CSCI 6900

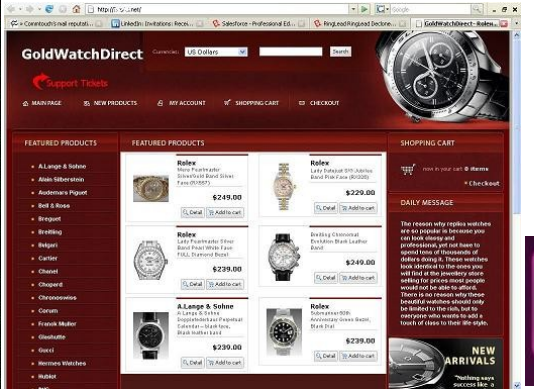
Computer Network Attacks and Defenses

Lecture 2: Overview of research topics in computer and network security (part B)

Instructor: Prof. Roberto Perdisci

Spam Detection

- SPAM = Unsolicited bulk messages
  - email spam, blog spam, **social network** spam
  - new email spam sent via **Gmail/Hotmail**...
- Detection strategies
  - content analysis (headers, body, images...)
  - network-level sender characteristics
    - e.g., IP reputation, sender behavior...



Intrusion Detection

- Detect attempted and successful attacks
- Types of IDS
  - host-based: monitor system events
  - network-based: monitor network traffic
  - signature-based (or misuse-based): rely on attack models
  - anomaly-based: rely on

    a model of normal events
  - hybrid approaches
  - IDS vs. IPS

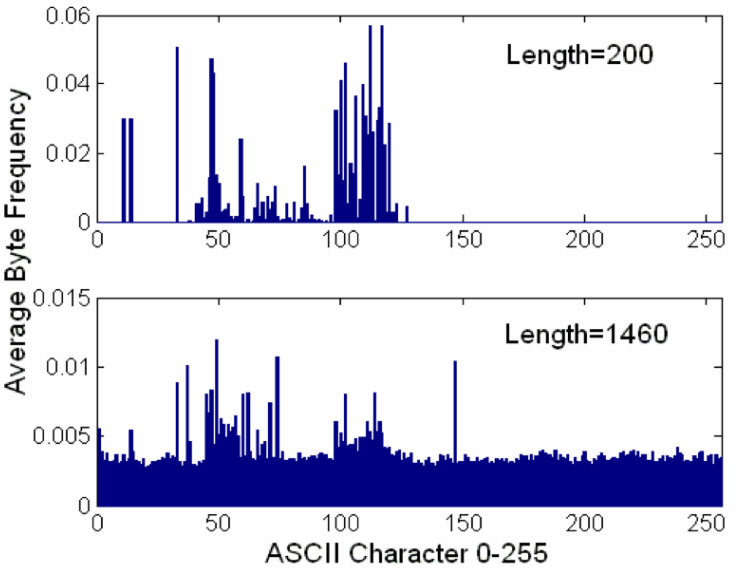
Intrusion Detection

- Example of signature-based network intrusion detection (www.snort.org)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MALWARE"; flow: to_server,established; content:"POST"; depth: 4; content:"srng/reg.php HTTP"; within: 50; content:"|0d0a|Host|3a|"; content:"2020search.com"; within: 40; content:"IpAddr="; nocase; within: 100; classtype: trojan-activity; sid: 2000934; rev:5;)

- Example of anomaly-based network intrusion detection system (PAYL)

GET /en/html/foo.php HTTP/1.1
User-Agent: Mozilla/5.0 Firefox/1.5.0.11
Host: www.example.com
Accept: text/xml,text/html;
Accept-Language: **A{~!b@#9#0)(@>?**
Accept-Encoding: gzip,deflate
Connection: keep-alive
Referrer: http://example.com



Vulnerability Discovery and Protection

- Automatically finding software bugs
- Automatic construction of vulnerability signatures from exploits
- Automatically building patches

