To Protect And Infect

The Militarization of the Internet
(Part Two; in three acts)

The 30c3 – December 30th, 2013

Jacob Appelbaum (@ioerror)

Act I

(Low end) corporate spying

- Commercial hardware solutions are rather boring
- Forensics hardware like the "Mouse Jiggler"
  - Now disabled in systemd (!)
- Power insertion attacks
  - Hotplug seizures
- Keystroke recorders
  - largely lame
- FinFisher, HackingTeam, VUPEN

Rafael is a journalist from Angola, who exposed corruption in the government.

Angola Attack

- Discovered at Oslo Freedom Forum
- Lamest OS X backdoor ever
  - Screencapture
  - Curl
  - Sleep
- Unsuspecting 8 GB of screenshots in the home directory
- Infrastructure connected with Operation Hangover
  - Appin Security
- Code signed
  - Apple revoked the signing permissions in a reasonable time frame

In Summer 2013 Rafael was arrested, then released and faced 11 criminal charges for his work exposing corruption.

These guys aren't impressive

They do harm to good people and they hand wave away their contribution to increasing the total amount of human suffering in the world.

Control, Baby!

Act II

Intelligence agency "solutions"

Meta-point: "non-attributable to NSA"
Meta-point: **Total** surveillance & control in *secrecy*

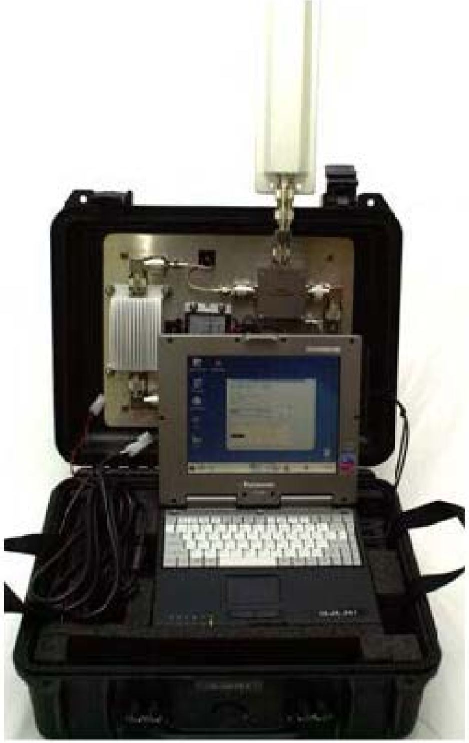
The Big Picture

- Planetary Strategic Surveillance and...
- Exploitation Systems
- Passive sensors
- Collect (TURMOIL)
- Active attacks
- Infect (TURBINE, QFIRE, etc)
- Wait, what about "Protect?!"
- Multi-pwn!
- Blackhats used to keep your box updated
- ... these guys step on each other's toes
- Operations – “Close Access Operations“ and “Off-Net”

(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.

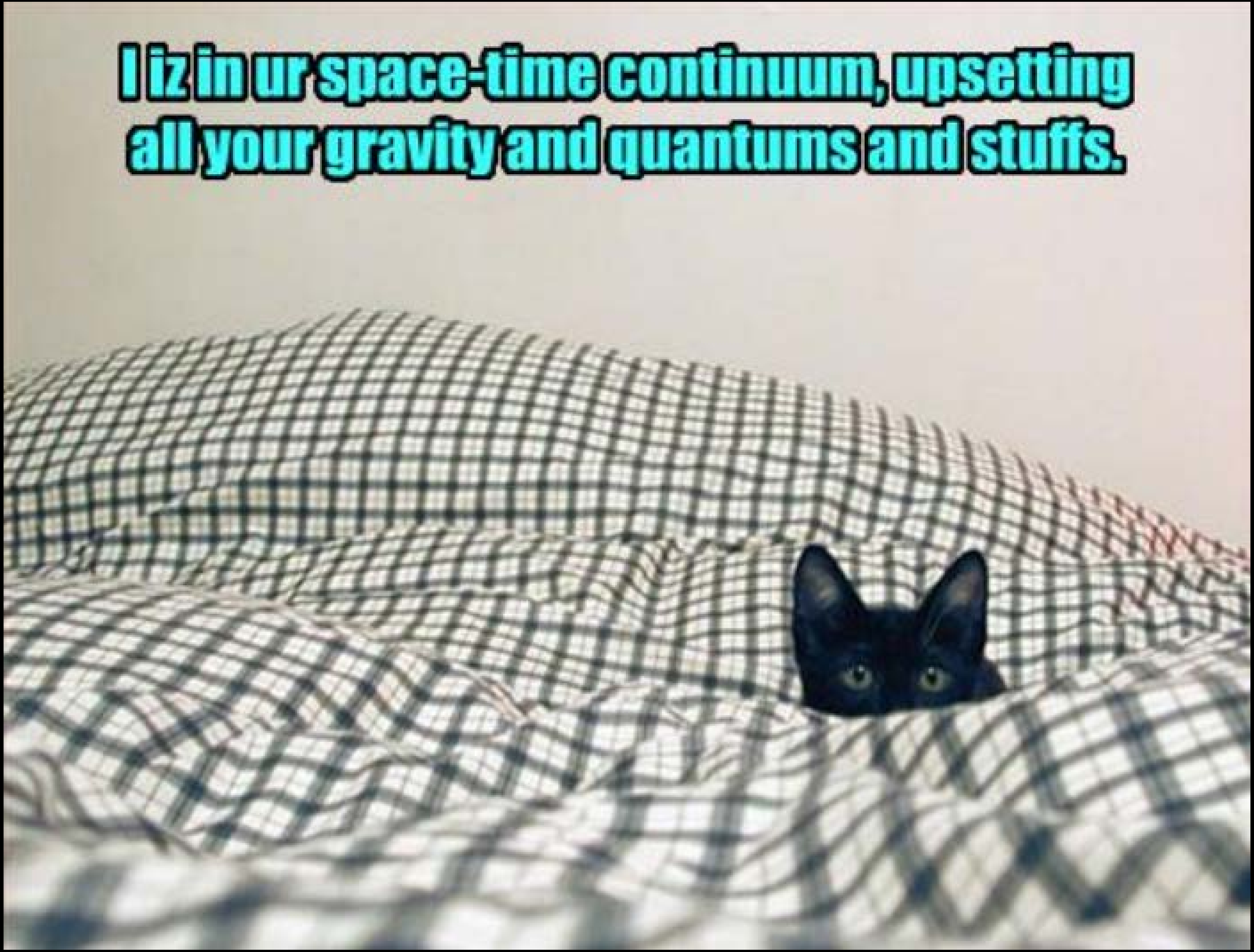


NIGHTSTAND Hardware

(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.

How do "they" do it?

- Dragnet surveillance
- Data retention
- ~15 years at least, including content!
- Tasking, exploitation
- QUANTUM THEORY and how each "solution" tries to meet this goal
- Man-On-The-Side as QUANTUM INSERTION
- PRISM, “upstream” and many other programs


I iz in ur space-time continuum, upsetting all your gravity and quantums and stuffs.

“They'll never find me!”

Dream on – Data Retention is an important part of total surveillance and the analysis is successful against us all.

Data totalitarianism or put another way:
totalitarianism

TURMOIL

Deep Packet Inspection
(Passive dragnet surveillance sensors)

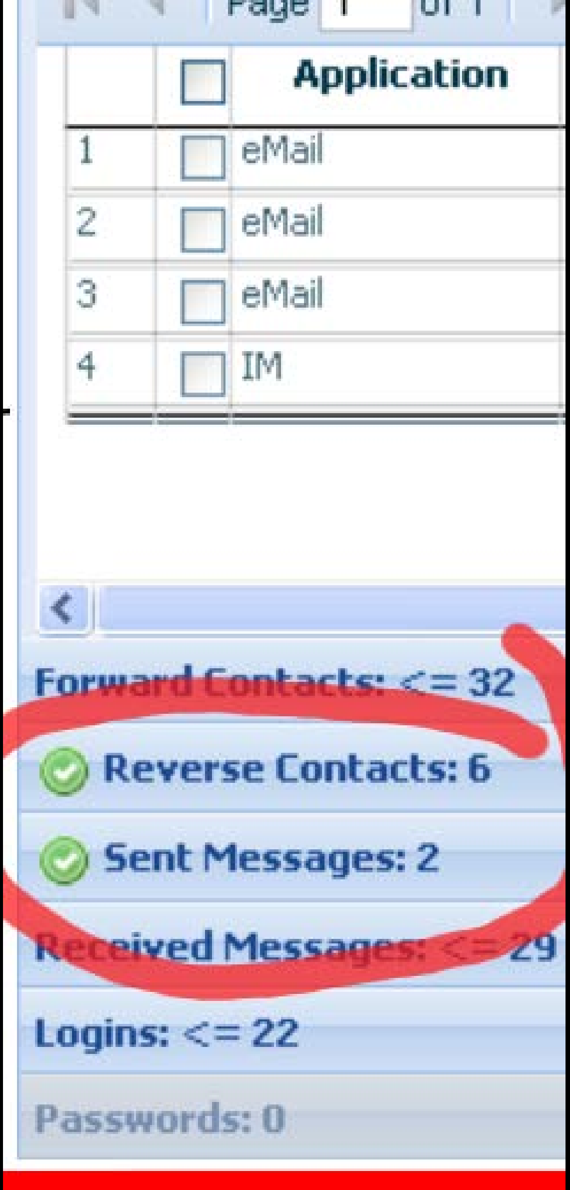
TURBINE

Deep Packet Injection

QFIRE

TURMOIL and TURBINE combined with additional infrastructure that they co-opt through pwnage of routers and other operations.

MARINA



Page 1 of 1

	□	Application
1	□	eMail
2	□	eMail
3	□	eMail
4	□	IM

Forward Contacts: <= 32

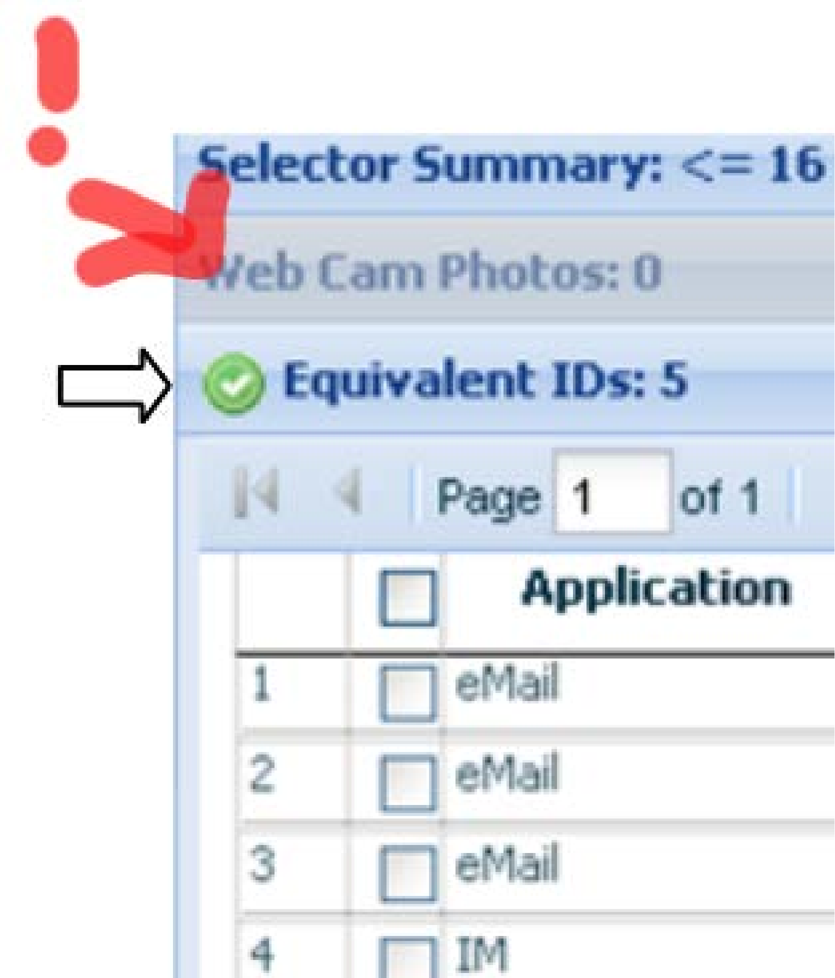
✓ Reverse Contacts: 6

✓ Sent Messages: 2

Received Messages: <= 29

Logins: <= 22

Passwords: 0



Selector Summary: <= 16

Web Cam Photos: 0

✓ Equivalent IDs: 5

Page 1 of 1

	□	Application
1	□	eMail
2	□	eMail
3	□	eMail
4	□	IM

From wiretapping to **whole life** surveillance

Example one: German Chancellor ***Merkel!***
(We revealed this operation in Der Spiegel)

Example two: Political and religious 'untasked'
targeting for some set of websites

Example three: three hops away? Uh oh!
(**That's you!**)

