An End-to-End Security Auditing Approach for

Service Oriented Architectures

Bharat Bhargava Purdue University and Mark Linderman and Asher Sinclair, AFRL

Service-Oriented Architecture (SOA) is becoming a major paradigm for distributed application development in the recent explosion of Internet services and cloud computing. However, SOA introduces new security challenges not present in the single-hop client-server architectures due to the involvement of multiple service providers in a service request. The interactions of independent service domains in SOA could violate service policies or SLAs. In addition, users in SOA systems have no control on what happens in the chain of service invocations. Although the establishment of trust across all involved partners is required as a prerequisite to ensure secure interactions, still a new end-to-end security auditing mechanism is needed to verify the actual service invocations and its conformance to the expected service orchestration. In this project, we provide an efficient solution for end-to-end security auditing in SOA. The proposed security architecture introduces two new components called taint analysis and trust broker in addition to taking advantages of WS-Security and WS-Trust standards. The interaction of these components maintains session auditing and dynamic trust among services. This solution is transparent to the services, which allows auditing of legacy services without modification. Moreover, we have implemented a prototype of the proposed approach and verified its effectiveness in a LAN setting and the Amazon EC2

cloud computing infrastructure.

A Trust-Based Approach for Secure Data Dissemination in a Mobile

Peer-to-Peer Network of AVs

 Bharat Bhargava, Purdue University

Mobile peer-to-peer networks of aerial vehicles (AVs) have become significant in collaborative tasks. However, the nature of the communication between the nodes in these networks makes the disseminated data prone to interception by malicious parties, which could cause serious harm for the designated mission of the network. In this project, we propose an approach for secure data dissemination in a mobile peer-to-peer network, where the data disclosed to a particular node in the network depends on the trustworthiness of that node as well as the matching of policies of the data source and destination. We demonstrate the use of active bundles for protecting sensitive data as they are sent from one node to another, on the simulation we developed for data dissemination in a mobile peer-to-peer network of AVs. We discuss filtering techniques for dissemination of sensitive data in such networks.

Secure and Efficient Access to Outsourced Data

Bharat Bhargava Purdue University and Chao Wang, UNCC

Providing secure and efficient access to large scale outsourced data is an important component of cloud computing. In this project, we propose a mechanism to solve this problem in owner-write-users-read applications. We propose to encrypt every data block with a different key so that flexible cryptography-based access control can be achieved. Through the adoption of key derivation method, the owner needs to maintain only a few secrets. Analysis shows that the key derivation procedure using hash functions will introduce very limited computation overhead. We propose to use over-encryption and/or lazy revocation to prevent revoked users from getting access to updated data blocks. We design mechanisms to handle both updates to outsourced data and changes in user access rights. We investigate the computation overhead and safety of the proposed approach, and study mechanisms to improve data access efficiency.

A Kolmogorov Complexity Approach for Measuring Attack Path Complexity

Bharat Bhargava Purdue University and Nokedi Idika MIT Lincoln Lab

The difficulty associated with breaching an enterprise network is commensurate with the security of that network. A security breach, or a security policy violation, occurs as a result of an attacker successfully executing some attack path. The difficulty associated with this attack path is critical to understanding how secure a given network is. Currently, however, there are no consistent methods for measuring attack path complexity that make the assumptions of a modeler explicit while providing visibility to how the modeler models the attack path. To provide these desirable attributes, we propose a regular-expressions-inspired language whose rationale for attack path complexity measurement is based on Kolmogorov Complexity. After detailing our Kolmogorov Complexity-based method, we demonstrate how it can be applied to a novel security metric: the K-step Capability Accumulation metric, a metric that defines the security of a network in terms of the network assets attainable for attack effort exerted.

Extending Attack Graph-Based Security Metrics and Aggregating Their Application

Bharat Bhargava, Purdue University and Nwokedi Idika, MIT Lincoln Lab

The attack graph is an abstraction that reveals the ways an attacker can leverage vulnerabilities in a network to violate a security policy. When used with attack graph-based security metrics, the attack graph may be used to quantitatively assess security-relevant aspects of a network. The Shortest Path metric, the Number of Paths metric, and the Mean of Path Lengths metric are three attack graph-based security metrics. However, one’s usage of these metrics can lead to misleading results. The Shortest Path metric and the Mean of Path Lengths metric fails to adequately account for the number of ways an attacker may violate a security policy. The Number of Paths metric fails to adequately account for the attack effort associated with attack paths. To overcome these shortcomings, we propose a complimentary suite of attack graph-based security metrics to aid network security evaluation and network hardening. Moreover, we specify an algorithm for combining the usage of these metrics. We present simulated results that suggest that our approach has the ability to reach a conclusion about which of two attack graphs correspond to a network that is most secure in many instances.

