COSC 734: Network Security
Chapter 9 - Intrusion

Dr. Wei Yu
Dept. of Computer and Information Sciences
Towson University
Email: wyu@towson.edu

Review: Classify Security Attacks

- **Passive attacks -** eavesdropping on, or monitoring of, transmissions to
  - Obtain message contents
  - Monitor traffic flows
- **Active attacks** – modification of data stream to
  - Masquerade of one entity as some other
  - Replay previous messages
  - Modify messages in transit
  - Denial of service

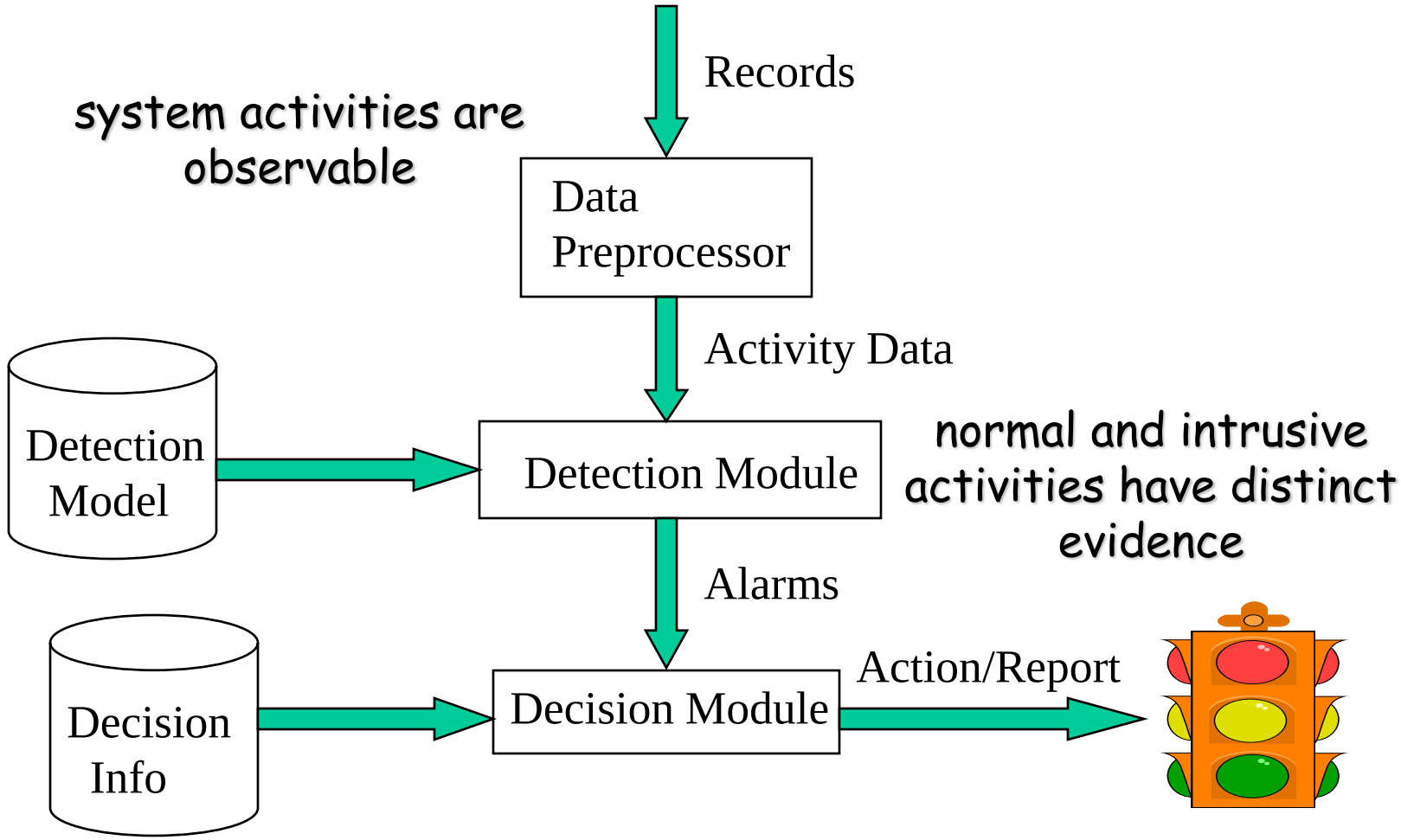
Outline

- Intrusion
- Intrusion detection system (IDS)
- Types of IDS
- Password protection

Definitions

- Intrusion
  - A set of actions aimed to compromise the security goals
    - Integrity, confidentiality, availability …
    - Computation and network resources
- Intrusion detection system (IDS)
  - The process of identifying and responding to intrusion activities
- Intrusion prevention system (IPS)
  - Extension of IDS with exercises of access control to protect system from exploitation

Components of Intrusion Detection System



Intrusion Detection Approaches

- Modeling
  - Features: **evidences** extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (signature-based)
    - Anomaly detection
- Deployment
  - Network based: monitor network traffic
  - Host based: monitor computer processes

Intruders

- Significant issue for networked systems is hostile or unwanted access
- Either through network or local system
- Can identify classes of intruders:
  - Masquerader: An individual who is not authorized to use the computer (outsider)
  - Misfeasor: A legitimate user who accesses unauthorized data, programs, or resources (insider)
  - Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection (either)
- Varying levels of competence:
  - Intruder attacks range from the benign (simply exploring network to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system).

Intruders

- Clearly a growing publicized problem
  - From “Wily Hacker” in 1986/87
  - To clearly escalating CERT stats
- Range
  - Benign: explore, still costs resources
  - Serious: access/modify data, disrupt system
- Led to the development of **computer emergency response teams (CERTs)**
  - These cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers.
- Intruder techniques & behavior patterns constantly shifting, have features
  - Exploits newly discovered weakness and to evade detection (**example?)**
  - Even so, intruders typically follow one of a number of recognizable behavior patterns, and these patterns typically differ from those of ordinary users.

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing / cracking passwords
- Copying viewing sensitive data / databases
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access net
- Impersonating a user to reset password
- Using an unattended workstation

Hackers

- Motivated by thrill of access and status
  - Hacking community a strong meritocracy
  - Status is determined by level of competence
- Benign intruders might be tolerable
  - Do consume resources and may slow performance
  - Can't know in advance whether benign or malign
- IDS / IPS / VPNs can help counter
  - Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are designed to counter this type of hacker threat. In addition to using such systems, organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network technology.
- Awareness led to establishment of CERTs
  - Collect / disseminate vulnerability info / responses: hacker can gain access to CERT report as well.
  - Internet threat monitoring system.

Hacker Behavior Example

- The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures.
- Even so, intruders typically follow one of a number of recognizable behavior patterns, and these patterns typically differ from those of ordinary users
  - Select target using IP lookup tools
  - Map network for accessible services
  - Identify potentially vulnerable services
  - Brute force (guess) passwords
  - Install remote administration tool
  - Wait for admin to log on and capture password
  - Use password to access remainder of network

Criminal *Enterprise*

- Organized groups of hackers have become a widespread and common threat to Internet-based systems
  - Corporation / government / loosely affiliated gangs
  - Typically young
  - Often Eastern European or Russian hackers
  - Often target credit cards on e-commerce server
- Whereas traditional hackers look for targets of opportunity, criminal hackers usually have specific targets, or at least classes of targets in mind
  - Once a site is penetrated, the attacker acts quickly, scooping up as much valuable information as possible and exiting.
- IDSs and IPSs can also be used for these types of attackers, but may be less effective because of the quick in-and-out nature of the attack
  - Prioritize the system component (e.g., sensitive data needs strong protection)

Criminal Enterprise Behavior

Summarize the example of criminal enterprise behavior

1. Act quickly and precisely to make their activities harder to detect
2. Exploit perimeter through vulnerable ports or applications
3. Use Trojan horses (hidden software) to leave back doors for re-entry
4. Use sniffers to capture passwords
5. Do not stick around until noticed
6. Make few or no mistakes

Insider Attacks

- Among most difficult to detect and prevent
- Employees have access & systems knowledge
- May be motivated by revenge / entitlement
  - When employment terminated
  - Taking customer data when move to competitor
  - Example: Kenneth Patterson, fired from his position as data communications manager for American Eagle Outfitters. Patterson disabled the company's ability to process credit card purchases during five days of the holiday season of 2002.
  - Example: Contractor launches an attack on a sewage control system in Queensland in 2000; Damage: more than 750,000 gallons of untreated sewage released into parks, rivers, and hotel grounds
- IDS / IPS may help but also need:
  - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Insider Behavior Examples

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn't normally use for their daily jobs
3. E-mail former and prospective employers
4. Conduct furtive instant-messaging chats
5. Visit web sites that cater to disgruntled employees, such as f'dcompany.com
6. Perform large downloads and file copying
7. Access the network during off hours.

