Wireless Security and Monitoring

Training materials for wireless trainers

The Abdus Salam
International Centre
for Theoretical Physics

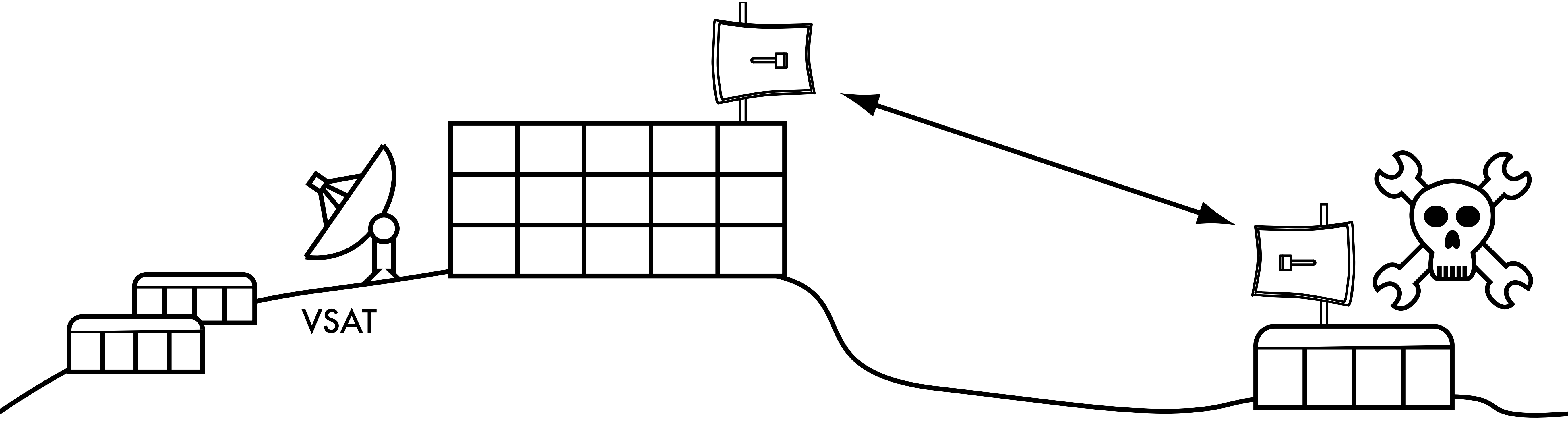
Goals

- 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?

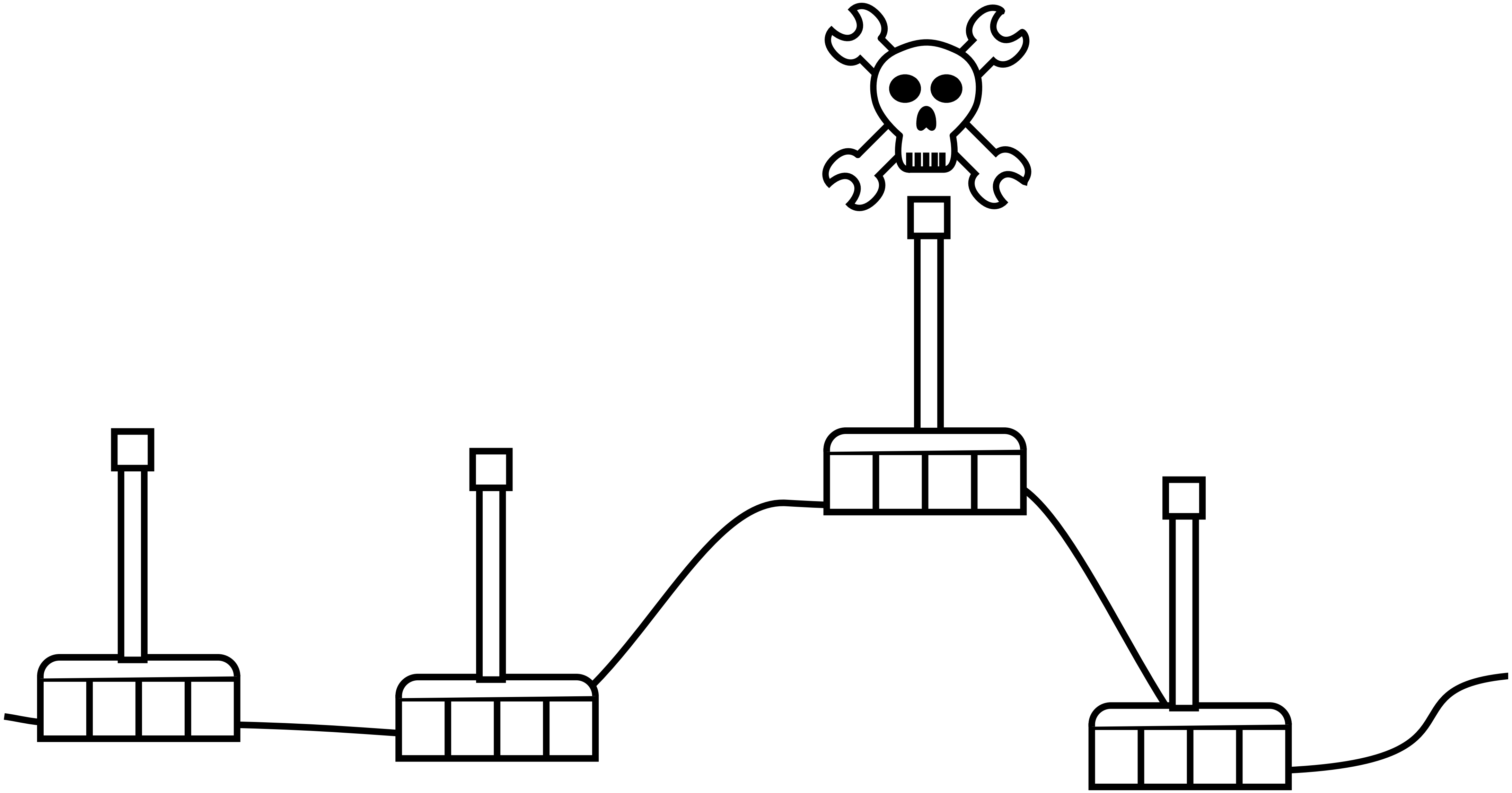
- Wireless is a ***shared medium***
- Attackers are relatively ***anonymous***
- End users are ***poorly educated***
- ***Denial-of-service*** is very simple
- ***Automated malicious attacks*** are increasingly complex
- ***Sophisticated tools*** are freely available

Attacks may come from far away



BANTAM

...or be completely undetectable.

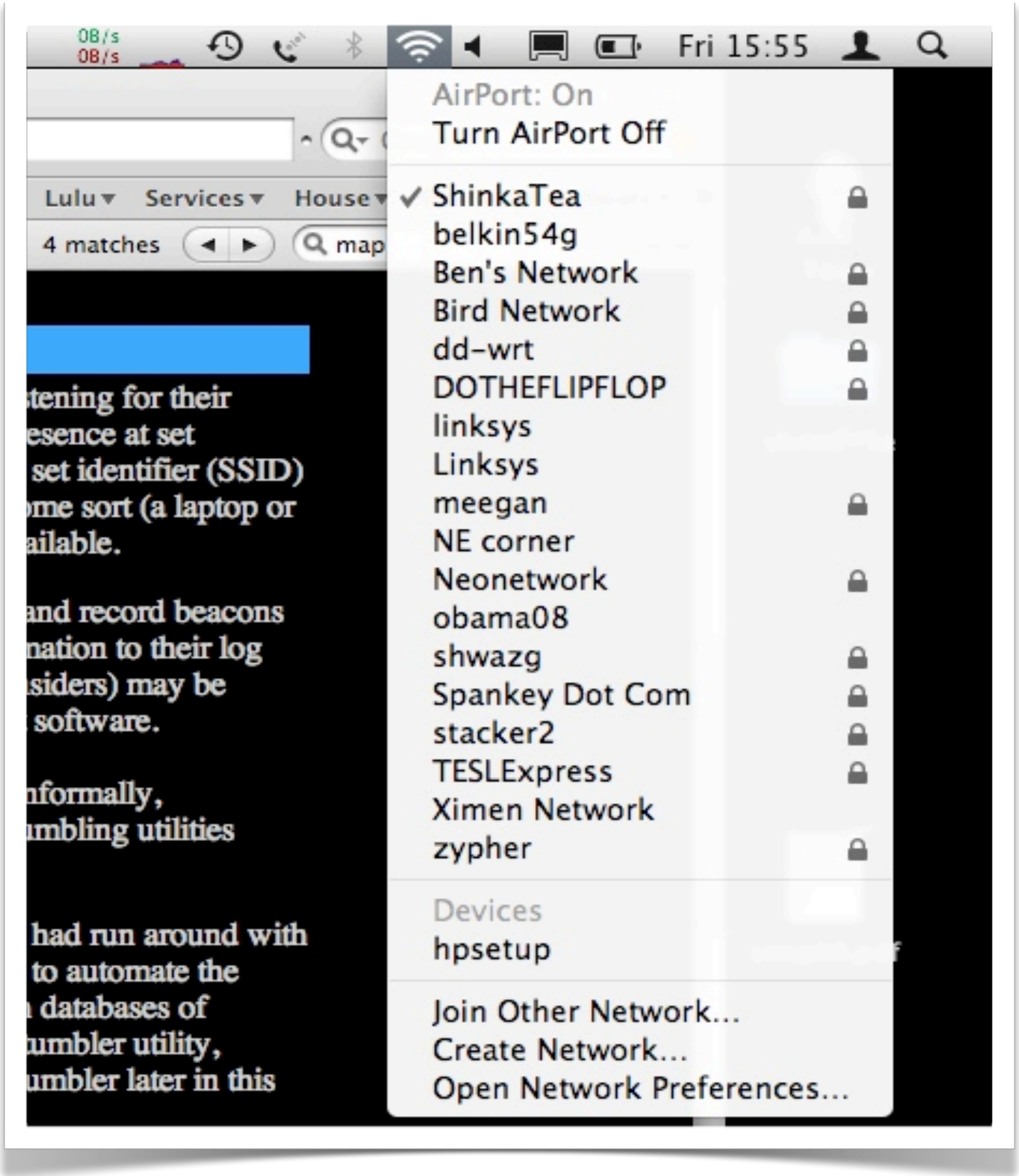


Who creates security problems?

- ***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.

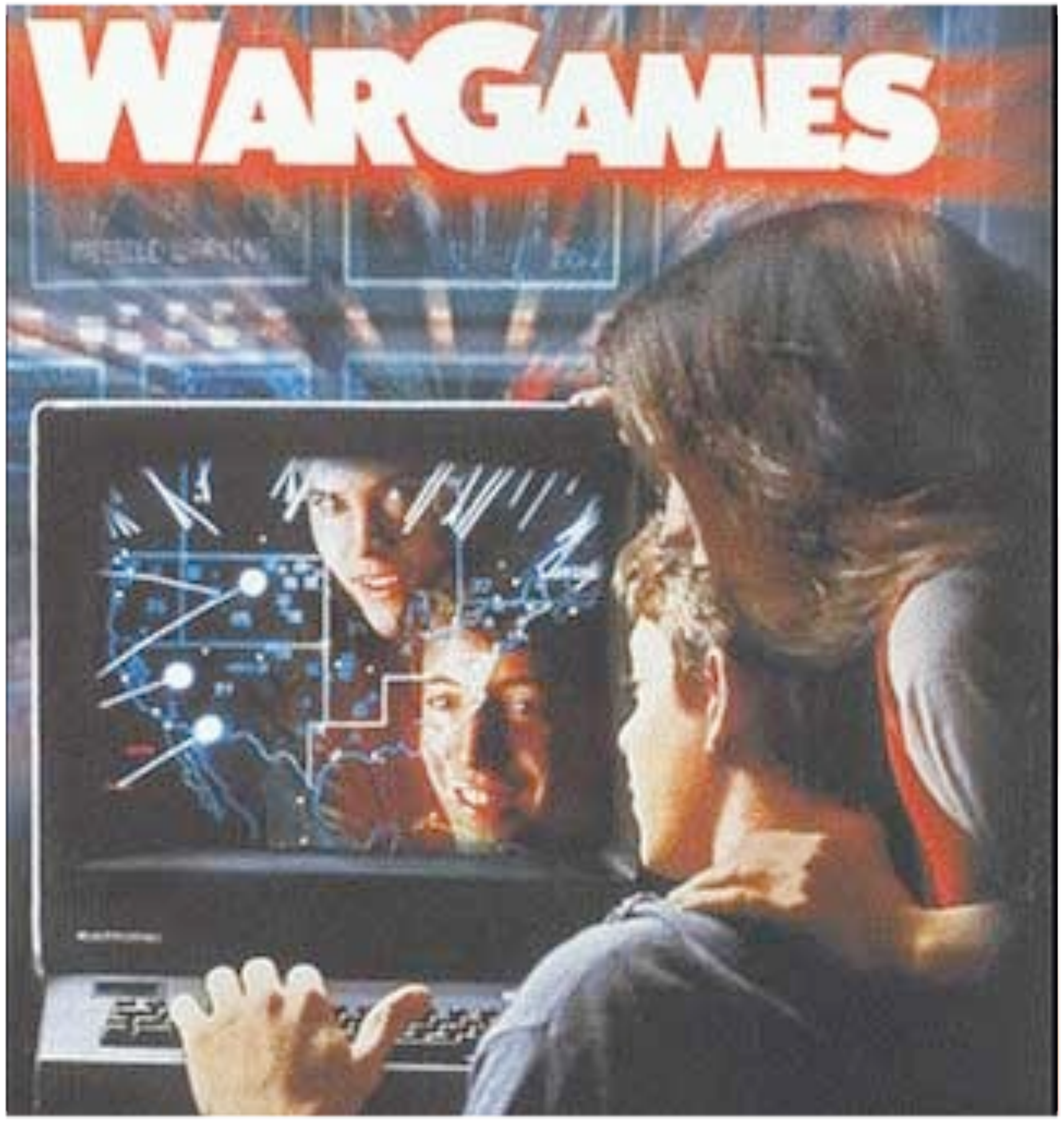


tening for their
esence at set
set identifier (SSID)
me sort (a laptop or
ailable.

