

Projects in Network Security with Microsoft Security Experts

- The projects will be performed as course 239999 (Project in Computer Security)
- Registration should be directed to:
 - Shai Rubin (shair@microsoft.com)
 - Tomer Shiran (tomers@microsoft.com)
 - Ron Karidi (ronkar@microsoft.com)

Project 1: Anomaly-based Malware Detection

Supervisor: Shai Rubin, PhD (shair@microsoft.com)

Background

Businesses devote significant resources to protect themselves from network attacks. Many organizations invest in attack detection systems like firewalls, network-based intrusion detection systems, and anti-virus software. Unfortunately, despite these sincere and expensive investments, network attacks continue to infect computers in almost every enterprise network.

The Problem

In this project we will try to identify infected, or compromised, machines using *network-based anomaly detection* techniques. The techniques we will develop inspect network traffic originating from a machine and classify the traffic as either *normal* or *anomalous*. For example, we will identify machines that send an unreasonable quantity of data to suspicious destinations. We assume that anomalous traffic is typically a symptom of a compromised machine.

Goals

- Describe the concepts and challenges of anomaly detection
- Design and implement an anomaly-based detection system that reads a network log file as an input and identifies suspicious (potentially compromised) machines

Requirements

In this project students will be required to get familiar and implement anomaly detection techniques based on large amount of network traffic.

- 1) Conduct a short literature survey about anomaly detection in network traffic
- 2) Implement and evaluate these techniques using a log of network traffic
- 3) Enhance known techniques and check their effectiveness on new network logs
- 4) Identify the compromised machines presented in the log file
- 5) Write a concise and self-contained report about the techniques and findings
- 6) Present the techniques and findings in a conference-like presentation

Project 2: Offline and Online Botnet Detection

Supervisor: Tomer Shiran (tomers@microsoft.com)

Background

One of the most significant threats to the Internet is the presence of large pools of compromised computers, also known as botnets, or zombie (drone) armies, sitting in homes, schools, businesses, and governments around the world. Under the control of a single hacker, commonly known as a botmaster, botnets are often used to conduct attacks ranging from Distributed Denial of Service (DDoS) to corporate espionage and spam delivery.

The Problem

In this project we will try to develop techniques to identify a bot (a machine that is part of a botnet).

Goals

- Describe the taxonomy and architecture of botnets
- Describe the actual network behavior of a specific botnet
- Play the role of a security vendor in conducting research and overcoming a specific botnet

Requirements

- 1) Conduct a short literature survey about botnets, their methods of operation, and their potential damage
- 2) Connect a vulnerable machine to the Internet so that the machine becomes infected with malware and becomes a member of a real botnet
- 3) Monitor and capture all incoming and outgoing network traffic for a few days. Analyze the captured traffic and identify the botnet-related activities. Consider questions like:
 - a. What protocols is the botnet using?
 - b. Can you identify other bots (machines that are part of the botnet) in the same botnet?
 - c. Can you identify the command and control (C&C) server of the botnet?
- 4) Develop a set of signatures for Snort (an open source Intrusion Detection and Prevention, or IDP, system) that will detect and block the botnet-related traffic
 - a. Offline (by injecting traffic into Snort)
 - b. Online (by deploying Snort between two networks)
- 5) Write a concise and self-contained report about the process and findings, and present them in a conference-like presentation

Project 3: Probabilistic Modeling of Distributed Security Systems

Supervisor: Ron Karidi, PhD (ronkar@microsoft.com)

Background

Enterprise-security solutions such as firewalls, IDS, IPS, or client protection solutions (malware detection and removal) are often stand-alone, independent solutions that are focused with one or sometimes few aspects of the enterprise security. Security-event management (SEM) systems and security-information management (SIM) systems can be seen as an attempt to consider the overall enterprise security challenge with a distributive approach. The independent endpoint solutions (firewalls, IDS, IPS, etc.) take the role of distributed agents, and the SEM engine provides the aggregation of their observations that can be used to generate alerts and take protection responses.

The Problem

In this project we will introduce the abstract concept of a distributed security system and try to propose probabilistic models for such systems. We will analyze statistical aspects of these models and try to quantify their accuracy as security-incident detection systems. We will refer to data-mining techniques such as classification and boosting.

Goals

- Describe a distributive security system as a classification system
- Analyze probabilistic aspects of distributive security system
- Design and implement a software simulation of a distributive-security probabilistic model

Requirements

- 1) Conduct a short literature survey about data-mining approaches for security systems
- 2) Propose a formal definition for a probabilistic model of a distributive security system
- 3) Implement a software simulation of the model
- 4) Propose metrics for several security aspects of the model, and quantify them for the implemented simulation
- 5) Write a concise and self-contained report about the process and findings, and present it in a conference-like presentation