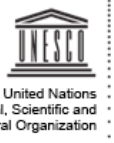
Wireless Security

Training materials for wireless trainers

The Abdus Salam
International Centre
for Theoretical Physics

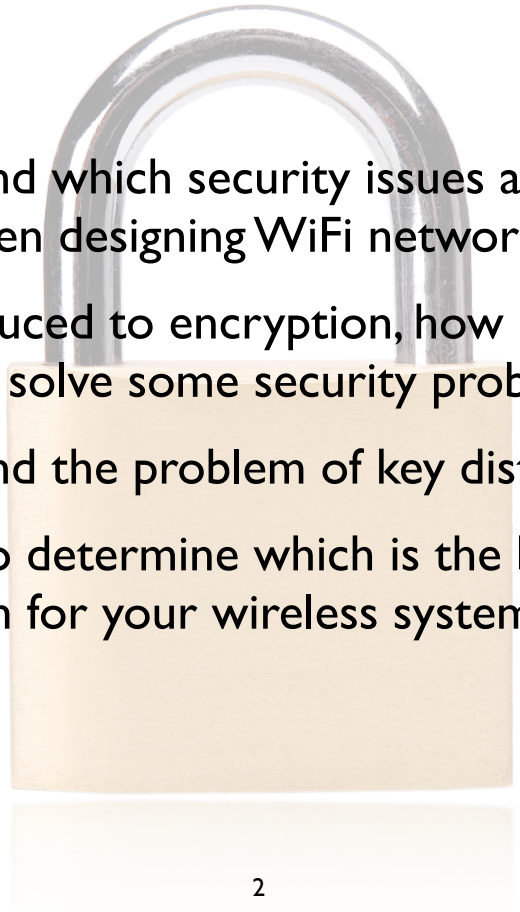


United Nations
Educational, Scientific and
Cultural Organization

This one hour talk covers the essential problems of wireless security, and some techniques to address them.

Version 1.2 by Rob, @2009-11-23
Version 1.3 by Rob, @2010-02-28
Version 1.4 by Rob, @2010-03-12
Version 1.5 by Carlo, @2011-03-24

Goals

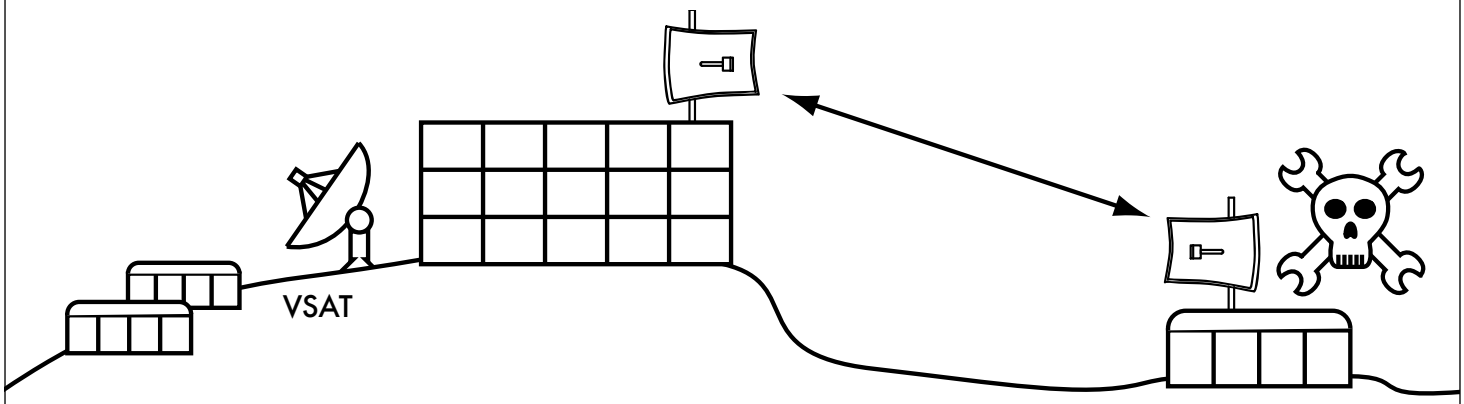


- To understand which security issues are important to consider when designing WiFi networks
- To be introduced to encryption, how does it works, and why can solve some security problems
- To understand the problem of key distribution
- To be able to determine which is the best security configuration for your wireless system

Why is wireless security a problem?

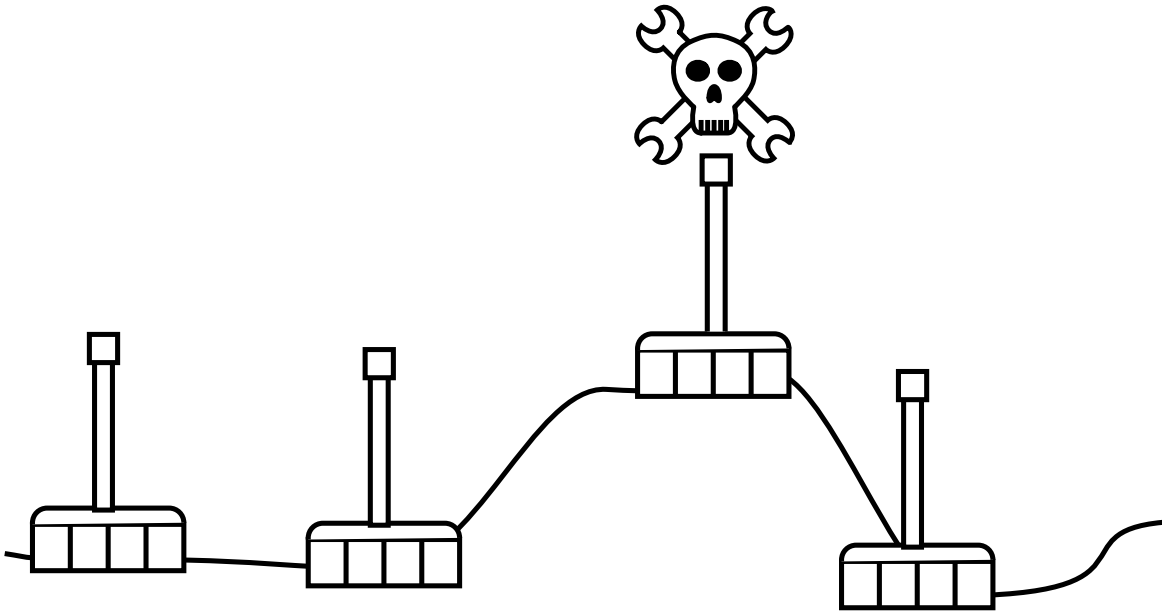
- Wireless is a ***shared medium***
- Attackers are relatively ***anonymous***
- End users are ***poorly educated***
- ***Denial-of-service*** is very simple
- ***Automated malicious attacks*** are increasingly complex
- ***Sophisticated tools*** are freely available

Attacks may come from far away



In this picture, the wireless network "under attack" is approximately 12 km away.

