COMS-W6185

Intrusion and Anomaly Detection Systems

Fall 2009
(updated June 2009)
Tuesday 4:10PM-6:00PM
8 September – 8 December
Room: 545 MUDD

Class Picture1 and Picture2

Salvatore J. Stolfo
606 CEPSR
212.939.7080

Email: sal@cs.columbia.edu
URL of sal: http://www.cs.columbia.edu/~sal
URL of IDS Lab: http://www.cs.columbia.edu/ids
(Access provided if you are a registered student.)
This course is a work in progress since the adversaries are constantly inventing new attacks for us to detect. Thank you for experimenting with me while we develop and debug the course together.

Recommended Reading (not required to be purchased):

- *Security Engineering - The Book*
  Ross Anderson
  Wiley
  [FREE ONLINE VERSION]

- *Data Mining for Security Applications.*
  Jajodia and Barbara (Eds.)
  Kluwer 2002

- *The Art of Computer Virus Research and Defense*,
  Peter Szor
  Symantec Press

- *Crimeware, Understanding New Attacks and Defenses*
  Markus Jakobsson and Zulfikar Ramzan
  Symantec Press

- *Insider Attack and Cyber Security: Beyond the Hacker*
  Springer

- *Stealing the Network: How to Own the Box*
  Russell et al
  Syngress Publishing
  ISBN: 1-931836-87-6

Recommended Readings are available on this website appearing in the “Papers and Projects” Column.
Pre- or Co-requisite: CSW4180 Network Security

SYLLABUS:

- The state of threats against computers, and networked systems
- Overview of computer security solutions and why they fail
  - Vulnerability assessment, firewalls, VPN’s
- Overview of Intrusion Detection and Intrusion Prevention
  - Network and Host-based IDS
- Classes of attacks
  - Network layer: scans, denial of service, penetration
  - Application layer: software exploits, code injection
  - Human layer: identity theft, root access
- Classes of attackers
  - Kids/hackers/sophisticated groups
  - Automated: Drones, Worms, Viruses
- A General IDS model and taxonomy
- Signature-based Solutions, Snort, Snort rules
- Assignment #1: Familiarity with Snort
- Evaluation of IDS, Cost sensitive IDS
- Anomaly Detection Systems and Algorithms
- Network Behavior Based Anomaly Detectors (rate based)
- Host-based Anomaly Detectors
  - Software Vulnerabilities
  - State transition, Immunology, Payload Anomaly Detection
- Attack trees and Correlation of alerts
- Autopsy of Worms and Botnets
- Malware detection
  - Obfuscation, polymorphism
  - Document vectors
- Email/IM security issues
  - Viruses/Spam
  - From signatures to thumbprints to zero-day detection
- Insider Threat issues
  - Taxonomy
  - Masquerade and Impersonation
  - Traitors, Decoys and Deception
- Future: Collaborative Security

Materials:

A number of materials have been gathered from open sources on the internet and provided in this course. These include slide presentations from other faculty at other universities who made their source materials openly available. In some cases the style formats were changed, but not the contents. Likewise, papers are provided for background reading that are also openly available on the internet. They have been copied and stored locally for convenience.
GRADING POLICY: Do quality work, and don’t cheat, and you will get an A. If you cheat you will get an F. See the Department’s Academic Honesty Policy.

NO FINAL EXAMINATION.

DETAILED COURSE SCHEDULE:

