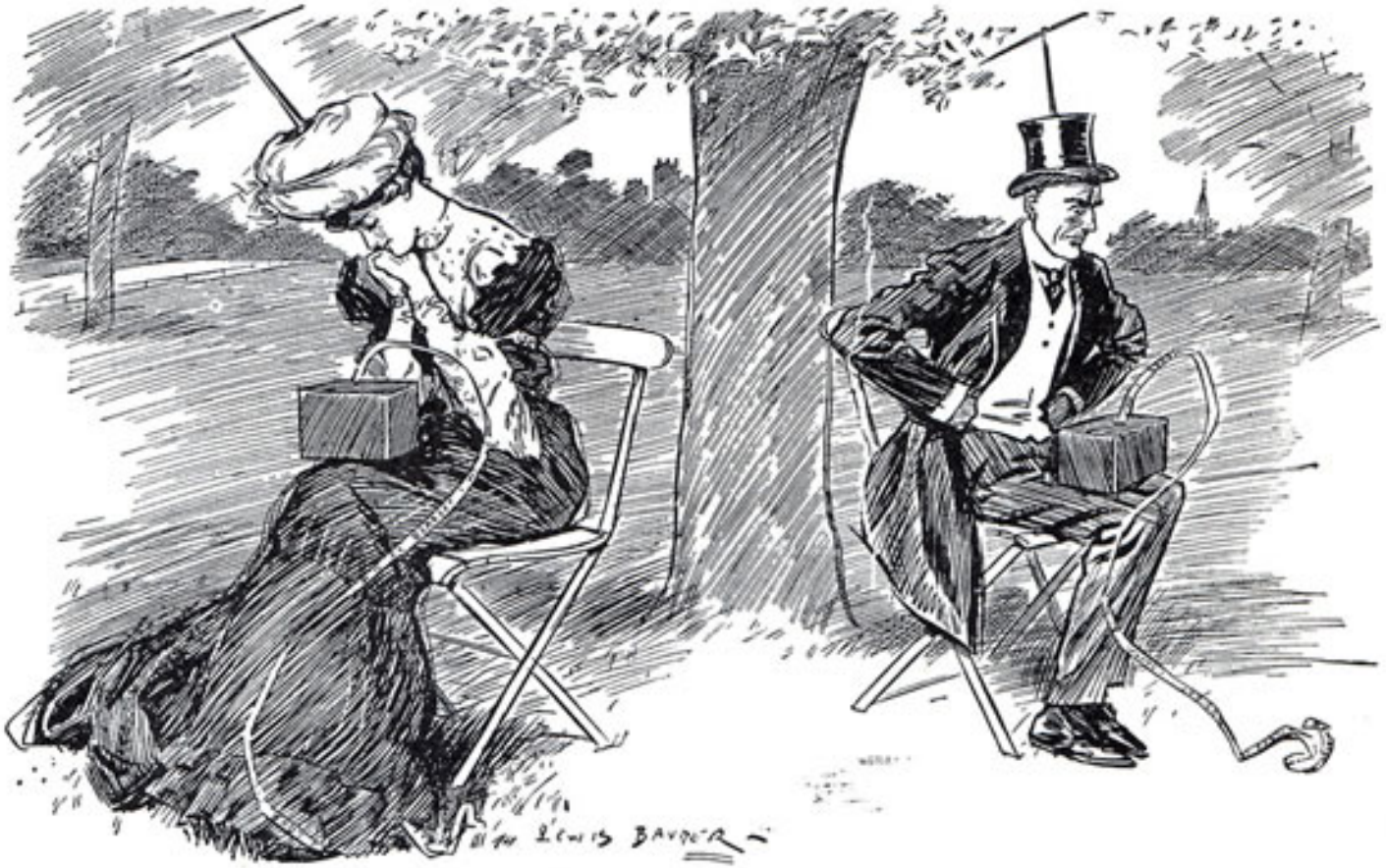
Wireless Network Security

Pieter van den Hombergh

Fontys Hogeschool voor Techniek en Logistiek

June 6, 2016



DEVELOPMENT OF WIRELESS TELEGRAPHY. SCENE IN HYDE PARK.

(These two figures are not communicating with one another. The lady is receiving an amatory message, and the gentleman some racing results.)

(1906)

Future vision from the past.

