Computer Security and Cryptography

CS381

来学嘉
计算机科学与工程系 电院3-423室
34205440 1356 4100825 laix@sjtu.edu.cn

2016-05

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions and MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- DDos
- Intrusion

Examples
- Bitcoin
- Hardware?
- Wireless?

contents

- Dos
- DDoS
- Password
- Intrusion
- example

Distributed Denial of Service Attacks (DDoS)

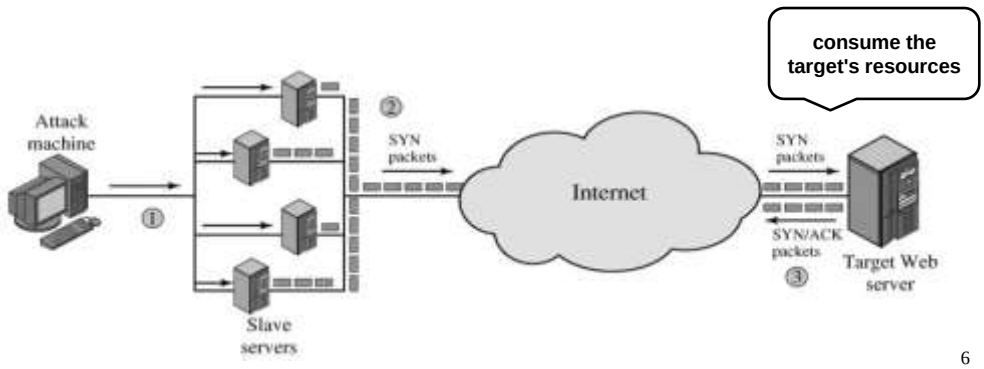
- Denial of Service (DoS) itself may be not an attack (too many users, low capacity .12306– no enemy)
- Distributed Denial of Service (DDoS) attacks: an attempt launched by enemy to make a resource unavailable to its intended users
  - DDoS is now a significant security threat
  - making networked systems unavailable by flooding with useless traffic
  - using large numbers of “zombies, 肉鸡”
  - growing sophistication of attacks
  - defense technologies struggling to cope

DDoS Direct Attacks

- sending a large number of attack packets directly towards a victim.
- Source addresses are usually spoofed so the response goes elsewhere.
- Example:
  - Ping of Death (POD), Feed the target more than he can handle

SYN flood

- SYN flood: legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections (spoofed source address so the response goes elsewhere).



6

Peer-to-peer attacks

- attacker acts as a “puppet master,” instructing clients of large P2P file sharing hubs to disconnect from their P2P network and to connect to the victim's website instead
- most web servers fail almost instantly under 5000 connections per second； a moderately large peer-to-peer attack, a site could be hit with up to 750,000 connections in short order
- can be prevented by specifying in the P2P protocol which ports are allowed or not. If port 80 is not allowed

7

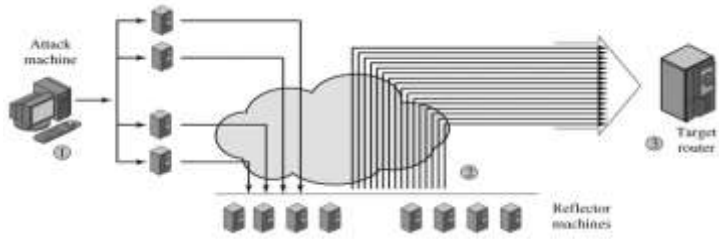
HTTP POST attack

- attack sends a legitimate HTTP POST header, which includes a 'Content-Length' field, “1000 bytes”
- then send the actual message body at an extremely slow rate (e.g. 1 byte/110 seconds).
- the target server will attempt to obey the 'Content-Length' field in the header, and wait

8

DDoS Reflector Attacks

- Uses innocent intermediary nodes (routers and servers) known as reflectors.
- An attacker sends packets that require responses to the reflectors with the packets' inscribed source address set to victim's address.
- Can be done using TCP, UDP, ICMP as well as RST packets.



