

# WLAN Security is in the Architecture

ICEFIN Workshop  
presentation 28.4.2004



# The History of WLAN Network Architecture 1/2

- Completely Open Networks
  - No WEP encryption, no MAC address lists, instant access
  - No problems unless the lack of encryption and access control is considered a one
- Closed and Hidden Networks
  - WEP encryption, no network name (ESSID) in beacon messages
  - Interoperability problems with the WEP key length and with the non-standard beacon messages (no ESSID)
- Enter the Access Control
  - MAC address access control lists in the access points or centralised in the RADIUS database
  - Scalability becomes an issue as only few access points are capable of using RADIUS. Usability is sacrificed because of the security, but the security on the other hand is reasonably strong.

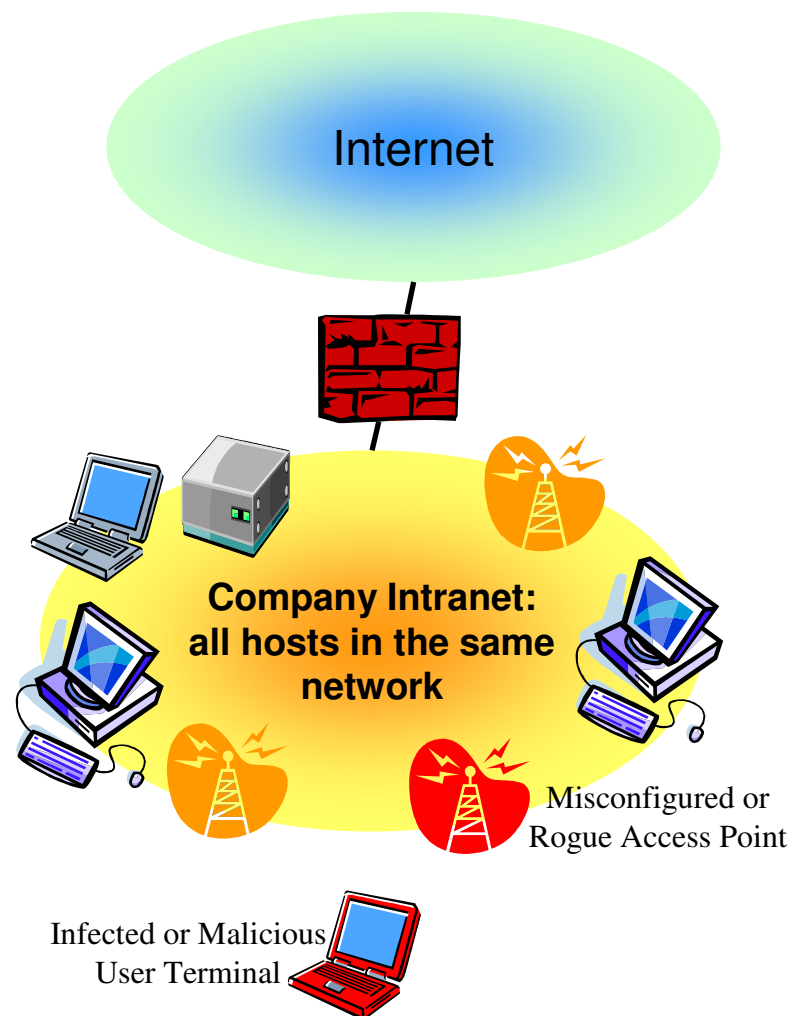
# The History of WLAN Network Architecture 2/2

- Separation of Networks, Access Controllers, VPN
  - The first real architectural change to improve security
  - Although presented here, some companies have been utilising this architecture the whole time
  - Less secure wireless networks are separated from the intranets, access is controlled via access controllers or VPN terminators.
  - Other methods may be used, but sufficient security and usability can be achieved even in the completely open networks.
  - VPN secures the traffic all the way from terminal to secured network.
- WPA, 802.1X, 802.11i, the future?
  - Dynamic (802.1X, WPA) and user/packet-specific (WPA) WEP keys, Dynamic VLAN assignment (802.1X), AES encryption (802.11i)
  - Rely heavily on RADIUS services
  - Will secure only the authentication credentials and the traffic over the radio network
  - Does not require changing the network architecture model.