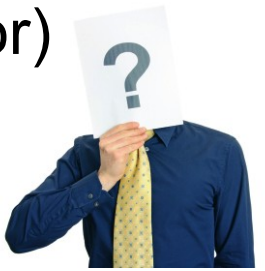
- Patch-based exploit construction
- Improving OS Security (e.g., DEP, ASLR...)
- Sandboxing/Virtualization

Web 2.0 Security

- Browser architecture/sandboxing
- Browser security policies
- Secure *mashups*
- Javascript security
  - static and dynamic analysis of code
  - e.g., automatic gadget security analysis

Privacy and Anonymity

- Information leakage in online social networks
- De-anonymizing public datasets
  - Netflix, Genomic Data, ...
- Attacking the confidentiality of encrypted communications
  - Inferring the language in VoIP conversations
  - Inferring content from HTTPS communications
- Communication (de-)anonymization
  - Mix networks
  - Improving/Attacking onion routing (e.g., Tor)
  - Traffic watermarking



Other topics

- Physical Security
  - Identifying keystrokes from audio
  - retrieving encryption keys from memory
  - seeing what other people are watching using reflections
- Wireless/Cellular Network Security
- RFID Security
- VoIP Security
- Cryptography/Crypto-analysis
- Electronic Voting Systems
- ... and many others ...

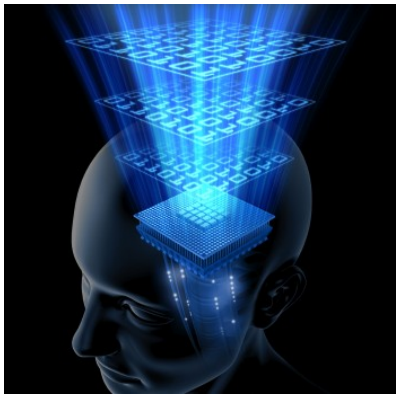
How do we choose a good research topic?

Think!

- What topics inspire you?
- Read as much as you can about them
- Not only academic papers
  - E.g.: interested in malware? Subscribe to malware/security blogs
    - SANS Internet Storm Center
    - Microsoft Malware Protection Center
    - Panda Research Blog
    - Krebs on Security
    - etc.
  - Stay up-to-date with real, current problems

Leverage you knowledge!

- Think about things you are very good at
  - System programming (C/C++, Assembly)?
  - System building?
  - Theory?
  - Algorithms?
  - Machine Learning, AI?



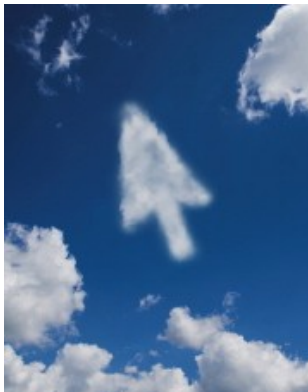
- While reading previous work, think about how your skills could help you solve an open problem

Problems that will likely grow big!

- Nobody can predict the future
- Look at what other people are working on
  - see what people at CMU, Berkeley, Stanford, GTISC, Wisconsin, UCSB, UIUC, etc., are doing
  - if a number of people are working in a particular (sub-)area, it must be of interested
  - try to see whether there is any emerging problem, with a *not too big* list of previous works
  - is there still something we can say about the topic, can we explore the problem from a new angle?
  - Depart from conventional thinking

Some topics are very hot!

- Malware Defense
  - current solutions are failing
  - detection is important
  - defense is even more important!
- Web Security
  - browsers are becoming a platform for applications
  - they are the most common Internet application
  - ... and they expose plenty of vulnerabilities!
- Cloud computing: is this the future?
  - security in the cloud
  - data privacy



Logistics

- Classroom changes: **GSRC 208** (M), HH 101 (TR)
- Reminder (if you have not yet done so...)
  - Please send me an email with
    - Name, PhD/MSc, year, advisor
    - Email needed to send out last-minute announcements
- **Choose 3 papers from the following list by 8/20**
  - http://www.cs.uga.edu/~perdisci/CSCI6900-F10/Paper_List.html
  - Papers the have been already chosen are marked accordingly

Next Time

- Monday 8/23
  - BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection
  - **Read the paper** (no review required)