Interworking 2006

Evaluation of current security mechanisms and lacks in wireless and Bluetooth networks

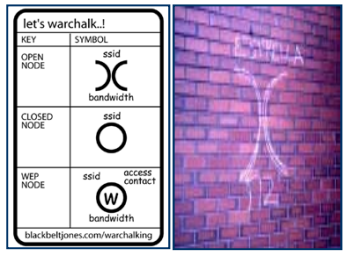
Interworking Conference, 15th - 17th of January 2007

Dr.-Ing. Kai-Oliver Detken
Business URL: http://www.decoit.de
Private URL: http://www.detken.net

Consultancy & Internet Technologies

Approaches

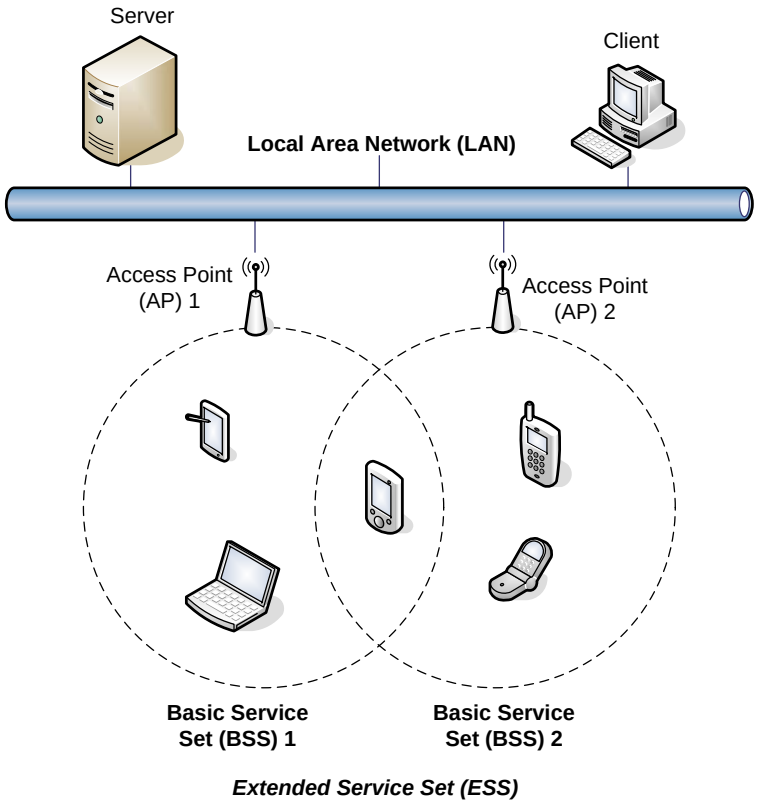
- Examination of both wireless technologies regarding
  - Weakness within the design of security concepts
  - Weakness within implementations
  - Weakness within applications
- Find out the risks
  - Record of data traffic
  - Smuggle in of viruses
  - Identification of clients
  - Disturb of communications and availability
  - …



Wi Fi HOTSPOT

Wireless technologies (1): WLAN

- WLAN utilises spread-spectrum technology based on radio waves to enable communication between devices in a limited area
- This gives users the mobility to move around within a broad coverage area and still be connected to the network
- This technology is becoming increasingly popular, especially with the rapid emergence of small portable devices such as PDAs (personal digital assistants)



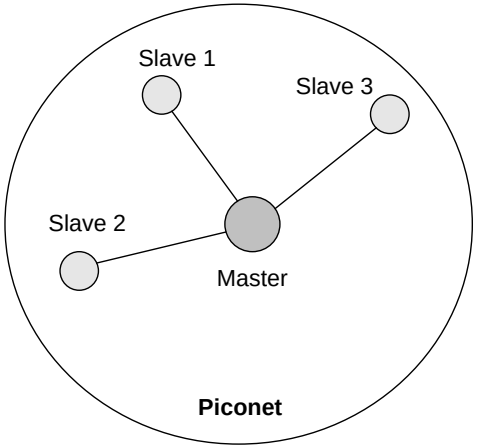
Wireless technologies (2): WLAN standards

