

# Wireless Security



Maureen Njue  
Systems Administrator



*The Abdus Salam*  
**International Centre  
for Theoretical Physics**



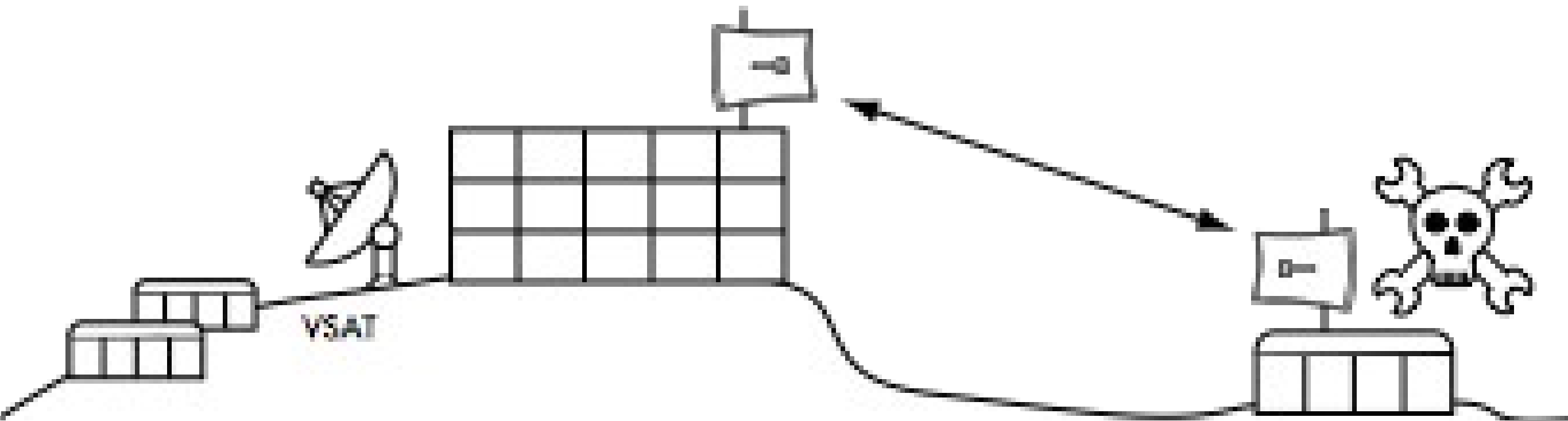
# Goals

- ▶ To understand which security issues are important to consider when designing WiFi networks
- ▶ To be introduced to encryption, how does it work, 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