9

DDoS Countermeasures

- prevention & preemption (before)
  - protect hosts from master and agent
  - Monitor network traffic
  - This method alone is inadequate
- detection & filtering (during)
  - Identifying DDoS attack packets, and dropping them.
  - Source Networks: can filter packets based on address spoofing
  - Victim's Network: detect attack based on volume of incoming traffic or degraded performance
- source traceback & identification (after)
  - IP Traceback: Identifying actual source of packet without relying on source information.
  - Routers can record information they have seen.
  - Routers can send additional information about seen packets to their destinations

contents

- DDoS
- Intrusion
- Password
- Intrusion Detection

Intruder

- aim to gain access and/or increase privileges on a system
- basic attack methodology
  - target acquisition and information gathering
  - initial access
  - privilege escalation
  - covering tracks
- key goal often is to acquire passwords

Intruder: classification

- Masquerader-冒充者
  - outside user who tries to access the information as an authorized user
- Misfeasor-滥用职权者
  - legit user who accesses unauthorized data
- Clandestine user-地下用户/潜伏
  - seizes supervisory control

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

常用口令

- 中国网民最常用**10**大密码
- abc123 123456 xiaoming 12345678 iloveyou
- admin qq123456 taobao root wang1234

- 国外网民常用的**25** 个**:**
- *password*、123456、12345678、qwerty、abc123、 monkey、1234567、letmein、trustno1、dragon、baseball、111111、iloveyou、master、 Sunshine、Ashley、Bailey、passw0rd、 Shadow、123123、654321 Superman、Qazwsx、Michael、football

15

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)
- **Phishing**
  - a fake website that is almost identical to the legitimate one

Password protection

- 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 protections - Education

- 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
  - PAO: Person+Action+Object (Alice-catch-bus)
  - Change password periodically
- but likely to be ignored by many users

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

contents

- DDoS
- Intrusion
- Intrusion Detection

Intrusion Detection

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

Approaches to Intrusion Detection

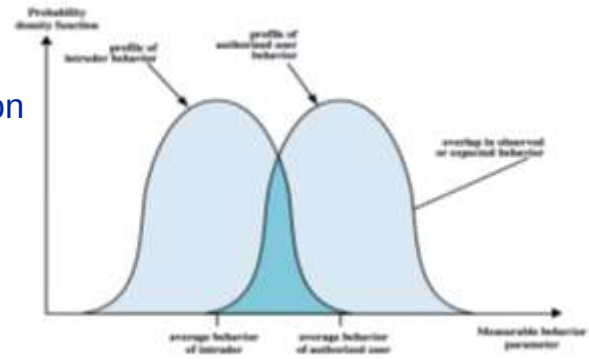
- statistical anomaly detection
  - threshold
  - profile based
- rule-based detection
  - anomaly
  - penetration identification

Intrusion Detection

Assumption

- System activities are observable
- Normal and intrusive activities have distinct evidence

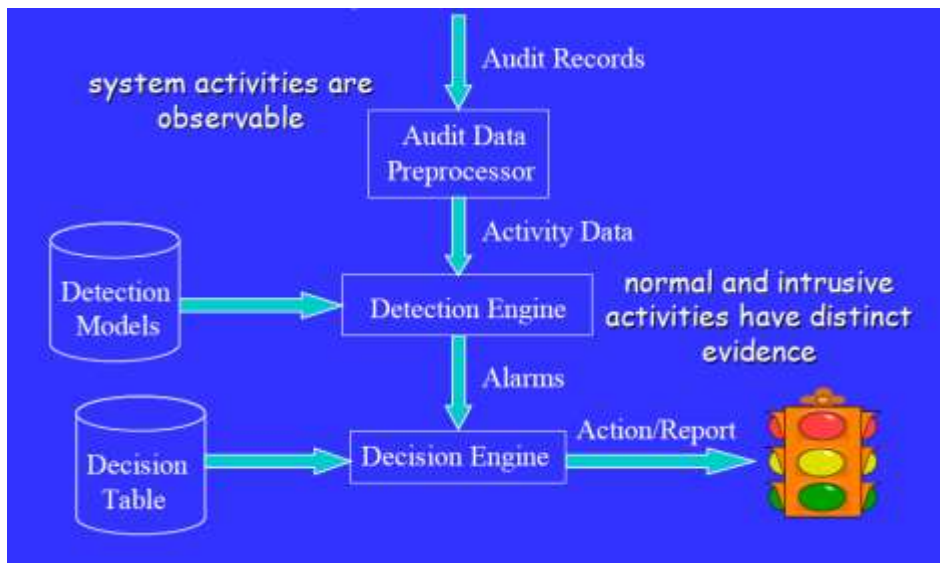
1. Statistical anomaly detection
2. Rule-based detection



Problems

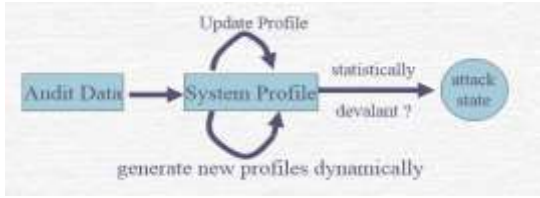
- **false positives**
- **false negatives**
- **must compromise**