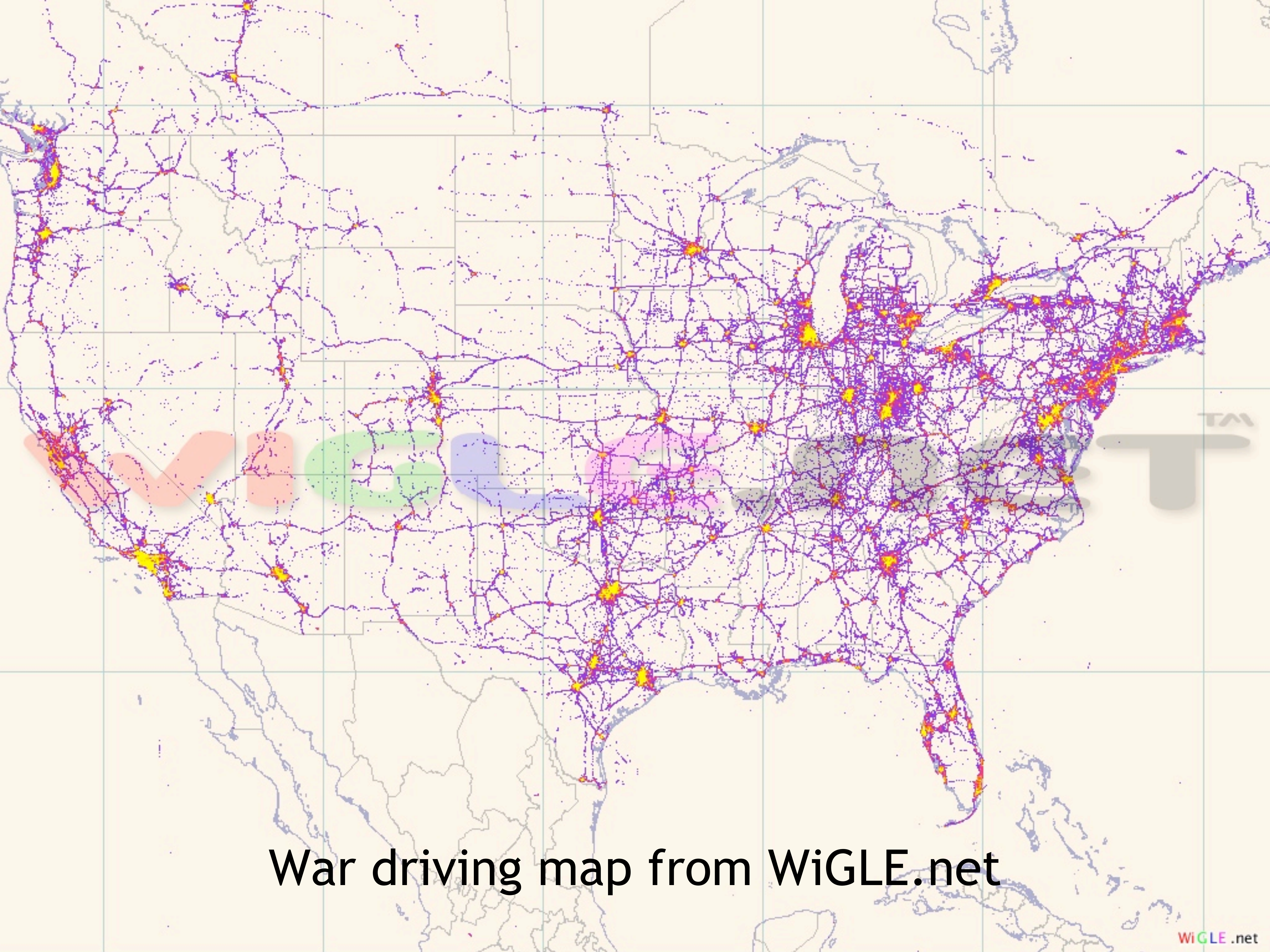
and record beacons
nation to their log
siders) may be
software.

nformally,
mbling utilities

had run around with
to automate the
databases of
umbler utility,
umbler later in this



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



War driving map from WiGLE.net

Rogue Access points

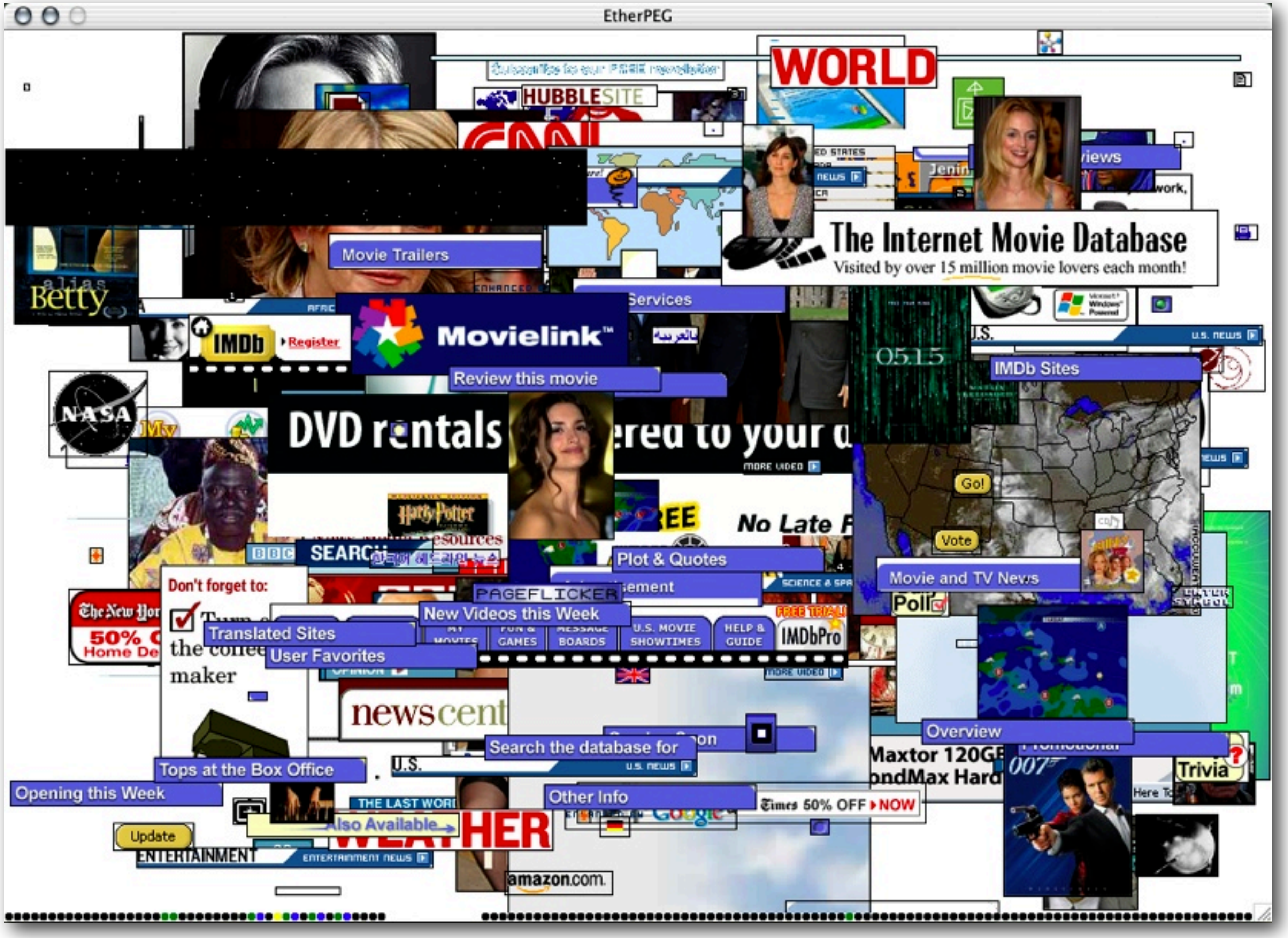
Access points may simply be installed incorrectly by legitimate users. Someone may want better wireless coverage in their office, or they might find security restrictions on the corporate wireless network too difficult to comply with.

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

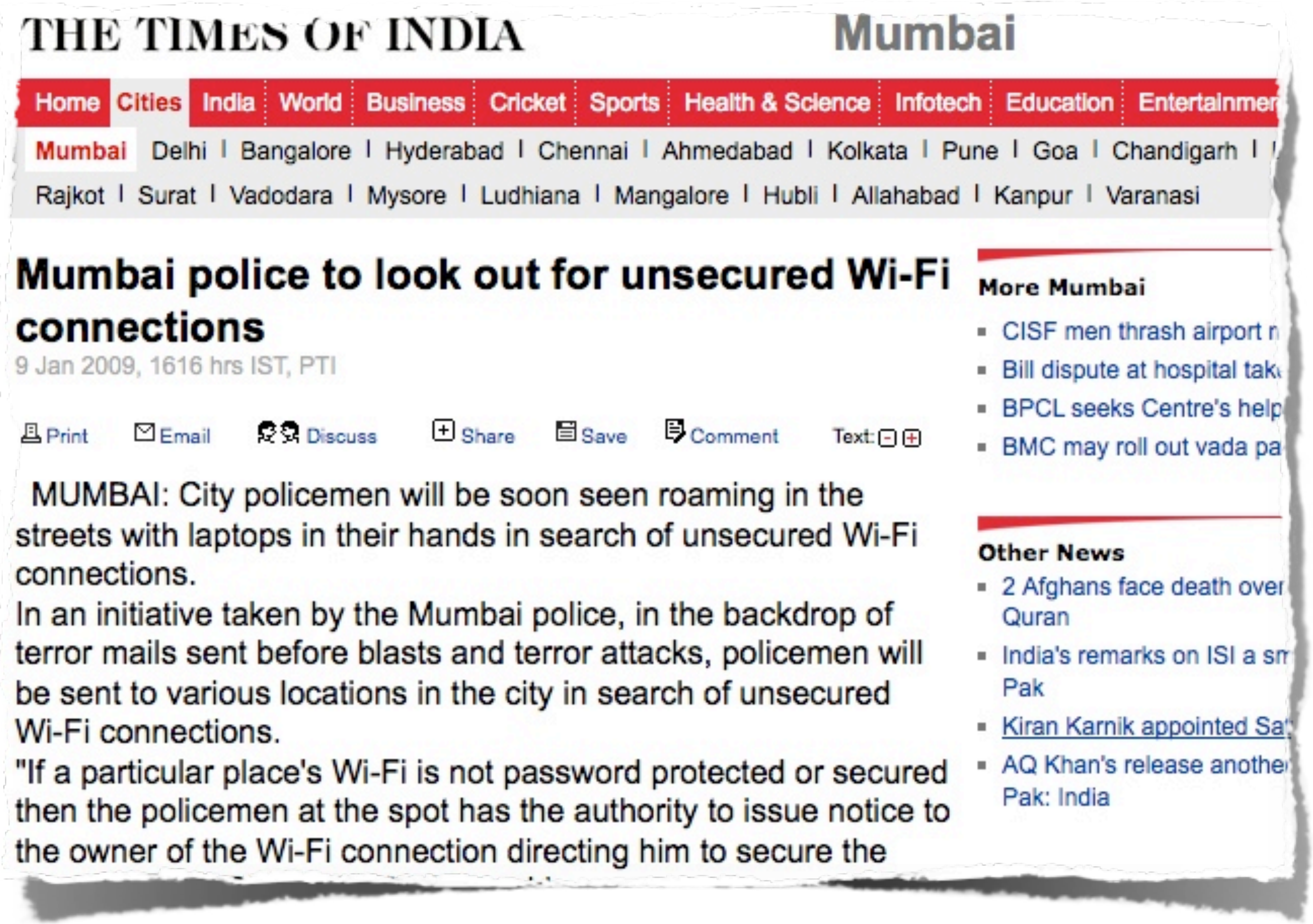
In addition, eavesdroppers who intend to collect data or do harm to the network may intentionally install an access point on your network, providing an effective “backdoor”.