Attacks may be completely undetectable.



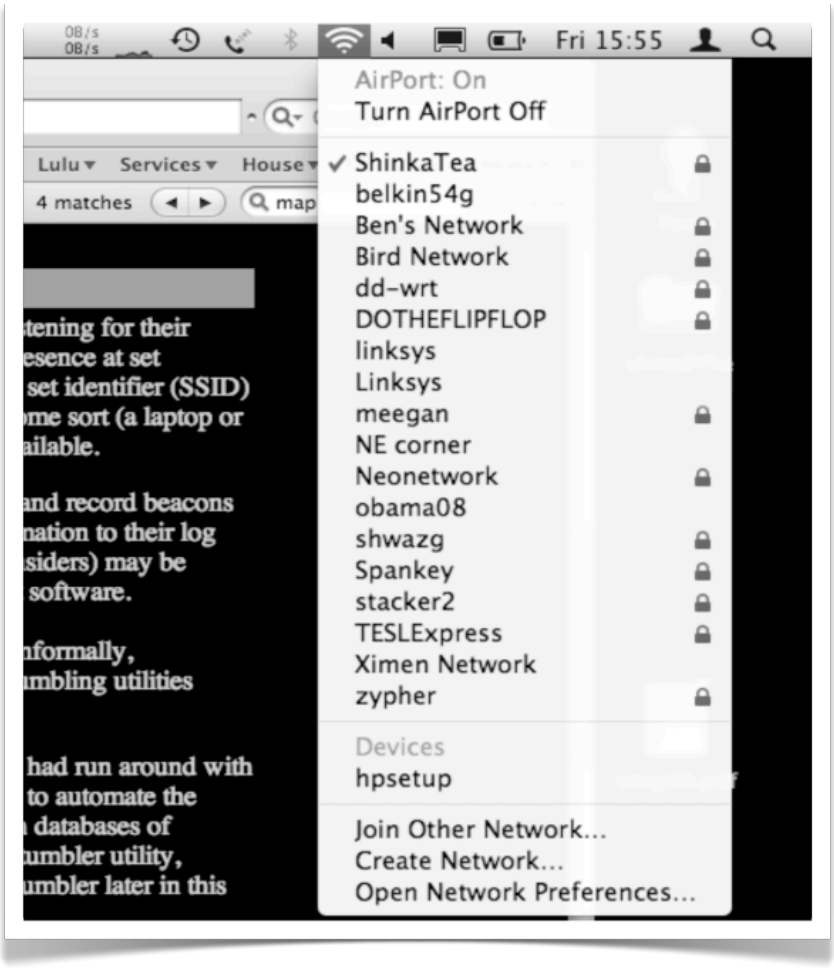
Radios may be configured to passively monitor all network traffic. Since the attacker never transmits a single packet, such eavesdropping is impossible to detect.

Who creates security problems?

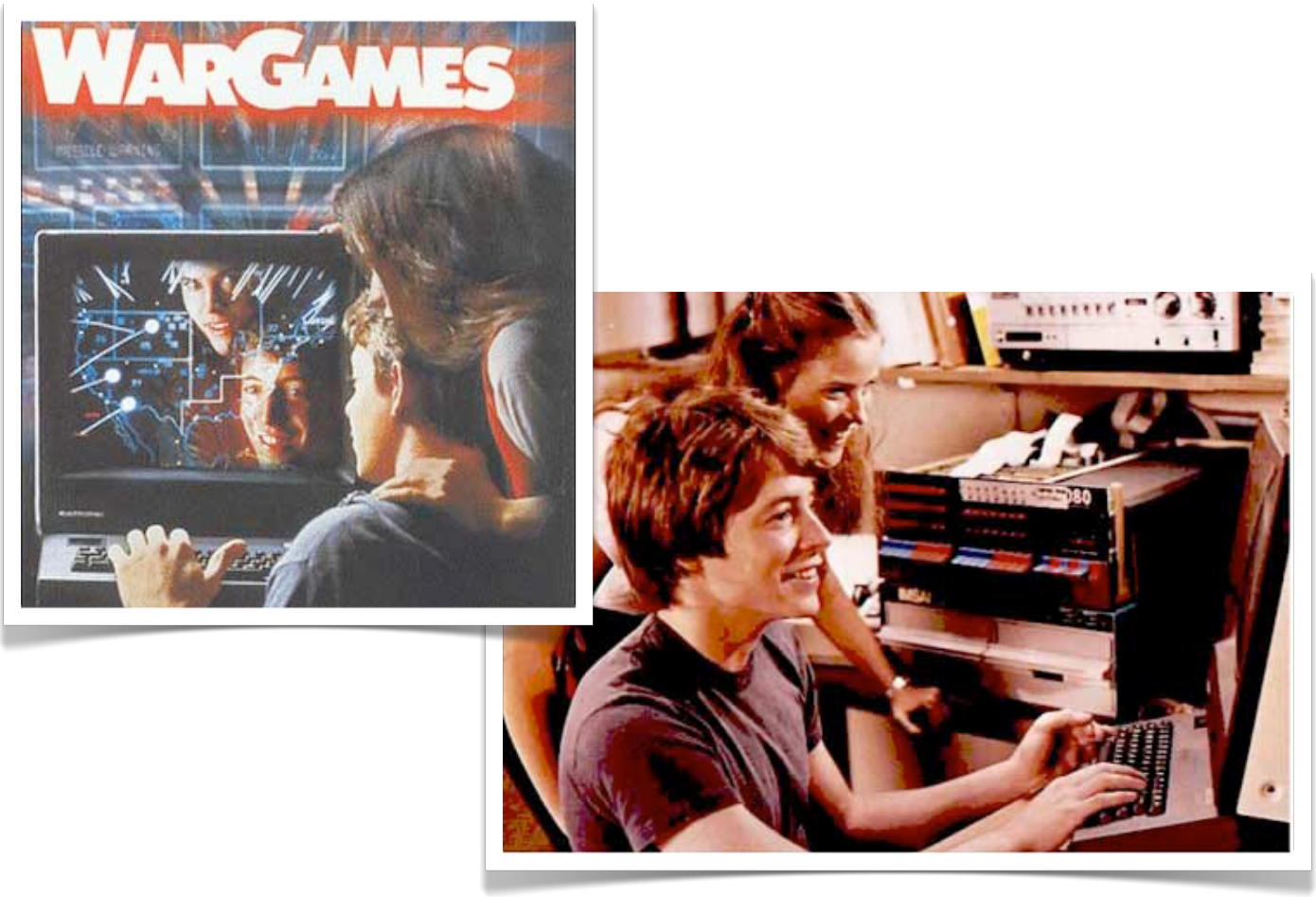
- ***Unintentional users***
- ***"War Drivers"***
- ***Eavesdroppers*** (personal and corporate spies)
- ***Virus-infected computers***
- ***Rogue access points***
- ***Malicious users***

Unintentional users can accidentally choose the wrong network without even realizing it.

