DECOIT

CAST-Workshop

COMPETENCE CENTER FOR APPLIED SECURITY TECHNOLOGY
CAST

Einführung in die Bluetooth- und WLAN-Sicherheit

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

Consultancy & Internet Technologies

Portfolio der DECOIT GmbH

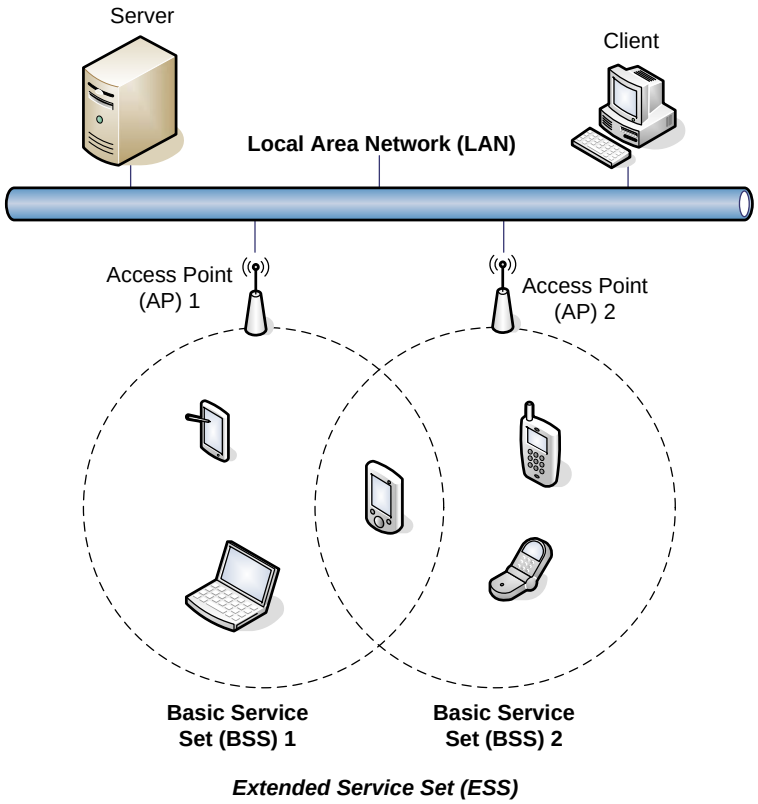
- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Solutions (Lösungen)** zur Identifizierung der Probleme und Angebot einer Lösung für die Umsetzung eines Projekts
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Entwicklung von Internet-Projekten
- Schaffung innovativer eigener **Produkte**
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen

Vortragsinhalt

- Wireless LAN (WLAN)
  - WLAN-Arbeitsweise
  - Basissicherheitsstandards
  - Angriffe
  - Schwachstellen
  - Empfehlungen
- Bluetooth
  - Bluetooth-Arbeitsweise
  - Angriffe
  - Designschwächen
  - Empfehlungen
- Zusammenfassung WLAN/Bluetooth
- Gesamtfazit

WLAN-Arbeitsweise

- WLAN verwendet eine Spread-Spectrum Technologie, die auf Radiowellen basiert
- Übertragungsrate: bis 300 MBit/s (802.11n)
- Reichweite: ca. 300 m im Freien / 30 m in Gebäuden
- Frequenz: 2,4 und 5 GHz
- Frequenzlizenz: nicht erforderlich
- Für Übertragung von Daten entwickelt worden, Sprache ist per VoIP auch möglich
- Ermöglicht dem Benutzer in einem WLAN-Gebiet hohe Mobilität
- Im Peer-to-Peer, Infrastructure, Bridging Mode einsetzbar



