School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko
Cybersecurity Fundamentals

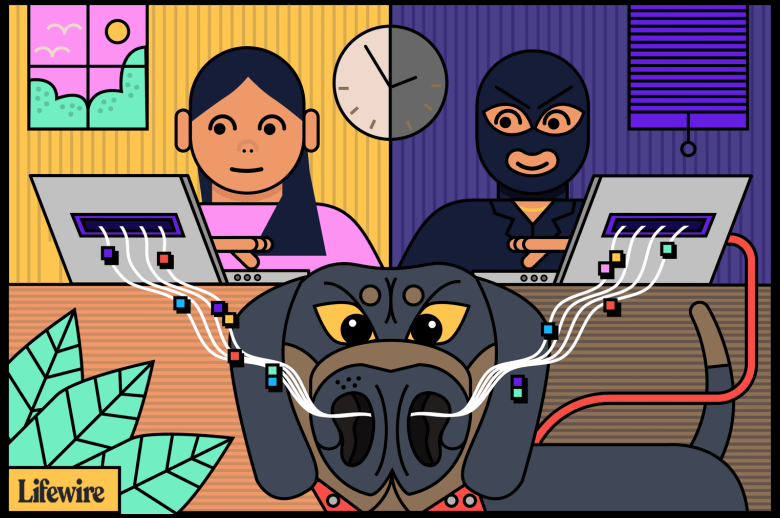
Why is the Internet insecure?

Examples of network vulnerabilities

Learning goals

- Use an example of **wireless networks** and **websites** to illustrate attacks on **confidentiality**, **integrity**, **authenticity** and **availability**
  - Packet sniffing attack
  - Securing wireless networks
  - The problem with ***free wifi***
  - HTTPS
  - Deauthorisation (deauth) attack

PART I:
Packet sniffing attacks

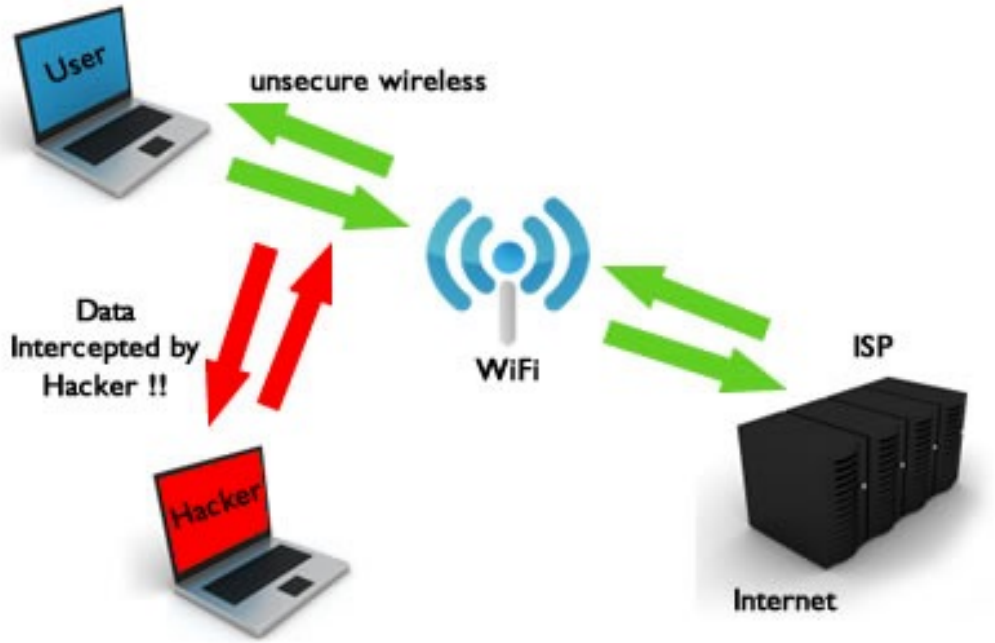


Wireless networks

- Wireless internet = **wifi**
- Most people use wifi, and it is **quite vulnerable**.
- Connect devices to a **single** local area network (LAN)
- The standard defined by IEEE is called **802.11 family** (variants 802.11**b**, 802.11**g**, 802.11**n** etc.)
- Each device is a **station** (like a radio station)
- Each wireless **access point** advertises a service set identifier(**SSID**)
- Example: Victoria, cbdfree etc.