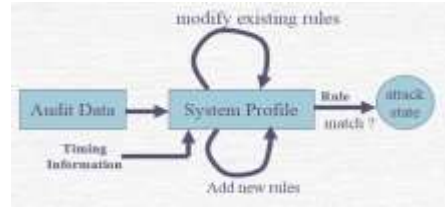
Components of Intrusion Detection System



Intrusion Detection Approaches

- Statistical anomaly detection
  - Attempt to define normal or expected behavior
  - effective against masqueraders
  - Not effective against misfeasors
- Rule-based detection
  - define a set of rules: decide whether a given behavior is of an intruder
  - attempt to define *proper* behavior
  - appropriate for misfeasors





Audit Records

- 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
  - no prior knowledge used

Statistical anomaly detection

- The detector learns what is "normal" behavior and then looks for deviations
- Metrics
  - Counter, gauge, interval timer, resource utilization
- Approaches
  - Mean and standard deviation, Multivariate, Markov process, Time series, Operational
- threshold
  - 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

Statistical anomaly detection

- Advantage
  - They adaptively learn the behavior of users.
  - A prior knowledge of security flaws is not required
  - Potentially more sensitive than humans.
- Problems with Statistical approaches
  - They can gradually be trained by intruders so that eventually, intrusive events are considered normal.
  - It is not known exactly what the subset of all possible measures that accurately predicts intrusive activities is.

Rule-based detection:

Rule-based anomaly detection

•Detect patterns that do not conform to an established normal behavior.

•Rules --past behavior patterns of users, programs, privileges, time slots, terminals, etc.

•Based on observing past behavior

•Assume that the future will be like the past

•Require a rather large database of rules

Rule-based penetration identification

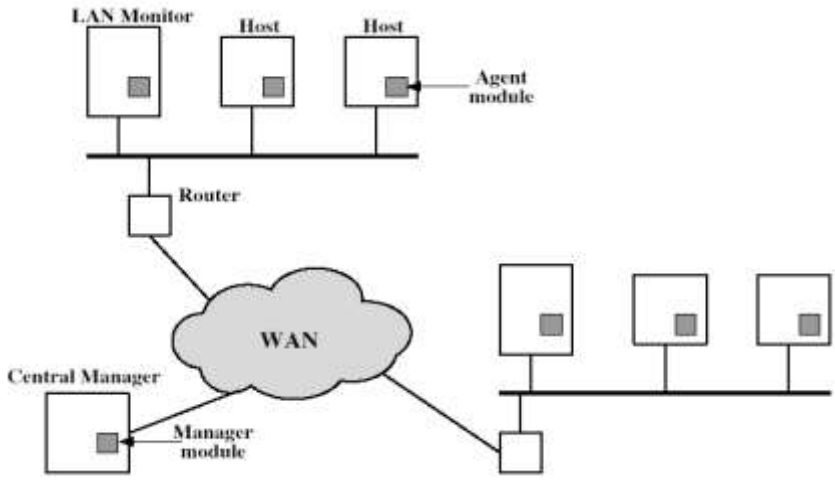
•Rules are generated by "**experts**" rather than by means of an automated analysis of audit records

•Strength depends on the **skill** of those who set up the rules.

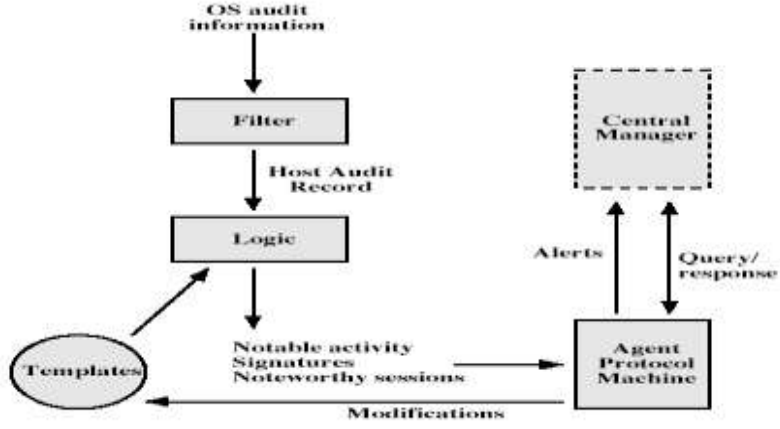
Distributed Intrusion Detection

- 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



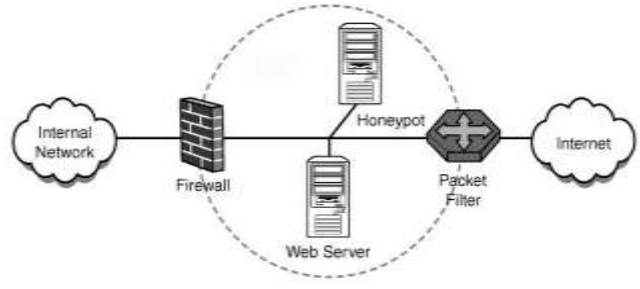
Distributed Intrusion Detection – Agent Implementation



Honeypots (蜜罐)

- Honeypot is a trap set to detect, deflect, counteract unauthorized attempts.
- Decoy (诱饵) 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

Honeypot



- filled with fabricated information
- collecting detailed information on attackers activities
- single or multiple networked systems
  - cf IETF Intrusion Detection WG standards

36

How to build a honeypot ?