This is the **militarization** of the internet

- We are under a kind of martial law
- This strategy is undermining the internet in a direct attempt to keep it insecure
- We are personally and socially left vulnerable and actively exploited, literally
- This is being done in our names with our tax money and without our consent; usually without the knowledge of our representatives!
- Those who know usually do not actually understand! (eg: Members of the US Congress)

Active exploitation of targets with FOXACID

Selector surveillance leads to exploitation:

- QUANTUMTHEORY
  - SEASONEDMOTH (SMOTH)
- QUANTUMNATION
  - VALIDATOR, COMMONDEER
- QUANTUMBOT
- QUANTUMCOPPER
  - Think “The Great Firewall of China”
  - Ahem, “The Great Firewall of Earth”
- QUANTUMINSERT
  - Think Man-on-the-side

TAO infrastructure

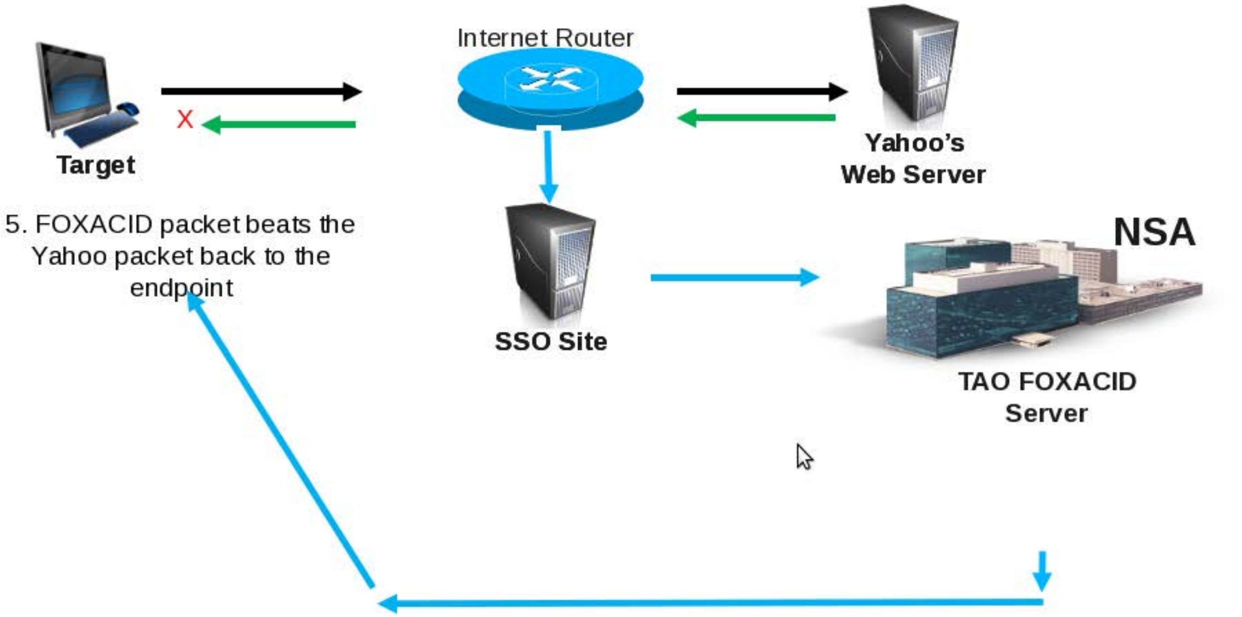
- First they find the target, then they redirect them
- QUANTUMINSERT and FOXACID
- Server's like to pretend that they're Apache servers
- Implemented in Python, easily fingerprinted
  - A few FOXACID URLs are public
  - Pay attention to the bugs in their implementation

When the NSA can't do it – they bring in GCHQ!

And boy oh boy do they love Yahoo!

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



5. FOXACID packet beats the Yahoo packet back to the endpoint

Re-purposing hardware and impersonating infrastructure

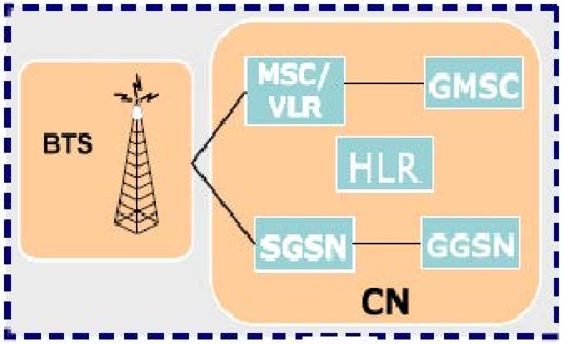
Re-purposing unused WiFi hardware

Cell base stations

TYPHON HX

GSM Base Station Router

Typhon Hx BSR

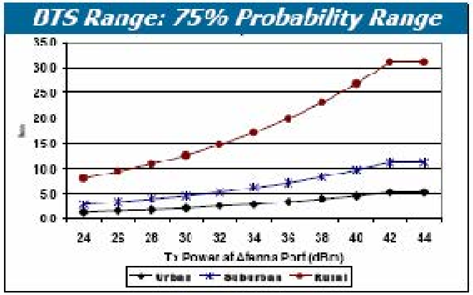


Typhon BSR

(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 LiIon Battery kit is offered separately.***

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

Typhon Hx Priced Options

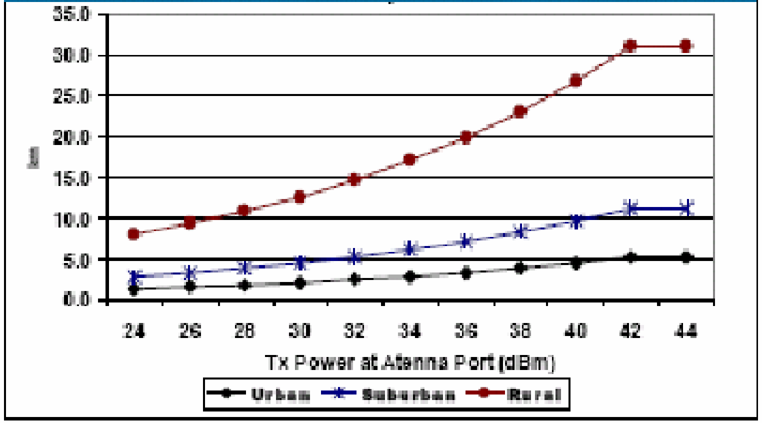
Deliverable	Duration	FFP COST ea.
1 to 25 units	4 Months	$175,800

Typhon Model/Color	Order Code (& Tool Spare kit)
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

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

Typhon BSR

BTS Range: 75% Probability Range



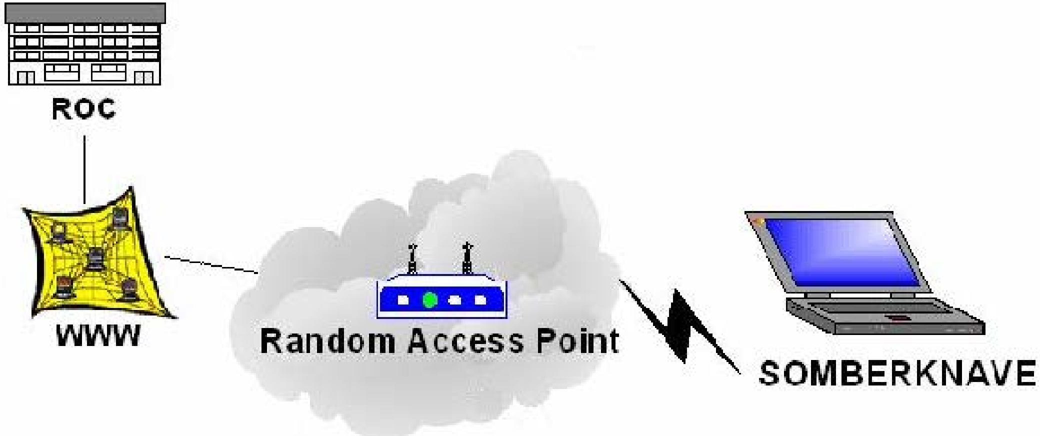
Typhon Hx Priced Options

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

Typhon Model/Color	Order Code (& Tool Spare kit)
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.

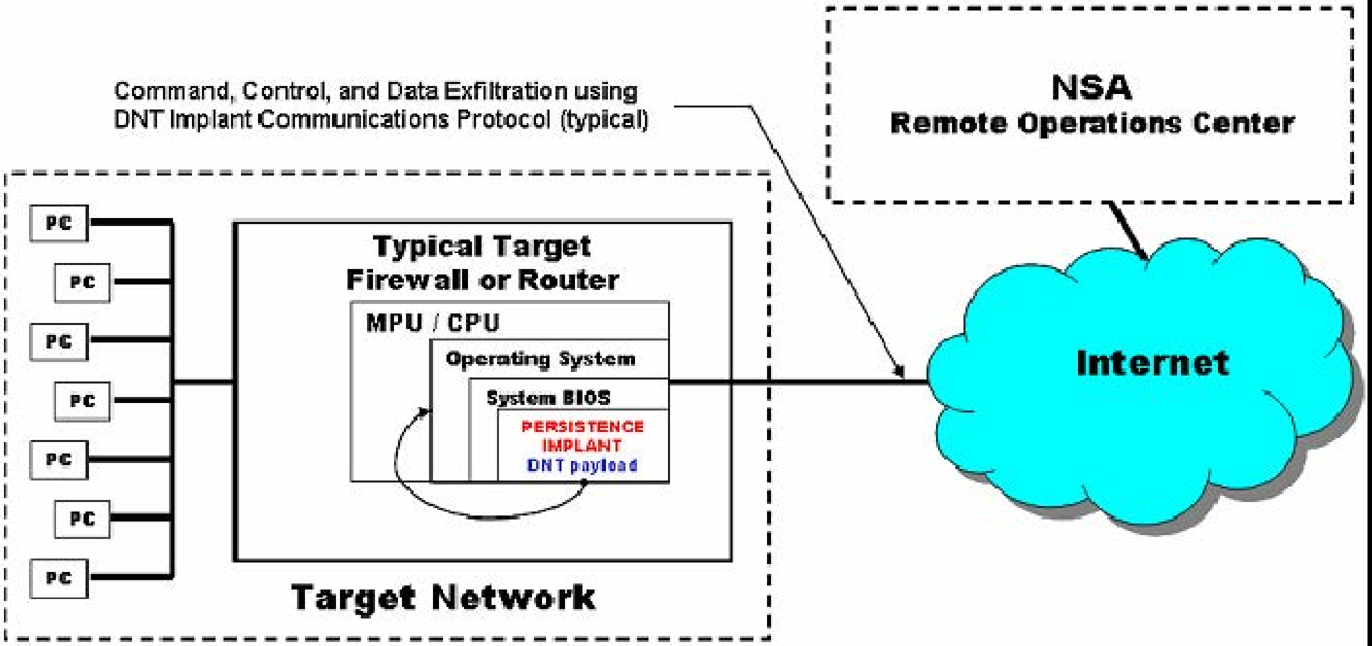
(TS//SI//REL) Operationally, VALIDATOR initiates a call home. SOMBERKNAVE triggers from the named event and tries to associate with an access point. If connection is successful, data is sent over 802.11 to the ROC. VALIDATOR receives instructions, downloads OLYMPUS, then disassociates and gives up control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



(software) “Implants”

- VALIDATOR, COMMONDEER, OLYMPUS, UNITED RAKE, STUXNET and many many more
- With payloads for you...
- #BADBIOS
- SMM
- iPhone
- Routers (Juniper, Huawei, Cisco, etc)
- SIM cards (remote, local)
- Hard drive firmware

(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.