Intrusion Techniques

- Aim to gain access and/or increase privileges on a system
- Often use system / software vulnerabilities
- Key goal often is to acquire passwords
  - So then exercise access rights of owner
- Basic attack methodology
  - Target acquisition and information gathering
  - Initial access
  - Privilege escalation
  - Covering tracks

Intrusion Stages

- Intelligence gathering
  - Probing the system to determine vulnerabilities
- Planning
  - Deciding what resource to attack and how
- Attack execution
- Hiding
  - Covering traces of the attack
- Preparation for future attacks
  - Install “back doors” for unhindered access

Password Guessing Attack

- One of the most common attacks
- Attacker knows a login (from email/web page etc)
- Then attempts to guess password for it
- Defaults, short passwords, common word searches
  - User info (variations on names, birthday, phone, common words/interests)
  - Exhaustively searching all possible passwords
- Check by login or against stolen password file
- Success depends on password chosen by user
- Surveys show many users choose poorly

Password Capture

- Another attack involves password capture
  - Watching over shoulder as password is entered
  - Using a Trojan horse program to collect
  - Monitoring an insecure network login using sophisticated network monitoring tools
    - eg., telnet, FTP, web, email
  - Extracting recorded info after successful login (web history/cache, last number dialed etc)
- Using valid login/password can impersonate user
- Users need to be educated to use suitable precautions/countermeasures
  - Beware of unknown source s/w, to use secure network connections (HTTPS, SSH, SSL), to flush browser/phone histories after use etc.

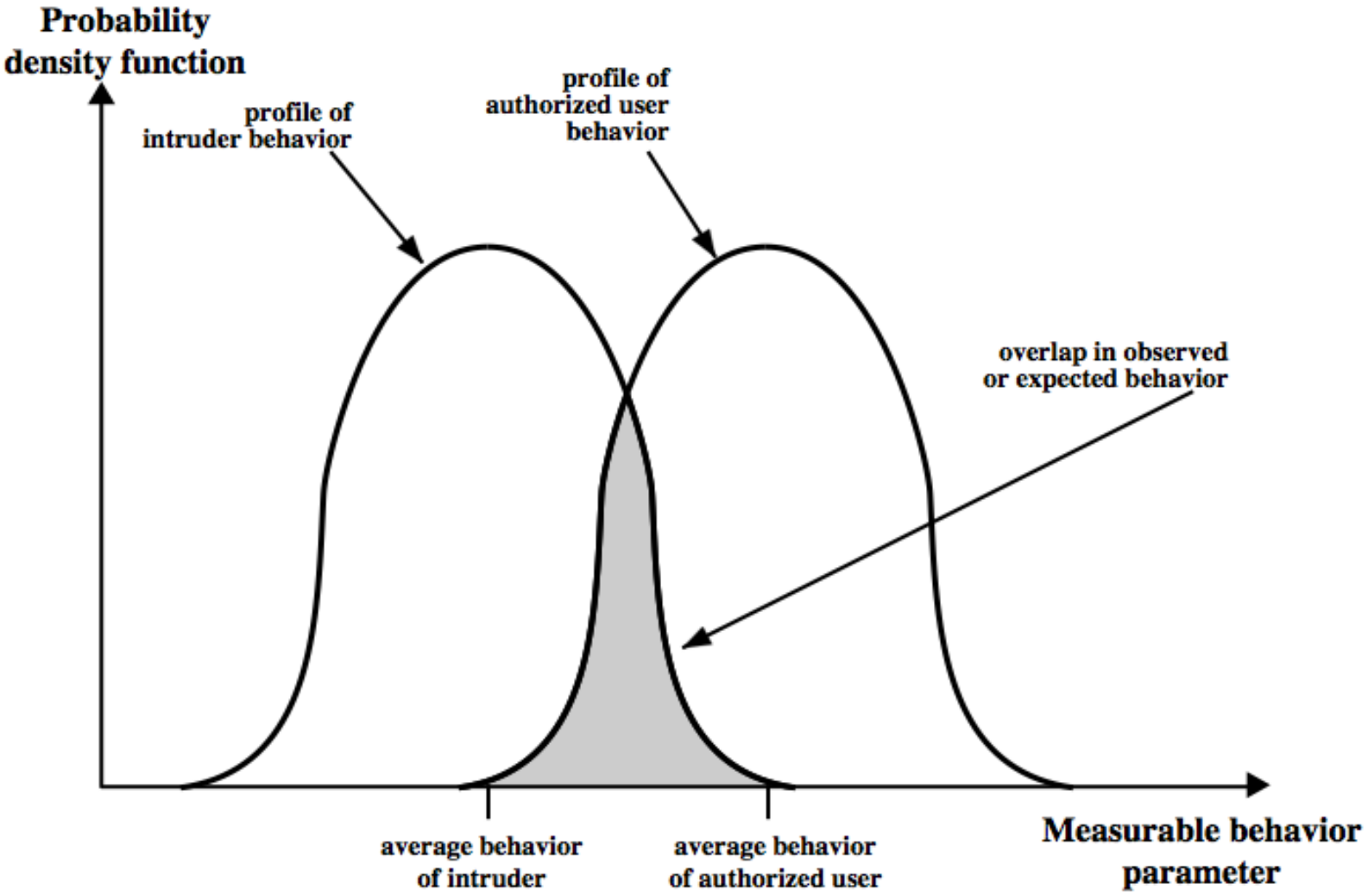
Intrusion Detection

- Inevitably the best intrusion prevention system will fail
- We need also to detect intrusions as the system's second line of defense, so we can
  - Block access & minimize damage if detected quickly
  - Act as deterrent given chance of being caught
  - Or can collect info on intruders to improve future security
- Intrusion detection is based on the assumption
  - Behavior of the intruder differs from that of a legitimate user in ways that can be quantified.
  - Will this always a valid assumption?

Intrusion Detection

- Detect if attacks are being attempted, or if system has been compromised
- Desirable features
  - Accuracy
  - Fast
  - Flexible, general
  - Results easy to understand

Intrusion Detection



How to Measure IDS Accuracy

- Events are actions occurring in the system (file accesses, login attempts, etc.)
  - An intrusion (I) is an event that is part of an attack
  - an alarm (A) is generated if an event is diagnosed as being an intrusion

	Intrusion	Not an Intrusion
Alarm Generated	True positive	False positive
Alarm Not Generated	False negative	True negative

How to Measure IDS Accuracy

- True positive rate: **fraction of intrusions correctly diagnosed (detected)**
- False negative rate: fraction of intrusions incorrectly diagnosed (not detected)
  - FNR = 1 - TPR
- True negative rate: fraction of non-intrusions correctly diagnosed
- False positive rate: **fraction of non-intrusions incorrectly diagnosed**
  - FPR = 1 – TNR

Example 1

- Her is a scenario

Say the IDS system in one organization generates *70,000 events*, *300 intrusions*, *2800 alarms (of which 298 are correct diagnoses, 2502 are incorrect)*

Example 1

- Scenario: 70,000 events, 300 intrusions, 2800 alarms (of which 298 are correct diagnoses, 2502 are incorrect)

- **TPR: 298 / 300 = 99.3%**
- FNR: 0.7%
- **TNR: (70000 - 300 - 2502) / (70000 - 300) = 96.4%**
- FPR: 3.6%
  - 2502/(70000-300)

Example 2

Here is another scenario

To detect malware on mobiles, our detection system use 200 applications, 100 are malware, 100 are good (benign). Say you develop an "IDS" algorithm and issue 110 alert events (where 90 are from true malware, and 20 are misclassifying)

