The 30C3, To Protect and Infect, The Militarization of the Internet
Jacob Appelbaum @ioerror, 30 December 2013
NSA catalog pages from video
https://www.youtube.com/watch?v=b0w36GAyZIA

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

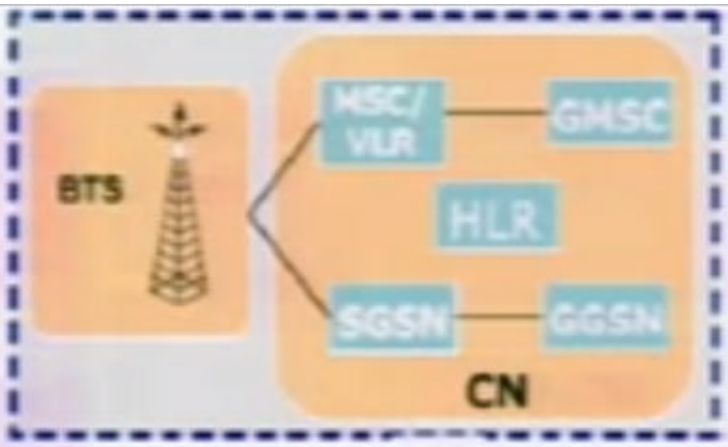
System Details

- (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.

Typhon Hx BSR

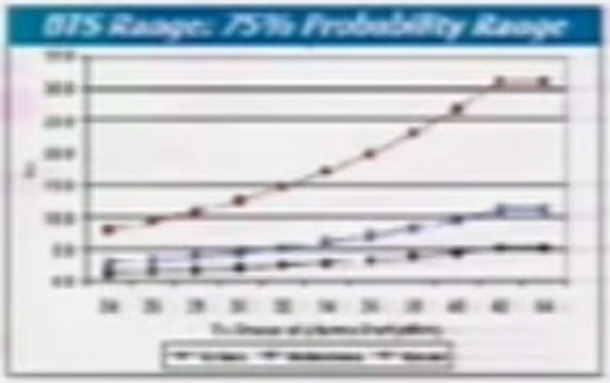


Typhon BSR

(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.



(S//SI//REL) The macro-class Typhon is a Network-in-a-Box (NIB), which includes all the necessary architecture to support Mobile Station call processing and SMS messaging in a stand-alone chassis with a pre-provisioning capability.

(S//SI//REL) The Typhon system kit includes the amplified Typhon system, OAM&P Laptop, cables, antennas and AC/DC power supply.

(U//FOUO) An ***800 WH Lilon Battery kit is offered separately.***

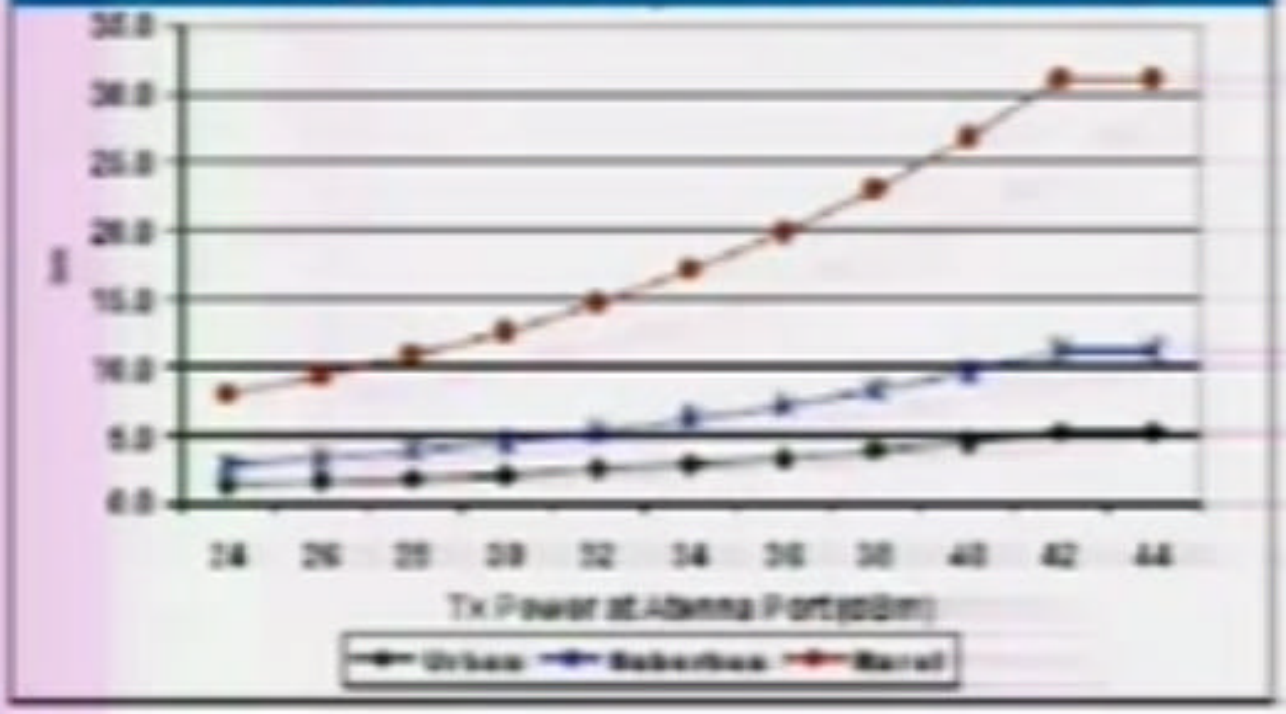
(U) A bracket and mounting kit are available upon request.

