MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Lecture 9:
Intrusion Detection

Unit Objectives

- ✓ OSI security architecture
  - **common security standards and protocols for network security applications**
  - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of **web servers**, and their possible countermeasures
- ✓ Wireless Network Security Issues
- ✓ security threats of **email systems** and their possible countermeasures
- ✓ IP security
- ✓ intrusion detection techniques for security purpose
- • risk of malicious software, virus and worm threats, and countermeasures
- • firewall deployment and configuration to enhance protection of information assets
- • network management protocol for security purpose

Review of Previous Lecture

Key points from the last lecture:

- **TCP/IP protocol suite used for transmitting data over the Internet does not employ any security feature**
- **However, security can be implemented additionally at different layers**
  - PGP, SET at application layer
- **A more general purpose solution would be to employ security at the network (IP) layer**
- **IPSec is a set of protocols to provide high quality, interoperable, and cryptology-based security for IP packets**
  - offers authentication, confidentiality and key management
- **IPSec consists of three major protocols:**
  - Authentication Header – adds an extra header for authentication
  - Encapsulating Security Payload – adds extra headers for confidentiality and authentication
  - Internet Key Exchange (IKE) – negotiates security parameters
- **IPSec operates in two modes**
  - Transport mode: host-to-host security
  - Tunnel mode (e.g., VPN): network-to-network, host-to-network and host-to-host security
- **Security Associations**
  - 3 parameters (SPI, IP destination, Security protocol identifier)

Lecture 9 : Objectives

On completion of this session you should:

- Understand the impact of intrusion on corporate organization
- Be familiar with different types of intruders
- Understand the importance of early intrusion detection
- Describe common techniques used by the intruders
- Discuss different intrusion detection techniques
- Be familiar with the general guidelines for intrusion detection
- Discuss the strategies for response to intrusion
- Be familiar with the CERT recommendation for responding to intrusion

Lecture 9: Outline

- **Why is intrusion detection necessary?**
- **Types of intruders**
- **Common intrusion techniques**
- **Intrusion detection techniques**
  - statistical anomaly detection
  - rule based detection
- **Response to Intrusion**
- **Password management**

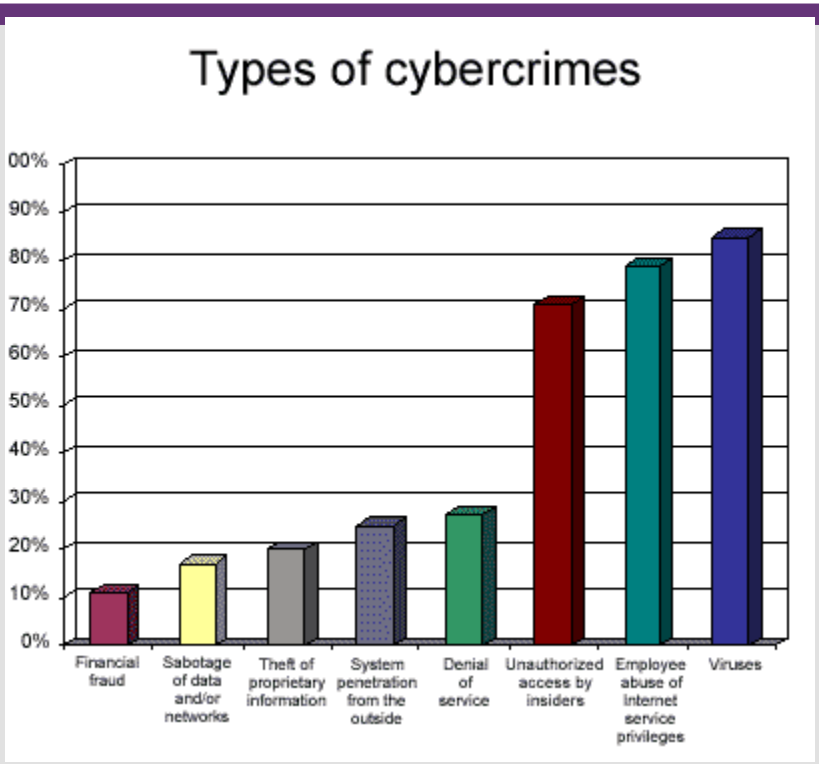
Intrusion

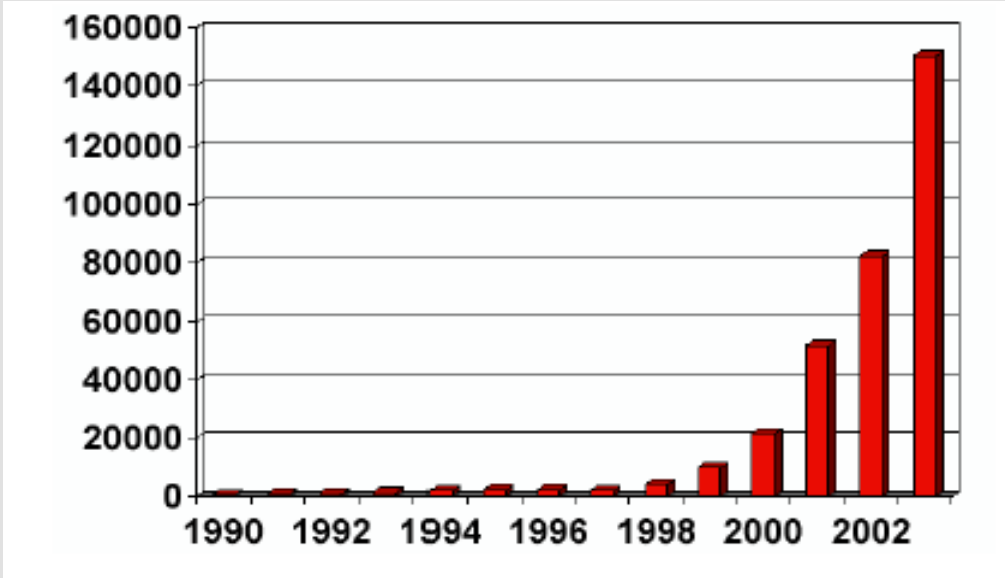
- **In the USA, intrusion on computer infrastructures of big organization are becoming an increasingly serious problem**
  - big telecommunication companies, universities, financial organizations have reported hacking
  - even CIA was no exception
  - commercial organizations are less willing to report such events
- **Intrusion, commonly known as hacking, is the unauthorized access or acquisition of higher than authorized access privileges into a computer system**
- **Early detection of intrusion and deployment of preventive measure is crucial for maintaining the security of the system**

