

Paul Royal

Poster Title

Ether: Malware Analysis via Hardware Virtualization Extensions

Poster Summary

Malware has become the centerpiece of many security threats on the Internet. Malware analysis is important for information security practitioners because it is the basis for understanding the intentions of malicious programs. Current malware analysis approaches reside in the guest OS or emulate part of its underlying hardware, which leaves them vulnerable to detection and attack by modern malware.

To combat this problem, we present an alternative, external approach to malware analysis. The resulting malware analysis tool, called Ether, operates outside of the guest through the use of hardware virtualization extensions such as Intel VT. Experiments with obfuscation tools used to create the vast majority of modern malware show that Ether is an effective, transparent tool for malware analysis.

Bio

Paul Royal is a Research Scientist at the Georgia Institute of Technology, where he engages in collaborative research on various facets of the online criminal ecosystem. Prior to Georgia Tech, Royal served as Principal Researcher at Purewire, Inc, where he worked with other researchers to identify threats and design methods that enhanced the company's web security service. Royal is a frequent press resource on security issues and has been quoted in USA Today, The Washington Post, Forbes, and others.

Notes:

Sam Burnett

Title:

Circumventing Censorship with Collage

Abstract:

Oppressive regimes and even democratic governments restrict Internet access. Existing anti-censorship systems often require users to connect through proxies, but these systems are relatively easy for a censor to discover and block. We explore a possible next step in the censorship arms race: rather than relying on a single system or set of proxies to circumvent censorship firewalls, we use the vast deployment of sites that host user-generated content to breach these firewalls. We have developed Collage, which allows users to exchange messages through hidden channels in sites that host user-generated content. To send a message, a user embeds it into cover traffic and posts the content on some site, where receivers retrieve this content. Collage makes it difficult for a censor to monitor or block these messages by exploiting the sheer number of sites where users can exchange messages and the variety of ways that a message can be hidden. We have built a censorship-resistant news reader using Collage that can retrieve content from behind a censorship firewall; we will show Collage's effectiveness with a live demonstration of its complete infrastructure.

Bio:

Sam Burnett is a third year graduate student advised by Professor Nick Feamster in the Network and Telecommunications group. He is generally interested in network security and availability, and has done work on Internet censorship and Web privacy.

Notes:

Hyoonoo (Joon) Kim

Abstract of demo:

This paper proposes a network control system that allows network operators to write network-wide policies as high-level, event-based programs instead of configuring individual low-level network devices. This framework, which we call Resonance, enables a network operator to specify policies for a network as a single, centralized program, thus decoupling the specification of network policy from how that policy is actually implemented in the network. Resonance allows network operators to write fine-grained, network-wide policies that are independent of network topology and can take actions based on events from a variety of network devices (e.g., IDS, vulnerability scanners, etc). Resonance is actually deployed within the KACB building at Georgia Tech for regular use. Client from outside the campus network is able to connect to the Resonance network as well. For this demo, we focus on network access control policies: we show how Resonance can be used to make network access control both simpler and more expressive. Our evaluation of Resonance both in controlled settings and in two campus deployments demonstrates that Resonance is expressive, and that it can operate and scale in operational settings.

Bio:

Hyojoon (Joon) Kim is first year Ph.D. student in Georgia Tech under the supervision of Professor Nick Feamster. He received my B.S in Computer Science from University of Wisconsin - Madison and M.S from Georgia Tech. He is broadly interested in overall network systems and technologies, but currently more focused on *network performance & reliability enhancement, network configuration, network management and security*. He is in search of various ways to enhance current network systems and [OpenFlow](#) happens to be one of them where most of his research is conducted so far. Currently, he is working on *Resonance* which is a novel dynamic network management framework for campus and enterprise networks that uses OpenFlow technology.