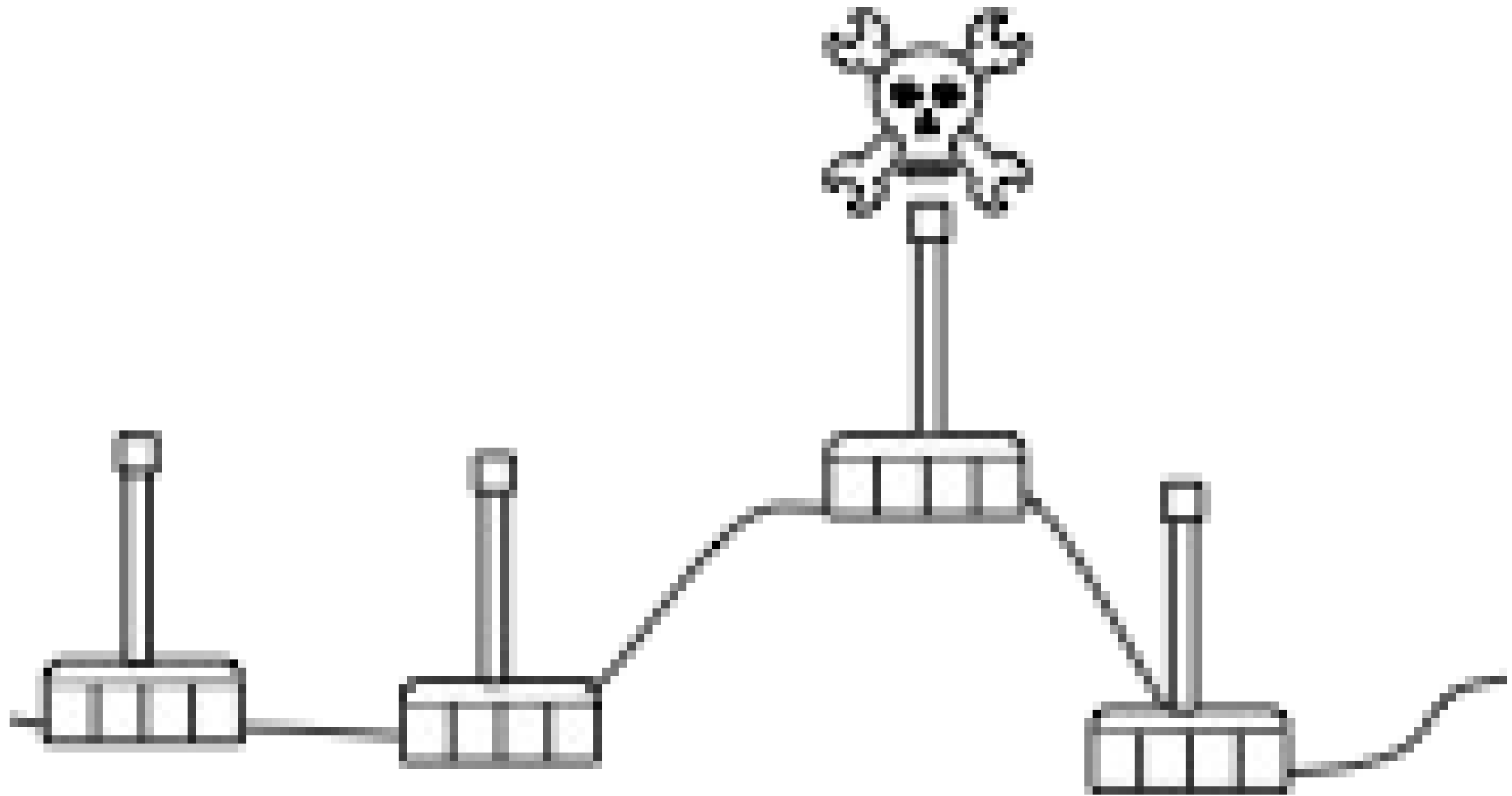
# Why is wireless security a problem?

- ▶ 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