Standard	Describtion
802.11a	54 Mbps WLAN on 5-GHz-band
802.11b	11 Mbps WLAN on 2,4-GHz-band
802.11c	Wireless bridging
802.11d	World mode, adaptation of region-specific regularisations
802.11e	Quality-of-Service (QoS) and streaming extensions for 802.11a/g/h
802.11f	Roaming for 802.11a/g/h with Inter Access Point Protocol (IAPP)
802.11g	54 Mbps WLAN on 2,4-GHz-band
802.11h	54 Mbps WLAN on 5-GHz-band with Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
802.11i	Authentication/Encryption for 802.11a/b/g/h (AES and 802.1X)

Wireless technologies (2): Bluetooth

- Bluetooth is a radio standard and communications protocol primarily designed for low power consumption, with a short range
- The devices use a radio communications system, so they do not have to be in line of sight of each other, as long as the received transmission is powerful enough
- As a result of different antenna designs, transmission path attenuations, and other variables, observed ranges are variable

- Up to 7 Slaves are supported from a Master within one Piconet
- Master controls the Piconet
- Slaves communicates every time via the Master



Global target for WLAN security

- There are three steps to take when securing a wireless network:
  - All wireless LAN devices need to be secured
  - All users of the wireless network need to be educated in wireless network security
  - All wireless networks need to be actively monitored for weaknesses and breaches

Basic security mechanisms

- MAC ID filtering: allows the administrator to only permit access to computers that have wireless functionalities which contain certain MAC IDs
- Static IP addresses: no automatically IP assignment function via DHCP server
- WEP encryption: this was the encryption standard for WLAN networks. WEP provides different key sizes: 128 and 256 Bit.
- Further security mechanisms: WiFi Protected Access (WPA), WPA2, 802.1X, LEAP, PEAP, TKIP, RADIUS

Unauthorised access via wireless (1)

- Accidental association: a user turns on the computer and the last latches on to a wireless access point from a neighbouring company's overlapping network arise. The user may not even be aware that this has occurred, but this information is sensible
- Malicious associations: describes situations in which wireless devices are used by crackers to connect to a company network via their cracking laptop instead of a company access point (AP)
- Ad-hoc networks can be a security threat if there has been less integrated security mechanisms
- Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk

Unauthorised access via wireless (2)

- MAC Spoofing occurs when a cracker is able to eavesdrop network traffic and identify the MAC address of a computer with network privileges
- A man-in-the-middle attack revolves around the attacker enticing computers to log into his/her computer which is set up as a rogue AP (Access Point)
- A denial-of-service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands
- Network injection attack: a cracker can make use of access points that are exposed to non-filtered network traffic. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs

Design weakness of WEP

- No key management
  - Static key
  - Has to distribute manually
  - In the most cases no changes
  - Exits in a simple manner
- Compromising of the key makes the whole WLAN unsecured
- No user authentication and identification
- No central authentication and authorisation

Design weakness of WPA

- Access control via 802.1X + EAP method with encryption via TKIP (RC4 algorithm)
  - Problem: Message Integrity Check (MIC) uses a leak hash algorithm
- WPA Personal (WPA-PSK) with pre-shared key
  - Problem: High risk of dictionary attacks; one pre-shared key for all stations of a SSID; high administrative effort
- WPA Enterprise (WPA RADIUS) with dynamical keys for each packet
  - Each user gets its own key; authentication via EAP with RADIUS
- WPA2 (802.11i)
  - Encryption and integrity check by CCMP (AES encryption)
  - CCMP has more powerful as TKIP (same key for frame encryption and integrity check)

