Cryptography and Network Security

Chapter 9

Intruders

Lectured by
Nguyễn Đức Thái

Outline

- Intruders
- Intrusion Detection
- Password Management

Key Points

- ***Unauthorized intrusion*** into a computer system or network is one of the most serious threats to computer security.
- ***Intrusion detection systems*** have been developed to provide ***early warning*** of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.
- One important element of intrusion prevention is ***password management***, with the goal of ***preventing unauthorized users*** from having access to the passwords of others.

Intruders

- A significant security problem for networked systems is ***hostile***, or at least ***unwanted***, ***trespass*** by users or software.
- User trespass can take the form of ***unauthorized logon*** to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized.
- ***Software trespass*** can take the form of a ***virus***, ***worm***, or ***Trojan horse***

Intruders

- **One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a *hacker* or *cracker*.**
- **3 classes of intruders:**
  - **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account
  - **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
  - **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

Intruders

- **Masquerader → outsider**
- **Misfeasor: → insider**
- **Clandestine user: *either* outsider *or* insider**
- Intruder attacks range (benign → serious)
  - **Benign:** simply wish to explore internets and see what is out there
  - **Serious:** access/modify data, disrupt system.

Examples of Intrusions

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

Intruders Behavior Pattern

- 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.

Hackers

- Motivated by thrill of access and status
  - the hacking community is a strong meritocracy.
  - status is determined by level of competence
- ***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***.
- IDSs and IPSs are designed to counter this type of hacker threat.
- One of the results of the growing awareness of the intruder problem has been the establishment of a number of **C**omputer **E**mergency **R**esponse **T**eams (CERTs).
  - collect / disseminate vulnerability info / responses

Hackers Behavior Examples

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

Criminals

- **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 Examples

1. Act quickly and precisely to make their activities ***harder to detect***.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
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
- 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

- The objective of the intruder is to ***gain access*** to a system or to ***increase the range of privileges accessible*** on a system.
- Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a back door into the system.
- Alternatively, the intruder ***attempts to acquire information*** that should have been protected.
- In some cases, this information is in the form of a user ***password***.
- With knowledge of some other user's password, an intruder can ***log in to a system*** and ***exercise all the privileges*** accorded to the legitimate user.

Intrusion Techniques

- Typically, a system must ***maintain a file*** that associates a password with each authorized user.
- If such a file is stored with no protection, then it is an easy matter to gain access to it and learn passwords.
- The password file can be protected in one of two ways:
  - ***One-way function***: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.
  - ***Access control***: Access to the password file is limited to one or a very few accounts.