Typhon Hx Priced Options		
Deliverable	Duration	FFP COST ea.
[illegible]	[illegible]	[illegible]
Typhon Model/Color	Order Code (& Total Spare kit)	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	
[illegible]	[illegible]	

(U) **Status:** Available 4 mos ARO

Typhon BSR

BTS Range: 75% Probability Range



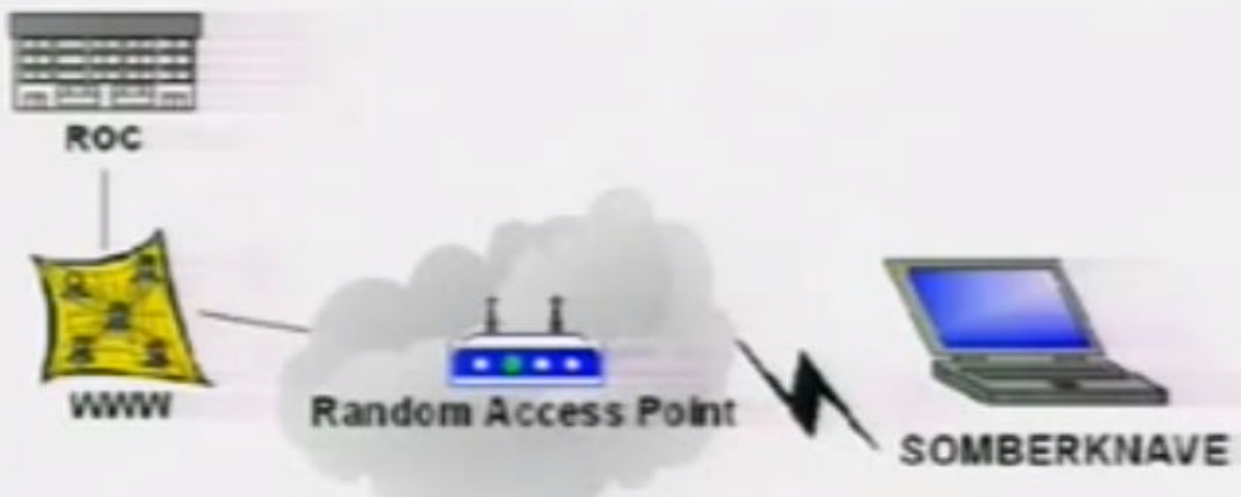
Typhon Hx Priced Options

Deliverable	Duration	FFP COST
1 to 25 units	4 Months	$175,800

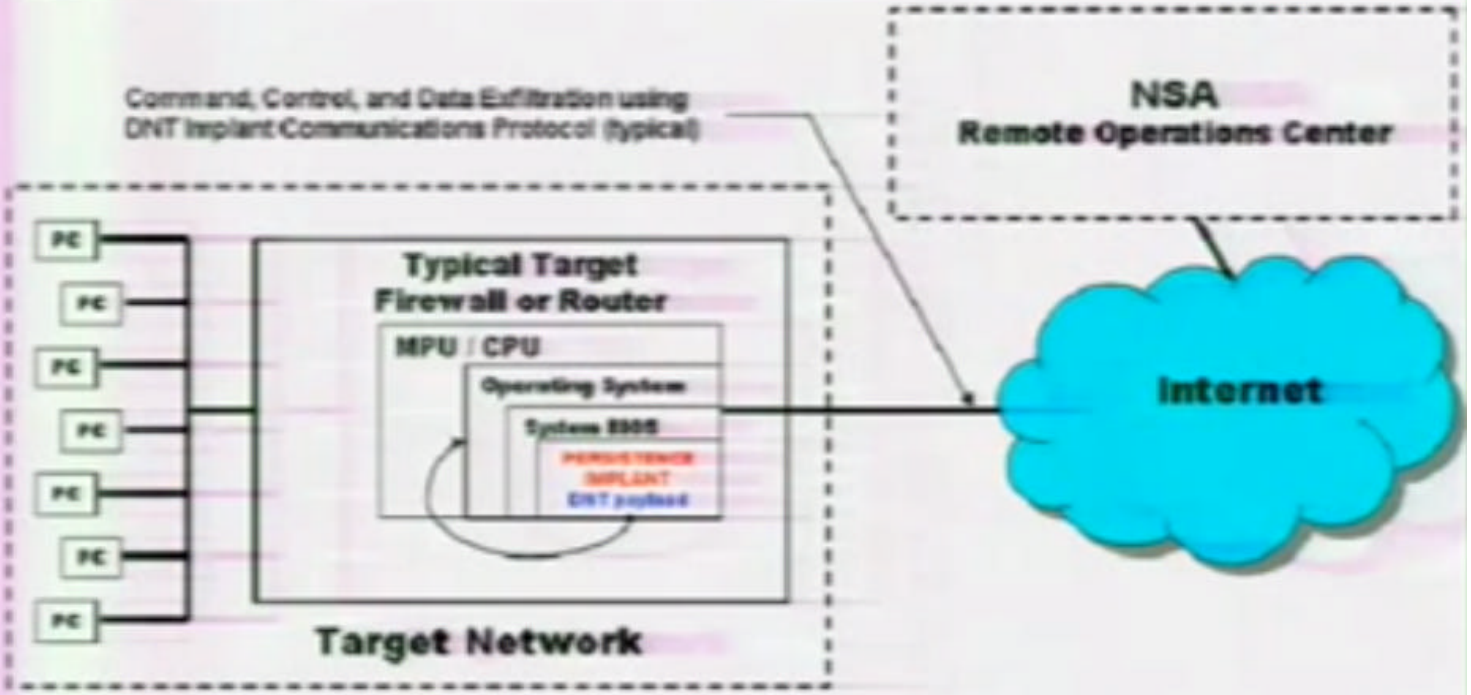
Typhon Model/Color	Order Code (& Total Signaling Loss)
Hx8 Black (GSM850)	G1004164 & G1004140
Hx8 Green (GSM850)	G1004161 & G1004137
Hx9 Black (EGSM900)	G1003727 & G1002665
Hx9 Green (EGSM900)	G1003726 & G1002037
Hx18 Black (DCS1800)	G1004165 & G1004141
Hx18 Green (DCS1800)	G1004162 & G1004138
Hx19 Black (PCS1900)	G1004166 & G1004142
Hx19 Green (PCS1900)	G1004163 & G1004139