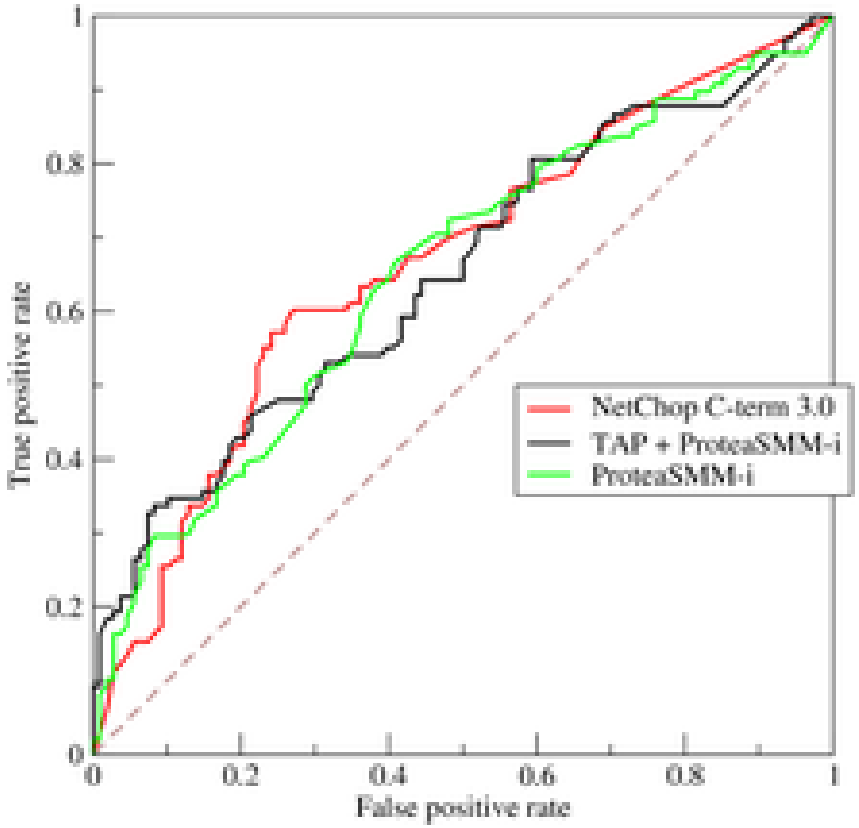
- What's the true positive and false positive rates?

Tradeoffs

- It’s trivial to have 100% TPR, and trivial to have 0% FPR
  - how?
- What about to achieve both?
  - Idea?
  - Tradeoffs

Receiver Operating Characteristic (ROC)

- True positive rate vs. False positive rate



http://en.wikipedia.org/wiki/Receiver_operating_characteristic

Receiver Operating Characteristic (ROC)

- True positive rate vs. False positive rate

In signal detection theory, a receiver operating characteristic (ROC), or simply ROC curve, is a graphical plot which illustrates the performance of a binary classifier system as its discrimination threshold is varied.

It is created by plotting the fraction of true positives out of the positives (TPR = true positive rate) vs. the fraction of false positives out of the negatives (FPR = false positive rate), at various threshold settings.

TPR is also known as sensitivity, and FPR is one minus the specificity or true negative rate.

Receiver Operating Characteristic (ROC)

		actual value		
		p	*n*	total
prediction outcome	*p'*	True Positive	False Positive	P'
	n'	False Negative	True Negative	N'
	total	P	N	

http://en.wikipedia.org/wiki/Receiver_operating_characteristic

Please read it offline

A

TP=63	FP=28	91
FN=37	TN=72	109
100	100	200

TPR = 0.63

FPR = 0.28

B

TP=77	FP=77	154
FN=23	TN=23	46
100	100	200

TPR = 0.77

FPR = 0.77

C

TP=24	FP=88	112
FN=76	TN=12	88
100	100	200

TPR = 0.24

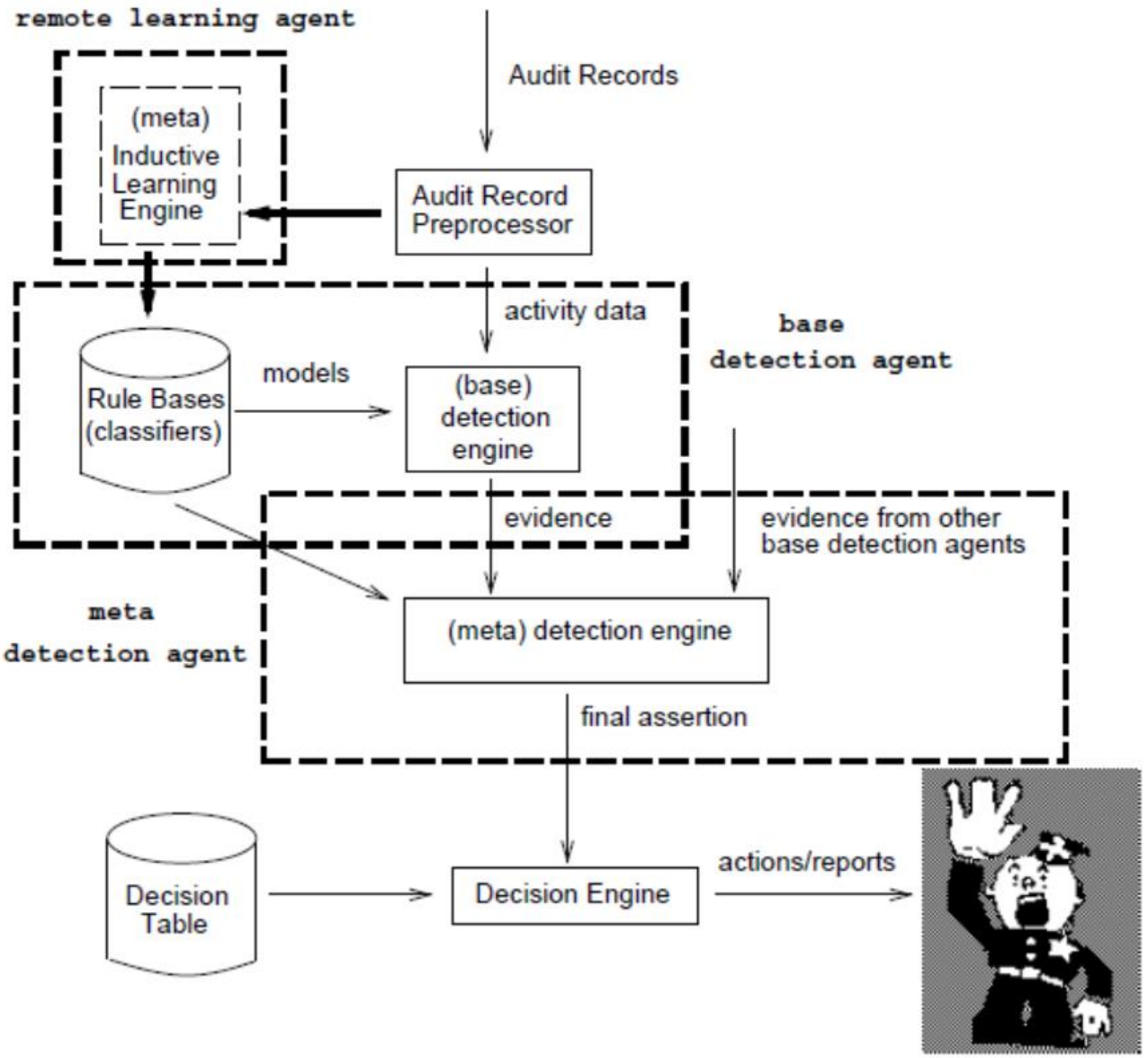
FPR = 0.88

Reading Material

1. Dorothy E. Denning, An Intrusion Detection Model, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, 1987
2. Wenke Lee and Salvatore J. Stolfo, “Data Mining Approaches for Intrusion Detection,” In Proceedings of the Seventh USENIX Security Symposium (SECURITY '98), San Antonio, TX, January 1998.

