

Overview Talk – Shambhu Upadhyaya (January 17, 2012)

Cyber Security: Fundamentals and Challenges for the Future

Abstract: In today's age of electronic connectivity, there are more than a billion computers in the world and this number is expected to double in the next three years. About 300 billion email messages are being exchanged every day which means that more than 3 million emails are sent every second. The explosive growth in computer systems and their interconnections via networks and the dependency on computers by organizations and individuals have heightened awareness of the need to protect data. The greatest threat of cyber attacks is being experienced by national critical infrastructures and defense systems, but the commercial domain is also equally impacted by viruses, worms, hackers, electronic eavesdropping, electronic fraud, and so on. In this talk, we will outline the current status of cyber security, the type of attacks and how do we approach the problem. We will review some of the hot topics in the cyber security arena and highlight some of the research projects that we have been working on in the academia.

Technical Talk 1 – Shambhu Upadhyaya (January 18, 2012)

Mitigating Insider Threats and Information Leak in High Value Systems

Abstract: Insider Threat Management products based on misuse signatures are a first step in dealing with insider attacks, but there are still several fundamental challenges, beginning with the understanding of the insider threat. In fact, any good model or assessment methodology will be already a significant advance. In this talk, we will first look into the challenges and examine some of the recent attempts to address them. This includes a new threat assessment methodology by which specific and targeted countermeasures can be deployed against stealthy attacks for which no effective solutions currently exist. Central to our approach is the information-centric threat model called *Capability Acquisition Graph* (CAG) model that works at a higher level of abstraction—viz. the user operation level—as opposed to low levels, such as network packets or system calls, which are considered in attack-centric models that are limited by implementation constraints. We briefly outline this scheme, present some theoretical results, demonstrate a proof-of-concept prototype and show how this scheme can be used to assess insider activities and harden the network against insider attacks. Adoption of the CAG model to detect sensitive information leak in high value systems will also be discussed. This research has been funded by DARPA.

Technical Talk 2 – Shambhu Upadhyaya (January 19, 2012)

Protecting Security Systems from Subversion Attacks on the Internet

Abstract: Complex software is not only difficult to secure but is also prone to exploitable software bugs. Hence, an anti-virus or intrusion detection system if deployed in user space is susceptible to security compromises. Thus, the 'watcher' of other software processes needs to be 'watched.' In this talk, we address this classic problem of 'Who watches the watcher?' We will first give an overview of current approaches for protecting security devices in a uni-core environment. This includes our scheme built with a cyclic monitoring topology of light-weight processes to protect intrusion detection systems. Our scheme will then be extended to protect the user space components deployed in a multi-core environment. Results of simulation to study the effectiveness and performance of our scheme on a multi-core simulator will also be presented. This research has been funded by U.S. Air Force Research Laboratory.

Speaker Biography:

Shambhu Upadhyaya

Professor of Computer Science and Engineering and

Director, Center of Excellence in Information Systems Assurance Research and Education (CEISARE)

University at Buffalo, The State University of New York

Prof. Shambhu J. Upadhyaya is with the Computer Science and Engineering department at the State University of New York at Buffalo where he directs the Center of Excellence in Information Systems Assurance Research and Education (CEISARE), designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS). His research interests are information assurance, computer security, fault tolerant computing and reliable distributed systems. He has authored or coauthored more than 240 articles in refereed journals and conferences in these areas. His current projects involve insider threat modeling, intrusion detection in databases, security in wireless networks, and protection against Internet attacks. His research has been supported by National Science Foundation, Rome Laboratory, U.S. Air Force Office of Scientific Research, DARPA, National Security Agency, IBM, Intel Corporation, Harris Corporation and Cisco.

