Network Security

Intruders and Viruses

Evening With Berferd

- Impressions?
- Called a cracker
- Early Internet Gateway -1990
- Password file
- SMTP protocol
- Lots of time – timezone analysis
- **rm –rf /**   - “Whoa! Now it’s personal!”
- Chroot “Jail” – Honeypot
- If hacker gets a login, you’re in trouble

alt.security FAQs

“The only system that is truly secure is one that is switched off and unplugged, locked in a titanium lines safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. *Even then, I wouldn’t stake my life on it.*”

Intruders

When all kinds of trials and temptations crowd into your lives, my brothers, don't resent them as intruders, but welcome them as friends. Realize that they come to test your faith and to produce in you the quality of endurance.

-Bible, James 1:2-3

Three Classes of Intruders

- Masquerader – unauthorized user who penetrates a system exploiting a legitimate user’s account *(outside)*
- Misfeasor - legitimate user who makes unauthorized accesses or misuses his privileges *(inside)*
- Clandestine user - seizes supervisory control to evade auditing and access controls or suppress audit collection *(inside|outside)*

American Heritage Dictionary

mis•feá•sance *n*, improper and unlawful execution of an act that in itself is lawful and proper

Intruders

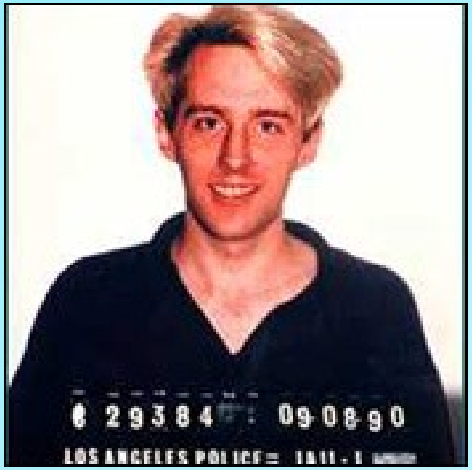
Intruder attacks range from benign to serious:

- Benign intruders tolerable but consume resources
- Difficult to know in advance the type of intruder
- Really growing problem
  - globalization
  - the move to Client/Server architectures
  - hacker’s steep learning curve

Types Of Hackers

- Old School – Capt Crunch – no malicious intent – believe in open system
- Script Kiddies – 12-30 yrs old, mostly males – limited knowledge – too much time on their hands – also called Cyber Punks – brag and get caught

Cyber Punk



Kevin Poulsen
1990

- Took over all the telephone lines of Los Angeles KISS-FM radio station - he then made himself the 102nd caller and won a $50,000 944 S2 Porche

- Indicted for 19 counts of conspiracy, fraud, wiretapping and money laundering - spent 3 years in prison

Types Of Hackers

- Professional Criminals – Crackers – careers built on criminal hacking – break into secure areas and sell information – often involved in espionage and organized crime

Crackers

Vladimir Levin
1994

- Russian mathematician – led group that hacked into Citibank computers and extorted 10 million dollars.
- Caught in 1995 by Interpol - sentenced to three years in prison and forced to give up his share of the money.

Types Of Hackers

- Coders – Virus Writers - see themselves as an elite group - they have a lot of programming background and write code, but won't use it themselves
- They have their own networks to experiment with, which they call **Zoos**
- They leave it to others to introduce their codes into **The Wild**, or the Internet.

Coder

Robert Morris
1988

- Crashes 6,000 computers on the internet with first **worm** program

- He is fined $10,000 and the Federal computer Emergency Response team (CERT) is formed

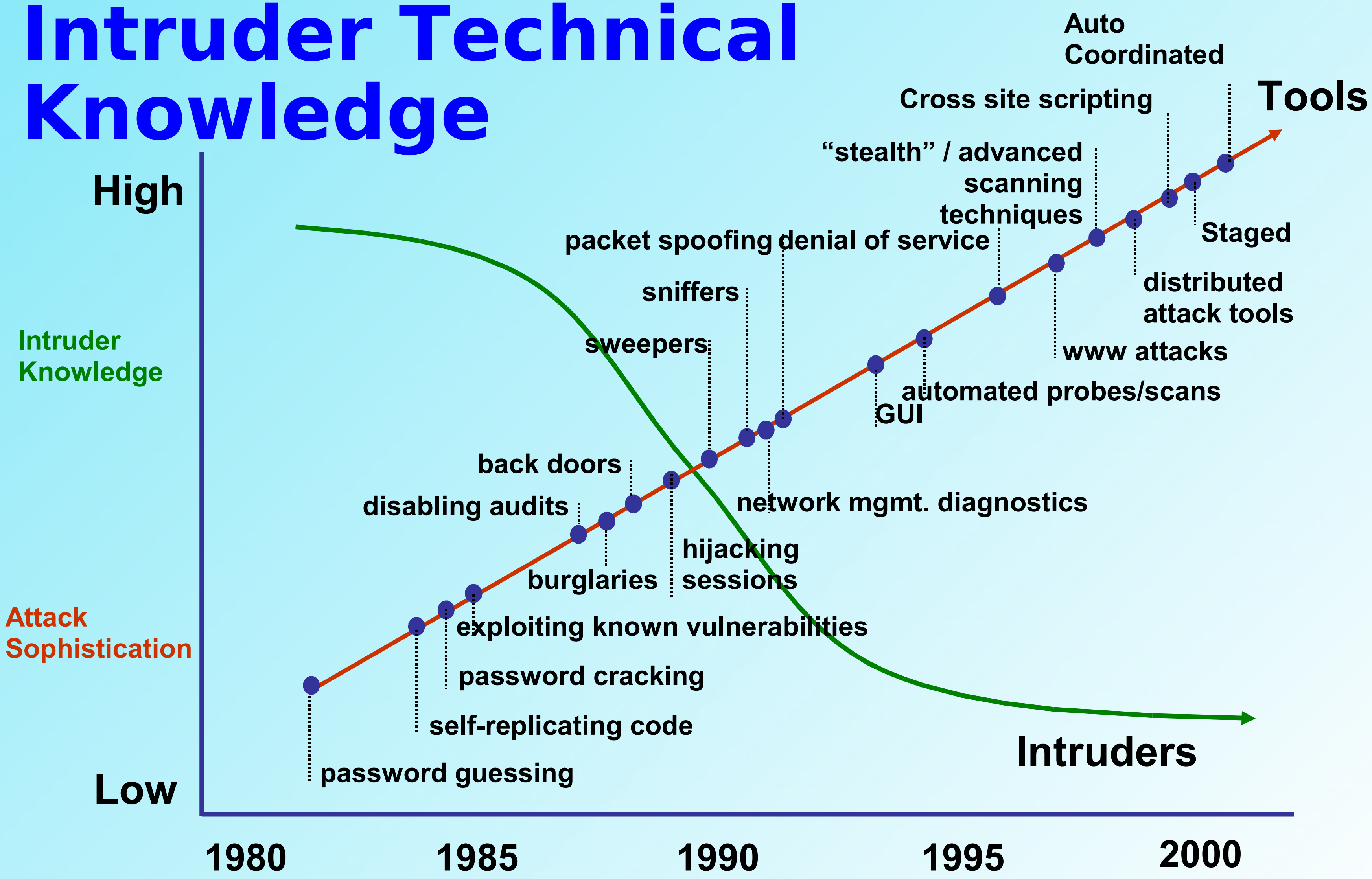
Psychology Of Hackers

- Underlying the psyche of the criminal hacker may be a deep sense of inferiority
- Consequently, the mastery of computer technology, or the shut down of a major site, might give them a sense of power
- "It's a population that takes refuge in computers because of their problems sustaining real world relationships. Causing millions of dollars of damage is a real power trip" - Jerrold M. Post, psychiatrist at George Washington University in Washington, D.C.
- http://tlc.discovery.com/convergence/hackers/hac - good overview - source of previous 6 slides

Some Are Even Good

- Chloe Can Break Into Anything And Load It Down To Jack's PDA!!!