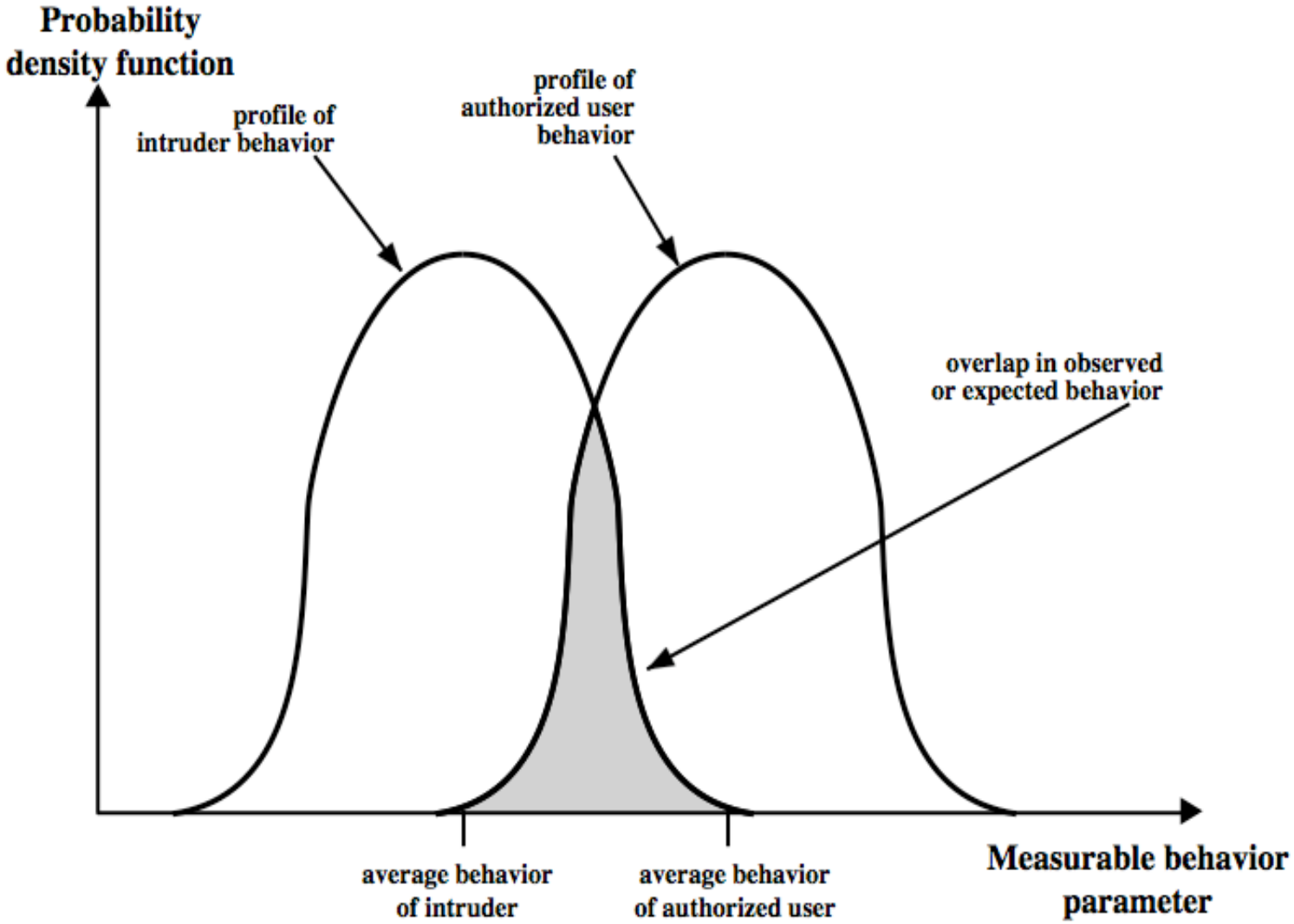
Learning Passwords

1. Try ***default passwords*** used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
2. Exhaustively ***try all short passwords*** (those of one to three characters).
3. Try words in the system's online dictionary or a list of likely passwords. Examples of the latter are readily available on hacker bulletin boards.
4. Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
5. Try users' phone numbers, Social Security numbers, and room numbers.
6. Try all legitimate license plate numbers for this state.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

Intrusion Detection

- Inevitably, the best intrusion prevention system will fail. A system's second line of defense is ***intrusion detection***, and this has been the focus of much research in recent years. This interest is motivated by a number of considerations, including the following:
  1. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
  2. An effective intrusion detection system can serve as a deterrent, so acting to ***prevent*** intrusions.
  3. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Intrusion Detection



Approaches to Intrusion Detection

- **statistical anomaly detection**
  - *Threshold detection*: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
  - *Profile based*: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.
- **rule-based detection**
  - *Anomaly detection*: Rules are developed to detect deviation from previous usage patterns
  - *Penetration identification*: An expert system approach that searches for suspicious behavior.