Attacks may be completely undetectable.



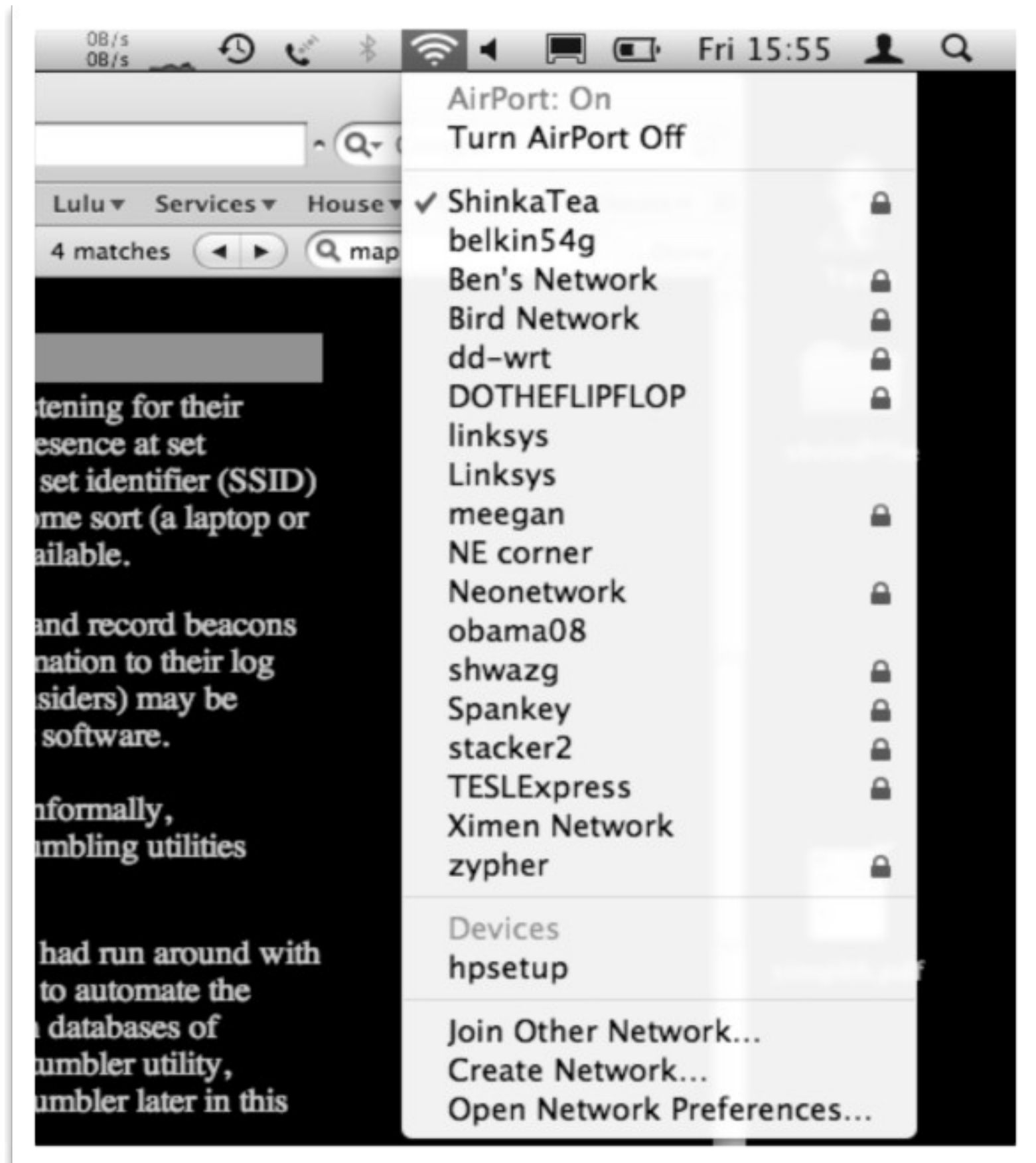
# Who creates security problems?