Attack Sophistication vs. Intruder Technical Knowledge



Source: Carnegie Mellon University

Intrusion Techniques

- Objective: Gain access to a system
- Frequent Goal: Acquiring a user password
- Most systems have a file that maps a password to each user
- Password file protection:
  - one-way encryption
  - access control

Password Learning Techniques

guess attack

1. Try default passwords used with standard accounts shipped with the system
2. Exhaustive try of all short passwords
3. Try words in system’s dictionary or list of likely passwords (hacker bulletin boards)
4. Collect information about users (full names, names of spouses and children, pictures and books in their office, related hobbies)
5. Try users’ phone numbers, social security numbers, room numbers
6. Try all legitimate license plate numbers
7. Use a trojan horse
8. Tap the line between a remote user and the system

Intrusion Detection

Intrusion Detection

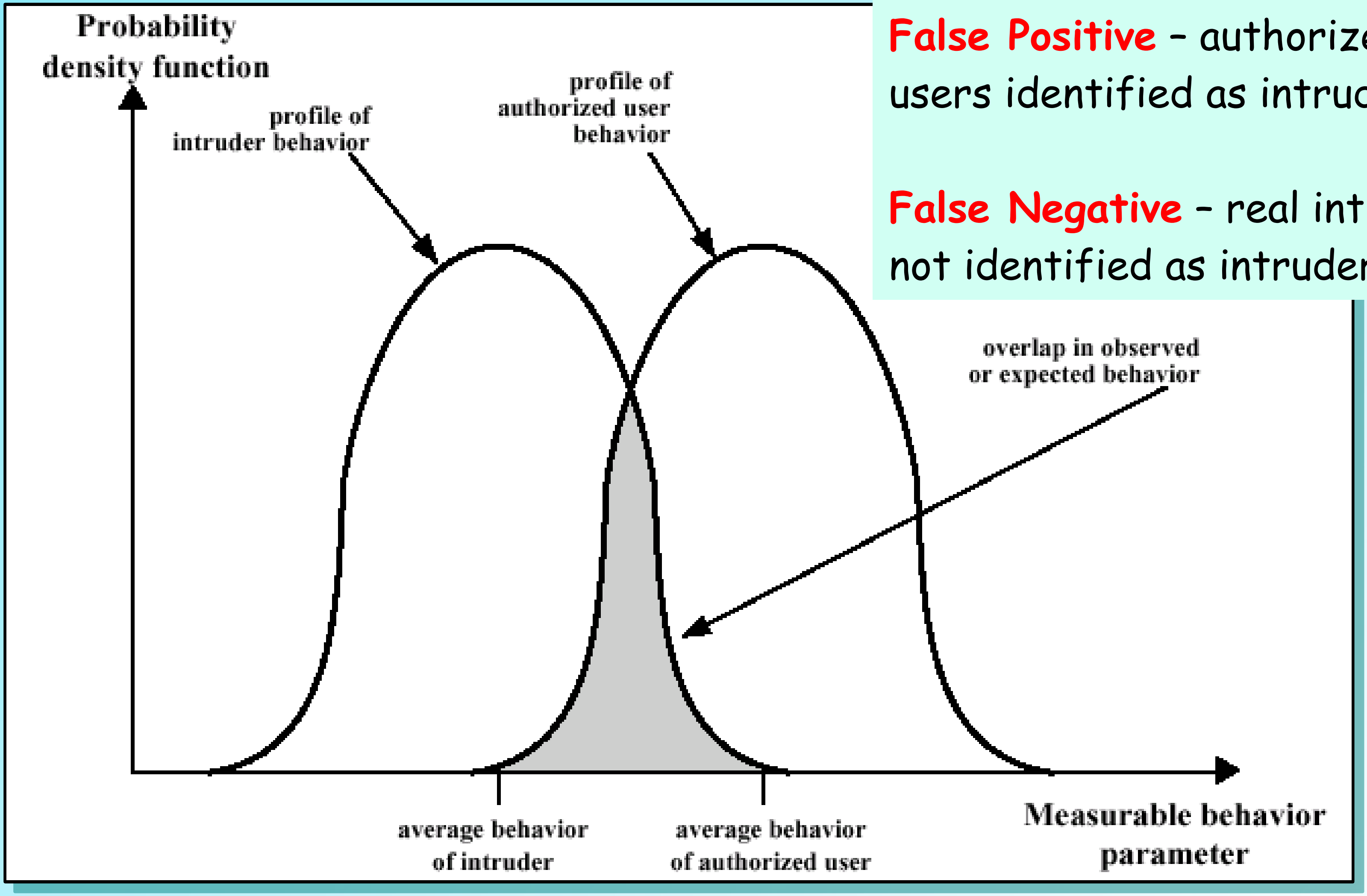
Second line of defense (firewall is 1st)

- Quick detection - minimize damage and quicker recovery
- Deterrent - an effective intrusion detection system helps to prevent intrusions
- Collection of techniques - information about intrusion techniques leads to stronger prevention facility

Intrusion Detection

- Basic Assumption:
  Behavior of the intruder *differs* from legitimate user in quantifiable ways
- There is an element of compromise and art in the practice of intrusion detection

Intruder & Authorized User Behavior


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

False Positive – authorized users identified as intruders

False Negative – real intruders not identified as intruders

Finding The Bad Guy

- Need to distinguish between a masquerader and a legitimate user
- Observe past history (Bayes Theorem)
- Establish patterns of behavior
- Look for significant deviations

Two Approaches:

Statistical Anomaly Detection

- Collection of data over a period of time about legitimate user behavior
- Statistical tests to observe behavior and confidently determine non-legitimate use
  - Threshold detection: for frequency of occurrence of certain events
  - Profile-based: profile of user activity and change detection
- Successful against masqueraders but not against misfeasors

Two Approaches:

Rule-based Detection

- Attempt to define set of rules that determine intruder's behavior
  - Anomaly detection: detect deviation from previous usage patterns
  - Penetration identification: expert system that searches for suspicious behavior
- Better approach for detecting penetration

Audit Record

Basic Tool of Intrusion Detection

- Native audit records
  - Information collected for accounting
  - No extra cost but not necessary or conveniently formed information
- Detection-specific audit records
  - Only info required by IDS
  - Extra overhead
  - Vendor independent
  - Subject, action, object, exception condition, resource usage, timestamp (Denning)

Dorothy Denning

- Professor of Computer Science at Georgetown, Senior Staff Scientist at SRI International, research staff at DEC
- 1982, “Cryptography and Data Security,” 1999, “Information Warfare and Security
- ACM Fellow, Distinguished Lecture in Computer Security Award
- http://www.cs.georgetown.edu/~denn

Detection Specific Audit Records

- Decomposition of user operations into elementary actions

```
COPY GAME.EXE TO <Library>GAME.EXE
```

sub	action	object	cond	usage	time-stamp
Smith	execute	<Library>COPY.EXE	0	CPU=0002	11058721678
Smith	read	<Smith>GAME.EXE	0	Rec = 0	11058721823
Smith	execute	<Library>COPY.EXE	Wr-viol	Rec = 0	11058722134

- Enables audit of all behavior affecting an object
- Single object, single action simplicity
- Easily extracted from native audit records

