Paranoia Hour

Nocturnes RMLL 2005

khorben <khorben@uberwall.org>
oz <oz@tuxaco.net>

A Word About Security

- it doesn't exist
- in fact it's more of a compromise: invest accordingly to the threat you want to be safe from
- paranoia helps...

1. Local networks

basically two types:

- “hubbed”
- switched

safer than the Internet? I doubt it...

1.1 Hubbed Networks

- Wireless networks can be seen as hubbed
- Basically, just open your ears:
  ```
  # tcpdump
  ```
- Consequently avoid any authentication in the clear: HTTP, POP, SMTP, ICQ, MSN/HTTP, ...

1.2 Wireless Specific

Hotspots offer no protection

WEP is easily defeated if there is traffic:

```
# airsnort
# aircrack
```

...but anyone can create some too:

```
# aireplay
```

WPA?

1.3 Switched Networks

- Thought you could just plug yourself in and be safe?
- ARP spoofing (switches' protections)
- DHCP spoofing
- DNS spoofing
- Man-in-the-middle
  Even SSH and SSL can be defeated!

2. A Wild Internet

Internet is constantly being hacked...

port scans

applications flaws (servers, web sites, ...)

worms

SPAM (the human factor)

2.1 Passive Protection

- Firewall the traffic is not enough:
- breaks some applications: FTP, H323, IRC, ...
- client applications flaws (web browsers, mail readers, ...)
- web sites flaws...

2.2 Web Sites

- HTML injection
- Cross-site scripting
- SQL injection

2.3 The Human Factor

- Malware
- SPAM
- Phishing

3. UW_sslmitm

Usage: UWsslmitm [-d][-c certificate][-l port][-p port][-f file] target

-d disable SSL decryption/encryption

-c certificate to use (default: "mitm.crt")

-l port to listen to (default: 443)

-p port to forward to (default: 443)

-f file to output sneaked data to (default: none)

3.1 Demonstration

Let the show begin...

Conclusion

Possible solutions:

SSL is not actually broken, it requires:
- further checking by the user
- proper use of certificates
- better clients

IPsec

It's up to you...