Intrusion: Case Histories

- **Intrusion reported in USA in the past**
  - hackers apparently working from Russia have systematically broken into Defense Department computers for more than a year
  - At NASA, the attack was massive
  - after NATO jets hit the Chinese Embassy in Belgrade in May 1999, hackers from China attacked a handful of U.S. government sites, including one maintained by the Energy Department
  - the White House Web site was shut down
  - three nuclear weapons labs were shut down
  - and many others …
  - a list of computer crimes with estimated $-loss at: http://www.justice.gov/usao/priority-areas/cyber-crime

Intrusion: Rising Trends



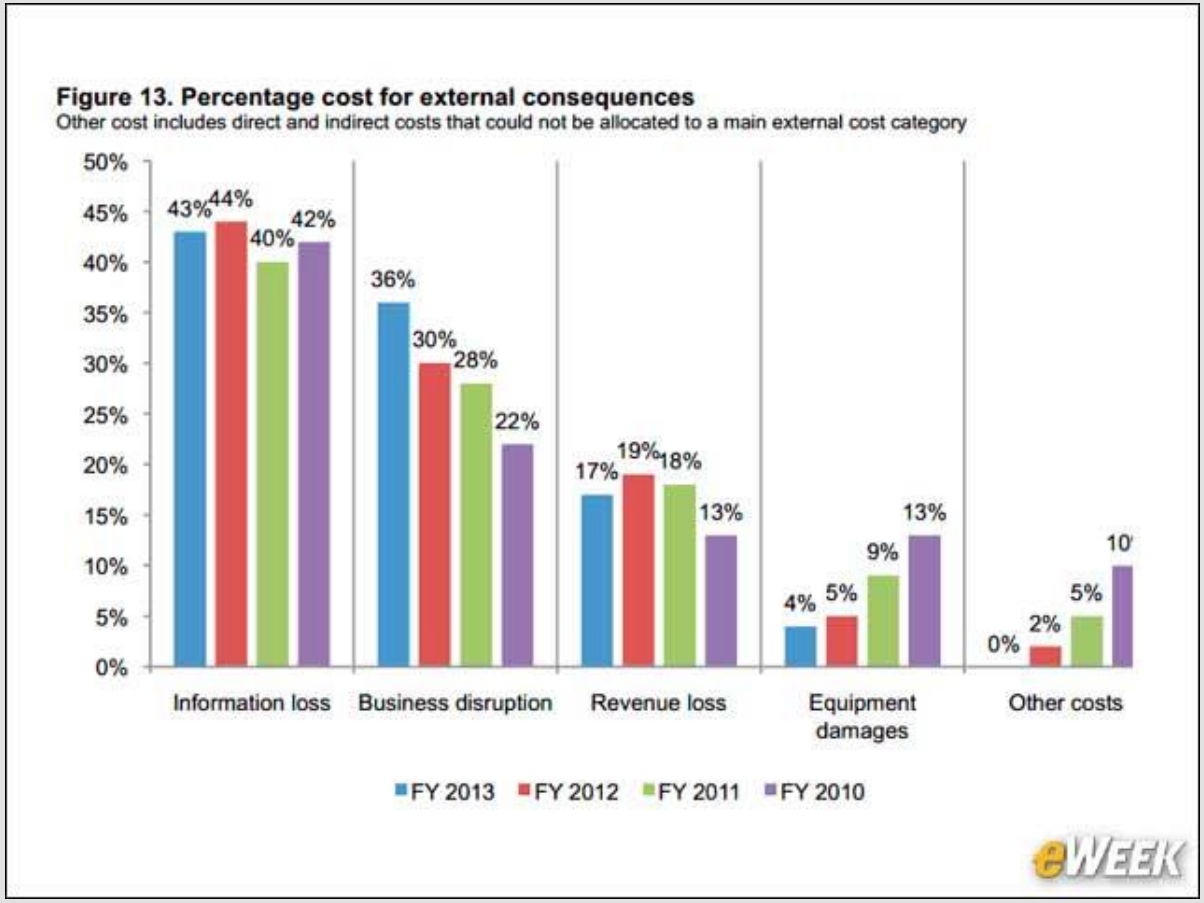


http://www.cert.org/stats/

These numbers are just a trend indicator, as:

- **only a small fraction of attacks is detected, and**
- **not all detected attacks are reported**

Intrusion: Rising Trends



Types of Intruders (1)

