Resilience of Backbone Provider Networks
Egemen K. Çetinkaya, Justin P. Rohrer, James P.G. Sterbenz

The Global Internet is a complex, critical infrastructure and the research community has been analysing the topology of the Internet for over a decade. The primary focus has been on the logical aspects of the topology, since tools were developed to collect, measure, and analyse IP-layer properties of the Internet. Physical topologies provide services for logical layers, and defining physical connectivity is a major research challenge. Moreover, to study behaviour of the Internet under correlated geographic failure scenarios, physical topologies are necessary.

Physical topologies provide the necessary connectivity, while logical topologies enable data communication between end systems. Resilience characteristics of the two topologies differ in part due to differences in the topological properties and in part due to different challenges networks face. For example, while a DDoS attack aims to consume network resources on an end host, the underlying physical infrastructure can be intact. Likewise, an earthquake might damage the physical infrastructure and if there is no geographical diversity built in the system this might cause the overlaid logical topology to become dysfunctional. We argue that resilience analysis of individual topologies (e.g. AS-level, IP-layer) alone is not enough and a collective analysis of networks is required to design resilient networks. Therefore, understanding the resilience characteristics of networks and further developing cost-efficient mechanisms to cope with network challenges of such complex systems is crucial.

While the physical topologies are crucial in understanding and modelling Internet, public data about physical topologies are limited. Two primary reasons that the service providers unwillingness to share the data are business competitiveness and security concerns. We discuss the necessity of physical topologies to realistically evaluate network resiliency. We argue that a collective topology information is needed to realistically evaluate resilience properties of networks. Furthermore, while geographic diversity is an essential mechanism to increase the resiliency of network, there is a trade-off between the increased level of resiliency and the cost of building such resilient systems.
Prioritizing Intrusion Analysis Using Dempster-Shafer Theory

Loai Zomlot
Kansas State University
lzomlot@ksu.edu

Sathya Chandran Sundaramurthy
Kansas State University
sathya@ksu.edu

Kui Luo
Kansas State University
kuiluo@ksu.edu

Xinming Ou
Kansas State University
xou@ksu.edu

S. Raj Rajagopalan
HP Labs
raj.rajagopalan@hp.com

Intrusion analysis and incident management, i.e. the process of combing through IDS alerts and audit logs to identify and remediate true successful and attempted attacks, remains a difficult problem in practical network security defense. The major root cause of this problem is the large rate of false positives in the sensors used by IDS systems to detect malicious activities. IDS systems are currently unable to differentiate nearly certain attacks from those that are merely possible, reducing the value of the alerts to an administrator. Standard Bayesian theory has not been effective in this regard because of the lack of good prior knowledge. This paper presents an approach to handling such uncertainty without the need for prior information, through the Dempster-Shafer (DS) theory that uses a generalization of probabilities called beliefs to characterize confidence in evidence in support of a given hypothesis. DS theory also provides a calculus to compute the level of belief in an aggregate of evidence. We address a number of practical but fundamental issues in applying DS to intrusion analysis, including how to model sensors’ trustworthiness, where to obtain such parameters, and how to address the lack of independence among alerts. We present an efficient algorithm for carrying out DS belief calculations on an IDS alert correlation graph, so that one can compute a belief score for a given hypothesis, e.g. a specific machine is compromised. The belief strength can be used to sort incident-related hypotheses and prioritize further analysis by a human analyst of the hypotheses and the associated evidence. We have implemented our approach for the open-source IDS system Snort and evaluated its effectiveness on a number of data sets as well as a production network. The resulting belief scores were verified through both anecdotal experience on the production system as well as by comparing the belief rankings of hypotheses with the ground truths provided by the data sets we used in evaluation, showing thereby that belief scores can be effective in taming the high false positive rate problem in intrusion analysis.
Device Authentication for the Medical Device Coordination Framework

Carlos Salazar and Eugene Vasserman
Kansas State University

Abstract (presentation)

Medical devices have a history of being implemented as stand-alone units. Most devices currently used in clinical environments stay true to this paradigm and even when a device manufacturer has implemented some interoperability features, they are not designed to work with other devices/software from other manufacturers, and connectivity is typically only used for passively logging device data. Simply put, medical devices do not play well with each other. As a result, there is increasing movement within the clinical and medical device community toward a “system of systems” approach for medical devices, similar to other safety-critical areas such as power generation and aviation. Integrated medical systems can provide numerous benefits such as improved patient safety through “smart” alarms that gather patient data from multiple sources, and automated clinical workflows that automatically reduce common medical errors. The exploration of this idea has lead to the creation of the emerging Integrated Clinical Environment (ICE) standard and the Medical Device Coordination Framework (MDCF) project. The MDCF is a framework for coordinating medical devices and is currently the most complete implementation of the ICE standard. However, there are serious safety and security concerns in the “system of systems” paradigm, given the importance of completeness, correctness, and privacy of patients’ medical data. An attacker who can alter data or prevent its transmission could seriously harm patients. Therefore, we need to ensure that only authenticated devices can connect.