Basissicherheitsstandards

- MAC ID Filter: ermöglicht dem Administrator nur den Endgeräten Zugriff zu erlauben, die die richtige MAC-Adresse besitzen
- Statische IP Adresse: keine automatische IP-Adresszuweisung über einen DHCP-Server
- WEP-Verschlüsselung: dies war lange der Verschlüsselungsstandard für WLANs. WEP ermöglicht verschiedene Schlüsselgrößen zu verwenden:128 und 256 Bit
- Weitere Sicherheitsmechanismen sind: WiFi Protected Access (WPA), WPA2, 802.1X, LEAP, PEAP, TKIP, RADIUS

WLAN-Standards (eine Auswahl)

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)

Angriffe

- WLANs werden im privaten Bereich und in Unternehmen jedweder Couleur eingesetzt. Im Heimbereich sind ca. 70 % der WLAN-Netze ungesichert
- Sicherheitsmechanismen wie WEP und teilweise WPA nicht ausreichend
- Wardriving und Warchalking sind zu einem Sport geworden
- Angriffe und Gefahren:
  - Mitschneiden von Datenverkehr im Netzwerk
  - Einschleusen von Daten wie auch schadhaftem Code in das Netzwerk
  - Manipulation von Daten
  - Stören der Kommunikation und damit Verfügbarkeit des Netzes
  - Unterbrechen und Übernahme von bestehenden Verbindungen
  - Ausspähen von Benutzerdaten
  - Identifikation von Clients und damit Benutzern
  - Fälschen von WLAN Access Points und Simulation von Hotspots
  - Kompromittierung von WEP-Schlüsseln
- Für Angriffe ist kein besonderes Know-how notwendig! Es gibt freie Tools im Netz.

Schwachstellen bei WEP

- Kein Schlüsselmanagement
  - Schlüssel ...
    - ist statisch
    - existiert nur einfach
    - muss „von Hand“ verteilt und eingetragen werden
    - wird sehr selten oder überhaupt nicht gewechselt
  - Offenbarung eines Schlüssels, z.B. durch Verlust eines Clients oder mittels frei verfügbarer Angriffs-Tools, kompromittiert das gesamte WLAN
- Keine Benutzeridentifikation und -Authentisierung
- Keine zentrale Authentisierung und Autorisierung

Alternative Sicherheitsmechanismen und Verfahren (1)

- Wi-Fi Protected Access (WPA):
  - Zugangssteuerung über 802.1X + EAP-Methode
  - Vertraulichkeit und Datenintegrität durch TKIP (RC4-Verschlüsselung). TKIP bietet Grundsicherheit auf der Bitübertragungsschicht. Kombiniert mit 802.1X ist es relativ sicher.
    - Problem: MIC nutzt einen schwachen Hash-Algorithmus. Ein Angreifer kann irgendwann zufällig ein Paket mit der richtigen Prüfsumme senden, das vom Access Point akzeptiert und durchgelassen wird.
  - WPA Personal (WPA-PSK): Einfachste Variante; für den Heimbetrieb ausgelegt. Für Anwender ohne 802.1X-Infrastruktur. Es kommt ein Preshared Key zum Einsatz.
    - Problem: Risiko von Wörterbuchattacken. I.d.R. ein Preshared Key für alle Stationen einer SSID. Angreifer kann Schlüssel ableiten. Qualität der Passphrase bestimmt die Sicherheit des Preshared Keys. Administrativer Aufwand in größeren WLANs nicht beherrschbar.

Alternative Sicherheitsmechanismen und Verfahren (2)

- Wi-Fi Protected Access (WPA):
  - WPA Enterprise (WPA RADIUS): Dynamische Schlüssel für jedes versendete Paket. Für jeden Benutzer ein Schlüssel. Authentisierung über EAP-Verfahren, oft RADIUS.
- 802.11i / WPA2:
  - Verschlüsselung und Integritätsprüfung durch CCMP (AES als Verschlüsselungsverfahren)
  - Im Vergleich zu WPA deutlich sicherer. CCMP ist wesentlich leistungsfähiger als TKIP, da ein und derselbe Schlüssel zur Frame-Verschlüsselung und Integritätsprüfung benutzt wird
  - WPA2 hat diverse Untersuchungen und Prüfungen von Kryptoanalytikern bestanden und entspricht dem Stand der Technik
  - 802.11i bietet geschützten Ad-hoc-Modus, Secure Fast Handoff und Pre-Authentication, sicheres De-Authentication und Disassociation