- **Intruders can be classified in three broad categories**
  - **Masquerader**
    - > an unauthorized user who penetrates a system's access control to exploit other's account;
    - > most likely an **outsider**
  - **Misfeasor**
    - > a legitimate user but accesses data, program or resources for which he/she is not authorized;
    - > generally an **insider**
  - **Clandestine**
    - > an individual who seizes supervisory control and evades auditing and access control;
    - > may be an **insider or outsider**

Types of Intruders (2)

- **Again there are two levels of Intruders:**
  - **People with high level of system expertise**
    - > personally constructed methods for breaking into systems
  - **Others are "foot soldiers", uses cracking programs developed and distributed by others**
    - > willing to spend countless hours looking for weakest links

Intruders

- **clearly a growing publicized problem**
  - from “Wily Hacker” in 1986/87
  - to clearly escalating CERT stats
- **Intruder attack ranges as**
  - **benign:** explore, still costs resources
  - **serious:** access/modify data, disrupt system
- **led to the development of CERTs**
- **intruder techniques & behavior patterns are constantly shifting, have common features**

Examples of Intrusion

- remote root compromise of an email server
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- running a packet sniffer
- distributing pirated software
- using an unsecured modem to access internal n/w
- 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**
- **awareness led to establishment of CERTs**
  - collect / disseminate vulnerability info / responses

Hacker Behavior Example

- **select target using IP lookup tools (NSLOOKUP)**
- **map network for accessible services (NMAP)**
- **identify potentially vulnerable services (pcAnywhere)**
- **brute force (guess) passwords**
- **install remote administration tool (Dame Ware)**
- **wait for admin to log on and capture password**
- **use password to access remainder of network**

Criminal Enterprise

- **organized groups of hackers now a threat**
  - corporation / government / loosely affiliated gangs
  - typically young
  - often Eastern European or Russian hackers
  - often target credit cards on e-commerce server
- **criminal hackers usually have specific targets**
- **once penetrated act quickly and get out**
- **IDS / IPS help but to some extent less effective**
- **sensitive data needs strong protection**

Criminal Enterprise Behavior

- **act quickly and precisely to make their activities harder to detect**
- **exploit perimeter via vulnerable ports**
- **use trojan horses (hidden software) to leave back doors for re-entry**
- **use sniffers to capture passwords**
- **do not stick around until noticed**
- **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
- **IDS / IPS may help but also need:**
  - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Insider Behavior Example

- **create network accounts for themselves and their friends**
- **access accounts and applications they wouldn't normally use for their daily jobs**
- **e-mail former and prospective employers**
- **conduct furtive instant-messaging chats**
- **visit web sites that cater to disgruntled employees, such as f'dcompany.com**
- **perform large downloads and file copying**
- **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

Password Guessing

- **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
    - > eg. telnet, FTP, web, email
  - extracting recorded info after successful login (web history/cache, like last number dialed etc.)
- **using valid login/password can impersonate user**
- **users need to be educated to use suitable precautions/countermeasures**

Intrusion Detection

- **inevitably Intrusion prevention System IPS will have security failures**
- **so need also to detect intrusions so can**
  - block if detected quickly
  - act as deterrent
  - collect info to improve security
- **assume intruder will behave differently to a legitimate user**
  - but will have imperfect distinction between regular ←→ intruder

Defensive Strategies

- **Principal defensive strategies:**
  - prevention
  - detection
  - response
- **Preventive strategies may not always be practical**
  - it is too **expensive** to prevent all potential attack techniques
  - legitimate **users get annoyed** by too many **preventive measures** and may even start to **circumvent** them (introducing new vulnerabilities)
  - preventive measures **may fail**:
    - > incomplete or erroneous specification / implementation / configuration
    - > inadequate deployment by users (just think of passwords...)

Why is Early Intrusion Detection Necessary?

- **Intruder can be identified and excluded from the system before any damage is done**
- **Can determine the damage**
  - which sensitive data, system, and network is attacked
  - what breaches (confidentiality, integrity or availability) have occurred
  - Appropriate response may mitigate the extent of damage and bring the system back to current operational state quickly
- **A strong and efficient detection system can act as a deterrent for other hackers**
- **Detection enables the system administrators to collect information on intrusion techniques**
  - can be used to review and reinforce the prevention policy