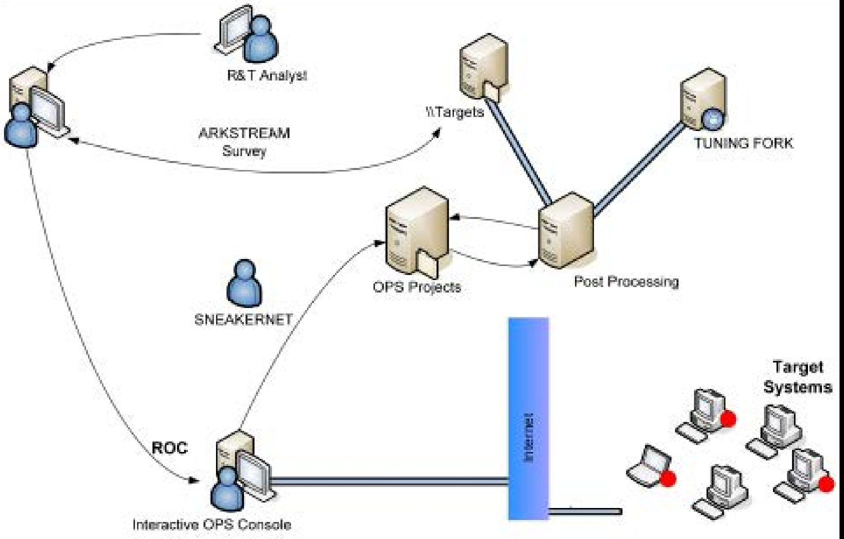


(S//SI//REL) STUCCOMONTANA Concept of Operations

(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

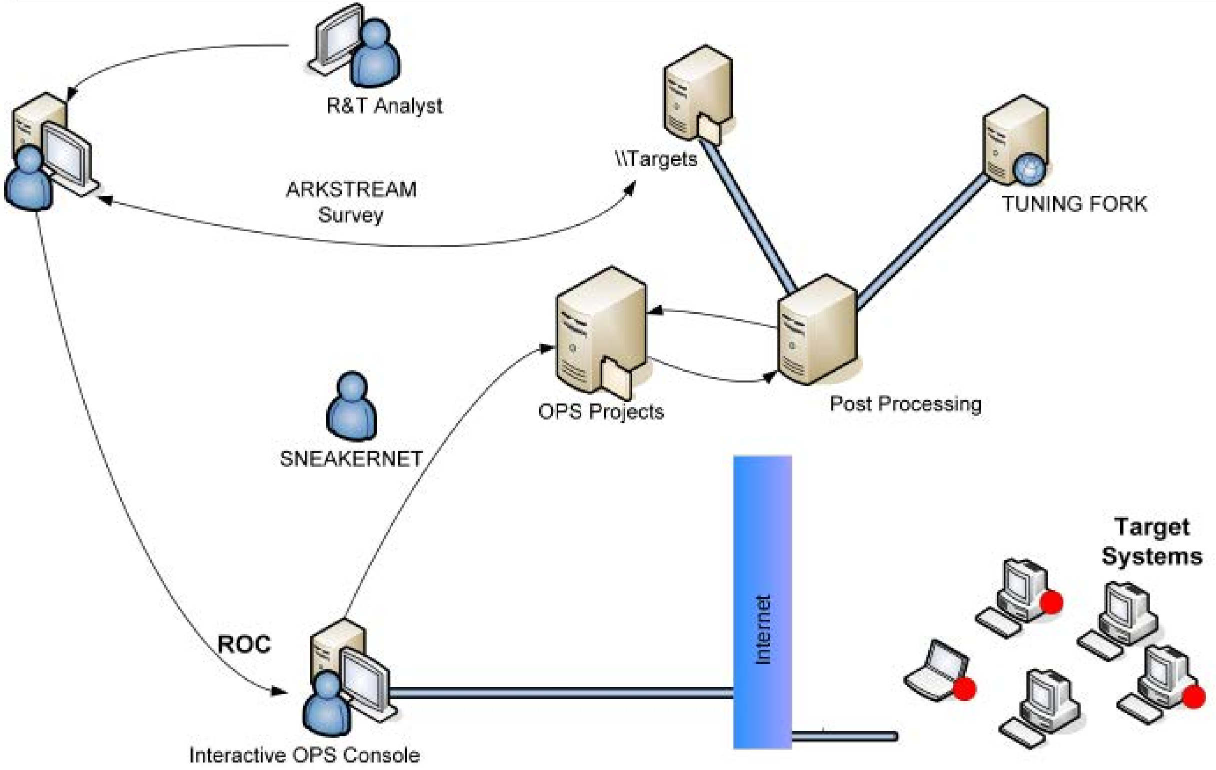
(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(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) 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.

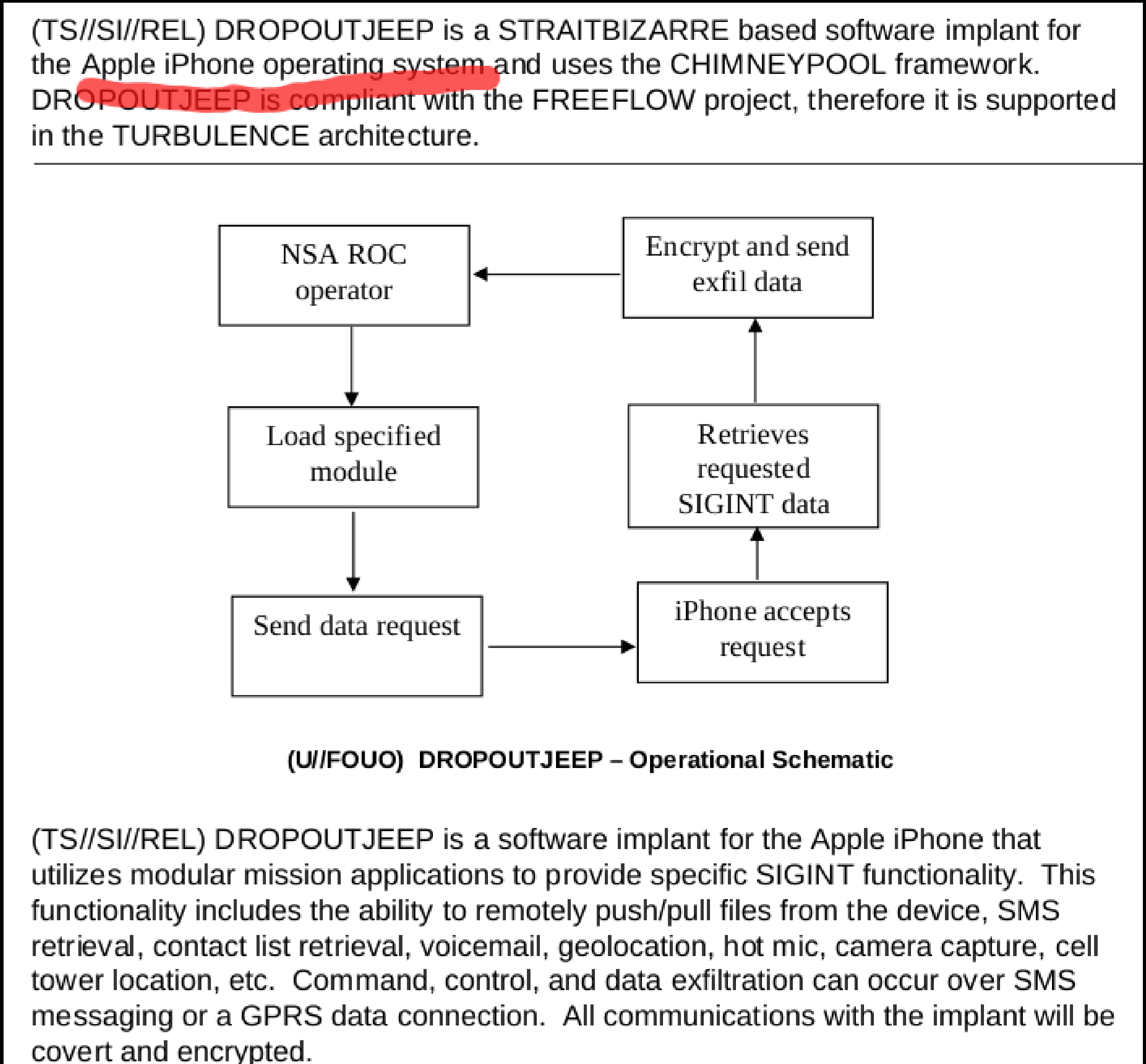


(TS//SI//REL) DEITYBOUNCE Extended Concept of Operations

(TS//SI//REL) This technique supports multi-processor systems with RAID hardware and Microsoft Windows 2000, 2003, and XP. It currently targets Dell PowerEdge 1850/2850/1950/2950 RAID servers, using BIOS versions A02, A05, A06, 1.1.0, 1.2.0, or 1.3.7.

Looking for NSA malware?

Look for samples that implement RC6 and that emit encrypted UDP traffic.



(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.

NSA ROC operator
Load specified module
Send data request
iPhone accepts request
Retrieves requested SIGINT data
Encrypt and send exfil data

(U//FOUO) DROPOUTJEEP – Operational Schematic

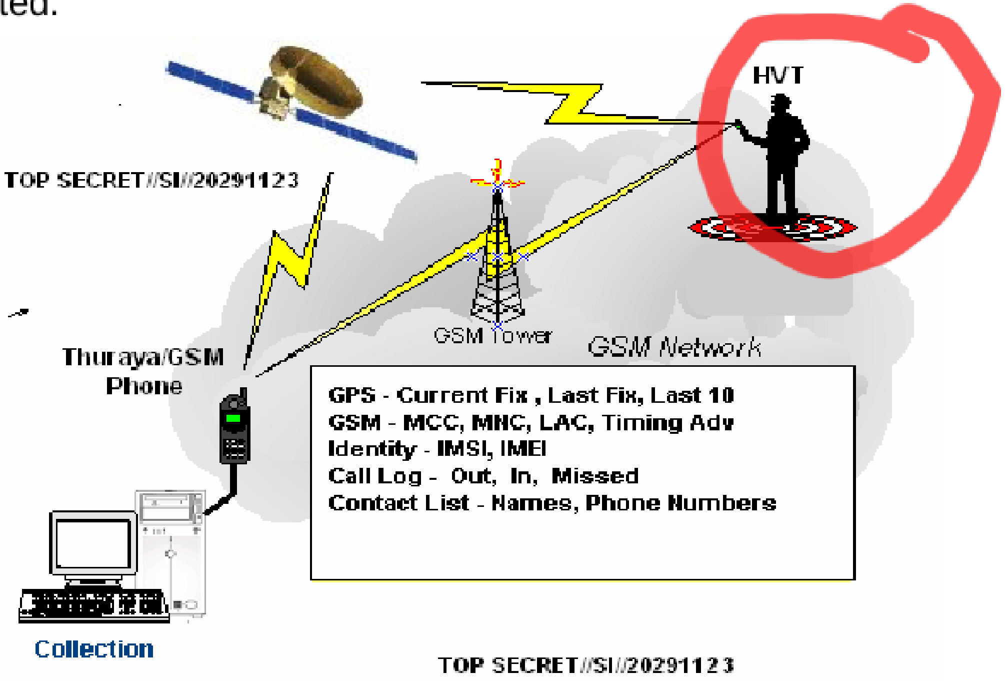
(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, 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.

iOS

The NSA claims in their QUANTUMTHEORY documents that every attempt to implant iOS will *always succeed*.

WTF?

(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.