# So What Is The Problem?

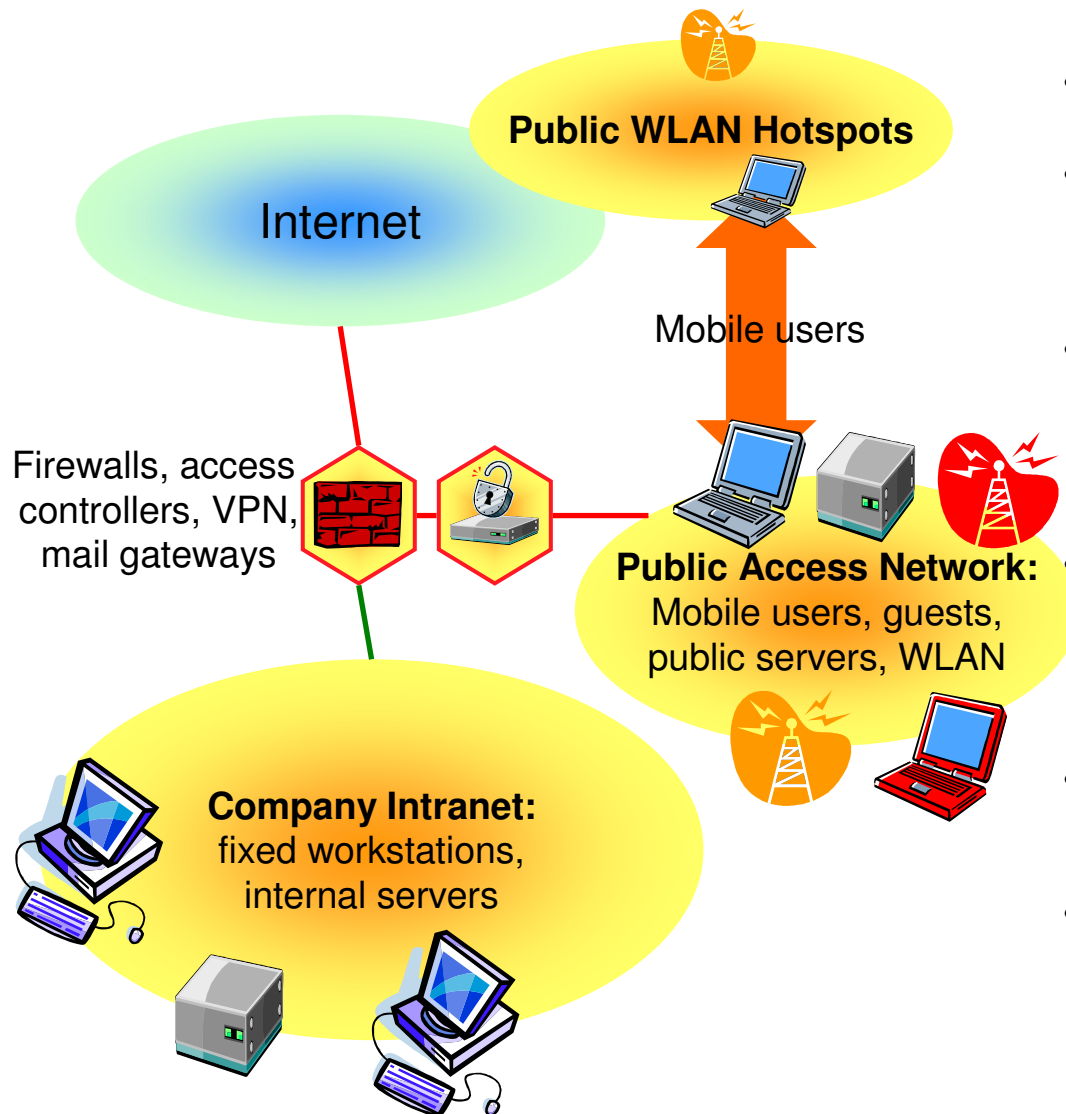
- While the WLAN (security) features have continued to evolve, the architecture and the related problems in several company networks have still stayed the same.
- Wireless networks are still considered to be just a cable-replacements when they should be treated like external mobile access networks.
- The company communication services are designed like they would always be used through secure network.
- The user terminal mobility is not considered when security is defined. The user terminal is often considered to stay in secure (home) network, not roaming in potentially hostile networks and environments.

# The Problems of Wireless Intranet Model



- In this model the fixed and wireless network are mixed. The wireless network is considered just a cable-replacement.
- Network services like e-mail and Windows shares are used without additional encryption.
- Network is protected from threats coming from Internet, but internal security is neglected.
- Single misconfigured or rogue access point may provide an attacker way straight to the heart of the network.
- Infected mobile terminal easily infects the whole company network.
- Malicious user (terminal) can eavesdrop network traffic without detection as the services generally are not protected with TLS/SSL.
- The mobility is often not considered, e.g. how does the user read her emails from/via a foreign network?

# The Wireless Access Network Solution



- WLAN network is separated from the intranet to a public access network.
- Several different access control and traffic securing solutions may be used from access controllers to 802.1X, from TLS/SSL to VPNs
- VPN secures user terminal traffic both in the public access network and when using for example public WLAN hotspots => user experience stays the same, whatever the location
- Malicious or infected terminal can attack hosts and services inside public access network => user terminal's mobile security and mobile services must be ready
- The area to be infected or infiltrated is however much smaller in this model.
- Rogue access points don't really matter as long as they are connected to public access network and/or relay traffic.

## And Why This Architecture Is A Good Thing?

- Wireless/mobile network is now a separate network => The special qualities and requirements of the network can now be handled better.
- Misconfigured/rogue access points and found WLAN weaknesses do not immediately invalidate the security of the whole network.
- Separate mobile network helps to confine and quarantine infected terminals (e.g. VPN terminator checks the terminal before letting it back to the company intranet)
- Security and usability are now considered also from mobility's viewpoint (mobile terminal security, similar mobile access experience etc.)
- Company communication services must be designed so that they are secure even if used by mobile terminal in a hostile network. This clarifies and adds security also to the company's service architecture.
- Secure services can be utilised also outside WLAN networks (e.g. using VPN to secure employee ADSL access)

# Thank You, Any Questions?

Karri Huhtanen  
kh@archred.com  
www.archred.com