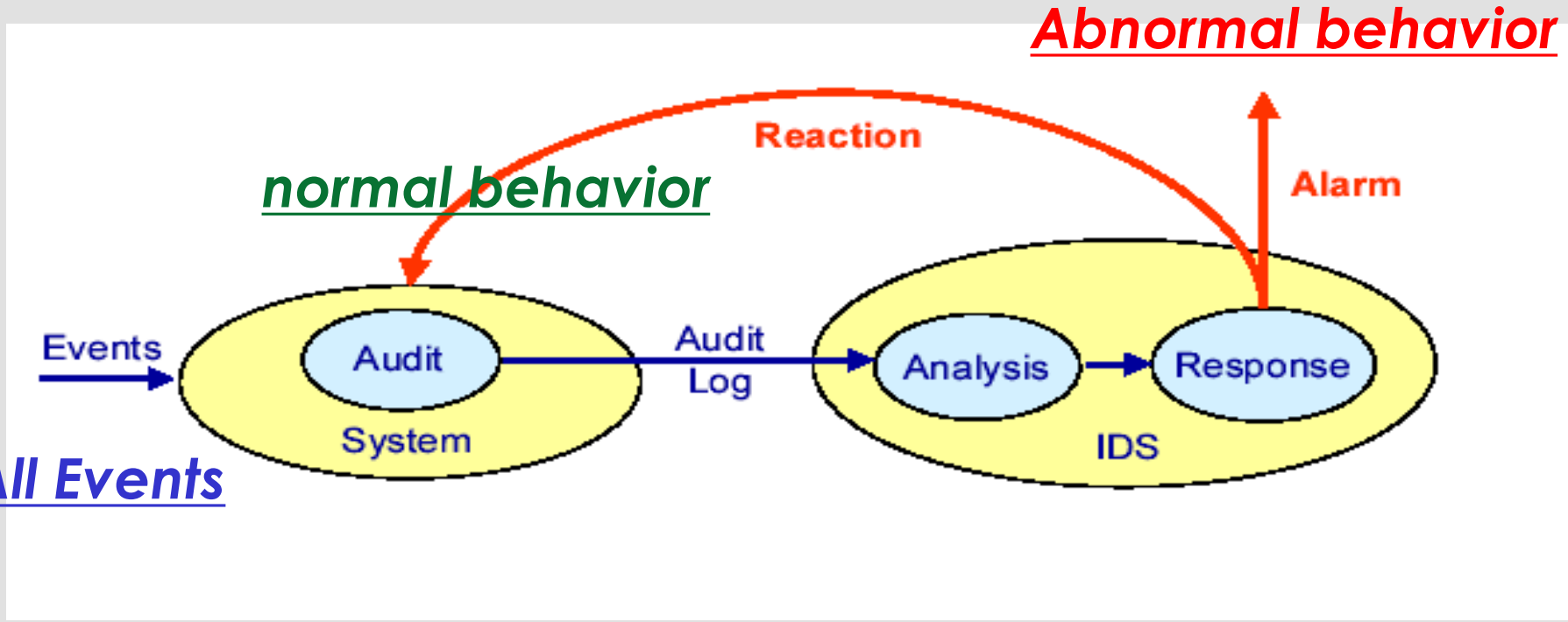
Common Intrusion Techniques (1)

- **System maintains a file that associates a password with each authorized user**
- **Password file can be protected with:**
  - **One-way encryption:**
    - password is used to generate a key for the encryption function
    - a fixed length output is produced
  - **Access control**
    - access to password file is limited to one or few system administrators

Intrusion Detection System (IDS)

- **The goal of IDS is the supervision of**
  - **computer systems and communication infrastructures in order to detect intrusions and misuse**
- **What can be attained with intrusion detection?**
  - Detection of **attacks and attackers**
  - Detection of **system misuse** (includes misuse by legitimate users)
  - Limitation of **damage** (if response mechanisms exist)
  - **Gain experience** in order to **improve** preventive measures
  - **Deterrence** of potential attackers

IDS Schematic Diagram



IDS Components

- **Main components of IDS**
  - **Audit Records:**
    - recording of all security relevant events of a supervised system
    - preprocessing and management of recorded audit data
  - **Detection:**
    - automatic **analysis of audit data**
    - analysis is based on the assumption that the **behavior** of the **intruder differs** from that of a **legitimate user** in ways that can be quantified
  - **Response:**
    - reporting of detected attacks **(alarms)**
    - potentially also initiating countermeasures **(reaction)**

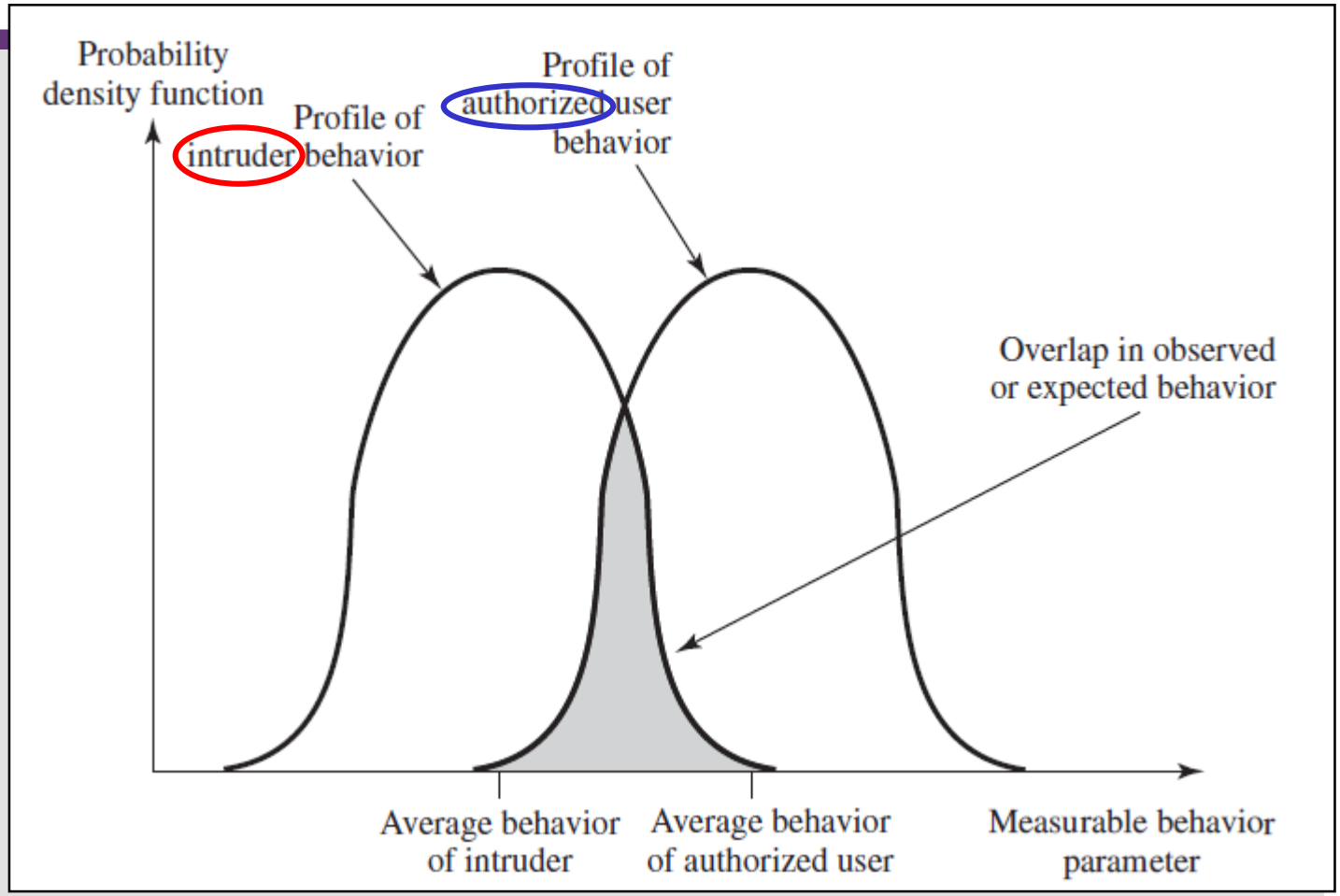
Audit Records (1)

