Cryptography and Network Security Chapter 20

Fifth Edition

by William Stallings

Lecture slides by Lawrie Brown

Intruders

- significant issue for networked systems is hostile or unwanted access
- either via network or local
- can identify classes of intruders:
  - masquerader
  - misfeasor
  - clandestine user
- varying levels of competence

- A significant security problem for networked systems is hostile, or at least unwanted, trespass being unauthorized login or use of a system, by local or remote users; or by software such as a virus, worm, or Trojan horse.
- One of the two most publicized threats to security is the intruder (or hacker or cracker), which Anderson identified three classes of:

- 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)

- • Intruder attacks range from the benign (simply exploring net 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
  - computer emergency response teams
- range
  - benign: explore, still costs resources
  - serious: access/modify data, disrupt system
- led to the development of CERTs
- intruder techniques & behavior patterns constantly shifting, have common features

- **Markus Hess**, a German citizen, is best known for his endeavours as a hacker in the late 1980s. Alongside fellow hackers Dirk Brzezinski and Peter Carl, Hess hacked into networks of military and industrial computers based in the United States, Europe and the East Asia, and sold the information to the Soviet KGB for US$54,000.[1] The hacked material included "sensitive semiconductor, satellite, space, and aircraft technologies

- Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there. At the serious end are individuals who are attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system.

CERT

- These cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers.
- 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.

Examples of Intrusion

- remote root compromise
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- running a packet sniffer – capture username /passwd
- distributing pirated software – anonymous FTP
- using an unsecured modem to access net
- impersonating a user to reset password
- using an unattended workstation without permission

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

1. select target using IP lookup tools – dig,
2. www.ssn.edu.in http://203.199.212.87/
3. map network for accessible services –Nmap port scanner
4. identify potentially vulnerable services - pcAnywhere Symantec tool
5. brute force (guess) passwords
6. install remote administration tool
7. wait for admin to log on and capture password
8. 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 less effective
- sensitive data needs strong protection

Criminal Enterprise Behavior

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
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.

- Benign intruders might be tolerable, although they do consume resources and
- may slow performance for legitimate users. However, there is no way in advance to know whether an intruder will be benign or malign. Consequently, even for systems with no particularly sensitive resources, there is a motivation to control this problem.

- 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.

