

The NSA Playset

Michael Ossmann

Dean Pierce

TourCamp 2014





HACKRF

Software Defined Radio Peripheral

(U//FOUO) HACKRF is a Software Defined Radio peripheral capable of transmission or reception of arbitrary radio signals from 10 MHz to 6 GHz.

12/31/13



(U//FOUO) HackRF One with optional enclosure

(U//FOUO) HACKRF is an open source hardware platform designed to enable education, experimentation, and deployment of Software Defined Radio (SDR) technology.

(U//FOUO) HackRF One Features:

- 10 MHz to 6 GHz operating frequency
- half-duplex transceiver
- portable
- Hi-Speed USB 2.0, bus powered
- low cost
- open source
- works with GNU Radio
- 20 MHz bandwidth
- 8 bit resolution
- external clock input and output

(U//FOUO) Applications:

- spectrum analysis
- vector signal analysis
- vector signal generation
- reverse engineering
- spectrum sensing
- wireless security testing
- radio research and development

(U//FOUO) HACKRF makes cutting edge SDR technology available to everyone. Now you can build any radio you want.

Status: Available Q1 2014

<http://greatscottgadgets.com/hackrf/>

Unit Cost: \$300 estimated

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

HackRF is open source hardware and software.
Anyone may use it, build it, or modify it,
not just the NSA.

It's
fun!



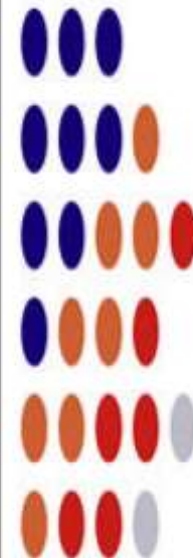
Wi-Fi

Wireless Exploitation / Injection Tool

07/25/08

System Details

-



NIGHTSTAND

Linux on a laptop

Aircrack-ng
metasploit etc.



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

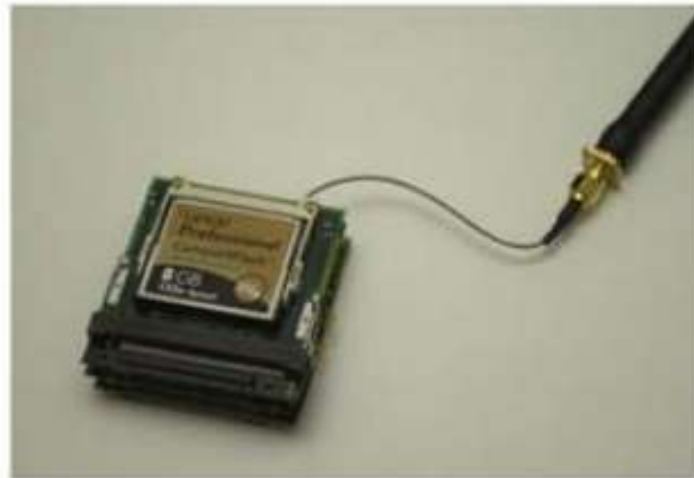
Memory: 64MB (SDRAM)
16MB (FLASH)

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

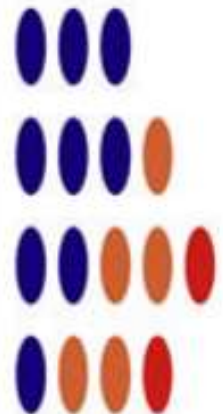
OS: Linux (2.4 Kernel)