- **Audit data delivers information on:**
  - who accessed – initiator of action
  - when, where and how – name, time, location of the action
  - whose and which resource? – resource usage
- **Events recorded in a computer system:**
  - opening of files
  - execution of programs
  - detected access violation
  - failed password verification etc.
- **Events recorded in a network:**
  - connection establishment and release
  - packets transferred from / to specific systems / ports
  - specific signalling events, e.g. ICMP network unreachable message, etc.

Audit Records (2)

- **Native audit records (Default types)**
  - part of all common multi-user O/S
  - already present for use
  - may not have info required in desired form
    - > needs further processing before applying to the detection system
- **Detection-specific audit records (Special IDS types)**
  - created specifically to collect required info
  - at cost of additional overhead on system

User Profile Analysis



Profiles of behavior of intruders and authorized Users

Measures for Analysis

- Login frequency by day and time
- Frequency of login at different locations
- Time since last login
- Password failures at login
- Execution frequency
- Execution denials
- Read, write, create, delete frequency
- Failure count for read, write, create and delete

Approaches to Analysis

- **Two main approaches to analysis:**
  - **Statistical anomaly detection**
    - > Assumption: “normal user behavior” can be described statistically
      - – requires a learning phase / specification of normal behavior
    - > Analysis: compares recorded events with reference profile of normal behavior
  - **Rule Based detection**
    - > defines a set of rules to decide whether a behavior is suspicious
    - > Two types:
      - – Anomaly detection
      - – Penetration identification

Statistical anomaly detection (1)

- **Two types:**
  - Type-I:-**Threshold detection:**
    - > counts the number of occurrence of a specific event (e.g., log on number during a given time)
    - > if the counter value exceeds certain number, an intrusion is suspected
    - > Problem:
      - ineffective against even moderately sophisticated attackers
      - determining the appropriate threshold is difficult because of the variability of users

Statistical anomaly detection (2)

- **Two types:**
  - Type-II:- **Profile Based:**
    - > characterize past behavior of users
    - > a profile of average user is build by analyzing audit records over a period of time
      - parameter used: counter, gauge, interval between events, resource utilization
    - > The learning model learns what is a normal behavior and any deviation from that is treated as intrusion

Statistical anomaly detection (3)

- **Audit Record Analysis used in Statistical AD**
  - 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
  - key advantage is no prior knowledge is used
    - > thus it should be readily portable among a variety of systems.

Rule-Based Intrusion Detection (1)

- **Defines a set of rules to decide whether a behavior is suspicious**
- **Two types:**
  - **Anomaly detection**
    - ✓ historical audit records are analyzed to generate rules that describes the user behavior pattern
    - ✓ current behavior is checked against these rules
    - ✓ any considerable deviation signals intrusion
    - ✓ a large database of rules is necessary (104 to 106 rules)
    - ✓ *does not require knowledge of security vulnerabilities within the system*

Rule-Based Intrusion Detection (2)

- **And the second type:**
  - **Penetration Identification**
    - > based on knowledge of known penetrations that would exploit known weakness
      - If we have knowledge of known penetration, we can devise rule to detect any such activity
    - > rules are specific to machine and OS
    - > rules are generated by experts rather than by analyzing audit records
      - no user profiling
      - Involves input from system administrator and security analyst to collect a suite of known scenarios and key events that threaten security
    - > audit records of a user are checked against the rules. If a match is found, then user's suspicion rating is increased. If this rating goes above a threshold, an anomaly is reported

CERT Guidelines for Intrusion Detection

1. Monitor and inspect system resource use
2. Monitor and Inspect network traffic and connections
3. Monitor and inspect user account and file access
4. Scan for viruses
5. Verify file and data integrity
6. Probe for system and network vulnerability
7. Reduce, scan, monitor, and inspect log files

Intrusion Detection Tools

- **Commercial products:**
  - **IDS (Cisco Systems)**
  - **IPS (Captus Network)**
  - **RealSecure (Internet Security Systems)**
  - **Computer misuse detection system (CMDS) (SAIC)**
  - **ClearICE (Clarion Developer)**
- **Public Domain**
  - **Shadow**
  - **Network Flight Record**

  (jointly developed by the **Naval Surface Warfare Center**, the **National Security Agency**, and the **SANS Institute**, USA)