Empfehlungen (1)

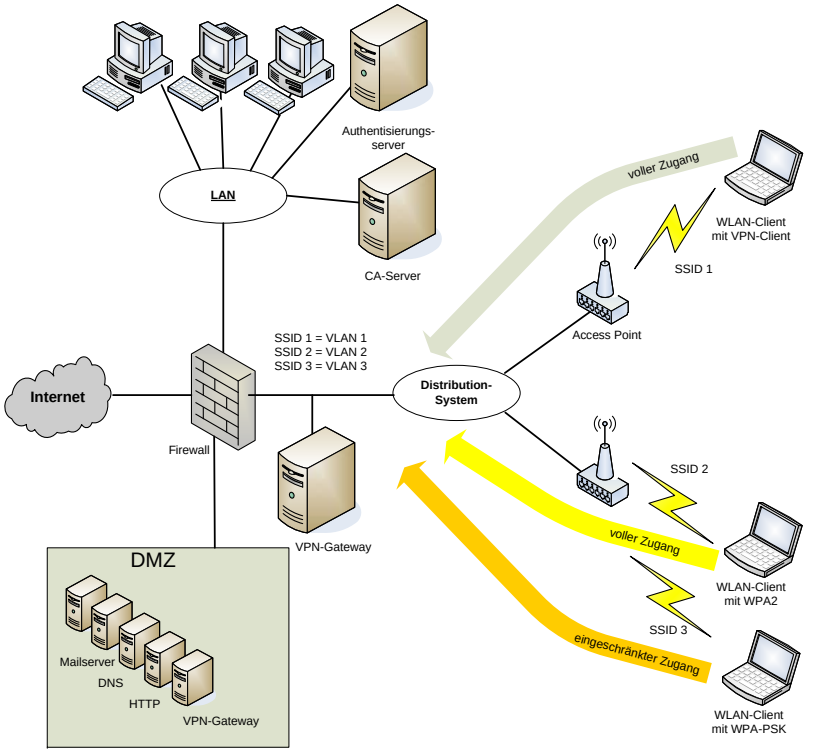
- Folgende Punkte sollten beachtet werden (u.a. von „802.11i Security Task Group“ sowie dem „WiFi WPA“-Standard empfohlen):
  - Gegenseitige Authentisierung
  - Dynamische Sitzungsschlüssel und Schlüsselmaterial: EAP-Methode sollte Schlüsselmaterial zur Verfügung stellen
  - Nachrichtenintegrität: Message Integrity Check (MIC) bei TKIP (WPA) sowie CCMP (WPA2)
  - Zentrale Authentisierung und Autorisierung: Zentralisierter AAA-Mechanismus muss Benutzer einzeln identifizieren und authentisieren (Policy-basierter Netzwerkzugang abbildbar)
  - Schnelles Re-Keying: Re-Keying fordert Clients auf, Schlüssel zu aktualisieren (z.B. periodisch)
  - Session-basierte Verschlüsselung: Kombination von 802.1X, EAP-TLS und RADIUS erlaubt pro Verbindung und Sitzung verschlüsselten Datenverkehr mit dynamischen Schlüsseln

Empfehlungen (2)

