



I Use Encryption So I'm Secure? – Advanced Traffic Interception Attacks

Making Sense of Risk

Luke Jennings

20th May 2010



Outline

- Introduction
- Interception Methods
- The Impact – What Can Be Done?
- Defeating Protection Mechanisms
- Defence
- Q&A



Introduction

- Basic Attacks = Easy
- High Impact
- Often Overlooked

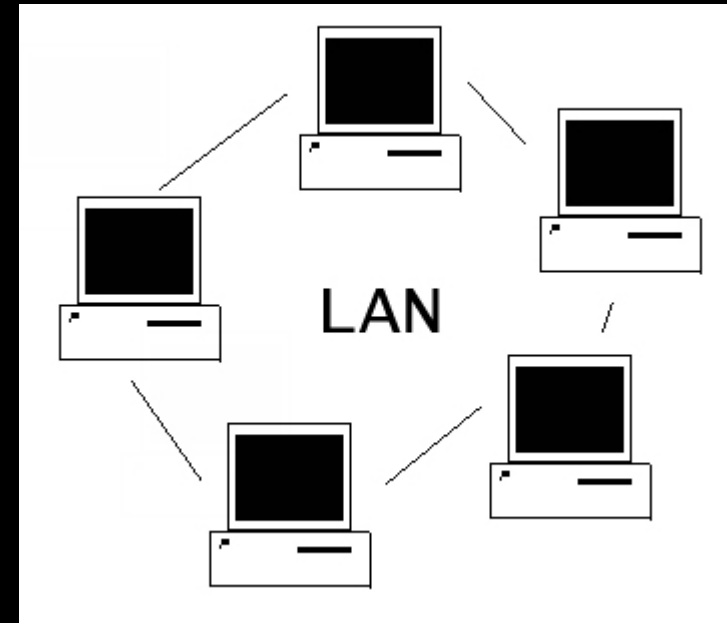


Outline

- Introduction
- **Interception Methods**
- The Impact – What Can Be Done?
- Defeating Protection Mechanisms
- Defence
- Q&A

Methods - Local

- ARP Spoofing
- Port Stealing
- ICMP Redirects
- DHCP Hijacking
- ...and many more





Methods – Wide/Global

- DNS Spoofing
- Routing Protocol Attacks
- Proxy Auto-Configuration
- Broadband – Cable Modems, ADSL etc



Methods – Wireless

- Passive Sniffing
- WEP/WPA Cracking
- Hotspot / Evil Twin Attacks





Outline

- Introduction
- Interception Methods
- The Impact – What Can Be Done?
- Defeating Protection Mechanisms
- Defence
- Q&A

Impact - Eavesdropping

- Capture Passwords
- Intercept Email
- Spy on Web Browsing
- Listen to VoIP Conversations





Impact – Disinformation

- False News Stories
- False Share Prices
- Social Engineering
- ...why encrypt public data?

How To Deceive



Disinformation Tactics

DEMO 1 – Playing the Stock Market

Impact – Trojans

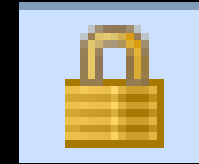
- Infect Installers
- Substitute PDFs with Exploits
- Hijack Auto-Update Procedures
- ...appear to be from trusted sources





Outline

- Introduction
- Interception Methods
- The Impact – What Can Be Done?
- Defeating Protection Mechanisms
- Defence
- Q&A



Defeating HTTPS

- Secure links often come over HTTP
- Replace all HTTPS links with HTTP
- Proxy HTTP traffic so server sees SSL
- Tool – SSLStrip does this (80+ vs 0)

DEMO 2 – Webmail Attacks

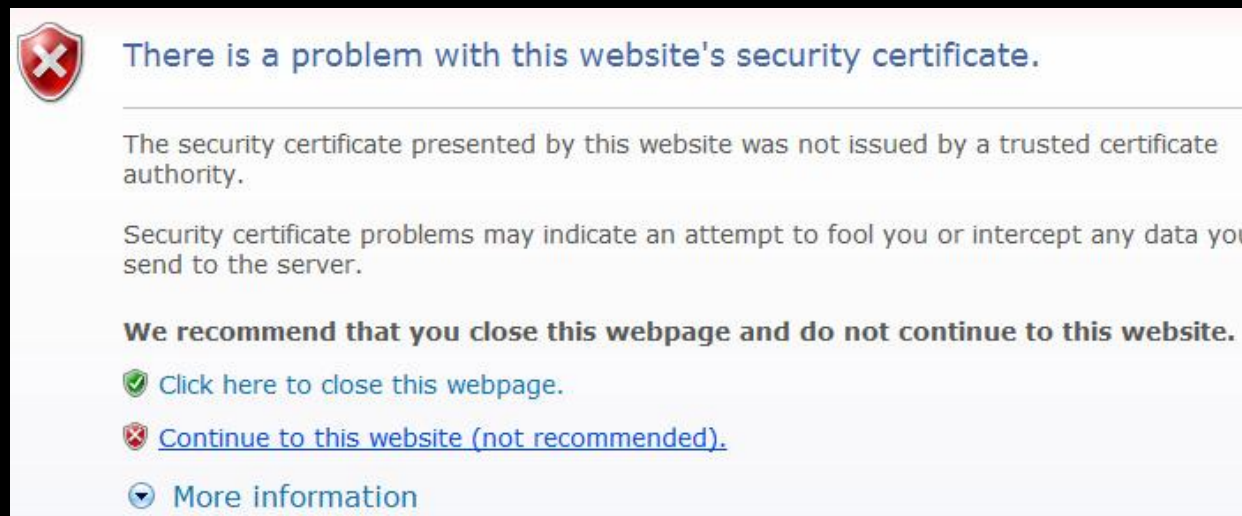


Defeating SSL

- SSLv2 Downgrade, Weak Ciphers
- Subvert a CA
- Social Engineering
- “There is no evidence of a single user being saved from harm by a certificate error, anywhere, ever.” – Microsoft Research



Defeating SSL





Common Misconception: Two Factor Authentication

- Most Common = One-Time Password
- Does not provide much protection
- Clever attackers can often still maintain persistence after compromise



Common Misconception: Cookie SECURE Flag

- “We do not need to set the SECURE flag”
- “Only port 443 (SSL) is open, so all traffic is always encrypted!”
- Wrong!



Common Misconception: Cookie SECURE Flag

- Clever NAT tricks can be used to compromise cookie
- Victim does not need even need to be actively using site

DEMO 3 – Beating SSL-only Websites



Outline

- Introduction
- Interception Methods
- The Impact – What Can Be Done?
- Defeating Protection Mechanisms
- **Defence**
- Q&A



Defence - Education

- Educate your users about the dangers of these attacks
- Educate your system administrators about secure configuration
- Educate your architects and developers about the importance of these issues

Defence - Encryption

- Use it and use it properly!
- Remember data integrity (not just confidentiality)
- Avoid allowing users to override encryption security warnings where possible





Defence – Limit Interception Opportunities

- Segregate your network
- Prevent Laptops/Phones connecting to unknown WiFi access points
- Secure your network routing protocols



Conclusion

- Traffic Interception Attacks are easy and dangerous
- Many disregard the risk they pose based on false assumptions
- Do not fall into this trap. Protect yourselves!



Questions?

