

NSA ANT W-Lan, 30C3, Jacob Appelbaum, 30 December 2013

Die NSA-Abteilung ANT entwickelt auch Methoden, um W-Lan-Netze von außen zu erfassen, anzuzapfen und eigene Software darüber einzuschleusen. Das NIGHTSTAND-System etwa kann für diverse Windows-Systeme aus der Ferne Datenpakete in den Traffic drahtloser Netzwerke injizieren – also beispielsweise Schadsoftware. Das System SPARROW II dagegen ist dazu gedacht, W-Lan-Netze aus der Luft zu kartieren; es ist klein genug, an Bord einer Drohne ("UAV") untergebracht zu werden.

NIGHTSTAND ist ein mobiles System für das Einschleusen von Software in Windows-Rechner über Wireless Lan nach dem 802.11-Standard. Dem Datenblatt zufolge funktioniert diese Methode bis zu Entfernungen von knapp 13 Kilometern.

SPARROW II ist ein Hardwaretool, um Drahtlosnetzwerke zu erfassen und zu kartieren, etwa von einer Drohne aus.



NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.



NIGHTSTAND Hardware



(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



SPARROW II

Wireless Survey - Airborne Operations - UAV

(TS//SI//REL) An embedded computer system running BLINDDATE tools. Sparrow II is a fully functional WLAN collection system with integrated Mini PCI slots for added functionality such as GPS and multiple Wireless Network Interface Cards.

07/25/08

(U//FOUO) System Specs

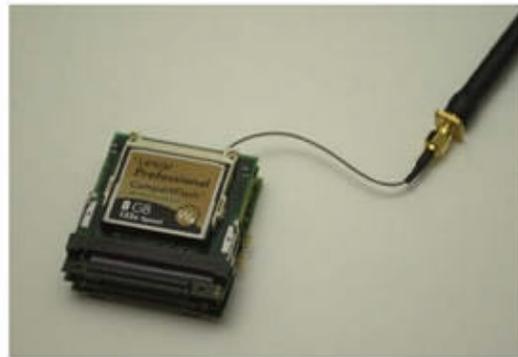
Processor: IBM Power PC 405GPR
Memory: 64MB (SDRAM)
16MB (FLASH)

Expansion: Mini PCI (Up to 4 devices) supports USB, Compact Flash, and 802.11 B/G

OS: Linux (2.4 Kernel)

Application SW: BLINDDATE

Battery Time: At least two hours



SPARROW II Hardware

(TS//SI//REL) The Sparrow II is a capable option for deployment where small size, minimal weight and reduced power consumption are required. PCI devices can be connected to the Sparrow II to provide additional functionality, such as wireless command and control or a second or third 802.11 card. The Sparrow II is shipped with Linux and runs the BLINDDATE software suite.

Unit Cost: \$6K

Status: (S//SI//REL) Operational Restrictions exist for equipment deployment.

POC: [REDACTED], S32242, [REDACTED], [REDACTED]@nsa.ic.gov