In Blackboard – Please read both papers (even both are relatively old)

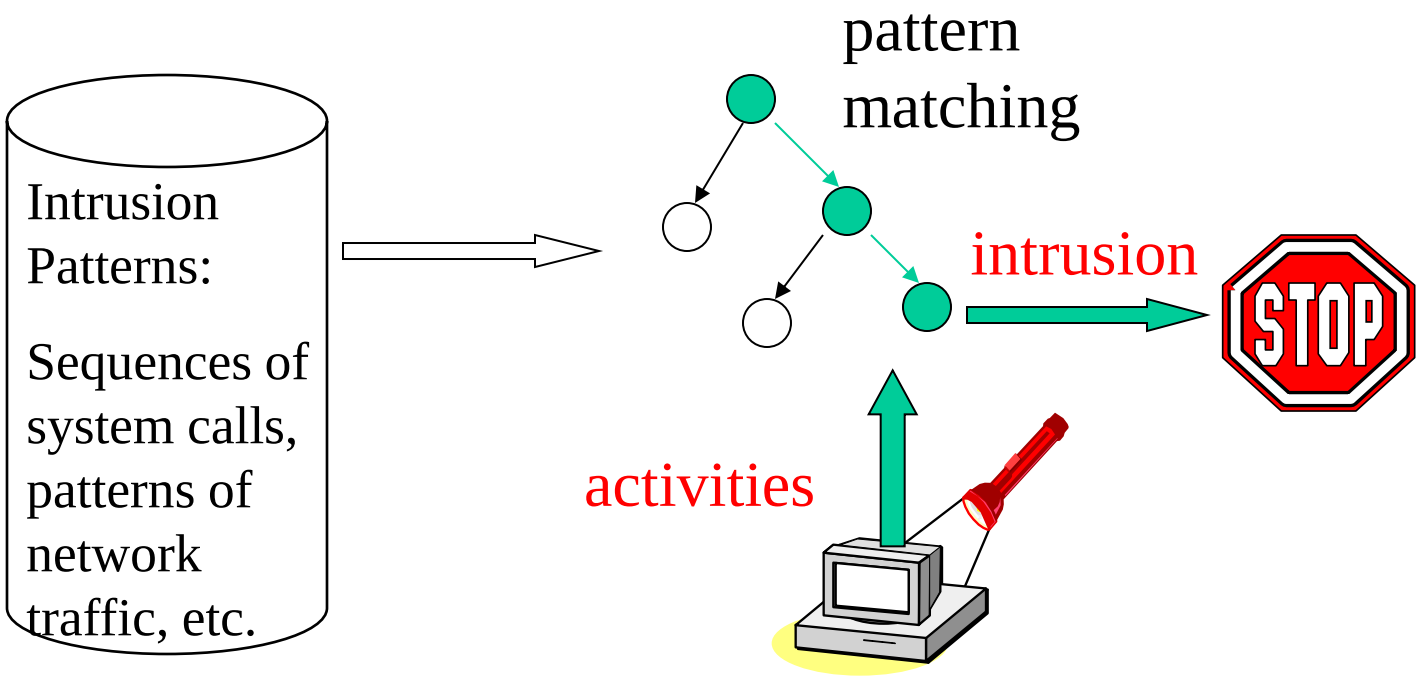
Reading Material (Wenke Lee's paper)



Signature and Anomaly Based Intrusion Detection

- Signature (Misuse detection)
  - Use attack *signatures (characteristics of real* attacks, e.g., illegal sequences of system calls, invalid packets, etc.)
  - Can only detect already-known attacks
  - False positive rate is low, but false negative rate is high
- Anomaly based detection
  - Uses a model of "normal" system behavior
  - Tries to detect deviations from this behavior,
    - e.g., raises an alarm when a statistically rare event occurs
  - Can potentially detect new (not previously encountered) attacks
  - Low false negative rate, high false positive rate
- Which is better?

Misuse Detection



Example: ***if*** (traffic contains "x90+de[^\r\n]{30}") ***then*** "attack detected"

Problems?

Limitation? – Cannot deal with new attacks

Examples of Signature

- A sequence of connection attempts to a large number of ports
- A privileged program spawning a shell
- A network packet that has lots of NOOP instruction bytes in it
- Program input containing a very long string (parameter value)
- A large number of TCP SYN packets sent, with
- No ACKs coming back

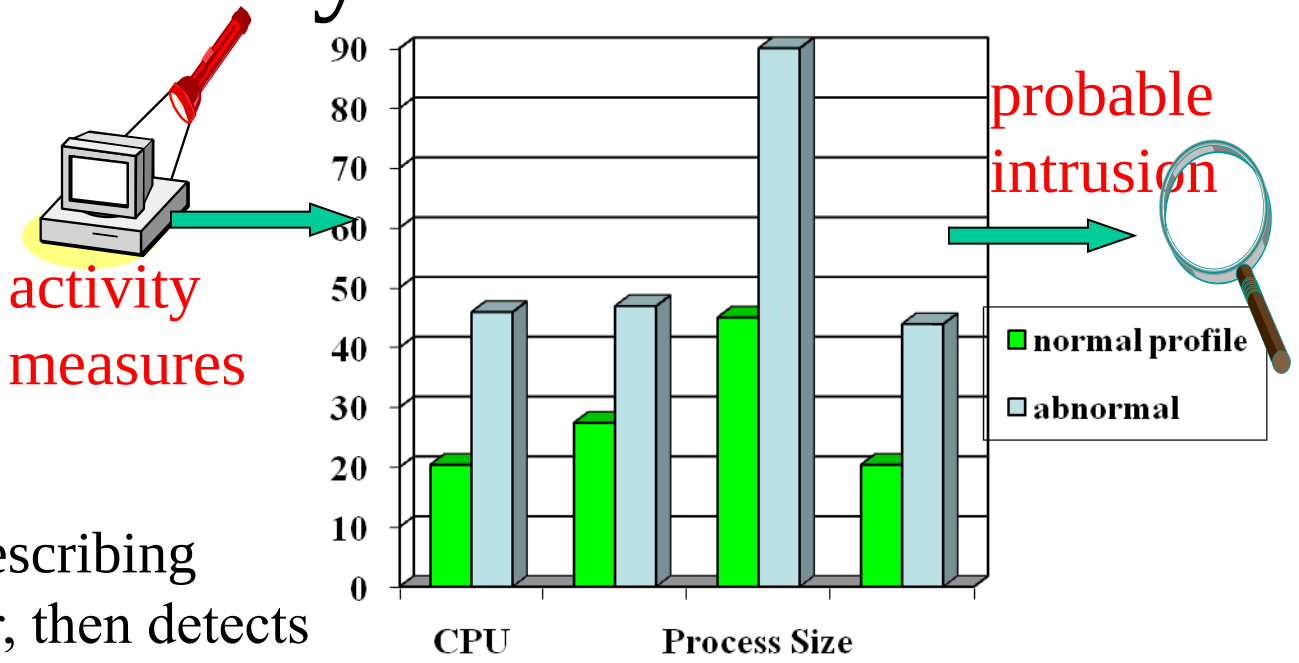
Signature Generation

- Research challenge
  - **Fast, automatic extraction of signatures for new attacks**
  - Honeypots are useful for attracting attacks to generate signatures
- Attack signatures are usually very specific
  - Automated engines now generate unlimited variants of a single attack
  - Program obfuscation, self-decrypting code
- Possible response
  - Find attack characteristics that are difficult to conceal / obfuscate

Anomaly Detection

- Collect a profile of “normal” behavior
  - Called *training phase*
  - Works best for small, well-defined, stable systems
- IDS compares operational system to this profile, and flags deviations

Anomaly Detection



Define a profile describing "normal" behavior, then detects deviations.

Any issue?

Relatively high false positive rates

- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
  - Examples: router failure or misconfiguration,
- Which method will detect DDoS SYN flooding ?

Examples of Metrics

- Count of the number of occurrences of an event per unit time
  - If count exceeded, raise an alarm
- Time elapsed between events
  - if time too small, raise an alarm
- Resource utilization
  - If utilization too high, raise an alarm
- Statistical measures
  - mean, standard deviation, etc.