This paper describes the implementation of a flexible device authentication framework within the existing MDCF. To accomplish this, we located the points within the MDCF device connection process at which authentication must occur and inserted, “hooks” where modular security providers can attach. This architecture allows arbitrary protocols to be implemented as drop-in modules in the future. For added flexibility, the MDCF can be configured via a local policy to either require authentication or not (accept to reject unauthenticated devices). The authentication providers are entirely self-contained, incorporating all protocol logic and reporting the failure or success of device authentication to the rest of the MDCF, in the latter case also returning negotiated cryptographic material for later usage in encrypted communication channels. All providers implement common interfaces and are lazily instantiated by the MDCF as requested by the device (“call-by-name”). The currently implemented proof of concept “null” authentication provider is similar to IPsec null encryption -- it does not provide cryptographically sound authentication. We evaluated the performance of this null provider (giving us the pure overhead of the authentication system and not a particular authentication algorithm) using various device connection rates and in various MDCF configurations -- prior to authentication implementation, with authentication but set to accept all devices, and with authentication required to connect.
A Secure Web Browser Without Isolation Kernels

Eugene Vasserman and Keith McVey
Kansas State University

Abstract (poster)

Web browsers have come to embody the interface to the Internet, and securing those interactions is more important than ever. Highly secure browsers have generally taken one of two approaches: use advanced operating system security features (e.g. Chromium and SELinux) or design an isolation kernel below the various browser components (e.g. OP). We present the design of a secure web browser, enforcing strong website isolation and cross-site scripting protection while also protecting the user in case of total browser compromise, all without using only light-weight OS-provided mechanisms.

Our “ultra-thin” browser design delegates security enforcement to the underlying operating system, using existing security mechanisms like user and process isolation, fine-grained object access permissions, and resource limits to prevent insecure interaction between different websites and between websites and the user’s system. We treat individual websites as “pseudo-users” of the operating system, with a subset of regular user permissions. Each website’s browser instance runs in a user context created only for that website (connected via a persistent socket to that website only), so even bugs in the browser will not allow malicious websites to take control of the user’s account or the underlying system, nor connect to third-party sites unless explicitly permitted. The proposed design offers many benefits over current browsers, including increased performance through lower security overhead, support for multiple client-side languages (not just JavaScript), a richer client-side storage infrastructure compatible with HTML5, and even the ability to run native code on the client (without static analysis), making full use of local features such as 3D acceleration (without the need for WebGL).

Our browser is made up of three logical components: a rendering engine to display test and graphics in a browser-like window, a language support module to execute untrusted code downloaded from websites, and a client-side storage modules to store website state (e.g. cookies). Each presents unique challenges in terms of design, implementation, and backward compatibility. The renderer must display websites in separate processes, but modern web pages are composed of many elements, some from different domains than the one hosting the page. For backward compatibility, all these elements must be displayed in the same window, but for security, they should run in different memory spaces. The language support module (LSM) accepts untrusted website code and runs it on the local machine, inheriting the permissions of the sending website’s pseudo-user. It must allow interaction between downloaded code and the displayed browser window, since a large number of websites modify their display elements dynamically, so the rendering engine exports hooks for inter-process communication-based interaction with the webpage DOM. Based on the OS process and user model, untrusted code is already prevented from interacting with other processes’ memory or files, and cannot access the network except to communicate with the sending site only, through the use of socket and file descriptor limits.
STEP: Source Traceability Elimination for Privacy against Global Attackers in Sensor Networks

Sejun Song*, Hyungbae Park†, and Baek-Young Choi†

* Texas A&M University, College Station, TX 77843, USA
Email: sjsong@tamu.edu

† University of Missouri - Kansas City, MO 64110, USA
Email: {hpark, choiby}@umkc.edu