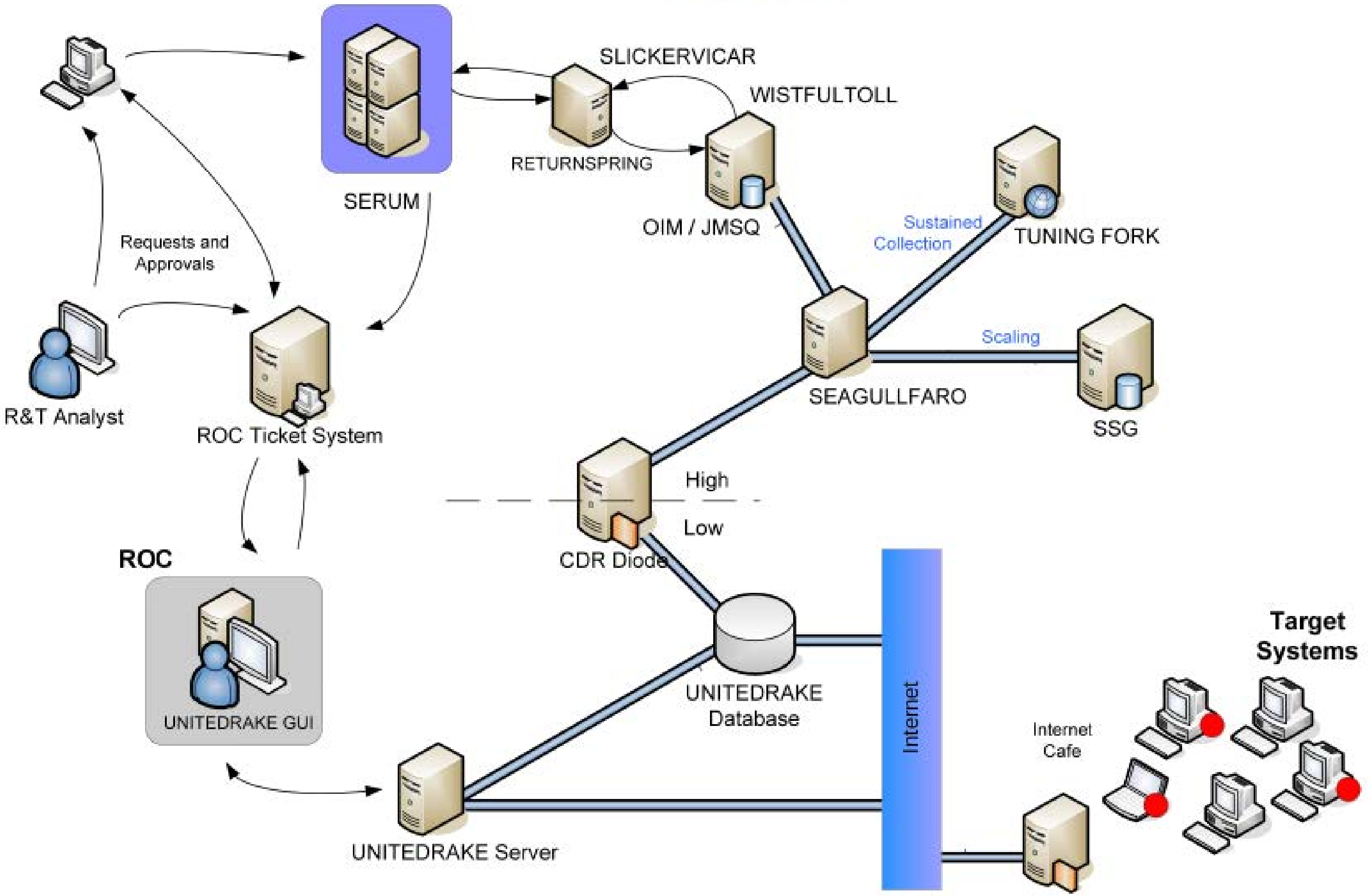


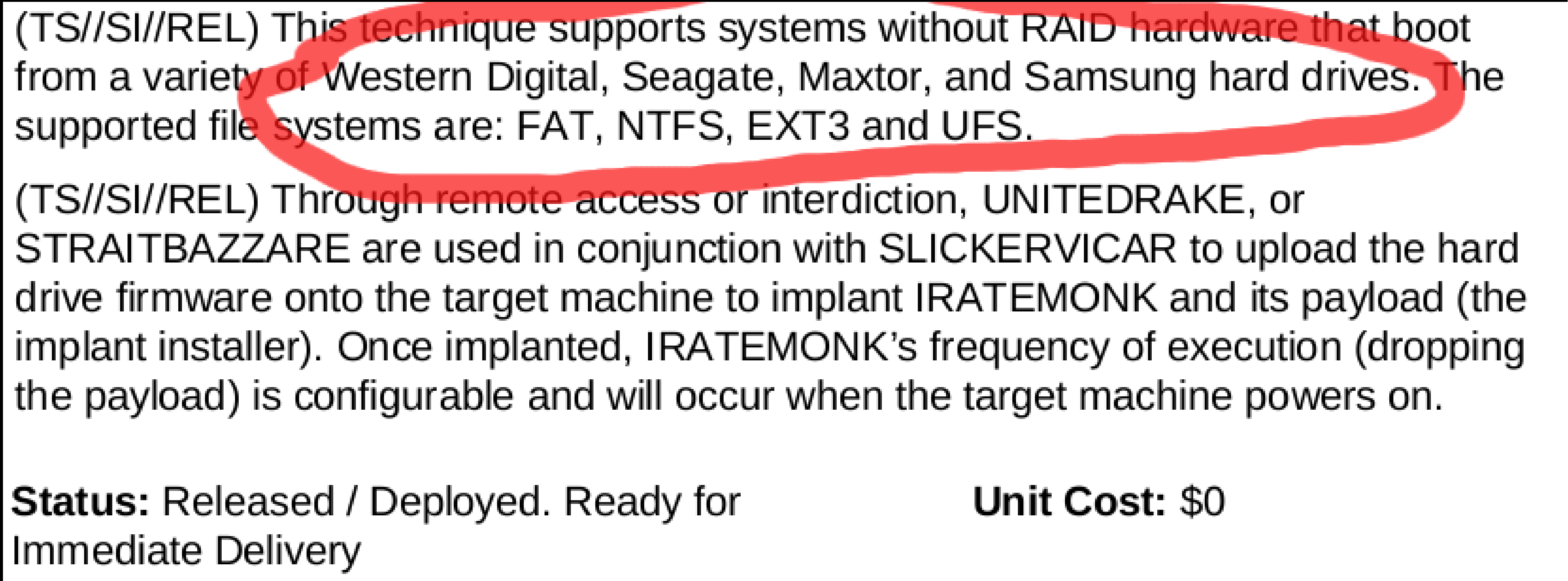
GPS - Current Fix , Last Fix, Last 10
GSM - MCC, MNC, LAC, Timing Adv
Identity - IMSI, IMEI
Call Log - Out, In, Missed
Contact List - Names, Phone Numbers

(U//FOUO) TOTECHASER – Operational Schematic

(TS//SI//REL) TOTECHASER will use SMS messaging for the command, control, and data exfiltration path. The initial capability will use covert SMS messages to communicate with the handset. These covert messages can be transmitted in

(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.



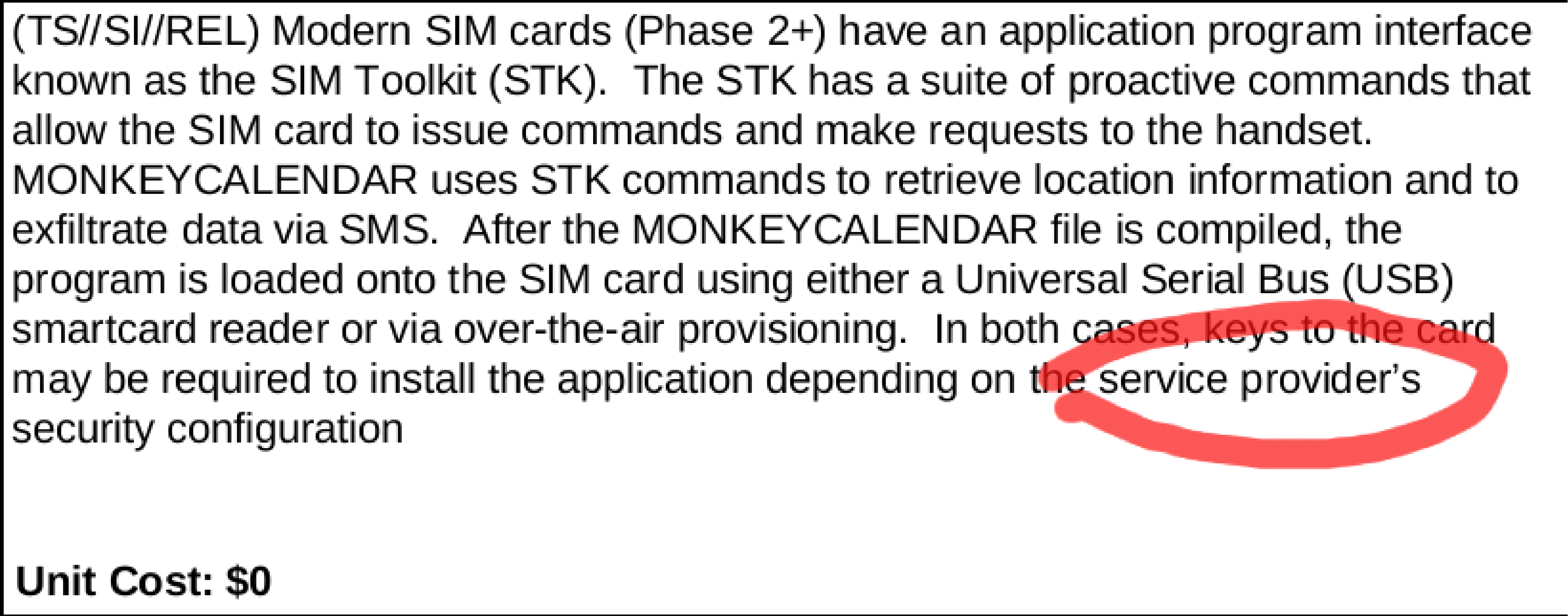


(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(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.

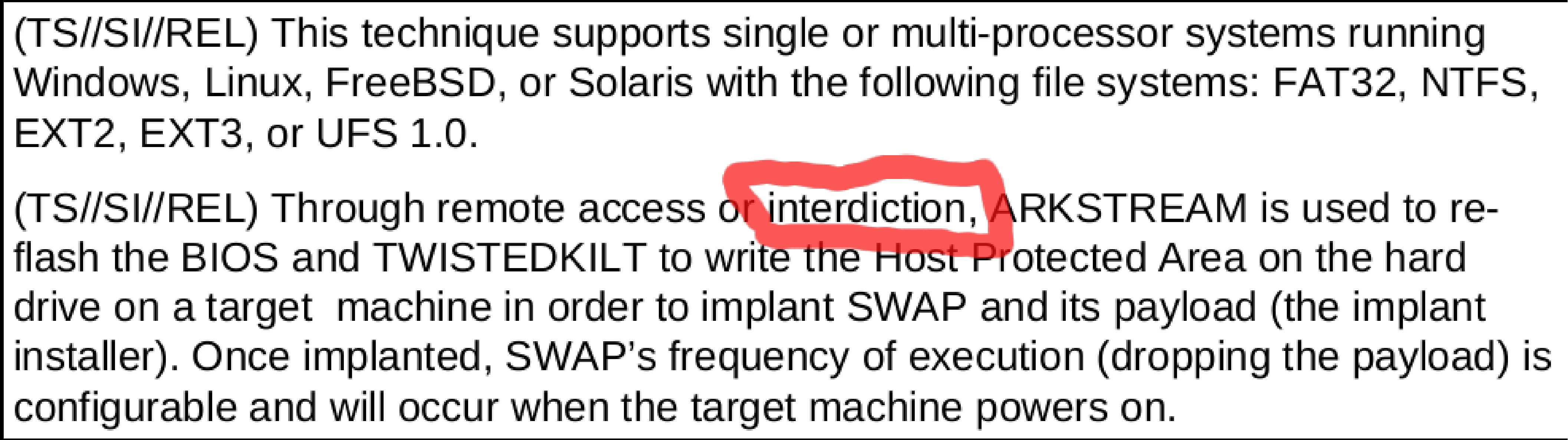
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0



(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. MONKEYCALENDAR uses STK commands to retrieve location information and to exfiltrate data via SMS. After the MONKEYCALENDAR file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration

Unit Cost: $0



(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.

Interdiction

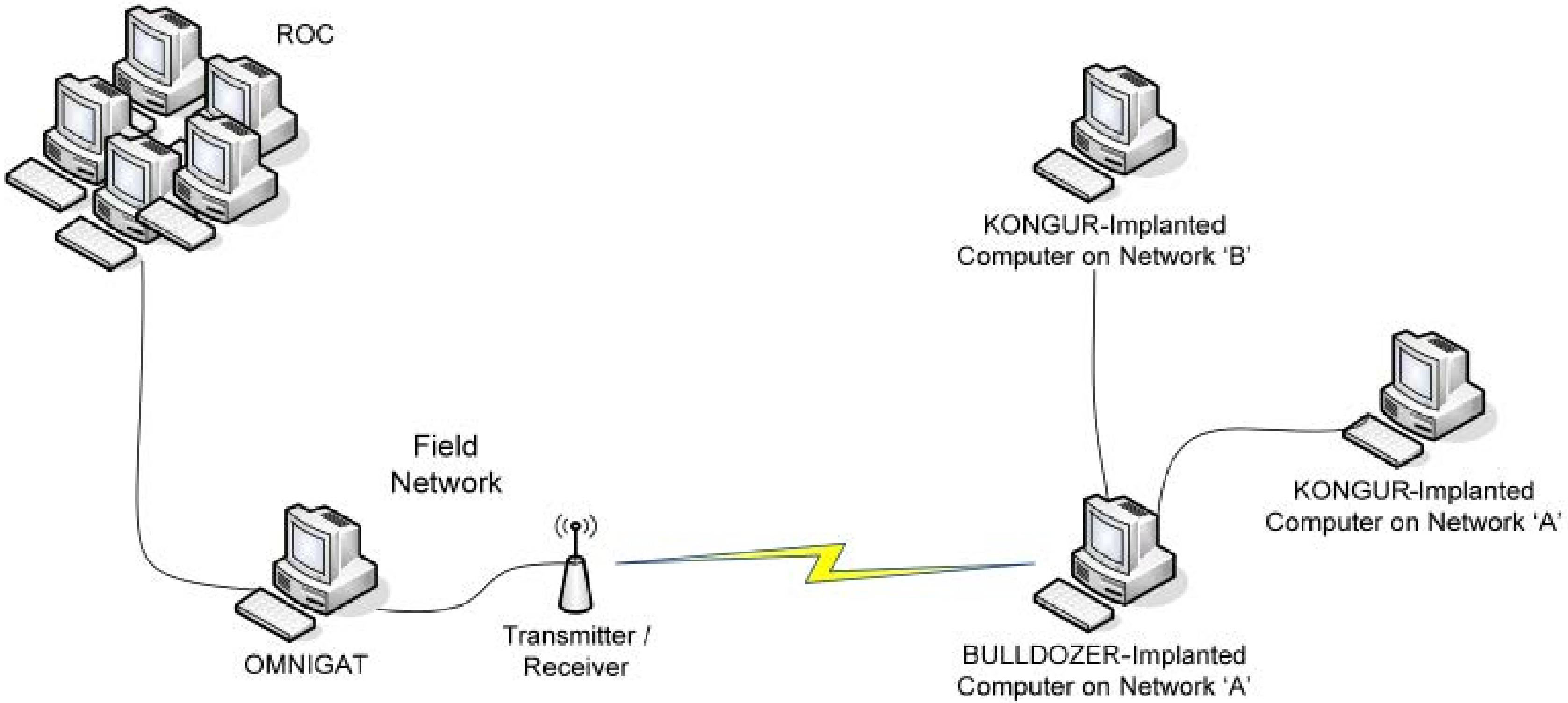
So-called “off-net' operations include tampering with your hardware while it is being shipped!