Response to Intrusion (1)

- **Organizations should have a well prepared plan in place on how to respond when an intrusion is detected**
- **The practices recommended by the CERT:**
  - **Analyze all available information**
    - > capture and record system information
    - > back up and isolate the compromised systems
    - > examine logs, identify the attack used to gain access and what traces the intruder left behind
  - **Communication with relevant parties**
    - > Inform the other affected sites using a secure communication channel
  - **Collect and protect information**
    - > collect all relevant system and network logs from the compromised system
    - > preserve evidence
    - > contact law enforcement

Response to Intrusion (2)

- **Recommended steps by CERT:**
  - **Contain the intrusion**
    - > temporarily shut down the system
    - > or disconnect the compromised system from the network
    - > disable access, services and accounts, and monitor system and network activities
  - **Eliminate all means of intruder access**
    - > change passwords
    - > reinstall compromised systems
    - > restore executable program from original distribution
    - > review system configurations, correct system and network vulnerabilities
    - > improve detection mechanism

Response to Intrusion (3)

- **Recommended steps by CERT:**
  - **Return systems to normal operation**
    - > restore user data
    - > reestablish availability of services and systems
    - > watch for signs of intruder's return.
  - **Implement lesson learned**
    - > re-evaluate and upgrade security policy
    - > revise security documents

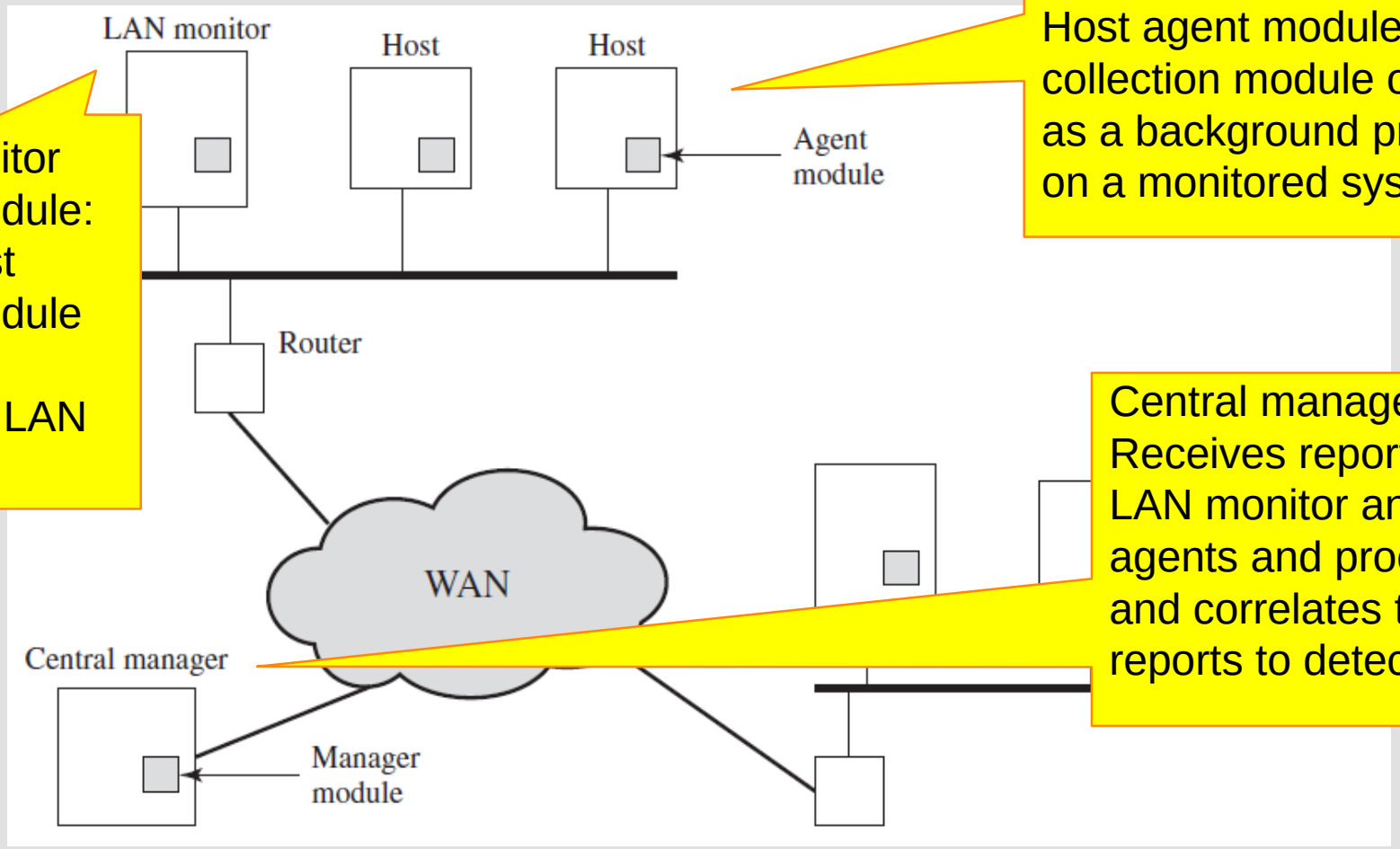
Base-Rate Fallacy

- **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**
- **A study of existing intrusion detection systems indicated that current systems have not overcome the problem of the base-rate fallacy.**

Distributed Intrusion Detection

- **traditional focus is on single systems**
- **but typically we 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