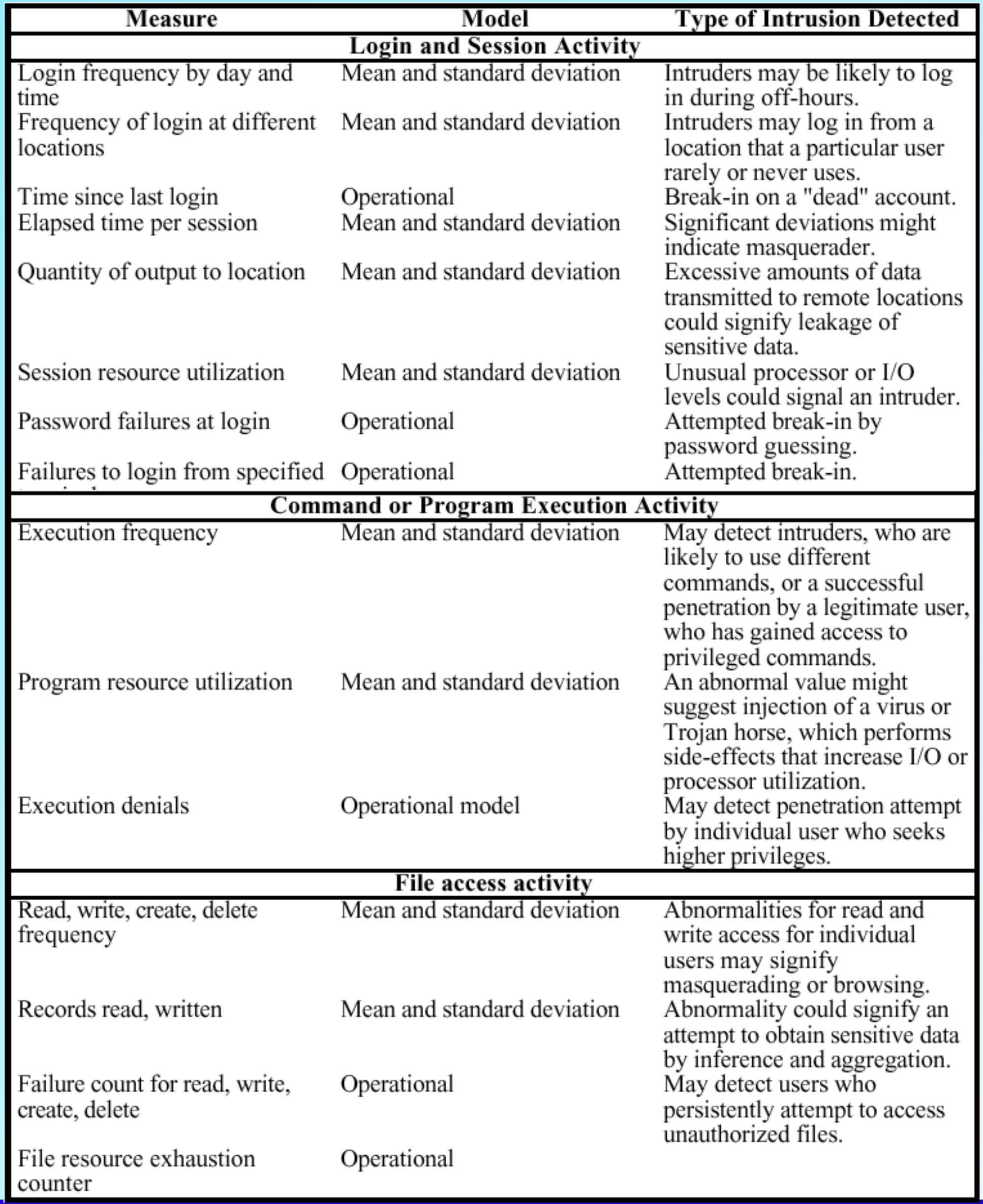
Statistical Anomaly Categories

- Threshold detection
  - Counting the *number of occurrences* of a specific event type over an *interval of time*
  - Generate either a lot of false positives or a lot of false negatives
- Profile-based systems
  - Characterizing the *past behavior* of individual users or related groups of users and then *detecting significant deviations*
  - A profile is a *set of parameters*
  - *Foundation* of this approach is an analysis of *audit records*
  - *Records over time* define typical behavior. *Current audit records* are used to detect intrusion

Statistical Anomaly Detection

- Various tests determine whether current activity fits within acceptable limits
  - Mean & standard deviation – crude for intrusion detection
  - Multivariate – correlation determines intruder behavior
  - Markov process – establish transition probabilities among various states
  - Time series – focus on time intervals
  - Operational model – exceeding fixed limits
- Prior knowledge of security flaws is not required

Measures Used For Intrusion



Measure	Model	Type of Intrusion Detected
Login and Session Activity		
Login frequency by day and time	Mean and standard deviation	Intruders may be likely to log in during off-hours.
Frequency of login at different locations	Mean and standard deviation	Intruders may log in from a location that a particular user rarely or never uses.
Time since last login	Operational	Break-in on a "dead" account.
Elapsed time per session	Mean and standard deviation	Significant deviations might indicate masquerader.
Quantity of output to location	Mean and standard deviation	Excessive amounts of data transmitted to remote locations could signify leakage of sensitive data.
Session resource utilization	Mean and standard deviation	Unusual processor or I/O levels could signal an intruder.
Password failures at login	Operational	Attempted break-in by password guessing.
Failures to login from specified	Operational	Attempted break-in.
Command or Program Execution Activity		
Execution frequency	Mean and standard deviation	May detect intruders, who are likely to use different commands, or a successful penetration by a legitimate user, who has gained access to privileged commands.
Program resource utilization	Mean and standard deviation	An abnormal value might suggest injection of a virus or Trojan horse, which performs side-effects that increase I/O or processor utilization.
Execution denials	Operational model	May detect penetration attempt by individual user who seeks higher privileges.
File access activity		
Read, write, create, delete frequency	Mean and standard deviation	Abnormalities for read and write access for individual users may signify masquerading or browsing.
Records read, written	Mean and standard deviation	Abnormality could signify an attempt to obtain sensitive data by inference and aggregation.
Failure count for read, write, create, delete	Operational	May detect users who persistently attempt to access unauthorized files.
File resource exhaustion counter	Operational	

Rule-Based Detection

- Observe events in the system and apply a set of rules that decide if activity is suspicious or not
- Approaches focus on either:
  - Anomaly detection
  - Penetration identification