They may unintentionally reveal information about themselves (passwords, email, web page visits, etc.) without realizing that anything is wrong.



This wireless client can see 18 networks, six of which use no encryption. Without encryption is very easy for users to accidentally use the wrong network, which presents the possibility of data leakage.



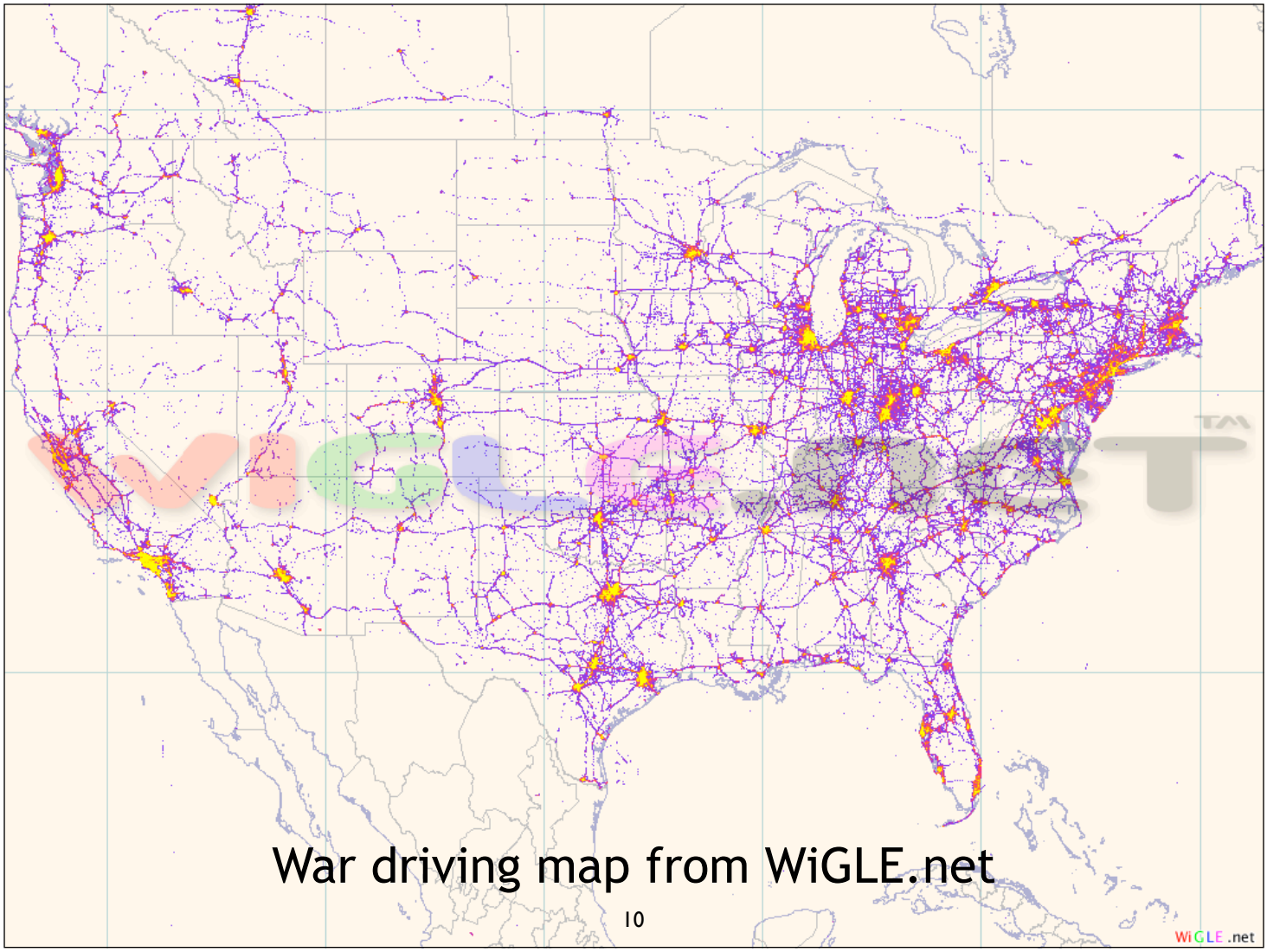
War Games (1983) starred Matthew Broderick, John Wood, and Ally Sheedy

War Games is a classic movie that helped define the idea of a "hacker" for the general public in 1983.

Matthew Broderick played a whiz-kid who uses his computer to dial thousands of phone numbers at random, making a note of phones that answered with a computer modem tone.

This process of finding computers by telephone number became known as "war dialing".

In 2001, Pete Shipley from San Francisco automated the process of driving around in a car with a Wi-Fi laptop, logging access points and correlating the data with his GPS location. He coined the term "war driving" as a reference to the classic hacker film.



War driving map from WiGLE.net

WiGLE.net has logged the location of over 16 million wifi hotspots around the world. The data was collected entirely through the effort of wireless enthusiasts.

Rogue Access points

Access points may simply be installed incorrectly by legitimate users. Someone may want better wireless coverage in their office, or they might find security restrictions on the corporate wireless network too difficult to comply with.

By installing an inexpensive consumer access point without permission, users can open the entire network up to potential attacks from the inside.

In addition, eavesdroppers who intend to collect data or do harm to the network may intentionally install an access point on your network, providing an effective "backdoor".

Eavesdroppers

By using a passive monitoring tool (such as ***Kismet***), an eavesdropper can log all network data from a great distance away, without ever making their presence known.

The monitoring utility Etherpeg is a packet monitor that shows a collage of graphics that are sent unencrypted across the network. It is a sort of "reverse web browser" that shows you what is happening on everyone else's screen.

Malicious Users

THE TIMES OF INDIA Mumbai

Home | Cities | India | World | Business | Cricket | Sports | Health & Science | Infotech | Education | Entertainment

Mumbai | Delhi | Bangalore | Hyderabad | Chennai | Ahmedabad | Kolkata | Pune | Goa | Chandigarh | L

Rajkot | Surat | Vadodara | Mysore | Ludhiana | Mangalore | Hubli | Allahabad | Kanpur | Varanasi

Mumbai police to look out for unsecured Wi-Fi connections

9 Jan 2009, 1616 hrs IST, PTI

Print | Email | Discuss | Share | Save | Comment | Text:

MUMBAI: City policemen will be soon seen roaming in the streets with laptops in their hands in search of unsecured Wi-Fi connections.