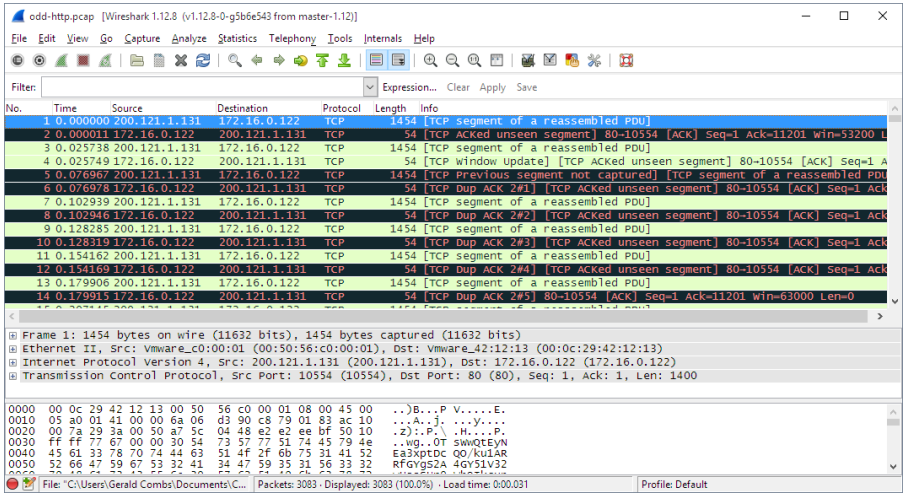
Who is listening to it? Packet sniffing

- Wireless networks are similar to the **bus topology**, anyone connected to the wi-fi access point **can see traffic sent to all other computers** connected to the same access point.



Local attacks: Packet sniffing

- The attacker joins LAN
- Uses a packet sniffer
- **Packet sniffing** = view all the packets crossing the network.
- **Wireshark** is a popular tool.
- Connect network adapter in "**promiscuous mode**": view every packet, even those *not intended for your computer*.



PART II:
Securing Wireless Networks

Securing wireless networks

- Can we **ensure** that only people who are **authorised** **can connect** to our wifi network?
- Can we **prevent** **unauthorised** people from **sniffing** the traffic sent on the wifi network?
- Aim is to be ***similar to a switched-wired network*** in terms of security.

Wired Equivalent Privacy (WEP)

- Wired equivalent privacy (WEP) in **1997**.
- Requires 10 or 26 hexadecimal key (characters).
- Security relied upon **never repeating** a seed used in the encryption (24-bit = 3 characters)
- On a busy network, **repetition happens**, essentially **same key is reused** again and again.
- An attacker can break the key in **a few minutes**, and as all communication sent using the same key so all traffic is open to the attacker on the network.

Wi-fi Protected Access 2 (WPA2)

- Wi-Fi protected access 2 since **2006**.
- WPA used a ***weaker*** encryption scheme, WPA2 uses **AES**.
- A **pre-shared key** is used for users to join the WiFi network.
- Key length **starts at** 64 hexadecimal digits
- It can be **longer** to help slow down **brute force attacks**.
- Each client gets their **own fresh encryption key** based upon the **pre-shared key**. This is used to protect its communications.

Wi-fi Protected Access 2 (WPA2)

- Assume the attacker **knows** the **pre-shared key**.
- Can join the network as a client.
- Cannot see the traffic to and from other clients because of the use of ***unique encryption keys***.
- The attacker is **prevented** from sniffing.

Cracking WPA2 networks

- While a **new client** joins the network, it is **vulnerable**.
- The attacker has to be **on the same network** and **captures messages** containing passwords exchanged while **authenticating**.
- Can force this to happen ("**deauth**").
- Brute force encryption key.

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/

Uhoh! KRACK attack

- Computer scientists from Belgium (KU Leuven) found a **vulnerability** in October 2017.
- The **KRACK** attack allows attackers to force the victim to use a **pre-used key** known by the attacker.
  https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/
- This affected Android, iOS and others (but not **Microsoft** because they never followed the standard!).
- **Good news**. As long as the client is **patched**, you should be okay.

PART III:

The problem with free WiFi

But problems persist

- WPA2 is secure against sniffing even if the attacker has the password for the network **but**…

- Problems remain:
  - Free wifi points (no password, just connect)
  - Free wifi plus **captive portals** (provide access control but all communications **unencrypted**)
  - Rogue wifi points and **evil twins** (look legitimate but are under control of an attacker)

Free wifi

- Capture portal used, no use of WPA2.
- Allows access control on a per user basis.
- **No encryption** to protect customers.

Evil twins

https://memory-alpha.fandom.com/wiki/Michael_Burnham

https://memory-alpha.fandom.com/wiki/Michael_Burnham_(mirror)

Rogue access points and evil twins

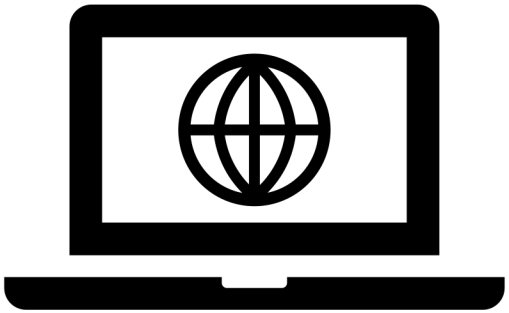
- https://www.youtube.com/watch?v=1luFsGbTUm0
- Rogue access point connected to wired network.
- Evil twin attack: access point configured to have same name as a legitimate one.
- User connects to evil twin, all communication now under control of the evil twin.
- Can be basis of a man-in-the-middle attack.

