Network Security

Hitesh Dharmdasani
Founder, Informant Networks

What is next to impossible to do?

- Hack into Gmail, Facebook, Yahoo Mail, etc…
- Read your WhatsApp (Especially now)
- Break into any server
- Change Websites at will

What can be done

- Make Products that defend networks
- Understand how a Malware works
- Tell you how things work in Security
- Make Security fun!

Agenda

- What is Network Security
- What do we need to defend?
- What are the most common attacks
- Security vs. Obscurity
- Security as a Trade Off
- Current Preventive Measures

What is a Network

- Set of interconnected ~~devices~~ services
- What Services
  - Internet
  - File Sharing
  - E-Learning
  - IP Cameras
  - Etc.

Protect those services

Protection Mechanisms

- Access Control
    - Login
    - Firewall Rules
    - DMZ
- Patch against Vulnerabilities

What is Access Control

- Login
  - Username and Password(Secret). Gives Authentication
- Firewall Rules
  - Prohibit Wrong Access, Misuse, Over use
- DMZ (De-Militarized Zone)
  - Separation of concerns

Vulnerabilities

- Problems in software
- Allow crafted input to crash programs in ways that leads to arbitrary code execution
- Major problem in Security
- Most targeted software: MS Windows, Internet Explorer, Java Runtime

Arbitrary code Execution

- Run something without will or consent
- Run programs irrespective of user choice
- Do operations on a computer without authorization
- Run X when what was desired was “Calculator”
- Etc…
- **Root of all evil on the Internet!**

Attacks on a Network

- Denial of Service(DoS), DDoS
- Worms, Trojans, Malware, Viruses
- Vulnerabilities in Services

Denial of Service

- Over whelm something
- Submit more requests than the capacity
- Do not allow legitimate users to access resource

Worms, Trojan, Malware, Viruses

- Malicious Code in General

- Compromise Computers to do work on behalf of Criminal. Eg: Send Spam, Key logging, Use your computer to do more bad things

- Worms are self propagating, Can cause large harm very soon

- MyDoom: Slowed the Internet down, Estimated Cost for recovery: $38 Billion

Vulnerabilities in Services

- If there is SQL Statement of the form

```
select * from users where username="%s"
and password="%s"
```

- If user gives password as

```
" or 1=1 ;
```

- The resultant query turns into

```
select * from users where username="%s"
and password="" or 1=1 ;"
```

- This gives you the entire list of username and passwords

Example of Bad Security

Security vs Obscurity

- The Process should not be secretive
- There should be a known secret key in use
- In Encryption, Don't keep the algorithm secret, Keep the key as a secret
- Obscurity can be reverse engineered

Trade Offs

- Security comes at a cost
  - Encrypting all data costs in disk space and time
- Network Security Products introduce latency
- User Experience can get hampered
- What are you trying to protect?
  - Music Collection has less importance than Nuclear Launch codes

Current Defenses

- Run a Firewall that works well
- Run an Updated Version of Windows and an Updated Anti Virus
- Use HTTPS over HTTP wherever available
- Don't Invent your own Cryptography
- If its too good to be true. it probably not true

Questions

What do you want to know?