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.



Malicious Users



Mumbai police to look out for unsecured Wi-Fi connections

9 Jan 2009, 1616 hrs IST, PTI

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

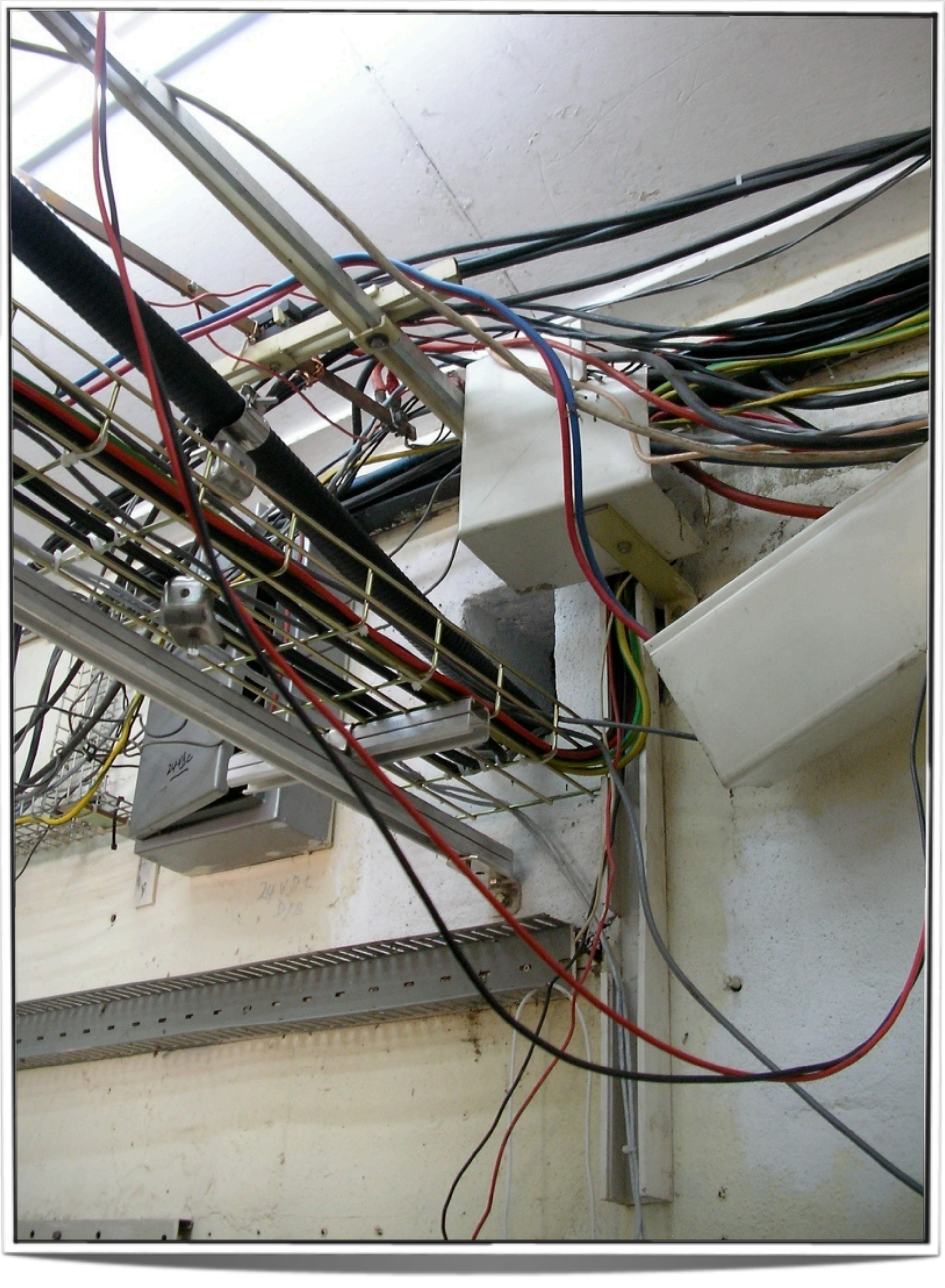
- CISF men thrash airport r
- Bill dispute at hospital tak
- BPCL seeks Centre's help
- BMC may roll out vada pa

Other News

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

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

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***

“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.

Captive Portals

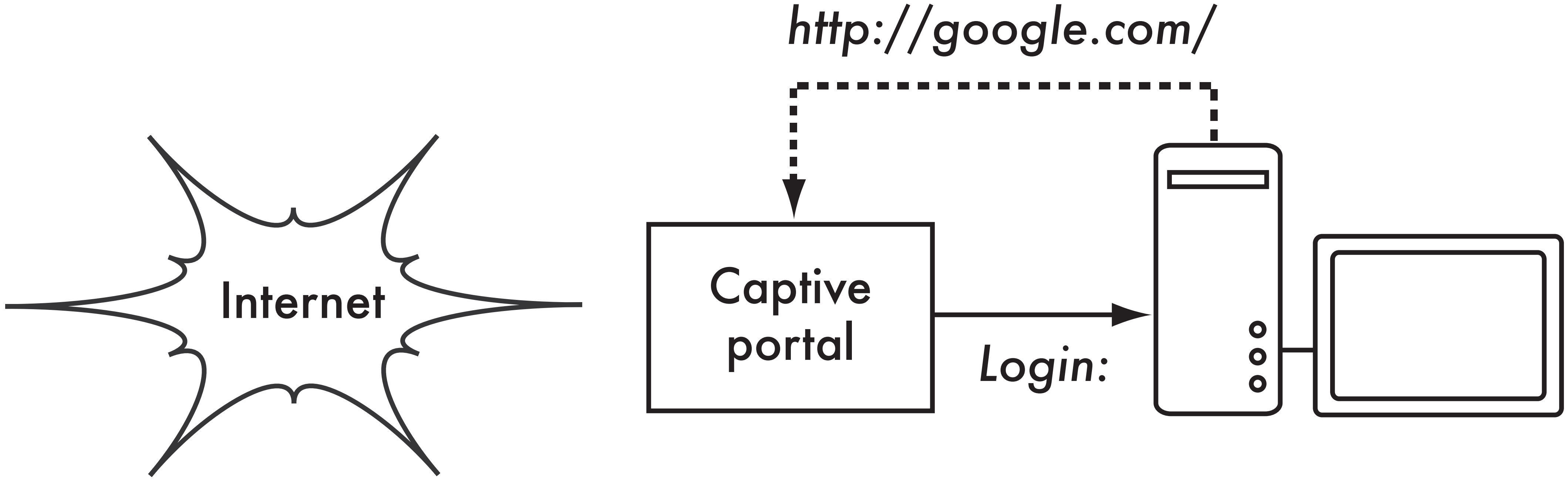
A captive portal is an authentication mechanism useful in cafés, hotels, and other settings where casual user access is required.

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.

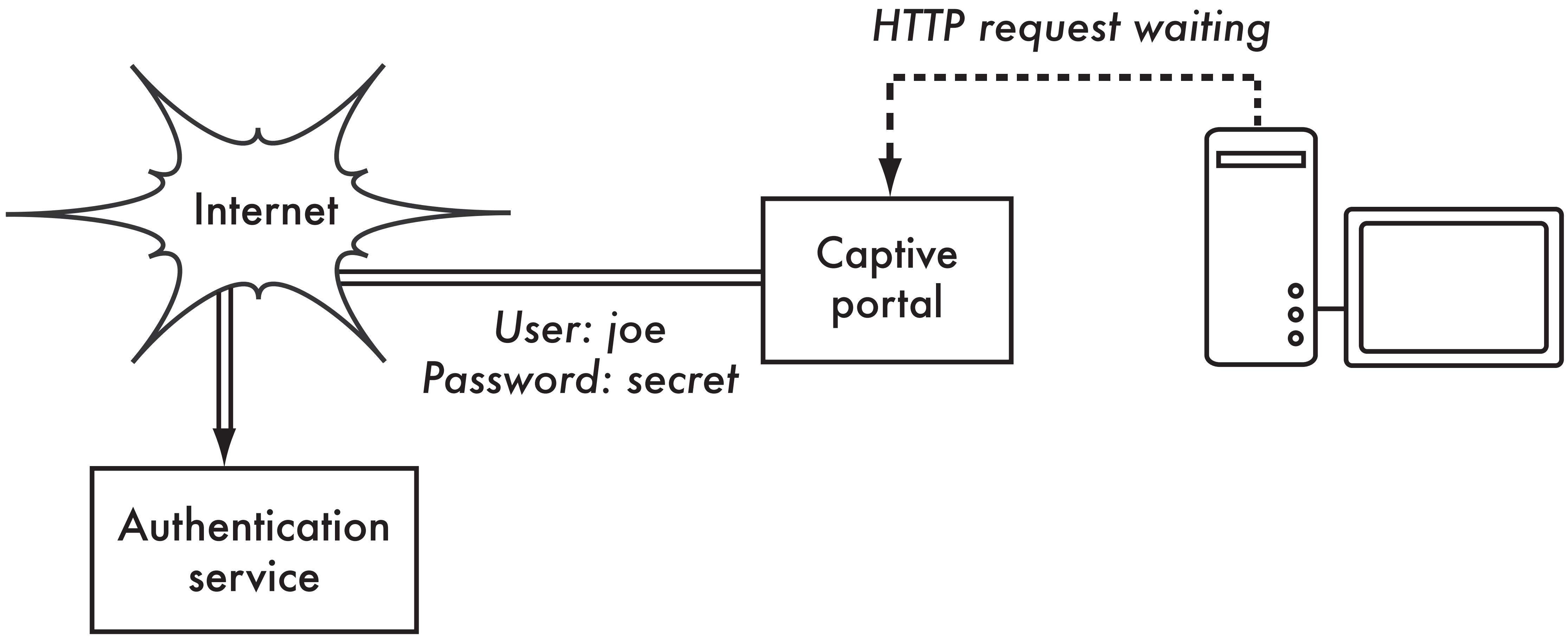
Captive portal: capture

To begin, a wireless user opens their laptop and selects the network. The computer requests a DHCP lease, which is granted. They then use their web browser to go to any site on the Internet.



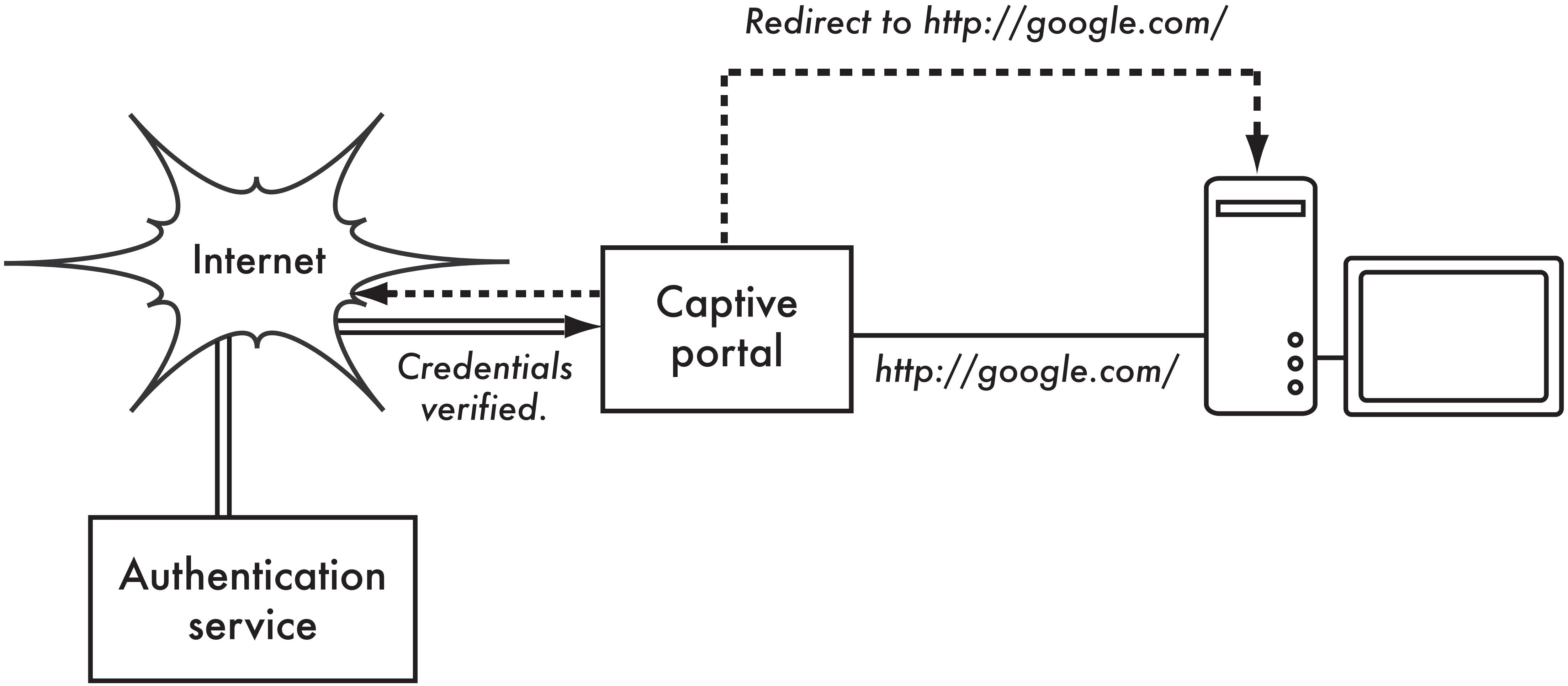
Captive portal: authenticate

Instead of receiving the requested page, the user is presented with a login screen. This page can require the user to enter a user name and password, simply click a "login" button, type in numbers from a pre-paid ticket, or enter any other credentials that the network administrators require.