They call this process “Interdiction”
Remember: Don't forget to check **your** gear!

Hardware implants

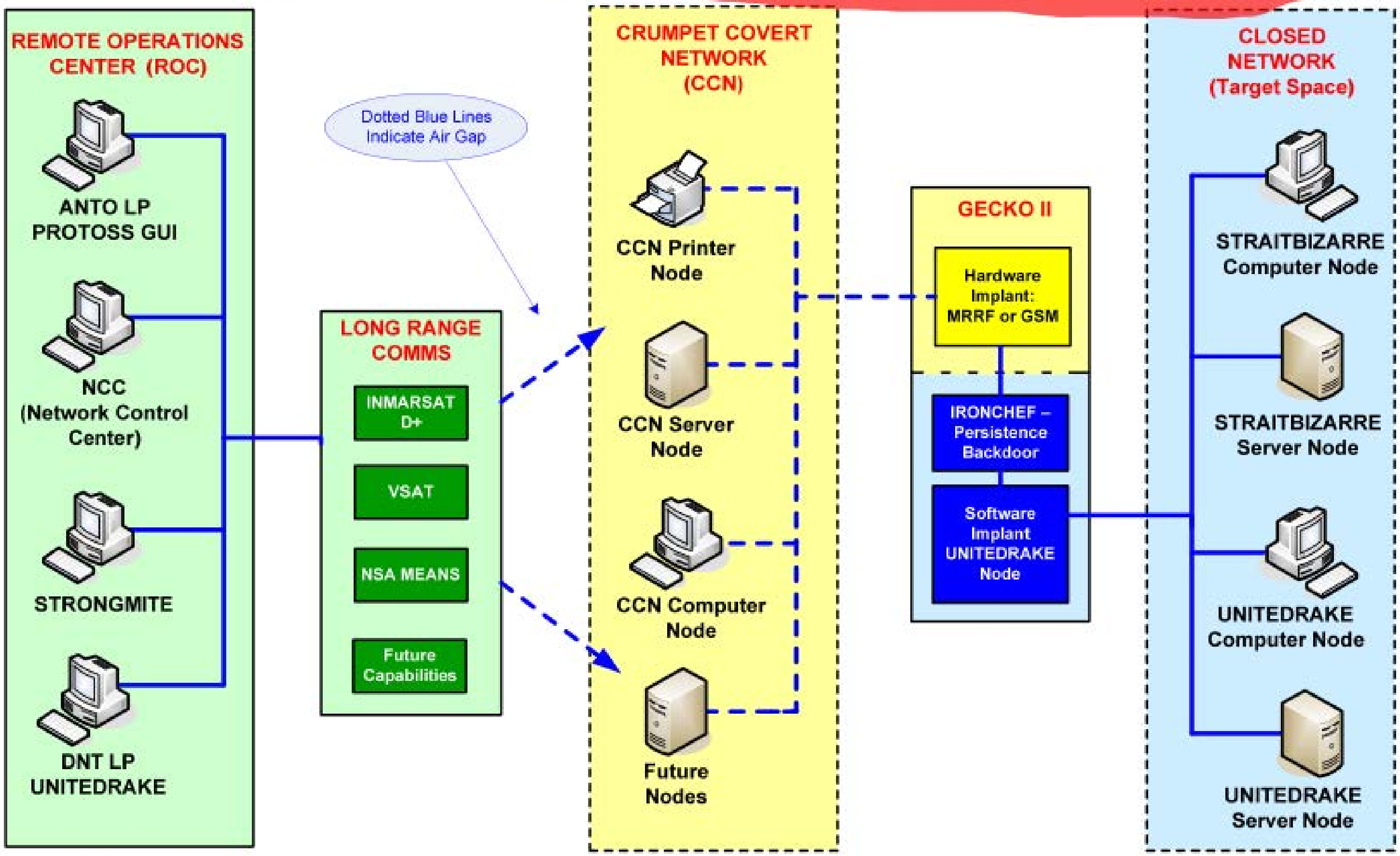
- Hardware interdiction is used to attack:
- PCI-BUS
- i2c bus
- JTAG (with persistence)
- Modification of cellphone hardware
- Modified USB cable and USB ports
- Modified network cards
- Lots of interesting custom hardware

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

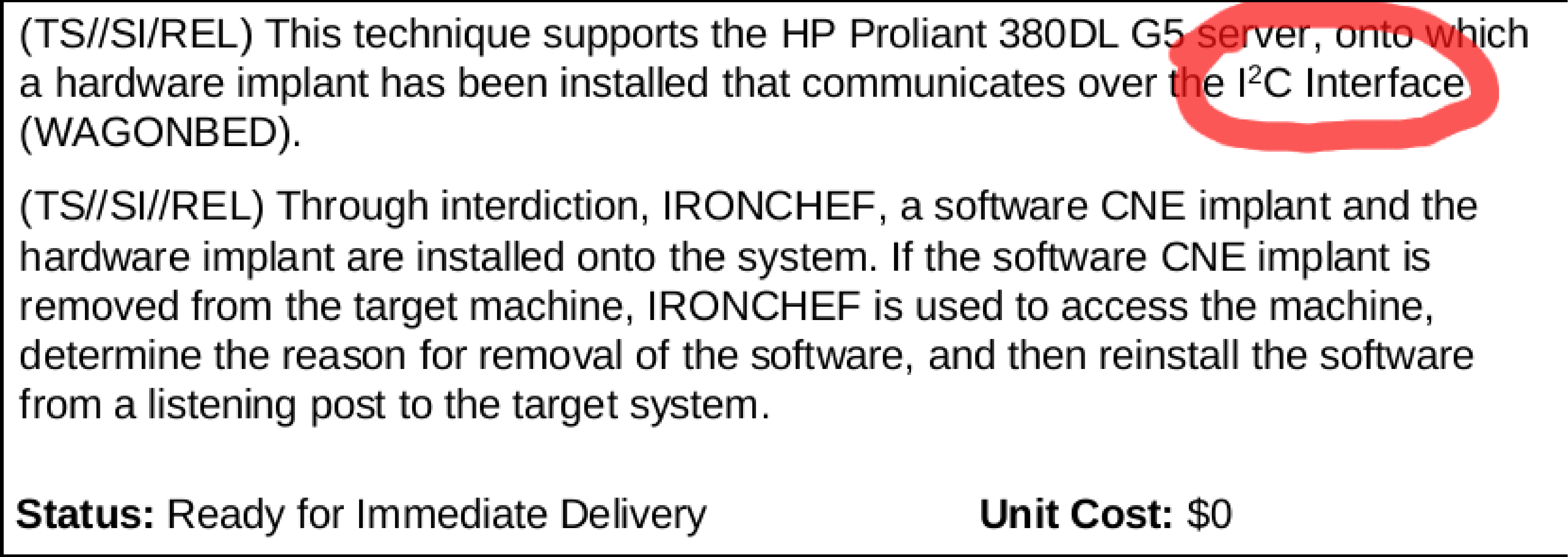

ROC
KONGUR-Implanted Computer on Network 'B'
Field Network
KONGUR-Implanted Computer on Network 'A'
OMNIGAT
Transmitter / Receiver
BULLDOZER-Implanted Computer on Network 'A'

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

(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.


REMOTE OPERATIONS CENTER (ROC)
ANTO LP PROTOSS GUI
NCC (Network Control Center)
STRONGMITE
DNT LP UNITEDRAKE
Dotted Blue Lines Indicate Air Gap
LONG RANGE COMMS
INMARSAT D+
VSAT
NSA MEANS
Future Capabilities
CRUMPET COVERT NETWORK (CCN)
CCN Printer Node
CCN Server Node
CCN Computer Node
Future Nodes
GECKO II
Hardware Implant: MRRF or GSM
IRONCHEF – Persistence Backdoor
Software Implant UNITEDRAKE Node
CLOSED NETWORK (Target Space)
STRAITBIZARRE Computer Node
STRAITBIZARRE Server Node
UNITEDRAKE Computer Node
UNITEDRAKE Server Node

(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 I^2C Interface (WAGONBED).

(TS//SI//REL) Through interdiction, IRONCHEF, a software CNE implant and the hardware implant are installed onto the system. If the software CNE implant is removed from the target machine, IRONCHEF is used to access the machine, determine the reason for removal of the software, and then reinstall the software from a listening post to the target system.

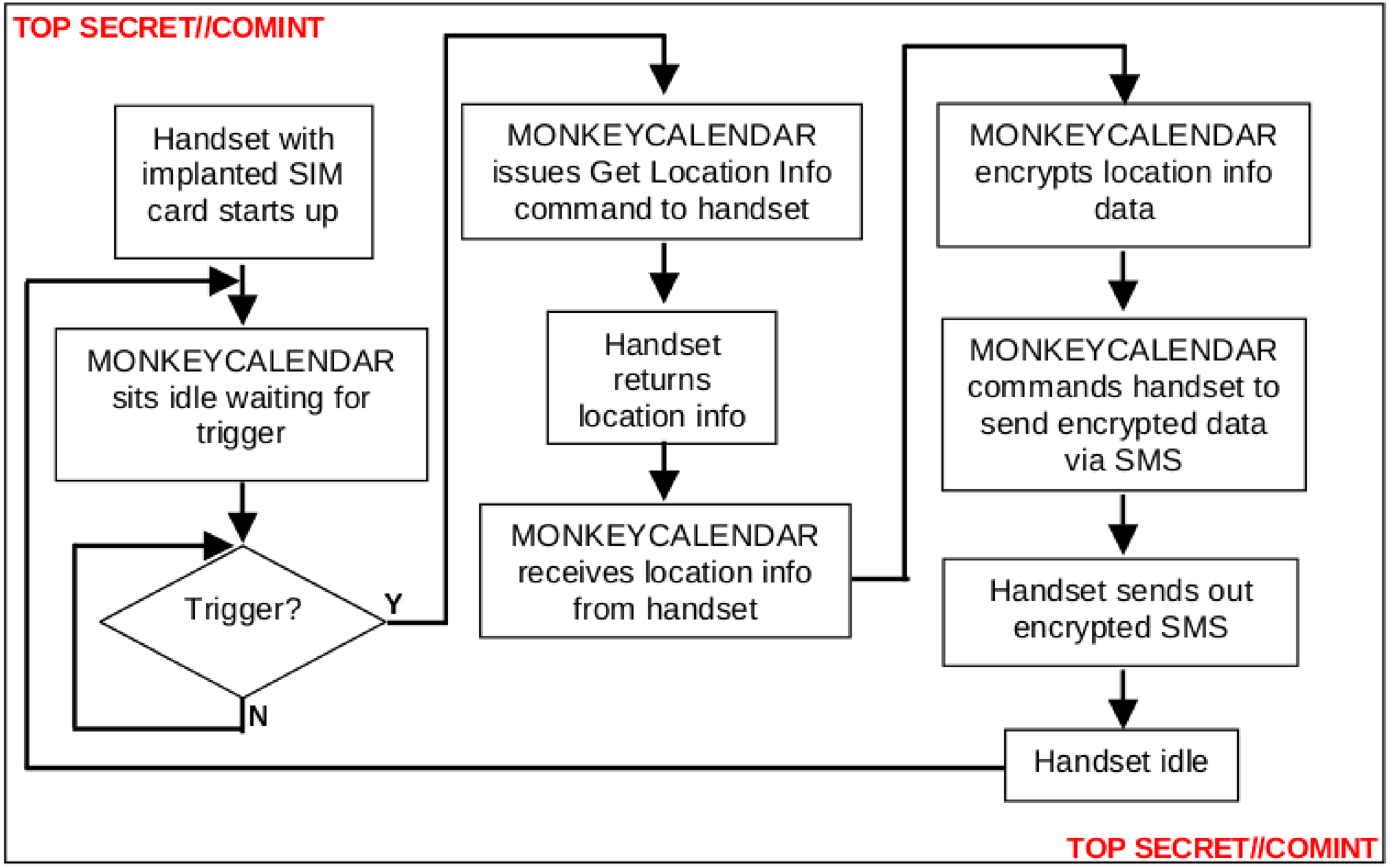
Status: Ready for Immediate Delivery **Unit Cost:** $0

Sabotage of US companies

Do you notice the common theme of sabotaging companies?

US President Obama's own advisors recently issued a report advising against this strategy.

(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).