Developing Attack Defense Ideas for Ad Hoc Wireless Networks

Bharat Bhargava Purdue University

Ad hoc networks are natively cooperative systems in the sense that their nodes have to relay data to one another. The inherent drawback of this scheme is that it renders these networks susceptible to intruders. Collaborative attacks, in which various attackers may coordinate actions to hit the network stronger, are also facilitated by the natural cooperation existing in ad networks. In this project, we discuss the most important forms of attacks, address possible collaborations among attackers, show how machine learning techniques and signal processing techniques can be used to detect and defend against collaborative attacks in such environments, and discuss implementation issues. We also perform evaluations to determine the best design options for our preliminary proposed scheme to collaboratively respond to attacks.

Developing Attack Defense Ideas for Ad Hoc Wireless Networks

Bharat Bhargava Purdue University

Ad hoc networks are natively cooperative systems in the sense that their nodes have to relay data to one another. The inherent drawback of this scheme is that it renders these networks susceptible to intruders. Collaborative attacks, in which various attackers may coordinate actions to hit the network stronger, are also facilitated by the natural cooperation existing in ad networks. In this project, we discuss the most important forms of attacks, address possible collaborations among attackers, show how machine learning techniques and signal processing techniques can be used to detect and defend against collaborative attacks in such environments, and discuss implementation issues. We also perform evaluations to determine the best design options for our preliminary proposed scheme to collaboratively respond to attacks.

Protecting PLM Data throughout their lifecycle

Bharat Bhargava Purdue University,

Enterprises operate in a global economy with their operations dispersed across internal processes and external partners. Product Lifecycle Management (PLM) systems play a significant role in modern product development and management. There are multiple stages in product lifecycle that streamline by sharing data among PLM entities. Shared data may contain highly sensitive information such as trade secrets, intellectual property, private organization or personal information. In large enterprise systems, it is difficult to understand and track data dissemination. Data sharing a cross global partners complicates and magnifies the problem further. The effect of shared data being leaked is one of the key risks. Existing approaches ensure security within the domain of an organization and don't address protection in a decentralized environment. We propose an approach for secure data dissemination using the Active Bundle scheme. This approach enables organizations to securely share information in their PLM steps and protects it throughout the product lifecycle.

Monitoring and Managing Cloud Computing Security using

Denial of Service Bandwidth Allowance

Bharat Bhargava Purdue University and Biswajit Panja, University of Michigan, Flint

Over the next decade, cloud computing has a good chance of becoming a widely used technology. However, many challenges face the cloud to be overcome before the average user or business team will trust their vital information with a cloud server. Most of these challenges tie into developing sound security measures for the cloud. One of the largest security obstacles is how to defend against a Denial of Service (DOS) or

Distributed Denial of Service (DDOS) attack and save the cloud server from crashing. DOS attacks are nothing new; many strategies have been proposed and tested against DOS attacks on networks. However, none have been able to completely prevent DOS attacks. The search continues for an effective solution to keep data available to legitimate users who need it when the cloud network that stores that data is the target of a DOS attack. The method proposed (DOSBAD) in this project will explain how effectively detecting the bandwidth limit of a cloud network and the bandwidth currently in use to know when a DOS is being launched.

A Method for Developing Acceptably Secure

Software using the Agile Development Approach

Bharat Bhargava and Lotfi ben Othmane, Purdue University and Eindhoven University of Technology

Organizations use iterative and incremental development approaches such as Agile Software Development (ASD) because they cope with the natural evolution of software. For instance, the most common methods used are Scrum and Extreme Programming (XP), which apply the ASD. There are several challenges that limit the use of ASD for developing secure Software. Secure software are software that continue to function correctly under malicious (intended) attacks. Proposed solutions for extending the ASD process to produce secure software fall short of ensuring the security of the increments produced in each iteration development cycles that last a fixed short period. This research proposes extending the agile development process to support the development of acceptably secure software. It addresses two questions:

1. How to ensure the security of software increments produced by development iterations?
2. How to extend the agile development process to support security engineering activities and produce acceptably secure software in each iteration.