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

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

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

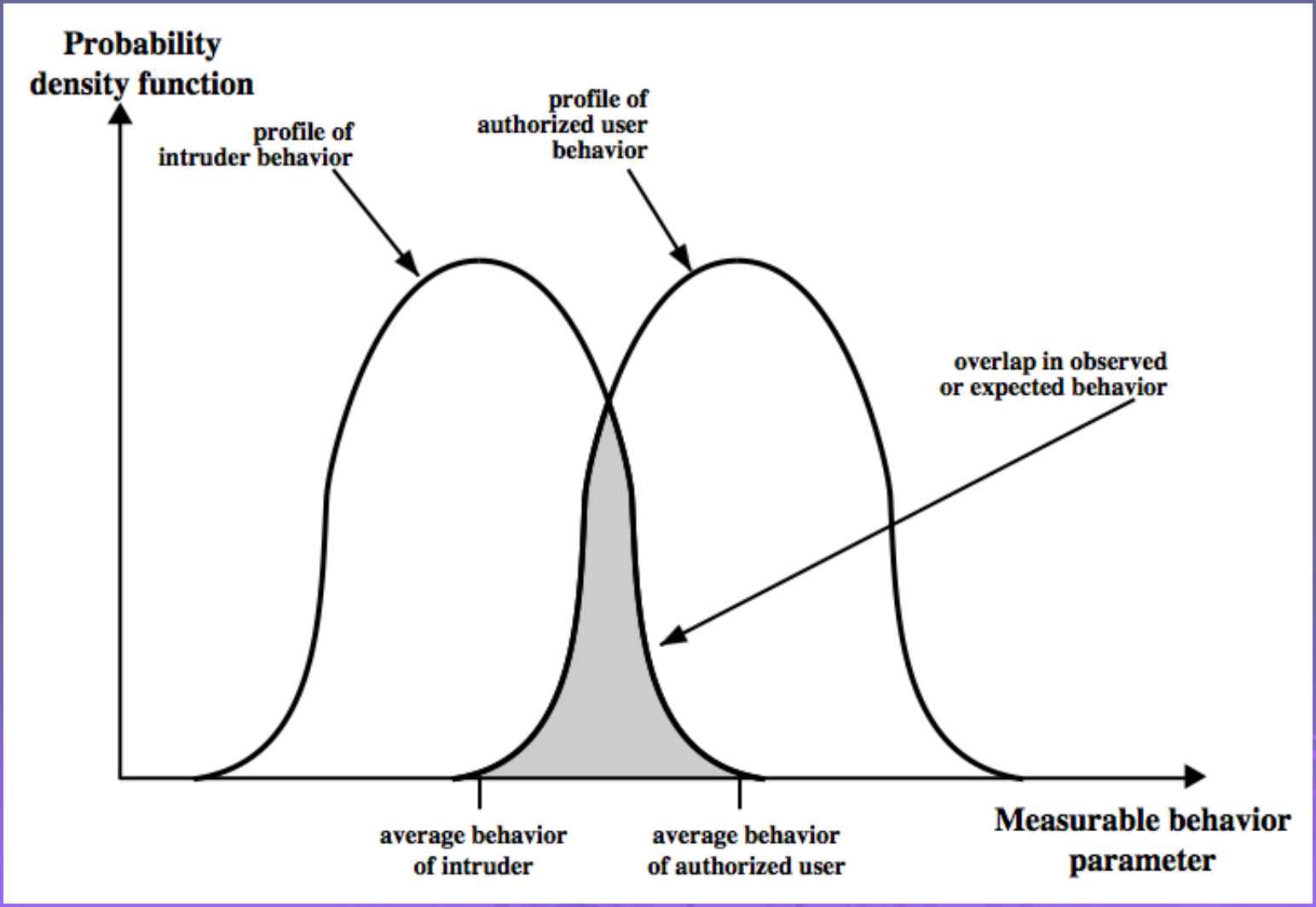
Password Capture

- 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, last number dialed etc)
- using valid login/password can impersonate user
- users need to be educated to use suitable precautions/countermeasures

Intrusion Detection

- inevitably 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

Intrusion Detection



Approaches to Intrusion Detection

- statistical anomaly detection
  - attempts to define normal/expected behavior
  - Threshold detection - threshold
  - profile based – profile of user
- rule-based detection
  - attempts to define proper behavior
  - Anomaly rules detect deviation from previous usage patterns
  - penetration identification

- statistical approaches attempt to define normal, or expected, behavior, whereas 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

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

- **Subject: Initiators of actions. A subject is typically a terminal user but might**
- also be a process acting on behalf of users or groups of users.
- • **Action: Operation performed by the subject on or with an object; for example,** login, read, perform I/O, execute.
- •

- **Object: Receptors of actions. Examples include files, programs, messages,** records, terminals, printers, and user- or program-created structures.
- **Exception-Condition: Denotes which, if any, exception condition is raised on**
- return.
- **• Resource-Usage: A list of quantitative elements in which each element gives**
- the amount used of some resource
- **• Time-Stamp: Unique time-and-date stamp identifying when the action took** place.

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

Smith	execute	<Library>COPY.EXE	0	CPU = 00002	11058721678

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

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
- key advantage is no prior knowledge used

Profile based intrusion metrics

- **Counter:** A nonnegative integer that may be incremented but not decremented until it is reset by management action. Typically, a count of certain event types is kept over a particular period of time. Examples include the number of logins by a single user during an hour, the number of times a given command is executed during a single user session, and the number of password failures during a minute.
- **Gauge:** A nonnegative integer that may be incremented or decremented. Typically, a gauge is used to measure the current value of some entity. Examples include the number of logical connections assigned to a user application and the number of outgoing messages queued for a user process.
- **Interval timer:** The length of time between two related events. An example is the length of time between successive logins to an account.
- **Resource utilization:** Quantity of resources consumed during a specified period. Examples include the number of pages printed during a user session and total time consumed by a program execution.