<table>
<thead>
<tr>
<th>Session</th>
<th>Date</th>
<th>Topic/chapter</th>
<th>Papers and Projects</th>
</tr>
</thead>
</table>
| 1       | 9/8  | Overview of Course | Failure of Security – background (May 2006)  
Introduction to IDS  
CERT-Guidelines\CERT-CC Intruder Detection Checklist.htm  
CERT-Guidelines\CERT®-CC Steps for Recovering from a UNIX or NT System Compromise.htm  
CERT-Guidelines\List of Security Tools.htm  
CERT-Vulnerability Stats  
Common Exploited Ports: http://www.iss.net/security_center/advice/Exploits/Ports/default.htm  
FBI reports Cybercrime eclipsed $200MM in 2007  
Threat Reports (2007-2008):  
Sans TOP 20 Threat Report  
Symantec Security Threat Reports  
P-Secure End of 2007 Report, The Storm Botnet  
McAfee Report on Malicious Websites 2008  
Verizon 2008 Data Breach Investigations Report  
Verizon 2009 Data Breach Investigations Report  
Sohpos 2008 Security Report  
Cyberwar  
Overview of network analytics circa 09 |
<p>| 2       | 9/15 | Failure of | Software_Vulnerabilities – Landwehr’s 1994 paper |</p>
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Course Material</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 9/22</td>
<td>Snort Intro</td>
<td><a href="http://www.snort.org/">http://www.snort.org/</a></td>
</tr>
<tr>
<td></td>
<td>Snort Installation</td>
<td><a href="http://www.snort.org/dl/">http://www.snort.org/dl/</a></td>
</tr>
<tr>
<td></td>
<td>TCP_Wrapper</td>
<td>Roesch paper on Snort</td>
</tr>
<tr>
<td></td>
<td>netfilter and iptables</td>
<td>Tcpdump pocket guide</td>
</tr>
<tr>
<td></td>
<td>General IDS Model and Evaluation of IDS’s</td>
<td>Project #1-snort/network project</td>
</tr>
<tr>
<td>4 9/29</td>
<td>General IDS Model and Evaluation of IDS’s</td>
<td>A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems</td>
</tr>
<tr>
<td></td>
<td>Automatically Computing IDS Models (Accuracy): Data Mining-based IDS</td>
<td>Data Mining-based Intrusion Detectors</td>
</tr>
<tr>
<td></td>
<td>Performance (Speed) Cost-sensitive IDS</td>
<td>Public Machine Learning Code: Weka</td>
</tr>
<tr>
<td></td>
<td>Scans/probes</td>
<td>Stealthy Surveillance Detection</td>
</tr>
<tr>
<td>5 10/6</td>
<td>Scans/probes</td>
<td>Defending Against Denial of Service Attacks in Scout 1999</td>
</tr>
<tr>
<td></td>
<td>Why 6?</td>
<td>Statistical Modeling background</td>
</tr>
<tr>
<td>Date</td>
<td>Topic</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td></td>
</tr>
</tbody>
</table>
| **6 10/13** | Sense of Self  
Taint Analysis  
Pointer Taint Analysis Fails  
Project #1 Due |
| **6 10/13** | Unsupervised Anomaly Detection  
Summary Unsupervised Anomaly Detection  
Spectrogram  
Network based Anomaly Detection (Ke’s list)  
Unsupervised Anomaly Detection  
NBAD  
Modeling System Calls for Intrusion Detection with Dynamic Window Sizes  
Project #2 – lipcap/winpcap/tcp_wrappers host project |
| **7 10/20** | Autopsy of network Worms  
Worms and Payload AD/PAYL  
Layered Defenses  
Code Red Analysis  
http://www.eeye.com/html/Research/Advisories/AL20010804.html  
Spread of Sapphire/Slammer  
Anatomy of the Network Worm  
Flash and Stealthy Worms and the Warhol Worm  
Abstract Payload Execution |
| **8 10/27** | GUEST LECTURE  
Joel Rosenblatt, Manager Computer&Network Security, Columbia University  
Security Metrics: A Solution in Search of a Problem  
Security Models From Corporate to ISP: one size does not fit all |
| **9 11/4** | NO CLASS  
Election Day |
| **10 11/10** | Advanced Threats  
Mimicry Attack/Anagram  
Futility of Modeling Polymorphic Shellcode  
Anomaly Detection of Web-based Attacks  
NIDAR |
<table>
<thead>
<tr>
<th>Training Strategy for AD: <strong>STAND</strong></th>