In an initiative taken by the Mumbai police, in the backdrop of terror mails sent before blasts and terror attacks, policemen will be sent to various locations in the city in search of unsecured Wi-Fi connections.

"If a particular place's Wi-Fi is not password protected or secured then the policemen at the spot has the authority to issue notice to the owner of the Wi-Fi connection directing him to secure the

More Mumbai

- CISF men thrash airport m
- Bill dispute at hospital take
- BPCL seeks Centre's help
- BMC may roll out vada pav

Other News

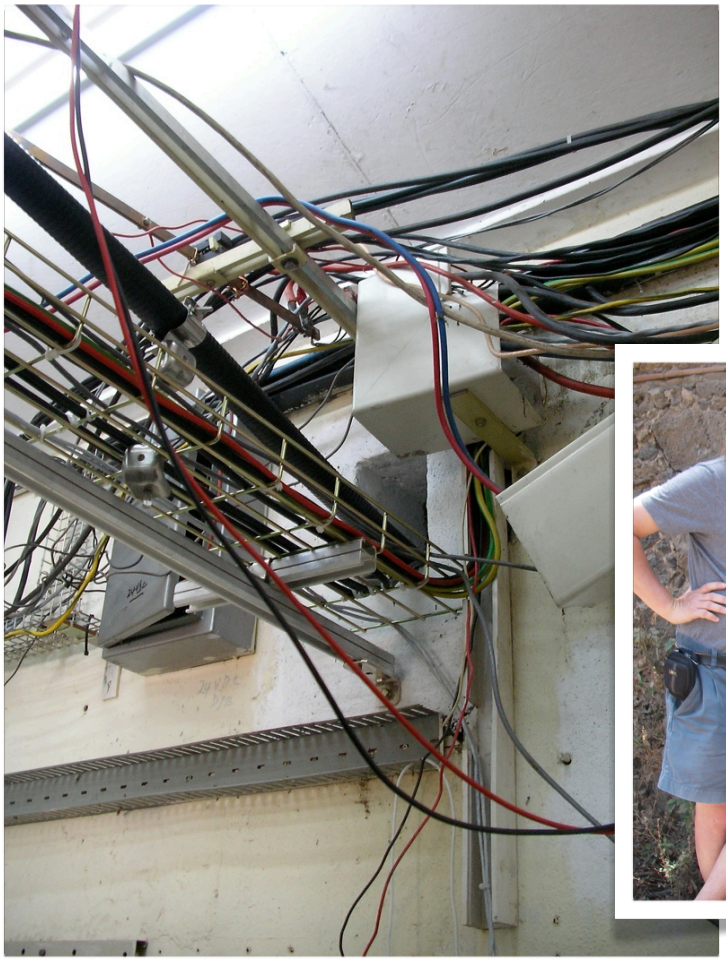
- 2 Afghans face death over Quran
- India's remarks on ISI a sm Pak
- Kiran Karnik appointed Sat
- AQ Khan's release another Pak: India

Malicious users are usually in the minority, but they may present a problem for you as an administrator. In this case, the malicious users had no intention of eavesdropping or stealing data from the local network; their objective was to use unsecured Internet connections to hide their identity while coordinating a violent crime.

Basic security considerations

- ***Physical security***: Is the equipment well protected?
- ***Authentication***: Who are you really talking to?
- ***Privacy***: Can communications be intercepted by a third party? How much data do you record about your users?
- ***Anonymity***: Is it desirable for users to remain anonymous?
- ***Accounting***: Are some users using too many resources? Do you know when your network is under attack and not simply overburdened?

Physical security problems



The photo on the left shows a "rat's nest" of wiring, mixing Ethernet, RF, power, and other cables in a tangle that makes it all to easy for someone to accidentally (or intentionally) cause problems.

On the right, an unlocked and open phone box by the side of the road in Mexico.

Protecting your wireless network

Here are a few security measures that can be used to protect your users and your wireless networks.

- ***"Closed" networks***
- ***MAC filtering***
- ***Captive Portals***
- ***WEP encryption***
- ***WPA encryption***
- ***Strong end-to-end encryption***

These methods are presented in increasing order of protection and complexity.

“Closed” Networks

By hiding SSID (i.e. not advertising it in *beacons*), you can prevent your network from being shown in network scan utilities.

Advantages:

- Standard security feature supported by virtually all access points.
- Unwanted users cannot accidentally choose a “closed” network from a network list.

Disadvantages:

- Users must know the network name in advance.
- “Closed” networks are not easily found in a site survey, and yet they are easily found using passive monitoring tools.

MAC filtering

A MAC filter may be applied to an access point to control which devices may be permitted to connect.

Advantages:

- Standard security feature supported by virtually all access points.
- Only devices with a matching MAC address may connect to your network.

Disadvantages:

- MAC tables are inconvenient to maintain.
- MAC addresses are transmitted in the clear (even when using WEP encryption), and are easily copied and reused.

MAC addresses can be changed on most cards and OSs.

Captive Portals

A captive portal is an authentication mechanism useful in cafés, hotels, and other settings where casual user access is required.

By using a web browser for authentication, captive portals work with virtually all laptops and operating systems. Captive portals are typically used on open networks with no other authentication methods (such as WEP or MAC filters).

Since they do not provide strong encryption, captive portals are not a very good choice for networks that need to be locked down to only allow access from trusted users.

Captive Portals

Popular captive portals

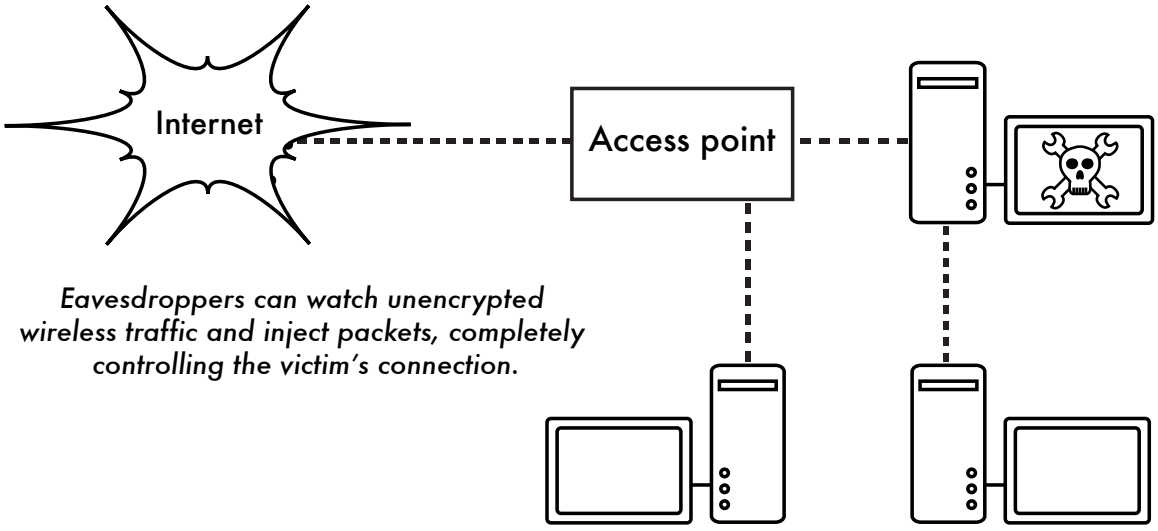
These open source captive portals support basic "splash pages", authentication to RADIUS, accounting, pre-paid ticketing, and many other features.