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

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

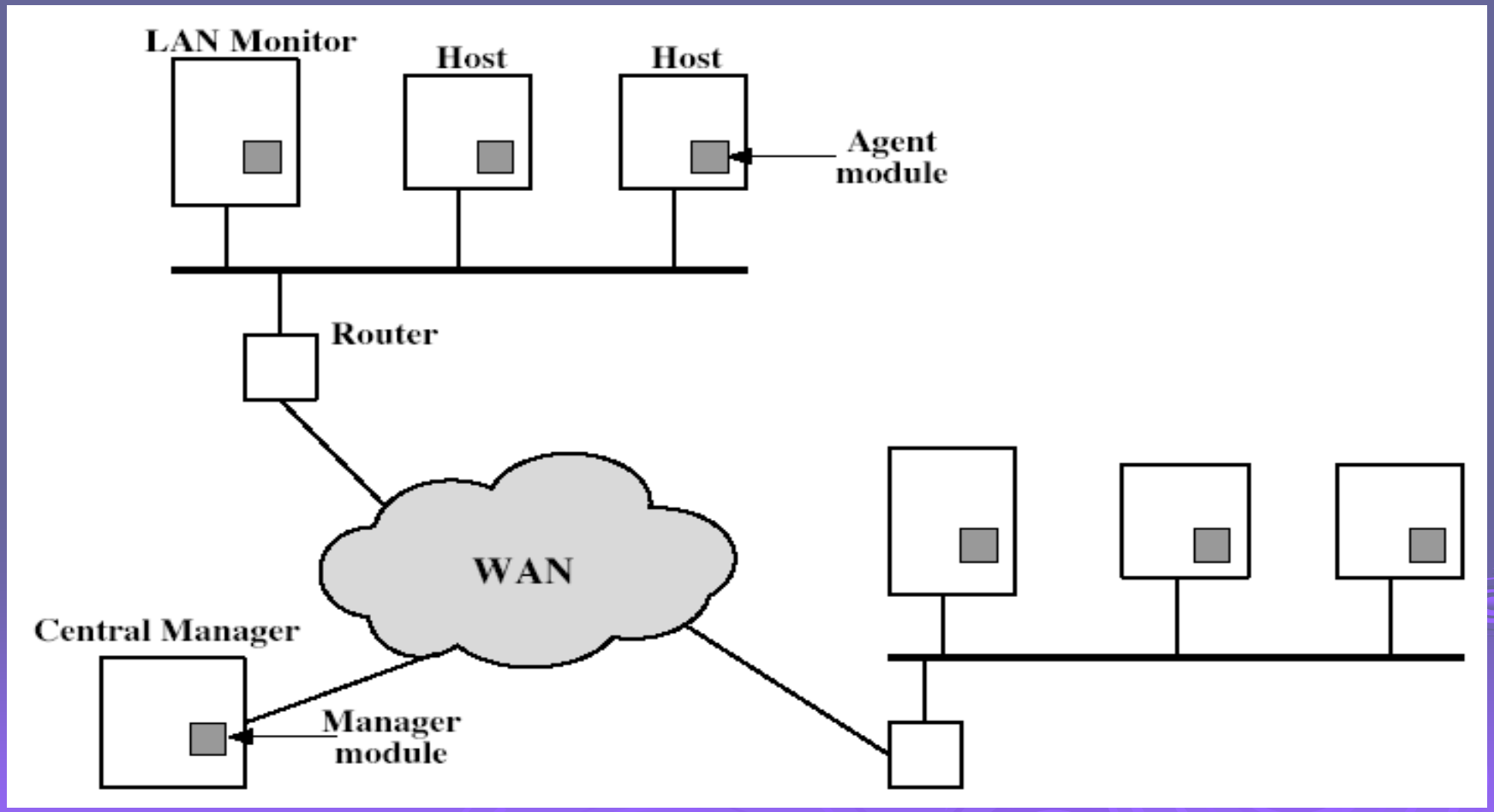
Base-Rate Fallacy

- 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

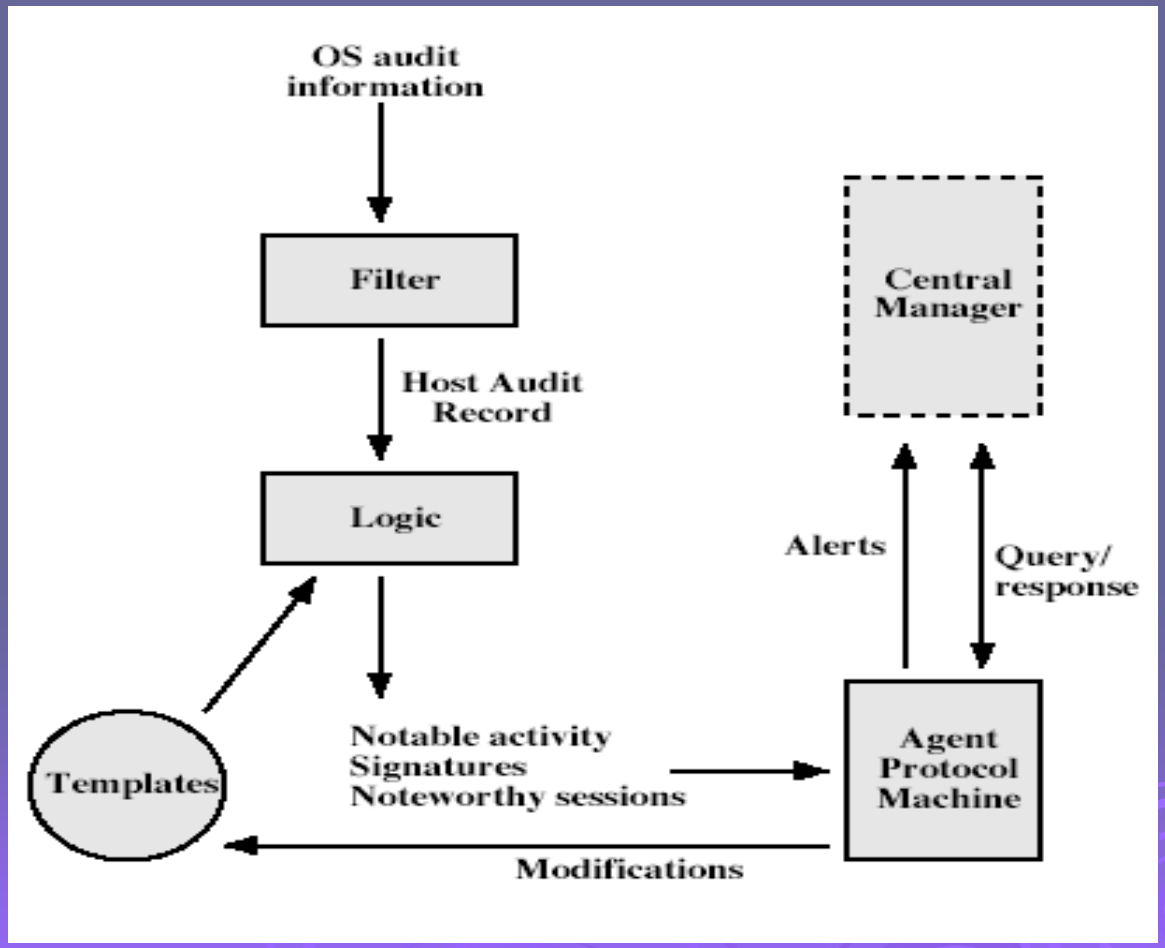
Distributed Intrusion Detection

- 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



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
- cf IETF Intrusion Detection WG standards

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
- 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 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

Summary

- have considered:
  - problem of intrusion, behavior and techniques
  - intrusion detection (statistical & rule-based)
  - password management