



COLLOQUIUM

School of Computing and Software Engineering (CSE)

Subjects: Invisible Traceback over the Internet
Speaker: Dr. Wei Yu
Date: Wednesday, March 18th, 2009
Time: 2:05 PM – 3:05 PM
Place: J-201

Abstract:

The Internet's prosperity has brought convenience to our daily lives and fueled prolific network-based business across the globe. However, it has also become a breeding ground for a variety of crimes. Because crime is spreading and increasing in severity along with the fast-growing Internet, network-based forensics, in particular, a fundamental network-based forensic technique, i.e., traceback, has gained increasing importance as part of legal surveillance. Successful network forensics relies on the accuracy and invisibility of traceback techniques. Here invisibility refers to the difficulty of detecting the traceback by anyone other than the investigators. Accuracy establishes the credibility of traceback, while invisibility prevents detection and loss of a valuable means to gather legal evidence.

In this talk, he will first overview traceback techniques in the Internet and then present our newly-designed flow-marking technique for invisible traceback. The technique is based on Direct Sequence Spread Spectrum (DSSS) by utilizing a Pseudo-Noise (PN) code. By interfering with a suspect sender's traffic and marginally varying its rate, an investigator can embed a secret spread-spectrum signal into the sender's traffic. The embedded signal is carried along with the traffic from the sender to the receiver, so the investigator can recognize the corresponding communication relationship and trace the messages despite the usage of anonymous networks. The secret PN code makes it difficult for others to detect the presence of such embedded signals, so the traceback, while available to investigators, is effectively invisible to suspects. Using a combination of analytical modeling, simulations, and experiments on Tor, a popular Internet anonymous communication system, he will demonstrate the effectiveness of our DSSS-based flow marking technique for invisible traceback. I will also discuss numerous extensions and applications of our proposed techniques.

Biographical Sketch

Wei Yu received his Ph.D. degree in Computer Engineering from Department of Computer Science and Engineering at Texas A&M University in May 2008. He also received his Ph.D. degree in Electrical Engineering from Shanghai Jiaotong University in 1998. He received his B.S. degree in Computer Engineering from Nan Jing University of Technology and his M.S. degree in Electrical Engineering from Tong Ji University. Since May 2001, he has been working as a senior networking software engineer for Cisco Systems, Inc. His work at Cisco involves developing the world's leading enterprise VoIP system and has been expanded to multiple areas, including the design of VoIP protocols, call routing, security and mobility features for large enterprises. His research interests are in the areas of cyber space security, computer networks and distributed systems. His research work has been published in premier security and system conferences and journals, including the IEEE Symposium on Security and Privacy (Oakland), the IEEE Transactions on Parallel and Distributed Systems (TPDS), the IEEE International Conference on Computer Communications (INFOCOM), the IEEE International Conference on Distributed Computing Systems (ICDCS), and the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). He won the best paper award from International Conference on Communications (ICC) 2008.

Visit <http://cse.spsu.edu/colloquia> for information on past colloquia

Contacts: Dr. Venu Dasigi, vdasigi@spsu.edu and/or Susan Bentzen-Gordet, sbentzen@spsu.edu