Rule-Based Anomaly Detection

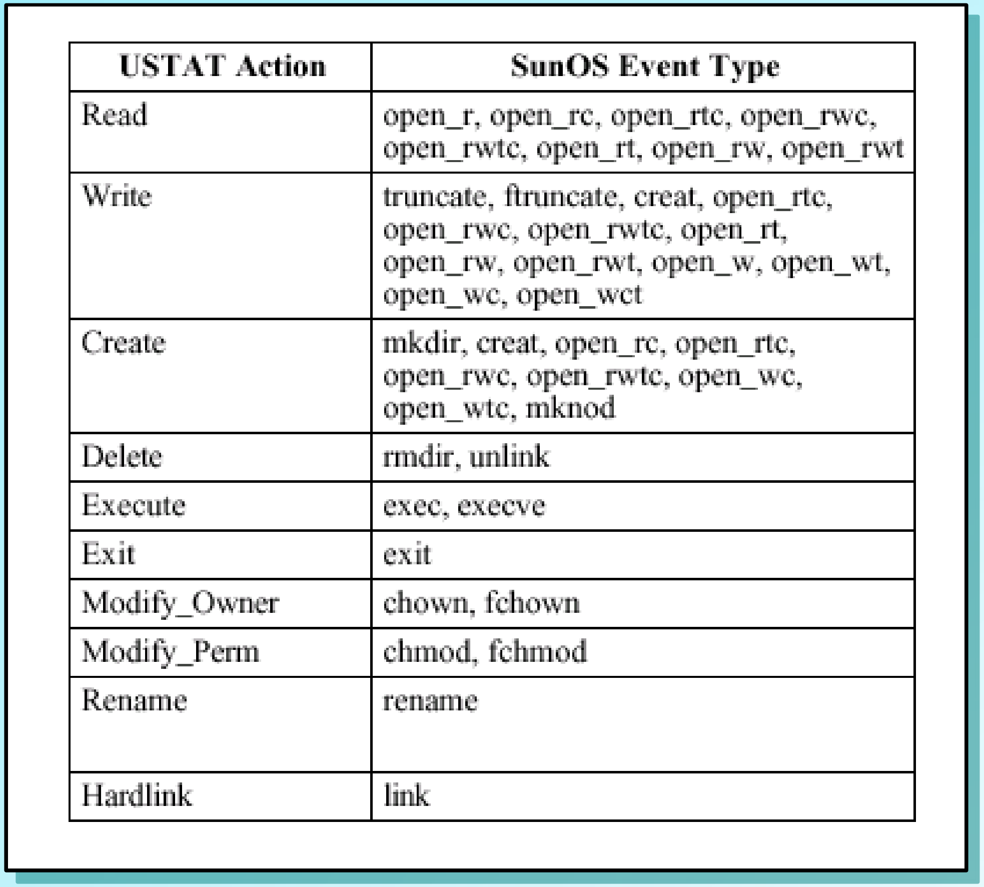
- Similar in terms of approach and strengths to statistical anomaly detection
- Automatically generate rules by analyzing historical audit records to identify usage patterns
- Assume the future will look like the past and apply rules to current behavior
- Does not require a knowledge of security vulnerabilities
- Requires a rather large database of rules (10^4 to 10^6)

Rule-Based Penetration Identification

- Based on expert system technology
- Uses rules for identifying known penetrations or ones that exploit known weaknesses – suspicion rating
- Rules generated by experts and system specific
- Strength is a function of the skills of the rule makers – hire a hacker
- Early systems: NIDX, IDES, Haystack – late 80’s
- Best approach is a high level model that is independent of specific audit records
- USTAT, a state transition model, deals with general actions and reduces the number of rules

USTAT Actions

State Transition diagram is developed that characterizes suspicious activity



USTAT Action	SunOS Event Type
Read	open_r, open_rc, open_rtc, open_rwc, open_rwtc, open_rt, open_rw, open_rwt
Write	truncate, ftruncate, creat, open_rtc, open_rwc, open_rwtc, open_rt, open_rw, open_rwt, open_w, open_wt, open_wc, open_wct
Create	mkdir, creat, open_rc, open_rtc, open_rwc, open_rwtc, open_wc, open_wtc, mknod
Delete	rmdir, unlink
Execute	exec, execve
Exit	exit
Modify_Owner	chown, fchown
Modify_Perm	chmod, fchmod
Rename	rename
Hardlink	link

10 general actions ← 239 SunOS events

Base-Rate Fallacy

- IDS system must meet the standard of high rate of detections with a low rate of false alarms
- False alarm rate is the limiting factor for the performance of an IDS
- This is due to the Base-Rate Fallacy - the belief that probability rates are false – i.e., failure to take base rates into account when judging probability

Base-Rate Fallacy

A cab was involved in a hit-and-run accident at night. Two cab companies, the Green and the Blue, operate in the city.

You are given the following data:

- 85% of the cabs in the city are Green and 15% are Blue.
- A witness identified the cab as a Blue cab.

The court tested his ability to identify cabs under the appropriate visibility conditions. When presented with a sample of cabs (half of which were Blue and half of which were Green) the witness made correct identifications in 80% of the cases and erred in 20% of the cases.

Question: What is the probability that the cab involved in the accident was Blue rather than Green?"

Base-Rate Fallacy

When people answer this, they tend to say that the probability it was Blue (the rare case) is about 80%, but the real probability is 41%, because this takes into account the fact that there are may more green cabs than blue ones.

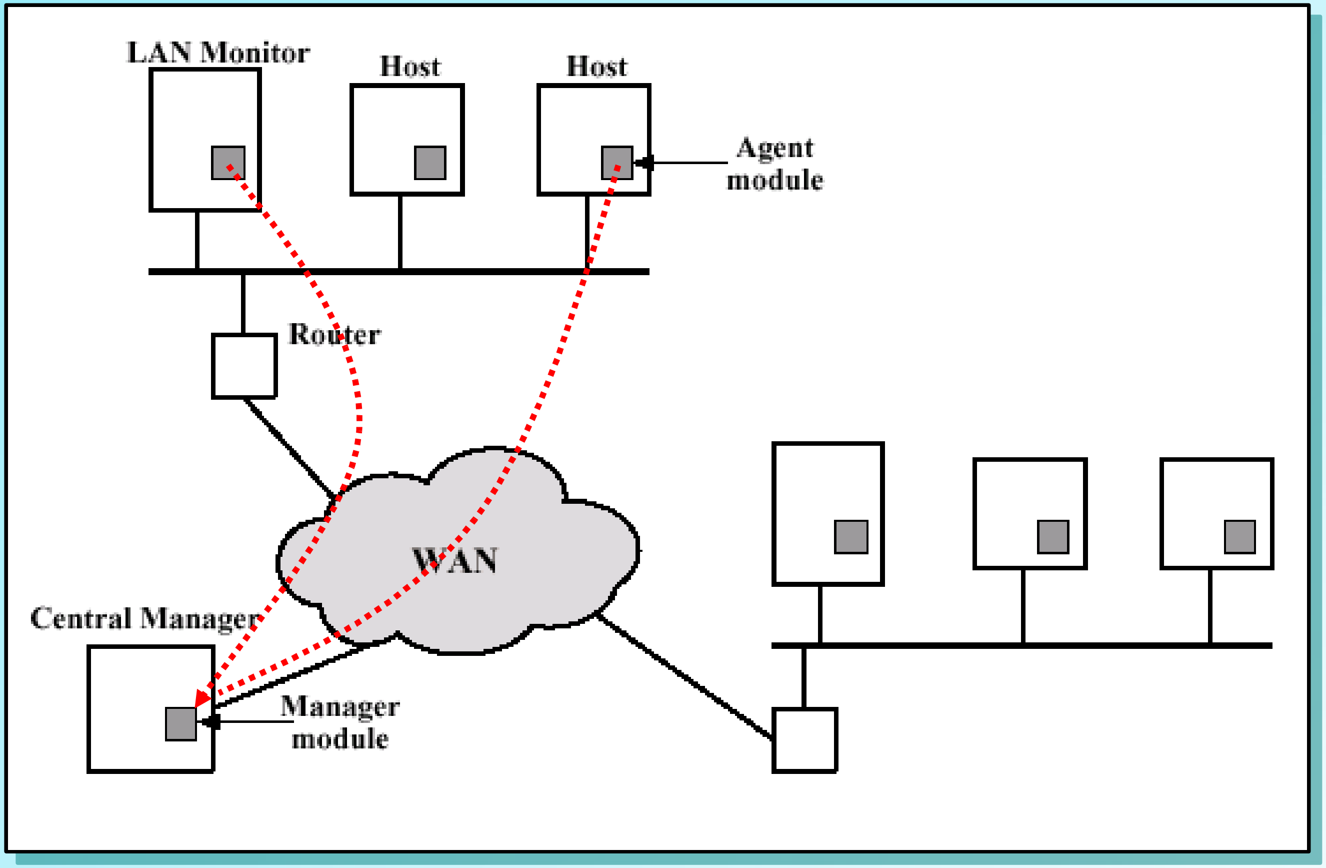
The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection - Stefan Axelsson

Bottom Line: IDS systems have a long way to go!

