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
ISBN 0-321-30545-3

Crimeware, Understanding New Attacks and Defenses
Markus Jakobsson and Zulfikar Ramzan
Symantec Press
ISBN: 978-0-321-50195-0 2008

Insider Attack and Cyber Security: Beyond the Hacker
S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, S. Smith, eds.
Springer
ISBN-13: 978-0-387-77321-6 2008

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:

ession	Date	Topic/chapter	Papers and Projects
1	9/8	Overview of Course Scale of security problem Attacks and Attackers – See Threat Reports	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 Cost of Cybercrime Doubles 2007: http://www.darkreading.com/document.asp?doc_id=133658&f_src=darkreading_section_29 Reasons for Cyberattacks – Miscreant Wealth http://www.darkreading.com/document.asp?doc_id=151736&f_src=drdaily FBI reports Cybercrime eclipsed $200MM in 2007 Threat Reports (2007-2008): Sans TOP 20 Threat Report Symantec Security Threat Reports F-Secure End of 2007 Report, The Storm Botnet Worldwide Infrastructure Security Report 2007 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
2	9/15	Failure of	Software Vulnerabilities – Landwehr's 1994 paper

		Software Security Failures of Network function protocols IDS Taxonomy	Writing Buffer overflow attacks 2002 Top 25 Common Software Programming Errors Design Flaws: DNS Cache Poisoning Protocol Flaws: BGP MITM Attacks 2008 Early Penetration ‘Testing: SATAN 1994 Early NIDS-1994 Early Taxonomy of IDS: IDS Taxonomy NIST Special Publication on IDS An Overview Overview of Attacks 2001
3	9/22	Snort Intro Snort Installation TCP_Wrapper netfilter and iptables	http://www.snort.org/ http://www.snort.org/dl/ Roesch paper on Snort Tcpdump pocket guide Project #1-snort/network project
4	9/29	General IDS Model and Evaluation of IDS’s Automatically Computing IDS Models (Accuracy): Data Mining-based IDS Performance (Speed) Cost-sensitive IDS	A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems Data Mining-based Intrusion Detectors Public Machine Learning Code: Weka Denning Model on IDS DARPA IDS Evaluations Methodology for Quantifying Security Investments
5	10/6	Scans/probes Host-based Anomaly Detection Why 6?	Stealthy Surveillance Detection Defending Against Denial of Service Attacks in Scout 1999 Cisco Netflow: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html Statistical Modeling background

			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

		Training Strategy for AD: STAND Polymorphic Threat Correlation (Alert Sharing, Attack Trees, Sensor Correlation) CV5 Collaborative Security and Application Communities Darpa Application Communities	Signatures are Dead, Whitelisting is in Online Malware Sources http://pandalabs.pandasecurity.com/archive/Another-trojan-creator_2E002E002E00_.aspx http://www.offensivecomputing.net/ http://www.viruspool.net/virus.cms http://vx.netlux.org/vl.php Correlation Engine-SRI Process Query System BlackBook Chapter Collaborative Distributed Intrusion Detection Collaboratively Fighting Fraud (FSTC with stats) Worminator Application Communities-Patching Project #2 DUE
11	11/17	Stealthy Malcode embedded in documents Email: Misuse, Spam, Viruses The Botnet Threat	VOIP-enabled SPAM Stegonography Site with Tools Why Fishing Works Detecting Viral Propagations Using Email Behavior Profiles Detecting Botnets Using Bot Behavior Profiles Supply Chain malfeasance, 2008 sales by Botnets
12	11/24	Overview Masqueraders, Impersonators (Goldring and Feature Sets) One-class training Insider Taxonomy	Masquerader Research (Core dump) CMU/SEI Inisder Threat Study 2005 US Navy report on Insider Attack of a Crypto System 2005 US Secret Service Insider Threat Study Outside attack due to insider mistakes Very close to home: ATT Masquerade Schonlau Data set Mitre's ELICIT System – RAID 07

13	12/1	Decoy Networking	Insider Threat overtakes Virus Threat Sep 07 Project# 3 - decoys and deception Host Sensor Download Site for Project#3 Background on Modeling
14	12/8	**LAST CLASS** **EPILOGUE:** Security in 30 minutes	Advanced Malware Threats-2008 Issues Regarding Law and Privacy Large Corporate Risk Management Process IT Security: Law Enforcement Response Crime Does not Pay: Hacker, Counterfeiter Comes Clean Ahead of Prison Stint Final Paper – **The Field of Cyber Security Circa 2005
	12/11	**FINAL PROJECT DUE**	

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%