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

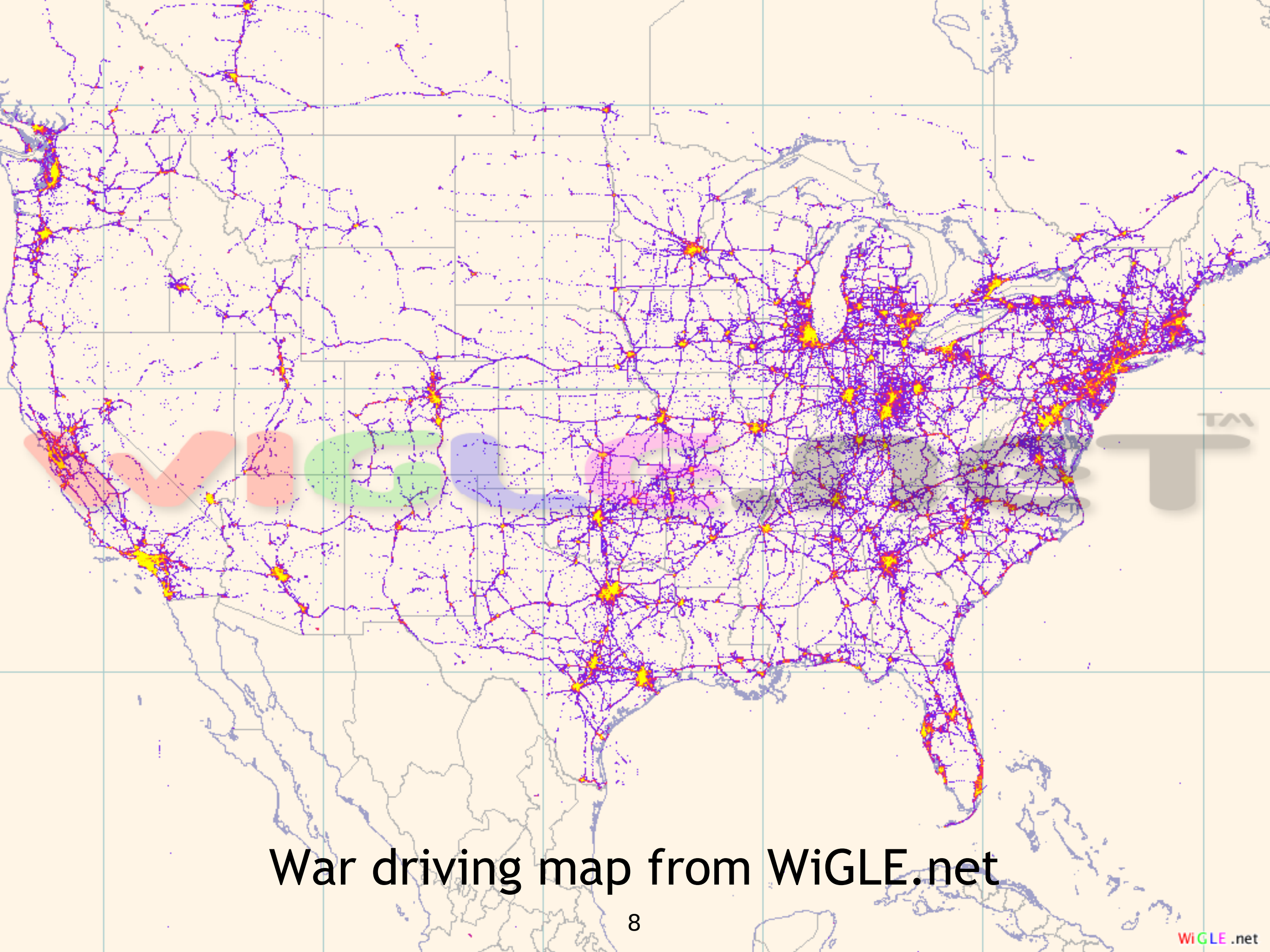
## ***Unintentional***

***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.







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.

```
Terminal
File Edit View Search Terminal Tabs Help
Terminal x Terminal x
Network List (Autofit)
Name      T W Ch  Packets  Flags  IP Range      Size
ACADEMIC  A N 001    1      0B     0.0.0.0
GUEST     A N 006    1      0B     0.0.0.0
. KSMS-HOUSES  A O 002    4      90B    0.0.0.0
. group-12  A O 011    7      0B     0.0.0.0
. group-11  A O 011    7      0B     0.0.0.0
! group-03  A O 001   12      0B     0.0.0.0
! GUEST    A N 001    8      0B     0.0.0.0
! group-16  A O 001   11      0B     0.0.0.0
! group-02  A O 001   11      0B     0.0.0.0
! STAFF    A N 001    6      0B     0.0.0.0
! group-15  A O 001   11      0B     0.0.0.0
! group-01  A O 001   10      0B     0.0.0.0
! ACADEMIC A N 001    9      0B     0.0.0.0
! group-14  A O 001   12      0B     0.0.0.0
! group-04  A O 001   10      0B     0.0.0.0
! group-13  A O 001   10      0B     0.0.0.0
! ACADEMIC A N 006   13      0B     0.0.0.0
! group-08  A O 006   16      0B     0.0.0.0
! group-07  A O 006   19      0B     0.0.0.0