Application SW: BLINDDATE

Battery Time: At least two hours



SPARROW II Hardware



SPARROW II

```
Kismet Sort View Windows
Name      BSSID      T C  Ch Freq  Pkts  Size Bcn% Sig Cnt Manuf  Cty Seen By
TRENDnet  00:14:D1:5F:97:12 A 0 1 2417 1 0B --- --- 1 TrendwareI --- wlan0 DRD1812
linksys_SES_45997 00:16:B6:1B:E4:FF A 0 6 2447 2 0B --- --- 1 Cisco-Link --- wlan0 Networks
QQP93 00:1F:90:F2:C0:C2 A W 1 2412 3 0B --- --- 1 ActiontecE US wlan0 17
landscapers 00:14:BF:07:2F:84 A N 6 2437 4 0B --- --- 1 Cisco-Link --- wlan0
linksys 00:1A:70:D9:BC:13 A N 6 2437 5 0B --- --- 1 Cisco-Link --- wlan0
WPA41 00:1F:90:E6:E0:84 A W 11 2462 5 0B --- --- 1 ActiontecE --- wlan0 Packets
6S103 00:1F:90:FA:FA:C8 A W --- 2412 9 0B --- --- 1 ActiontecE --- wlan0 1813
Autogroup Probe 00:13:E8:92:3F:CB P N --- --- 10 0B --- --- 1 IntelCorpo --- wlan0 Pkt/Sec
TFS 00:09:5B:D7:9D:B2 A N 11 2462 13 0B --- --- 1 Netgear --- wlan0 0
meskas 00:18:01:F5:65:E1 A 0 11 2462 17 0B --- --- 1 ActiontecE US wlan0
Xu Chen 00:18:01:F9:70:F0 A N 6 2442 19 0B --- --- 1 ActiontecE US wlan0
TK421 00:18:01:FE:68:77 A 0 6 2442 23 0B --- --- 1 ActiontecE --- wlan0 Elapsed
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0 --- --- --- --- --- --- --- --- 00:02:29
7JAR0 00:1F:90:E6:04:F1 A W --- --- --- --- --- --- --- --- wlan0
Pickles 00:1F:33:F3:C5:4A A 0 --- --- --- --- --- --- --- --- wlan0
38cB 00:16:CE:07:60:77 A W --- --- --- --- --- --- --- --- wlan0
Danish Penguin 00:13:10:35:59:C8 A W --- --- --- --- --- --- --- --- wlan0
BSSID: 00:13:10:35:59:C8 Crypt: WEP Manuf:

( ) Lock (*) Hop ( ) Dwell
Channels 157,3,7,11,48,64,161,4,8,36,52,149,165
Rate B
[ Cancel ] [ Change ]

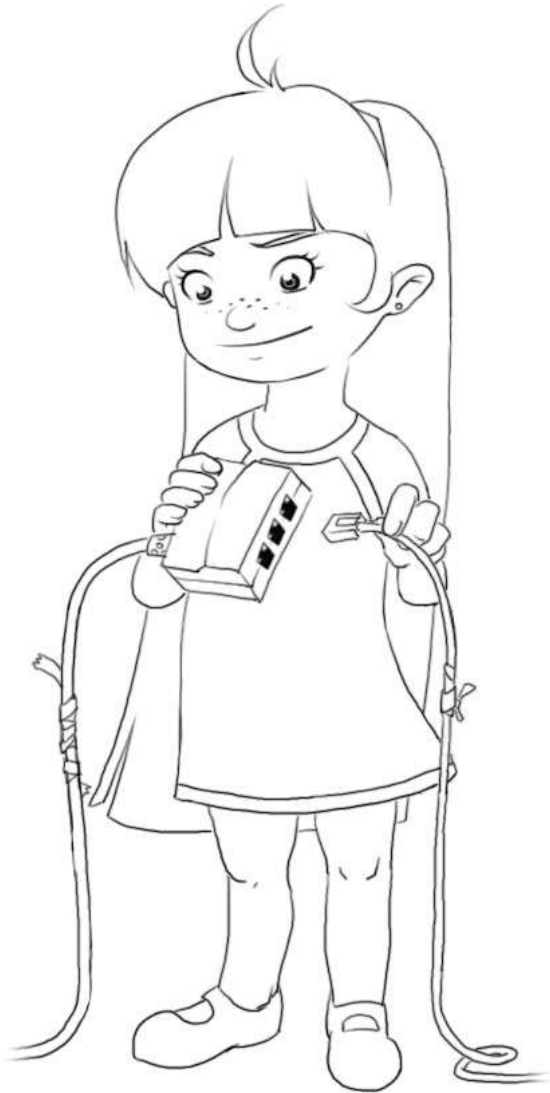
No GPS info (GPS not connected)
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: Could not connect to the spectools server localhost:30569
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

Kismet
is
great!

Fly a phone?

Open WRT:
Wifi Pineapple
Carambola 2 etc.

Hardware Implants



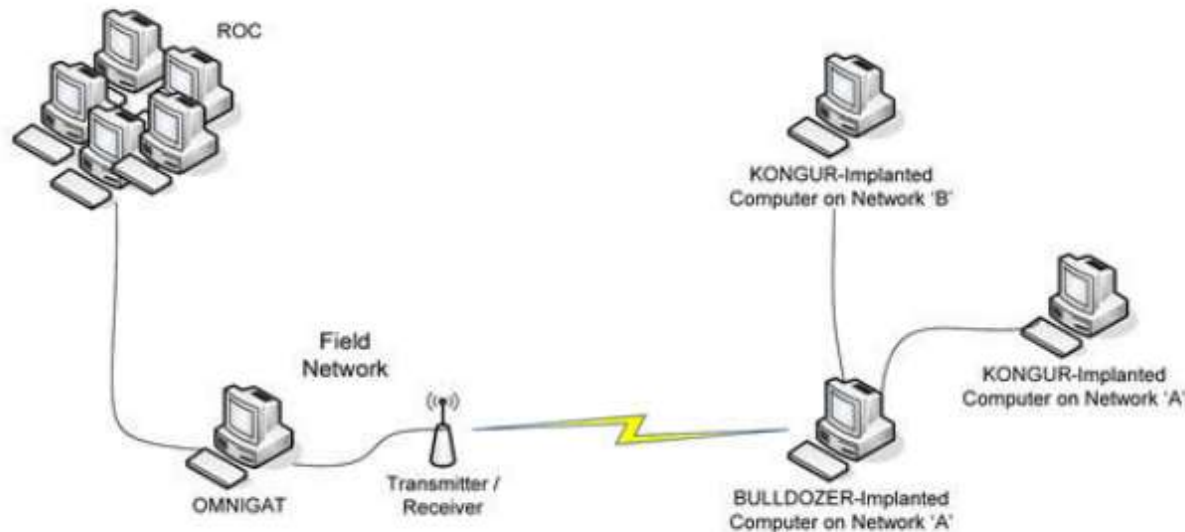


GINSU

ANT Product Data

(TS//SI//REL) GINSU provides software application persistence for the CNE implant, KONGUR, on target systems with the PCI bus hardware implant, BULLDOZER.

06/20/08



(TS//SI//REL) GINSU Extended Concept of Operations

(TS//SI//REL) This technique supports any desktop PC system that contains at least one PCI connector (for BULLDOZER installation) and Microsoft Windows 9x, 2000, 2003, XP, or Vista.



BULLDOZER

FPGA

USB3380

86duino

Intel Galileo



Non-Transparent Bridge
(NTB)



bplus.com.tw



HOWLERMONKEY

ANT Product Data

(TS//SI//REL) HOWLERMONKEY is a custom Short to Medium Range Implant RF Transceiver. It is used in conjunction with a digital core to provide a complete implant.

08/05/08

HOWLERMONKEY -
SUTURESAILOR



1.23" (31.25 mm)
x 0.48" (12.2 mm)

HOWLERMONKEY - YELLOWPIN



2" (50.8 mm) x 0.45" (11.5 mm)

(Actual Size)

HOWLERMONKEY -
SUTURESAILOR



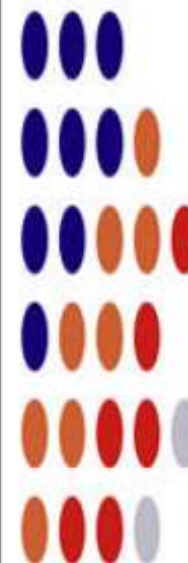
1.20" (30.5 mm)
x 0.23" (6 mm)

HOWLERMONKEY -
FIREWALK



0.63" (16 mm) x
0.63" (16 mm)

(TS//SI//REL) HOWLERMONKEY is a COTS-based transceiver designed to be compatible with CONJECTURE/SPECULATION networks and STRIKEZONE devices running a HOWLERMONKEY personality. PCB layouts are tailored to individual implant space requirements and can vary greatly in form factor.



HOWLERMONKEY

YARD Stick One



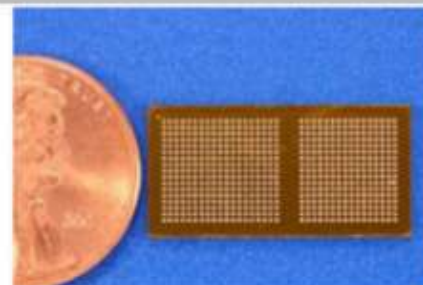
Ubertooth
Bluetooth module
any wireless
transceiver IC

So cool! So connected!

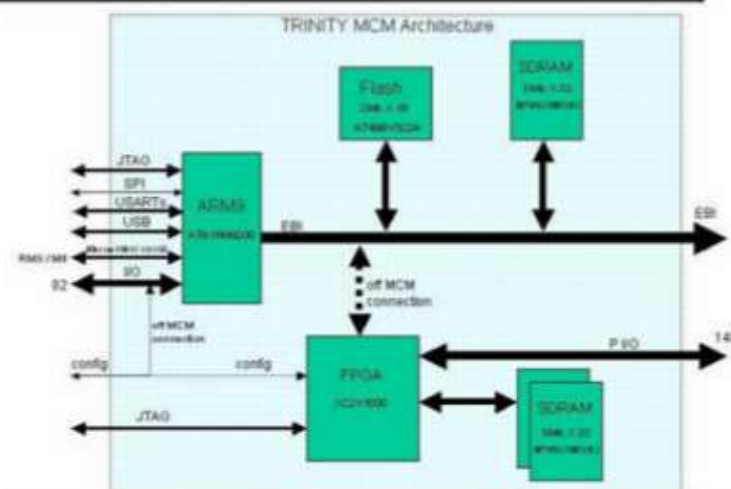


08/05/08

Technical drawing of a rectangular plate. The drawing shows a top view and a side view. The top view is a rectangle with a width of 4'80 ± 0.010 and a length of 8'300 ± 0.012. The side view shows a thickness of 2'240 ± 0.004. The drawing includes several dimension lines and tolerances. The width is 4'80 ± 0.010. The length is 8'300 ± 0.012. The thickness is 2'240 ± 0.004. There are also dimension lines for the distance from the edges to the center of the plate, which are 2'197 ± 0.4 and 2'197 ± 0.4. The drawing is labeled with '2'197 (5.4)' and '2'197 (5.4)'.



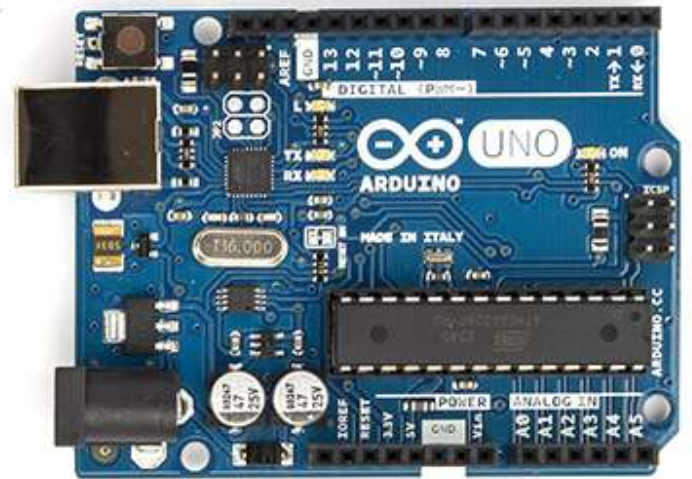