Distributed Intrusion Detection Scalability Issues

- Too much overhead for standalone IDS on each host
- Heterogeneous environment – different audit records
- Need IDS across the network
- Centralized vs decentralized issues

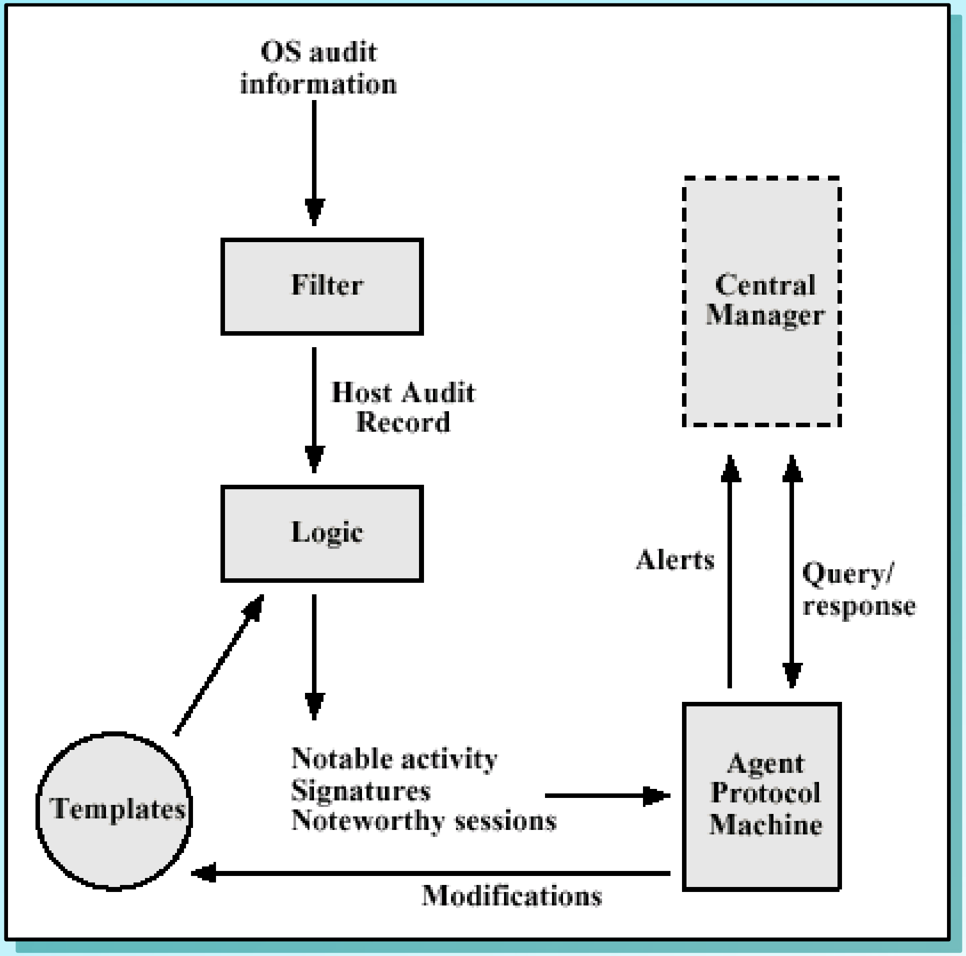
Distributed Intrusion Detection



Distributed Intrusion Detection

- Host agent module – background process collects data and sends results to the central manager
- LAN monitor agent module – analyzes LAN traffic and sends results to the central manager
- Central manager module – processes and correlates received reports to detect intrusion

Agent Architecture
Machine Independent



Honeypots

- Decoy systems
- Lure attacker from critical systems
- Collect information about the attacker
- Keep attacker around long enough to respond
- Jury is still out on this!

Password Management

Password Protection

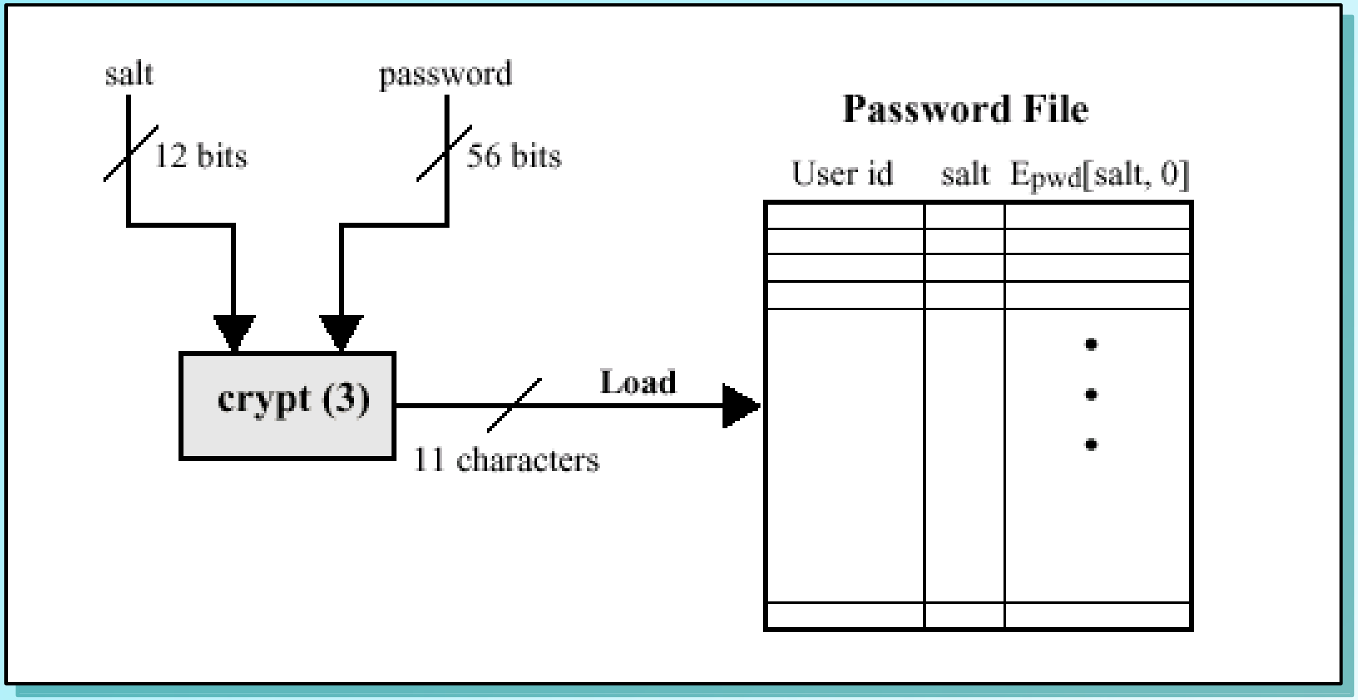
User ID and password:

- User authorized to gain access to the system
- Privileges accorded to the user
- Discretionary access control

Password Protection

- Unix system (user ID, cipher text password, plain text salt)
  - password 8 printable characters - 56-bit value (7-bit ASCII)
  - encryption routine (crypt(3)) based on DES
  - modified DES algorithm with 12-bit salt value (related to time of password assignment)
  - 25 encryptions with 64-bit block of zeros input
  - 64-bit - 11 character sequence