Audit Records

- A fundamental tool for intrusion
- Basically, two plans are used
  - ***Native audit records***: Virtually ***all multiuser operating systems*** include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.
  - ***Detection-specific audit records***: A collection facility can be implemented that generates audit records containing ***only that information required by the intrusion detection system***. One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

Statistical Anomaly Detection

- **threshold detection**
  - counting the number of occurrences of a specific event type over an interval of time
  - if exceed reasonable value assume intrusion
- **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**

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

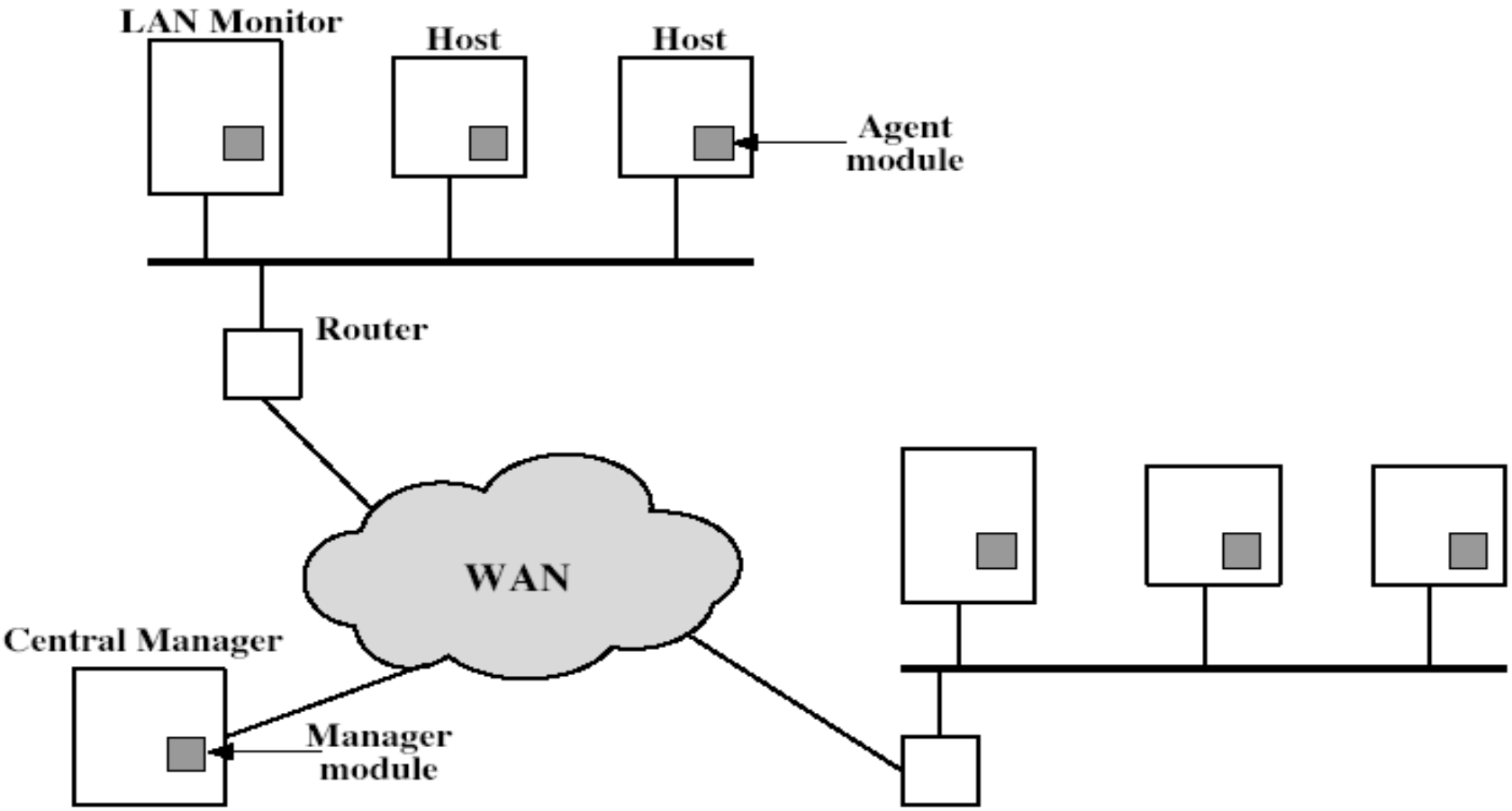
Base-Rate Fallacy