uController	Flash	SDRAM (3)	FPGA
ARM 9 180 Mhz	AT49BV322A 4 MBytes	MT48LC8M32 96 MBytes	XC2V1000 1M gates



TRINITY

Arduino

BangleBone Black
or
any microcontroller!



also JUNIORMINT, MAESTRO

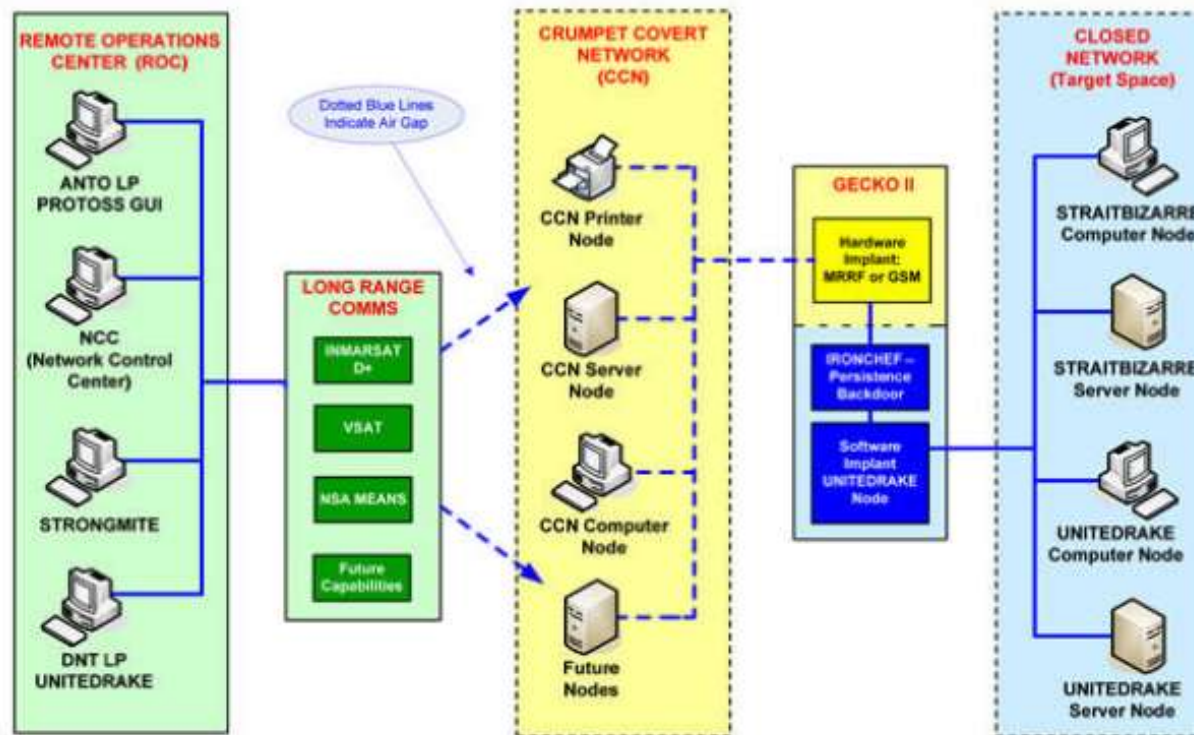


IRONCHEF

ANT Product Data

(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

07/14/08



(TS//SI//REL) IRONCHEF Extended Concept of Operations

(TS//SI//REL) This technique supports the HP Proliant 380DL G5 server, onto which a hardware implant has been installed that communicates over the I²C Interface (WAGONBED).



WAGONBED

Any microcontroller with
I²C

(Arduino, BeagleBone Black,
etc.)



CROSSBEAM

ANT Product Data

(TS//SI//REL) CROSSBEAM is a GSM module that mates a modified commercial cellular product with a WAGONBED controller board.

08/05/08

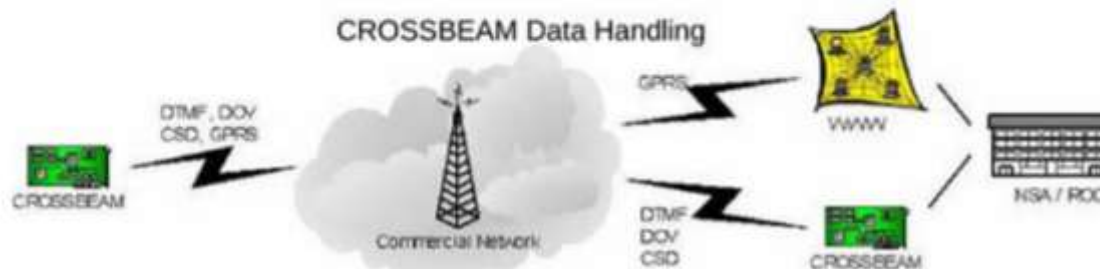


(TS//SI//REL) CROSSBEAM is a reusable CHIMNEYPOOL-compliant GSM communications module capable of collecting and compressing voice data. CROSSBEAM can receive GSM voice, record voice data, and transmit the received information via connected modules or 4 different GSM data modes (GPRS, Circuit Switched Data, Data Over Voice, and DTMF) back to a secure facility. The CROSSBEAM module consists of a standard ANT architecture embedded computer, a specialized phone component, a customized software controller suite and an optional DSP (ROCKYKNOB) if using Data Over Voice to transmit data.

CROSSBEAM Voice Handling



CROSSBEAM Data Handling



CROSSBEAM

GSM
module



sparkfun.com

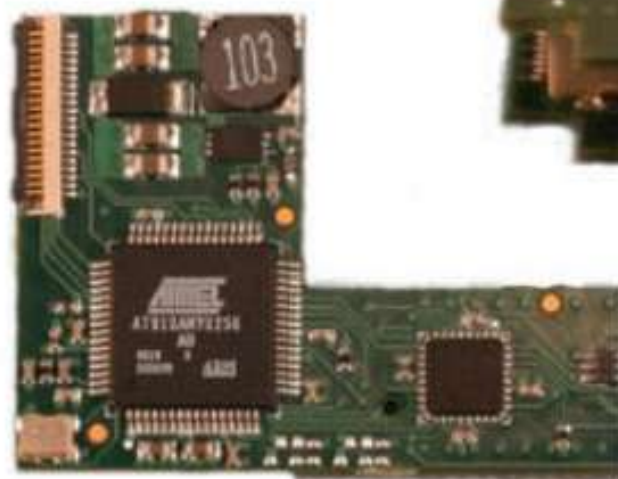


GODSURGE

ANT Product Data

(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

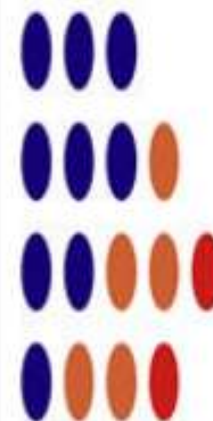
06/20/08



(TS//SI//REL) FLUXBABBITT Hardware
Implant for PowerEdge 1950



(TS//SI//REL) FLUXBABBITT Hardware
Implant for PowerEdge 2950



FLUXBABBIT

Who does x86

JTAG?

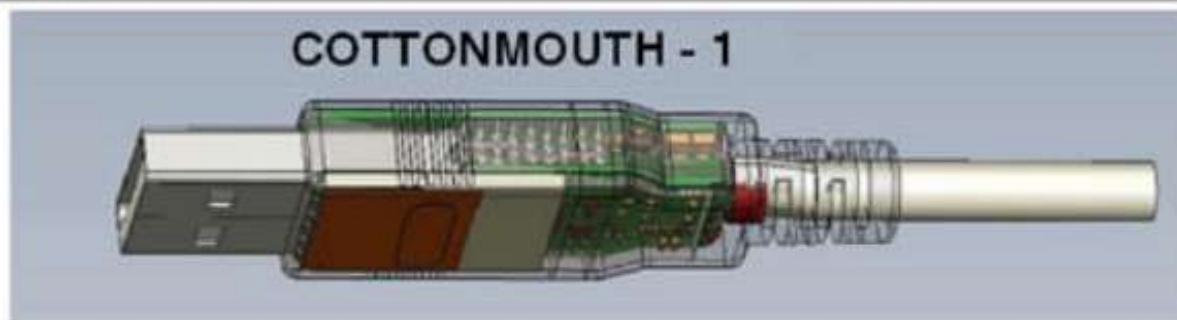


COTTONMOUTH-I

ANT Product Data

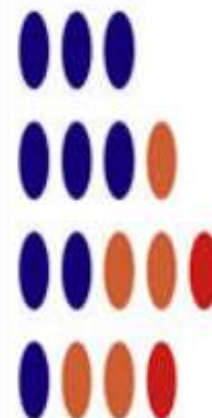
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

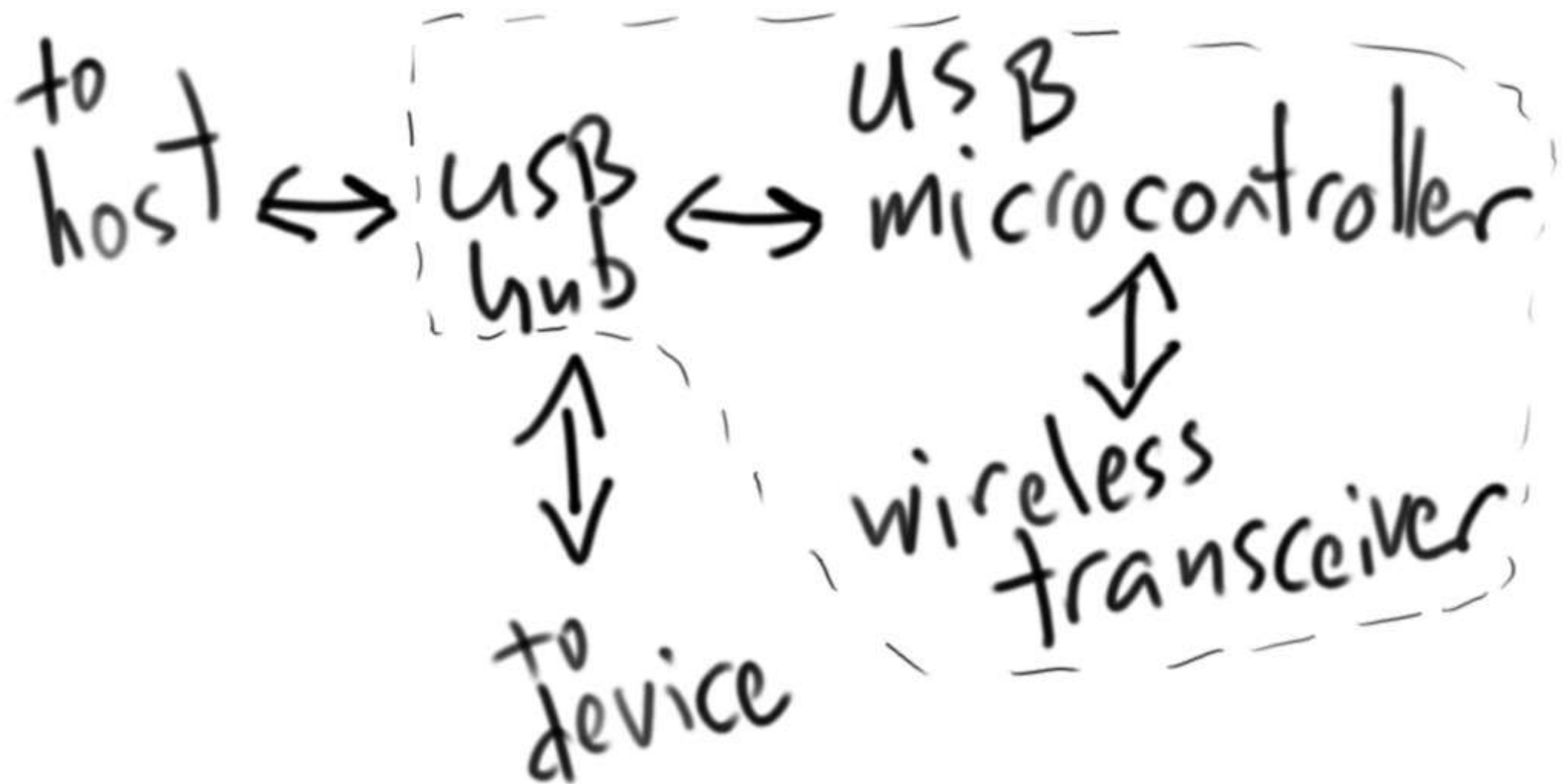


(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

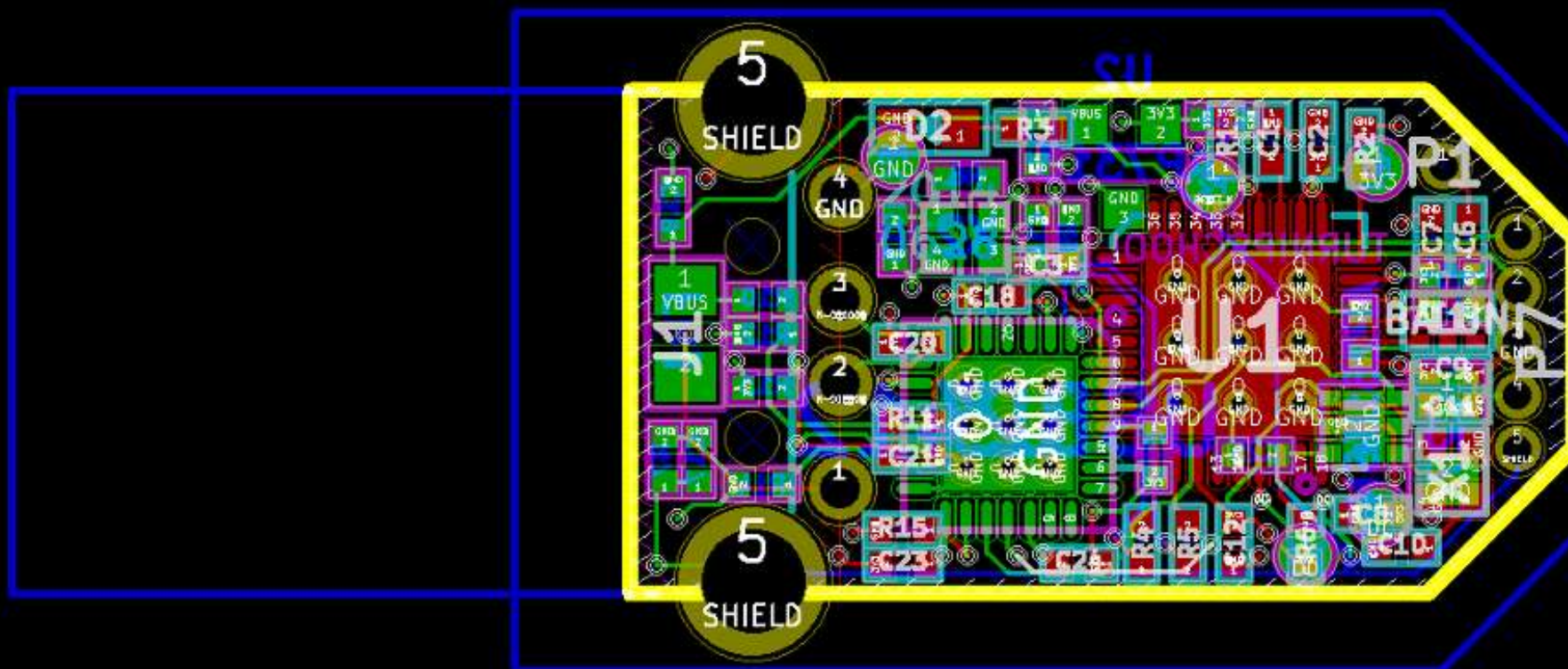


COTTONMOUTH-I





Track 5.0 mils * Via 18.0 mils * Grid 1.0 Zoom 38100



Pads	Vias	trackSegm	Nodes	Nets	Links	Connect	Unconnected
232	54	385	205	44	162	162	0

D? not found

Z 38100 X 4.829000 Y 3.990000 dx 4.829000



COTTONMOUTH-II

ANT Product Data

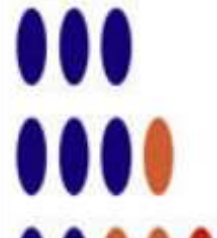
(TS//SI//REL) COTTONMOUTH-II (CM-II) is a Universal Serial Bus (USB) hardware Host Tap, which will provide a covert link over USB link into a targets network. CM-II is intended to be operate with a long haul relay subsystem, which is co-located within the target equipment. Further integration is needed to turn this capability into a deployable system.

08/05/08



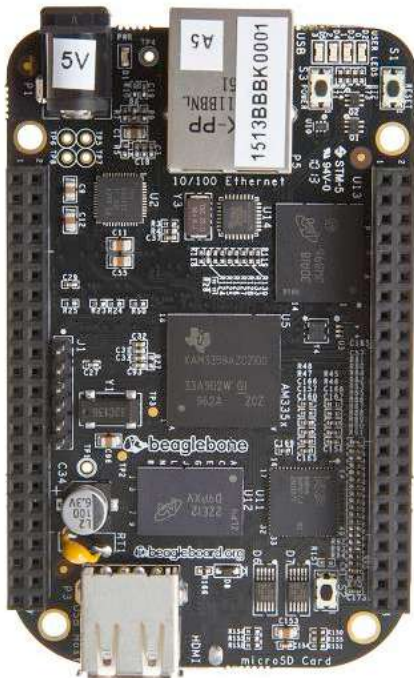
(TS//SI//REL) CM-II will provide software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. CM-II will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-II will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay concealed somewhere within the target chassis. A USB 2.0 HS hub with switches is concealed in a dual stacked USB connector, and the two parts are hard-wired, providing a intra-chassis link. The long haul relay provides the wireless bridge into the target's network.



COTTON MOUTH - II

BeagleBone Black
with USBProxy



or
Daisho

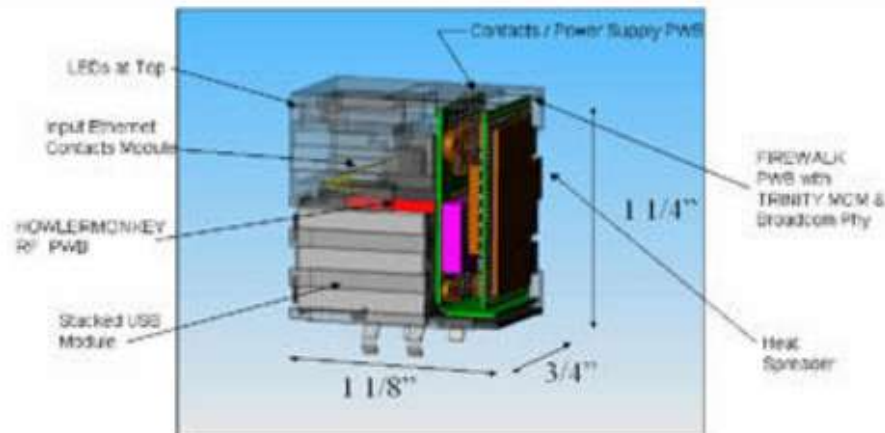


FIREWALK

ANT Product Data

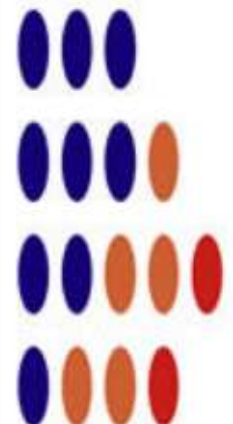
(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.

08/05/08



(TS//SI//REL) FIREWALK is a bi-directional 10/100/1000bT (Gigabit) Ethernet network implant residing within a dual stacked RJ45 / USB connector. FIREWALK is capable of filtering and egressing network traffic over a custom RF link and injecting traffic as commanded; this allows an ethernet tunnel (VPN) to be created between target network and the ROC (or an intermediate redirector node such as DNT's DANDERSPRITZ tool.) FIREWALK allows active exploitation of a target network with a firewall or air gap protection.