Common abbreviations in Wireless Networks

AP	access point
BSS	Basic Service Set
DS	Distribution System
ESS	Extended Service Set
MAC	Message Authentication Code
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit

New Dangers Ahead?

Traditional corporate computer use was:

- Company supplied PC, controlled by and connected to the company (controlled) wired network inside the company's buildings.

Now:

- Use of lap tops is much more common.
- As is they being "connected" using WiFi.
- Employees bring in their own devices
  - Often with WiFi connectivity (smart phones, tablets, wearables).
  - Have recording and listening capability.
  - Less often, outside of the control of the company, yet still brought to the premises.
  - These devices should be categorized untrusted.

New Dangers Ahead

Although not only related to wireless networking, the following adds to the mix:

- Cloud based applications. Instead of being confined to the corporate network, applications are accessible from and through the internet, mobile device included, even wanted.
- Use of the company application outside of the premises perimeter. Stallings calls this de-perimeterization.
- External business requirements such as **Guest Accounts**.
-

Mobility Threats

- BYOD is en vogue.
- Lack of physical control. The device is “onwed” and controlled by the user who can take (and leave) it anywhere. Theft is also a risk.
- Use of untrusted devices.
- Use of untrusted networks, either on or off premises.
- Use of applications of unknown origin. It is (too) easy to install an App.
- Interaction with other systems. Bluetooth, QR code, RFID, all of which can be counterfeited to send out malicious urls for instance.
- Location devices such as GPS or beacons, which may provide useful information to an attacker.

M Device Security Strategy

- Inspection of the device should take place before it is allowed onto the corporate network.
- Rooted and jail-broken devices should not be permitted.
- Storage (even caching) of corporate contacts on the device should be prohibited.
  - A web like application for e.g. email can be made more secure then a fat app. The contacts (email lists) do not have to leave the server. The could be addresses for intra-company use only.
- Enable auto-lock and make sure a “secure” unlock code is used, like a pin-code.
- Enable password or pin protection.
- Avoid auto-complete for user name and password.
- Enable remote wipe.

M Device Security Strategy, cont'd

- Use SSL protection.
- Make sure device OS and apps are up to date.
- Use anti-virus (if available) and keep that up to date too.
- Prohibit saving of sensitive data or insist on encryption of the device.
- IT staff should be able to do a remote wipe.
- Disallow third part apps.
- Apply restrictions on what is allowed with could storage.
- Maybe disable location devices altogether.

Wireless Network Threats

- Wireless is broadcasting, so eavesdropping is made really easy.
- Wireless devices are typically mobile and easily installed.
- Wireless sensor devices have little computing and memory resources which are a handicap when implementing strong security.
- Wireless devices are easily placed somewhere, either for eavesdropping (bug on the wall) or for monitor other wireless traffic.

Threats continued

Accidental association Occurs in overlapping neighboring WLAN networks.

Malicious association A access point is set up to lure people to connect to it.

Ad hoc networks missing (central) point of control. As if someone is spanning a network outside of the control of the owner of the location (premises, office, campus).

Non traditional networks Blue tooth, barcode readers, PDAs might be used for or victim to attacks.

Indentity theft or MAC spoofing, assuming the identity of another device. Some

Man in the middle attacks WiFi networks make this very easy. As a hacker, you do not have to own a real router, a well placed WiFi access point intended for malicious association does the trick.

Denial of service Because the access point is not only a

Wireless security

- Wireless encryption can use the following modes
  - None. Insecure by definition: double  .
  - WEP (Wired Equivalence Privacy, nowadays also  , but still better then nothing.
  - WPA for Wi-Fi Protected Access, the follow up and improvement on WEP, now a  .
  - WPA2, also known as RSN for Robust Security Network.
- Notice how the marketing names sound okay, even if the product does not warrant the description over time.
- WPA2/RSN provides:
  - Authentication, providing mutual (server and client).
  - Access control, forcing the use of the authentication function.
  - Privacy with message integrity.

Wireless Security Measures

- Signal hiding techniques
  - Not broadcasting the access point ID (SSID).
  - Using a cryptic SSID (no meaning full name)
  - Reducing the signal strength. Keep the signal within the building.
- Encryption like using WPAx in stead of WPE
  - WPE means Wired Equivalent Privacy and is deprecated nowadays. The protection it provides is considered weak.