(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.



(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.

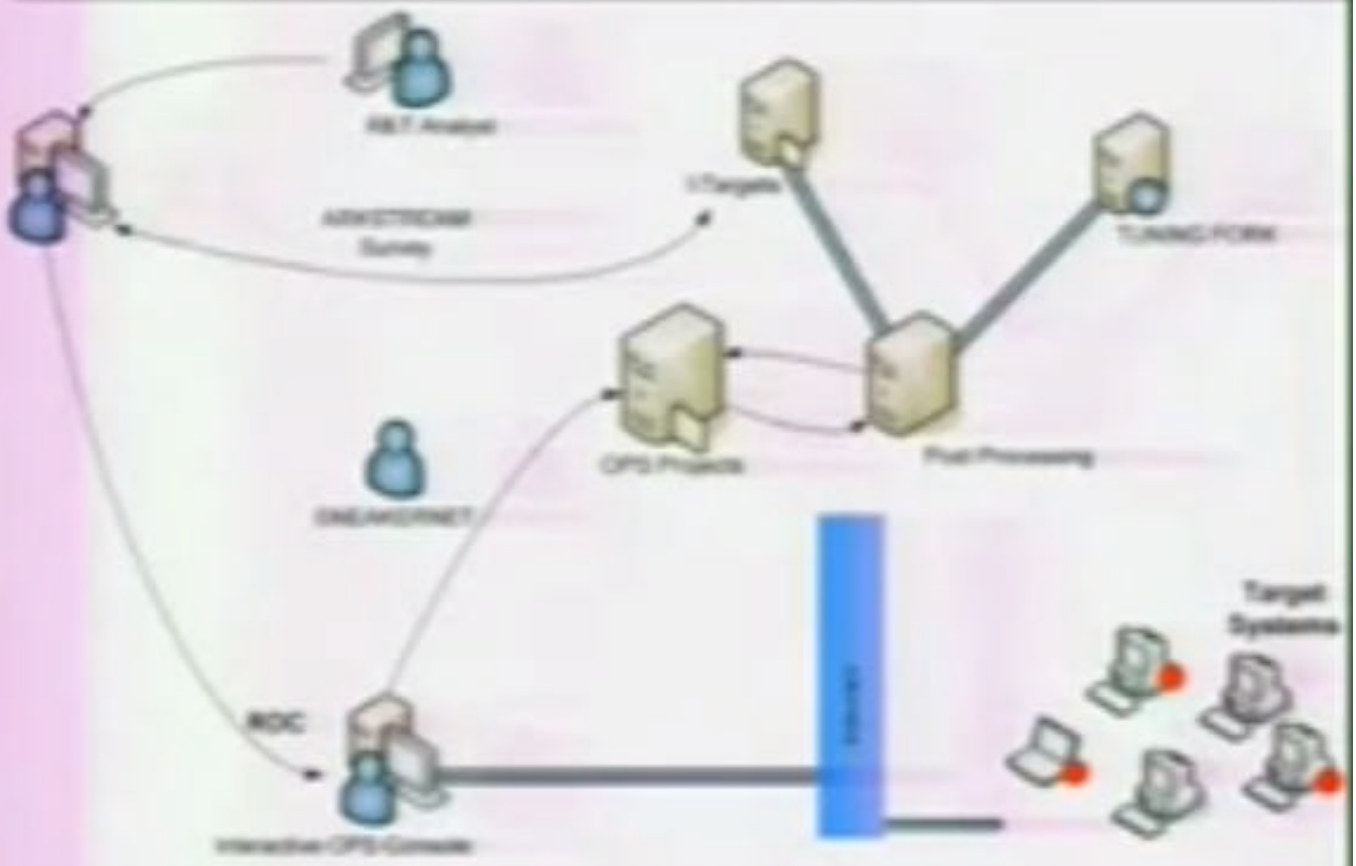


(S//SI//REL) STUCCOMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the STUCCOMONTANA implant at the end of its native System Management Mode (SMM) handler.