(TS//SI//REL) FIREWALK uses the HOWLERMONKEY transceiver for back-end communications. It can communicate with an LP or other compatible HOWLERMONKEY based ANT products to increase RF range through multiple hops.



FIREWALK

Daisho

AM335x
starter Kit

OpenWRT



Software

Implants

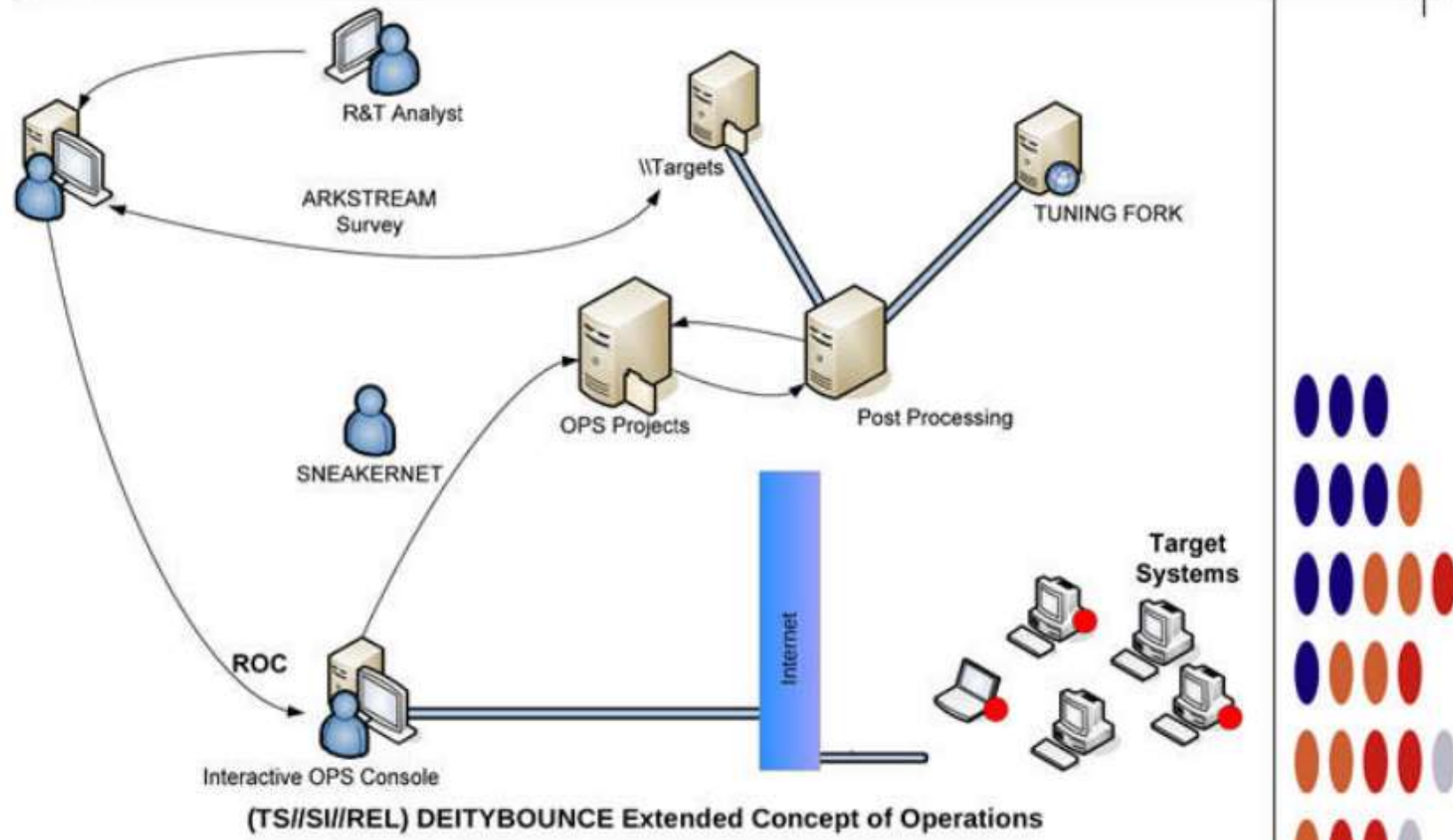


DEITYBOUNCE

ANT Product Data

(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

06/20/08



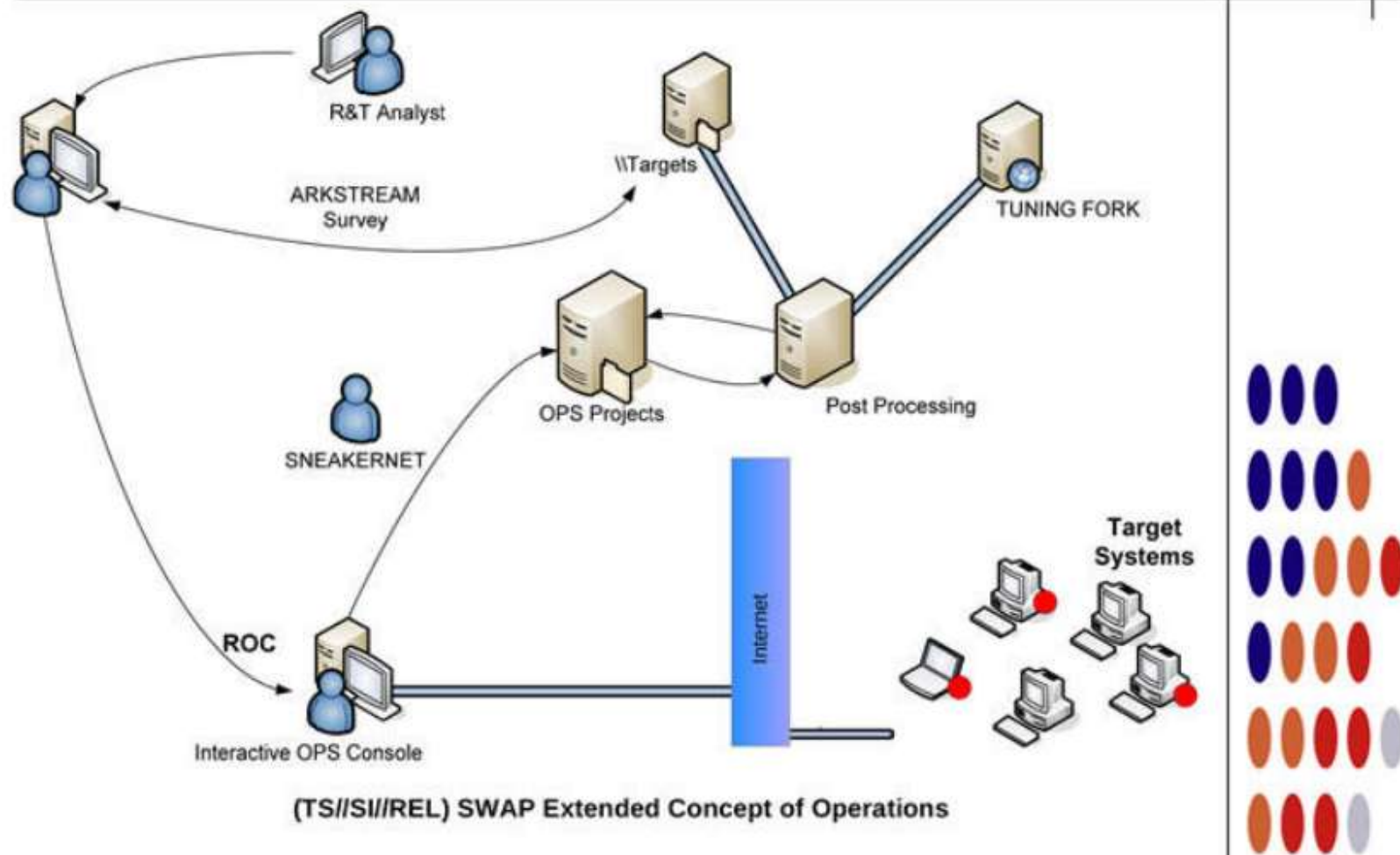


SWAP

ANT Product Data

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.

06/20/08



(TS//SI//REL) SWAP Extended Concept of Operations

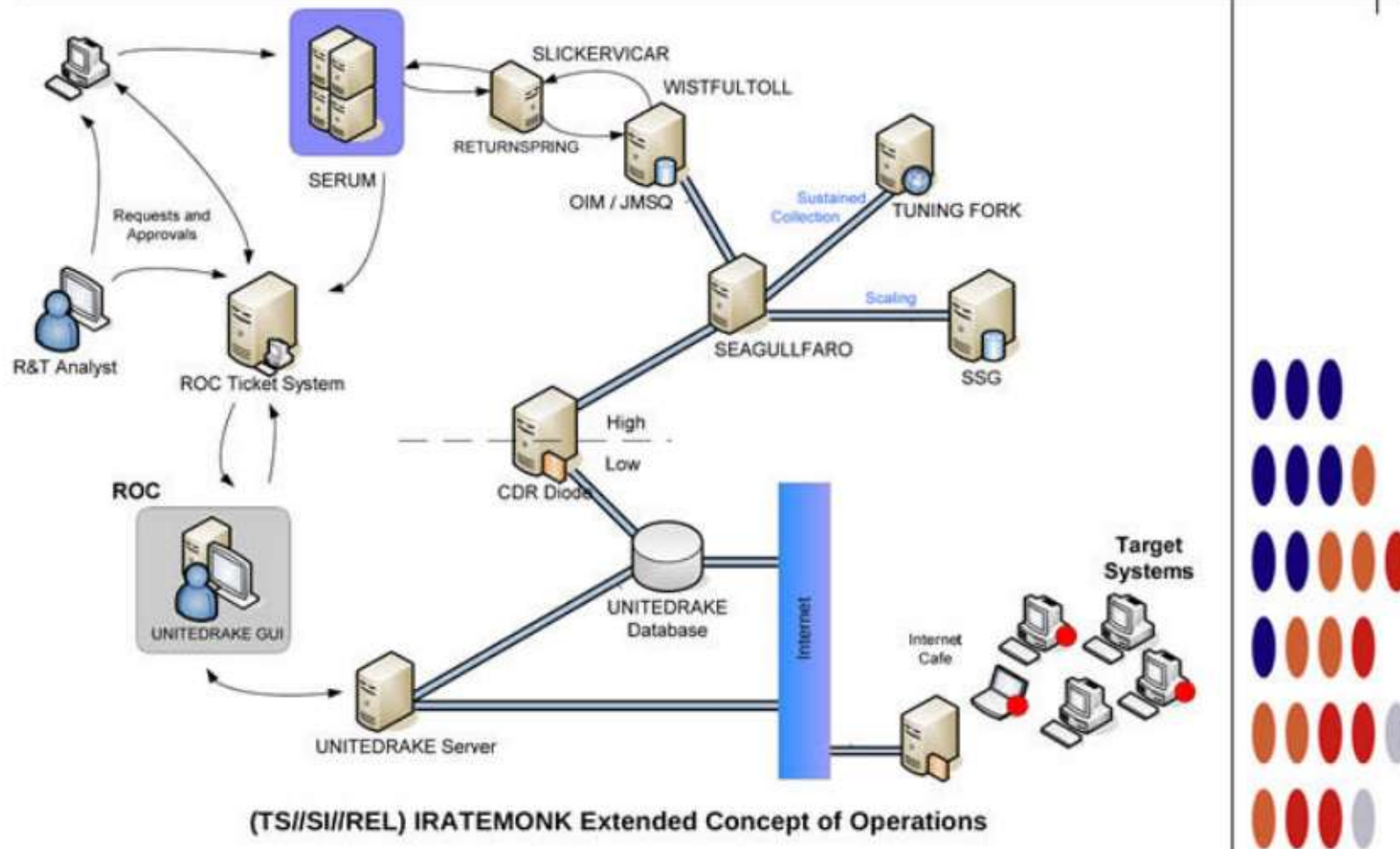


IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08



(TS//SI//REL) IRATEMONK Extended Concept of Operations

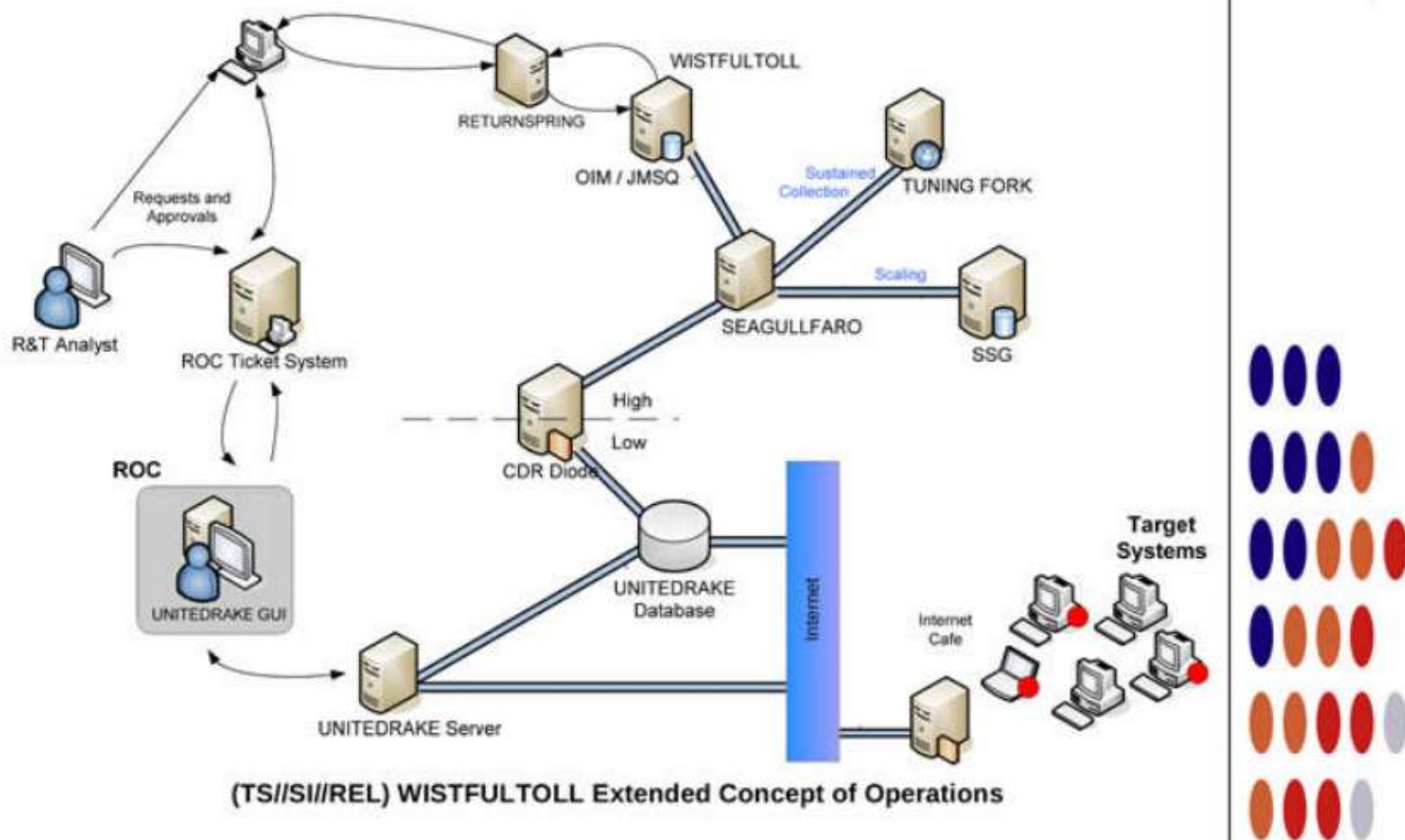


WISTFULTOLL

ANT Product Data

(TS//SI//REL) WISTFULTOLL is a UNITEDRAKE and STRAITBIZZARE plug-in used for harvesting and returning forensic information from a target using Windows Management Instrumentation (WMI) calls and Registry extractions.

06/20/08



(TS//SI//REL) This plug-in supports systems running Microsoft Windows 2000, 2003, and XP.

(TS//SI//REL) Through remote access or interdiction, WISTFULLTOLL is executed as either a UNITEDRAKE or STRAITBAZZARE plug-in or as a stand-alone executable. If used remotely, the extracted information is sent back to NSA through UNITEDRAKE or STRAITBAZZARE. Execution via interdiction may be accomplished by non-technical operator through use of a USB thumb drive, where extracted information will be saved to that thumb drive.



SOMBERKNAVE

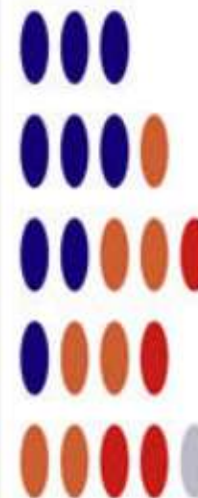
ANT Product Data

(TS//SI//REL) SOMBERKNAVE is Windows XP wireless software implant that provides covert internet connectivity for isolated targets.

08/05/08

(TS//SI//REL) SOMBERKNAVE is a software implant that surreptitiously routes TCP traffic from a designated process to a secondary network via an unused embedded 802.11 network device. If an Internet-connected wireless Access Point is present, SOMBERKNAVE can be used to allow OLYMPUS or VALIDATOR to "call home" via 802.11 from an air-gapped target computer. If the 802.11 interface is in use by the target, SOMBERKNAVE will not attempt to transmit.

(TS//SI//REL) Operationally, VALIDATOR initiates a call home. SOMBERKNAVE triggers from the named event and tries to associate with an access point. If connection is successful, data is sent over 802.11 to the ROC. VALIDATOR receives instructions, downloads OLYMPUS, then disassociates and gives up control of the 802.11 hardware. OLYMPUS will then be able to communicate with the ROC via SOMBERKNAVE, as long as there is an available access point.



Persistent Backdoors (routers)



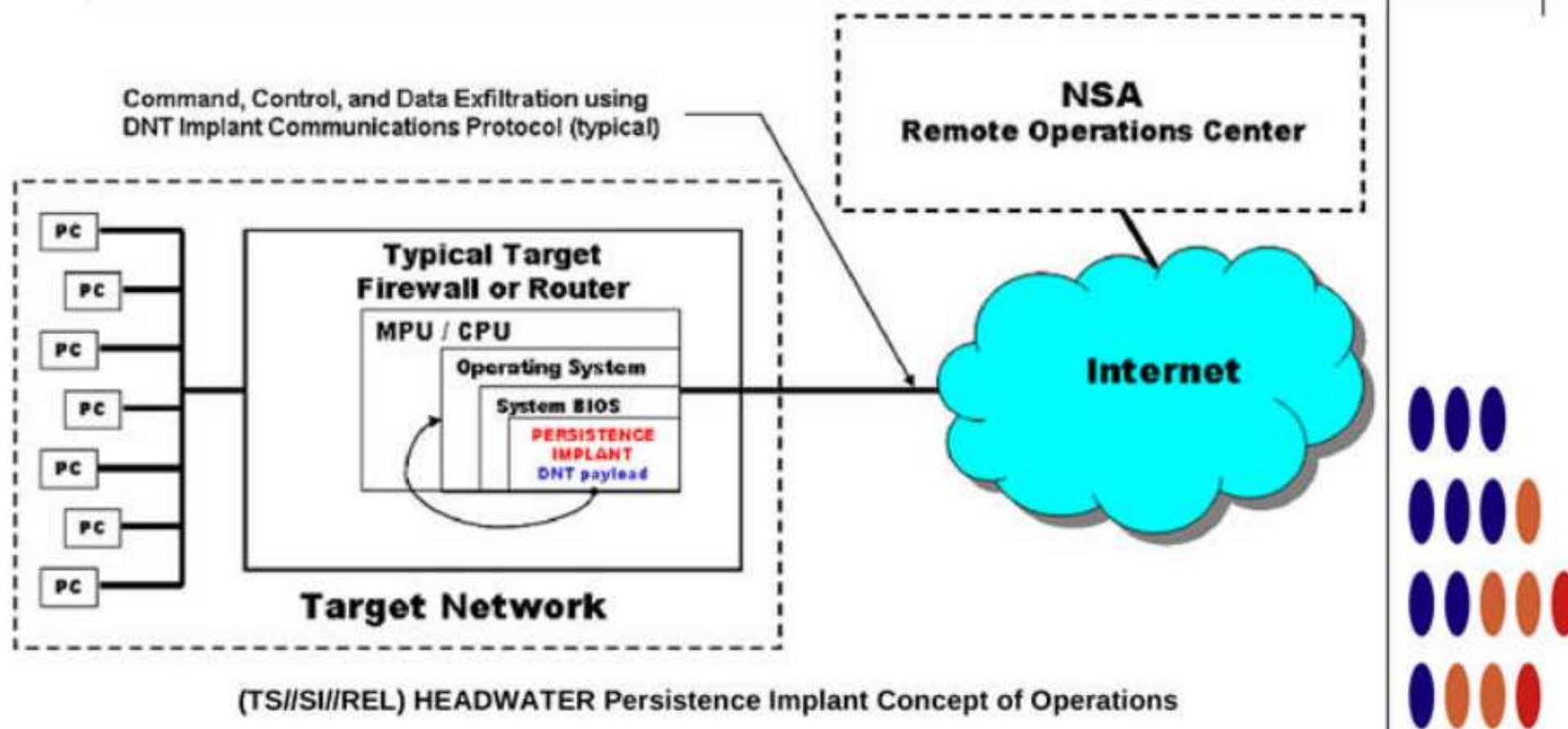


HEADWATER

ANT Product Data

(TS//SI//REL) HEADWATER is a Persistent Backdoor (PBD) software implant for selected Huawei routers. The implant will enable covert functions to be remotely executed within the router via an Internet connection.

06/24/08



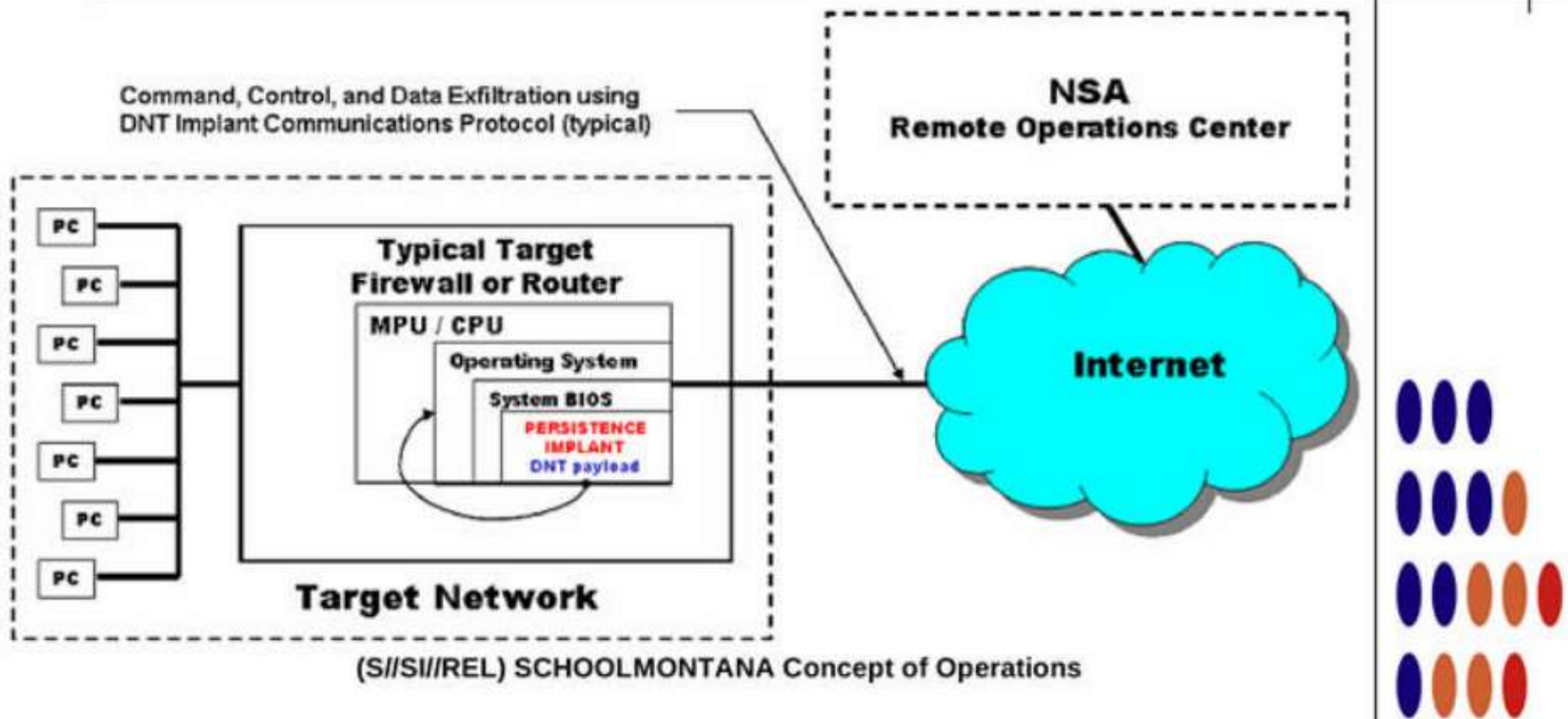


SCHOOLMONTANA

ANT Product Data

(TS//SI//REL) SCHOOLMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



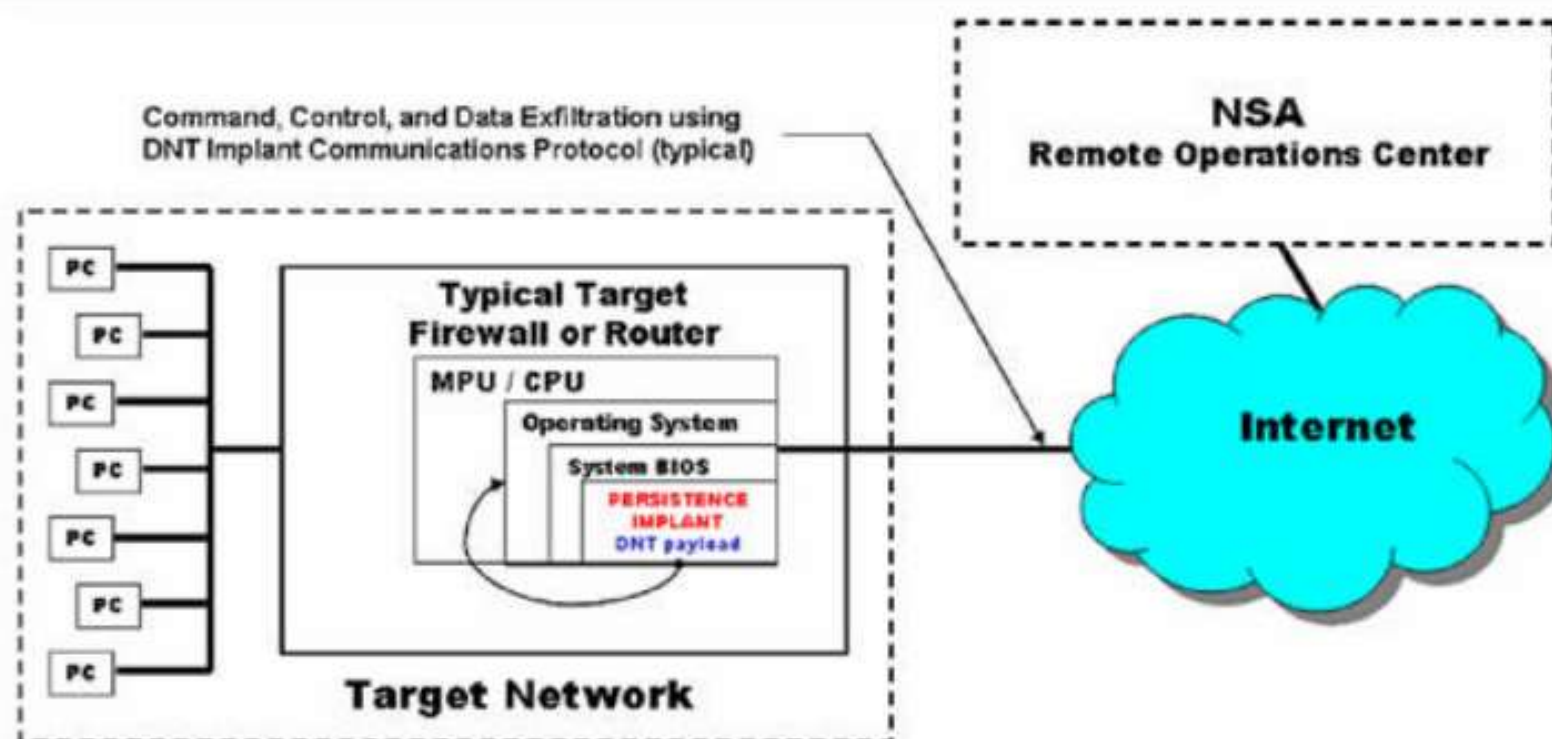


SIERRAMONTANA

ANT Product Data

(TS//SI//REL) SIERRAMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



(S//SI//REL) SIERRAMONTANA Concept of Operations

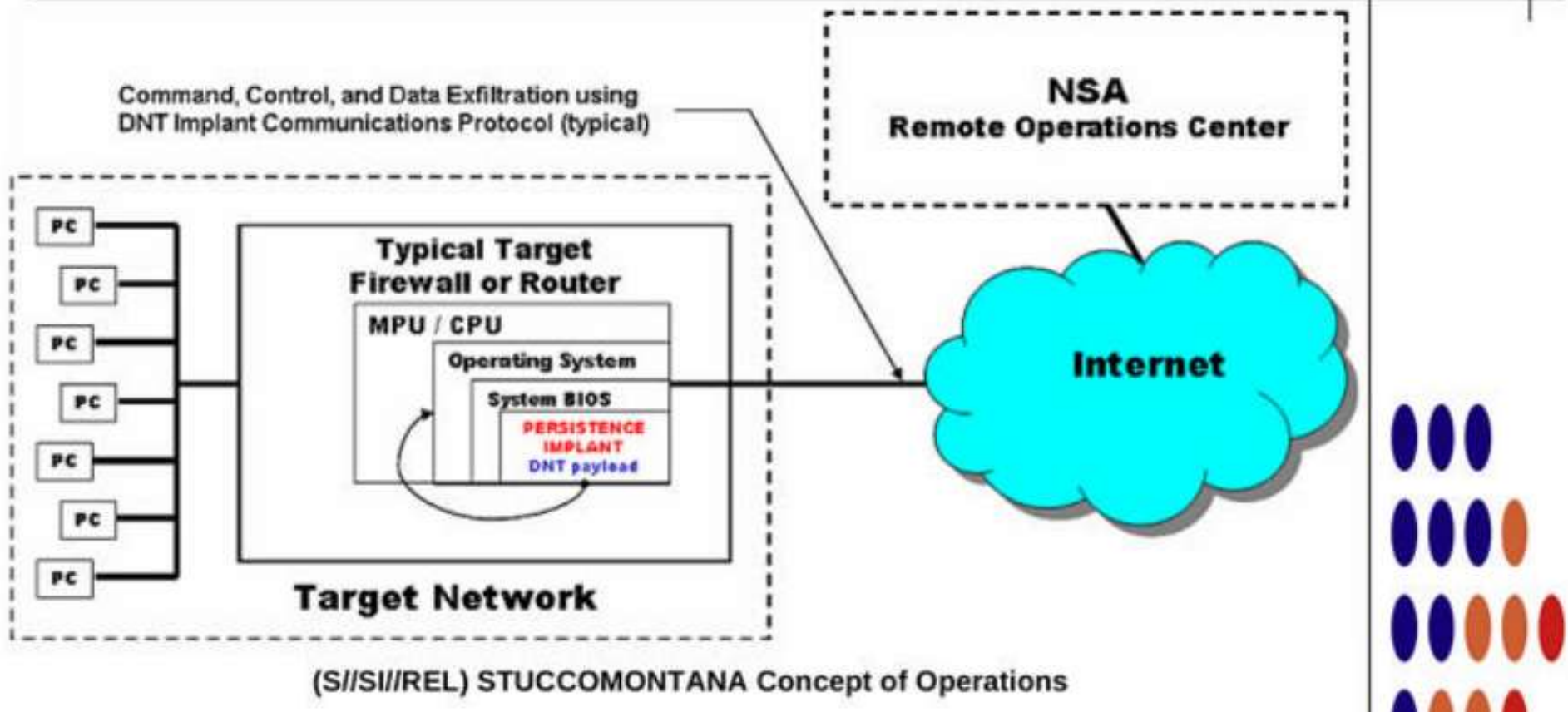


STUCCOMONTANA

ANT Product Data

(TS//SI//REL) STUCCOMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

06/24/08



Persistent
Backdoors
(firewalls)

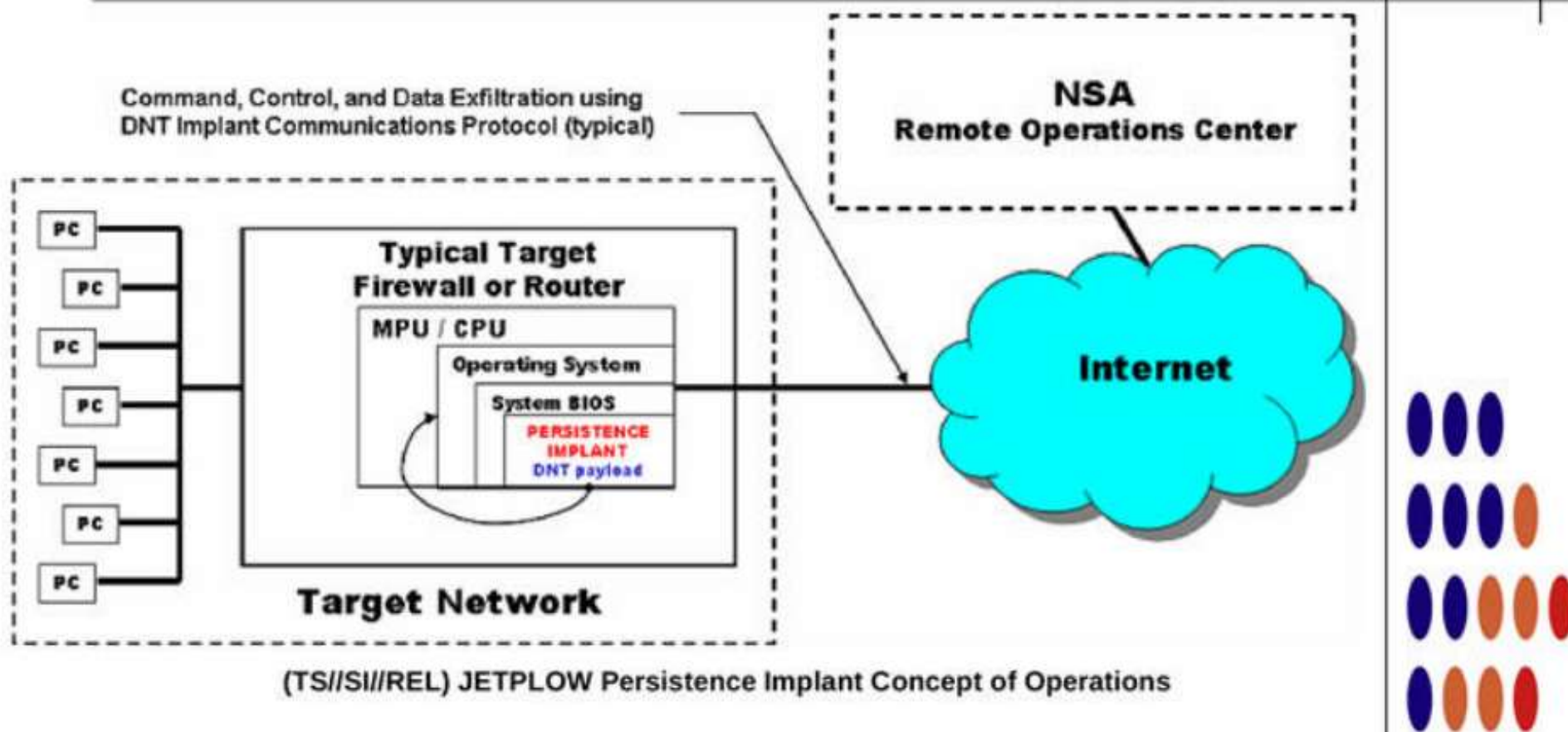


JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



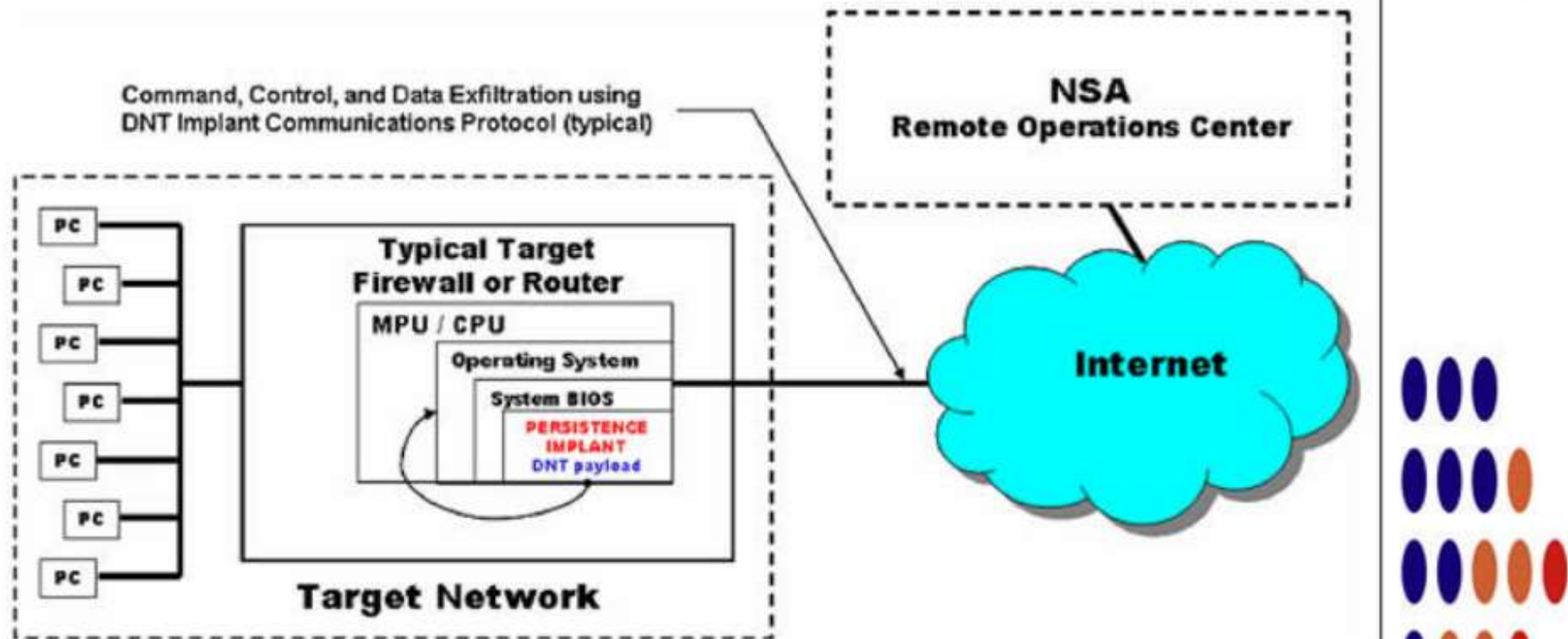


HALLUXWATER

ANT Product Data

(TS//SI//REL) The HALLUXWATER Persistence Back Door implant is installed on a target Huawei Eudemon firewall as a boot ROM upgrade. When the target reboots, the PBD installer software will find the needed patch points and install the back door in the inbound packet processing routine.

06/24/08



(TS//SI//REL) HALLUXWATER Persistence Implant Concept of Operations

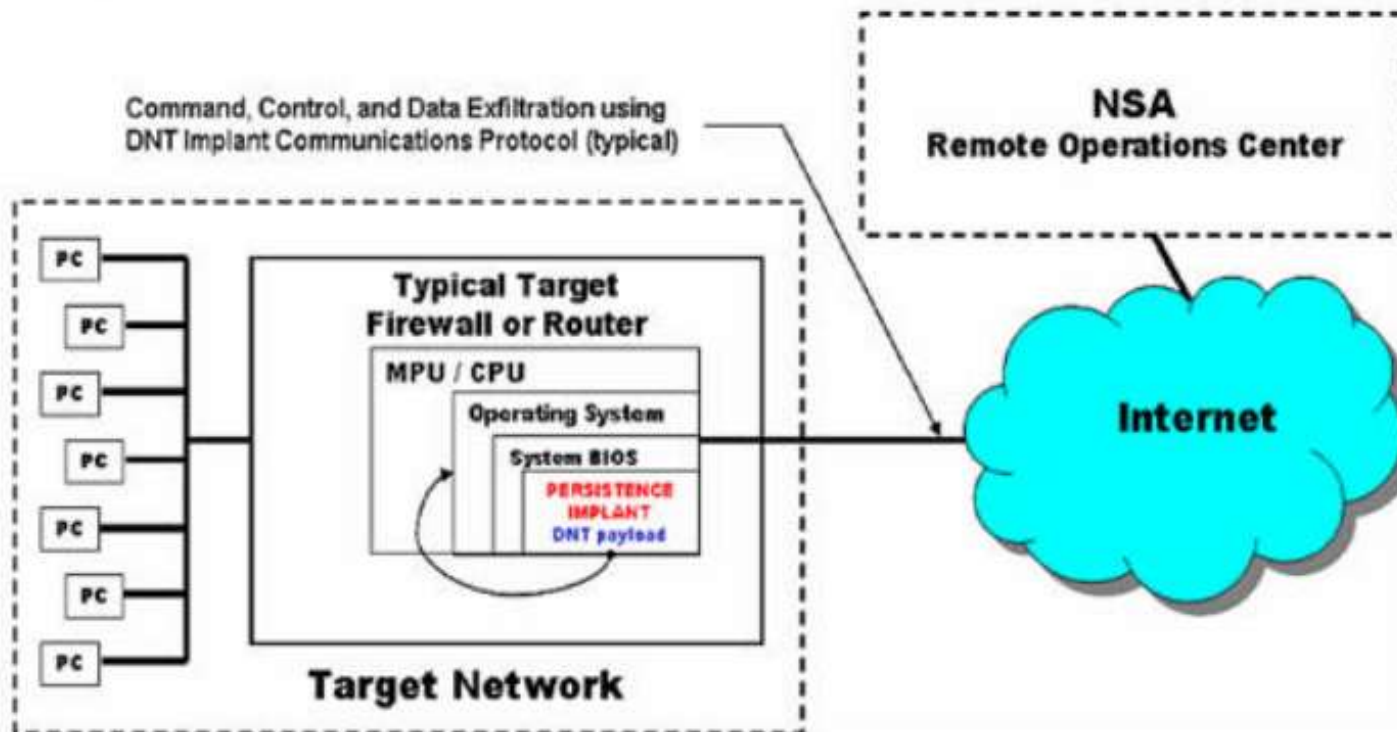