Demo:

YES

Poster:

YES

Notes:

Vijay A. Balasubramaniyan, Kelsey Francis

Title:

PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance

Demo: Phone customers have long relied on Caller-ID to assist in identifying the source of an incoming call. Unfortunately, the recent and vast diversification of telephony infrastructure has created significant opportunities to maliciously alter such call source metadata. For example, calls that come from Skype show a Caller-ID of 123456 or 000000. We demonstrate PinDr0p, which uses single-ended audio features such as signal degradations along with machine learning to determine whether or not an incoming call exhibits similar path characteristics to previous calls from the claimed source (call provenance). Prior to the actual demo, we will create a training set of call messages from varied sources (e.g., Skype, Google Voice, Landline, Cell Phone). During the demo, we will randomly pick one of those sources to make a call, and successfully identify the source.

Bio: Vijay is a fifth year Ph.D. student at the College of Computing at Georgia Tech. He completed his undergraduate degree in Computer Science at R.V.C.E., Bangalore, after which he worked at Intel for a year and at Siemens for over 2 years before coming to pursue his Ph.D. His research interests include VoIP, Spam, Identity Management and Network Security and he have been working on VoIP related research both at the GTISC lab and as a summer intern for IBM Research labs, T. J. Watson and the Google Talk team. Vijay's advisor is Prof. Mustaque Ahamad.

Bio: Kelsey is a graduate student in the School of Computer Science and a research scientist at the Georgia Tech Research Institute in the Cyber Technology and Information Security Laboratory. His interests include identity management and mobile infrastructure security. His work at GTRI focuses on applications wherein mandatory access control is a fundamental requirement. Kelsey received his undergraduate degree in Computer Science from Georgia Tech in 2006.

Notes:

Vijay A. Balasubramaniyan, Manojh Ananthakrishnan

Title:

A Crow or a Blackbird?: Using True Social Network and Tweeting Behavior to Detect Malicious Entities in Twitter

Demo: Twitter is a leading micro-blogging service provider that allows users to post limited length messages. With millions of registered users, including news sources such as CNN and shopping sites like Woot that inform customers of latest deal, a user can obtain important information in a timely fashion. However there are a significant number of users who misuse this service by providing wrong or misleading information. Many of these users have characteristics of good users, making the job of a user looking for pertinent information sources much harder. We propose a novel system that looks at the true social network structure and the behavioral characteristics of a user to determine whether he is legitimate or malicious.

Bio: Vijay is a fifth year Ph.D. student at the College of Computing at Georgia Tech. He completed his undergraduate degree in Computer Science at R.V.C.E., Bangalore, after which he worked at Intel for a year and at Siemens for over 2 years before coming to pursue his Ph.D. His research interests include VoIP, Spam, Identity Management and Network Security and he have been working on VoIP related research both at the GTISC lab and as a summer intern for IBM Research labs, T. J. Watson and the Google Talk team. Vijay's advisor is Prof. Mustaque Ahamad.

Bio: Manojh is a 2nd year Masters student in Computer Science. He did his undergraduation from BITS, Pilani, India following which he worked with the Security Technology Group in Cisco Systems, Bangalore for 2 years. His interests include security and embedded operating systems. He has worked on projects related to these areas in Georgia Tech and during his internship with Cisco Systems in the Summer of 2010.

Notes:

Danesh Irani

Title:

"Study of Trend-Stuffing on Twitter through Text Classification". Following is the

Poster Presentation Abstract:

Reaching hundreds of millions of users, major social networks have become important target media for spammers. Although practical techniques such as collaborative filters and behavioral analysis are able to reduce spam, they have an inherent lag (to collect sufficient data on the spammer) that also limits their effectiveness. Through an experimental study of over 1.9 million MySpace profiles, we make a case for analysis of static user profile content, possibly as soon as such profiles are created. We compare several machine learning algorithms in their ability to distinguish spam profiles from legitimate profiles.

Bio:

Danesh Irani is a Ph.D student in the School of Computer Science, College of Computing at Georgia Institute of Technology. He received an Honours Bachelor of Science with distinction from the University of Toronto, Toronto, Canada with a specialization in Software Engineering. His current research is focused on protection of online information systems including preventing malicious information from entering (including spam, phishing) and preventing good information from leaking out of these systems. His experience in the industry with Amazon, Motorola Research, and IBM cover areas in network security, data management, information retrieval, and information integration. He received a best paper award from the APWG eCrime research summit 2008.