ANT Prod

(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.



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

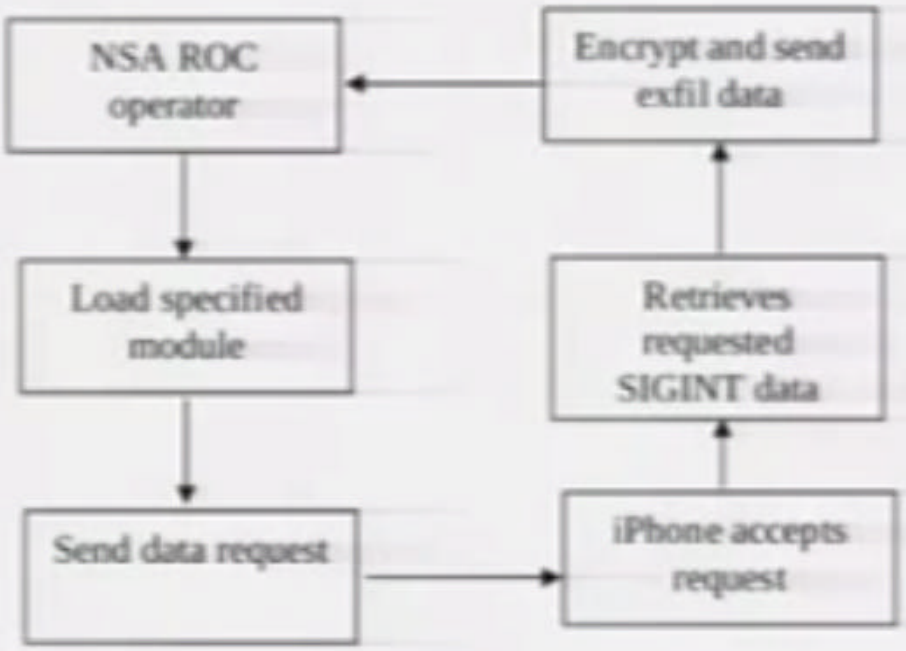
(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

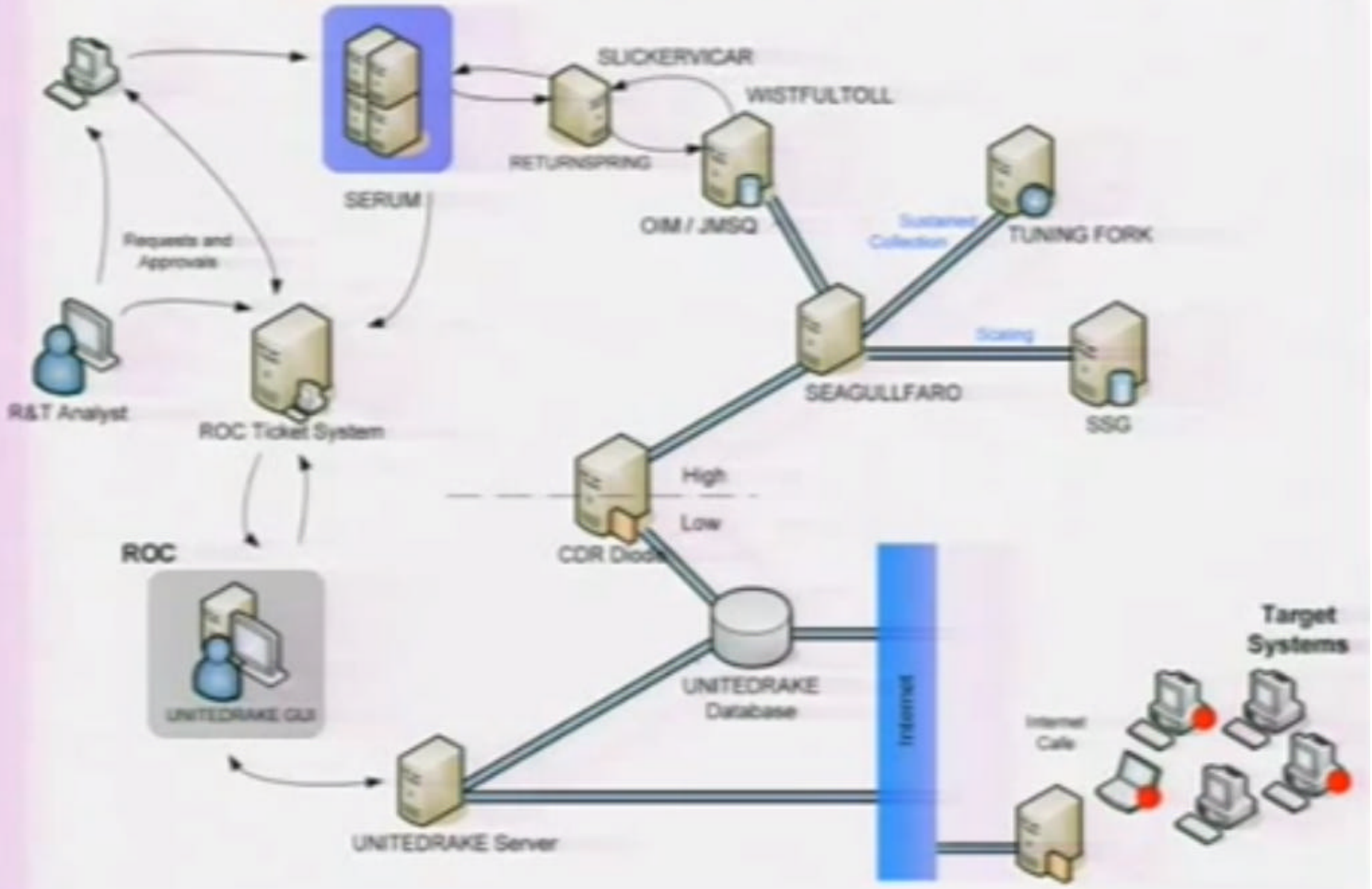
(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.