Anomaly-based IDS

- Statistical anomaly detection
  - Attempts to define normal/expected behavior
  - Threshold: Define thresholds, independent of user, for the frequency of occurrence of events.
  - Profile based: Develop profile of activity of each user and use to detect changes in the behavior
- Rule-based Anomaly detection
  - Attempts to define proper behavior
  - Anomaly: rules detect deviation from previous usage patterns
  - Penetration identification: expert system approach that searches for suspicious behavior

Approaches to Intrusion Detection

- Statistical approaches attempt to define normal, or expected, behavior
- Rule-based approaches attempt to define proper behavior. In terms of the types of attackers listed earlier,
  - Statistical anomaly detection is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate.
  - On the other hand, such techniques may be unable to deal with misfeasors. For such attacks, rule-based approaches may be able to recognize events and sequences that, in context, reveal penetration. In practice, a system may exhibit a combination of both approaches to be effective against a broad range of attacks.

Statistical Anomaly Detection

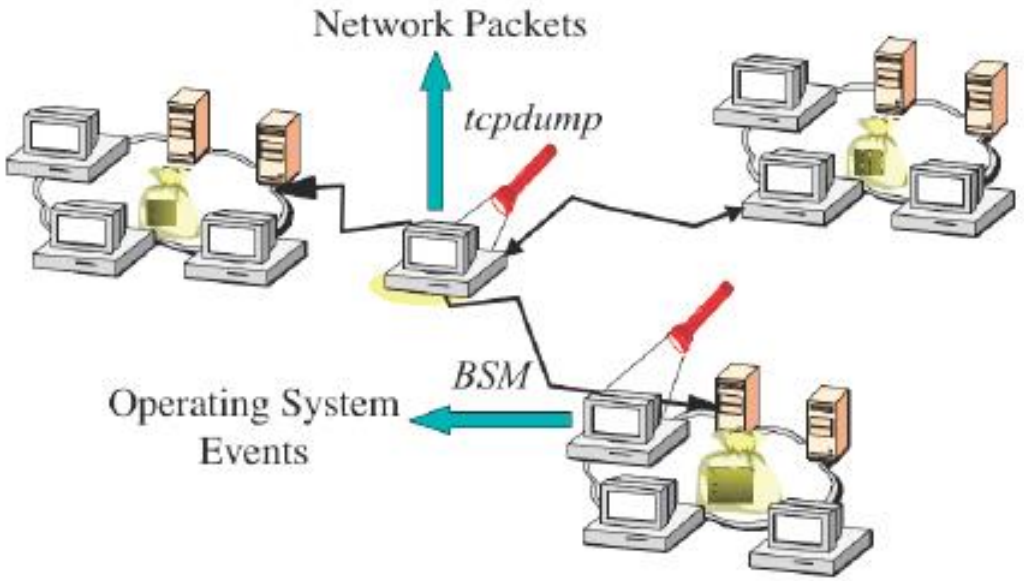
- Threshold detection
  - Count occurrences of specific event over time
  - If exceed reasonable value assume intrusion
  - Alone is a crude & ineffective detector
- Profile based
  - Characterize past behavior of users
  - Detect significant deviations from this
  - Profile usually multi-parameter
- A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert. Foundation of this approach is analysis of audit records.

Convention View

- Anomaly-based IDS by itself generates too many false positives
- Combination of anomaly-based and signature-based is best

Host-based &Network-based IDS

- Depending on where IDS was deployed
- Host-based intrusion detection
  - Monitor activity on a single host
- Network-based intrusion detection (NIDS)
  - Monitor traffic, examine packet headers and payloads



Host-Based IDS

- Use OS auditing and monitoring mechanisms to find applications taken over by an attacker.
  - example
    - Log all system events (e.g., file accesses)
    - Monitor shell commands and system calls executed
  - Advantage: better visibility into behavior of individual applications running on the host
    - Example application: detecting rootkits
    - Rootkit is a set of "Trojan" system binaries Break into a host, download rootkit by FTP, unpack, compile and install
    - Possibly turn off anti-virus / IDS
    - Hides its own presence!
    - Installs hacked binaries for common system
    - Monitoring commands, e.g., **netstat, ps, login**
    - "Sniff" user passwords

Host-Based IDS

- Drawbacks / limitations
  - Need an IDS for every machine
  - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
  - Only local view of the attack

Network-Based IDS

- Inspects network traffic
  - Passive (unlike packet-filtering firewalls)
  - Often handled by a router or firewall
- Monitors user activities
  - e.g., protocol violations, unusual connection patterns, attack strings in packet payloads
- Advantage
  - Single NIDS can protect many hosts and look for widespread patterns of activity

Network-Based IDS

- Limitations
  - May be easily defeated by encryption (data portions and some header information can be encrypted)
  - Not all attacks arrive from the network
  - Must monitor, record and process huge amount of traffic on high-speed links
  - Attack: overload NIDS with huge data streams, then attempt the intrusion

Audit Records

- Fundamental tool for intrusion detection
- Native audit records
  - Part of all common multi-user O/S
  - Already present for use
  - May not have info wanted in desired form
- Detection-specific audit records
  - Created specifically to collect wanted info
  - At cost of additional overhead on system

Audit Record Analysis

- Foundation of statistical approaches
- Analyze records to get metrics over time
  - Counter, gauge, interval timer, resource use
- Use various tests on these to determine if current behavior is acceptable
  - Mean & standard deviation, multivariate, markov process, time series, operational
- The main advantage of the use of statistical profiles is that a prior knowledge of security flaws is not required. Thus it should be readily portable among a variety of systems.

Rule-Based Intrusion Detection

- Observe events on system & apply rules to decide if activity is suspicious or not
- Rule-based anomaly detection
  - Analyze historical audit records to identify usage patterns & auto-generate rules for them
  - Then observe current behavior & match against rules to see if conforms
  - Like statistical anomaly detection does not require prior knowledge of security flaws
  - **Look at decision rule!**

Rule-Based Intrusion Detection

- Rule-based penetration identification
  - Uses expert systems technology
  - With rules identifying known penetration, weakness patterns, or suspicious behavior
  - Compare audit records or states against rules
  - Rules usually machine & O/S specific
  - Rules are generated by experts who interview & codify knowledge of security admins
  - Quality depends on how well this is done