Loading A New Password

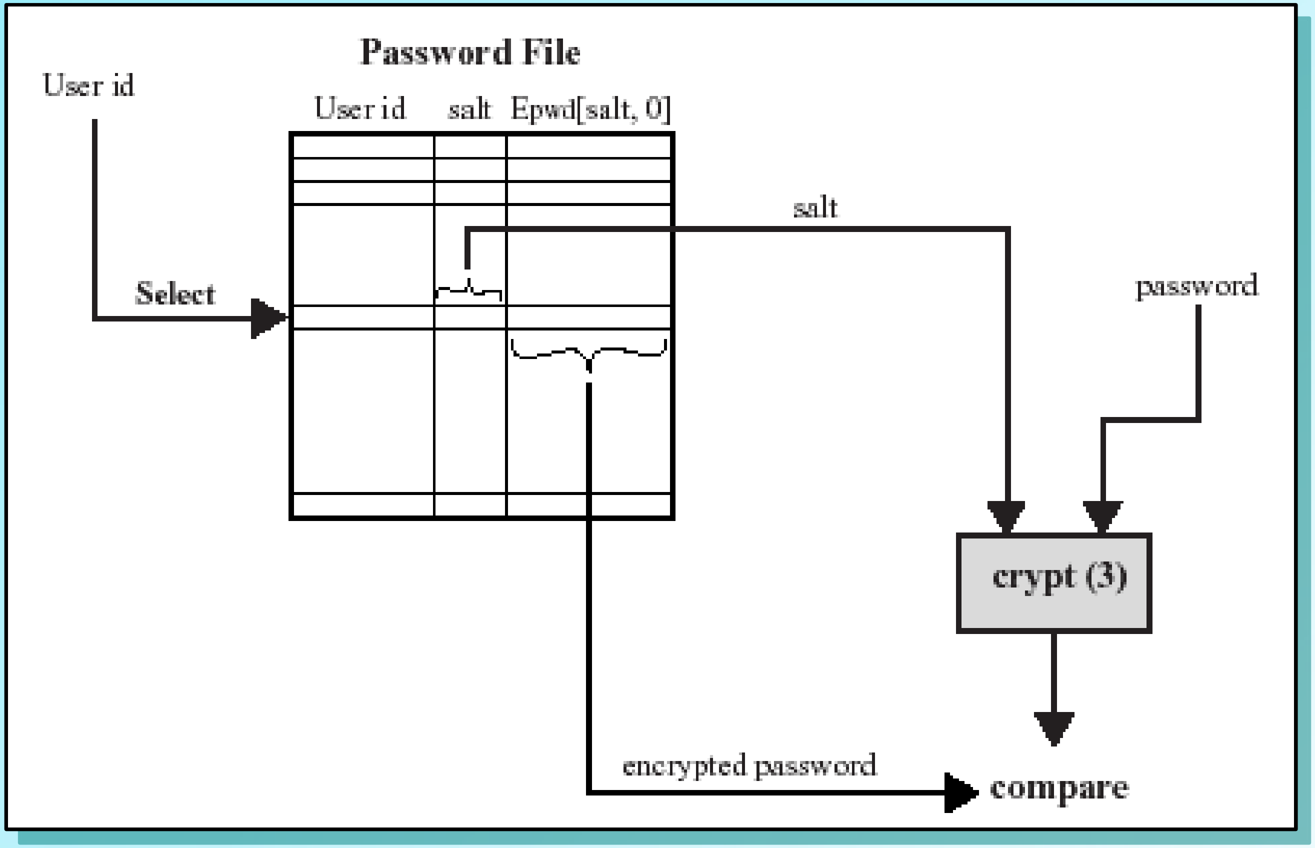


Password Protection

Purposes of salt:

- Prevents duplicate passwords from being visible
- Effectively increases password length without the user needing to remember additional 2 characters (possible passwords increased by 4096)
- Prevent use of hardware DES implementation for a brute-force guessing attack

Verifying A Password



Password Protection

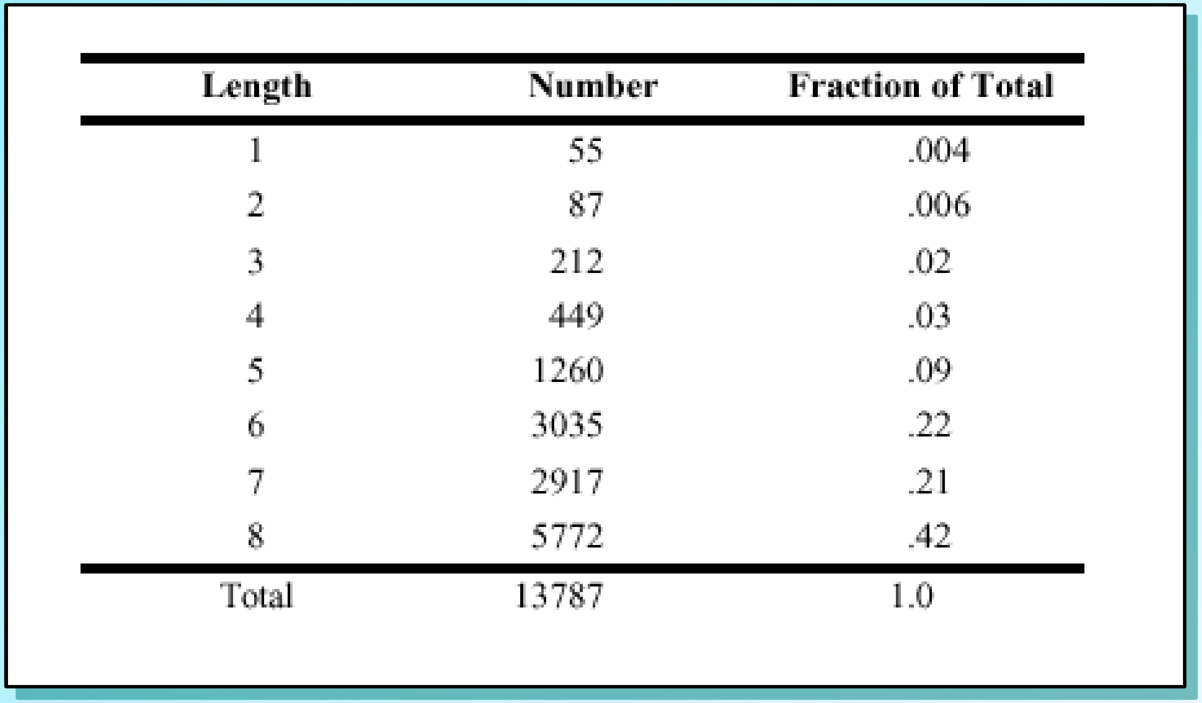
Unix password scheme threats:

- Gain access through a guest account and run a password cracker
- Obtain a copy of the password file and run a password cracker

Goal: Run a password cracker

- Rely on people choosing easily guessable passwords!