Captive portal: release

Once authenticated, the user is permitted to access network resources, and is typically redirected to the site they originally requested.



Popular captive portals

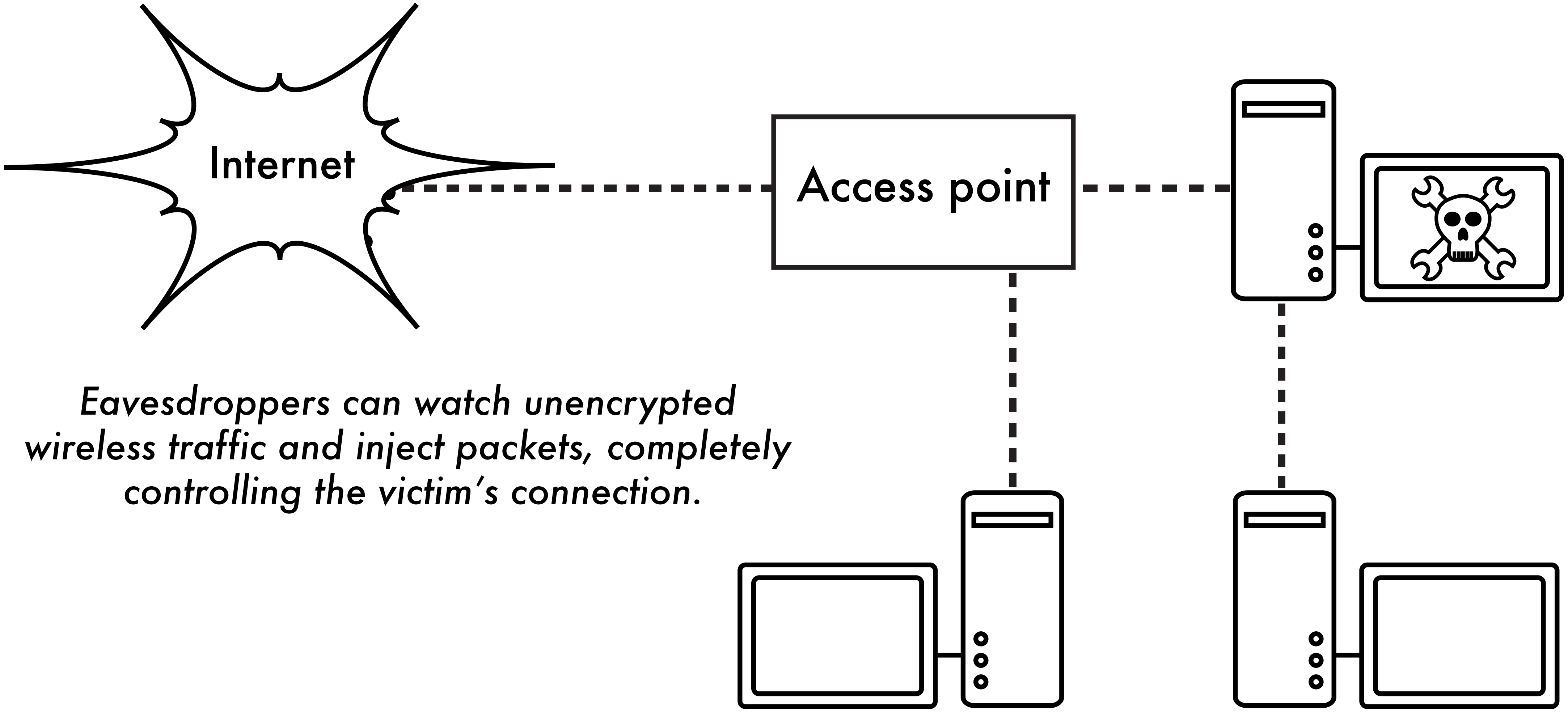
These open source captive portals support basic “splash pages”, authentication to RADIUS, accounting, pre-paid ticketing, and many other features.

- Chillispot (*http://www.chillispot.info/*)
- WiFi Dog (*http://www.wifidog.org/*)
- m0n0wall (*http://m0n0.ch/wall/*)
- NoCatSplash (*http://nocat.net/download/NoCatSplash/*)

Encryption 101

Eavesdropping

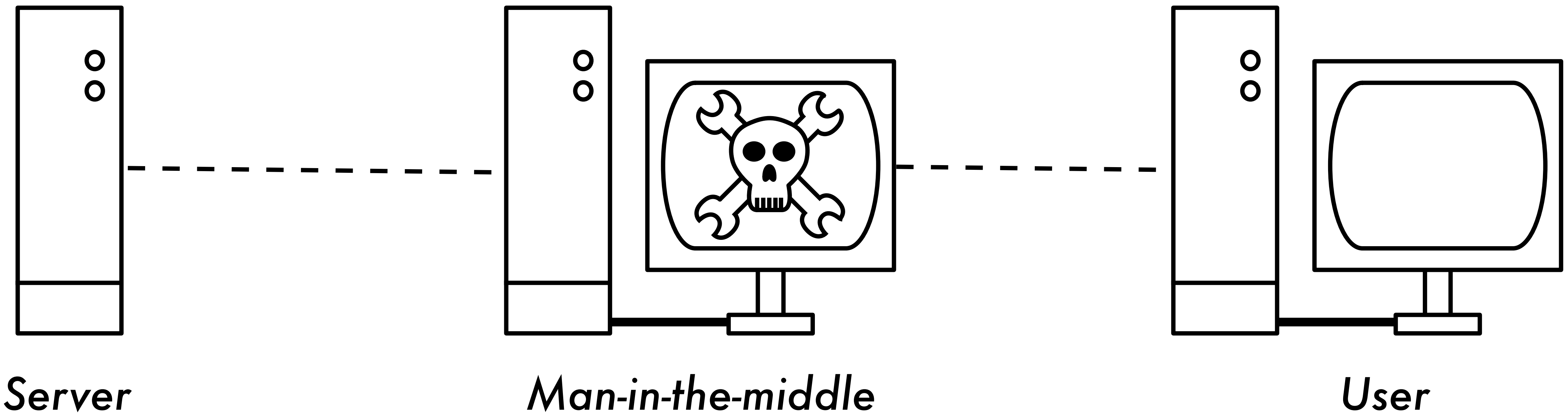
By passively listening to network data, malicious users can gather valuable private information.



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

Man-in-the-middle (MITM)

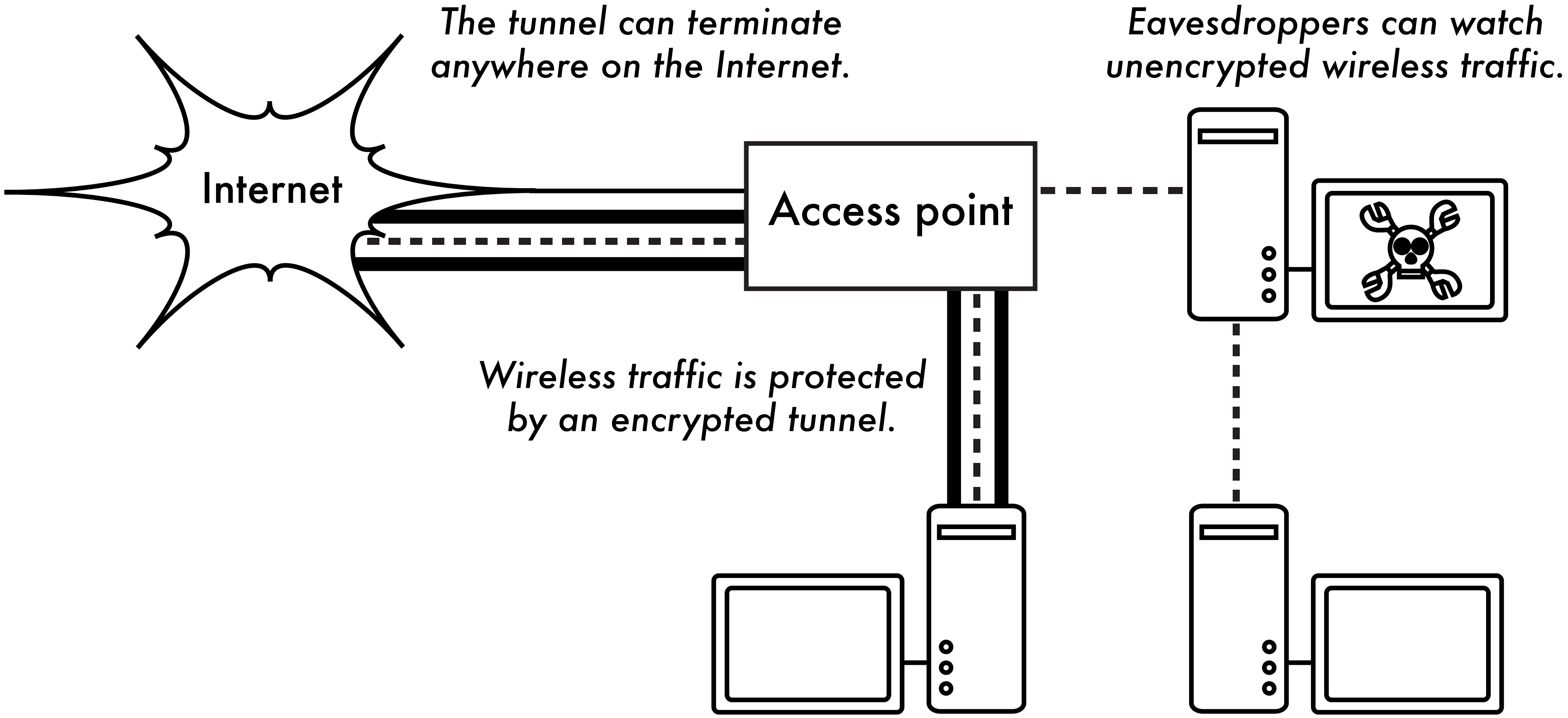
The man-in-the-middle effectively controls everything the user sees, and can record and manipulate all traffic.