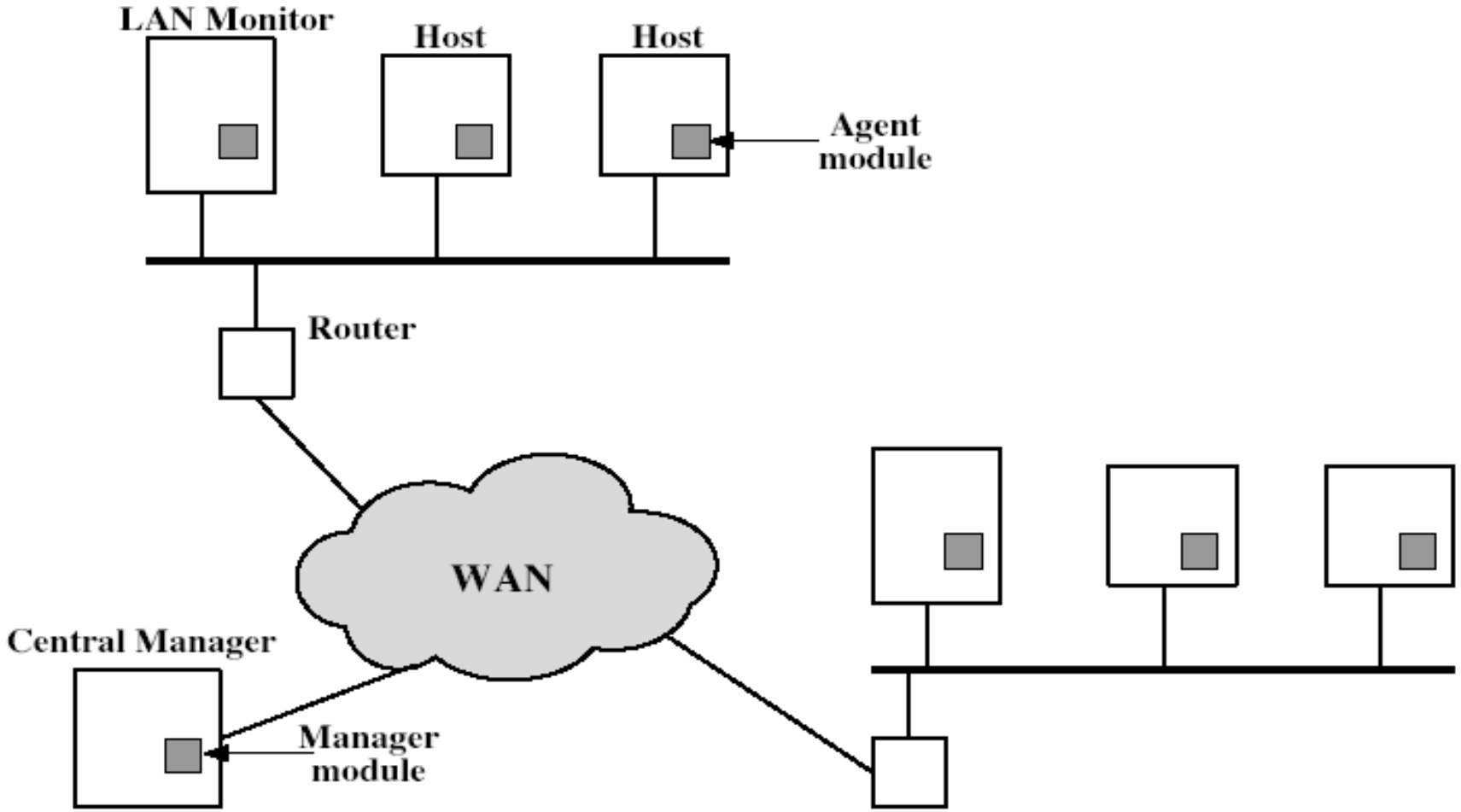
Base-Rate Fallacy

- Practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
  - if too few intrusions detected -> false security
  - if too many false alarms -> ignore / waste time
- This is very hard to do
- Existing systems seem not to have a good record

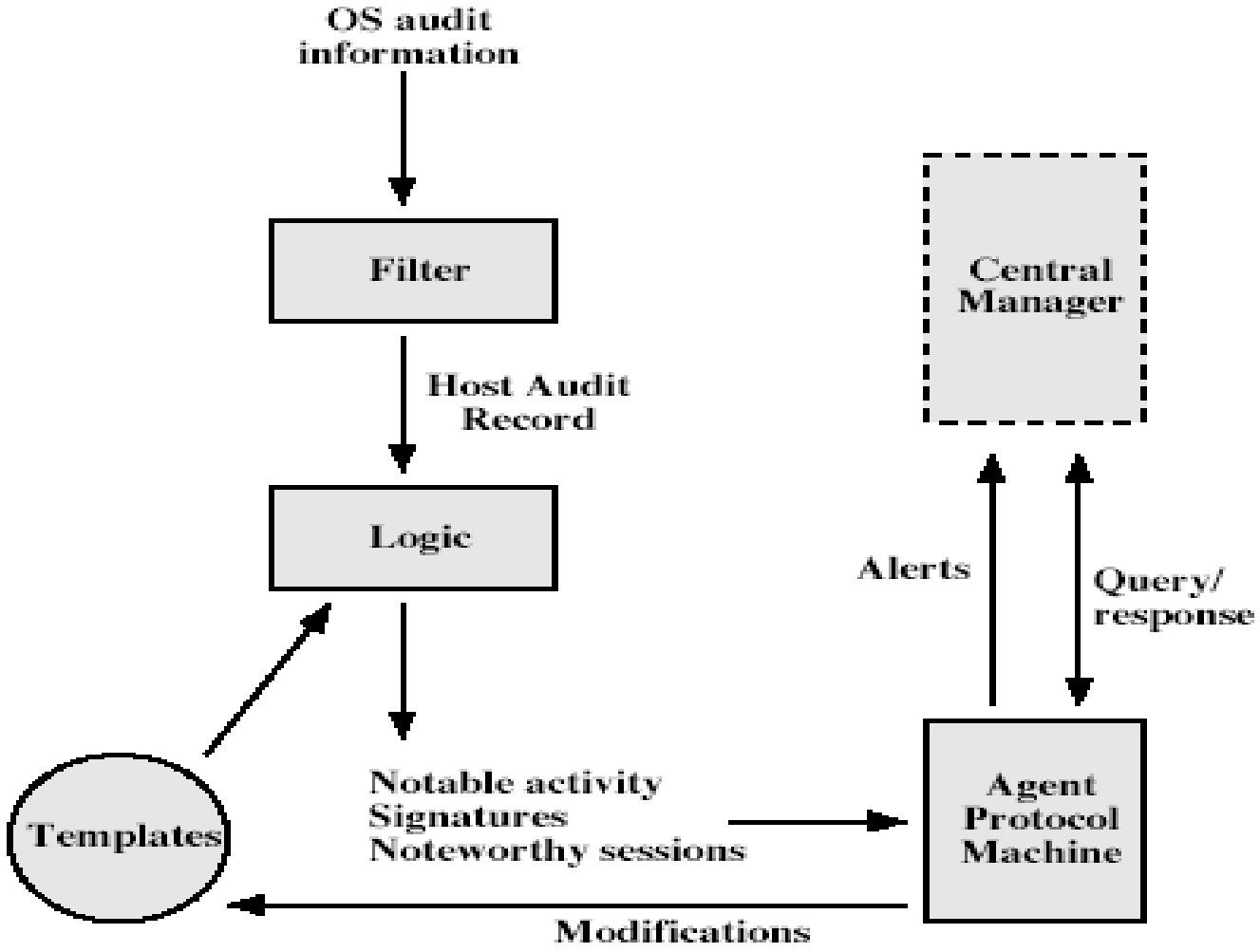
Distributed Intrusion Detection

- Traditional focus is on single systems
- But typically have networked systems
- More effective defense has these working together to detect intrusions
- Issues
  - Dealing with varying audit record formats
  - Integrity & confidentiality of networked data
  - Centralized or decentralized architecture

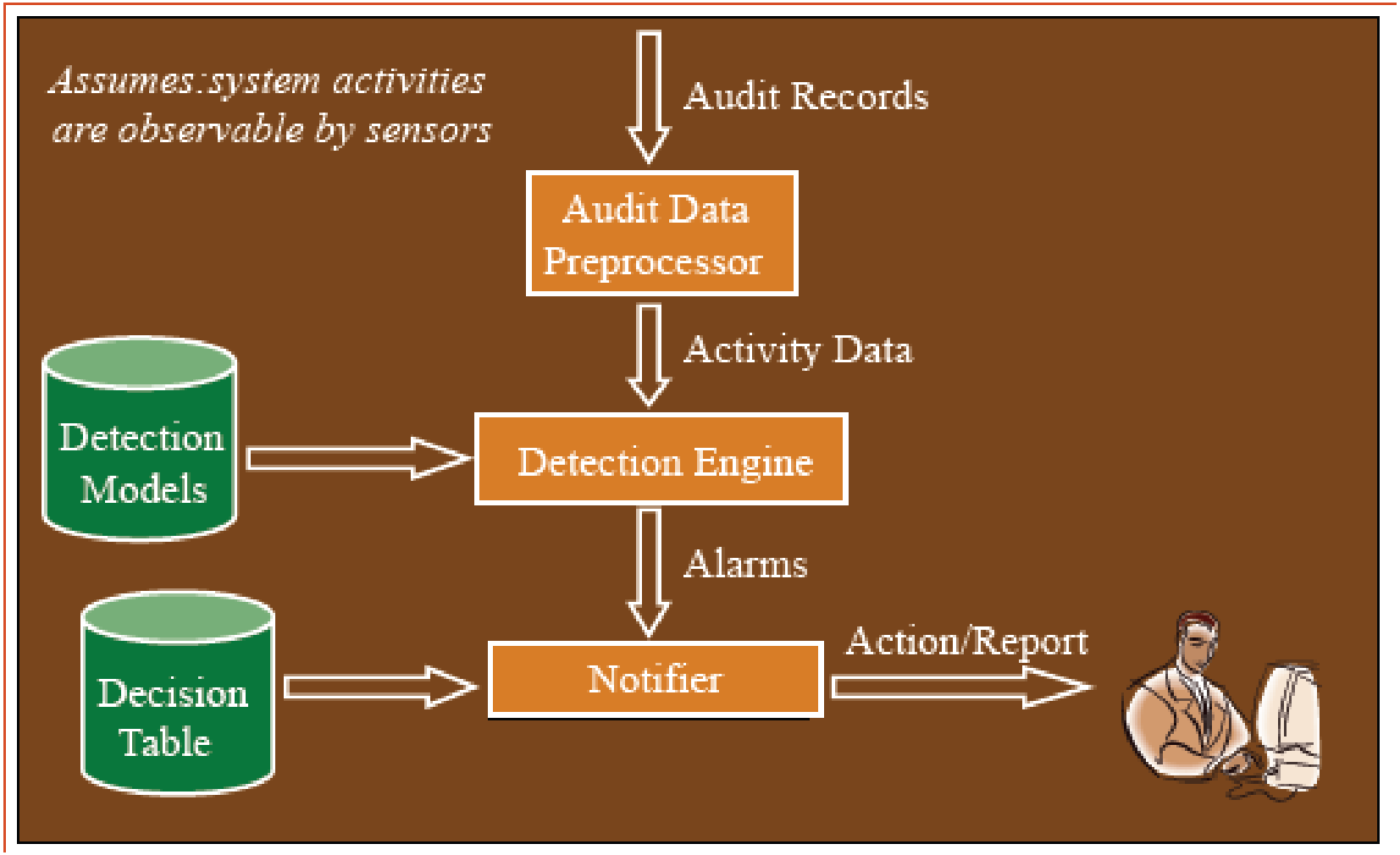
Distributed Intrusion Detection - Architecture