Prof. Upadhyaya has held visiting research faculty positions at the Center for Reliable and High Performance Computing, University of Illinois, Urbana-Champaign, Intel Corporation, Folsom, CA, Air Force Research Laboratory, Rome, NY and the Naval Research Laboratory, Washington DC. He has been awarded an IBM Faculty Partner Fellowship for year 2000-01 in recognition of his research accomplishments. He was also an NRC faculty fellow in 2001 and 2002. He received the Best Paper Award in IEEE Malware 2007 for his work on “SpyCon: Emulating User Activities to Detect Evasive Spyware.”

Prof. Upadhyaya has served as the Program Chair and General Chair of several IEEE conferences in areas ranging from security and privacy, distributed systems, and VLSI testing. He was an associate editor of IEEE Transactions on Computers from 2001 to 2006, and is a member of the editorial board of the International Journal on Reliability, Quality, and Safety Engineering published by the World Scientific Publishers and the Transactions on Security and Safety published by the Institute of Computer Sciences, Social Informatics and Telecommunications (ICST).



Technical Talk 3 – M. Sethumadhavan (January 17, 2012)

Development of Visual Cryptographic schemes

Abstract: Visual cryptography is a perfectly secure way to protect secrets and is characterized by its decryption method. In this, a secret image is split into a set of shares so that some authorized shares can access to the secret whereas other unauthorized shares cannot leak out any secret information. To recover the secret image, one has to collect a set of qualified shares and print them onto transparencies. As long as all the transparencies are stacked up, the secret image will reveal on the stacked image. Since the secret image can be identified with human eyes without any complex decryption algorithms or the aid of computers, visual cryptography schemes can be very suitable for the situation when computers are not available.

In this talk we give a tutorial introduction to various visual cryptographic schemes. We will also explain some methods for constructing basis matrices for some basic visual cryptographic schemes.

Technical Talk 4 – M. Sethumadhavan (January 17, 2012)

Cryptographic Protocols

Abstract: In this talk we present a systematic approach to the fundamental concepts required to understand cryptographic protocols. Understanding protocol failures is very much essential for protocol verification. We review some of the design principles and study some protocol failures. We will concentrate on authentication protocols.

Speaker Biography:

M. Sethumadhavan obtained his PhD (Number Theory) from Calicut Regional Engineering College. Currently, he is working as a Professor in the Department of Mathematics and Computer Science, Amrita Vishwa Vidyapeetham University, Coimbatore. He is heading TIFAC CORE in Cyber Security.



Technical Talk 5 – Jayaraj Poroor (January 18, 2012)

Formal Modeling and Analysis of Cryptographic Protocols

Abstract: Cryptographic protocols play a critical role in ensuring security in distributed systems. However, experience has shown that the design of robust and secure cryptographic protocols is extremely difficult. To quote Roger Needham, "Cryptographic protocols are three line programs that people still manage to get wrong." Formal approaches have been successfully applied in modeling and analyzing cryptographic protocols. The session will begin by reviewing the necessary background in cryptographic protocols. The Dolev Yao model will be introduced. The session will focus on protocol modeling using the applied pi-calculus and verification using the ProVerif tool. An example protocol will be taken and studied during the session.

Technical Talk 6 – Jayaraj Poroor (January 19, 2012)

Language-based Approaches to Security

Abstract: Programming languages play an important role in ensuring security of programs. For instance, type-safe languages such as Java or OCaml completely eliminate buffer-overflow vulnerabilities which constitute a serious security problem in languages such as C. Language-based approaches to security aim to use program analysis and program rewriting techniques to ensure run-time security of programs. The session will introduce the basic ideas of language-based security and then examine the roles of theorem-proving and model-checking in proving security properties.

Speaker Biography:

Jayaraj Poroor is the chief technology officer at Amrita Research Laboratories. He has led several R&D projects in the areas of secure distributed and embedded systems, sponsored by agencies such as Bhabha Atomic Research Centre, Board of Research for Nuclear Sciences, Dept. of Science & Technology, Technology Information Forecasting and Assessment Council, and Konkan Railways. His papers have appeared in reputed scholarly venues such as IEEE and Elsevier journals.