- Welches EAP-Verfahren?
  - Wenn eine PKI vorhanden ist:
    - EAP-TLS kann genutzt werden
    - Jedoch hoher infrastruktureller Aufwand
    - Sicheres Verfahren, wenn das Authenticator-Zertifikat sicher zum Supplicant übertragen wird oder durch eine CA überprüft wird
  - Wenn keine PKI vorhanden ist:
    - EAP-TTLS/PEAP, besonders bei einem heterogenen Netzwerk
    - Braucht nur Server-Zertifikat
    - Ist abhängig von nachgelagerter Authentisierung
  - Geeignete Grundlage: 802.1X + EAP:
    - Einheitliche Authentisierungsmethodik mittels EAP
    - Flexibel in der Zugangstechnik, da AAA-Infrastruktur nicht nur für WLAN, sondern auch für LAN und VPN einsetzbar ist
    - Änderung der Authentisierungsmethode haben kaum Auswirkungen auf Client und Netzwerkinfrastruktur

Mischbetrieb von WPA und 802.11i

- Verschlüsselung entweder per TKIP (WPA) oder AES-CCMP (WPA2)
- Einige Access Points erlauben Mischbetrieb von 802.11i und schwachen Verfahren wie WEP
- SSID/VLAN-Mapping ist empfehlenswert; mit verschiedenen SSIDs Funkzellen logisch voneinander trennbar (pro SSID unterschiedliche Sicherheitslevel)
- Access Point leitet Benutzer entsprechend SSID in verschiedene VLANs



Bluetooth-Arbeitsweise (1)

- Bluetooth-Geräte senden als Short Range Devices im lizenzfreien ISM-Band zwischen 2,402 GHz und 2,480 GHz
- Störungen können z.B. durch WLAN-Netze, schnurlose (drahtlose) Telefone, Garagentoröffner oder Mikrowellenherde verursacht werden, die im gleichen Frequenzband arbeiten
- Um Robustheit gegenüber Störungen zu erreichen, wird ein Frequenzsprungverfahren (Frequency Hopping) eingesetzt, bei dem das Frequenzband in 79 Frequenzstufen im 1-MHz-Abstand eingeteilt wird, die bis zu 1600 Mal in der Sekunde gewechselt werden
- Am unteren und oberen Ende gibt es jeweils ein Frequenzband als Sicherheitsband (Guard Band) zu benachbarten Frequenzbereichen

Bluetooth-Arbeitsweise (2)

- Theoretisch kann eine Datenübertragungsrate von 1 MBit/s beim Download bei gleichzeitigen 57,6 kBit/s beim Upload erreicht werden
- Seit der Version 2.0 können Daten durch EDR (Enhanced Data Rate) maximal etwa dreimal so schnell übertragen werden, also mit rund 2,1 MBit/s
- Bereits seit Version 1.1 kann ein Bluetooth-Gerät gleichzeitig bis zu sieben Verbindungen aufrechterhalten, wobei sich die beteiligten Geräte die verfügbare Bandbreite teilen müssen (Shared Medium)
- Bluetooth unterstützt die Übertragung von Sprache und Daten
- Eine Verschlüsselung der transportierten Daten ist ebenfalls möglich

Angriffe

- **Lokalisierung:** Standort des Zielgeräts herausfinden
- **Bluesnarf:** Firmware-Bugs werden genutzt, um Adressverzeichnisse einzusehen
- **BTChaos:** Es werden Daten mit AT-Befehlen ausgelesen; Daten können geschrieben werden
- **Bluebug:** mittels AT-Befehle können SMS gesendet werden
- **PIN:** Attacke auf den PIN Code
- **Spoofing:** Geräteschlüssel wird als Angriffsmedium verwendet
- **Bluejacking:** es werden unerwünschte Nachrichten versendet
- **Bluesniping:** Attackieren aus großer Entfernung
- **Bluetooth Wardriving:** Verfolgung von Benutzerbewegungen
- **Location-Tracking:** Lokalisierung innerhalb von Hotspots
- **Denial-of-Service:** ständige Kommunikationsabfragen, um das Bluetooth-Gerät zu belasten
- **Man-in-the-Middle:** Pakete abfangen und manipulieren
- **Re-Pairing:** Pairing-Prozess wird erzwungen, um Attacke zu fahren
- **Backdoor:** Zugriff über Invisible-Mode ohne Kenntnisnahme des Benutzers
- **Brute-Force:** 4stelliger PIN kann abgeleitet werden, um daraus den Link Key zu ermitteln