Notes:

Italo DaCosta

Poster Presentation

Authentication is an important mechanism for the reliable operation of any Voice over IP (VoIP) infrastructure. Digest authentication has become the most widely adopted VoIP authentication protocol due to its simple properties. However, even this lightweight protocol can have a significant impact on the performance and scalability of a VoIP infrastructure. In this poster we present Proxychain – a novel VoIP authentication protocol based on a modified hash chain construction. Proxychain not only improves performance and scalability, but also offers additional security properties such as mutual authentication. Through experimental analysis we demonstrate an improvement of greater than 1700% of the maximum call throughput possible with Digest authentication in the same architecture. We show that the more efficient authentication mechanisms of Proxychain can be used to improve the overall security of a carrier-scale VoIP network.

Short Biography

Italo Dacosta is a PhD student in the School of Computer Science at the Georgia Institute of Technology, Atlanta, where he is also a member of the Georgia Tech Information Security Center (GTISC). He received a BS in Electronic and Communication Engineering from the Universidad de Panama, Panama in 2002 and a MS in Information Security from the Georgia Institute of Technology in 2007. He is also a former Fulbright grant recipient and a student member of the IEEE, IEEE Computer Society, ACM and USENIX. His research interests include the security, performance and scalability of distributed systems, data privacy and the security of mobile devices.

Notes:

Chaitrali Amrutkar

Title:

Spy vs Spy: Location Oblivious Rendezvous at Starbucks
(Efficient privacy preserving context sensitive applications on mobile devices)

Chaitrali Amrutkar, Rishikesh Naik, Italo Dacosta, Patrick Traynor

Demo:

The demo shows an application for setting an appointment between two spies at the mutually closest Starbucks location, without disclosing their current locations to one another. Context aware applications produce relevant results based on people's contexts such as time and location. Preserving privacy of user information in these applications is a difficult problem. Existing privacy preserving protocols, which calculate output of a function (application) without necessarily revealing the inputs are computationally and memory intensive. We have designed and developed an ad-hoc framework, which converts required computation in an application to private search. Our protocol maintains privacy of the contextual data of the parties involved in the application and can be efficiently run on mobile devices.

Bio:

Chaitrali Amrutkar is a second year PhD student working with Prof. Patrick Traynor. Her research interests are cellular security, user and content privacy and web security. Her awards include the Google Anita Borg scholarship (finalist 2009), Best IMS application prize at the 'Innovative Convergence Applications' competition (CIC'09) at Georgia-Tech and 1st prize in 'Emerging rural technology' category at Asia's largest technical festival Techfest'06 at IIT Bombay, India. Her industry experience includes internships at IBM, Motorola and Qualcomm.

I will be presenting demo and poster

Notes:

Balaji Palanisamy

Title:

PRIVACYGRID: Supporting Anonymous Location Queries in Mobile Environments

Demo:

PrivacyGrid – is a framework for supporting anonymous location-based queries in mobile information delivery systems. In PrivacyGrid, mobile users explicitly define their preferred location privacy requirements in terms of location hiding measures (e.g., location k-anonymity and location l- diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). The framework supports dynamic bottom-up and top-down grid cloaking algorithms that achieve high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. We implement a visualization tool to visualize the spatial cloaking process given the privacy requirements of the users. The tool demonstrates the working of the location perturbation process and helps naïve users understand the location privacy metrics.

Bio:

Balaji Palanisamy is a second year Ph.D student in the College of Computing at Georgia Tech. He works with Professor Ling Liu, and his interests are broadly in Distributed and Mobile Systems. Before coming to Georgia Tech, he obtained a B.Tech in Computer Science from Pondicherry Engineering College in 2006. He spent summer 2008 and summer 2009 with Google, where his work was related to monitoring and troubleshooting the Google's Video Conferencing Infrastructure.