TOP SECRET//COMINT

Handset with implanted SIM card starts up

MONKEYCALENDAR sits idle waiting for trigger

MONKEYCALENDAR issues Get Location Info command to handset

Handset returns location info

MONKEYCALENDAR receives location info from handset

MONKEYCALENDAR encrypts location info data

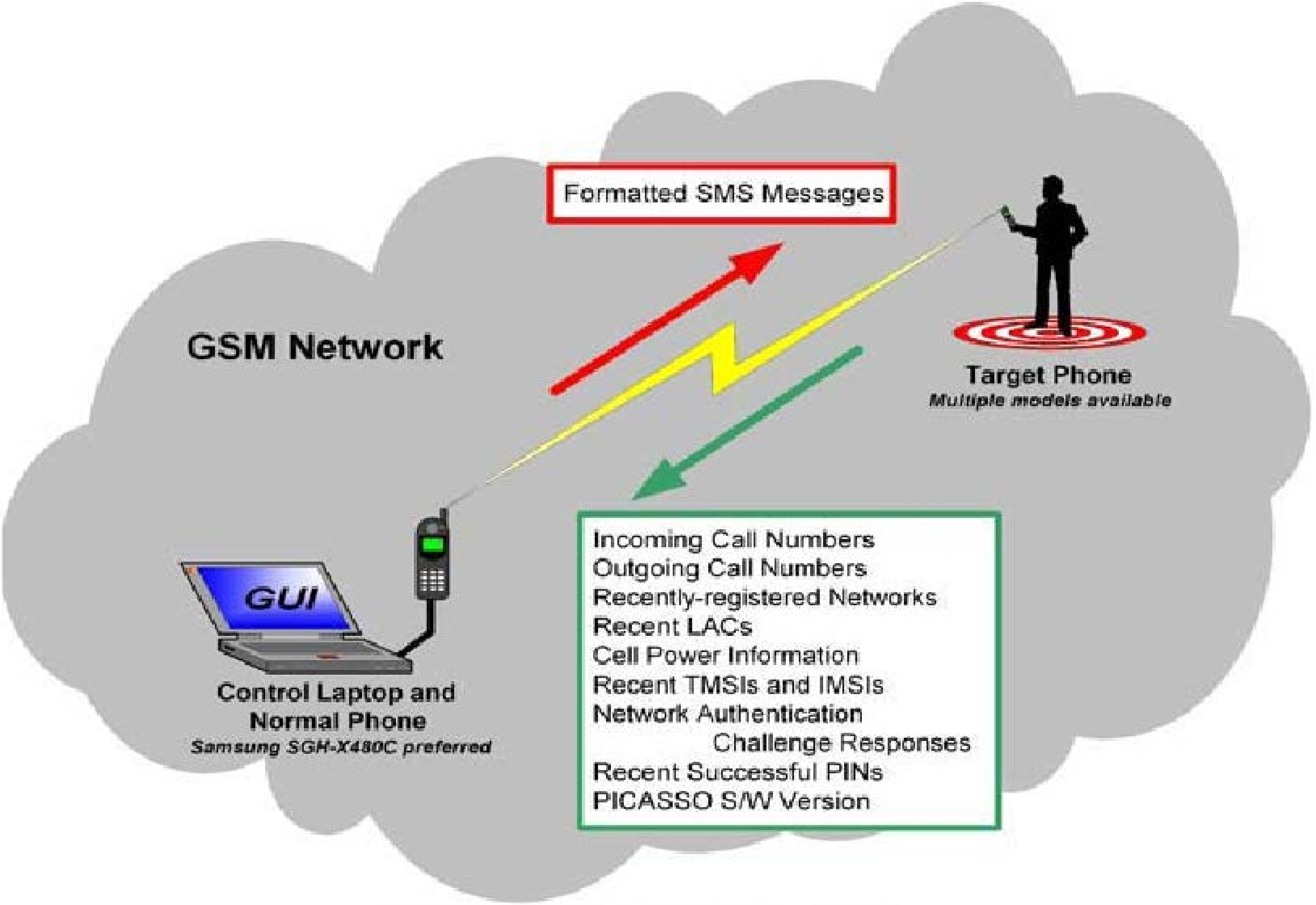
MONKEYCALENDAR commands handset to send encrypted data via SMS

Handset sends out encrypted SMS

Handset idle

TOP SECRET//COMINT

(U//FOUO) MONKEYCALENDAR – Operational Schematic



GSM Network

Formatted SMS Messages

Target Phone

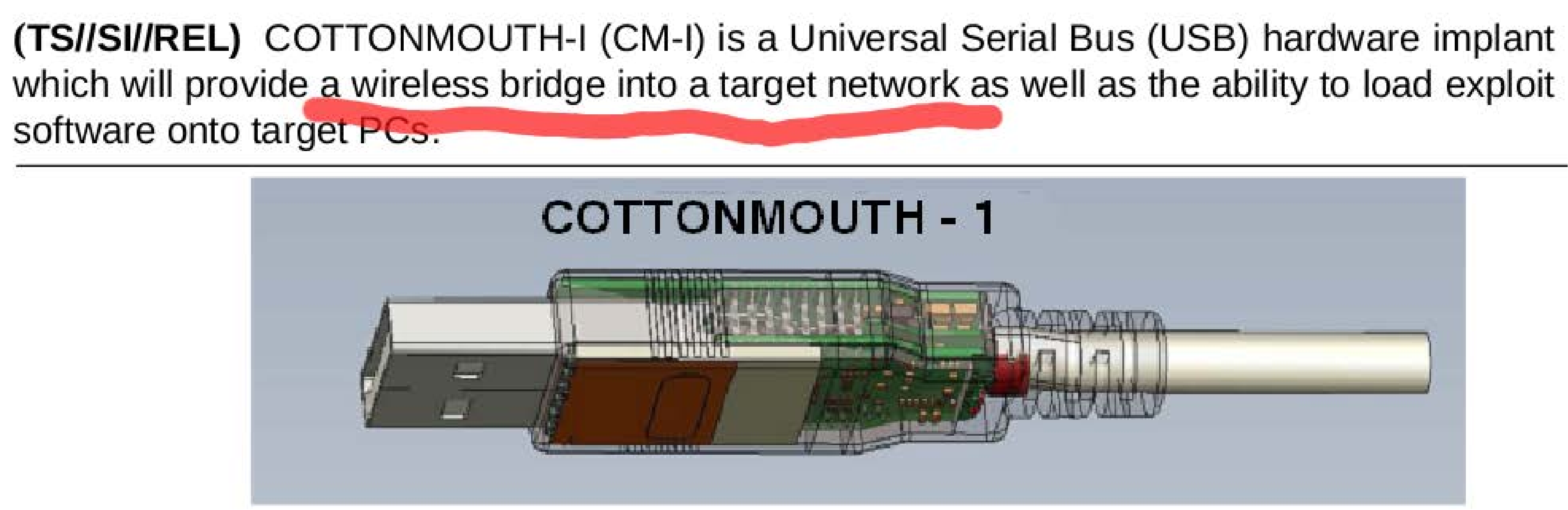
Multiple models available

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



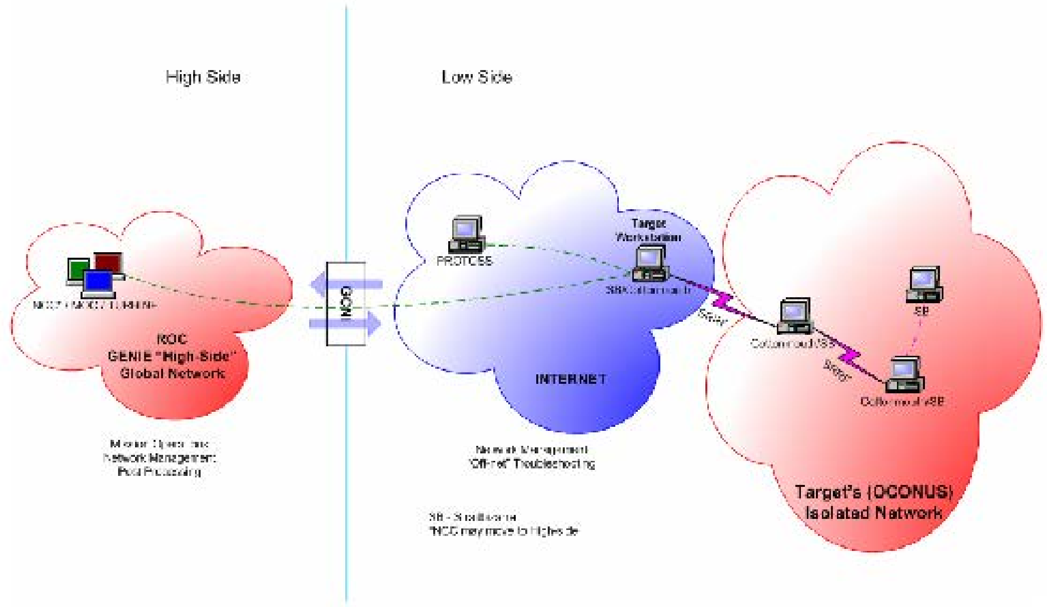
(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

COTTONMOUTH - 1

(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

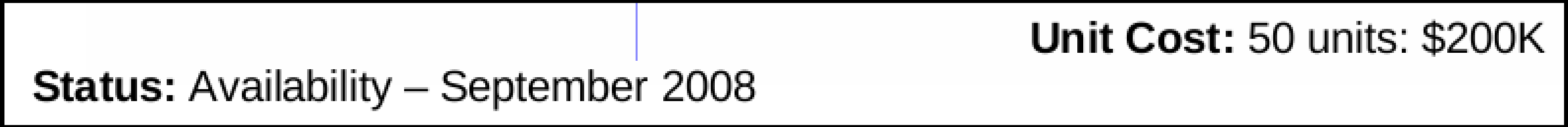
Unit Cost: 50 units: $1,015K

(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

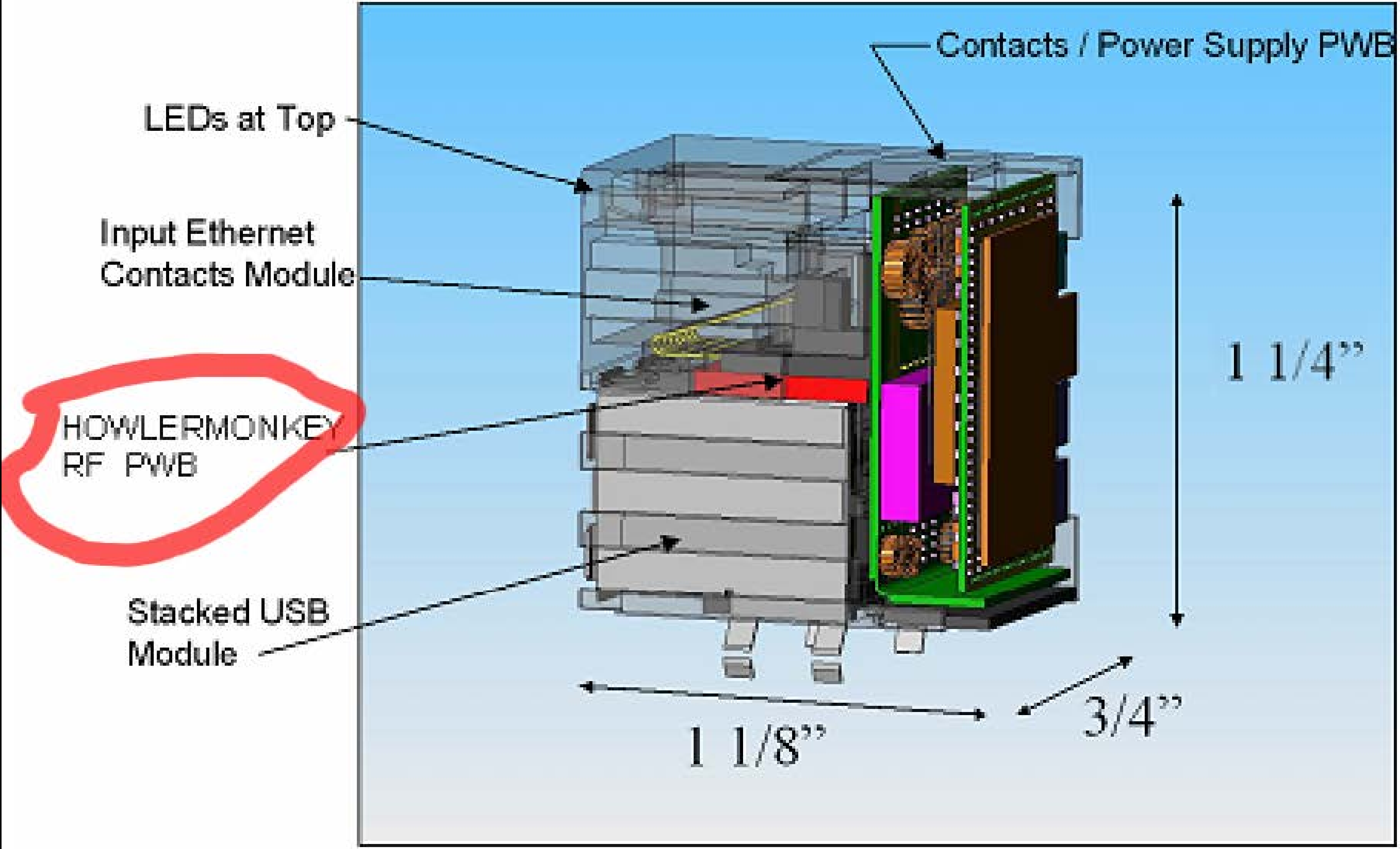
COTTONMOUTH-II is cheap too!