Zusammenfassung der Angriffe

- Die am meisten genannten Bedrohungen beziehen sich auf die Bluetooth-Schnittstelle. Angriffe nutzen dabei die Sicherheitslücken in instabilen Implementierungen des Bluetooth-Protokollstacks
- Viele Sicherheitseinstellungen sind nur optional nutzbar, so dass durch die Nichtnutzung oder durch schlechte Implementierungen Sicherheitslöcher entstehen
- Eine weitere Schwäche ist die eindeutige Geräteadresse, die nicht nur zum Verbindungsaufbau verwendet wird. Es lassen sich daher Bewegungsprofile erstellen
- Durch Kombinationen (Object Push, Synchronisation, IrDA, Bluetooth und OBEX) werden Sicherheitslücken offen gelegt

Designschwächen

- Verschlüsselung ist bei Bluetooth nicht grundsätzlich vorgeschrieben
- In der Bluetooth-Spezifikation werden keine Anforderungen an den Zufallsgenerator gestellt und er wird unzureichend definiert
- Im Bluetooth-Standard liegt keine Beschreibung vor, wie der Unit Key im Gerät gespeichert werden soll
- Die Länge des Sitzungsschlüssels (Encryption Key) ist variabel und kann weniger als 128 Bit betragen
- PIN-Codes, die eine zu geringe Länge aufweisen (4stellig), können während des Pairing-Prozesses abgehört werden
- In der Bluetooth-Spezifikation ist das Verhalten des Geräts für den Fall, dass es sich aus der Sendereichweite eines gepairten Endgeräts wegbewegt, nicht definiert (Bewegungsprofile)

Sicherheitsmodi

- Da alle Sicherheitsdienste in der Datenübertragungsschicht (Layer 2) angesiedelt sind, ist bei Bluetooth keine Ende-zu-Ende-Sicherheit möglich
- Nur einzelne Verbindungen werden verschlüsselt und authentisiert
- Diese Schwächen werden in den Sicherheitsmodi folgendermaßen aufgelistet:
  - Modus 1: Verschlüsselung wird nicht aktiviert
  - Modus 2: Verschlüsselung, die von der Applikationsebene aus aktiviert wird
  - Modus 3: Verschlüsselung, die unabhängig von der Applikationsebene aktiviert wird

Bewertung

- Der Benutzer von Bluetooth-Geräten hat keine Informationen über die korrekte Implementierung vorhandener Sicherheitstechniken (z.B. Authentifizierung)
- Es können Bewegungsprofile erstellt werden. Es ist dadurch möglich, mittels eines dichten Netzes von Bluetooth-Geräten, regelmäßig die Umgebung nach neuen unbekannten Geräten durchzusuchen
- Es wäre generell zu empfehlen, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und gegebenenfalls anzupassen
- Mobile Geräte, die sich mit fremden Geräten beziehungsweise mit Geräten unterschiedlicher Benutzer verbinden, müssen besonders abgesichert werden

Empfehlungen

- Die bei dem Pairing-Prozess benutzte PIN muss ausreichend lang sein
- Jedes Gerät, das mehrere Dienste mit verschiedenen Sicherheitsniveaus zur Verfügung stellt, sollte im Sicherheitsmodus 2 betrieben werden. Hierbei ist darauf zu achten, dass die Security Policys sorgfältig erstellt werden
- Geräte, die nur einen Dienst oder mehrere Dienste mit gleichem Sicherheitsniveau anbieten, sind im Sicherheitsmodus 3 zu betreiben
- In den Geräten sollte außerdem die PIN nach der Initialisierung gelöscht werden. Somit wird sie im Gerät nicht gespeichert und muss nach jedem Einschalten des Gerätes erneut angegeben werden
- Bei Verlust beziehungsweise Diebstahl eines Geräts sollten alle zugehörigen Link Keys (Verbindungsschlüssel) in den verbliebenen Geräten gelöscht werden
- Eine bessere Maßnahme zur Unterbindung oder Abschwächung möglicher Attacken wäre, beim Kauf des Gerätes darauf zu achten, dass keine Verbindung zwischen der Basisadresse und der Identität des Käufers hergestellt werden kann