- Coova (*http://coova.org/*)
- WiFi Dog (*http://www.wifidog.org/*)
- m0n0wall (*http://m0n0.ch/wall/*)

NOTE: Coova supersedes Chillispot, which is no longer maintained.

Eavesdropping

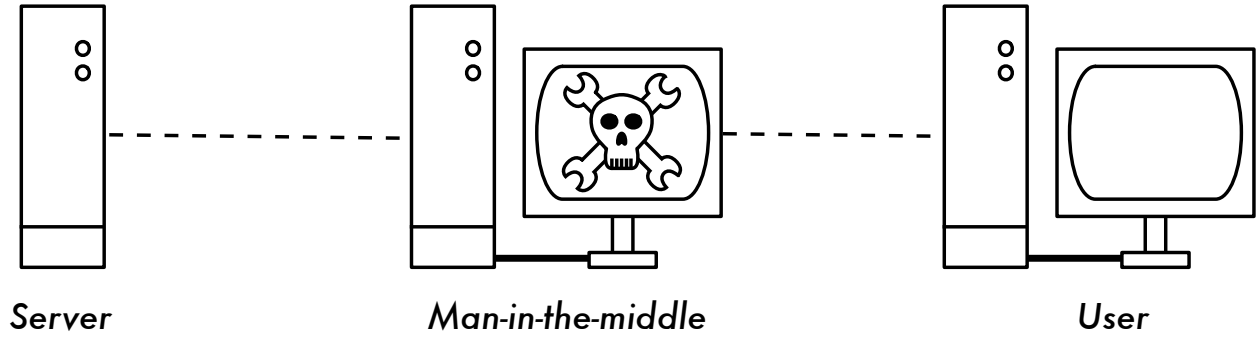
By passively listening to network data, malicious users can gather valuable private information.



Eavesdroppers can watch unencrypted wireless traffic and inject packets, completely controlling the victim's connection.

Man-in-the-middle (MITM)

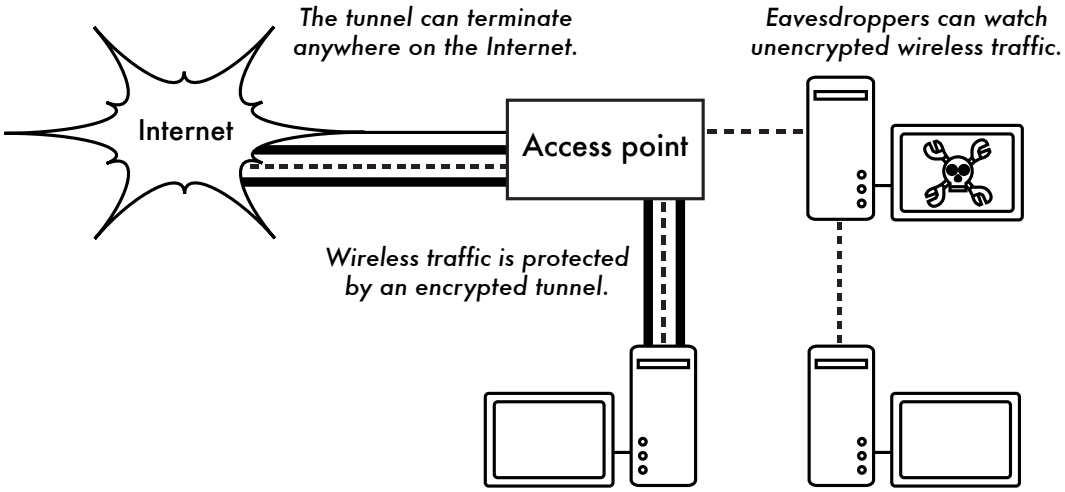
The man-in-the-middle effectively controls everything the user sees, and can record and manipulate all traffic.



Encryption can help

Encryption can help to protect traffic from eavesdroppers. Some access points can attempt to isolate client devices.

But without a public key infrastructure, strong encryption alone cannot completely protect against this kind of attack.



Encryption basics

- Encrypting information is relatively **easy**
- Key distribution is **difficult**
- Unique identification is a challenge with wireless
- Public key cryptography solves many (but not all) problems
- Man-in-the-middle is still possible if encryption is used without a ***public key infrastructure*** (***PKI***)
- No PKI is completely secure

PKI failure: 2001

http://amug.org/~glguerin/opinion/revocation.html

"In late January 2001, VeriSign erroneously issued two Class 3 code-signing certificates to someone falsely claiming to represent Microsoft. The certificates were issued in Microsoft's name, specifically "*Microsoft Corporation*". After issuing the certificates, a routine VeriSign audit uncovered the error in mid-March, about 6 weeks later."

PKI failure: 2009

http://www.networkworld.com/news/2009/010609-verisign-ssl-certificate-exploit.html

NETWORKWORLD

News | Blogs & Columns | Subscriptions | Videos | Events | More

Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SMB

Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall / UTM | IDS / IPS | NAC

Rogue SSL certificate exploit puts VeriSign on the spot

Wishes "white hat" researchers had notified VeriSign before public demo

By Ellen Messmer , Network World , 01/06/2009

Share/Email | Buzz up! | 3 Comments | Print

Following the success of researchers last week in creating a false SSL certificate based on VeriSign's RapidSSL brand, the company is scrambling to explain how it happened, how it's preventing it from reoccurring, and whether its other SSL certificate-generation services are at risk.