Unit Cost: 50 units: $200K

Status: Availability – September 2008

...unless you count the cost to our liberty!



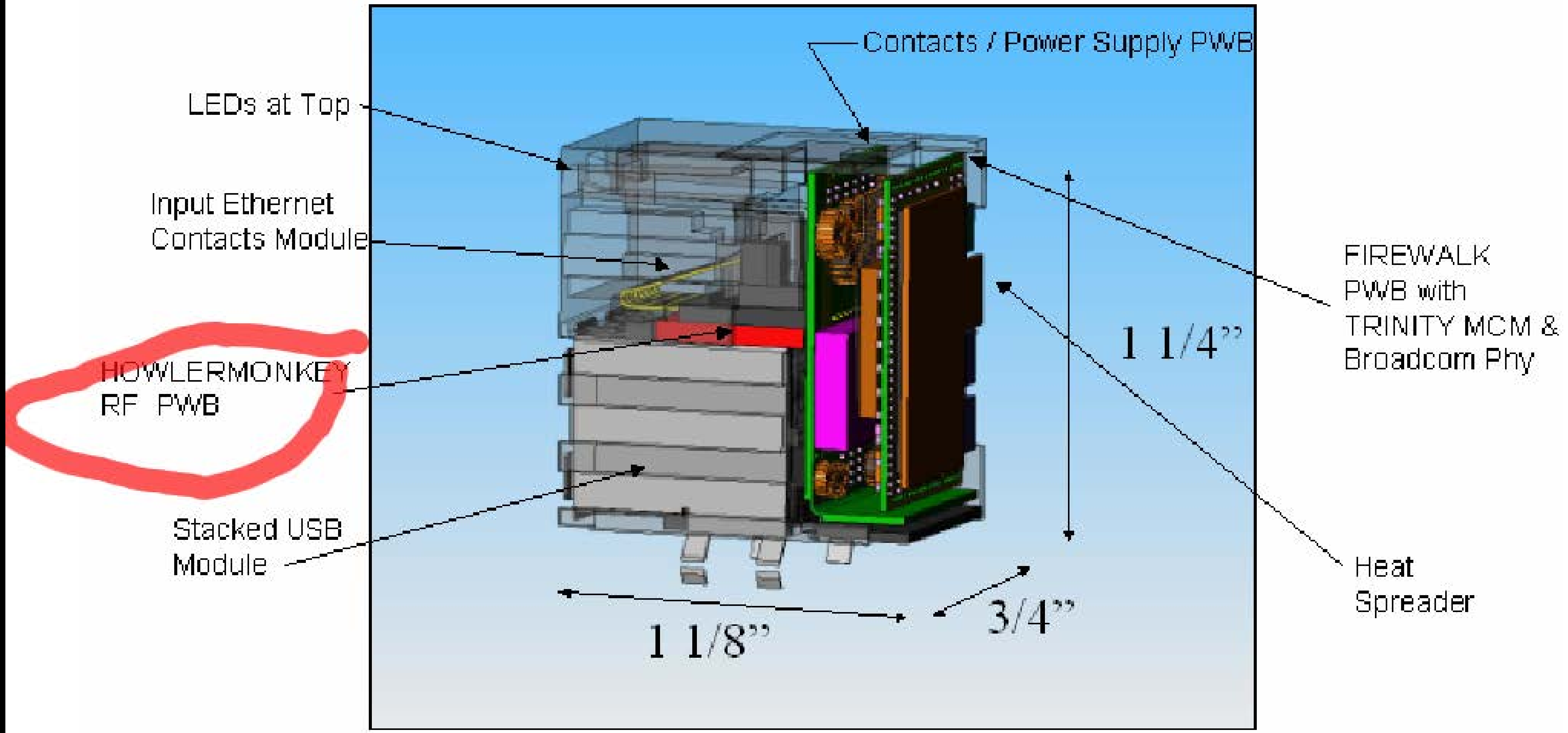
Contacts / Power Supply PWB

LEDs at Top

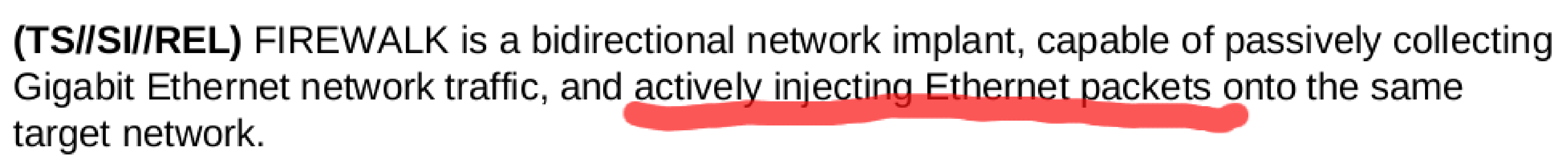
Input Ethernet
Contacts Module

HOWLERMONKEY
RF PWB

Stacked USB
Module


Contacts / Power Supply PWB
LEDs at Top
Input Ethernet Contacts Module
HOWLERMONKEY RF PWB
Stacked USB Module
FIREWALK PWB with TRINITY MCM & Broadcom Phy
Heat Spreader
1 1/4"
1 1/8"
3/4"

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



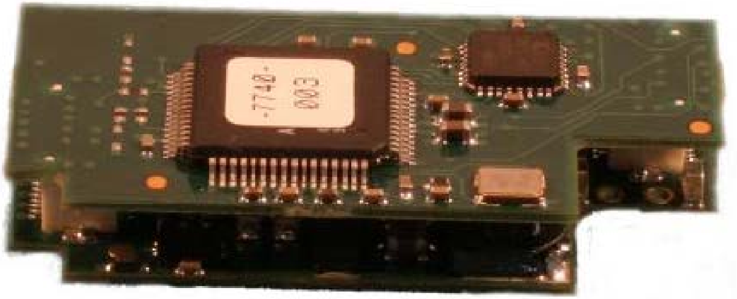
(TS//SI//REL) FIREWALK is a bidirectional network implant, capable of passively collecting Gigabit Ethernet network traffic, and actively injecting Ethernet packets onto the same target network.

GODSURGE

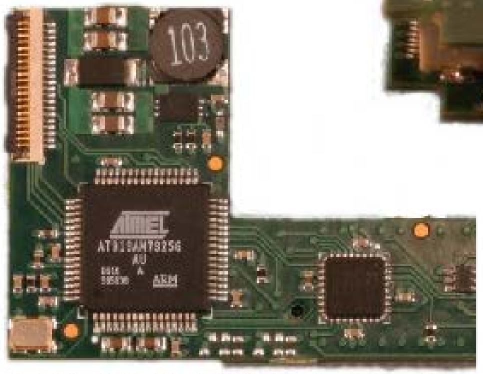
ANT Product Data

(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.

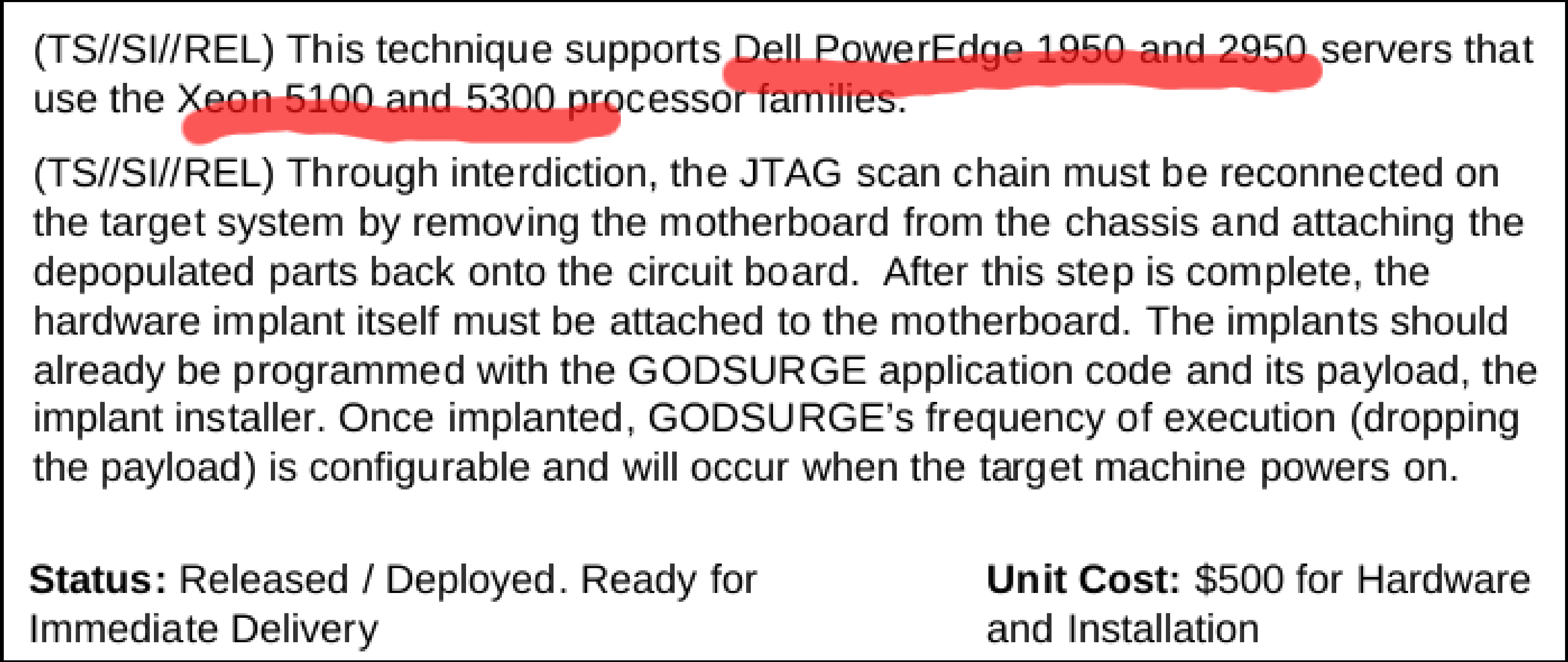
06/20/08



(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.

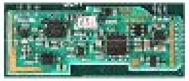
(TS//SI//REL) Through interdiction, the JTAG scan chain must be reconnected on the target system by removing the motherboard from the chassis and attaching the depopulated parts back onto the circuit board. After this step is complete, the hardware implant itself must be attached to the motherboard. 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

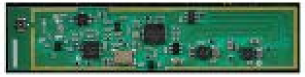
(TS//SI//REL) HOWLERMONKEY is a custom Short to Medium Range Implant RF Transceiver. It is used in conjunction with a digital core to provide a complete implant.

HOWLERMONKEY - SUTURESAILOR



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

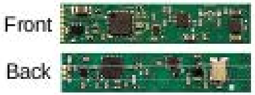
HOWLERMONKEY - YELLOWPIN



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

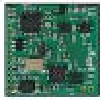
(Actual Size)

HOWLERMONKEY - SUTURESAILOR



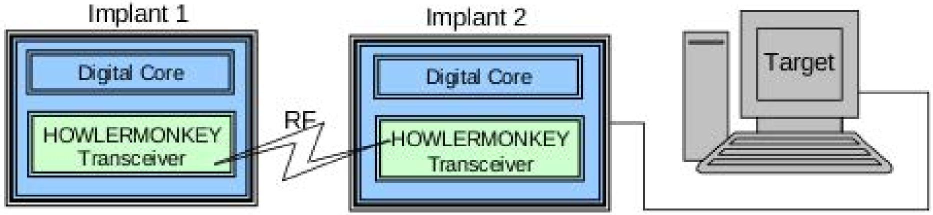
1.20" (30.5 mm)
x 0.23" (6 mm)

HOWLERMONKEY - FIREWALK



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

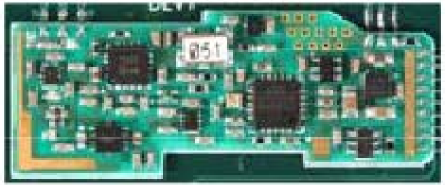
(TS//SI//REL) HOWLERMONKEY is a COTS-based transceiver designed to be compatible with CONJECTURE/SPECULATION networks and STRIKEZONE devices running a HOWLERMONKEY personality. PCB layouts are tailored to individual implant space requirements and can vary greatly in form factor.