Evil Twin Attack

Access Point

Evil Twin Access Point Under control of the attacker

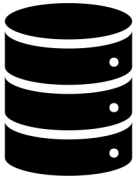
Same **SSID** for both
e.g.WellingtonUniversity



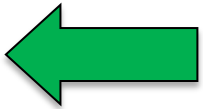
Confused user, tricked into connecting with the attacker's access point

Evil Twin: Monster-in-the-Middle (MiTM)

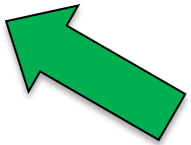
User **thinks** they are connecting to **bank.com**

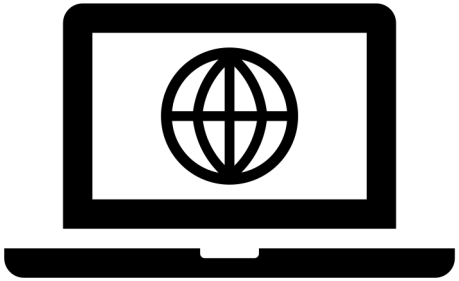


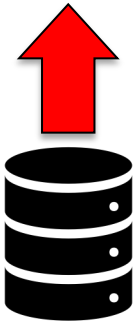
bank.com



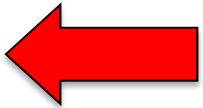
Access Point



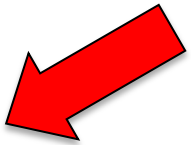




evilbank.com



Evil Twin
Access Point

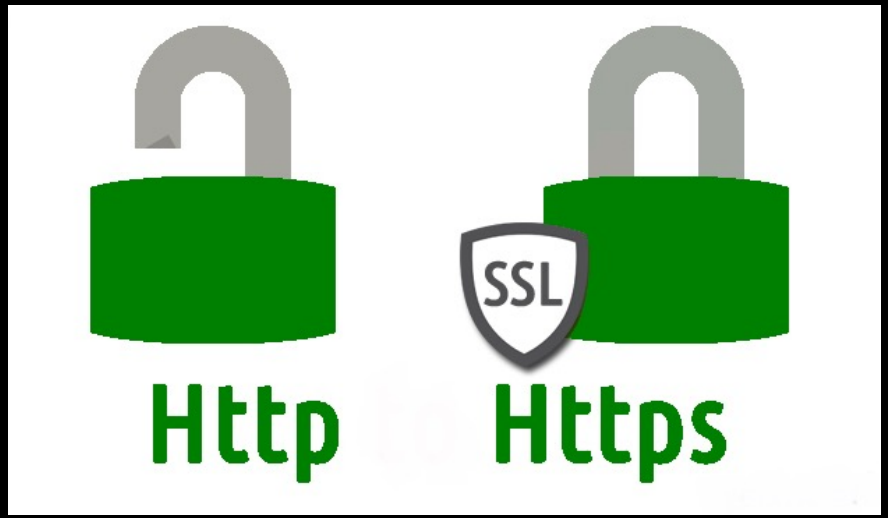


Confused user, tricked into connecting with the attacker's access point

User **actually** they are connecting to **evilbank.com**

PART IV:

HTTPS Hypertext Transport Protocol Secure



Solution: HTTPS revisited

- HTTP = Hypertext Transport Protocol
- HTTP**S** = Hypertext Transport Protocol **Secure** from **1994**
- Data is secured using **Secure Socket Layer** (**SSL**) or **transport layer security** (TLS) protocol.
- HTTP messages are **automatically** encrypted and decrypted for you.
- Uses the **public key** belonging to the website to establish a **secure connection**.