FEEDTROUGH

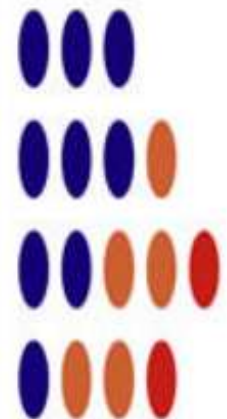
ANT Product Data

(TS//SI//REL) FEEDTROUGH is a persistence technique for two software implants, DNT's BANANAGLEE and CES's ZESTYLEAK used against Juniper Netscreen firewalls.

06/24/08



(S//SI//REL) Persistence Operational Scenario



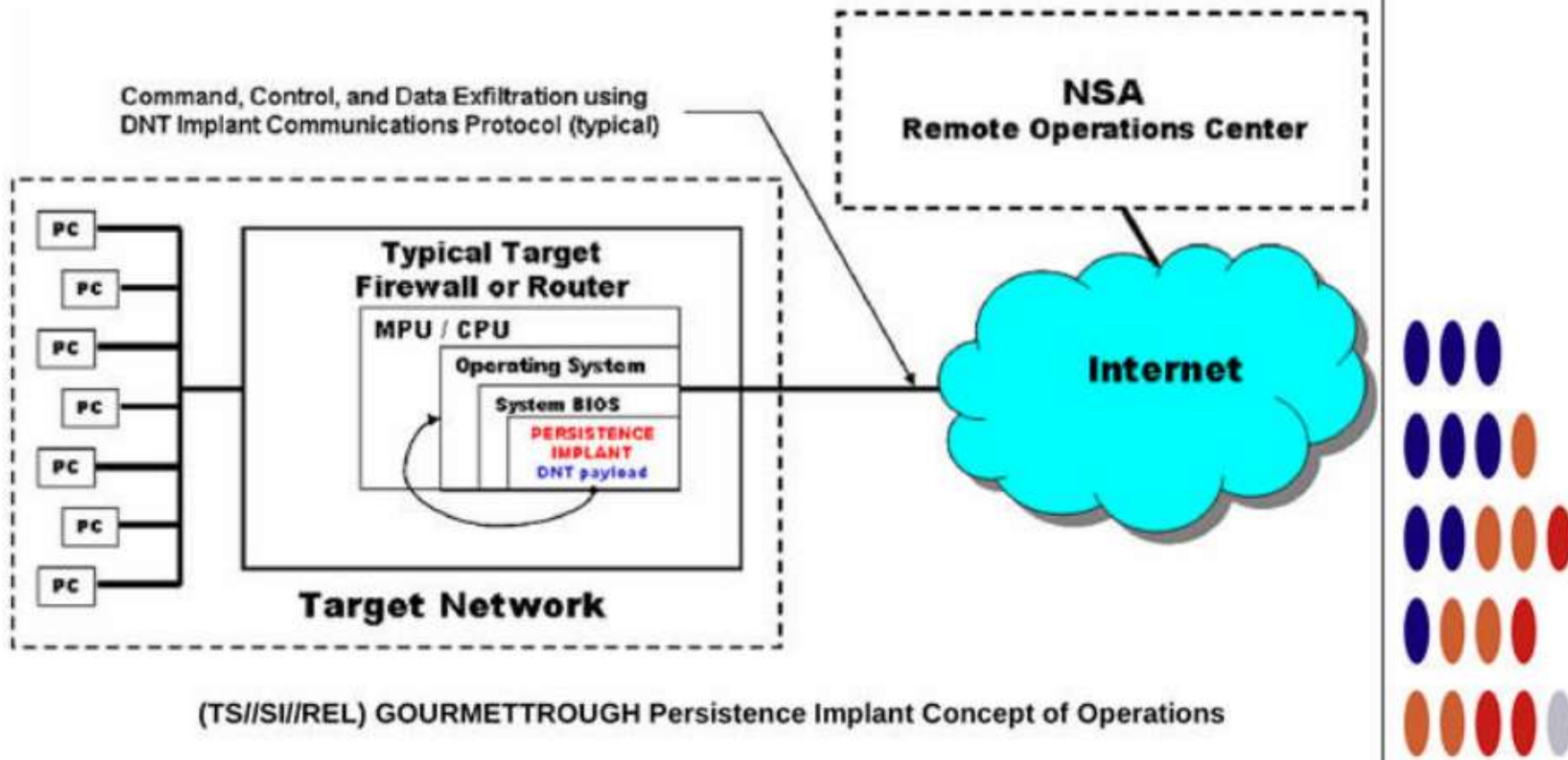


GOURMETTROUGH

ANT Product Data

(TS//SI//REL) GOURMETTROUGH is a user configurable persistence implant for certain Juniper firewalls. It persists DNT's BANANAGLEE implant across reboots and OS upgrades. For some platforms, it supports a minimal implant with beaconing for OS's unsupported by BANANAGLEE.

06/24/08



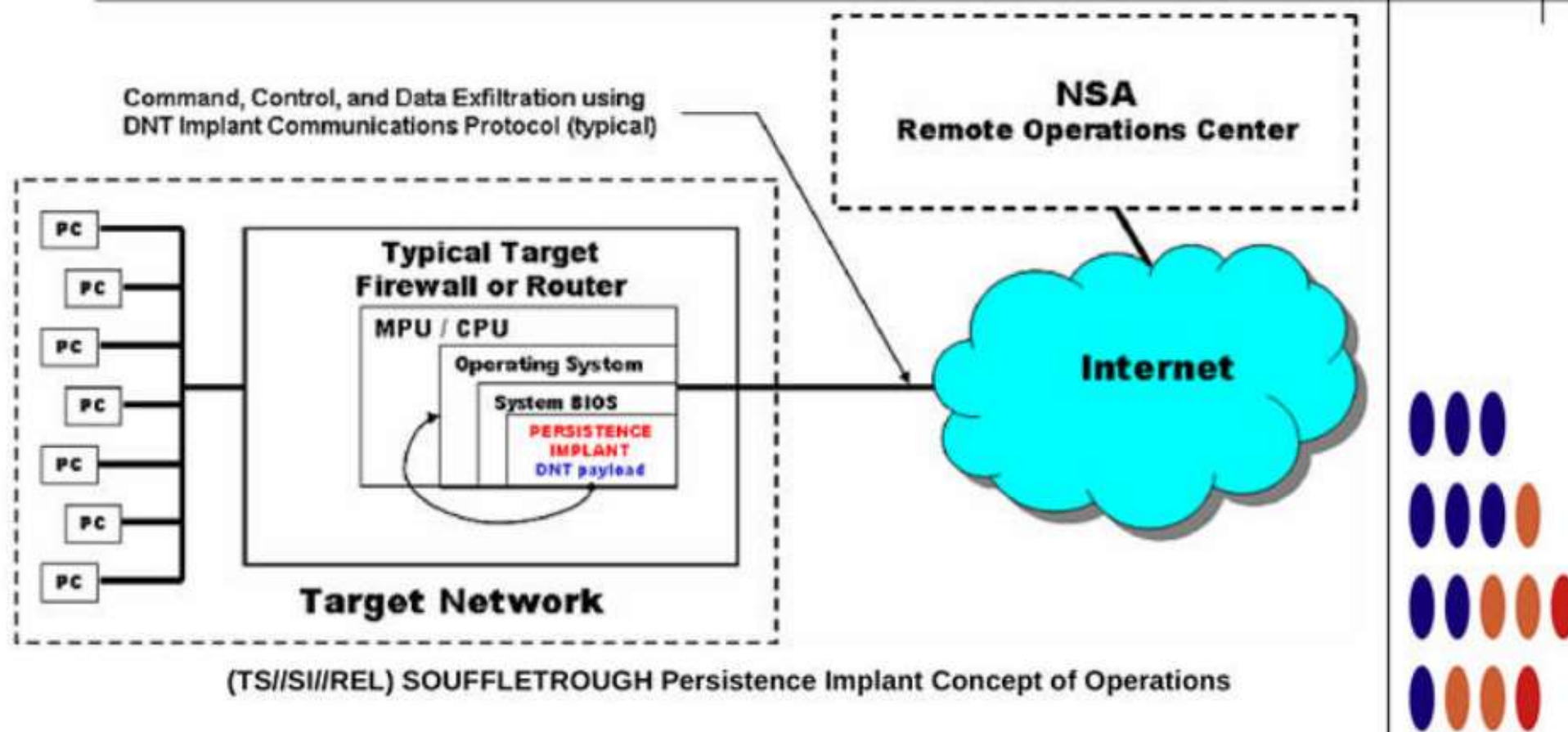


SOUFFLETROUGH

ANT Product Data

(TS//SI//REL) SOUFFLETROUGH is a BIOS persistence implant for Juniper SSG 500 and SSG 300 series firewalls. It persists DNT's BANANAGLEE software implant. SOUFFLETROUGH also has an advanced persistent back-door capability.

06/24/08

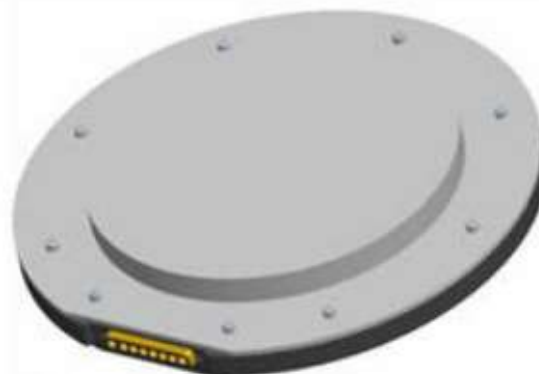


Direction Finding



(S//SI//REL) Direction Finding on HollowPoint Platform

01/27/09



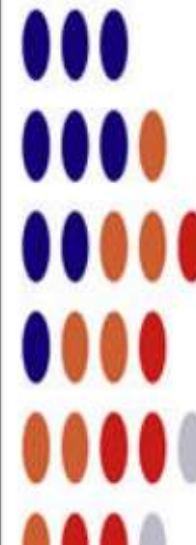
(S//SI//REL) HOLLOWPOINT SDR Platform and Antenna

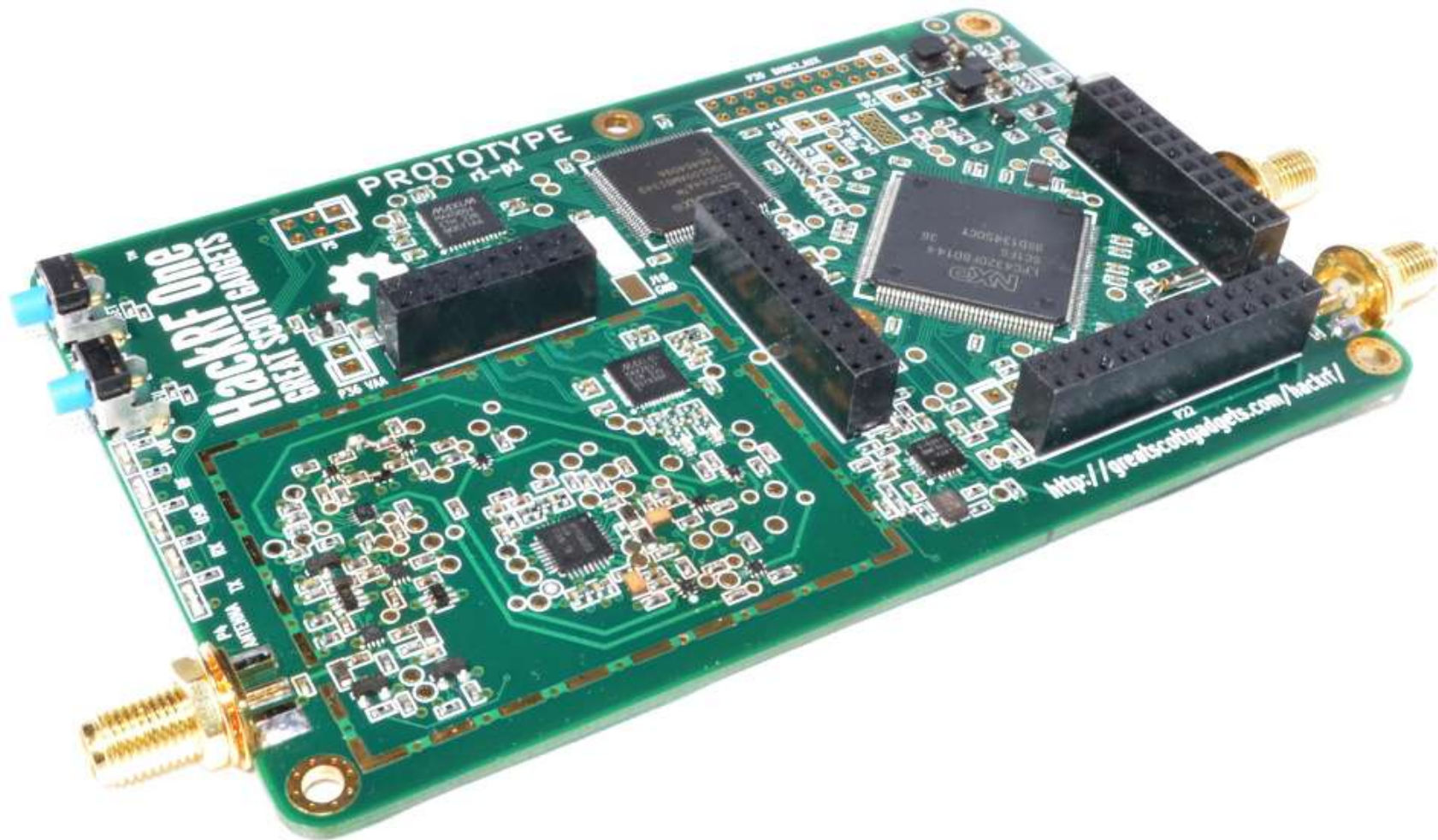
(S//SI) The ENTOURAGE application leverages the 4 Software Defined Radio (SDR) units in the HOLLOWPOINT platform. This capability provides an "Artemis-like" capability for waveforms of interest (2G,3G,others). The ENTOURAGE application works in conjunction with the NEBULA active interrogator as part of the Find/Fix/Finish capabilities of the GALAXY program.

➤ (S//SI//REL) Enclosure:

- Software Defined Radio System
- Operating range 10MHz – 4GHz
- 4 Receive paths, all synchronized

- 1.8"H x 8.0"W x 8.0"D
- Approximately 3 lbs
- 15 Watts





HackRF One



WATERWITCH

Handheld Finishing Tool

(S//SI) Hand held finishing tool used for geolocating targeted handsets in the field.

07/30/08

(S//SI) Features:

- Split display/controller for flexible deployment capability
- External antenna for DFing target; internal antenna for communication with active interrogator
- Multiple technology capability based on SDR Platform; currently UMTS, with GSM and CDMA2000 under development
- Approximate size 3" x 7.5" x 1.25" (radio), 2.5" x 5" x 0.75" (display); radio shrink in planning stages
- Display uses E-Ink technology for low light emissions



(S//SI) WATERWITCH Handset DF Set

(S//SI) Tactical Operators use WATERWITCH to locate handsets (last mile) where handset is connected to Typhon or



HackRF PortaPack





GENESIS

Covert SIGINT Transceiver

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

01/27/09



(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

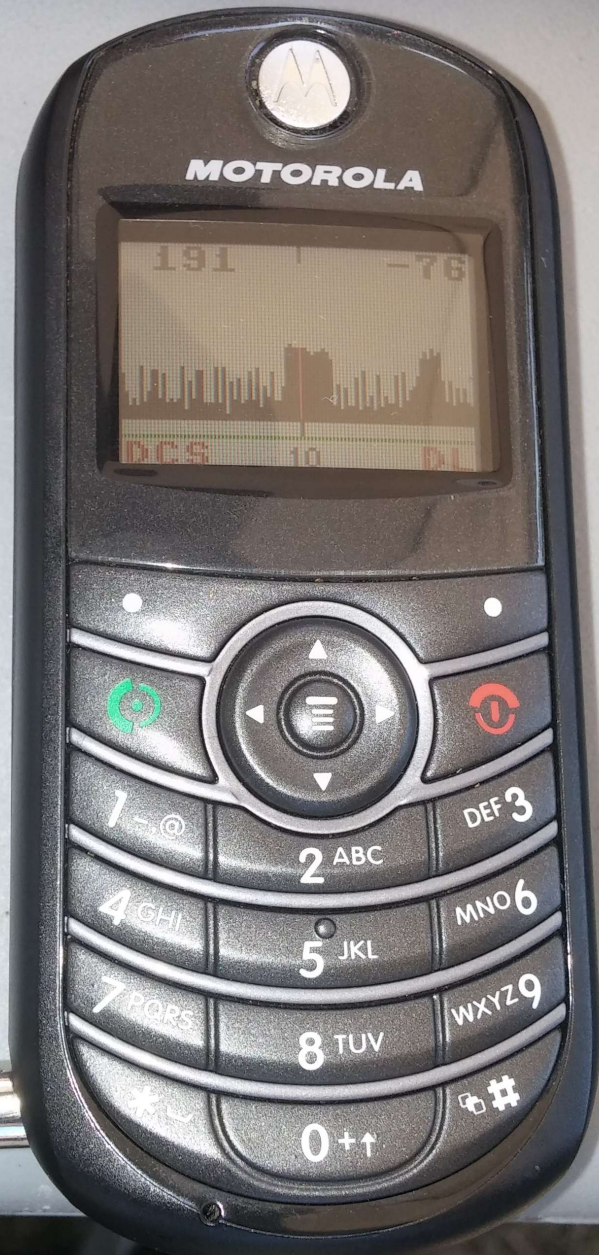
➤ (S//SI//REL) Features:

- Concealed SDR with Handset Menu Interface
- Spectrum Analyzer Capability
- Find/Fix/Finish Capability
- Integrated Ethernet

➤ (S//SI//REL) Future Enhancements:

- 3G Handset Host Platform
- Additional Host Platforms
- Increased Memory Capacity
- Additional Find/Fix/Finish Capabilities





OsmocomBB
RSSI



The Smart Software Radio Device

Welcome to the Whitebox Software Radio Project, a cross between a smartphone and a software defined radio with an open hardware and software license.



So cool! So connected!



Base Stations,

Interrogation

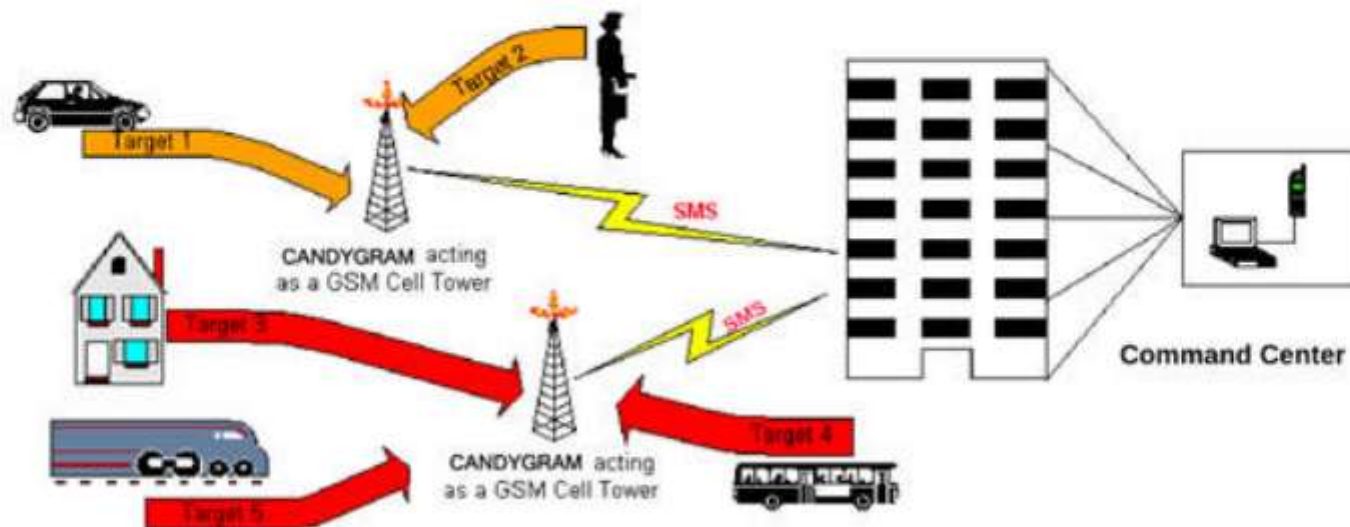


CANDYGRAM

GSM Telephone Tripwire

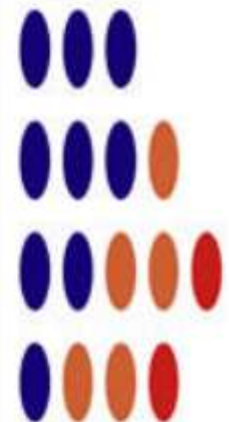
(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08



(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.





CYCLONE Hx9

Base Station Router

(S//SI//FVEY) EGSM (900MHz) macro-class Network-In-a-Box (NIB) system. Uses the existing Typhon GUI and supports the full Typhon feature base and applications.

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



➤ (S//SI//REL) Enclosure:

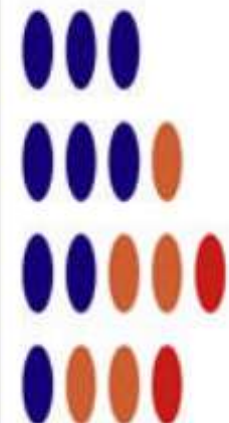
- 3.5"H x 8.5"W x 9"D
- Approximately 8 lbs
- Actively cooled for extreme environments

➤ (S//SI//REL) Cyclone Hx9 System Kit:

- Cyclone Hx9 System
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➤ (S//SI//REL) Features:

- EGSM 900MHz
- Macro-class (+43dBm)