Recommendations regarding WLAN

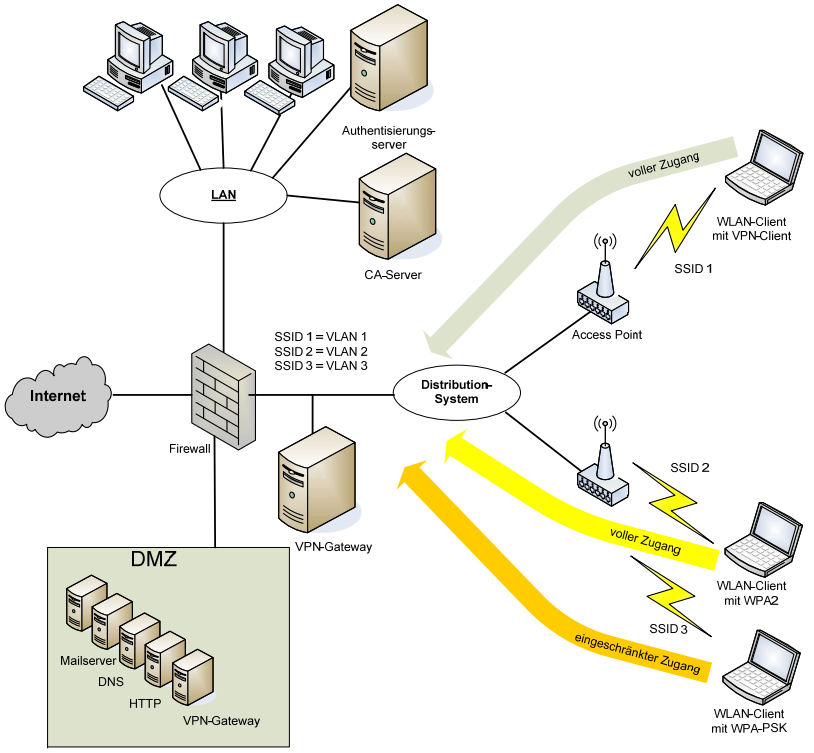
- Authentication each other
- Dynamical session key and key material: EAP method should bring in the key material
- Message integrity: Message Integrity Check (MIC) on TKIP (WPA) and CCMP (WPA2)
- Central authentication and authorisation: central AAA mechanism has to identifier and authenticate user (policy-based network access)
- Quick re-keying: re-keying invite clients to actualise the key (e.g. periodically)
- Session-based encryption: combination of 802.1X, EAP-TLS and RADIUS makes encryption data traffic possible per session and connection with dynamic keys

EAP method

- With Public Key Infrastructure (PKI)
  - EAP-TLS can be used
  - High effort for infrastructure
  - Secure method if authenticator certificate will transfer on a secure way to the supplicant or check with Certification Authority (CA)
- Without PKI
  - EAP-TTLS/PEAP in heterogeneous area; needs only a server certificate; it depends from the authentication
    - EAP-TTLS is more flexible; simpler to integrate; can not fulfil higher secure requirements
    - PEAP is secure for the most applications; less implementation effort; supports only EAP methods
- Suitable basis: 802.1X and EAP!

Mixed operation of WPA and 802.11i

- Regarding a high security level difficult to implement
- Encryption either with TKIP (WPA) or with AES-CCMP (WPA2)
- Some access points allow mixed operation of 802.11i and weak approaches like WEP
- SSID/VLAN mapping is recommended (SSIDs divided in different areas)



Weakness of Bluetooth

- Damaging content such as viruses, worms or Trojan horses, which can be transmitted to user terminals via Bluetooth, SMS or MMS or through WAP pages. Taking advantage of their vulnerability (for instance through attacks to the Bluetooth protocol or through specially „deformed" SMS or MMS messages) such applications can also be installed on the device
- Episodes of denial of service (DoS) attacks or system interruption, caused by the propagation of mal-ware or other types of attacks
- Unauthorised access to information using Trojan horse, spy-ware and eavesdropping attacks, etc.
- Deletion, corruption or modification of data kept on the device