Auffinden von Bluetooth-Geräten

- Für Unternehmen sollten insbesondere Softwarelösungen zur Identifikation von Bluetooth-Geräten Einsatz finden
- Es lassen sich nicht nur Geräte mit falscher bzw. mangelhafter Konfiguration identifizieren, sondern auch herauszufinden, welche Geräte (und Art) in Betrieb sind und mit welchen anderen Geräten sie kommunizieren
- Beim Monitoring von Bluetooth-Aktivitäten können Administratoren spezifische Gefahren erkennen und potenzielle Einbrüche abwehren
- Typische Funktionen solcher Programme sind:
  - Identifikation unterschiedlicher Klassen von Bluetooth-Geräten (PDAs, Keyboards, Headsets, Laptops, Mobiltelefone etc.)
  - Ausgabe von zusätzlichen Informationen über das gefundene Gerät (u.a. Hersteller, Signalstärke des Gerätes etc.)
  - Informationen über Verbindungen zwischen Geräten
  - Identifikation verfügbarer Dienste auf Geräten

Zusammenfassung WLAN/Bluetooth

- WLAN
  - Eindeutige Authentifizierung mittels EAP (EAP-TLS, PEAP, EAP-TTLS) durchführen
  - Flexible Zugangstechnologien mit AAA-Infrastruktur realisieren
  - Änderung der Authentifizierungmethode sollten Clients und Netzwerk nicht beeinträchtigen
- Bluetooth
  - Alle relevanten Geräte sollten in Authentifizierungstabellen angelegt werden
  - Ein Re-keying per PIN sollte nicht möglich sein
  - Der Benutzer-PIN sollte mehr als 4 Stellen betragen
  - Unerwartete Einladungen sollten vor einer neuen Authentifizierung überprüft werden

Gesamtfazit

- Drahtlose Technologien besitzen insgesamt einen Sicherheitsrückstand gegenüber drahtgebundenen Verfahren
- WLAN und Bluetooth haben inzwischen ausreichende Sicherheitsmechanismen zur Verfügung, die aber in den meisten Fällen falsch konfiguriert oder nicht genutzt werden
- Die meisten Unternehmen haben in ihren globalen Sicherheitsrichtlinien mobile Endgeräte nicht berücksichtigt
- Dies wird in Zukunft immer wichtiger werden, da die Attacken auf mobile Endgeräte zunehmen
- Um ein Unternehmensnetz effizient schützen zu können, müssen mobile Endgeräte in das bestehende Sicherheitskonzept integriert werden (inkl. Benutzer- und Kommunikationsprofile)
- WLAN-Technologien und Bluetooth werden weiter bzgl. der Sicherheitsmechanismen erweitert und verbessert werden

Das Buch zum Thema

- Autoren: Dr.-Ing. Kai-Oliver Detken und Prof. Dr.-Ing. Evren Eren
- Inhalte:
  - Grundlagen mobiler Kommunikation und Sicherheit
  - Gefahren- und Angriffspotenziale in der mobilen Kommunikation sowie bei mobilen Geräten und Anwendungen
  - Sicherheitskonzepte und -strategien sowie Handlungsempfehlungen, mit denen Angriffe auf mobile Netze, Systeme und Endgeräte wie Laptops, Handys, Smartphones, Organiser, PocketPCs oder PDAs abgewehrt werden können
  - Mit Beispiel- und Referenzimplementierungen sowie konkreten Handlungsempfehlungen

Danke für Ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Phone: +49-421-596064-0
Fax: +49-421-596064-09
E-Mail: info@decoit.de

Consultancy & Internet Technologies