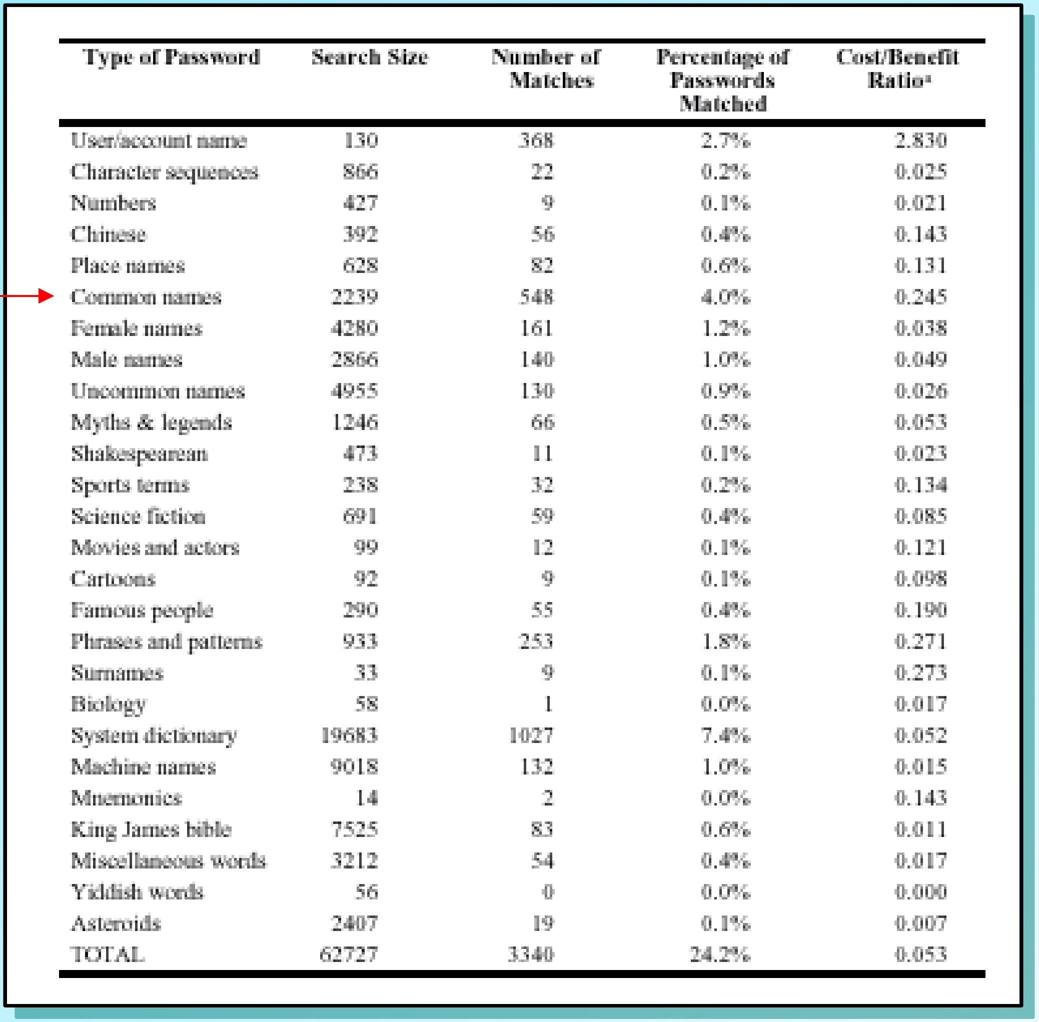
Observed Password Lengths In a Purdue Study



Length	Number	Fraction of Total
1	55	.004
2	87	.006
3	212	.02
4	449	.03
5	1260	.09
6	3035	.22
7	2917	.21
8	5772	.42
Total	13787	1.0

Passwords Cracked From A Sample Set

easy pickin's →



Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths & legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Access Control

One Method: *Deny access to password file*

- Systems susceptible to unanticipated break-ins
- An accident in protection may render the password file readable compromising all accounts
- Users have accounts in other protection domains using the same passwords

Access Control

- *Answer:*
  Force users to select passwords that are difficult to guess
- *Goal:*
  Eliminate guessable passwords while allowing the user to select a password that is memorable

Password Selection Strategies
(Basic Techniques)

- User education
  - Users may ignore the guidelines
- Computer-generated passwords
  - Poor acceptance by users
  - Difficult to remember passwords

Password Selection Strategies

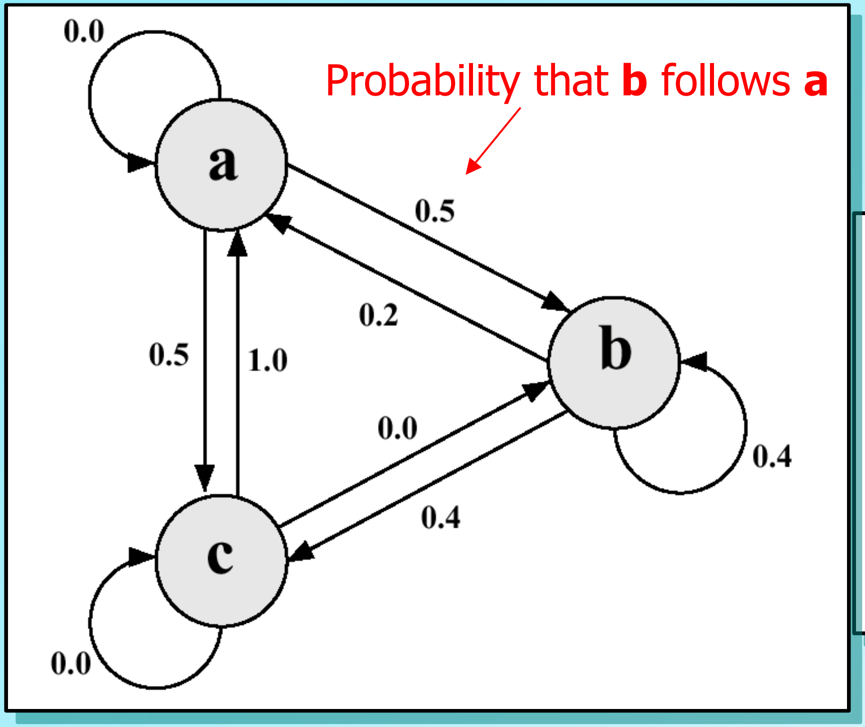
- **Reactive password checking**
  - System runs its own password cracker
  - Resource intensive
  - Existing passwords remain vulnerable until reactive checker finds them
- **Proactive password checking**
  - Password selection is guided by the system
  - Strike a balance between user accessibility and strength
  - May provide guidance to password crackers (what not to try)
  - Dictionary of bad passwords (space and time problem)

Proactive Password Checker

There are two techniques currently in use:

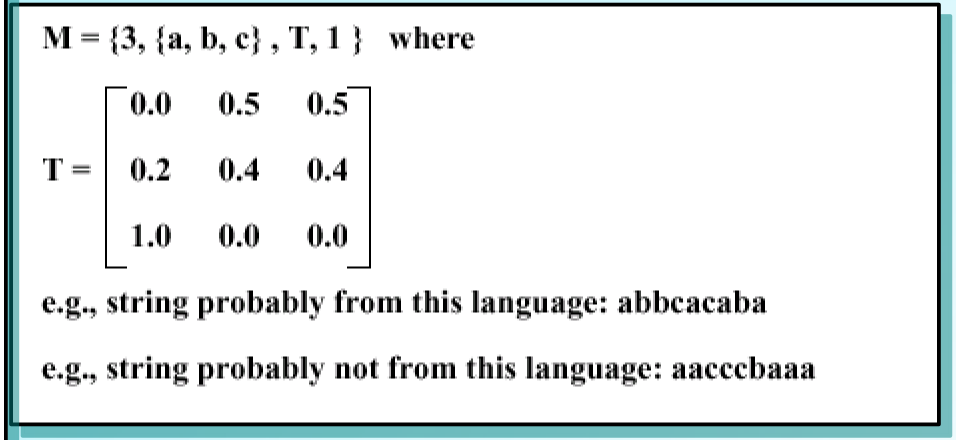
- Markov Model – search for guessable password
- Bloom Filter – search in password dictionary