Netscape navigator 1.22

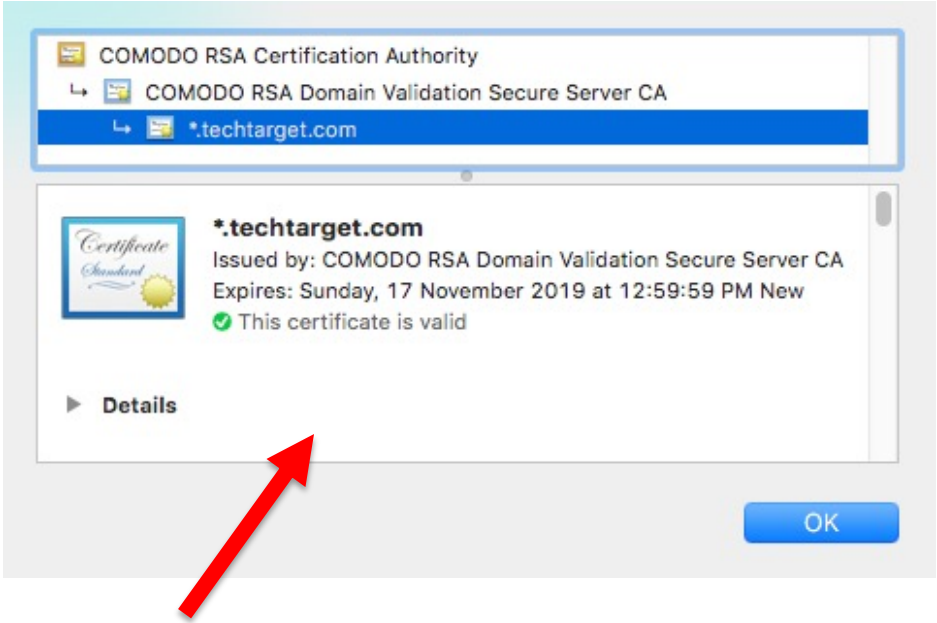
Digital certificates

- Used to support the **distribution** of **public keys**.
- **Contains**:
  - Owner's distinguished name (e.g. organisation).
  - Owner's public key (to be used for setting up the secure communications).
  - Issuer's distinguished name (e.g. certification authority that issued the certificate and has verified that you own the domain name).
  - Issuer's digital signature (hash of the whole certificate encrypted using the issuer's private key).

Example: Digital Certificates

Structure of a digital certificate (also called *SSL certificate*).

Standardised around **1998** as X.509 Public key certificates



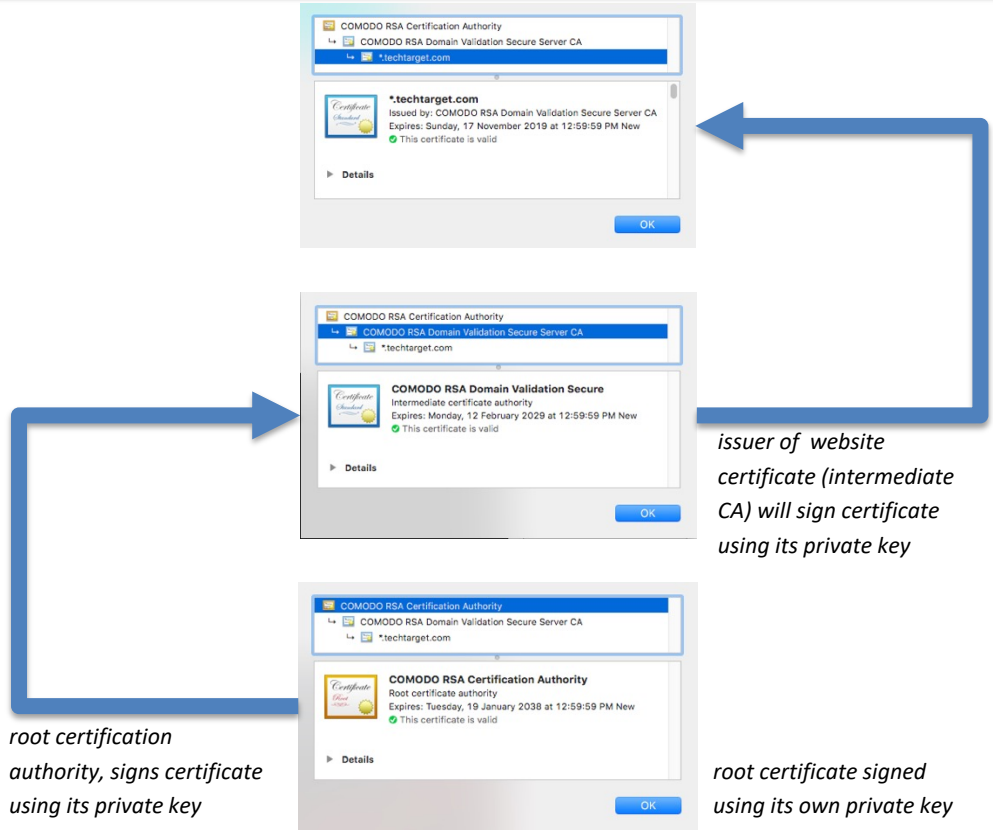
Certificate returned when visiting https://www.techtarget.com

Contained public key used to setup encrypted communication with my browser and website with domain name ending in techtarget.com (**note the * above is a wildcard**)

Chain of trust

We establish **trust** in the certificate by following a chain back to the ***root certification authority*** (***CA***).

