Davetli Konuşmacılar

Mark Harris

Director of Sophos Labs, VP SophosLabs & GEO

Konu : Threat Landscape Demystified

Abstract : Mark Harris will look at the current threat landscape and highlight current trends, such as Blackhat SEO techniques and social networking threats. Mark will also present anatomy of an attack, which is a demonstration of a live malware attack. This session will show in gory detail the true capabilities of modern malware, focusing on how chains of attacks link up together.

Berry Schoenmakers

Eindhoven University of Technology
Coding and Crypto group

Konu : Secure Multiparty Computation: A Showcase for Modern Cryptography

Abstract : Modern cryptography started in the 1970s with several important developments such as the introduction of the Data Encryption Standard (DES) algorithm for computer-based encryption, and the invention of public key cryptography (Diffie-Hellman key Exchange and RSA for encryption and digital signatures). Soon after the toolkit for modern cryptographers was extended with many more intriguing tools such as blind signatures, commitments, zero-knowledge proofs, secret sharing, oblivious transfer, and many more still.

In this talk, we demonstrate how some of these modern cryptographic tools can be used to solve--often paradoxical--problems which lie at the heart of secure multiparty computation. Secure multiparty computation is about the joint computation by a set of mutually distrusting parties of any agreed upon function applied to private data supplied by these or other parties. For example, how can one compute the election result and convince anyone of the correctness of the final tally without breaching ballot secrecy, i.e., without anyone seeing the people's votes?

Jianying Zhou

Head of Network Security Group
Institute for Infocomm Research

Konu : Non-repudiation Protocols and Applications

Abstract : With more and more businesses shifting emphasis toward the Internet, new ways of protecting transacting parties are needed in the world of electronic commerce. Non-repudiation is a security service that establishes cryptographic evidence for dispute resolution of electronic transactions.

In this talk, the background that facilitated electronic commerce and the risks that hinder the popularity of electronic commerce will be introduced. Then, possible disputes arising from the paper-based business transactions and the established mechanisms supporting dispute resolution will be presented. Finally, two important issues in non-repudiation service (i.e., fairness and validity of evidence) will be discussed and various mechanisms to achieve fairness and to maintain validity of evidence will be investigated.