Markov Model



Probability that **b** follows **a**

M = {states, alphabet, prob, order}



M = {3, {a, b, c} , T, 1 } where

$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

e.g., string probably from this language: abbcacaba

e.g., string probably not from this language: aacccbaaa

Markov Model

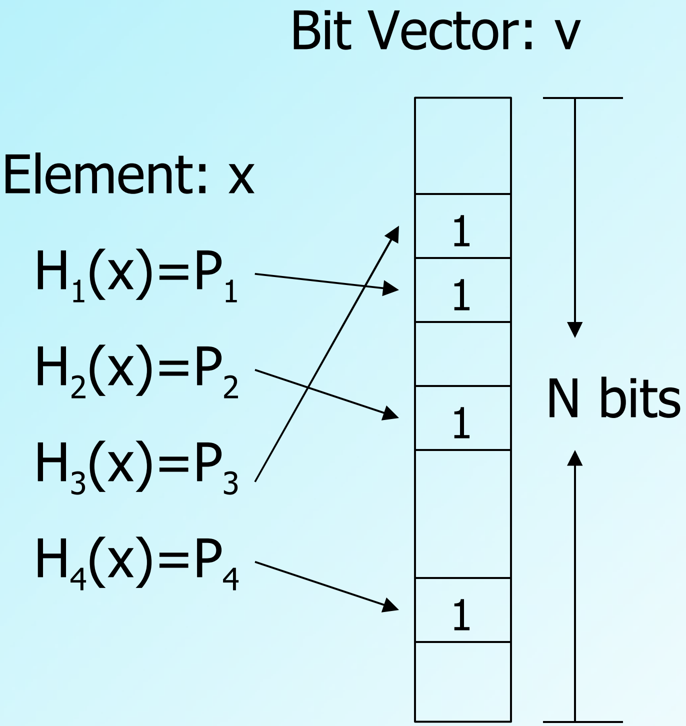
- "Is this a bad password?"...same as...
- "Was this password generated by this Markov model?"
- Passwords that are likely to be generated by the model are rejected
- Good results for a second-order model

Bloom Filter

- A probabilistic algorithm to quickly test membership in a large set using multiple hash functions into a single array of bits
- Developed in 1970 but not used for about 25 years
- Used to find words in a dictionary also used for web caching
- Small probability of false positives which can be reduced for different values of *k*, # hash funcs
- www.cs.wisc.edu/~cao/papers/summary-cache/node8.html – a good tutorial

Bloom Filter

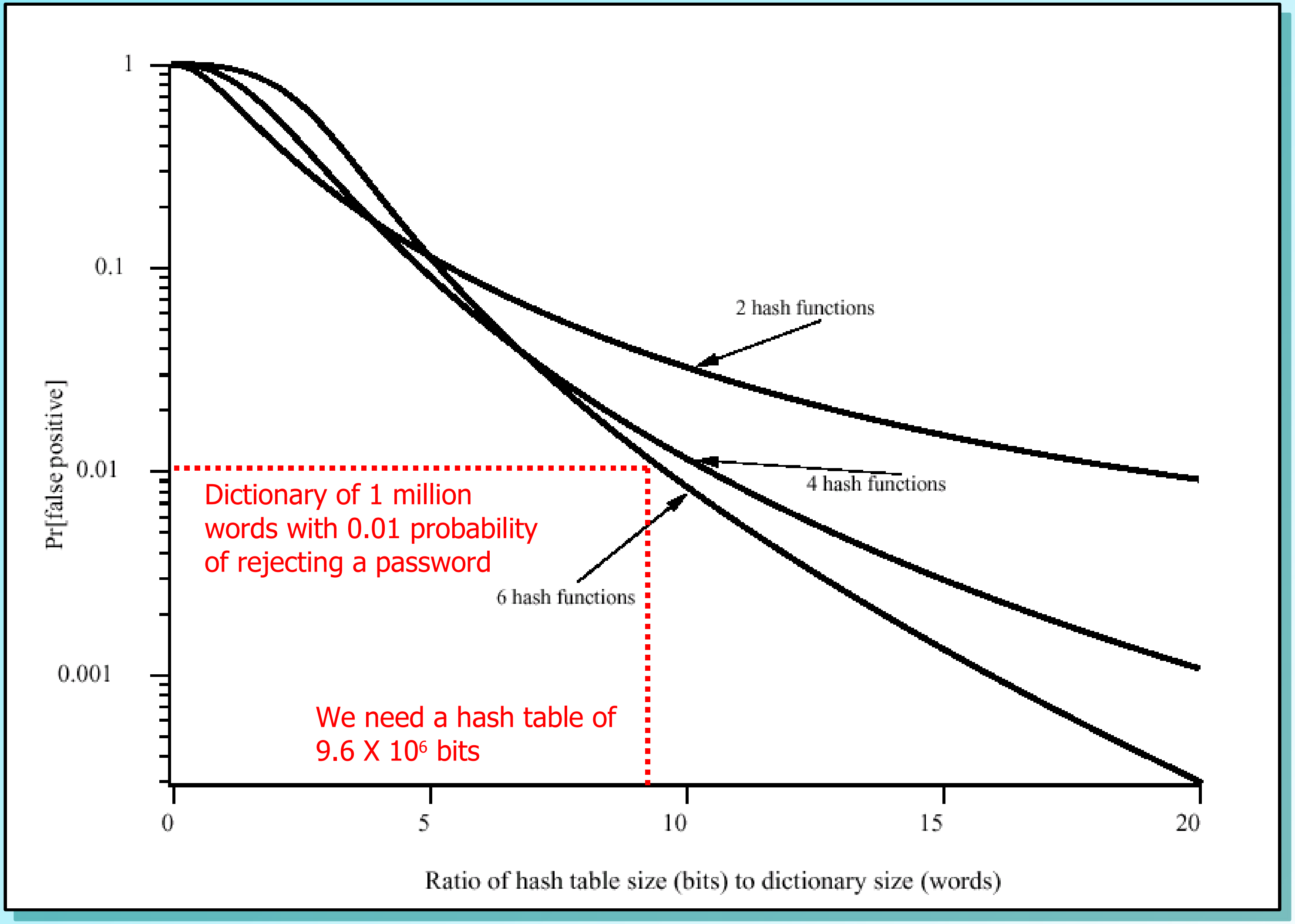
- A vector v of N bits
- k independent hash functions. Range 0 to N-1
- For each element x, compute hash functions $H_1(x)$, $H_2(x)$…$H_k(x)$
- Set corresponding bits to 1
- *Note:* A bit in the resulting vector may be set to 1 multiple times



Bloom Filter

- To query for existence of an entry x, compute $H_1(x)$, $H_2(x)$…$H_k(x)$ and check if the bits at the corresponding locations are 1
- If not, x is definitely not a member
- Otherwise there may be a false positive (passwords not in the dictionary but that produce a match in the hash table). The probability of a false positive can be reduced by choosing k and N

Performance of Bloom Filter



Dictionary of 1 million words with 0.01 probability of rejecting a password

We need a hash table of 9.6×10^6 bits

Important URLs

- http://www.cert.org/
  Originally DARPA’s computer emergency response team. An essential security site
- http://project.honeynet.org/
  Organization of security professionals dedicated to learning the tools, tactics, and motives of the blackhat community - interesting tools and papers
- http://tlc.discovery.com/convergence/hackers/ha

  Good overview of the psychology of hackers
- http://www.aaai.org/AITopics/html/uncert.html
  Good probability and Bayes overview

Homework

- Read Chapter Nine
- Final Project/Term Paper Due Next Week
- No lateness! (Problems? Let Me Know Before)

Happy Cinco de Mayo!!!