Notes:

Apurva Mohan

Demo: MedVault

Abstract:

The MedVault project aims to develop new techniques for storage, maintenance and control of sensitive data that permit open sharing of sensitive medical data among a wide variety of legitimate users while protecting the data against unauthorized use and disclosure. To achieve these objectives, we have developed a number of solutions goals for verifying data source, privacy-conscious data sharing, fine-grained access control using attributes and monitoring the disclosure of this medical data.

We have developed an architecture for implementing these solutions goals. Based on this architecture, we have developed a research prototype to demonstrate the sharing of personal health records (PHR) to healthcare providers in emergency scenarios. The patient sets up a policy outlining who can access his PHR in 'normal' and 'emergency' scenarios. In this policy, the patient defines the attributes of medical personals who can view his PHR. The healthcare provider like an EMT can use his mobile device or any computer to provide these attributes (in the form of digital credentials) and access the patient's PHR. These PHR are digitally signed by the source at creation time and this signature can be verified by the EMT to confirm the authenticity of the PHR.

Bio:

Apurva Mohan is a PhD student in computer engineering. His research interests are in policy-based authorization systems, PHR/EMR systems and developing authorization solutions for medical databases.

Notes:

Manos Antonakakis

Title:

Demo:

Notos is a dynamic reputation system for DNS. DNS is an essential protocol used by both legitimate Internet applications and cyber attacks. But the problem so far is (1) Malware families utilize large number of domains for discovering the “up-to-date” C&C address, (2) IP-based blocking technologies have well-known limitation and are very hard to maintain, (3) DNS blacklisting based technologies cannot keep up with the volume of new domain names used by botnet, and (4) detecting such type of agile botnets cannot be achieved by the current state of the art detection mechanism. Thus, we've designed Notos, a dynamic, comprehensive reputation system for DNS.

Notos use passive DNS query data, and extract three features from network-based feature vector, zone-based feature vector, and evidence-based feature vector, respectively. It involves a network modeling step along with two clustering steps that one uses the network and the other one the zone feature vectors. As such, we are able to characterize unknown domains with known network behaviors (for example content delivery network and dynamic DNS domains) but also with clusters based upon already labeled domains in close proximity. Their reputation function uses the product of both supervised and unsupervised learning steps to compute a reputation score for a new domain indicative of whether the domain is malicious or legitimate. Based on this behavioral modeling of DNS, Notos can identify malicious domains with high accuracy (true positive rate of 96.8%) and low false positive rate (0.38%), and can identify these domains weeks or even months before they appear in various public blacklists. Notos is currently being used for targeted detection (i.e., Zeus botnet, RBN and spam campaigns).

Manos Antonakakis received his diploma in 2004 from the University of the Aegean, Department of Information and Communication Systems Engineering. From November 2004 up to July 2006, he was working as a guest researcher at the National Institute of Standards and Technology, in the area of wireless ad hoc network security, at the Computer Security Division. Currently he is a Ph.D graduate student in the Georgia Institute of Technology, College of Computing, under Professor Wenke Lee's supervision. His main research interests includes DNS protocol security analysis and mobile client authentication using virtual machines.

Notes:

Junjie Zhang

Poster Title:

BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection

Description:

Botnets are now the key platform for many Internet attacks, such as spam, distributed denial-of-service, identity theft, and phishing. Most of the current botnet detection approaches work only on specific botnet command and control (C&C) protocols and structures, and can become ineffective as botnets change their C&C techniques. In this work, we present a general detection framework that is independent of botnet C&C protocol and structure, and requires no a priori knowledge of botnets. We have implemented our BotMiner prototype system and evaluated it using many real network traces. The results show that it can detect real-world botnets with very low false positives.

Bio:

Junjie is a Ph.D. candidate supervised by Prof. Wenke Lee in GTISC. His current research is on network security, with emphasis on botnet detection.

Notes:

Martin Carbone, Long Lu

Title:

BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections
To appear in Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010), Chicago, IL, October 2010.