As wireless sensor networks (WSNs) are self-organized cooperative ad hoc networks built with low-power, low-cost, and small-sized sensor nodes, it has been considered as an enabling technology, especially, for the remote resource surveillance applications in harsh environments. For example, sensor nodes can be deployed to assist the strategic movement of field deployed soldiers or to track the habitat of endangered animals. For the successful deployment of WSN applications in the open area, harnessing the security service is a must. While the content privacy protection can be achieved by applying the traditional encryption and authentication mechanisms for the most of the applications, preserving contextual privacy is still one of the most challenging issues. Since WSNs use the open-architecture based broadcast medium, adversaries can easily observe data communications to infer critical information such as source locations and target movement patterns without knowing the content of messages. For example, attackers can catch the field deployed soldier’s physical location by just seeing the source of communication messages without cracking the protected data. Attackers also can trace the movement patterns of endangered animals from the changing message sources.

As the cost of sensors and radio devices becomes reasonable, in many applications, the reward of successful target tracking can be much higher than the cost of global sensor deployment. Considering the big potential gain of successful attack and the low cost of sensor deployment, the more adversaries may want to deploy the attacker nodes globally to maximize the chance of detection. As the global attacker model becomes more realistic, it is critical to equip WSNs with a privacy preserving technology against global attackers.

There are a few recent source location privacy solutions against global attacker model are to hide the original source location by adding fake sources or by sending network-wide periodic/statistical messages, they are not practical due to the significant overheads and latency. On the other hand, the existing source simulation technique creates multiple fake candidate traces to extend the detection time of the original trace, thus the safety period is bounded by the number of candidates.

We propose a source location privacy preserving approach against global attacker model, named Source Traceability Elimination for Privacy (STEP). STEP uses tethered throwboxes to hide the communication of an original source location and stealthily scatter it to a remote location. The tethering link between sensors and throwboxes is a stealthy communication path that can be established in various ways, for example, a wire-line or an out of band long-range wireless transmission. Once tethering links are established, messages are sent by the original source sensor node on one end through the link without incurring wireless communication on this node on a regular channel, and are stored in a throwbox that is a stationary device equipped with wireless interfaces and storage. The message is repackaged at the throwbox for a regular wireless communication when a mobile dispatcher nodes pass by the throwbox. The throwbox acts as a dynamic rendezvous point, creating a contact opportunity and the message will be eventually relayed to the sink via mobile dispatchers. Therefore, unless a global attacker knows the phantom pattern of tethered throwboxes, it cannot capture the original source location. Thus, STEP disguises original source locations and movement patterns by eliminating the trace toward original source locations.

STEP is a novel privacy preserving technique against global attackers that maximizes the safety period by eliminating the original source location without incurring additional traffic overhead. It is one of few privacy preserving approaches against global attackers, and takes a drastically different approach than others where excess traffic is used for privacy. Our approach can be used with other existing schemes for the synergistic impact. We quantify contextual privacy levels, and evaluate the effectiveness of STEP via analysis and simulation. We also show its impact when combined with other approaches.
Stalking Online: on User Privacy in Social Networks

ABSTRACT
With the extreme popularity of Web and online social networks, a large amount of personal information has been made available over the Internet. On the other hand, advances in information retrieval, data mining and knowledge discovery technologies have enabled users to efficiently satisfy their information needs over the Internet or from large-scale data sets. However, such technologies also help the adversaries such as web stalkers to discover private information about their victims from mass data.

In this paper, we study privacy-sensitive information that are accessible from the Web, and how these information could be utilized to discover personal identities. In the proposed scenario, an adversary is assumed to possess a small piece of “seed” information about a targeted user, and conduct extensive and intelligent search to identify the target over both the Web and an information repository collected from the Web. In particular, two types of attackers are modeled, namely tireless attackers and resourceful attackers. We then analyze detailed attacking mechanisms that could be performed by these attackers, and quantify the threats of both types of attacks to general Web users. With extensive experiments and sophisticated analysis, we show that a large portion of users with online presence are highly identifiable, even when only a small piece of (possibly inaccurate) seed information is known to the attackers.
Modelling Challenges and Attacks to Wireless Networks

Dongsheng Zhang, Santosh Gogi, Egemen Çetinkaya, and James P.G. Sterbenz

Understanding network behaviour under perturbations can improve today's networks performance, as well as lead to a more resilient and survivable Future Internetwork. Therefore, it is essential to have a thorough understanding of the network behaviour when exposed to challenges, such as component failures, attacks, large-scale disasters, and effects of the mobile wireless communication environment. Recognition of network disruptions and their causes is crucial for planning and designing networks. We cannot thoroughly study the effects of challenges in live networks without impacting users. Testbeds are useful, but do not provide the scope and scale necessary to understand the resilience of large, complex networks, although progress is being made in this direction. Simulations arguably provide the best compromise between tractability and realism to study challenges, however this is nontrivial. We develop the KU Challenge Simulation Module (KU-CSM) to evaluate network dependability and performability in the face of challenges. We utilise ns-3 network simulator as the main component of our framework and KU-CSM consists of four distinct steps: challenge specification, network topology, ns-3 C++ code, simulation and post-processing. As a result, we can study the impact of challenges on networks in a cost-efficient way.