<th>Signatures are Dead, Whitelisting is in Online Malware Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Polymorphic Threat</strong></td>
<td><a href="http://pandalabs.pandasecurity.com/archive/Another-trojan-creator_2E002E002E00_.aspx">http://pandalabs.pandasecurity.com/archive/Another-trojan-creator_2E002E002E00_.aspx</a></td>
</tr>
<tr>
<td><strong>Correlation</strong> (Alert Sharing, Attack Trees, Sensor Correlation)</td>
<td><a href="http://www.offensivecomputing.net/">http://www.offensivecomputing.net/</a></td>
</tr>
<tr>
<td><strong>CV5</strong></td>
<td><a href="http://www.viruspool.net/virus.cms">http://www.viruspool.net/virus.cms</a></td>
</tr>
<tr>
<td><strong>Collaborative Security and Application Communities</strong></td>
<td><a href="http://vx.netlux.org/v1.php">http://vx.netlux.org/v1.php</a></td>
</tr>
<tr>
<td><strong>Darpa Application Communities</strong></td>
<td>Correlation Engine-SRI</td>
</tr>
<tr>
<td><strong>Collaborative Distributed Intrusion Detection</strong></td>
<td>Process Query System</td>
</tr>
<tr>
<td><strong>Application Communities-Patching</strong></td>
<td>BlackBook Chapter</td>
</tr>
<tr>
<td><strong>Worminator</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>Project #2 DUE</strong></td>
<td>Worminator</td>
</tr>
<tr>
<td><strong>11/17</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>11/24</strong></td>
<td>Worminator</td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>Masqueraders, Impersonators</strong></td>
<td>Worminator</td>
</tr>
<tr>
<td>(Goldring and Feature Sets)</td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>One-class training Insider Taxonomy</strong></td>
<td>Worminator</td>
</tr>
<tr>
<td><strong>Masquerader Research (Core dump)</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>CMU/SEI Insider Threat Study 2005</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>US Navy report on Insider Attack of a Crypto System 2005</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>US Secret Service Insider Threat Study</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>Outside attack due to insider mistakes</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>Very close to home:</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>ATT Masquerade Schonlau Data set</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td><strong>Mitre’s ELICIT System – RAID 07</strong></td>
<td>Collaboratively Fighting Fraud (FSTC with stats)</td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>12/1</td>
<td>Decoy Networking</td>
</tr>
<tr>
<td></td>
<td>Insider Threat overtakes Virus Threat Sep 07</td>
</tr>
<tr>
<td></td>
<td>Project# 3 - decoys and deception</td>
</tr>
<tr>
<td></td>
<td>Host Sensor Download Site for Project#3</td>
</tr>
<tr>
<td></td>
<td>Background on Modeling</td>
</tr>
<tr>
<td>12/8</td>
<td>LAST CLASS EPILOGUE:</td>
</tr>
<tr>
<td></td>
<td>Security in 30 minutes</td>
</tr>
<tr>
<td></td>
<td>Advanced Malware Threats-2008</td>
</tr>
<tr>
<td></td>
<td>Issues Regarding Law and Privacy</td>
</tr>
<tr>
<td></td>
<td>Large Corporate Risk Management Process</td>
</tr>
<tr>
<td></td>
<td>IT Security: Law Enforcement Response</td>
</tr>
<tr>
<td></td>
<td>Crime Does not Pay: Hacker, Counterfeiter Comes Clean Ahead of Prison Stint</td>
</tr>
<tr>
<td></td>
<td>Final Paper – **The Field of Cyber Security Circa 2005</td>
</tr>
<tr>
<td>12/11</td>
<td>FINAL PROJECT DUE</td>
</tr>
</tbody>
</table>

**TA DETAILS: TBA**

Name: YINGBO SONG  
Office: 604 CEPSR  
Phone:  
E-mail: yingbo@cs.columbia.edu  
URL: www.cs.columbia.edu/~yingbo  
TA office hours: TBA

**GRADE DISTRIBUTION:**

Final grades are curved. The distribution is

```
   HW/Test Percentage
Project #1  33%  
Project #2  33%  
Project #3  34%  
```