(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(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.



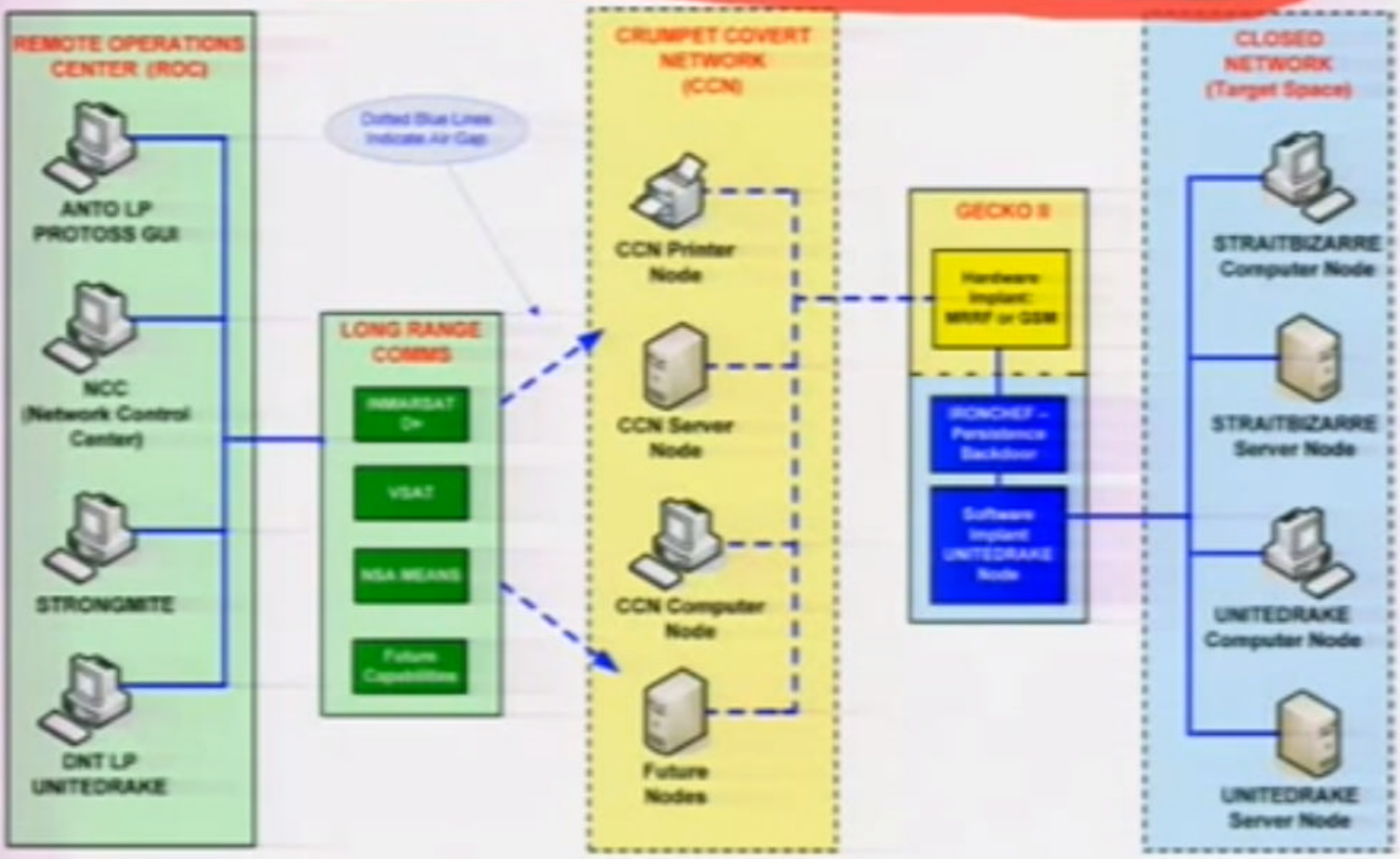
(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