Encryption can help

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

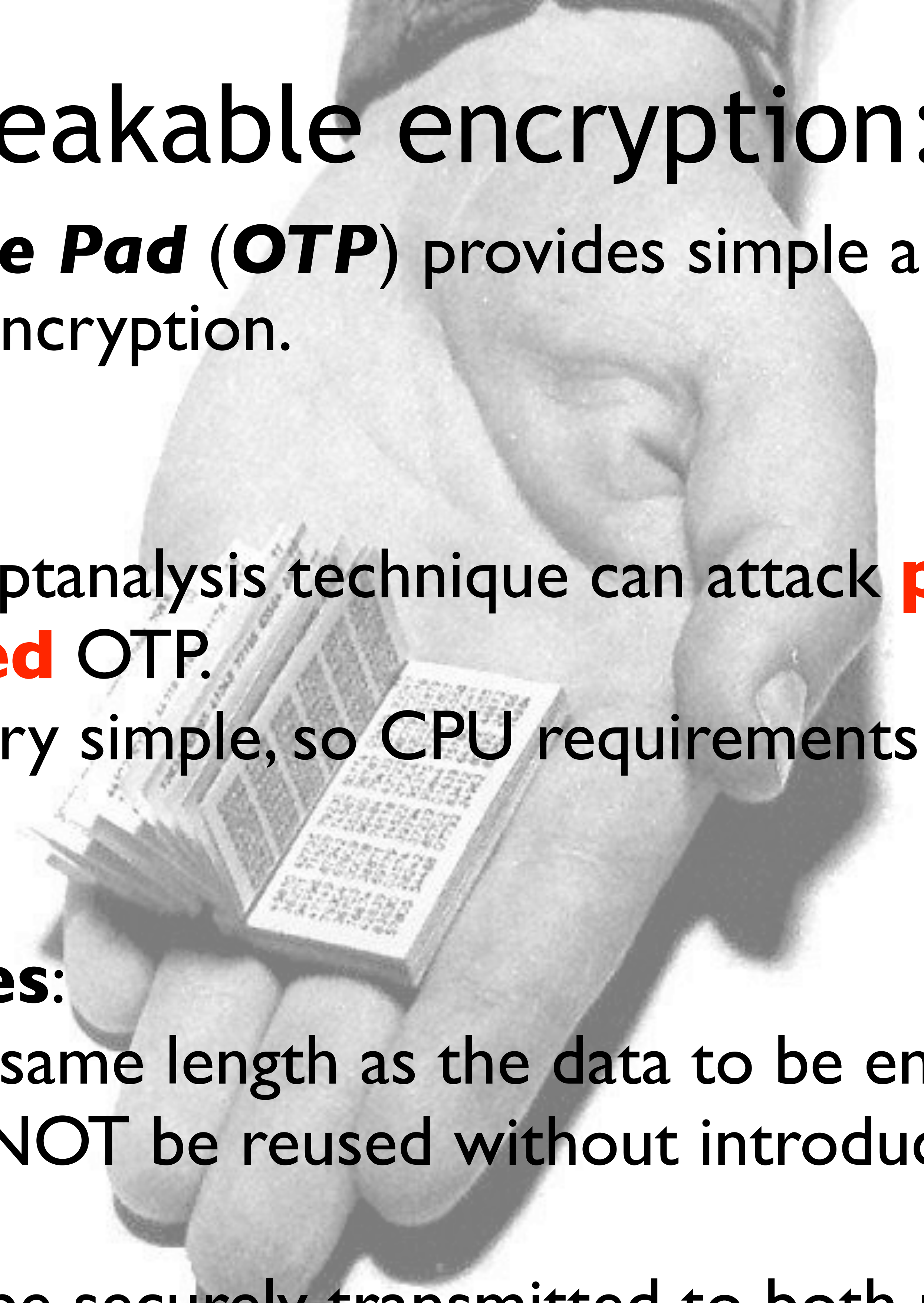
But without a public key infrastructure, strong encryption alone cannot completely protect against this kind of attack.


The tunnel can terminate anywhere on the Internet.
Eavesdroppers can watch unencrypted wireless traffic.
Internet
Access point
Wireless traffic is protected by an encrypted tunnel.

Encryption basics

- Encrypting information is **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

Unbreakable encryption: OTP



The ***One-Time Pad*** (***OTP***) provides simple and completely unbreakable* encryption.

Advantages:

- No known cryptanalysis technique can attack **properly implemented** OTP.
- The math is very simple, so CPU requirements are extremely minimal.

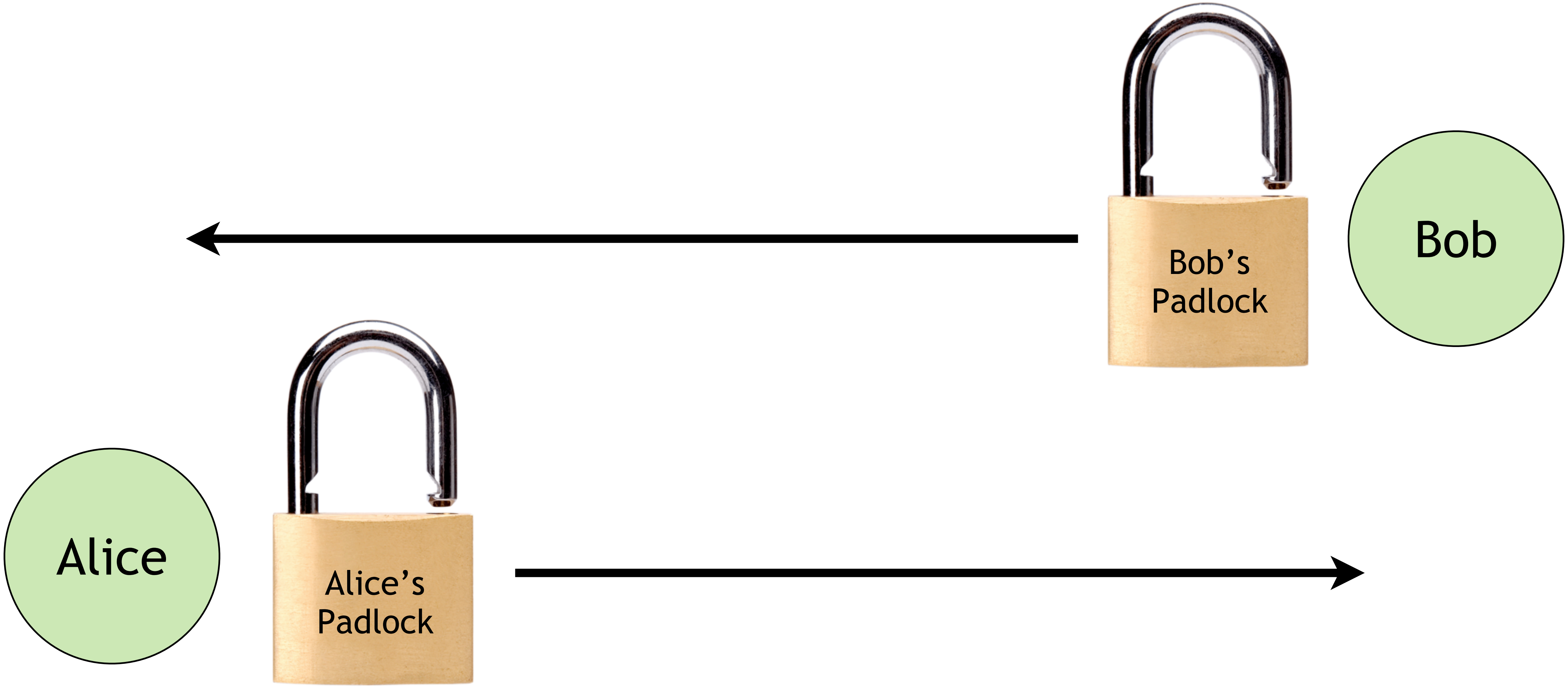
Disadvantages:

- The key is the same length as the data to be encrypted.
- The key CANNOT be reused without introducing exploitable weaknesses.
- The key must be securely transmitted to both parties, and completely destroyed after use.

Public key cryptography

Public Key cryptography is one (partial) solution to the key distribution problem.

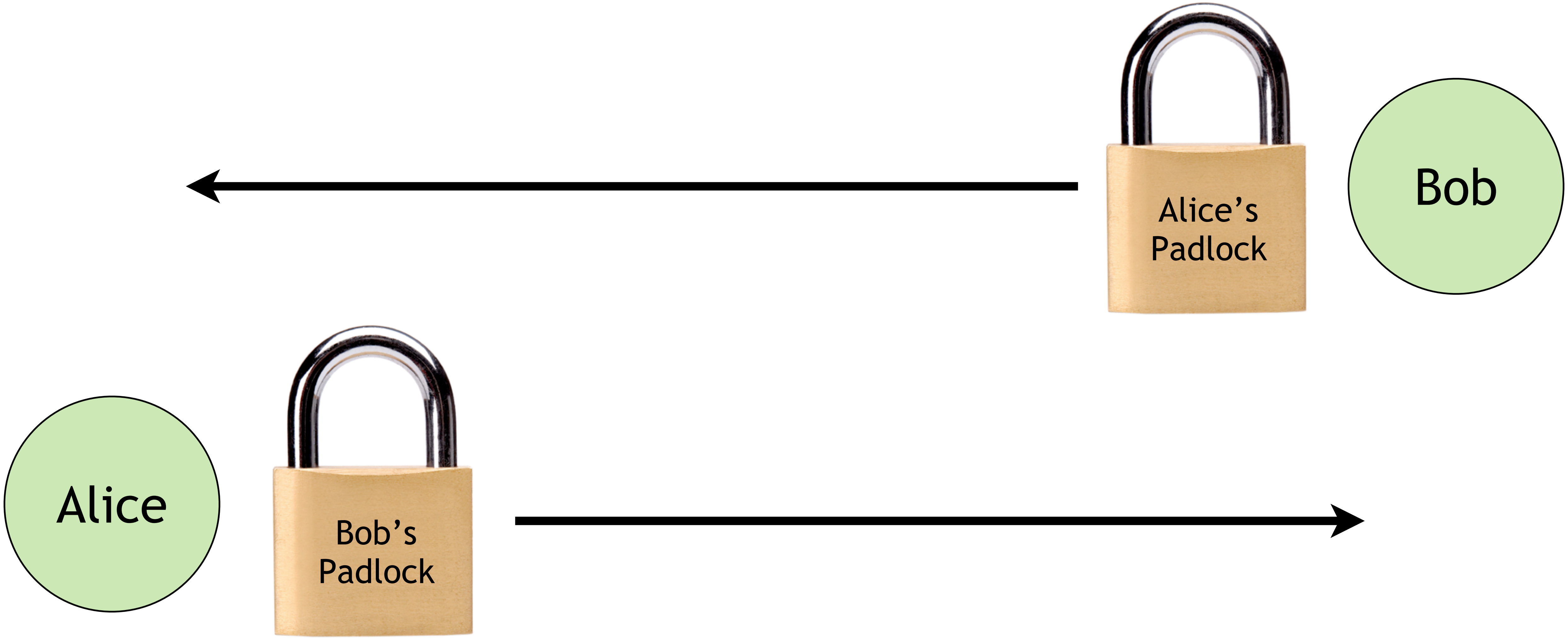
Step one: Alice and Bob exchange open padlocks through the mail. They keep their keys in their pockets.



Public key cryptography

Step two: When Alice wants to send Bob a message, she puts it in a box and locks it with Bob's padlock, then mails it back to him. Bob does the same to send a message to Alice.

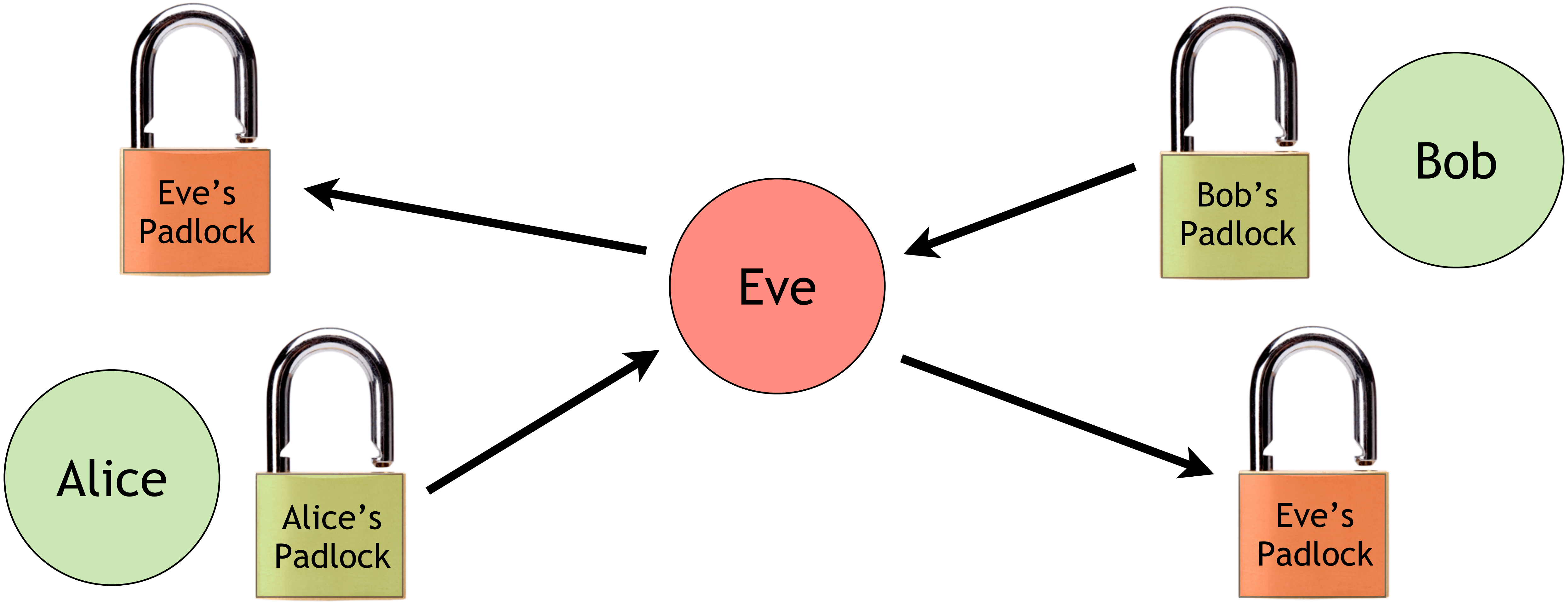
Since they kept their keys in their pockets, only they can open the locked boxes.



(Wo)Man in the Middle

Eve is an evil person who works in the post office. Eve wants to spy on Alice and Bob.