- 32+Km Range
- Optional Battery Kits





EBSR

Low Power GSM Active Interrogator

(S//SI//REL) Multi-purpose, Pico class, tri-band active GSM base station with internal 802.11/GPS/handset capability.

01/27/09

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



➤ (S//SI//REL) EBSR System Kit:

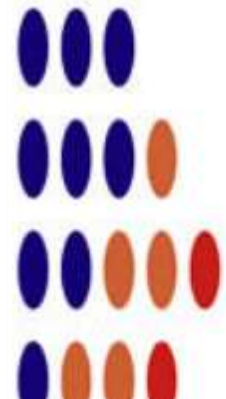
- EBSR System
- AC/DC power converter
- Antennas to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➤ (S//SI//REL) Separately Priced Options:

- 90 WH Lilon Battery Kit

➤ (S//SI//REL) Features:

- LxT Model: 900/1800/1900MHz
- LxU Model: 850/1800/1900MHz
- Pico-class (1Watt) Base station
- Optional Battery Kits
- Highly Mobile and Deployable





NEBULA

Base Station Router

(S//SI//FVEY) Multi-Protocol macro-class Network-In-a-Box (NIB) system. Leverages the existing Typhon GUI and supports GSM, UMTS, CDMA2000 applications. LTE capability currently under development.

01/27/09

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



➤ (S//SI//REL) Features:

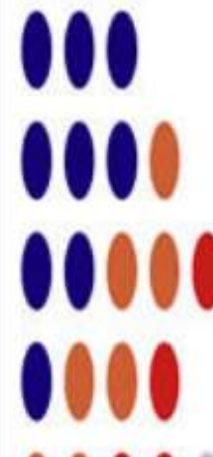
- Dual Carrier System
- EGSM 900MHz
- UMTS 2100MHz
- CDMA2000 1900MHz
- Macro-class Base station

➤ (S//SI//REL) Enclosure:

- 8.5"H x 13.0"W x 16.5"D
- Approximately 45 lbs
- Actively cooled for extreme environments

➤ (S//SI//REL) NEBULA System Kit:

- NEBULA System
- 3 Interchangeable RF bands
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories





TYPHON HX

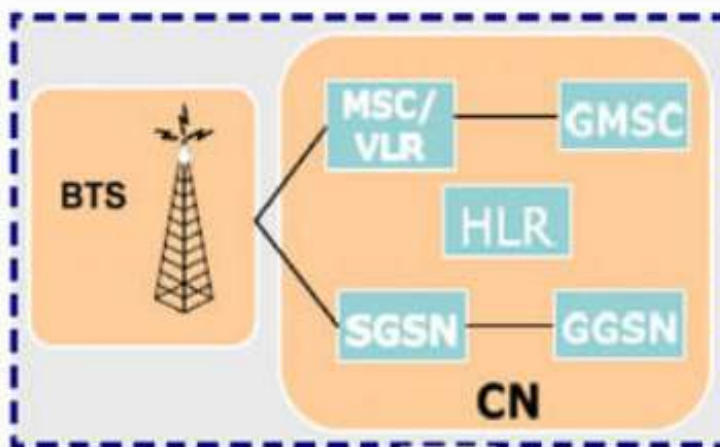
GSM Base Station Router

(S//SI//FVEY) Base Station Router - Network-In-a-Box (NIB) supporting GSM bands 850/900/1800/1900 and associated full GSM signaling and call control.

06/20/08



Typhon Hx BSR

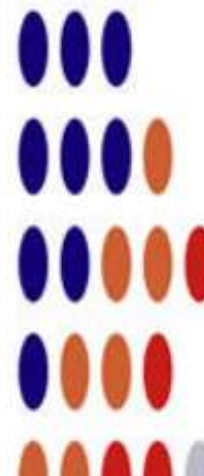
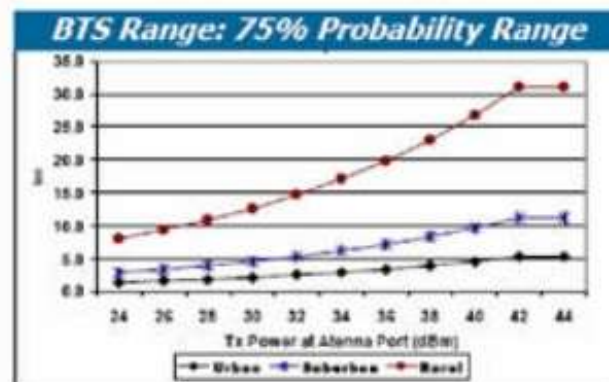


Typhon BSR

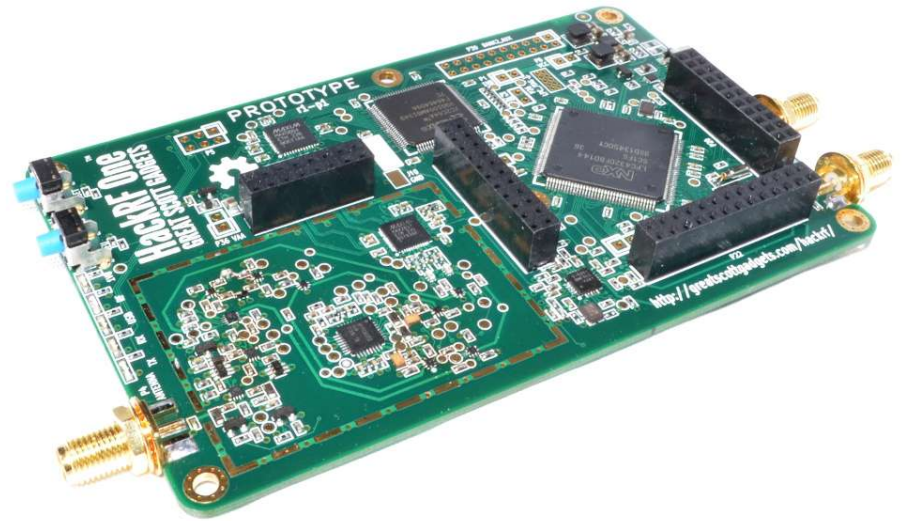
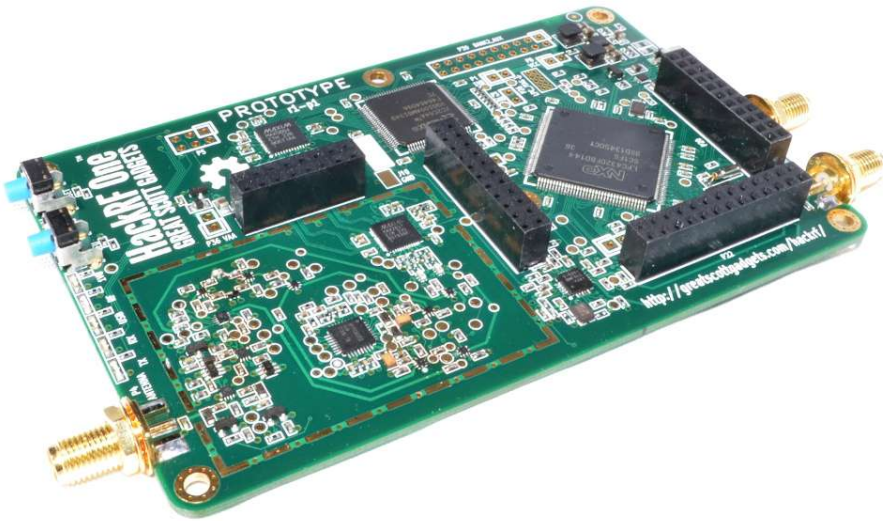
(S//SI//FVEY) Tactical SIGINT elements use this equipment to find, fix and finish targeted handset users.

(S//SI) Target GSM handset registers with BSR unit.

(S//SI) Operators are able to geolocate registered handsets, capturing the user.



HackRF One x2



U_mTRX



fairwaves.co

USRP



ettus.com



The Osmocom project is a family of projects regarding Open **s**ource **m**obile **c**ommunications. It includes software and tools for a variety of mobile communication standards, including GSM, DECT, TETRA and others. Choose from the following project list:

Osmocom { [BB](#) | [OpenBSC](#) | [DECT](#) | [TETRA](#) | [SIMTRACE](#) | [SECURITY](#) | [GMR](#) | [SDR](#) | [OP25](#) | [planet](#) | [lists](#) }

For a more comprehensive list of projects and short descriptions, please check out the [Osmocom Overview](#) page.

[Contact](#)

Mobile
Software
Implants

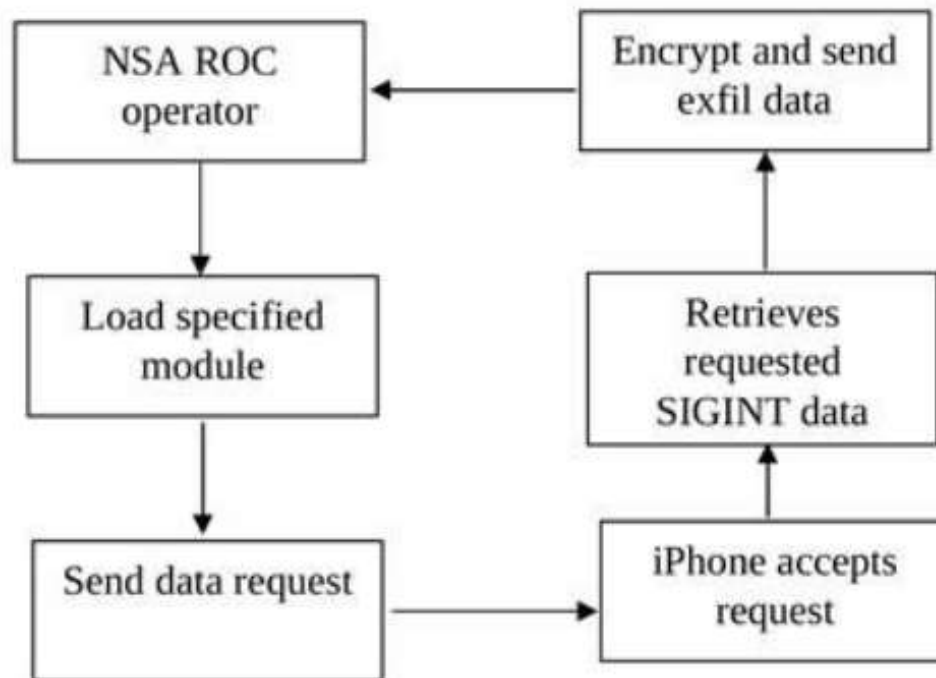


DROPOUTJEEP

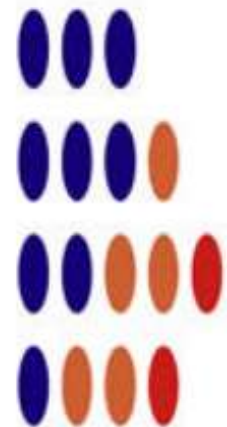
ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) DROPOUTJEEP – Operational Schematic



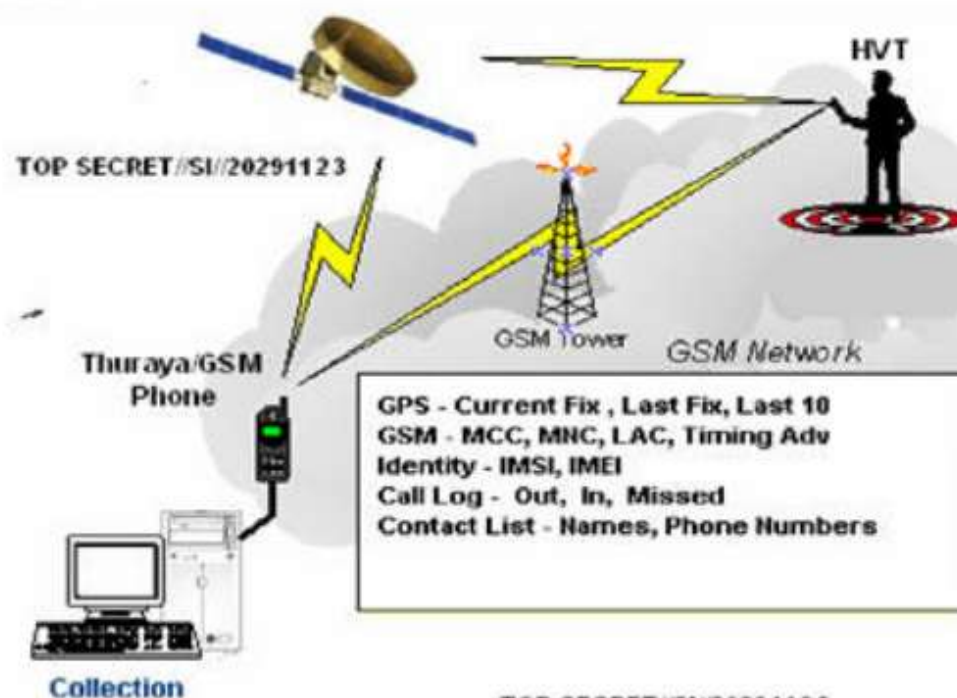


TOTECHASER

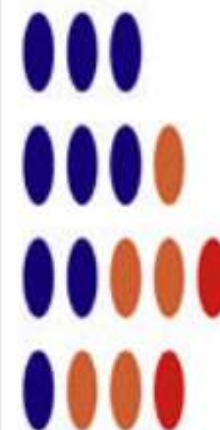
ANT Product Data

(TS//SI//REL) TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. The Thuraya 2520 is a dual mode phone that can operate either in SAT or GSM modes. The phone also supports a GPRS data connection for Web browsing, e-mail, and MMS messages. The initial software implant capabilities include providing GPS and GSM geo-location information. Call log, contact list, and other user information can also be retrieved from the phone. Additional capabilities are being investigated.

10/01/08



(U//FOUO) TOTECHASER - Operational Schematic



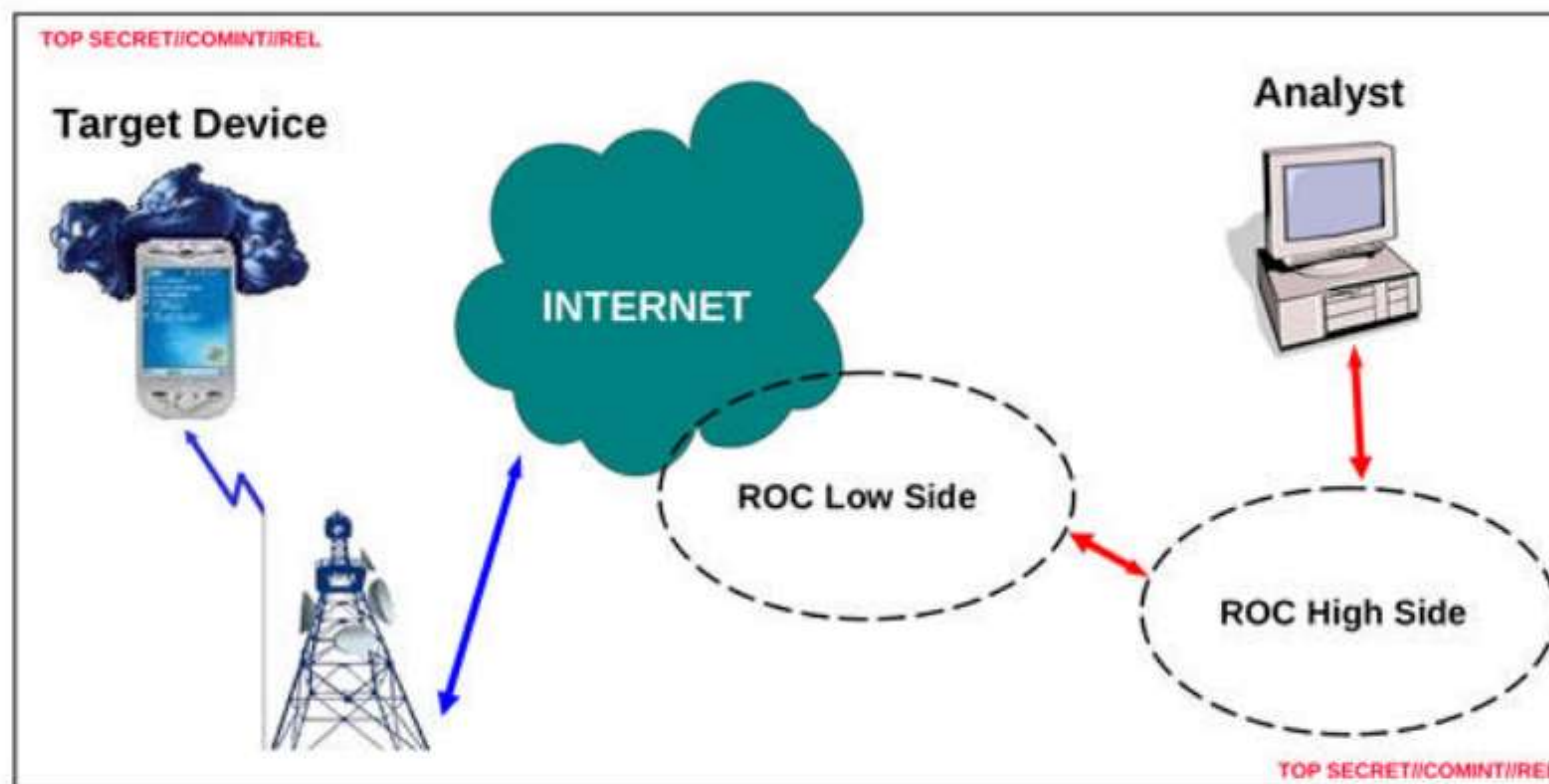


TOTEGHOSTLY 2.0

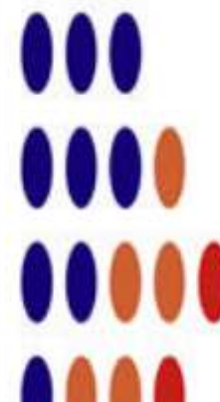
ANT Product Data

(TS//SI//REL) TOTEGHOSTLY 2.0 is a STRAITBIZARRE based implant for the Windows Mobile embedded operating system and uses the CHIMNEYPOOL framework. TOTEGHOSTLY 2.0 is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) TOTEGHOSTLY – Data Flow Schematic



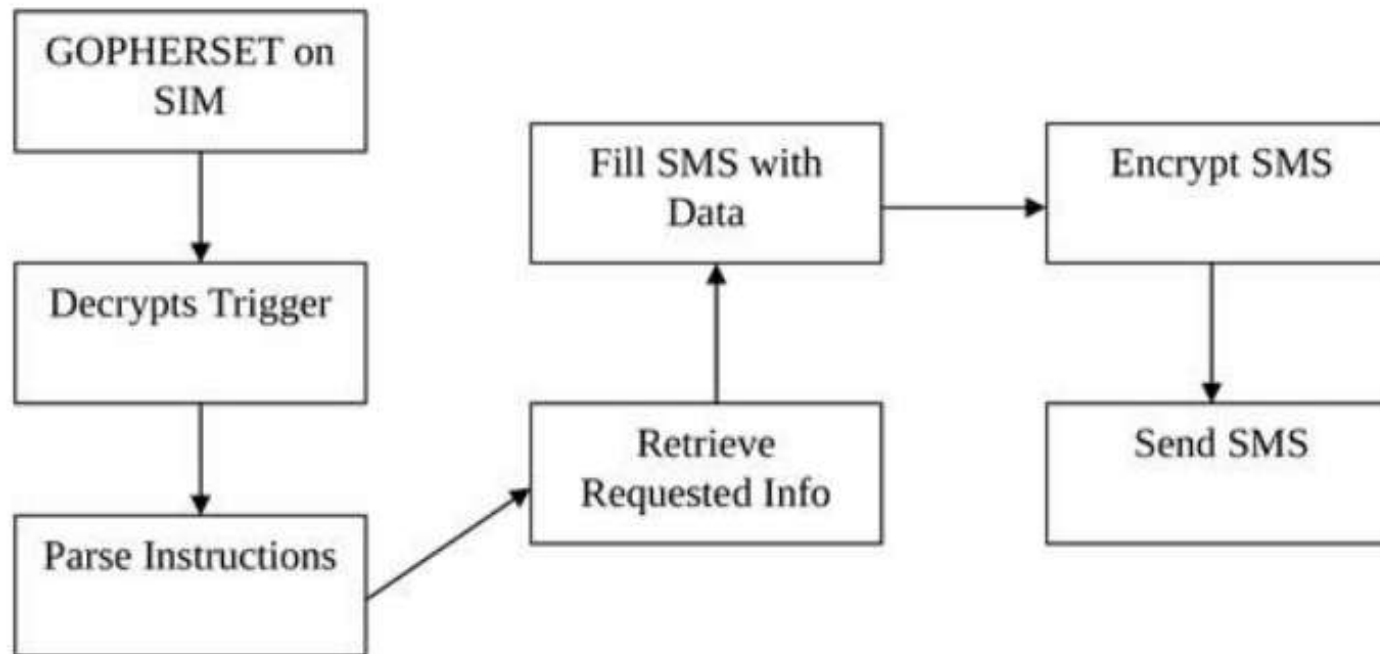


GOPHERSET

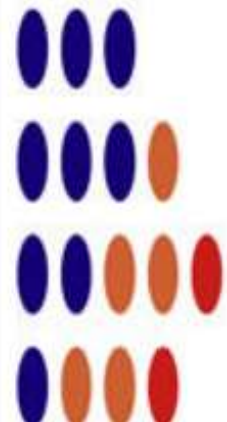
ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08



(U//FOUO) GOPHERSET – Operational Schematic