! GUEST    A N 006   10     A4     172.16.3.144
! group-06  A O 006   16      0B     0.0.0.0
! STAFF    A N 006   15     A4     172.16.5.204
! group-05  A O 006   14      0B     0.0.0.0
! JFE Library A N 006    8     A4     192.168.1.59    156B
! group-10  A O 011   10      0B     0.0.0.0
! group-09  A O 011   12      0B     0.0.0.0
. STAFF    A N 006    1      0B     0.0.0.0
. ACADEMIC A N 006    1      0B     0.0.0.0
. KSMS RESIDENCE 4 A Y 011    1      0B     0.0.0.0
! RESIDENCE A N 002    1      0B     0.0.0.0

Info
Ntwrks    29
Pckets   451
Cryptd     1
Weak       0
Noise      0
Discrd     0
Pkts/s   108

area51
Ch: 4

Elapsd
00:00:06

Status
Connected to Kismet server version 2008.05.R1 build 20050815211952 on localhost:2501
Found new network "RESIDENCE" bssid 00:3A:9A:67:42:70 Crypt N Ch 2 @ 18.00 mbit

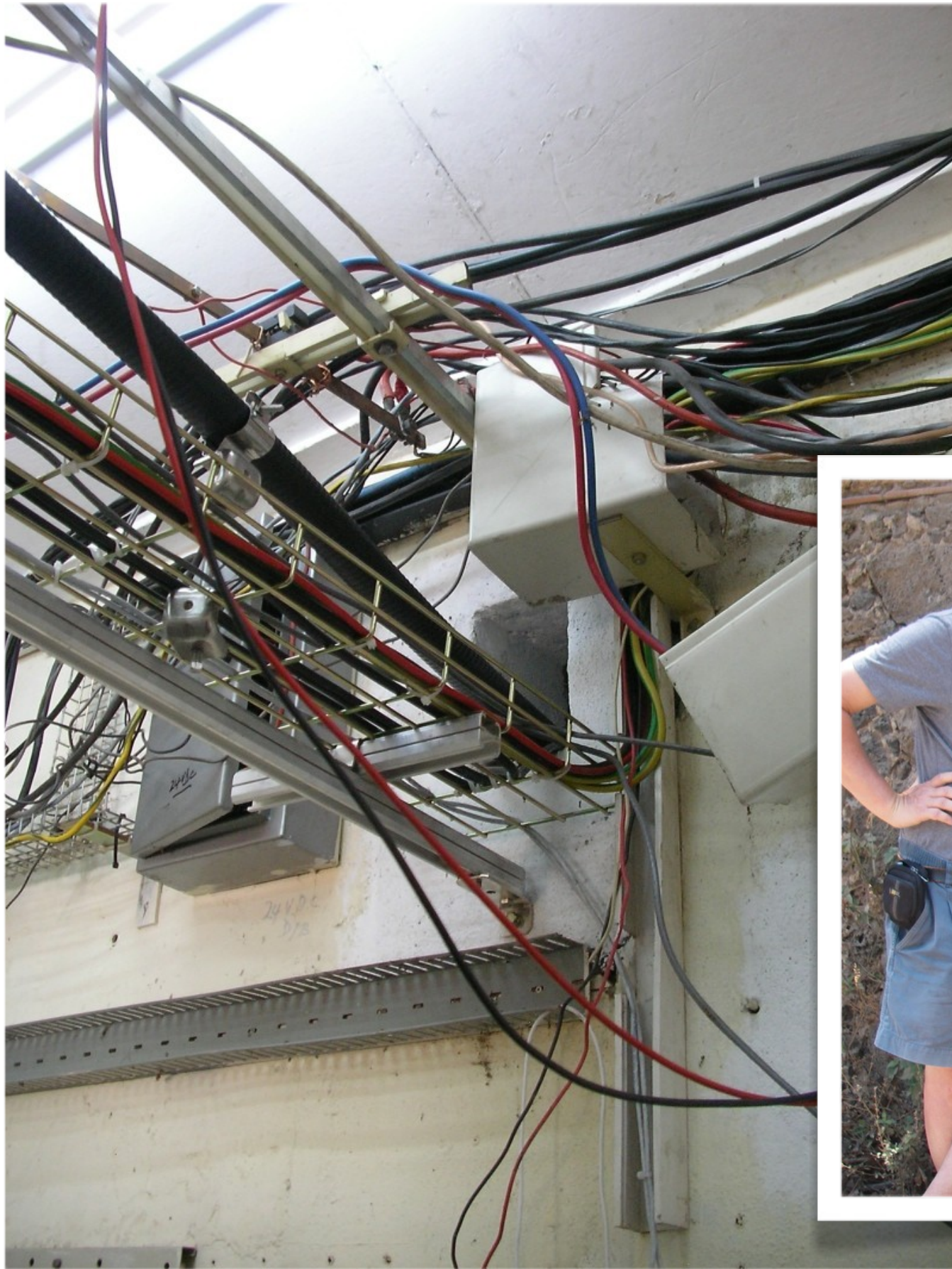
Battery: unavailable
Wi... Ter... fb... CC... S ... 20... [a... ca... KE... ub... ca... IC... Do... Tra... 14... 14... 6:55 PM
```

# 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 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/>)

# 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<sub>19</sub> 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/>*