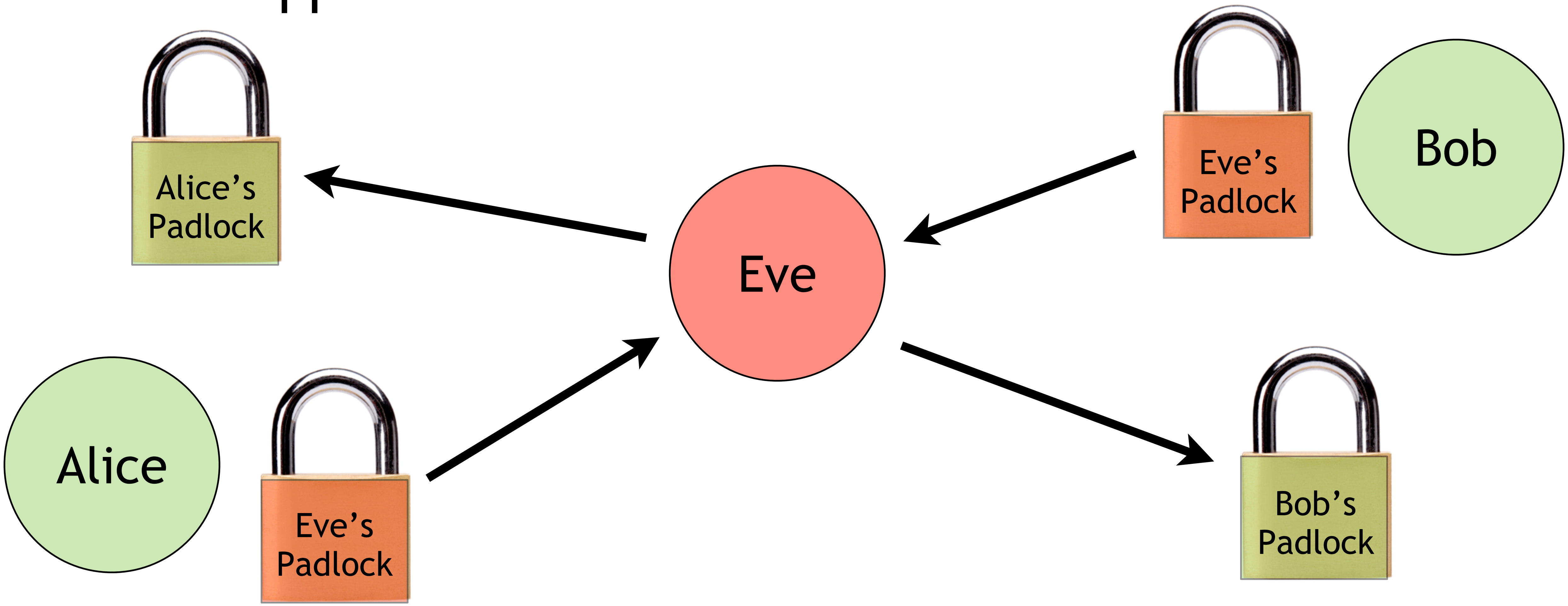
She intercepts the unlocked padlocks in step one and replaces them with her own unlocked padlocks, keeping Alice and Bob's original unlocked padlocks.



(Wo)Man in the Middle

Alice and Bob lock their secrets in boxes using Eve's padlocks without realizing it.

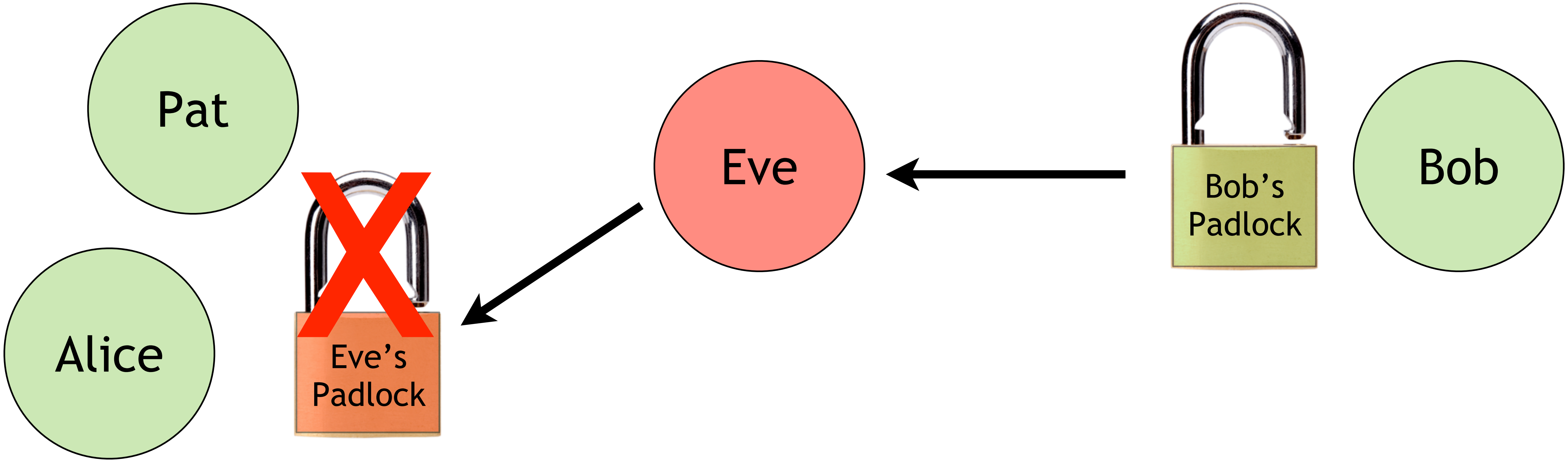
Eve then intercepts the locked boxes, unlocks them with her key, reads the messages, and locks them up again using Alice and Bob's unlocked padlocks. Alice and Bob have no idea that this has happened.



PKI (almost) foils Eve

Pat is a friend of Alice and Bob who can identify their locks by looking at them. When Alice receives an open padlock apparently from Bob, she calls Pat.

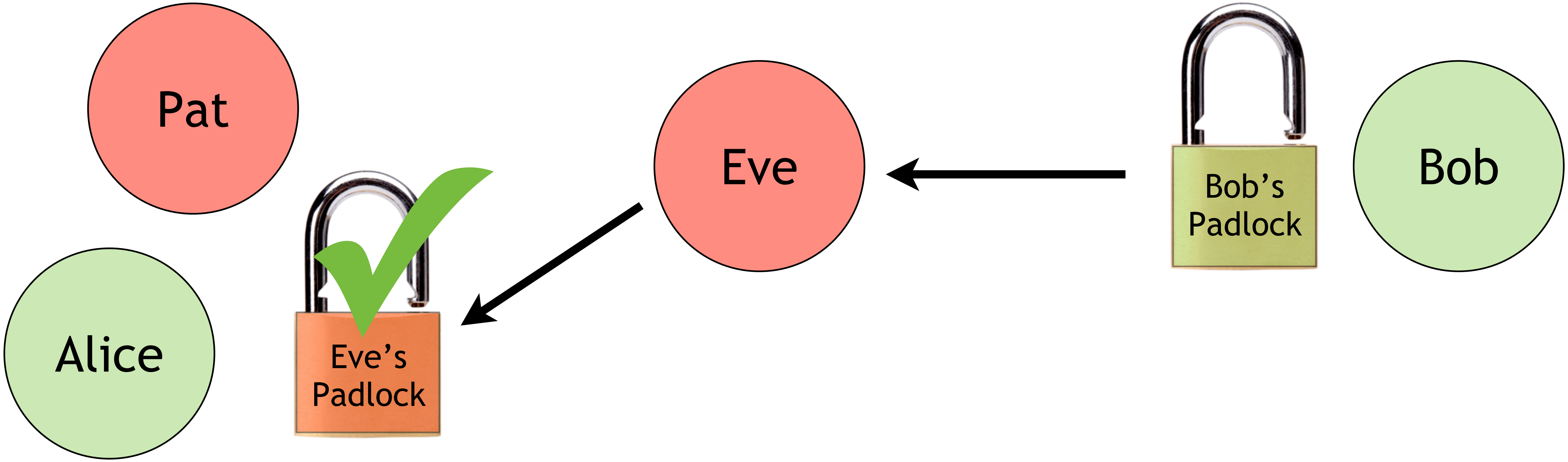
Alice will only use the lock if Pat can verify that it really belongs to Bob.



Who can you really trust?

Of course, this only works if Pat can be trusted not to be secretly working for Eve.

This is the essence of the problem with improperly implemented public key infrastructure. If the PKI is compromised, the whole system can fail catastrophically.



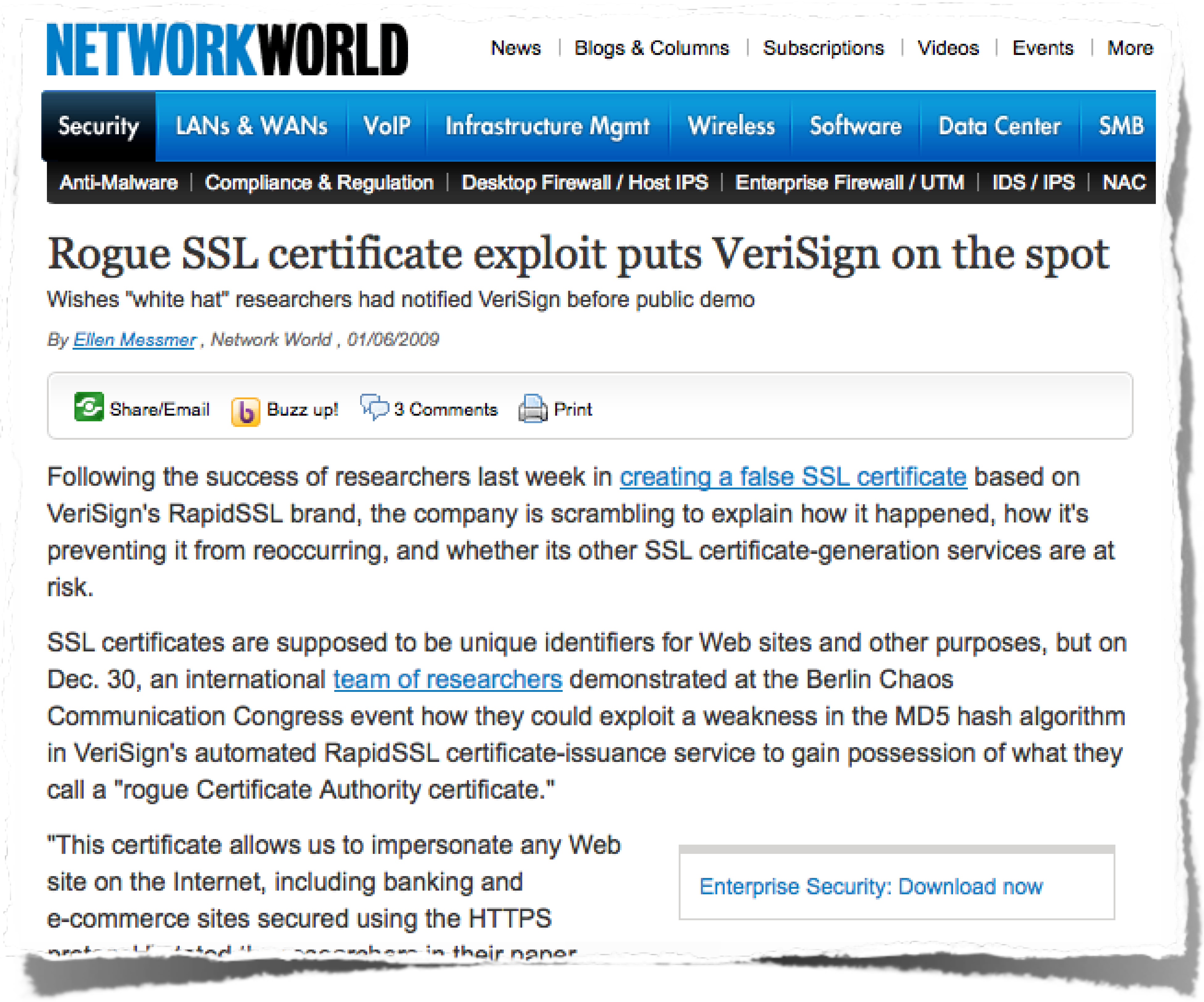
PKI failure: 2001

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
Share/Email
Buzz up!
3 Comments
Print
Enterprise Security: Download now

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

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 protocol," stated the researchers in their paper