Main hacking methods

- BlueSnarf: based on the OBEX Push service, which is the type of service that is commonly used to exchange electronic business cards. Easy to set in place when a cellular has Bluetooth set on visible mode, BlueSnarf allows connecting to a cellular phone and accessing the phone book and agenda without authorisation.
- Bluejacking: Taking advantage of the IDs that devices exchange at the beginning of a connection – e.g. when a cell phone associates to a computer - short deceitful text messages can be transmitted (e.g. user could be invited to dial a code)
- BlueBug: allows to access the AT Commands of the cellular phone – a set of commands that give instructions to the cellular phone – allowing the aggressor to use the phone services without the user's knowledge
- BlueBump: takes advantage of the vulnerability linked to the Bluetooth connection type that is always active giving the possibility to unauthorised cellular phones to continue accessing as if they were still part of the list of authorised cell phones

Overview about the design weakness

- Most of the attacks are using typical interfaces of Bluetooth
- Here attacks use security lacks in the implementation of the protocol stack
- Further attacks for Bluetooth are available, like PIN hacking, Bluesniping, spoofing, war driving, location tracking, DoS, man in the middle, re-pairing, brute force

Attacks	C	I	A	L	AU	R
E_0	X	X		X	X	
Generator	X	X		X	X	
Key strength	X	X		X	X	
PIN code	X	X		X	X	
Unit Key	X	X		X	X	
FH method	X			X	X	
Security modes	X	X		X	X	
Receive area			X			X

Table 2: Design weakness (C=Confidence; I=Integrity; A=Availability; L=Liability;A=Authenticity; R=Reliability)

Bluetooth recommendations (1)

- Be careful when **downloading new software or applications** from the Internet: before proceeding with the installation of new software or downloading new applications from the Internet, always verify the reliability of the source.
- Pay attention to **possible anomalies in the functioning of the device:** considering that without an installed security application it is rather difficult to identify a virus, there are nonetheless situations that can alarm the user.
- Remember to **deactivate Bluetooth after use** and if this is not possible, at least set the device on „hidden" mode. This precaution ensures at least a minimal level of security since it elongates the time necessary for a potential aggression.

Bluetooth recommendations (2)

- Modify the cellular phone's ID name: Many users tend to maintain the default ID name of their cell phones set by the producer which is usually associated with the specific model of the device.
- Always update security and antivirus software: to successfully counteract attacks, all security software must be updated. Software that is not updated is not useful since computer insecurity is in constant evolution and old software is not designed to face new issues.
- Be careful when choosing PIN numbers to associate devices: too often the codes given by the manufacturer are maintained or, even worse, easily traceable information is used (birthdates for instance)

Conclusions regarding WLAN

- The WLAN community has developed new security features within 802.11i (802.1X and EAP) to make WLAN secure
  - To make sure that you have a uniform authentication with EAP (EAP-TLS, PEAP, EAP-TTLS)
  - Flexible access technology with AAA infrastructure (useful for WLAN, VPN, and LAN)
  - Changing of authentication methods should not be effected the clients and network infrastructure

Conclusions regarding Bluetooth

- To implement a base security all relevant distant terminals should be stored within authentication tables
- A re-keying per PIN has to deactivated
- User PINs has to use more than 4 characters if the software implementation allows that (Bluetooth allows up to 16 characters in its standard)
- Unexpected invitations for a new authentication should be checked immediately

Conclusions of wireless technologies

- Wireless technologies had a real backlog demand regarding security mechanisms
- WLAN and Bluetooth technologies have enough security mechanisms available to make these techniques secure, but in most cases these mechanisms are not well tuned
- Additionally, many companies do not implement wireless security requirements in their common security policy for the wired network
- However, this is essential, because the attacks to wireless equipment will increase in the future and will reach a higher level
- To protect company's networks in an efficient way, the wireless environment has to be an integral part of the existing security concept with defined user and communication profiles
- Further developments of WLAN and Bluetooth will provide improved security mechanisms in the future

Thank you for your attention

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Germany
Phone: +49-421-596064-01
Fax: +49-421-596064-09
E-Mail: detken@decoit.de

Consultancy & Internet Technologies