The Wireless Challenge Simulation Module (WCSM) extends the previous work of KU-CSM. The mobile ad hoc network (MANET) environment has a dynamic and intermittent network connectivity due to channel fading and the mobility of the nodes; hence, it is more complex and difficult to model these networks and their challenges. We begin by applying a maximum range propagation model to our simulation and then extend to more sophisticated radio models. We model MANETs as time-varying graphs represented as a weighted adjacency matrix, in which the weights refer to the link availability during a period of time. A wide range of network attacks are modeled including several attacks models used for wired network. We concentrate on malicious attack scenarios, in which we model attacking the most significant nodes in the network, based on clustering coefficient and several centrality metrics such as degree, betweenness, and closeness. Our ultimate goal is to provide a comprehensive network challenge framework incorporating both wired and wireless networks.
Conceive of the Future Internet Based on the Research of TCP/IP Vulnerabilities

By Yanyan Li, Keyu Jiang

Abstract

With the popularity of Internet, people are increasingly dependent on Internet. At the same time, however, some malicious persons conduct unscrupulous invasion on Internet by taking the vulnerabilities of TCP/IP protocols. TCP/IP protocols, which once acted as the cornerstone of Internet, have been unable to provide a secure platform for the communication taken place above it. Gradually, the security problems of TCP/IP protocols have begun to drawn people’s attention. This paper explores and reveals that TCP/IP protocols have a large number of vulnerabilities that make Internet easily exposed to attacks by testing some different kinds of attacking labs, and then describes the most fundamental reason of the insecurity of TCP/IP protocols. Finally, this paper proposes an assumption to the future Internet based on the current research of TCP/IP protocols and Internet architecture.

Keywords: TCP/IP protocols, vulnerabilities, Internet Architecture
HyXAC: a Hybrid Approach for XML Access Control

Manogna Thimma, Bo Luo
University Of Kansas

Abstract:

While XML has been widely adopted for sharing and managing information over the Internet, the need for efficient XML access control naturally arise. Various access control models and mechanisms have been proposed in the research community, such as view-based approaches and preprocessing approaches. All categories of solutions have their inherent advantages and disadvantages. For instance, view based approach provides high performance in query evaluation, but suffers from the view maintenance issues.

To remedy the problems, we propose a hybrid approach, namely HyXAC: Hybrid XML Access Control. HyXAC provides efficient access control and query processing by maximize the utilization of available (but constrained) resources. HyXAC uses pre-processing approach as a baseline to process queries and define sub-views. It dynamically allocates the available resources (memory and secondary storage) to materialize sub-views to improve query performance. Dynamic and fine-grained view management is introduced to utilize cost-effectiveness analysis for optimal query performance. Fine-grained view management also allows sub-views to be shared across multiple roles to eliminate the redundancies in storage.
View for Computer Forensic Education, Training, and Awareness

This paper tries to describe view for computer forensic education, training, and awareness. The paper introduction is why the staffs are required to receive computer forensic training and education. Employees could through security policy increase awareness of computer forensic. The employees should be divided into several types. As management, they need to receive education for computer forensic. Education for forensic will introduce core value of forensic, and study how to build a forensic policy. The technical staff would need to receive training. They need to understand the basic technology of computer forensic. Through training, technical personnel need to know what they should do when discovery of hacking.