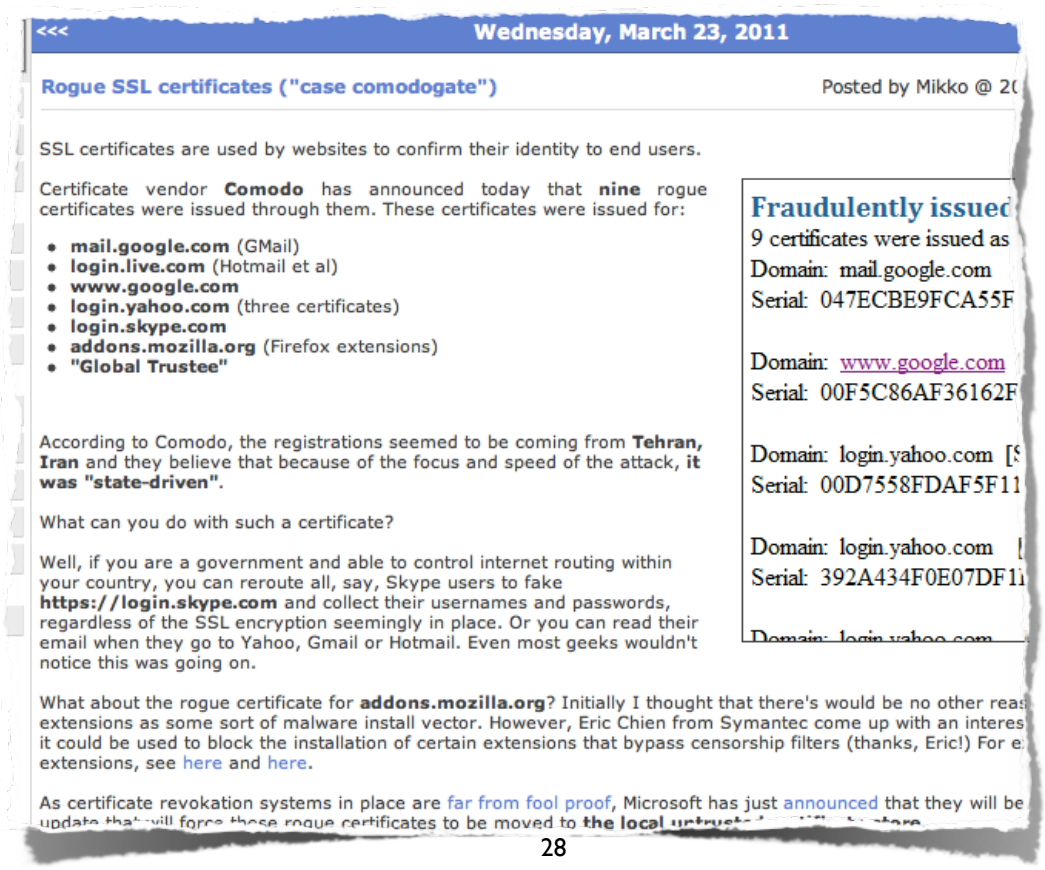
SSL certificates are supposed to be unique identifiers for Web sites and other purposes, but on Dec. 30, an international team of researchers demonstrated at the Berlin Chaos Communication Congress event how they could exploit a weakness in the MD5 hash algorithm in VeriSign's automated RapidSSL certificate-issuance service to gain possession of what they call a "rogue Certificate Authority certificate."

"This certificate allows us to impersonate any Web site on the Internet, including banking and e-commerce sites secured using the HTTPS

Enterprise Security: Download now

More rogue SSL certificates: 2011

http://www.f-secure.com/weblog/archives/00002128.html



<<< Wednesday, March 23, 2011

Rogue SSL certificates ("case comodogate") Posted by Mikko @ 2(

SSL certificates are used by websites to confirm their identity to end users.

Certificate vendor **Comodo** has announced today that **nine** rogue certificates were issued through them. These certificates were issued for:

- **mail.google.com** (GMail)
- **login.live.com** (Hotmail et al)
- **www.google.com**
- **login.yahoo.com** (three certificates)
- **login.skype.com**
- **addons.mozilla.org** (Firefox extensions)
- **"Global Trustee"**

Fraudulently issued
9 certificates were issued as
Domain: mail.google.com
Serial: 047ECBE9FCA55F

Domain: www.google.com
Serial: 00F5C86AF36162F

Domain: login.yahoo.com [S
Serial: 00D7558FDAF5F11

Domain: login.yahoo.com [
Serial: 392A434F0E07DF1

According to Comodo, the registrations seemed to be coming from **Tehran, Iran** and they believe that because of the focus and speed of the attack, **it was "state-driven"**.

What can you do with such a certificate?

Well, if you are a government and able to control internet routing within your country, you can reroute all, say, Skype users to fake **https://login.skype.com** and collect their usernames and passwords, regardless of the SSL encryption seemingly in place. Or you can read their email when they go to Yahoo, Gmail or Hotmail. Even most geeks wouldn't notice this was going on.

What about the rogue certificate for **addons.mozilla.org**? Initially I thought that there's would be no other rea extensions as some sort of malware install vector. However, Eric Chien from Symantec come up with an interes it could be used to block the installation of certain extensions that bypass censorship filters (thanks, Eric!) For e extensions, see here and here.

As certificate revokation systems in place are far from fool proof, Microsoft has just announced that they will be update that will force these rogue certificates to be moved to **the local untrust**

WEP Encryption

Part of the 802.11 standard, ***Wired Equivalent Privacy*** provides basic shared encryption at layer two. WEP works with nearly all modern WiFi devices.

Advantages: Standard security feature supported by virtually all access points.

Disadvantages: Shared key, numerous security flaws, incompatible key specification methods, long-term maintenance is impossible on large networks.

In short: **Use WPA2-PSK instead**.

WPA encryption

WPA2 (802.11i) is now the standard for protected Wi-Fi access. It uses 802.1x port authentication with the Advanced Encryption Standard (AES) to provide very strong authentication and encryption.

Advantages:

- Significantly stronger protection than WEP
- Open standard
- Verification of clients and access points.
- Good for "campus" or "office" networks

Disadvantages: Some vendor interoperability problems, complex configuration, protection only at layer two.

WPA-PSK (pre-shared key)

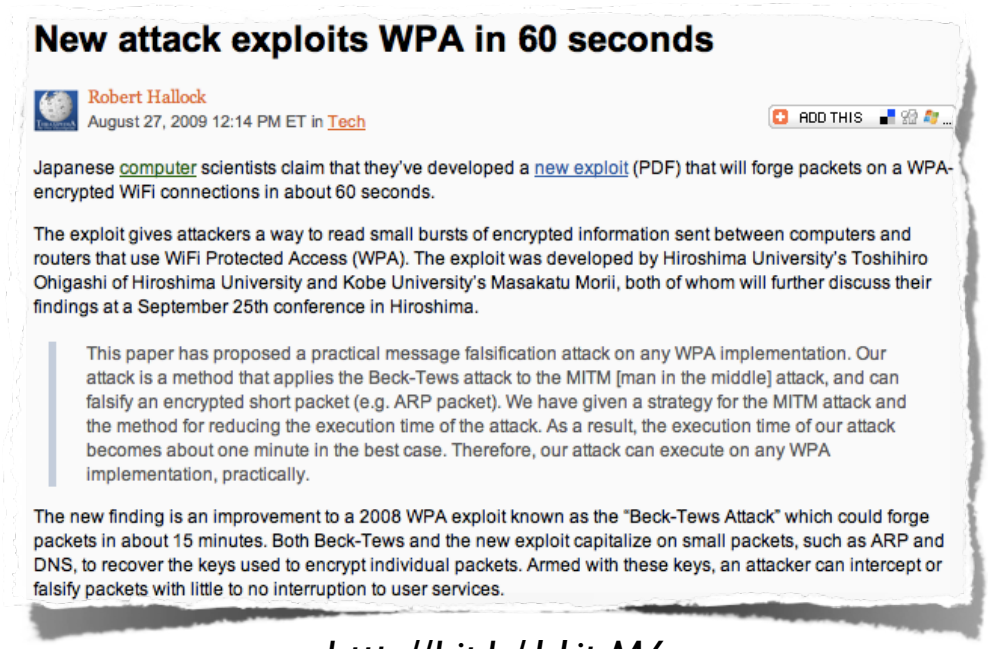
PSK stands for Pre-Shared Key. The intent behind WPA-PSK was to provide a simple WPA solution comparable to WEP, but more secure.