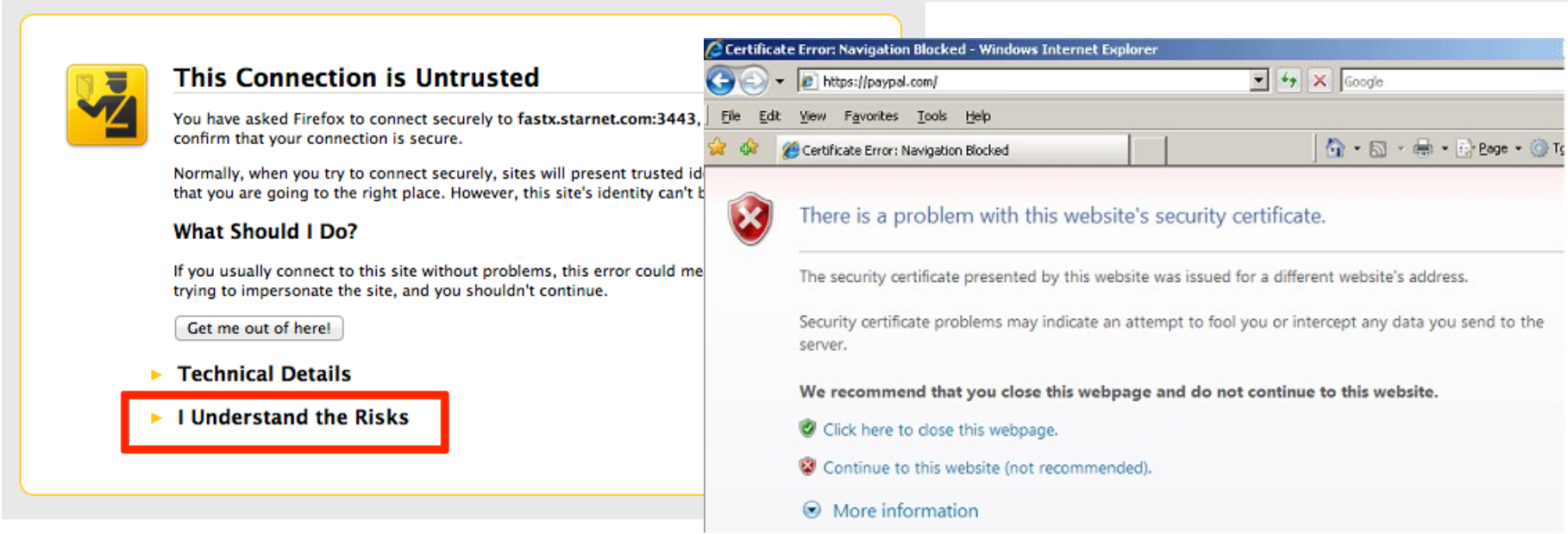
Verify chain is not broken by verifying the signature at each stage.



Trusted X.509 public key certificates

- Each browser has a set of **pre-installed** trusted **Certificate Authority** certificates.
- These are **pre-approved** as being valid, and any certificate signed by them is **treated as trusted**.
- The assumption is that they would not be in the browser **unless** they are **valid certificates** (can't validate any other way if it is a self-signed certificate).
- For example: Firefox:
  https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport

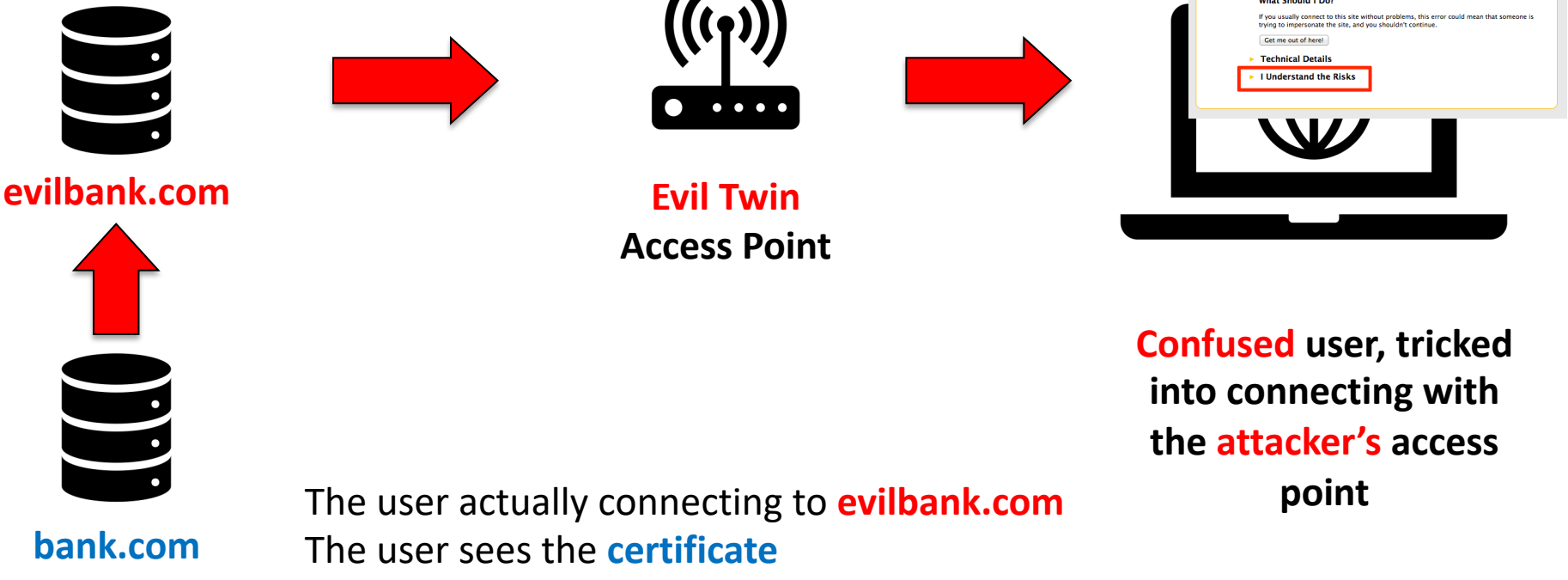
So what happens when a certificate is *invalid*?



