM in a multicore environment even in the presence of malicious attacks from both within and outside the cloud infrastructure.

Ning Zhang
Virginia Tech, USA

System Security

Polite: A Policy Framework for Building Managed Mobile Apps

1569610777

The proliferation of smart phones inside enterprises and the number of enterprise apps (applications) available for various smart phone platforms has been increasing. This trend is expected to continue as smart phones tend to become the device of choice to access both enterprise and personal data. Making enterprise sensitive data accessible on smart phones requires that adequate protection mechanisms be available on these devices to ensure that sensitive data is not compromised due to various reasons, such as employees losing phones to malicious apps (installed by the user) running on the phones. Most of the existing solutions either provide device level control or have an external agent monitoring the application's behavior, and has numerous limitations. In this paper we propose a framework, \textit{Polite}, to build enterprise mobile apps that can be managed at run-time, which is less intrusive to the end user while providing stronger security guarantees to the enterprise. We describe several critical scenarios where controlling the run time behavior of apps on the phone is essential and how our architecture can provide security guarantees that are not possible with existing solutions. Performance results from the implementation indicate that our framework induces a minimal overhead of only $6\%$ that may be acceptable for most enterprise mobile apps.

Udayan Kumar
University of Florida, USA