Keywords: evidence, type, training, education, awareness
The Importance of Web Vulnerability Detection

Yali Yu & Keyu Jiang

Fort Hays State University

yuyali1227@yahoo.cn

March 9, 2012

Abstract

The tide of today’s information technology, web vulnerabilities detected for every enterprise or organization and even individual, play an increasingly critical role, and web vulnerability detection is an important link in the information security system. This paper will show three points to illustrate the importance of active detection web vulnerabilities. A survey found, shows the different types of web vulnerabilities. This paper is based on this survey to analyze the importance of web vulnerability detection. First, the survey types and quantity of web vulnerabilities are in different years to analyze the development trend of the web vulnerability. Secondly, according to the probability of occurrence and hazards of survey web vulnerability you can divide the vulnerability rating. Thirdly, it investigates the harmful effects on people based on different web vulnerabilities.
Abstract

The construction of digital campus is far from perfect in many higher educational institutions, proved by the existence of massive problems relating to data store, data transmission, and data security. Taking the practice of the university where the author works, this article analyzes the defects haunting current digital campus database system, and proposes a corresponding solution—“campus database system” based on the concept of “cloud database”. By virtue of the foregoing system, a brand-new data network characterized by high efficiency and flexibility will be established. Moreover, the paper delivers a systematic discussion about the merits and disadvantages of the proposed solution. In particular, the article reveals some potential security threats concerning “cloud database”, and raise feasible countermeasures.
Classification of UDP Traffic for DDoS Detection

Alex Bardas
Kansas State University

Abstract:

"UDP (User Datagram Protocol) traffic has recently been used in flooding-based distributed denial of service (DDoS) attacks, most notably by those launched by the Anonymous group. Despite extensive past research in the general area of DDoS detection/prevention, the industry still needs effective tools to deal with DDoS attacks leveraging UDP traffic. This work presents our investigation into the proportional-packet rate assumption, and the use of this criterion to classify UDP traffic with the goal of detecting malicious addresses that launch flooding-based UDP DDoS attacks. We performed our experiments on data from a large number of production networks including large corporations (edge and core), ISPs, universities, financial institutions, etc. In addition, we also conducted experiments on the DETER testbed as well as a testbed built in the Argus cybersecurity lab. All the experiments indicate that the proportional-packet rate assumption generally holds for benign UDP traffic and can be used as a reasonable criterion to differentiate DDoS and non-DDoS traffic. We designed and implemented a prototype classifier based on this assumption and discuss ways it can be used to effectively detect UDP-based flooding attacks."
Network Resilience, Survivability, and Disruption Tolerance: Architectural Framework, Strategy, Analysis, Simulation, Tools, and Experimentation

James P.G. Sterbenz and Egemen Çetinkaya

Abstract:
As the Internet becomes increasingly important to all aspects of society, the consequences of disruption are increasingly severe. Thus it is critical to increase the resilience and survivability of the future networks in general, and the Internet in particular. We define resilience as the ability of the network to provide desired service even when the network is challenged by attacks, large-scale disasters, and other failures. Resilience subsumes the disciplines of survivability, fault-tolerance, disruption-tolerance, traffic-tolerance, dependability, performability, and security.

After an introduction to the disciplines and challenges to network resilience, this presentation will first present the ResiliNets framework developed in the NSF FIND (Future Internet Design) PoMo and EU FIRE (Future Internet Research and Experimentation) ResumeNet projects. We then discuss analytical, simulation, and experimental emulation techniques for understanding, evaluating, and improving the resilience of the Future Internet. This includes a multilevel state-space based approach that plots network service delivery against operational state that is the basis for both mathematical- and simulation-based analysis, and approaches that embed fundamental properties such as redundancy and diversity into all aspects of network structure, mechanism, and protocols. A set of tools to help in this analysis has been developed: KU-LoCGen (Location and Cost-Constrained Topology Generation), KU-TopViwe (Topology Viewer), and KU-CSM (Challenge Simulation Module). Plans to experimentally evaluate resilience include using the international programmable testbed GpENI: Great Plains Environment for Network Innovation.
Moving Target Defenses for Computer Networks

By Dr. Simon Ou and Dr. Scott A. DeLoach

This presentation will discuss the proposed design and some initial simulation results for a prototype moving-target defense (MTD) system, whose goal is to exponentially increase the difficulty of attacks on enterprise networks. In most computer networks, services are run on well-known ports and are located at fixed IP addresses that can be easily identified through reconnaissance, which provides attackers with a great advantage. The goal of our MTD system is to continuously adapt the network configuration over time in ways that seem random or chaotic to attackers, thus negating their advantage. The novelty of our approach lies in the use of runtime models that explicitly capture a computer network's operational and security goals, the functionality required to achieve those goals, and the logical and physical configuration of the system. Our MTD system uses these runtime models in concert with a novel conservative attack graph to analyze both known and unknown vulnerabilities to ensure that adaptations occur often enough and in the right areas to protect the system against specific attacker profiles.