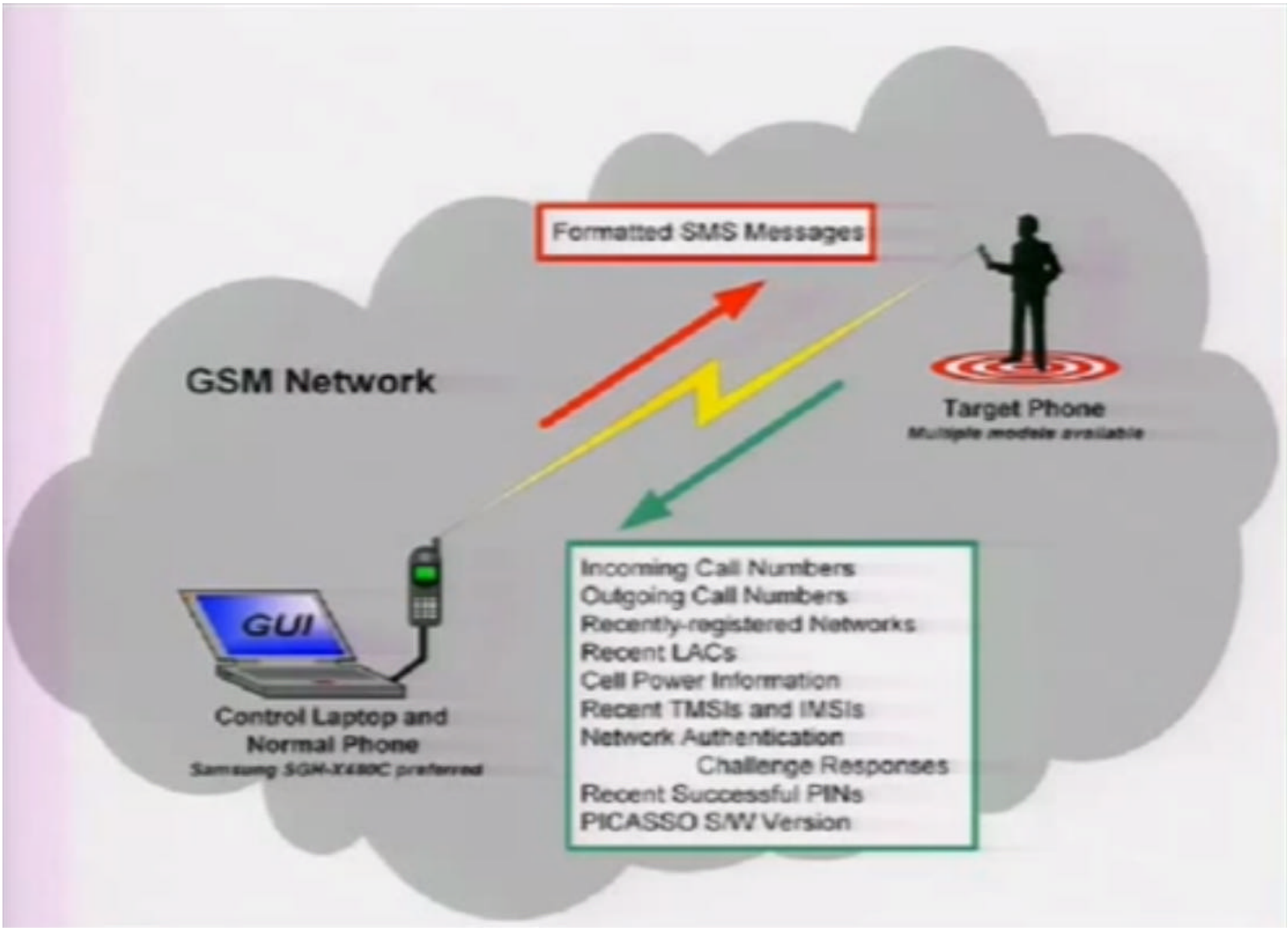
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

(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.



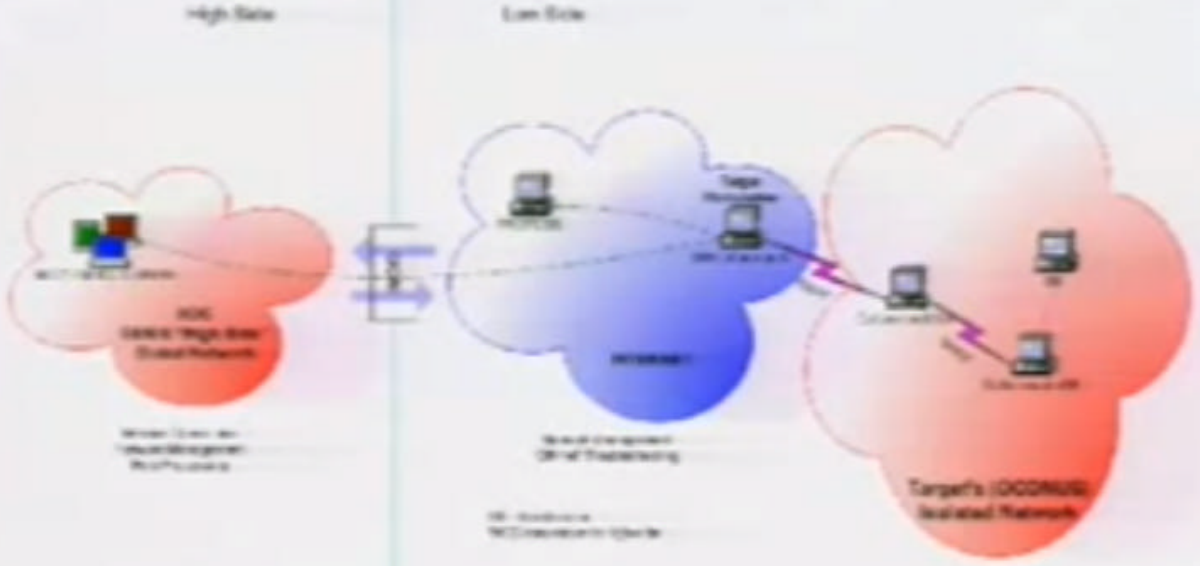
(TS//SI//REL) IRONCHEF Extended Concept of Operations