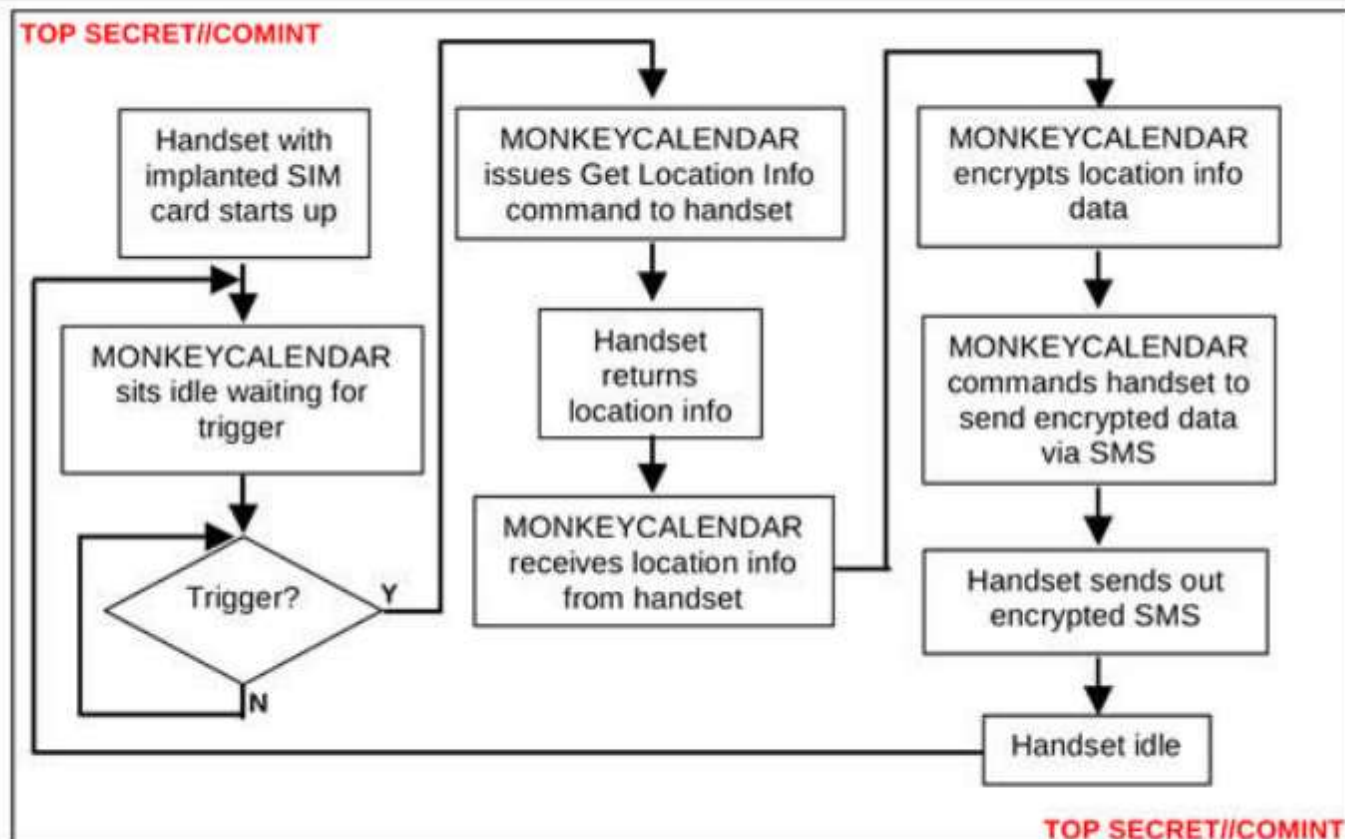


MONKEYCALENDAR

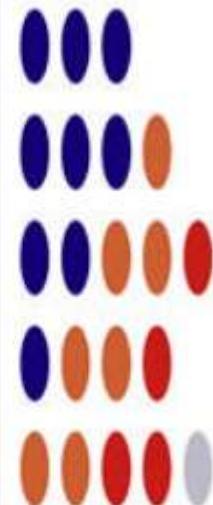
ANT Product Data

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08



(U//FOUO) MONKEYCALENDAR – Operational Schematic





PICASSO

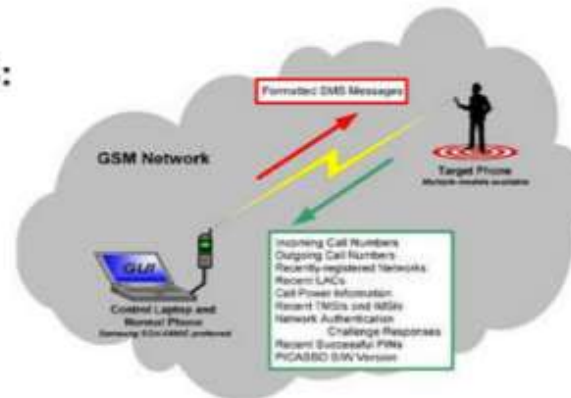
GSM HANDSET

(S//SI//REL) Modified GSM (target) handset that collects user data, location information and room audio. Command and data exfil is done from a laptop and regular phone via SMS – (Short Messaging Service), without alerting the target.

06/20/08

(S//SI) Target Data via SMS:

- Incoming call numbers
- Outgoing call numbers
- Recently registered networks
- Recent Location Area Codes (LAC)
- Cell power and Timing Advance information (GEO)
- Recently Assigned TMSI, IMSI
- Recent network authentication challenge responses
- Recent successful PINs entered into the phone during the power-on cycle
- SW version of PICASSO implant
- 'Hot-mic' to collect Room Audio
- Panic Button sequence (sends location information to an LP Operator)
- Send Targeting Information (i.e. current IMSI and phone number when it is turned on - in case the SIM has just been switched).
- Block call to deny target service.



(S//SI) PICASSO Operational Concept

(S//SI//REL) Uses include asset validation and tracking and target templating. Phone can be hot mic'd and has a "Panic Button" key sequence for the witting user.

Status: 2 weeks ARO (10 or less)

Unit Cost: approx \$2000

(S//SI//REL) Handset Options

- Eastcom 760c+
- Samsung E600, X450
- Samsung C140
- (with Arabic keypad/language option)





RF
Retro reflectors



RAGEMASTER

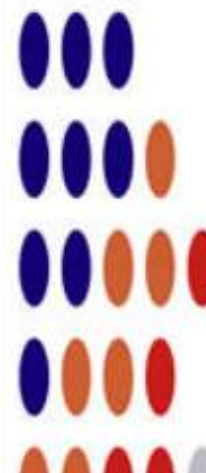
ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



The Thing



(Great Seal Bug)



CTX4000

ANT Product Data

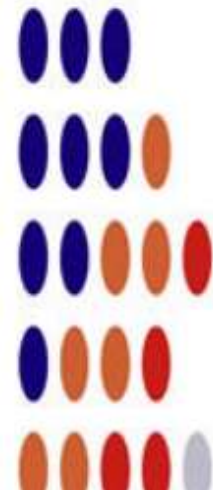
(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

8 Jul 2008



(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.





PHOTOANGLO

ANT Product Data

(TS//SI//REL TO USA,FVEY) PHOTOANGLO is a joint NSA/GCHQ project to develop a new radar system to take the place of the CTX4000.

24 Jul 2008

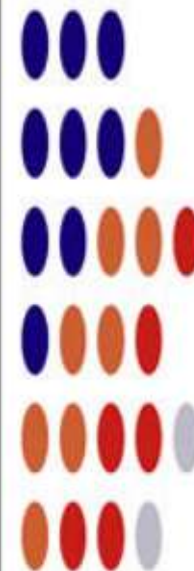
(U) Capabilities

(TS//SI//REL TO USA,FVEY) The planned capabilities for this system are:

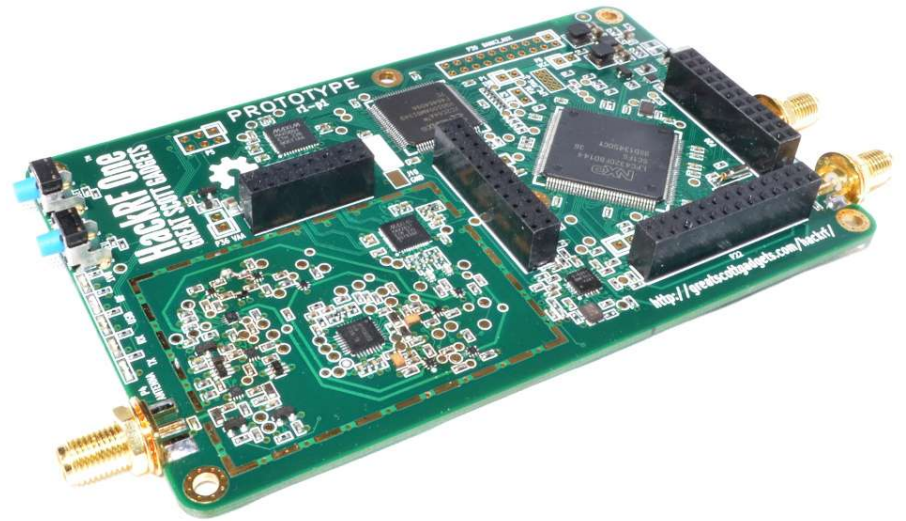
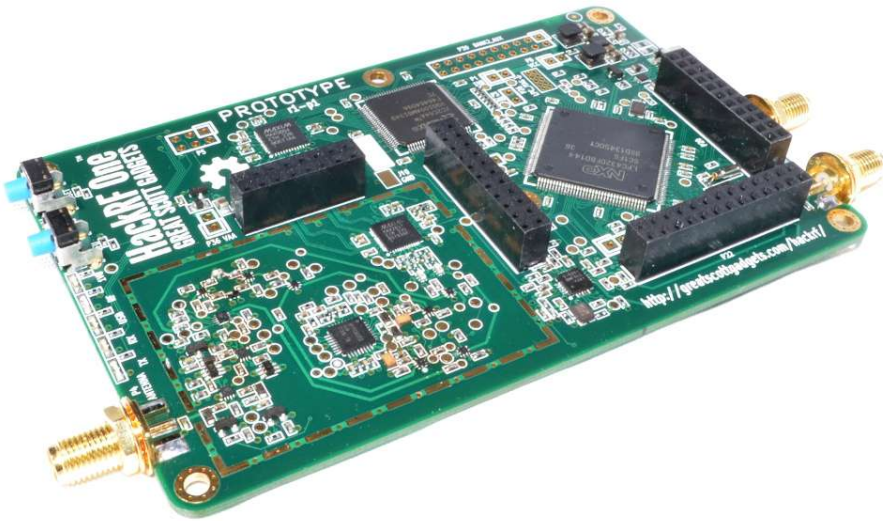
- Frequency range: 1 - 2 GHz, which will be later extended to 1 - 4 GHz.
- Maximum bandwidth: 450 MHz.
- Size: Small enough to fit into a slim briefcase.
- Weight: Less than 10 lbs.
- Maximum Output Power: 2 W
- Output:
- Video
- Transmit antenna
- Inputs:
- External oscillator
- Receive antenna

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) (TS//SI//REL TO USA,FVEY) The radar unit generates an un-modulated, continuous wave (CW) signal. The oscillator is either generated internally, or externally through a signal generator or cavity oscillator. The unit amplifies the signal and sends it out to an RF connector, where it is directed to some form of transmission antenna (horn, parabolic dish, LPA, spiral). The signal illuminates the target system and is re-radiated. The



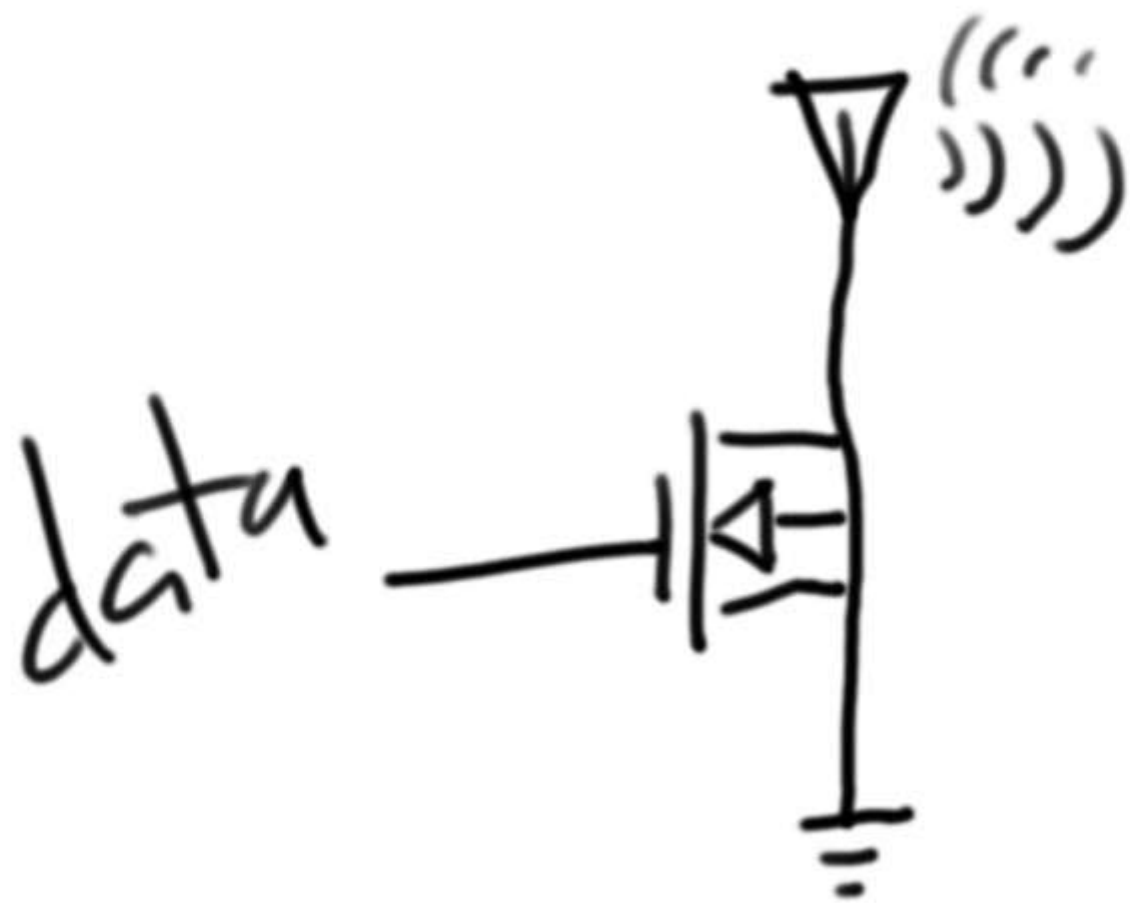
HackRF One x2





Hot Wheels Radar Gun!

Simple RF Retroreflector





SURLYSPAWN

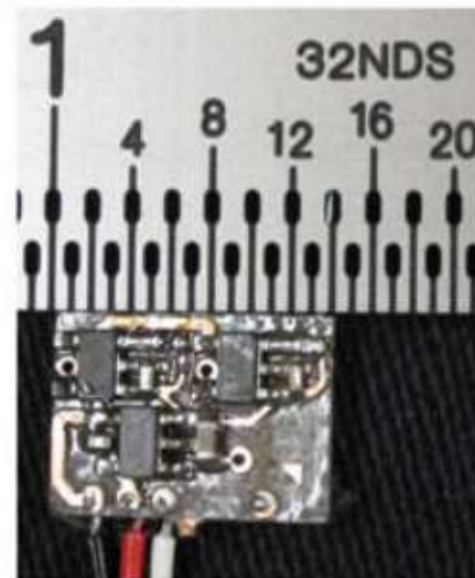
ANT Product Data

(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

07 Apr 2009

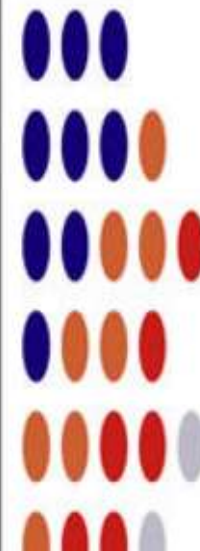
(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated,





TAWDRYYARD

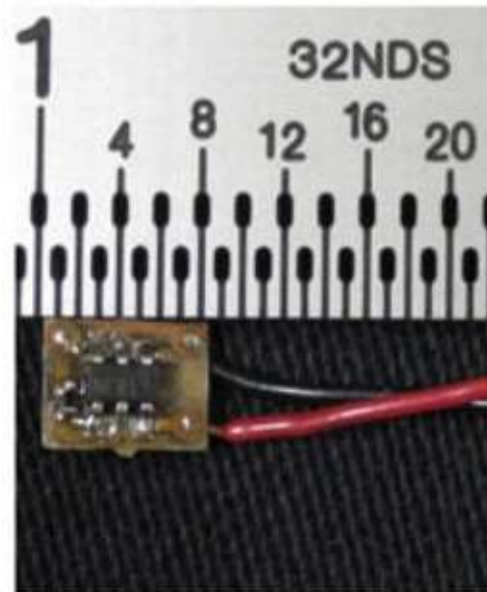
ANT Product Data

(TS//SI//REL TO USA,FVEY) Beacon RF retro-reflector. Provides return when illuminated with radar to provide rough positional location.

07 Apr 2009

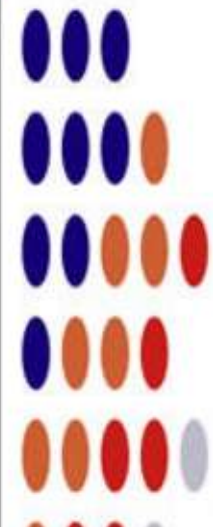
(U) Capabilities

(TS//SI//REL TO USA,FVEY) TAWDRYYARD is used as a beacon, typically to assist in locating and identifying deployed RAGEMASTER units. Current design allows it to be detected and located quite easily within a 50' radius of the radar system being used to illuminate it. TAWDRYYARD draws as 8 μ A at 2.5V (20 μ W) allowing a standard lithium coin cell to power it for months or years. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities being considered are return of GPS coordinates and a unique target identifier and automatic processing to scan a target area for presence of TAWDRYYARDS. All components are COTS and so are non-attributable to NSA.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board generates a square wave operating at a preset frequency. This square wave is used to turn a FET (field effect