Distributed Intrusion Detection – Agent Implementation

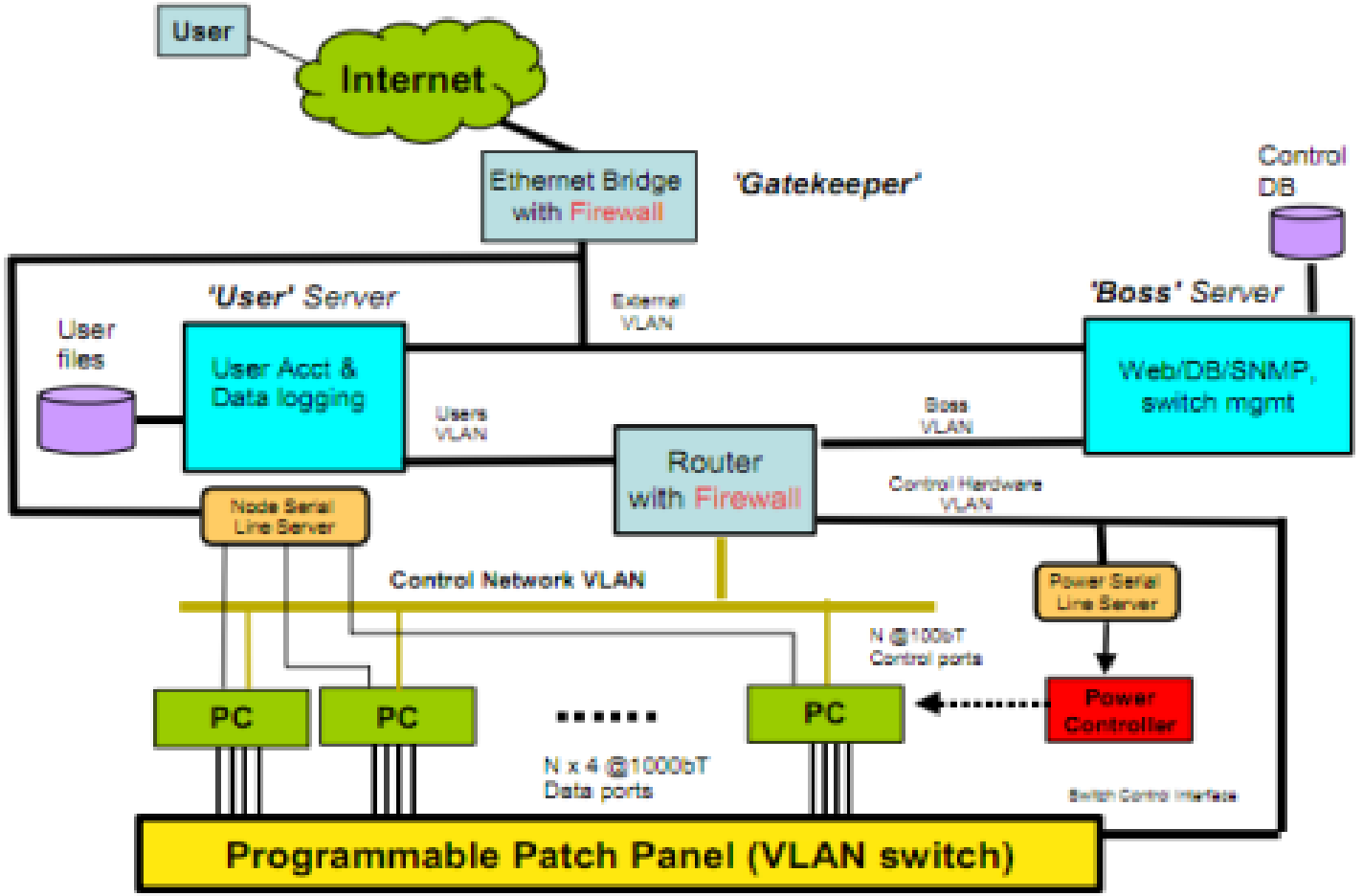


IDS System Workflow



DETER Project

- http://www.techrepublic.com/blog/security/the-deter-project-researching-cyber-security/4981
- http://www.deter-project.org/research



DETER Project

- **Please read the following paper to understand DETER project**

- "The Science of Cyber-Security Experimentation: the DETER Project," by Terry Benzel. In Proceedings of the Annual Computer Security Applications Conference (ACSAC) 2011

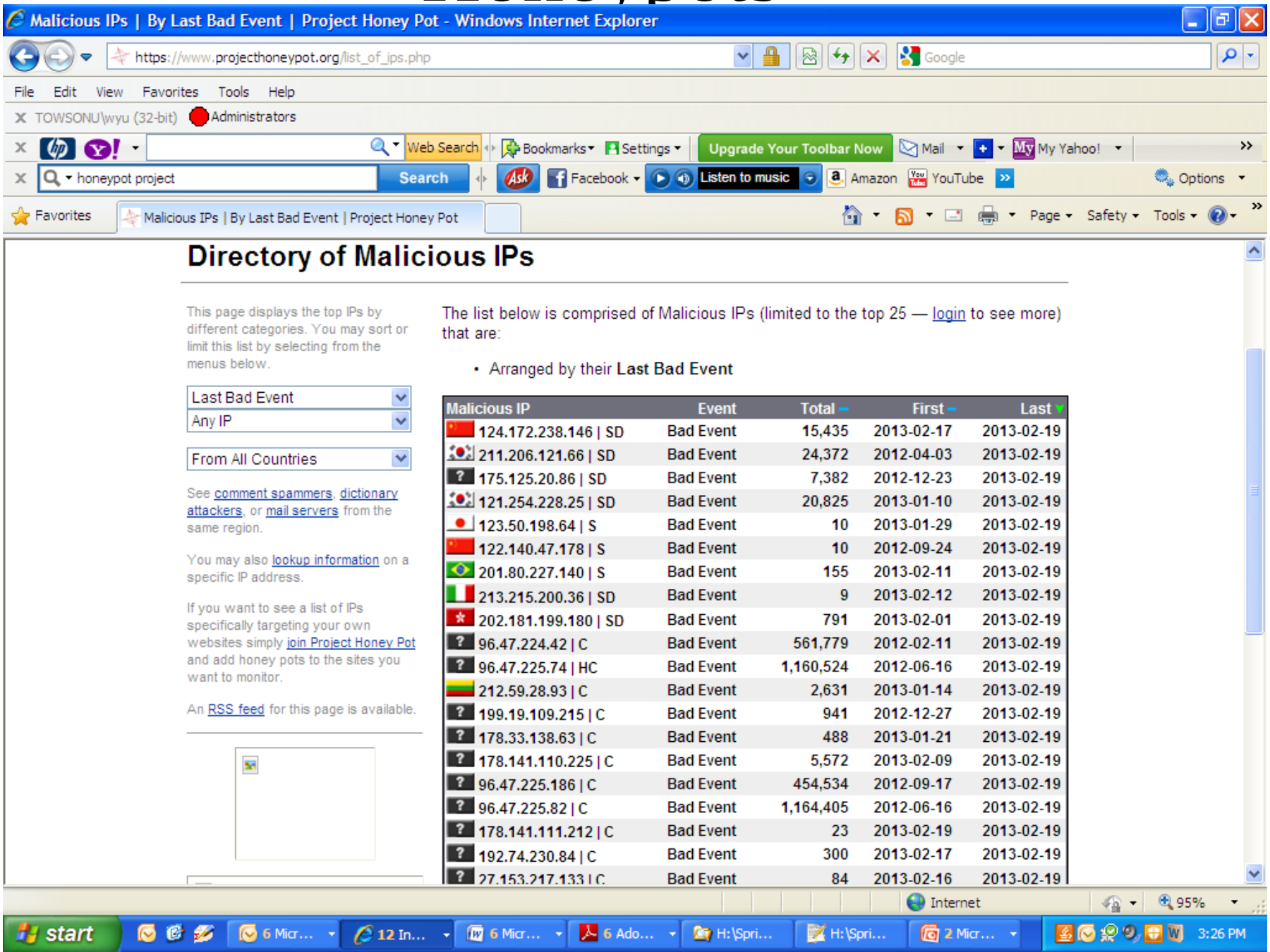
http://www.deter-project.org/DETER-publications-papers-video-newsletters