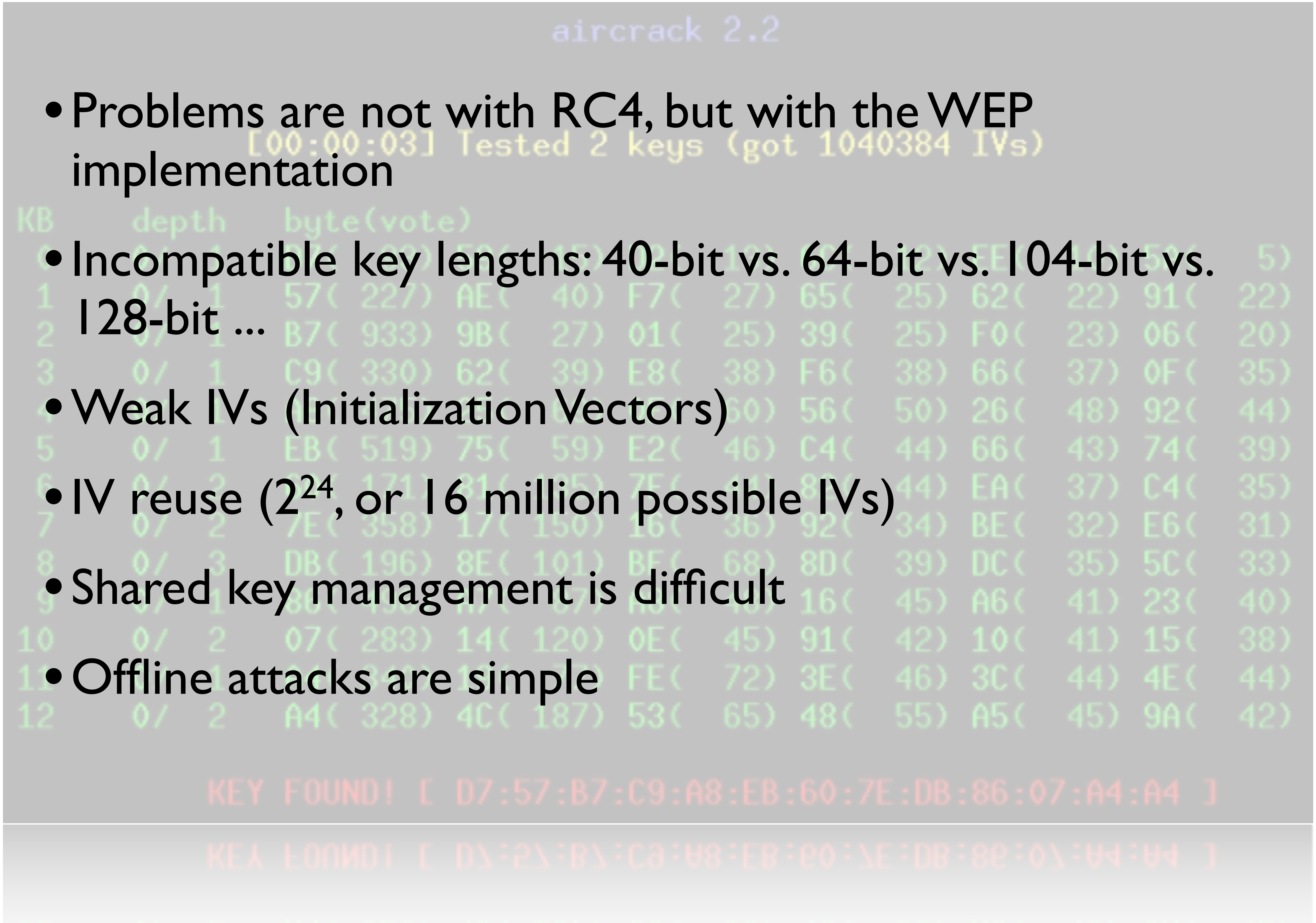
WEP Encryption

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.

WEP problems in detail



- Problems are not with RC4, but with the WEP implementation
- Incompatible key lengths: 40-bit vs. 64-bit vs. 104-bit vs. 128-bit ...
- Weak IVs (Initialization Vectors)
- IV reuse (2^{24}, or 16 million possible IVs)
- Shared key management is difficult
- Offline attacks are simple

```
                    aircrack 2.2

        [00:00:03] Tested 2 keys (got 1040384 IVs)

KB    depth   byte(vote)
 1    0/  1   57( 227) AE(  40) F7(  27) 65(  25) 62(  22) 91(  22)
 2            B7( 933) 9B(  27) 01(  25) 39(  25) F0(  23) 06(  20)
 3    0/  1   C9( 330) 62(  39) E8(  38) F6(  38) 66(  37) 0F(  35)
 5    0/  1   EB( 519) 75(  59) E2(  46) C4(  44) 66(  43) 74(  39)
 7    0/  2   7E( 358) 17( 150) 16(  36) 92(  34) BE(  32) E6(  31)
 8    0/  3   DB( 196) 8E( 101) BF(  68) 8D(  39) DC(  35) 5C(  33)
10    0/  2   07( 283) 14( 120) 0E(  45) 91(  42) 10(  41) 15(  38)
12    0/  2   A4( 328) 4C( 187) 53(  65) 48(  55) A5(  45) 9A(  42)

     KEY FOUND! [ D7:57:B7:C9:A8:EB:60:7E:DB:86:07:A4:A4 ]
```

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.

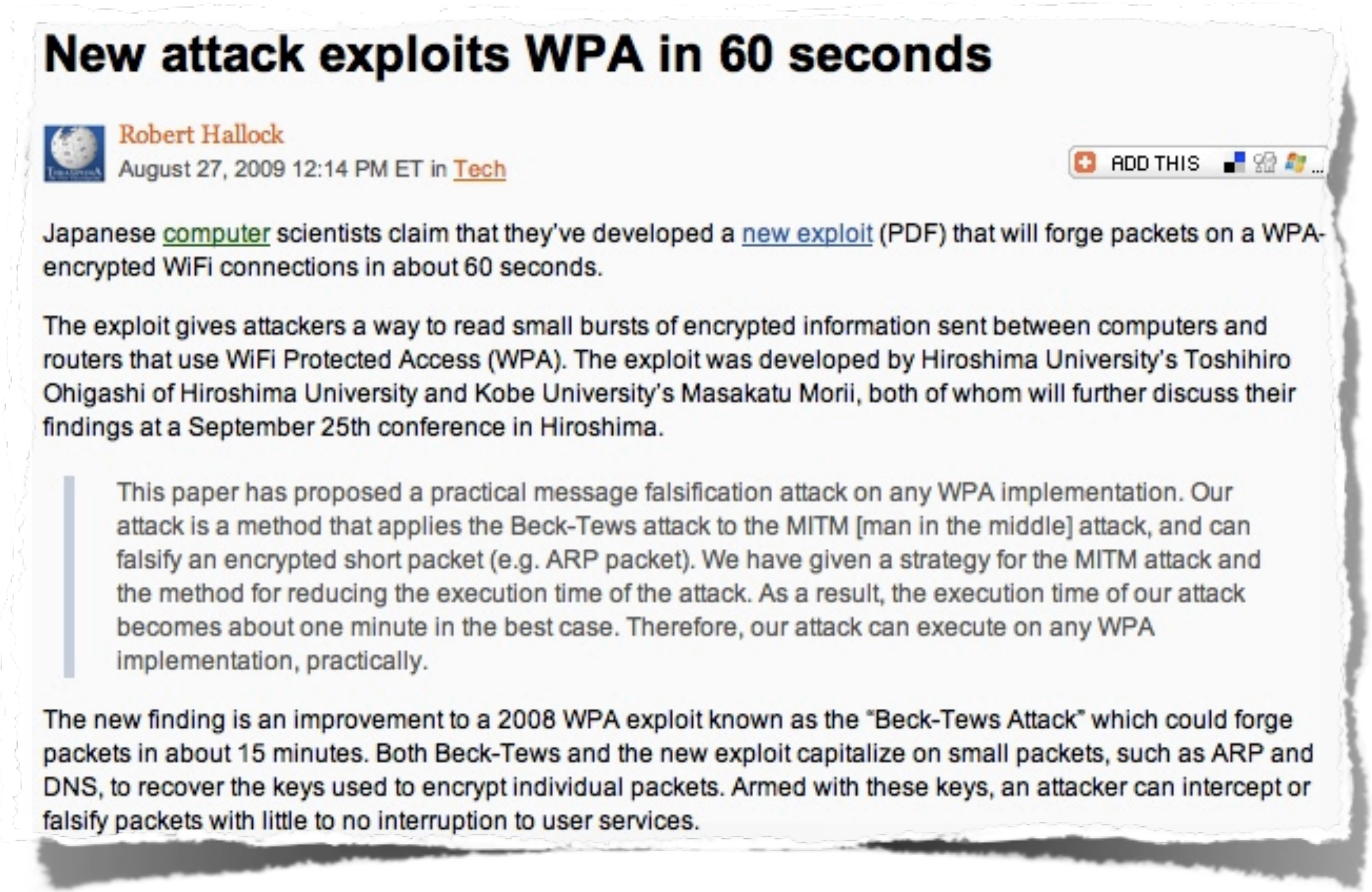
http://www.renderlab.net/projects/WPA-tables/

CHURCH OF WIFI

TIME TO PLAY

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

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

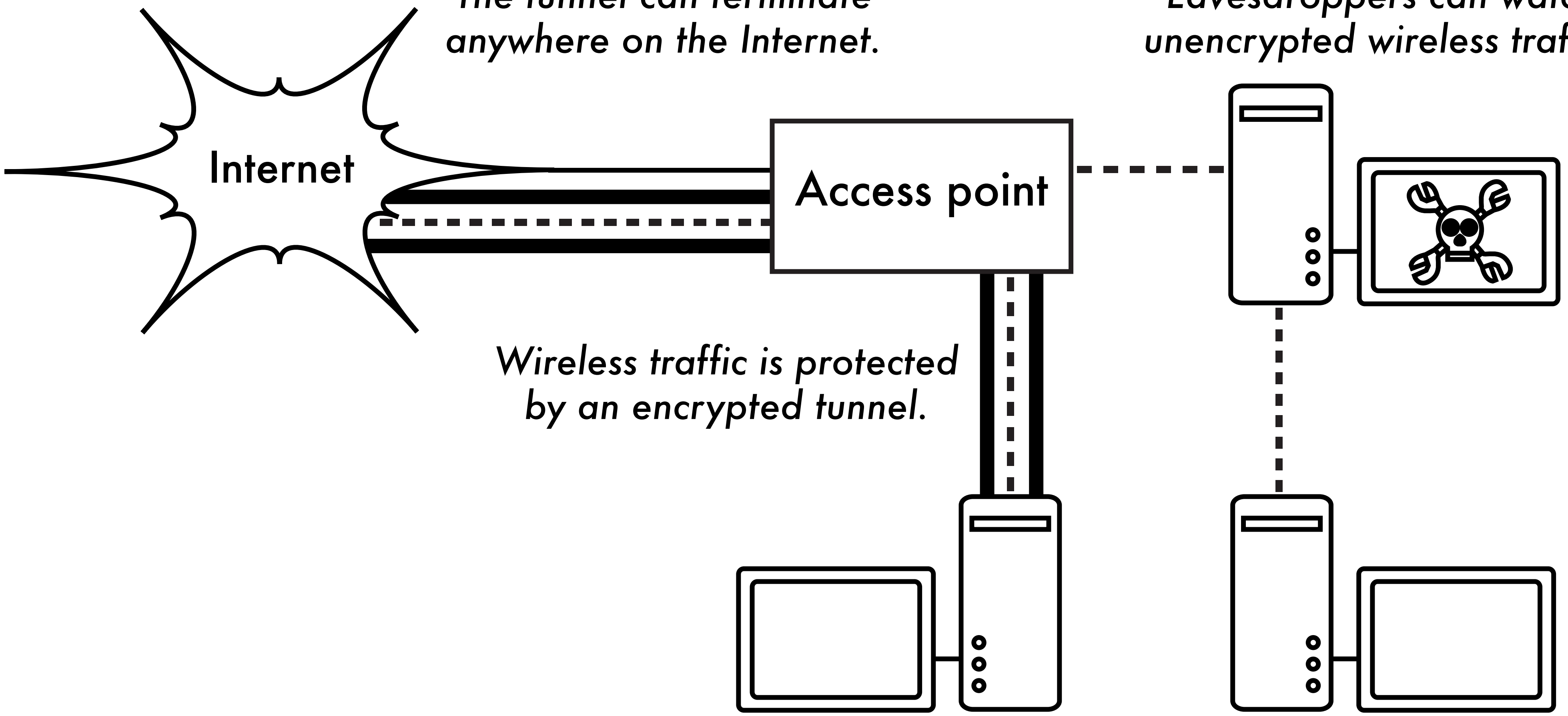
Good end-to-end security software should provide strong **Authentication**, **Encryption**, and **Key Management**.