LOUDAUTO

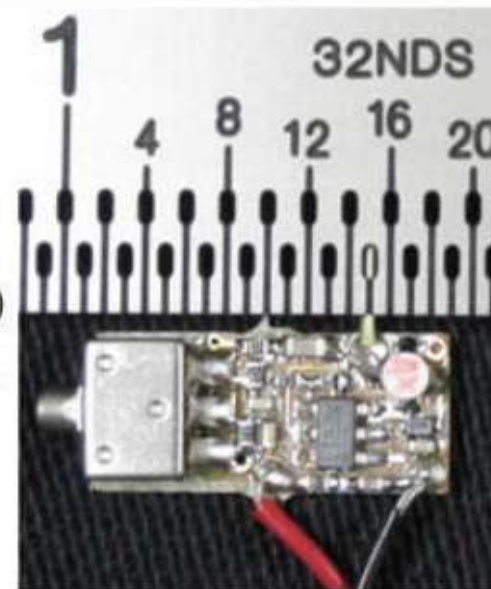
ANT Product Data

(TS//SI//REL TO USA, FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

07 Apr 2009

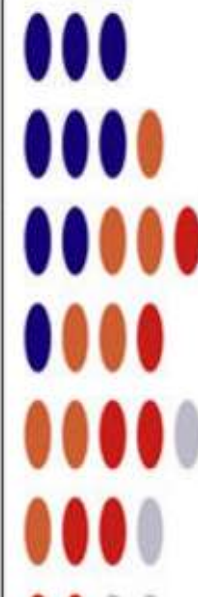
(U) Capabilities

(TS//SI//REL TO USA, FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components are COTS and so are non-attributable to NSA.



(U) Concept of Operation

(TS//SI//REL TO USA, FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This



Contribute your
tools!

nsaplayset.org

(silly name required)

NSA Playset

Site Information
Contributions
Project Requirements
Open Problems
Passive Radio Interception
TWILIGHTVEGETABLE (GSM)
TINYALAMO
Active Radio Injection
Physical Domination
SLOTSCREAMER (PCI)
ADAPTERNOODLE (USB)
Hardware Implants
BROKENGLASS
CHUCKWAGON
TURNIPSCHOOL
Software Implants
Network Reconnaissance

Open Problems

The following is an annotated list of ANT projects pulled from : https://en.wikipedia.org/wiki/NSA_ANT_catalog
<http://cryptome.org/2014/01/nsa-codenames.htm>
http://www.nsaplayset.org/nsa_ant_catalog.pdf

NEEDED **WANTED** **UNDER DEVELOPMENT** **COVERED** **UNINTERESTING**

Plug-N-Pwn:

COTTONMOUTH-I: COTTONMOUTH-I is a USB plug that uses TRINITY as digital core and HOWLERMONKEY as RF transceiver. Cost in 2008 was \$1.25M for 50 units.
 COTTONMOUTH: (see image at right) A family of modified USB and Ethernet connectors that can be used to install Trojan horse software and work as a network interface.
 COTTONMOUTH-II is deployed in a USB socket (rather than plug), and costs only \$200K per 50 units, but requires further integration in the target machine.
 COTTONMOUTH-III is a stacked Ethernet and USB plug costing approximately \$1.25M for 50 units.

The USB components are covered by ADAPTERNOODLE. SLOTSCREAMER intends to act as a generic DMA over PCI via PCI jumpers, ExpressCard, etc.

Network Recon:

BANANAGLEE : High level Cisco/Juniper trojan
 ZESTYLEAK: High level Juniper trojan
 JETPLOW(6): firmware rootkit for cisco routers
 FEEDTROUGH(3) : BIOS rootkit for Juniper netscreen firewalls
 GOURMETTROUGH(4): BIOS rootkit for other Juniper firewalls
 SOUFFLETROUGH(7): BIOS rootkit for Juniper SSG 500 and 300
 HALLUXWATER(5): boot ROM rootkit for Huawei routers
 HEADWATER(8): trojan for Huawei routers

SCHOOLMONTANA(9): rootkit for Juniper J-series routers/firewalls
 SIERRAMONTANA(10): rootkit for Juniper M-series routers/firewalls
 STUCCOMONTANA(11): rootkit for Juniper T-series routers/firewalls

While we don't need to recreate tools for these specific use cases, it would be interesting to recreate some high level / low level functionality in other code.

GSM Stuff:

CANDYGRAM(35): A \$40,000 tripwire device that emulates a GSM cellphone tower.
 CYCLONE-HX9: EGSM base station router
 EBSR(38): 1 watt (pico class) GSM base station
 NEBULA(41): (macro class) Base station router GSM/UMTS/CDMA2000/ LTE coming soon*
 TYPHON HX(42): GSM base station router
 HOLLOWPOINT: GSM/UTMS/CSMA2000/FRS signal platform. Operates in the 10MHz to 4GHz range. Includes receiver and antenna. Can both transmit and receive.
 WATERWITCH(43): A portable "finishing tool" that allows the operator to find the precise location of a nearby mobile phones.

GENESIS(40): Modified GSM handset (Motorola SLVR L9) to sniff and monitor traffic (covered by TWILIGHTVEGETABLE)
PICASSO(32): Modified GSM handset for jamming, sniffing, recording from microphone
ENTOURAGE(39): locates wireless devices (phones etc)

SIM stuff:

GOPHERSET: SIM implant to exfiltrate Phonebook, SMS/Call logs

Thanks to Dean Pierce
for the "NSA Playset" name.

Thanks to Nick Malar
for illustrations
(the good ones).

Coming Soon!

NSA Playset: RF Retroreflectors

NSA Playset: GSM

NSA Playset: PCIe

NSA Playset: I2C

nsaplayset.org