- **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

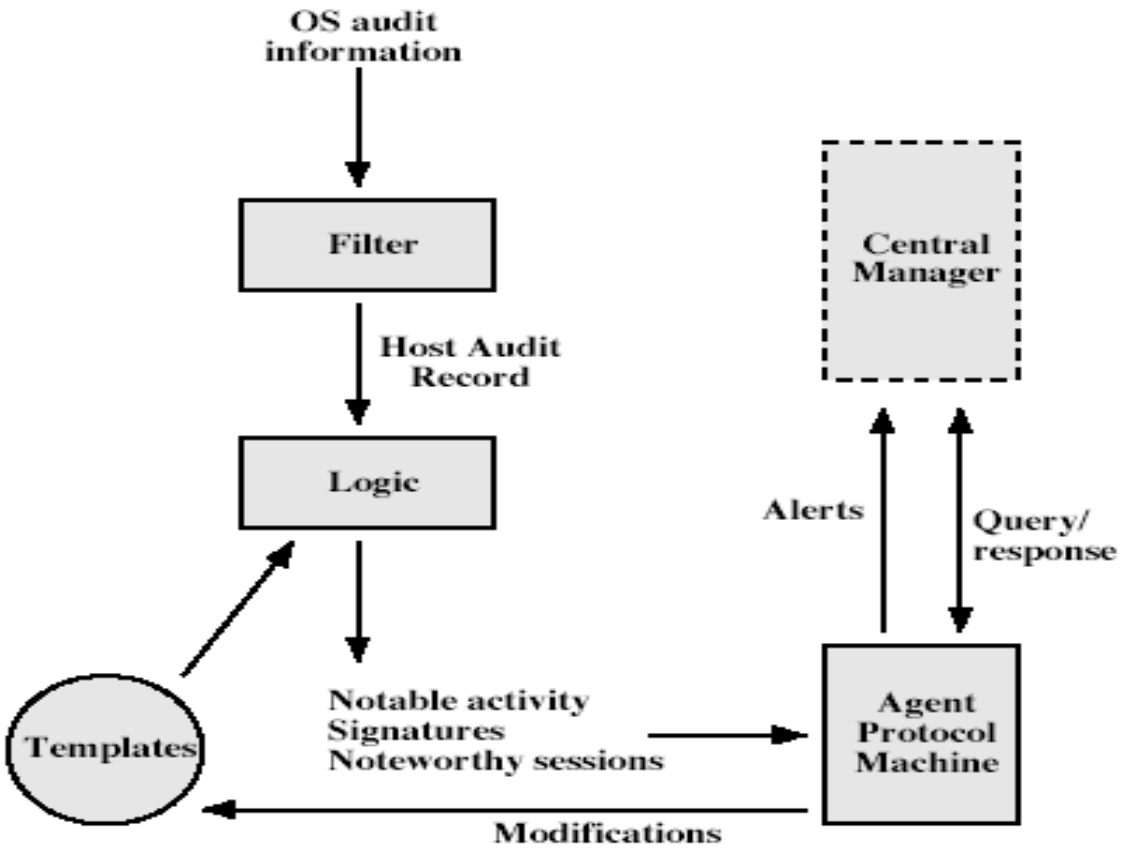
- **traditional focus is on single systems**
- **but typically have networked systems**
- **more effective defense has these working together to detect intrusions**
- **issues**
  - dealing with varying audit record formats
  - integrity & confidentiality of networked data
  - centralized or decentralized architecture

Distributed Intrusion Detection – Arch.



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 – Comp. Generated

- **let computer create passwords**
- **if random likely not memorizable, 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

- Intruders
- Intrusion Detection
- Password Management

References

- *Cryptography and Network Security*, Principles and Practice, William Stallings, Pearson, 7th Edition, 2017