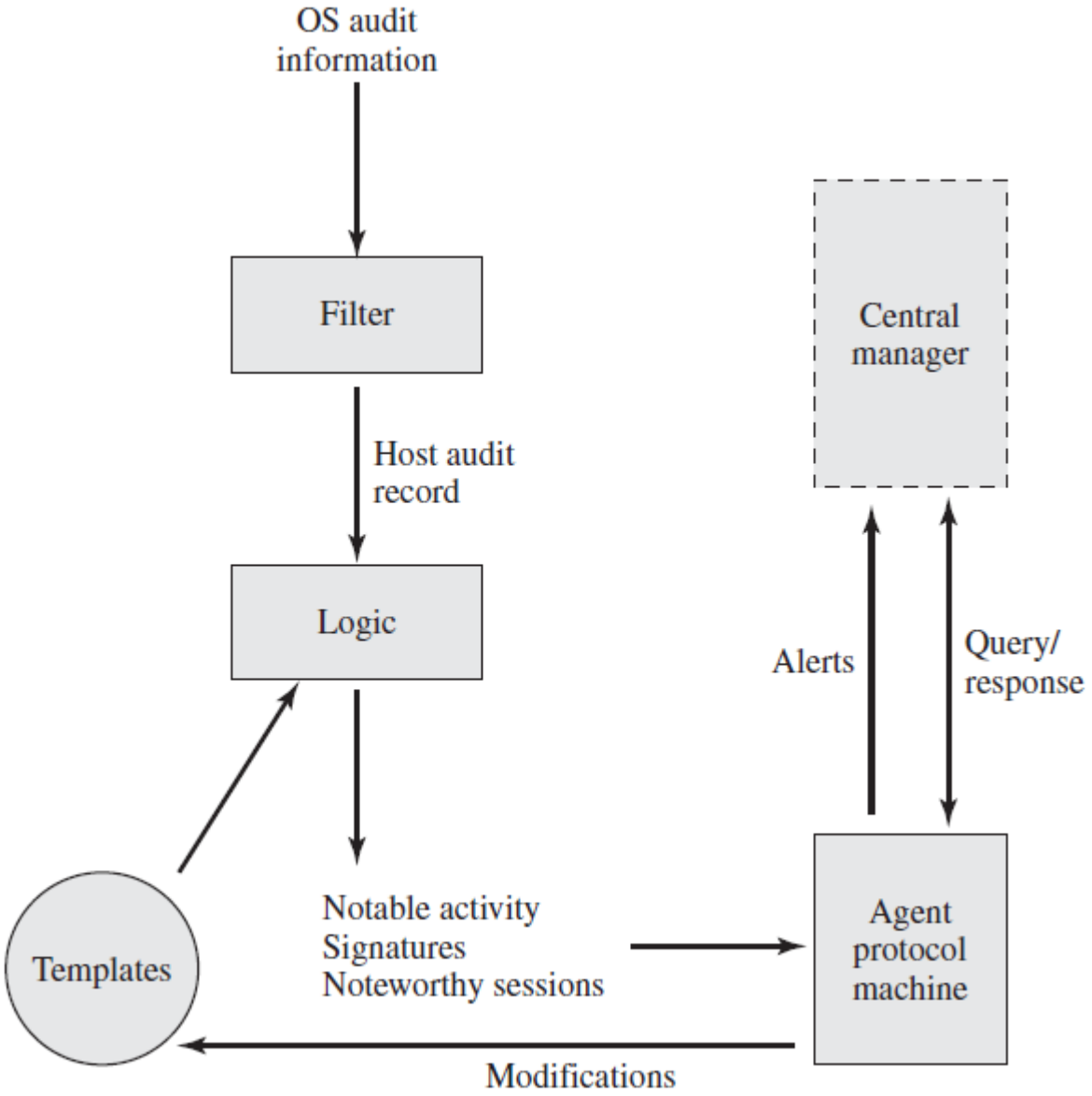


LAN monitor agent module: like a host agent module except it analyzes LAN traffic

Host agent module: audit collection module operating as a background process on a monitored system

Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion

Distributed Intrusion Detection – Agent Implementation



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
- **are filled with fabricated information**
- **instrumented to collect detailed information on attackers activities**
- **single or multiple networked systems**
- **IETF Intrusion Detection WG standards**

Password Management

- **front-line defense against intruders**
- **users supply both:**
  - login ID – 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**
- **Klein 1990 - many guessable passwords**
- **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**
- **but is resource intensive**
- **bad passwords are vulnerable till found**

Managing Passwords - **Proactive Checking**

- **most promising approach to improving password security**
- **allow users to select own password**
- **but have system verify it so that it is acceptable**
  - simple rule enforcement (see earlier slide-user education)
  - compare against dictionary of bad passwords
  - use algorithmic (markov model or bloom filter) to detect poor choices