Formatted SMS Messages
GSM Network
Target Phone
Multiple models available
GUI
Control Laptop and
Normal Phone
Samsung SGH-X480C preferred
Incoming Call Numbers
Outgoing Call Numbers
Recently-registered Networks
Recent LACs
Cell Power Information
Recent TMSIs and IMSIs
Network Authentication
Challenge Responses
Recent Successful PINs
PICASSO S/W Version

(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 CONOP
INTERNET Scenario

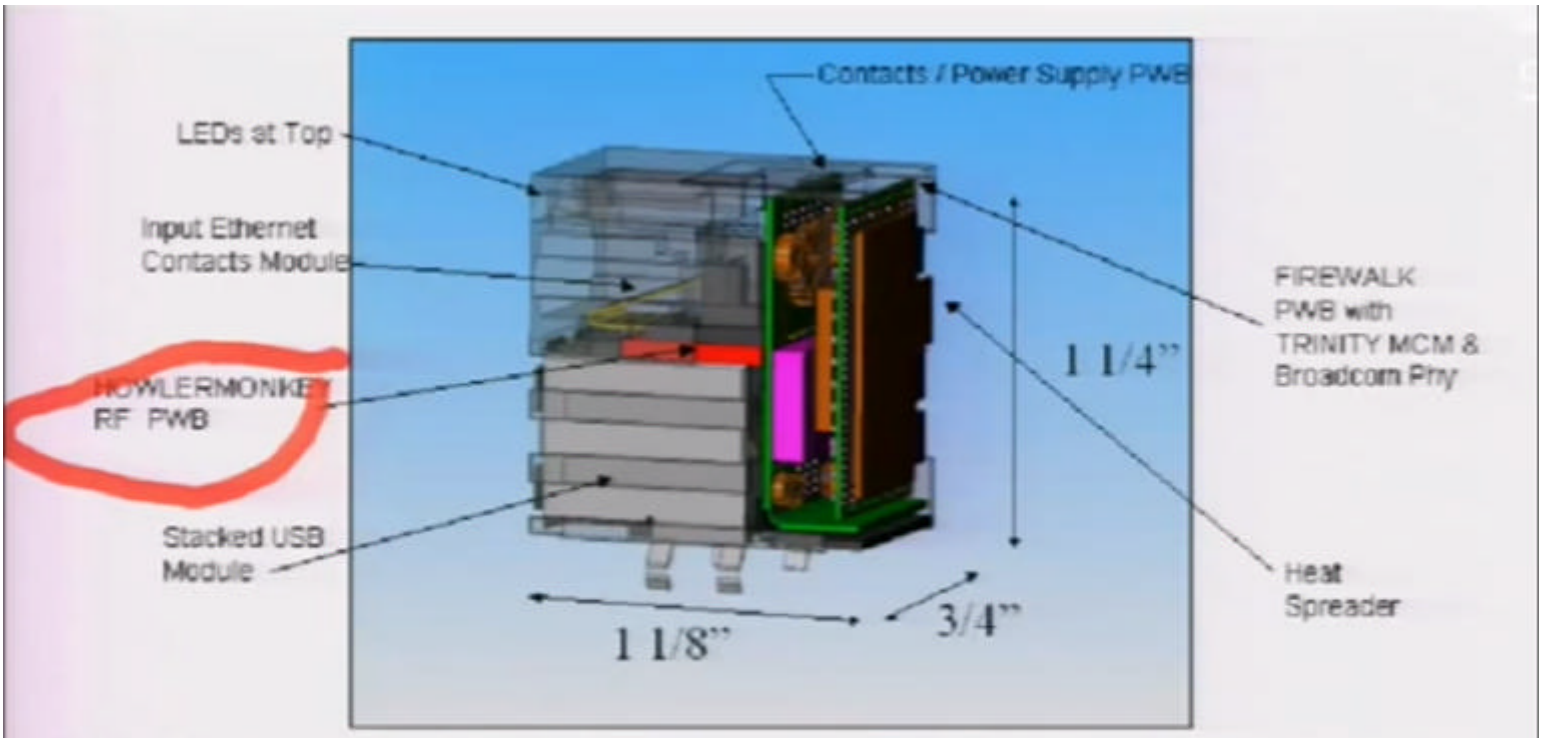


Status: Availability – January 2009 **Unit Cost:** 50 units: $1,015K

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

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

(TS//SI//REL) CM-II consists of the CM-I digital hardware and the long haul relay co
somewhere within the target chassis. A USB 2.0 HS hub with switches is concea
dual stacked USB connector, and the two parts are hard-wired, providing a intra-chas



EWALK is a bi-directional 10/100/1000bT (Gigabit) Ethern
within a dual stacked RJ45 / USB connector. FIREWALK is

TOP SECRET//COMINT//REL TO USA, FVEY

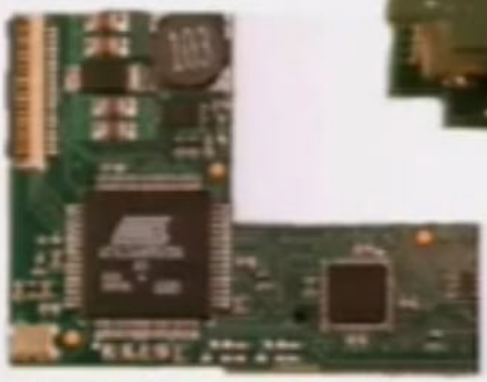
GODSURGE

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 2950



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

(TS//SI//REL) This technique supports Dell PowerEdge 1950 and 2950 servers that use the Xeon 5100 and 5300 processor families.