Honeypots

- Decoy systems to lure attackers
  - Away from accessing critical systems
  - To collect information of their activities
  - To encourage attacker to stay on system so administrator can respond
- These systems are filled with fabricated information designed to appear valuable but which any legitimate user of the system wouldn't access, thus, any access is suspect.
- They are instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.
- Single or multiple networked systems
- IETF Intrusion Detection WG standards
  - Project idea?

Look at honeypot project website:
https://www.projecthoneypot.org/

Honeypots


Malicious IPs | By Last Bad Event | Project Honey Pot - Windows Internet Explorer
https://www.projecthoneypot.org/list_of_ips.php
Google
File Edit View Favorites Tools Help
TOWSONU\wyu (32-bit) Administrators
Web Search Bookmarks Settings Upgrade Your Toolbar Now Mail My Yahoo!
honeypot project Search Facebook Listen to music Amazon YouTube Options
Favorites Malicious IPs | By Last Bad Event | Project Honey Pot
Page Safety Tools
Directory of Malicious IPs
This page displays the top IPs by different categories. You may sort or limit this list by selecting from the menus below.
Last Bad Event
Any IP
From All Countries
See comment spammers, dictionary attackers, or mail servers from the same region.
You may also lookup information on a specific IP address.
If you want to see a list of IPs specifically targeting your own websites simply join Project Honey Pot and add honey pots to the sites you want to monitor.
An RSS feed for this page is available.
The list below is comprised of Malicious IPs (limited to the top 25 — login to see more) that are:
• Arranged by their Last Bad Event
Malicious IP | Event | Total | First | Last
124.172.238.146 | SD | Bad Event | 15,435 | 2013-02-17 | 2013-02-19
211.206.121.66 | SD | Bad Event | 24,372 | 2012-04-03 | 2013-02-19
175.125.20.86 | SD | Bad Event | 7,382 | 2012-12-23 | 2013-02-19
121.254.228.25 | SD | Bad Event | 20,825 | 2013-01-10 | 2013-02-19
123.50.198.64 | S | Bad Event | 10 | 2013-01-29 | 2013-02-19
122.140.47.178 | S | Bad Event | 10 | 2012-09-24 | 2013-02-19
201.80.227.140 | S | Bad Event | 155 | 2013-02-11 | 2013-02-19
213.215.200.36 | SD | Bad Event | 9 | 2013-02-12 | 2013-02-19
202.181.199.180 | SD | Bad Event | 791 | 2013-02-01 | 2013-02-19
96.47.224.42 | C | Bad Event | 561,779 | 2012-02-11 | 2013-02-19
96.47.225.74 | HC | Bad Event | 1,160,524 | 2012-06-16 | 2013-02-19
212.59.28.93 | C | Bad Event | 2,631 | 2013-01-14 | 2013-02-19
199.19.109.215 | C | Bad Event | 941 | 2012-12-27 | 2013-02-19
178.33.138.63 | C | Bad Event | 488 | 2013-01-21 | 2013-02-19
178.141.110.225 | C | Bad Event | 5,572 | 2013-02-09 | 2013-02-19
96.47.225.186 | C | Bad Event | 454,534 | 2012-09-17 | 2013-02-19
96.47.225.82 | C | Bad Event | 1,164,405 | 2012-06-16 | 2013-02-19
178.141.111.212 | C | Bad Event | 23 | 2013-02-19 | 2013-02-19
192.74.230.84 | C | Bad Event | 300 | 2013-02-17 | 2013-02-19
27.153.217.133 | C | Bad Event | 84 | 2013-02-16 | 2013-02-19
Internet 95%
start 3:26 PM

Password Management

- Front-line defense against intruders
- Users supply both:
  - Login – determines privileges of that user
  - Password – to identify them
- Passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - More recent systems use crypto hash function
- Should protect password file on system

Password Studies

- Purdue 1992 - many short passwords
  - A study at Purdue University in 1992 observed password change choices on 54 machines, for 7000 users, and found almost 3% of the passwords were three characters or fewer in length, easily exhaustively searched!
- Klein 1990 - many guessable passwords
  - A study by Klein 1990 collected UNIX password files, containing nearly 14,000 encrypted passwords, and found nearly one-fourth of these passwords were guessable.
- Conclusion is that users choose poor passwords too often
- Need some approach to counter this

Managing Passwords - Education

- Can use policies and good user education
- Educate on importance of good passwords
- Give guidelines for good passwords
  - Minimum length (>6)
  - Require a mix of upper & lower case letters, numbers, punctuation
  - Not dictionary words
- But likely to be ignored by many users

Managing Passwords - Computer Generated

- Let computer create passwords
- If random likely not memorisable, so will be written down (sticky label syndrome)
- Even pronounceable not remembered
- Have history of poor user acceptance
- FIPS PUB 181 one of best generators
  - Has both description & sample code
  - Generates words from concatenating random pronounceable syllables

Managing Passwords - Reactive Checking

- Reactively run password guessing tools
  - Note that good dictionaries exist for almost any language/interest group
- Cracked passwords are disabled and the system cancels any passwords that are guessed and notifies the user.
- Drawbacks
  - It is resource intensive if the job is done right,
  - Any existing passwords remain vulnerable until the reactive password checker finds them.

Managing Passwords - Proactive Checking

- Most promising approach to improving password security
- Allow users to select own password
- But have system verify it is acceptable
  - Simple rule enforcement (see earlier slide)
  - Compare against dictionary of bad passwords
  - Use algorithmic (markov model or bloom filter) to detect poor choices

Graphical Passwords

- Limitation of text-based passwords ?
  - Difficulty of remembering passwords
    - Easy to remember -> easy to guess
    - Hard to guess -> hard to remember
  - Users tend to write passwords down or use the same passwords for different accounts
- An alternative: Graphical Passwords
  - Psychological studies: Human can remember pictures better than text

Graphical Passwords

Select a sequence of images as password

http://searchsecurity.techtarget.com/definition/graphical-password

Case Study

- Towson University: Intrusion Detection on Tactical Environment
  - Sampling/Aggregation on MANET
  - Malware Classification on Android Platform

- Robin Sommer at Lawrence Berkeley National Lab
  - Network Security Today: Fining Complex Attacks at 100Gb/S

Reading

- Teresa Lunt at Xerox Palo Alto Research Center, "*Intrusion Detection: New Directions*"

  www.blackhat.com/presentations/bh-usa-99/teresa-lunt/tutorial.ppt

- Robin Sommer at Lawrence Berkeley National Lab: "*Outside the Closed World: On Finding Intrusions with Anomaly Detection*"

  http://oakland31.cs.virginia.edu/slides/anomaly-oakland.pdf

Summary

- We have considered:
  - Problem of intrusion, behavior and techniques
  - Intrusion detection
  - Password management