

2 网络安全攻击与安全威胁

2.1 各类网络攻击：5种 ✓

2.1.1 恶意软件、病毒、蠕虫及如何防范病毒攻击 ✓✓

2.1.2 勒索软件攻击 ✓

2.1.3 中间人攻击 ✓

2.1.4 拒绝服务攻击 ✓

2.1.5 拒绝服务与分布式拒绝服务 (DDOS) 攻击的基本概念

2.1.6 SYN洪水攻击原理及实施方式

2.1.7 计算：发起DOS攻击需要多少数据

2.1.8 数据包大小会产生什么影响？

2.1.9 链路速度如何影响DOS攻击效果？

2.1.10 DNS洪水攻击

2.2 密码认证优缺点:2+3

2.3 密码计算

2.4 生物原理，优缺点 3+2，取代密码

2.1 website attack method

① malware : ① It execute unauthorized actions on victim's system

② user click suspicious link and download attachments or use infected drive

③ malicious software

Viruses,

worms

logical boom

Botnet

trojan

Ransomware : ① block access to the network

② pay (Bitcoin)

③ you may not grant access after pay.

spyware

Adware

Rootkit

Measure

① antivirus software

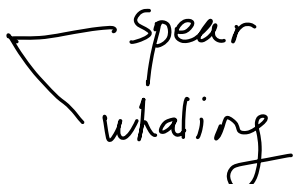
② firewall

③ built in firewall

④ don't click

⑤ update OS & browsers

② Social Engineering Attack

- ① art of manipulating people so that giving confidential information
- ② trust
- ③ click
- ④ install malware
- ⑤ get confidential information & account credentials
- ⑥ phishing attack 
 - spear
 - whaling

③ Password attack

④ man in the middle attack

- ① attack come in between two party communication
- ② cut off
- ③ website security
- ④ encryption
- ⑤ Refrain use public wifi

④ SQL injecting

⑤ DOS: Deny of service.

2.1.5 packet \rightarrow overwheming \rightarrow service

DOS: one source

DDOS: multiple..

2.1.6 TCP \rightarrow SYN \rightarrow SYN/ACK \rightarrow wait ACK
 \rightarrow SYN \rightarrow port \rightarrow DOS.

2.1.7 $DOS = \frac{V}{Size.}$ packets

2.1.8 \bar{V} s \uparrow n \downarrow

2.1.9 \bar{S} V \uparrow n \uparrow

2.1.10 DNS: Domain Name system

example \rightarrow 192...-

unavailable for most people

2.2 Ad: 1. free + easy implement

2. compromised \rightarrow change + security

Dis Ad: 1. ^{can} crack

2. simple \rightarrow weak \rightarrow less security,

3. complex \rightarrow remember & management

2.3 calculate $\frac{C^L}{V}$

2.4 biometric:

✓ — Difficult to hack

✓ — Convenient

✓ — always available

x — Not 100%: False rejection

False acceptance

Complacency 自滿

High risk cloning: card, key