- Pass phrase of 8 to 64 characters
- While WPA-PSK is stronger than WEP, problems still exist
- Church of WiFi's WPA2-PSK Rainbow Tables: 1 million common passwords x 1,000 common SSIDs. 40 GB of lookup tables available on DVDs.

http://www.renderlab.net/projects/WPA-tables/

WPA-TKIP exploits

New attacks are constantly released as new methods are discovered. This technique can inject small packets (such as ARP or DNS packets) into a WPA-TKIP network.



New attack exploits WPA in 60 seconds

Robert Hallock
August 27, 2009 12:14 PM ET in Tech

ADD THIS

Japanese computer scientists claim that they've developed a new exploit (PDF) that will forge packets on a WPA-encrypted WiFi connections in about 60 seconds.

The exploit gives attackers a way to read small bursts of encrypted information sent between computers and routers that use WiFi Protected Access (WPA). The exploit was developed by Hiroshima University's Toshihiro Ohigashi of Hiroshima University and Kobe University's Masakatu Morii, both of whom will further discuss their findings at a September 25th conference in Hiroshima.

> This paper has proposed a practical message falsification attack on any WPA implementation. Our attack is a method that applies the Beck-Tews attack to the MITM [man in the middle] attack, and can falsify an encrypted short packet (e.g. ARP packet). We have given a strategy for the MITM attack and the method for reducing the execution time of the attack. As a result, the execution time of our attack becomes about one minute in the best case. Therefore, our attack can execute on any WPA implementation, practically.

The new finding is an improvement to a 2008 WPA exploit known as the "Beck-Tews Attack" which could forge packets in about 15 minutes. Both Beck-Tews and the new exploit capitalize on small packets, such as ARP and DNS, to recover the keys used to encrypt individual packets. Armed with these keys, an attacker can intercept or falsify packets with little to no interruption to user services.

http://bit.ly/11ipM6

Strong encryption software

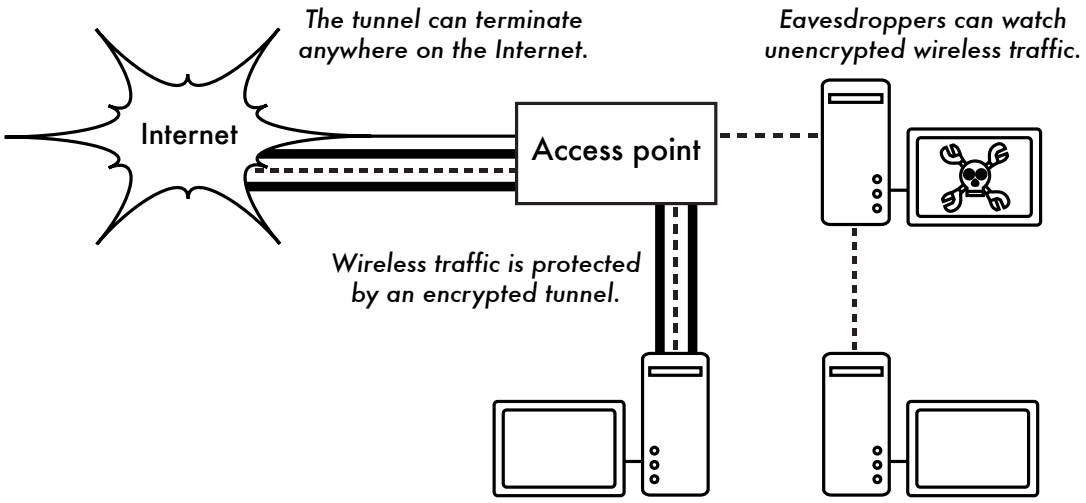
Good end-to-end security software should provide strong **Authentication**, **Encryption**, and **Key Management**.

Examples include:

- ***SSL*** (Secure Socket Layer)
- ***SSH*** (Secure Shell)
- ***OpenVPN***
- ***IPSec*** (Internet Protocol Security)
- ***PPTP*** (Point-to-Point Tunneling Protocol)

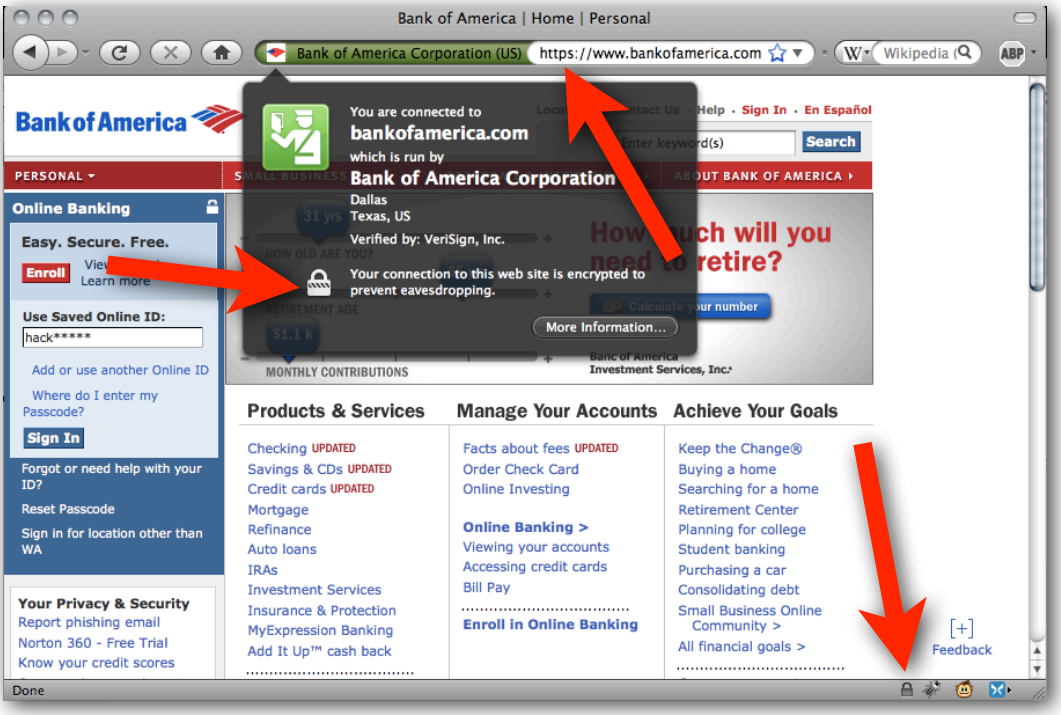
Encrypted tunnels

End-to-end encryption provides protection all the way to the remote end of the connection.