Examples include:

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

Encrypted tunnels

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



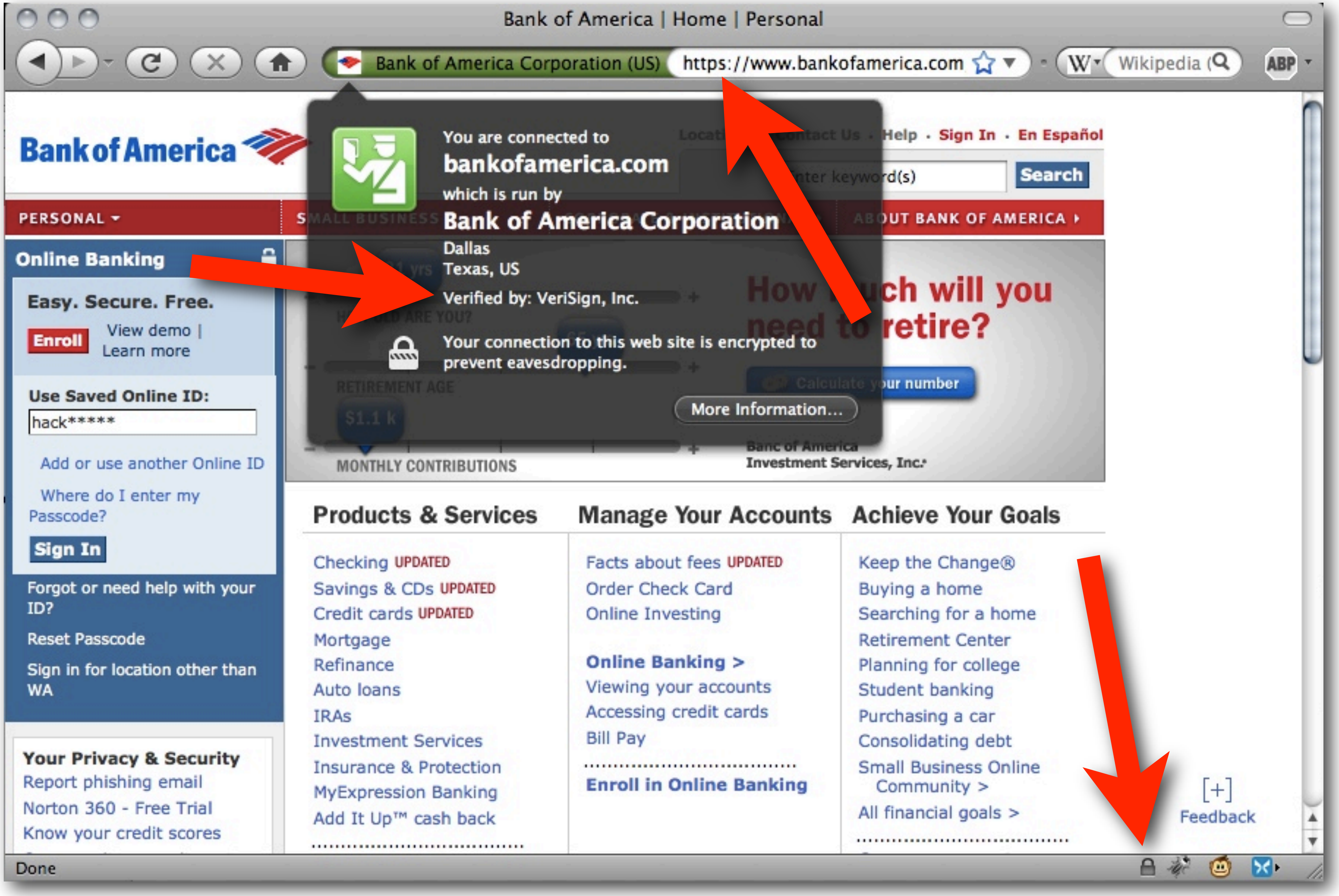
The tunnel can terminate anywhere on the Internet.

Eavesdroppers can watch unencrypted wireless traffic.

Wireless traffic is protected by an encrypted tunnel.

SSL encryption

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



Bank of America | Home | Personal
Bank of America Corporation (US)
https://www.bankofamerica.com
Wikipedia
ABP
Bank of America
Help · Sign In · En Español
Search
PERSONAL
ABOUT BANK OF AMERICA
Done

You are connected to
bankofamerica.com
which is run by
Bank of America Corporation
Dallas
Texas, US
Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

More Information...

Online Banking

Easy. Secure. Free.
Enroll View demo | Learn more

Use Saved Online ID:
hack*****

Add or use another Online ID
Where do I enter my Passcode?
Sign In

Forgot or need help with your ID?
Reset Passcode
Sign in for location other than WA

Your Privacy & Security
Report phishing email
Norton 360 - Free Trial
Know your credit scores

How much will you need to retire?
Calculate your number
MONTHLY CONTRIBUTIONS
RETIREMENT AGE
Banc of America Investment Services, Inc.

Products & Services
Checking UPDATED
Savings & CDs UPDATED
Credit cards UPDATED
Mortgage
Refinance
Auto loans
IRAs
Investment Services
Insurance & Protection
MyExpression Banking
Add It Up™ cash back

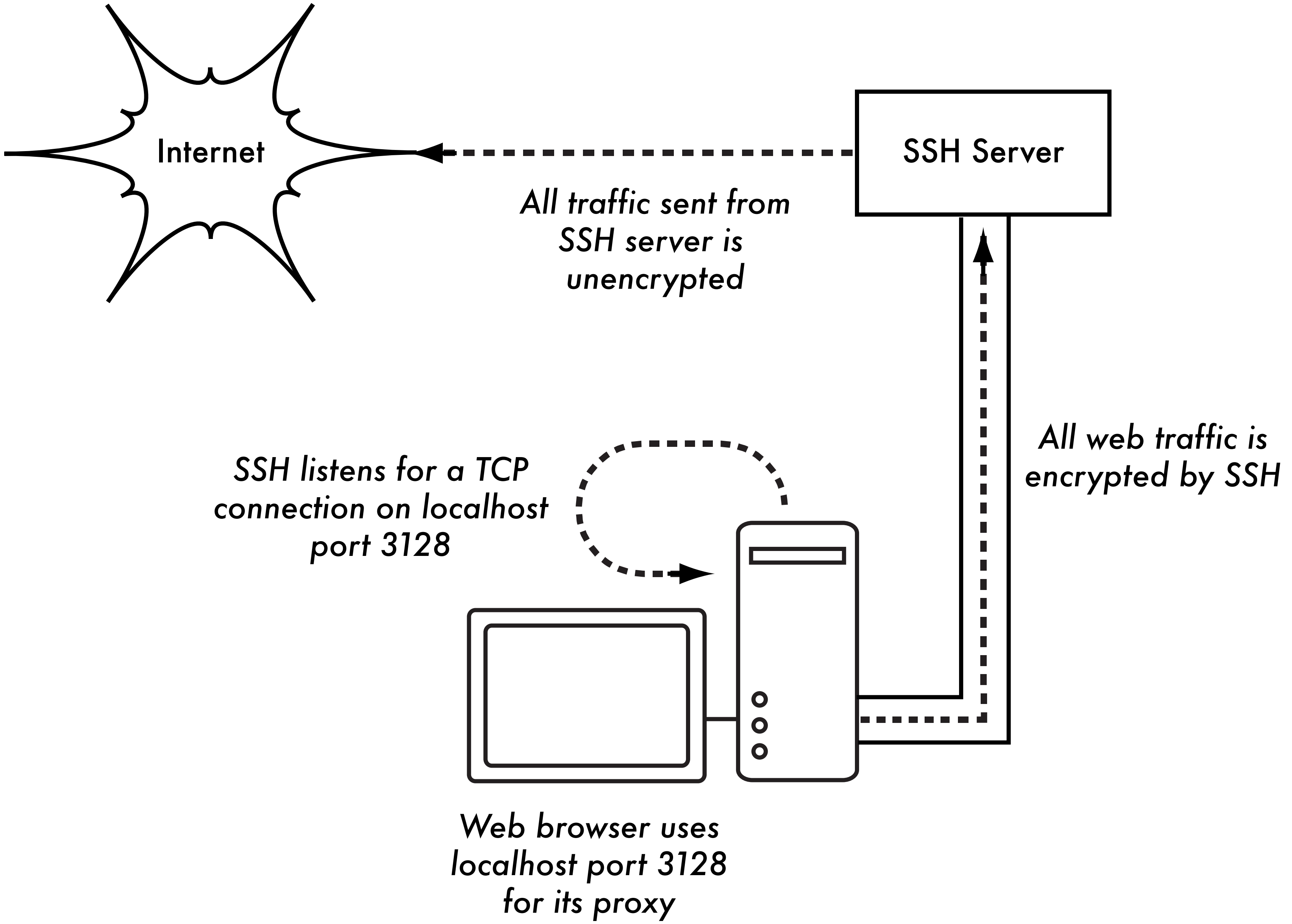
Manage Your Accounts
Facts about fees UPDATED
Order Check Card
Online Investing
Online Banking >
Viewing your accounts
Accessing credit cards
Bill Pay
Enroll in Online Banking

Achieve Your Goals
Keep the Change®
Buying a home
Searching for a home
Retirement Center
Planning for college
Student banking
Purchasing a car
Consolidating debt
Small Business Online Community >
All financial goals >

[+] Feedback

SSH tunnels

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

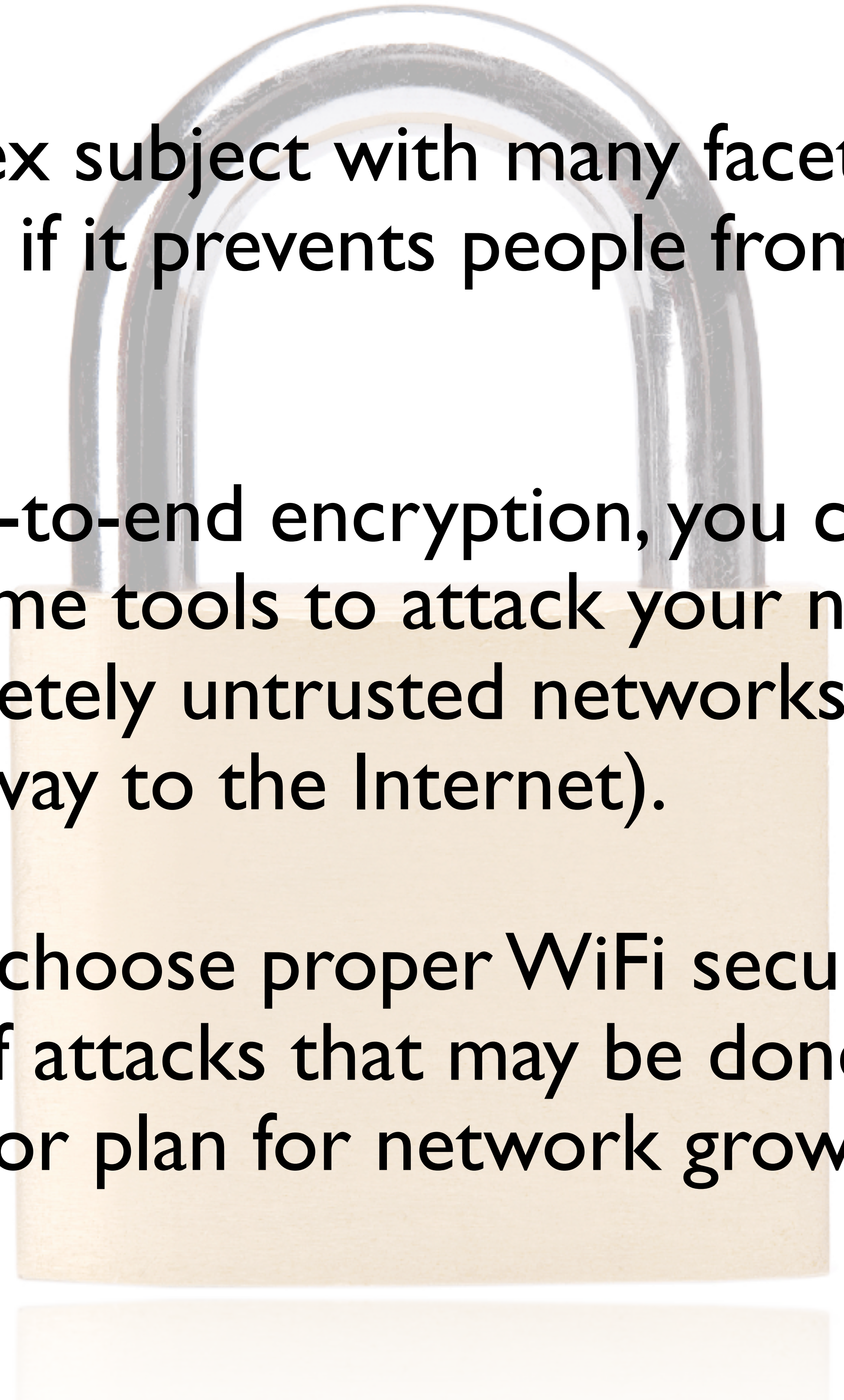

Internet
SSH Server
All traffic sent from SSH server is unencrypted
SSH listens for a TCP connection on localhost port 3128
All web traffic is encrypted by SSH
Web browser uses localhost port 3128 for its proxy

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!

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

WIRELESS
NETWORKING
IN THE DEVELOPING WORLD
SECOND EDITION
A practical guide to planning and building low-cost telecommunications infrastructure
wndw.net