- Either an unsigned or **self-signed** certificate (Let's Encrypt) or attackers try to **fake** the certificate (**so the signature fails**)
- Problem is that it could be **an attack**, or it might just be a **badly configured server**
- In either case, perhaps better ***not to trust*** unless you have no other choice.

Evil Twin: Monster-in-the-Middle (MiTM)

Attacker is using HTTPS and their **own unsigned** certificate



Confused user, tricked into connecting with the **attacker's** access point

The user actually connecting to **evilbank.com**
The user sees the **certificate**

Problem: Attacker issues own certificate in name of the real website

- The **private** key got disclosed and is **valid** until **2039**, anyone with the private key could now ***forge a valid certificate*** for a website

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=703ed9d1-6c3b-42cf-b64e-ea4a697d1784&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://www.cisa.gov/news-events/alerts/2015/11/24/dell-computers-contain-ca-root-certificate-vulnerability

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About | REPORT A CYBER ISSUE

Home / News & Events / Cybersecurity Advisories / Alert

SHARE:

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ALERT

Dell Computers Contain CA Root Certificate Vulnerability

Last Revised: November 27, 2015

Dell personal computers using the preinstalled certificate authority (CA) root certificate (eDellRoot) contain a critical vulnerability. Exploitation of the vulnerability could allow a remote attacker to read encrypted web browser traffic (HTTPS), impersonate (spoof) any website, or perform other attacks on the affected system.

The eDellRoot certificate originated from an update to the Dell Foundation Services (DFS) application on August 18, 2015. As of November 23, that update is no longer being provided. The certificate was also preinstalled on some systems November 20–23, 2015. Dell is pushing a DFS software update to remove the vulnerable certificate from affected systems.

US-CERT encourages users and administrators to review Vulnerability Note VU#870761 and Dell's blog post for more information and guidance on removing the certificate.

Problem: Fraudulently issued certificates

- Certification authorities are **supposed to check** that you are the person or ***own*** the website that you claim you own… sometimes they get it wrong.

CERT Coordination Center

Home | Notes | Search | Report a Vulnerability | Disclos

Home › Notes › VU#869360

Unauthentic "Microsoft Corporation" certificates issued by Verisign to an unidentifed person

Vulnerability Note VU#869360

Original Release Date: 2001-03-27 | Last Revised: 2001-03-31

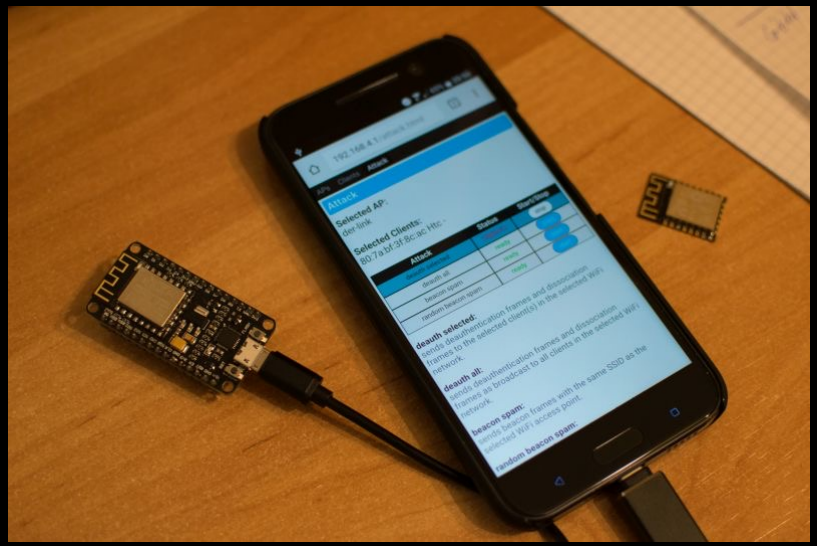
Overview

On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. Although users who try to run code signed with these certificates will generally be presented with a warning dialog, there will not be any obvious reason to believe that the certificate is not authentic.