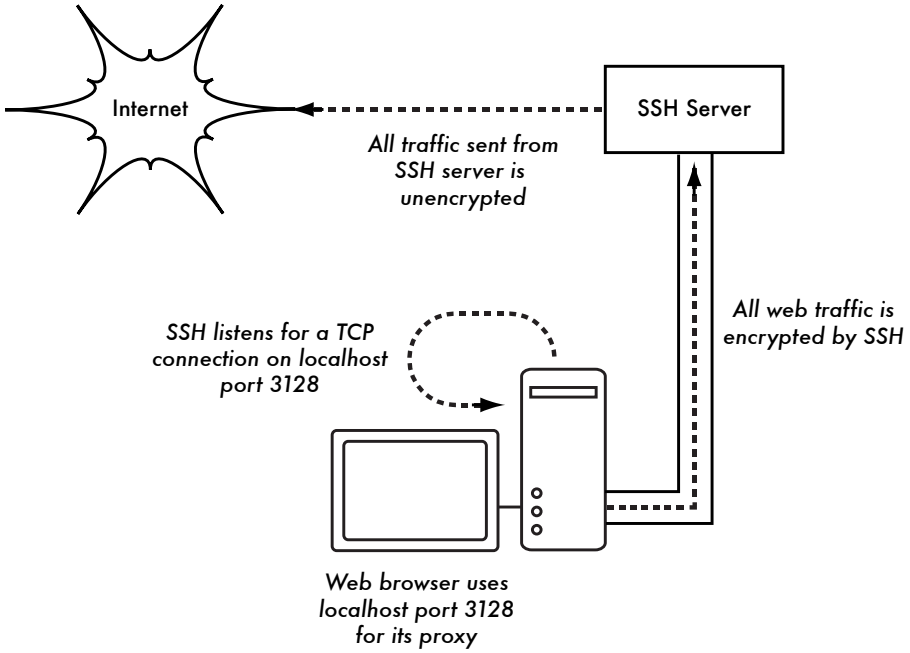
SSL encryption

SSL is built into many popular Internet programs, including web browsers and email clients.



SSH tunnels

SSH is known for providing command line shell access, but it is also general-purpose TCP tunneling tool and encrypting SOCKS proxy.



OpenVPN

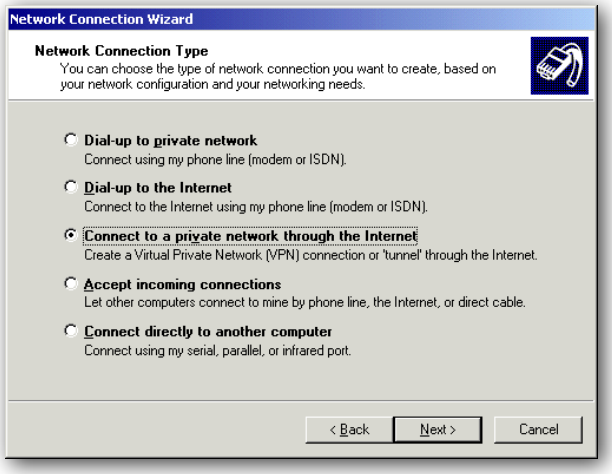
OpenVPN is a powerful cross-platform VPN solution.

- Supports Windows Vista/XP/2000, Linux, BSD, Mac OS X
- SSL/TLS or shared-key encryption
- VPN for layer 2 or layer 3 traffic
- Robust and very flexible: can operate over TCP, UDP, or even SSH!

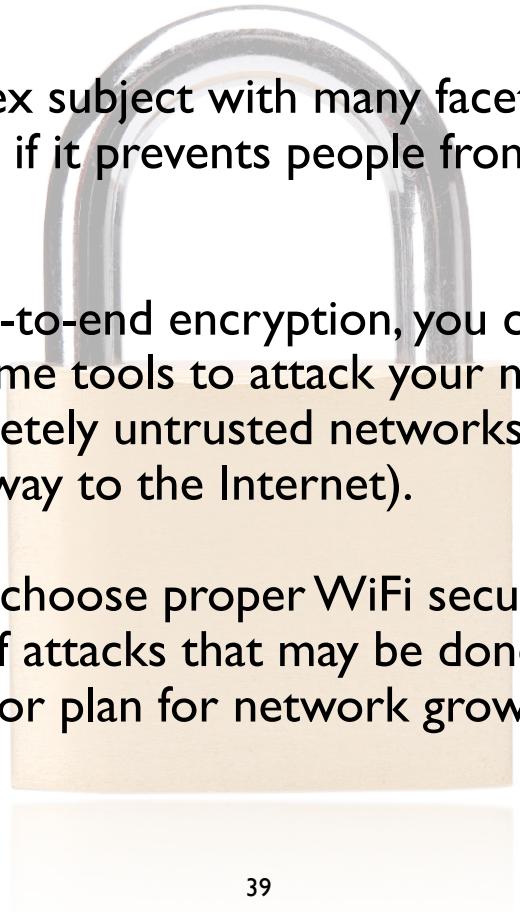
Other VPNs

IPSec, PPTP, Cisco VPN, etc. provide strong end-to-end encryption.

By providing strong authentication and encryption, VPNs make it safe to use untrusted networks, such as open wireless hotspots and the Internet.



Summary



Security is a complex subject with many facets. No security system is successful if it prevents people from effectively using the network.

By using strong end-to-end encryption, you can prevent others from using these same tools to attack your networks, and make it safe to use completely untrusted networks (from a public wireless AP all the way to the Internet).

By learning how to choose proper WiFi security settings, you can limit the type of attacks that may be done to your network, react to a problem or plan for network growth.

Thank you for your attention

For more details about the topics presented in this lecture, please see the book ***Wireless Networking in the Developing World***, available as free download in many languages at:

http://wndw.net/

See Chapter 6 of the book for more detailed information about the material covered in this talk.