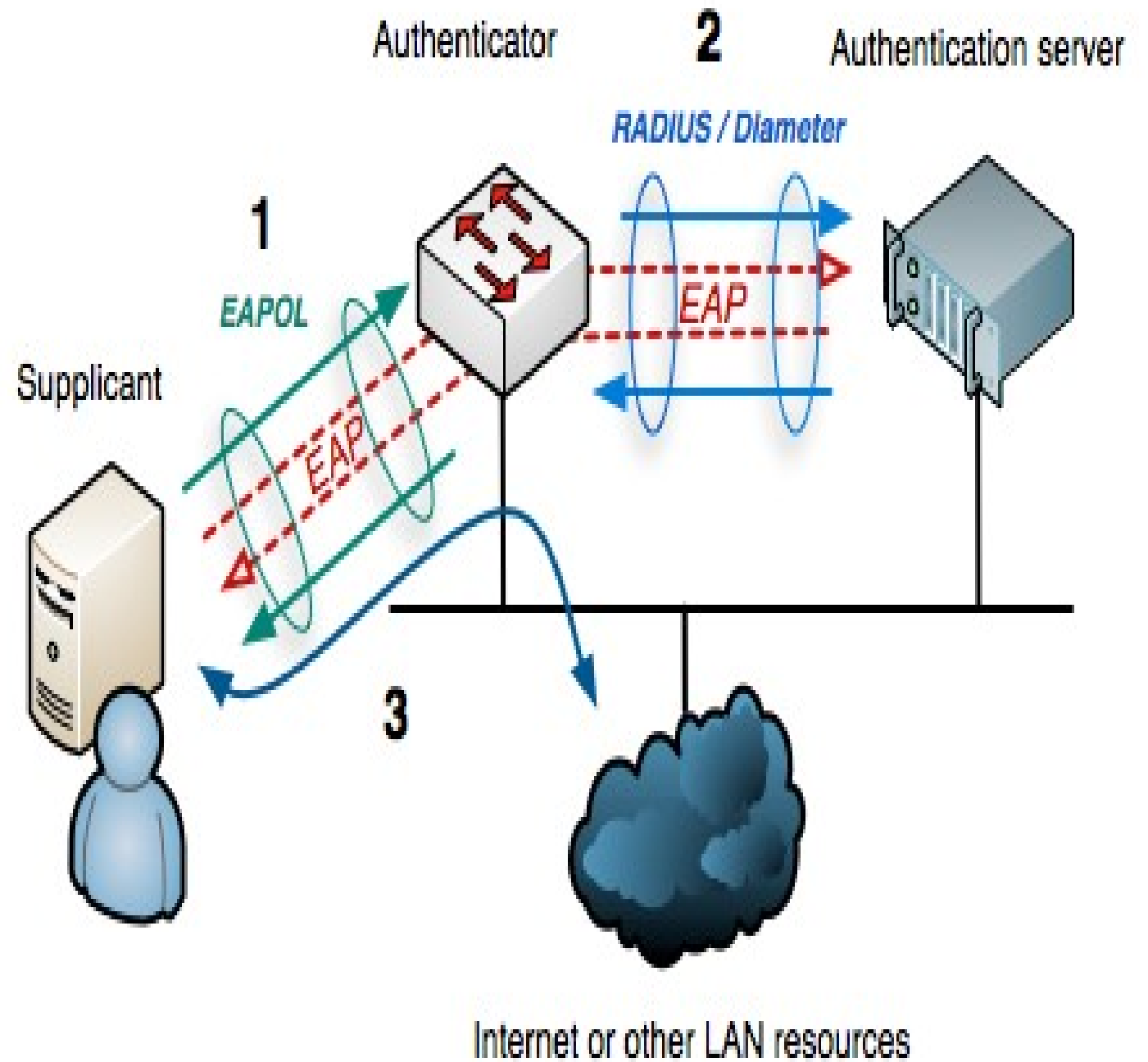
# IEEE02.1x Security

- Architectural Components
- Access Point features
- RADIUS
- Database Options
- Advantages
- Challenges

# Architectural Components

[http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)

- Database of Users
- Authentication server (Radius)
- Access Point(authenticator)
- Supplicant (module to authenticate)



# Access Point Features

- IEEE802.1x compatible

## **Additional features**

- VLAN Support
- Multiple SSID



# RADIUS

Remote Authentication Dial In User Service  
(RADIUS)