Description

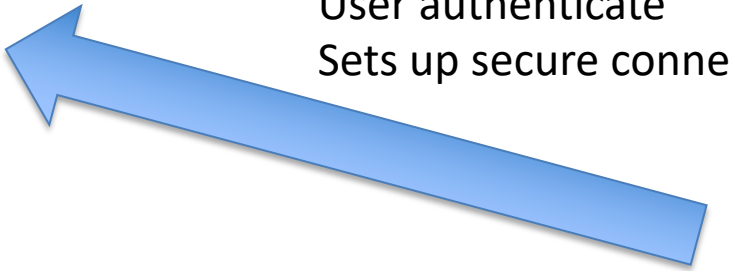
Microsoft released a security bulletin on March 22, 2001, describing two certificates issued by VeriSign to an individual fraudulently claiming to be an employee of Microsoft. The full text of Microsoft's security bulletin is available from their web site at

PART V:
Deauthorisation attack

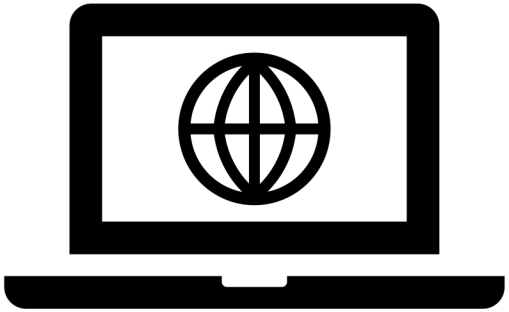


Deauth (Deauthorisation) Attack

Access Point



User authenticate
Sets up secure connection



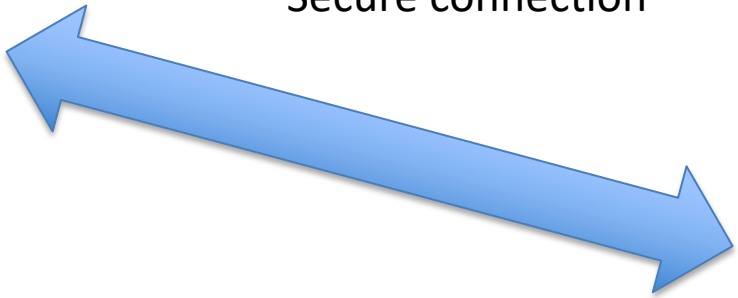
A user connecting with the access point

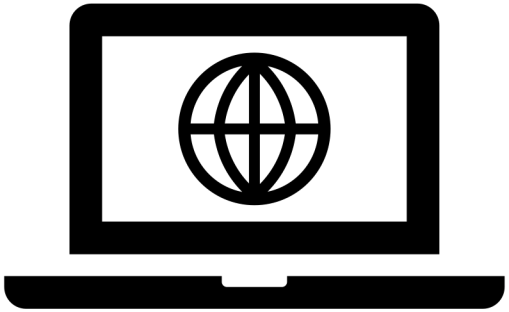