- how do we attract intruders ?
  - choose enticing names (e.g., mail.sjsu.edu)
- how do we know we're probed ?
  - put honeypot on isolated net behind a firewall
  - set firewall to log all traffic
- how do we protect our peers ?
  - set firewall to allow all in-coming traffic, but limit out-going traffic
  - ICMP, FTP, DNS are common protocols intruders need

APT1

- **APT-Advanced Persistent Threat**： usually refers to a group, with both the capability and the intent to persistently and effectively target a specific entity.
  - *Advanced* -combine multiple targeting methods, e.g., telephone-interception, satellite imaging, travel records, hobby, shopping, GPS, GSM,…
  - *Persistent-* the attackers are guided by external entities，through continuous monitoring and interaction in order to achieve the defined objectives. "low-and-slow"
  - *Threat* –have a specific objective by coordinated human actions，and are skilled, motivated, organized and well funded.
- 典型例： Stuxnet, Duqu, and Flame

61398

- 2014年5月19日, 美国司法部宣布起诉5名中国军官,美方声称这5名军官来自所谓的解放军61398部队. 美国联邦调查局(FBI)网站公布了被美国司法部起诉的五名中国军方人员的名单和照片
- On 18 February 2013, Mandiant released a report[6] documenting evidence of cyber attacks by the PLA (specifically Pudong District, Shanghai-based PLA Unit 61398-总参三部二局) targeting at least 141 organizations in the US and other countries extending as far back as 2006. In the report, Mandiant refers to the espionage unit as APT1
- APT1 get technology blueprints, proprietary manufacturing, processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.
- Kevin Mandia, CEO, founded Mandiant as Red Cliff Consulting in 2004 prior to rebranding in 2006, was acquired by FireEye on December 30, 2013 for 1b.

39

Who??

- Attacking IP: many from 浦东高桥大同路
  - 业余？肉鸡？
  - 怕麻烦，疏忽；
  - 是任务，无顾虑

- 被人肉的ID：
- “UglyGorilla”
  - 注册中国军网；
  - rootkit.com; (UglyGorilla@163.com, IP浦东高桥)
  - 开发人网 （美国发现 UglyGorilla--汪东）

41

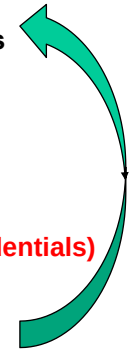
- “DOTA”
  - 注册多个邮箱：dota001@gmail.com, doata015,,,
  - 口令未管好，被Mandiant攻入。手机验证码-〉手机号
  - password “2j3c1k” – 2局3处1科

- “SuperHard,”
  - the accounts disclosed from rootkit.com- mei_qiang_82@sohu.com”
  - SH offering to write Trojans for money

42

APT1 cycle

1. **Initial Compromise**
   - **Fake business email of CEO with a Zip attachment containing a.exe pretended as pdf, opens backdoor**
2. **Establishing a Foothold**
   - **initiate outbound connections to the intruder's "comments" server; web-page**
3. **Standard Backdoors**
4. **Covert Communications**
5. **privilege escalation (search passwords/hash**
6. **Internal Reconnaissance –(set of legitimate credentials)**
7. **Lateral Movement -- Remote Desktop and FTP**
8. **Maintain Presence**
   - **Install new backdoors on multiple systems**
9. **Completing the Mission**



43

Standard Backdoors

Create/modify/delete/execute programs
Upload/download files
Create/delete directories
List/start/stop processes
Modify the system registry
Take screenshots of the user's desktop
Capture keystrokes
Capture mouse movement
Start an interactive command shell
Create a Remote desktop (i.e. graphical) interface
Harvest passwords
Enumerate users
Enumerate other systems on the network
Sleep (i.e. go inactive) for a specified amount of time
Log off the current user
Shut down the system

44

Exercise 18

1. what is the most important thing against intrusion?
2. Describe the 2 approaches of intrusion detection
3. Describe effective rules to detect/prevent the Standard Backdoors

- Deadline: before next lecture

45