- RADIUS is a network protocol

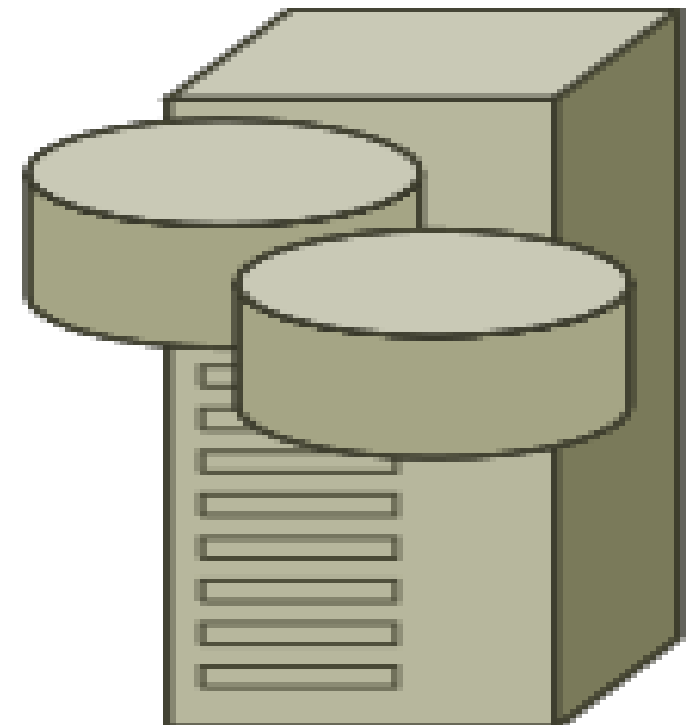
## **Functions**

- To authenticate users or devices before granting them access to a network,
- To authorize those users or devices for certain network services and
- To account for usage of those services.