Abstract:

Web-based surreptitious malware infections (i.e., drive-by downloads) have become the primary method used to deliver malicious software onto computers across the Internet. To address this threat, we present a browser-independent operating system kernel extension designed to eliminate drive-by malware installations. The BLADE (Block All Drive-by download Exploits) system asserts that all executable files delivered through browser downloads must result from explicit user consent and transparently redirects every unconsented browser download into a nonexecutable secure zone on disk. BLADE thwarts the ability of browser-based exploits to surreptitiously download and execute malicious content by remapping to the file system only those browser downloads to which a programmatically inferred user-consent is correlated. BLADE provides its protection without explicit knowledge of any exploits and is thus resilient against code obfuscation and zero-day threats that directly contribute to the pervasiveness of today's drive-by malware. We present the design of our BLADE prototype implementation for the Microsoft Windows platform, and report results from an extensive empirical evaluation of its effectiveness on popular browsers. Our evaluation includes multiple versions of IE and Firefox, against 1,934 active malicious URLs, representing a broad spectrum of web-based exploits now plaguing the Internet. BLADE successfully blocked all drive-by malware install attempts with zero false positives and a 3% worst-case performance cost.

Bio:

Martim Carbone

Martim Carbone is a fifth-year Computer Science Ph.D. student. He works with Prof. Wenke Lee on systems security topics related to operating systems and virtualization. He is originally from Brazil and holds a BSc and MSc in Computer Science from the State University of Campinas.

Long Lu

Long Lu is a third-year Ph.D. student in GTISC, advised by Prof. Wenke Lee. His research mainly focuses on operating systems security, virtualization, and web-based malware prevention.

Notes:

Arif Selcuk Uluagac

Poster 1:

Title: TIme-Based DynamiC Keying and En-Route Filtering (TICK) for Sensor-Based Cyber Physical Systems (CPS)

Description: As transmission cost is significant in resource-constrained devices (e.g., sensors), TICK is an energy-efficient technique to secure the network, without the transmission of explicit keying messages needed to avoid stale keys using time values as one-time dynamic keys.

Poster 2:

Title: The Design of NetSecLab: A Small Competition-Based Network Security Lab

Description: The NetSecLab is a competition-based exercise developed for the purpose of increasing the amount of hands-on experience obtained by students in a lecture-based class environment.

Bio:

Arif Selcuk Uluagac obtained his Ph.D. in the School of ECE at the Georgia Institute of Technology as a member of the Communications Systems Center. He received his B.Sc. in Comp. Eng. from the Turkish Naval Academy and M.Sc. degrees in ECE from Carnegie Mellon University in 1997 and 2002, respectively. He also holds an M.Sc. in Information Security from the School of Computer Science at Georgia Institute of Technology in 2009. He received "2007 Outstanding ECE Graduate Teaching Assistant Award" from the School of ECE at Georgia Institute of Technology. He is a member of IEEE, ACM, and ASEE.

Notes:

Emily Ivey and Jillian Pilch

eDemocs: Electronic Distributed Election Monitoring over Cellular Systems

Demo: As computing plays an increasingly important role in democratic processes, it is essential that the lessons and principles of computer security be applied as new systems are designed and old methodologies are updated. This demonstration we will show a smartphone-based system that uses secure SMS messages to relay election observations and map the locations of observers over a 2G network. In conjunction with the Carter Center, this technology was successfully beta tested during the May 2010 Filipino Presidential election. This project is continuing to improve to further enhance the election observation system.

Bio: Emily Ivey has a MS in Public Policy from Georgia Tech with a focus in Science and Technology policy She has been involved in e-Democracy initiatives for several years and continues to do so while working for Dr. Rich DeMillo. Previously, she has worked for the Center for Assistive Technology and Environmental Access researching accommodations for people with disabilities in STEM classrooms, and for the Center for Advanced Communication Policy studying the ways in which technological advance help people with disabilities find employment. Emily also has a BA in English from Georgia State University.

Jillian Pilch is in her final year at Agnes Scott College double majoring in French and International Relations. She plans to pursue a Masters in Public Policy from Georgia Tech in Spring 2012.

Notes: