Bluetooth Sicherheitslücken -
von der Entdeckung bis zur Enthüllung

Heise Forum '05 – Sicherheit und IT Recht

CeBIT 2005 (Halle 5, Stand E38)
11 März, Messegelände Hannover, Germany

Martin Herfurt <martin.herfurt@trifinite.org>

CeBIT 2004 / Halle 11 - Toilette

Ganz in der Nähe des Gemeinschaftsstandes der FH-Salzburg und Salzburg Research Forschungsgesellschaft

Bluetooth Eckdaten

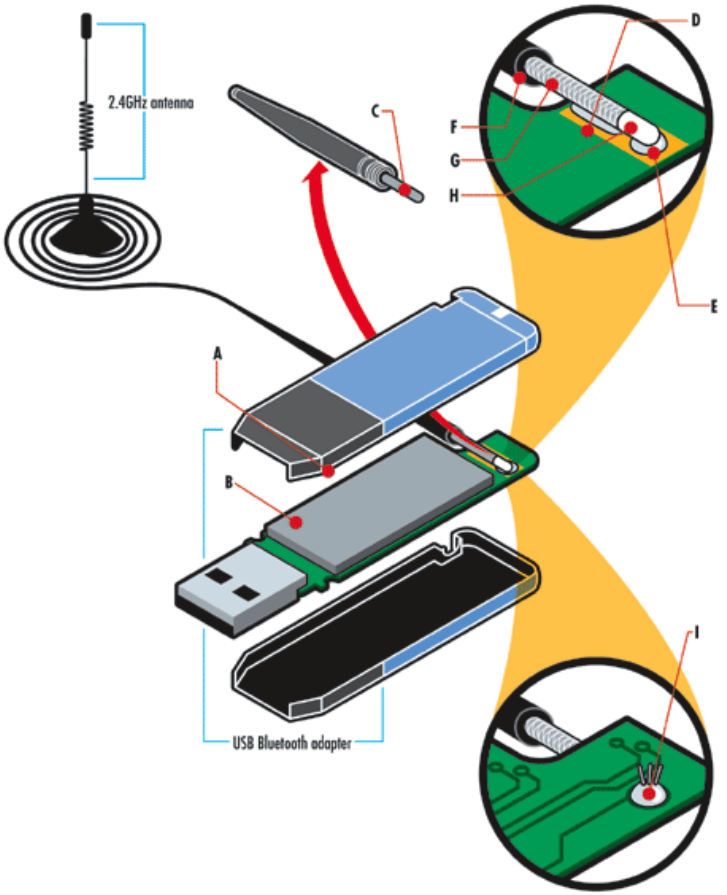
- Kabel Ersatz Technologie
- Geringer Stromverbrauch
- Kleine Reichweite 10m - 100m
  - Je nach Geräteklasse
- 2.4 GHz
- 1 Mb/s Durchsatz

- Zuerst entdeckt von Marcel Holtmann
  - Oktober 2003
  - Wireless Technologie Kongress, Sindelfingen, Germany
- Adam Laurie, A L Digital, November 2003
  - Bugtraq, Full Disclosure
  - Houses of Parliament
  - London Underground
- 'Snarf' – Jargon Wort für 'unautorisierte Kopie'

- Entdeckt im February 2004
  - Anlass: FH Salzburg 'Forum IKT 2004'
  - Zur Aufwertung einer Presentation zu Wardriving
- Motiviert durch Kenntnis von BlueSnarf
- Resultat: neuer Exploit namens BlueBug
- Bekanntheit durch CeBIT Feldtest Report
- Weitere Stichproben an Flughäfen etc.
- Durch BlueBug können Kosten am Gerät verursacht werden
  -> Relevanz für Herstellerfirmen

Bluetooone™

- Modifikation eines Bluetooth Dongels
- Veränderung zum Anschluss einer externen Antenne
- Idee von Mike Outmesguine (Autor des Buches: “Wi-Fi Toys”)
- Genaue Beschreibung auf trifinite.org



Attacke aus großer Entfernung

- Anfang August 2004
  (kurz nach DEFCON 12)
- Durchgeführt in
  Santa Monica, Kalifornien
- Verwendetes Equipment
  - 'Getooonter' Klasse 1
    Bluetooth Dongel
  - Anfälliges Nokia 6310i
- Entfernung:
  1,78 km (1.01 Meilen)

trifinite.group

- Gegründet Ende August 2004
  - Adam Laurie (the Bunker Secure Hosting)
  - Marcel Holtmann (BlueZ)
  - Collin Mulliner (mulliner.org)
  - Tim Hurman (Pentest)
  - Mark Rowe (Pentest)
  - Martin Herfurt (trifinite.org, Gründer)
  - Spot (Sony)

trifinite.org

- http://trifinite.org/
- Loser Verbund von Bluetooth Sicherheitsexperten
- Inhalte der Seite trifinite.org
  - **trifinite.**blog : Neuigkeiten
  - **trifinite.**stuff : Projekte (Bluetooth)
  - **trifinite.**download : Vortragsfolien, Toools,...

Blooover™

- Blooover - *Bluetooth* Wireless Technology Hoover
- Proof-of-Concept Anwendung bzw. Geräte Auditing Tool
- Veröffentlichung am 28. Dezember 2004 beim 21C3 in Berlin
- Bisher 35.000 Downloads
- Läuft auf J2ME MIDP 2.0 Geräten mit Bluetooth API

Blueprinting™

- Fingerprinting von *Bluetooth* Geräten
- Begonnen von Collin R. Mulliner and Martin Herfurt
- Für viele verschiedene Anwendungen
  - Sicherheitsaudits
  - Geräte-Statistiken
  - Automatisierte Applikations-Distribution
- Veröffentlicht am 21C3 (December 2004, Berlin)

- Entdeckt im September 2004
- Vergleichbar mit dem Ping-of-Death (Win95)
- Bluetooth Kiss-of-Death
- Denial of Service Attacke
- Bluetooth Stack und/oder Gerät müssen nachher neu gestartet werden
- ... weitere Attacken bereits bekannt

Präsentationen bei Konferenzen

- Besuchte Konfernzen
  - BlackHat USA 2004 (Juli 2004, Las Vegas)
  - DEFCON-12 (August 2004, Las Vegas)
  - CCC (21C3) (Dezember 2004, Berlin)
- Geplante Konferenzen
  - BlackHat Europe 2005 (März 2005, Amsterdam)
  - BlackHat USA 2005 (Juli 2005, Las Vegas)
  - DEFCON-13 (August 2005, Las Vegas)

Kooperation mit Bluetooth SIG

- Offizielles Bluetooth SIG Security Test Team
- Mitwirkung an UnPlugFests
  - UPF-15 (Oktober 2004, Fankfurt)
  - UPF-20 (Februar 2005, Vancouver)
  - UPF-21 (Juni 2005, Singapur)
  - UPF-22 (September 2005, Prag)
- Entwicklung einer Security Test Suite für BT SIG
  - Wird Bluetooth SIG Mitgliedern kostenlos zur Verfügung gestellt

Erreichte Ziele

- Reaktion der Hersteller
  - Es gibt Firmware Fixes für die betroffenen Geräte
  - Aus diesem Grund auch Full Disclosure erst 13 Monate später
- Sensibilisierung der Hersteller für Security
  - Erste Reaktionen der Hersteller waren eher negativ
- Förderung der Zusammenarbeit von Industrie und Open-Source Community

Fragen / Anregungen / Kritik

- http://trifinite.org/
- Martin Herfurt <martin.herfurt@trifinite.org>