Status: Available – Delivery 3 months

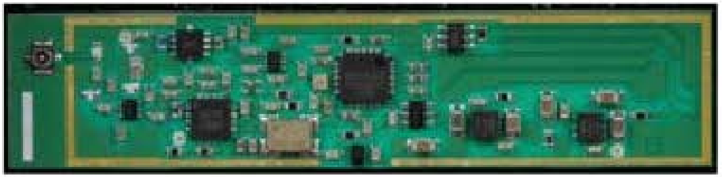
Unit Cost: 40 units: $750/ each
25 units: $1,000/ each

HOWLERMONKEY - SUTURESAILOR



1.23” (31.25 mm) x 0.48” (12.2 mm)

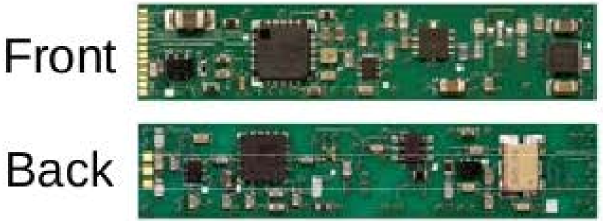
HOWLERMONKEY - YELLOWPIN



2” (50.8 mm) x 0.45” (11.5 mm)

(Actual Size)

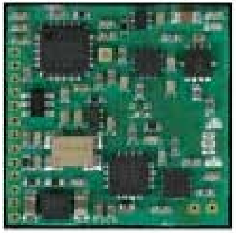
HOWLERMONKEY - SUTURESAILOR



1.20” (30.5 mm) x 0.23” (6 mm)

!

HOWLERMONKEY - FIREWALK



0.63” (16 mm) x 0.63” (16 mm)

Whew, it's all stuff we thought...

Ha, just kidding!

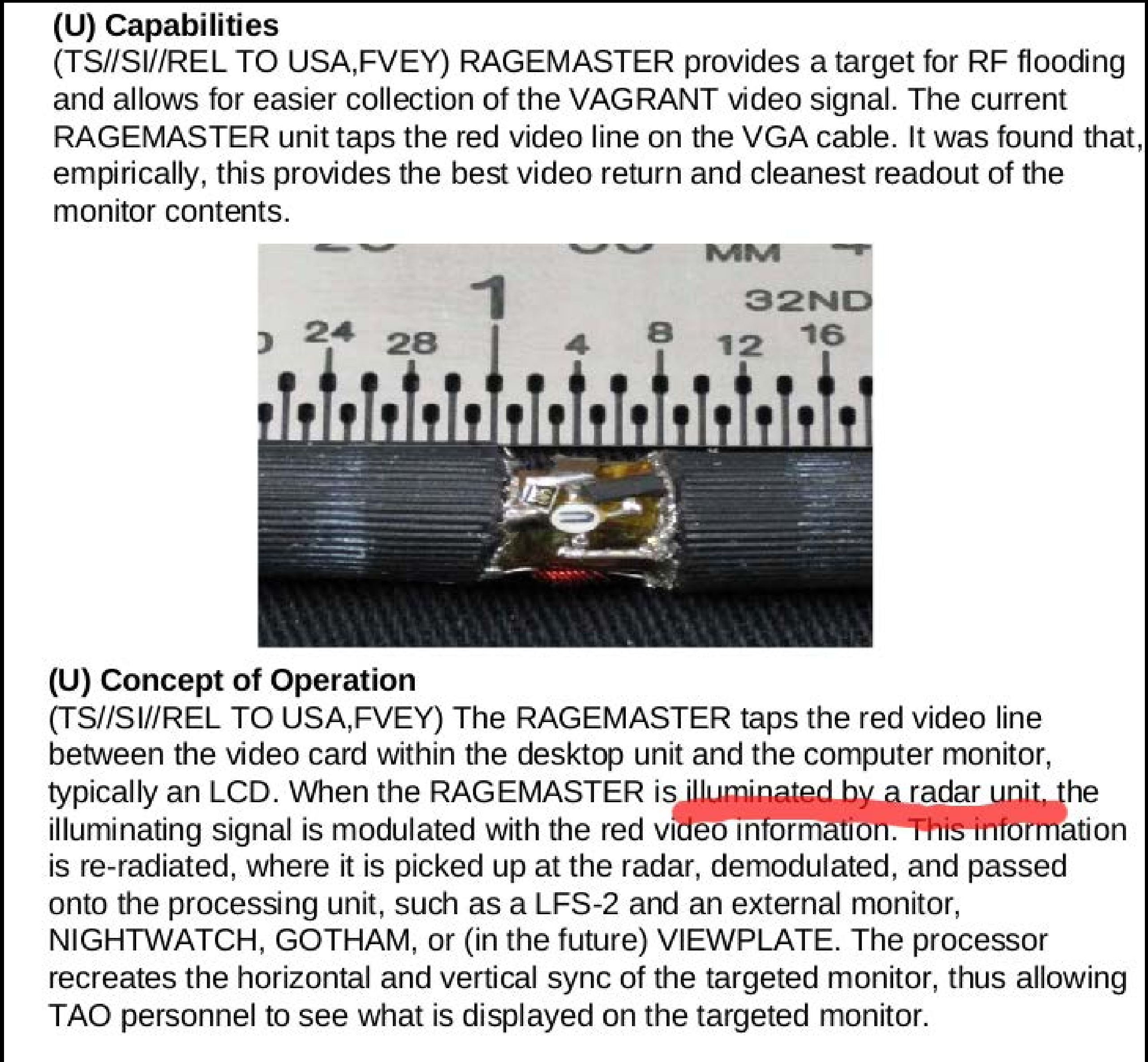
Specialized Philip K. Dick inspired nightmares

- Continuous Wave generators
  - ...beaming into people
- Huh, no data on human safety for these tools?
  - What happened to Hugo exactly? :-)
- Room bugs
- Data exfiltration via active radar
- Video exfiltration via added hardware with radar
- Keyboard retro-reflector data exfiltration
- Location tracking of targets (kill 'em w/drones)

(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) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

(U) Capability Summary

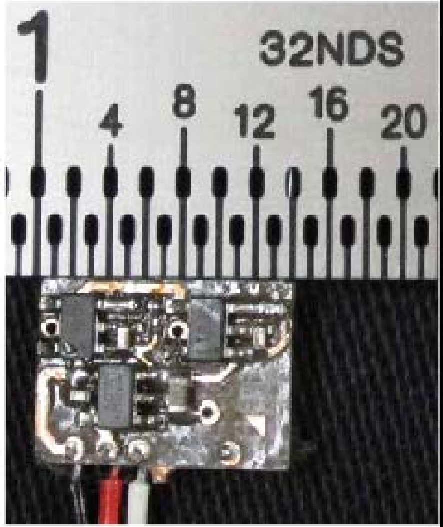
(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^16 (65536) frames.

(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.

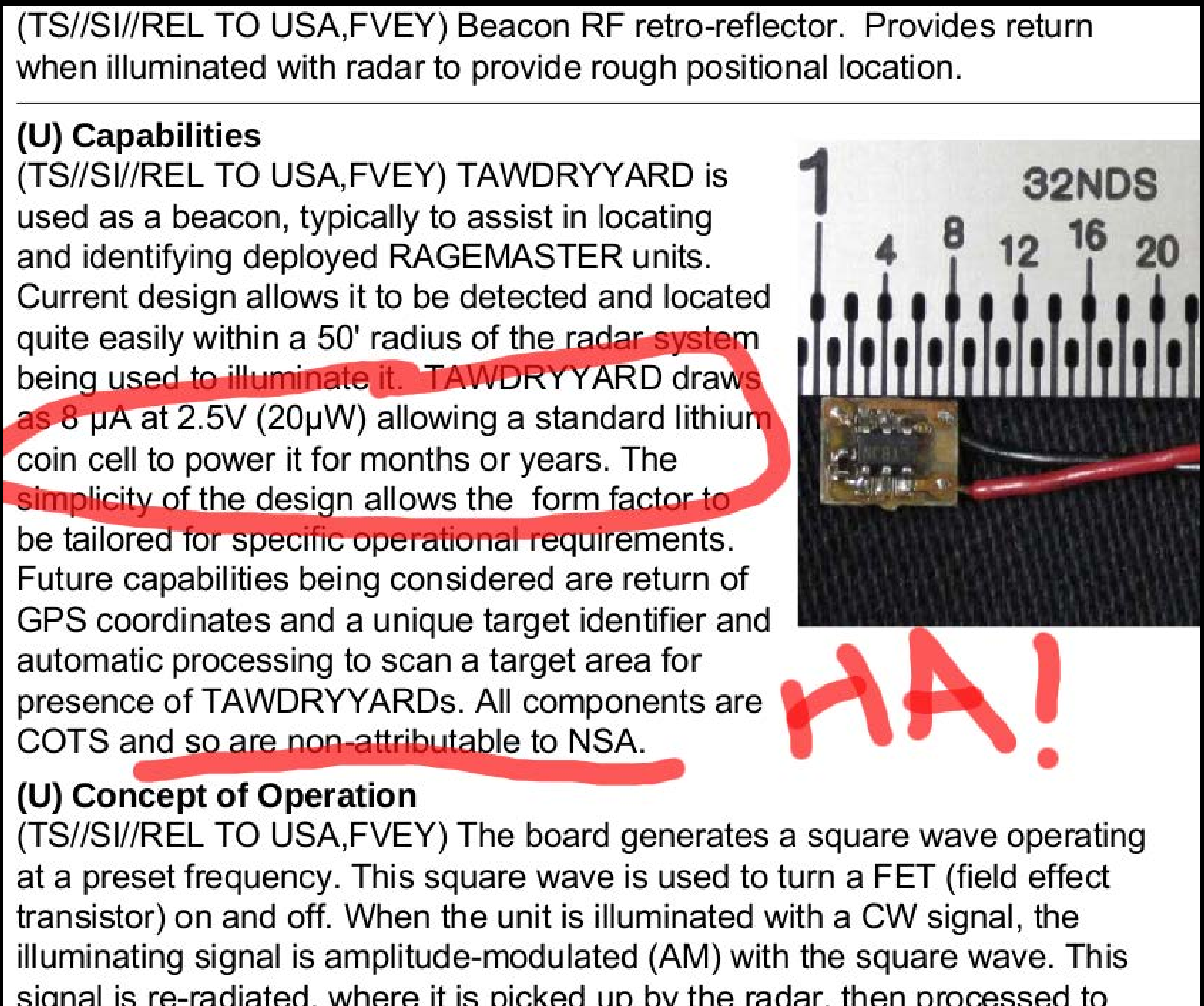
(U) Capabilities

(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!

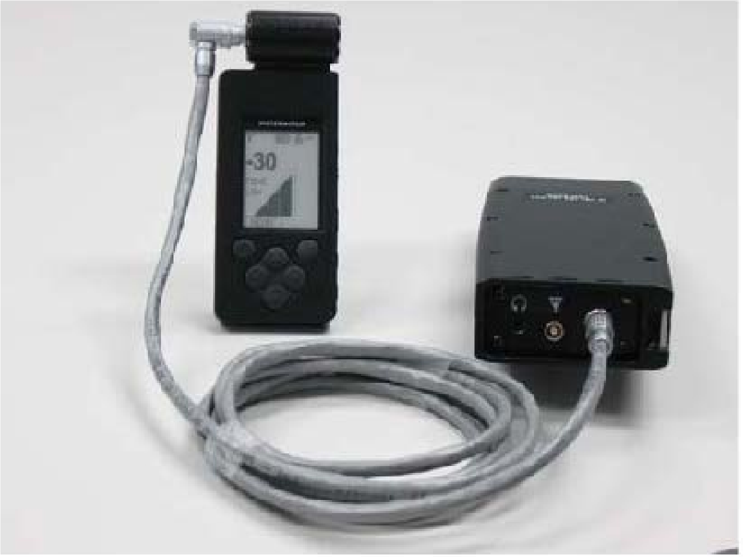
(U) Concept of Operation

(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:

- 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

Happy New Year!

Thanks for your material support!

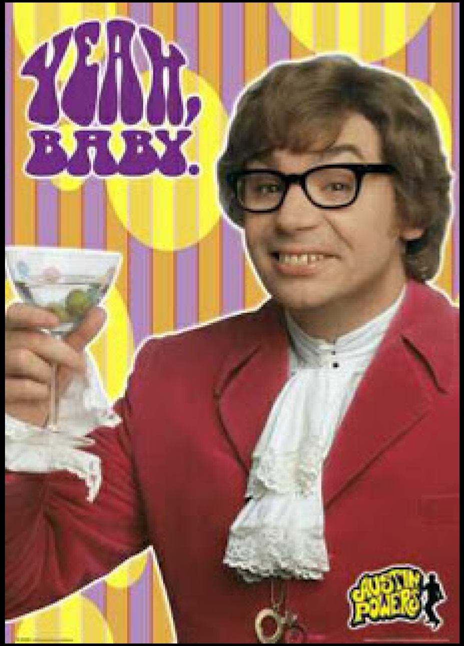
- Andy Müller-Maguhn
- Eric Holder (Jr)
- Emperor Alexander
- Julian Assange
- Laura Poitras
- Marcel, Judith, Christian, Holger, Jorg and others Der Spiegel
- US President Obama
- The brave people who came forward to tell us their stories
  - Especially our anonymous supporters, thank you!

We encourage you to visit Der Spiegel Online for our extensive coverage in English and German!

Thank you!

Questions?

“Resistance isn't futile, it's the new mode of participation.”



Act III? - It's up to you!
Leak more documents!