(TS//SI//REL) Through interdiction, the JTAG scan chain must be reconnected on the target system by removing the motherboard from the chassis and attaching the depopulated parts back onto the circuit board. After this step is complete, the hardware implant itself must be attached to the motherboard. The implants should already be programmed with the GODSURGE application code and its payload, the implant installer. Once implanted, GODSURGE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $500 for Hardware and Installation

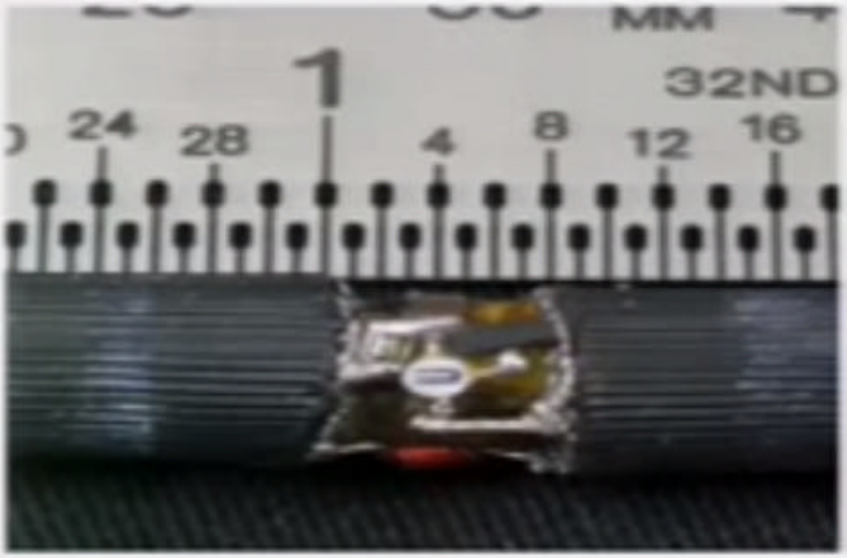
(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

(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.
- Phase adjustment with front panel knob

(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.



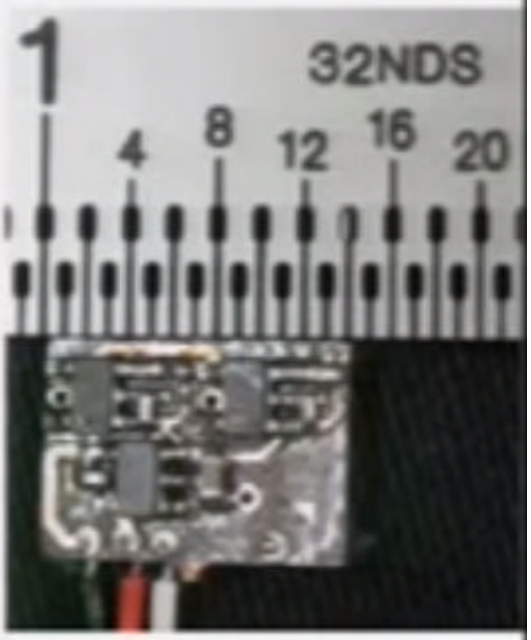
(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

(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.

(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.



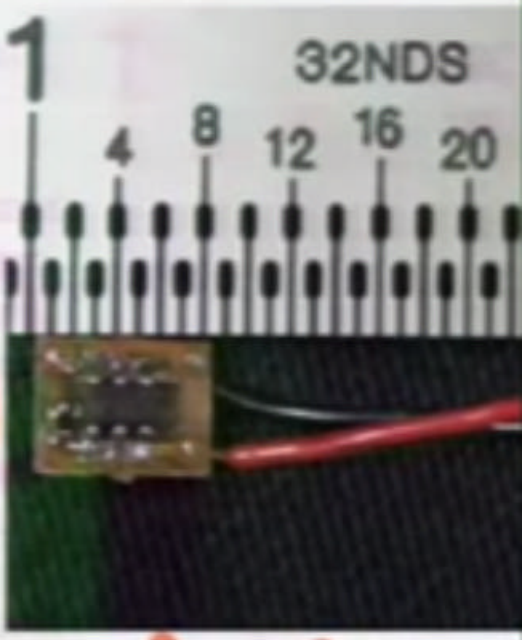
(U) Concept of Operation

(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, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

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

(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 µA at 2.5V (20µW) 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.



HA!

(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 transistor) on and off. When the unit is illuminated with a CW signal, the illuminating signal is amplitude-modulated (AM) with the square wave. This signal is re-radiated, where it is picked up by the radar, then processed to

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

(S//SI) Features:

(S//SI) WATERWITCH Handset DF Set

- 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