Password Vulnerabilities

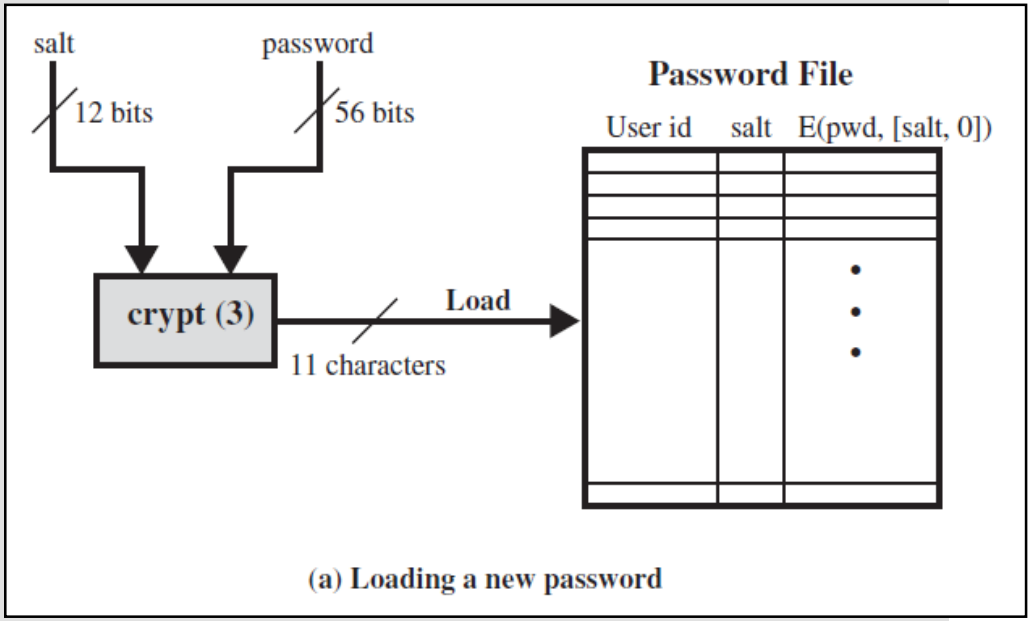
- User can gain access on a machine using guest account and run password cracker program
- Or copy the password file and run cracking program on another machine
- Password cracker rely on the fact that some people choose easily guessable passwords
  - own name
  - common name, street name
  - too short
  - common dictionary words
- Measures should be taken to deny opponents access to password file

Table 9.5 Passwords Cracked from a Sample Set of 13,797 Accounts [KLEI90]

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

UNIX Password Scheme (1)

- **Each user selects a password of up to 8 characters in length**
  - this is converted to 56-bit
  - this 56-bit serves as a key to a modified DES algorithm
- **A salt of 12-bit is generated**
  - usually related to the time when password is created
- **DES algorithm is modified using salt, called crypt (3)**
- **Crypt (3) is exercised on 64-bit block of zeros**
- **The encryption process is repeated 25 times**
  - output of first encryption is fed to the 2nd
- **The final output is translated into 11 character sequence**



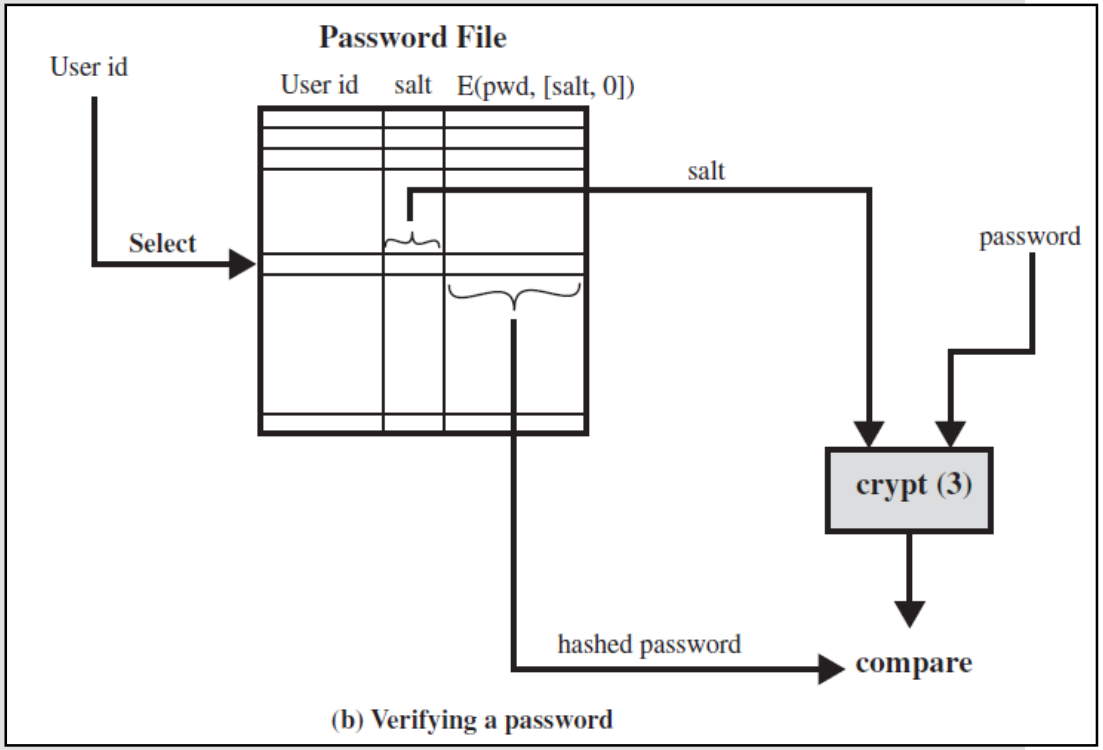
(a) Loading a new password

Crypt(3) utility:

- mkpasswd;
- openssl passwd -crypt <myPassword>

UNIX Password Scheme (2)

- **Salt serves three purposes:**
  - prevents **duplicate passwords** from being visible in the password file
  - effectively **increases the length** of the password
  - prevents the use of **hardware** implementations of DES



Further Reading

- **Study Guide 9**
- **Chapter 9 of the textbook: *Network Security Essentials-Application & Standards" by William Stallings* 5th Edition, Prentice Hall, 2013**
- **Additional resources for this week**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor's Manual and other resources made available by the author of the textbook.**