## RADIUS Servers

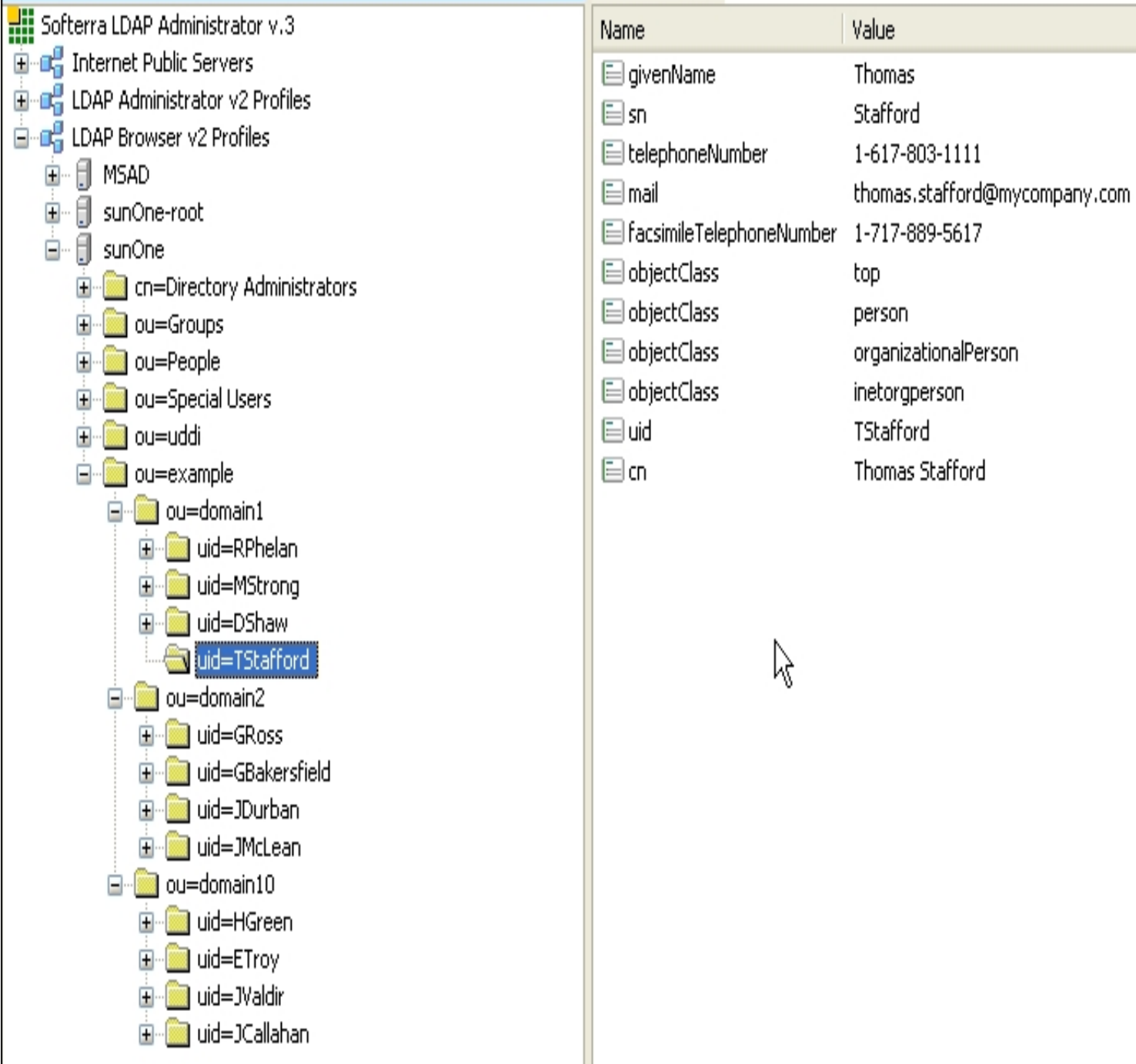
1.FreeRADIUS

2.Network Policy Server (Windows 2008,  
Windows 2012)



# Database Options

- LDAP
- SQL
- Active Directory
  - Text File
  - RADIUS



The screenshot displays the Softerra LDAP Administrator v.3 interface. On the left, a directory tree is shown with the following structure:

- Internet Public Servers
- LDAP Administrator v2 Profiles
- LDAP Browser v2 Profiles
- MSAD
- sunOne-root
  - sunOne
    - cn=Directory Administrators
    - ou=Groups
    - ou=People
    - ou=Special Users
    - ou=uddi
    - ou=example
      - ou=domain1
        - uid=RPhelan
        - uid=MStrong
        - uid=DShaw
        - uid=TStafford
      - ou=domain2
        - uid=GRoss
        - uid=GBakersfield
        - uid=JDurban
        - uid=JMcLean
      - ou=domain10
        - uid=HGreen
        - uid=ETroy
        - uid=JValdir
        - uid=JCallahan

The user 'uid=TStafford' is selected, and the details are shown in the table on the right:

Name	Value
givenName	Thomas
sn	Stafford
telephoneNumber	1-617-803-1111
mail	thomas.stafford@mycompany.com
facsimileTelephoneNumber	1-717-889-5617
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	inetorgperson
uid	TStafford
cn	Thomas Stafford



# Advantages of database Authentication

- Centralized management
  - Enhanced security
  - Detailed logs
- Scalable architecture
  - RADIUS open protocol

ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload (Bytes)	Download (Bytes)	Termination	NAS IP Address
11267		1022859@cuea.ac.ke	172.21.0.37	2013-07-01 00:18:40	2013-07-01 00:33:02	14 minutes, 22 seconds	104.02 Kb	19.17 Kb	Idle-Timeout	172.21.0.2
11268		1022859@cuea.ac.ke	172.21.0.131	2013-07-01 00:59	2013-07-01 01:00:59	58 seconds	24.08 Kb	6.71 Kb	User-Request	172.21.0.2
11269		1020469@cuea.ac.ke	172.21.0.131	2013-07-01 00:41	2013-07-01 00:47:41	6 minutes, 7 seconds	2.9 Kb	1.79 Kb	Idle-Timeout	172.21.0.2
11270		1022859@cuea.ac.ke	172.21.0.131	2013-07-01 00:37	2013-07-01 00:40:37	3 minutes, 1 seconds	239.64 Kb	664.94 Kb	User-Request	172.21.0.2
11271		1022859@cuea.ac.ke	172.21.0.37	2013-07-01 03:29:08	2013-07-01 03:34:38	5 minutes, 30 seconds	48.12 Kb	26.38 Kb	Idle-Timeout	172.21.0.2
11272		1022859@cuea.ac.ke	172.21.0.37	2013-07-01 04:46:56	2013-07-01 04:52:07	5 minutes, 11 seconds	11.56 Kb	2.4 Kb	Idle-Timeout	172.21.0.2
11273		1021768@cuea.ac.ke	172.21.0.131	2013-07-01 05:21:56	2013-07-01 07:05:49	1 hours, 43 minutes, 53 seconds	2.01 Mb	3.96 Mb	Idle-Timeout	172.21.0.2

[Edit User](#)

Upload: **1.11 Gb**  
Download: **4.78 Gb**

[Close](#) | [Don't show this message again](#)

# Challenges

- Updating database with current details

# 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/>*

