

CSW6185

***Intrusion and Anomaly Detection
Systems***

Fall 2008

(updated June 2008)

Tuesday 4:10PM-6:00PM

2 September – 2 December

Room: TBA MUDD

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>

URL of this password protected page:

<http://www.cs.columbia.edu/~sal/IDS/Fall06/index.html>

(Access provided if you are a registered student.)



This is the fourth time this course is offered.
It 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
- 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:

Session	Date	Topic/chapter	Papers and Projects
1	9/2	Overview of Course Scale of security problem Attacks and Attackers	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_296 Reasons for cyberattacks – Miscreant Wealth http://www.darkreading.com/document.asp?doc_id=151736&f_src=drdaily Threat Reports: Sans TOP 20 Threat Report Symantec Security Threat Reports McAfee Report on Malicious Websites 2008 Worldwide Infrastructure Security Report 2007 Cyberwar
2	9/9	Failure of Software Security IDS Taxonomy	Software Vulnerabilities – Landwehr's 1994 paper Writing Buffer overflow attacks 2002 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	9/16	Snort Intro Snort Installation	http://www.snort.org/ http://www.snort.org/dl/ Roesch paper on Snort Tcpdump pocket guide Project #1-snort/network project
4	9/23	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
5	9/30	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 Project #1 Due
6	10/7	Unsupervised Anomaly Detection	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	10/14	Autopsy of network Worms	Layered Defenses Code Red Analysis http://www.eeye.com/html/Research/Advisories/AL20010804.html

		Worms and Payload AD/PAYL	Spread of Sapphire/Slammer Anatomy of the Network Worm Flash and Stealthy Worms and the Warhol Worm
8	10/21	<p>Advanced Threats</p> <p>Mimicry Attack/Anagram</p> <p>Training Strategy for AD: STAND</p> <p>Polymorphic Threat</p>	<p>Malicious Payload Detection and Buffer Overflow Code Detection</p> <p>Futility of Modeling Polymorphic Shellcode: http://mice.cs.columbia.edu/getTechreport.php?techreportID=444&format=pdf&</p> <p>Anomaly Detection of Web Based Attacks</p> <p>NIDAR</p> <p>Online Malware Sources: www.offensivecomputing.net http://www.viruspool.net/virus.cms http://vx.netlux.org/vl.php</p> <p>Signatures Obsolete, White-/Black-/Gray-listing is in</p>
9	10/28	<p>Correlation Attack Trees and CV5</p> <p>Process Identification</p> <p>Collaborative Security and Application Communities</p> <p>Self-Repairing Software and Application Communities</p>	<p>aLADS Correlation Engine</p> <p>Correlation Engine-SRI</p> <p>Process Query System</p> <p>Fighting Fraud...sharing across domains</p> <p>BlackBook Chapter</p> <p>Collaborative Distributed Intrusion Detection</p> <p>Worminator</p> <p>Dshield Alert Sharing Site: http://www.dshield.org/indexd.html</p> <p>Project #2 DUE.</p>
10	11/4	NO CLASS	ELECTION DAY
11	11/11	<p>Stealthy Malcode embedded in documents</p>	<p>SPAM</p> <p>VOIP-enabled SPAM</p> <p>Why Fishing Works</p>

		Email: Misuse, Spam, Viruses	Detecting Viral Propagations Using Email Behavior Profiles
12	11/18	Insider Problem Traitors, Masqueraders, Impersonators One-class training	CMU/SEI Insider Threat Study 2005 US Navy report on Insider Attack of a Crypto System 2005 US Secret Service Insider Threat Study Very close to home: http://www.darkreading.com/document.asp?doc_id=151052&f_src=drdaily Masquerade Detection and One-class ATT Masquerade Data set Mitre's ELICIT System – RAID 07
13	11/25	Decoy Networking TAXONOMY	Insider Threat overtakes Virus Threat Sep 07: http://www.techworld.com/security/news/index.cfm?newsID=10082 Project # 3- decoys and deception
14	12/2	LAST CLASS EPILOGUE: Security in 30 minutes	ISSUES REGARDING THE LAW and PRIVACY IT Security: Law Enforcement Response Final Paper – **The Field of Cyber Security Circa 2005**
	12/16	FINAL PROJECT DUE	

TA DETAILS:

Name: Leon Wu
Office: 6LE1 CEPSR
Phone: (646) 266-3323
E-mail: leon@cs.columbia.edu
URL: <http://www1.cs.columbia.edu/~leon>
TA office hours: 4:10pm-6:10pm Friday

GRADE DISTRIBUTION:

Final grades are curved. The distribution is

HW/Test	Percentage
Project #1	30%
Project #2	30%
Project #3	40%