Attacker

Deauth (Deauthorisation) Attack

Access Point

Secure connection

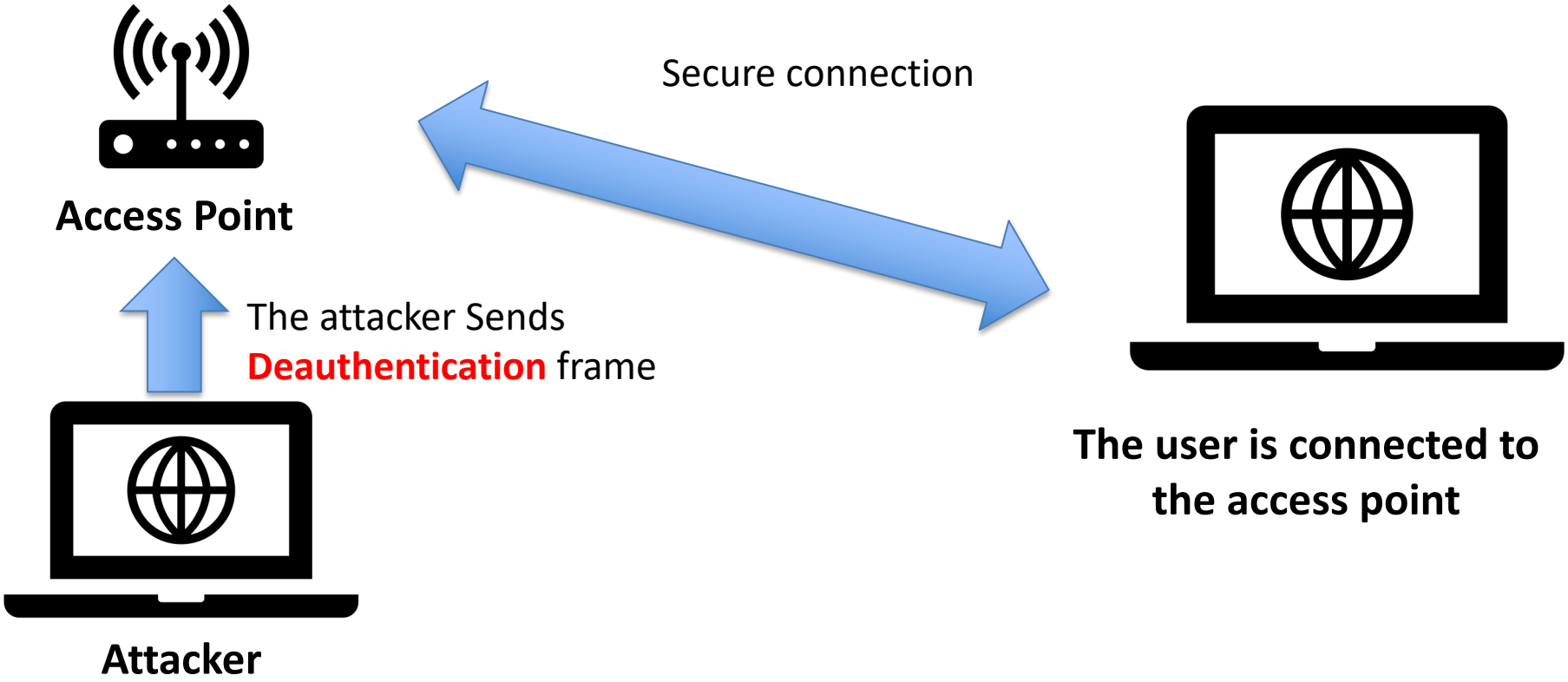




The user is connected to the access point

Attacker

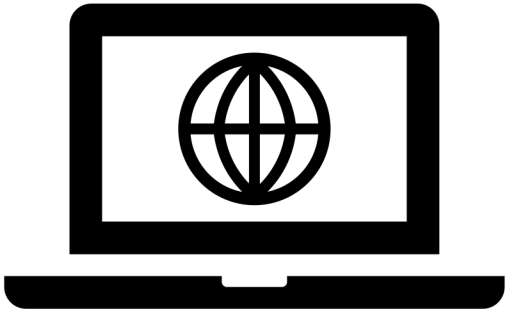
Deauth (Deauthorisation) Attack



Deauth (Deauthorisation) Attack

Access Point

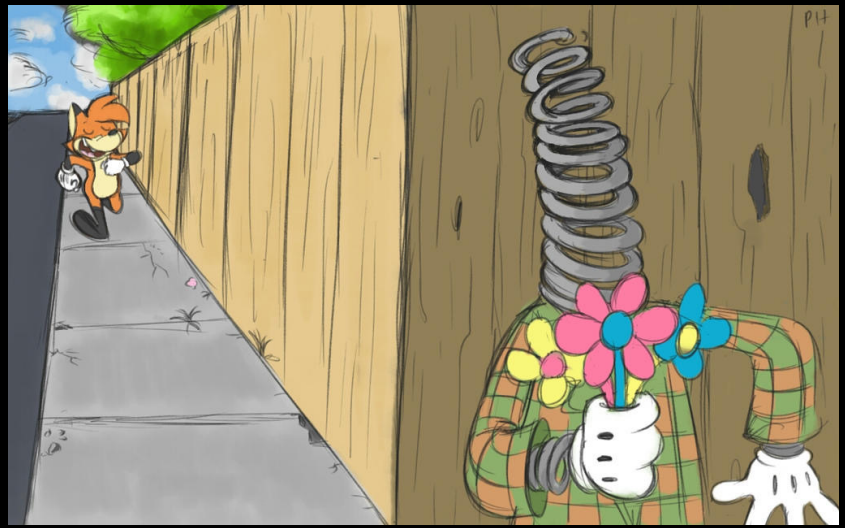
Connection broken and data lost between user and access point



The user lost connection with the access point

Attacker

PART V:
What’s next



What's up next

- The break!! After you hand in assignment 1.
- Lisa is taking over lecturing second half (apart from week 7).