

NSA ANT Rechner, 30C3, Jacob Appelbaum, 30 December 2013

Für das Kapern fremder Computer hat die NSA-Abteilung ANT eine ganze Reihe von Varianten im Angebot. Es gibt Hardware-Einheiten, die in die Rechner eingebaut werden können – etwa, indem man die Computer bei der Auslieferung abfängt. Diesen Prozess nennt die NSA "Interdiction". Andere Spionageprogramme lassen sich aus der Ferne auf dem Rechner unterbringen, durch "remote access". Manche der NSA-Programme sorgen dafür, dass der gehackte Computer heimlich über W-Lan-Verbindungen Daten ausleitet, wenn sich die Gelegenheit bietet (SOMBERKNAVE). Manche Spähsoftware-Varianten nisten sich im Bios des Rechners ein, der untersten Programmebene, um auf diese Weise auch Neustarts und sogar Software-Updates zu überstehen (SWAP). Andere verstecken sich im Master Boot Record, der Firmware der befallenen Festplatte (IRATEMONK).

Bei GINSU handelt es sich um eine Software, welche die Haltbarkeit von KONGUR Software-Implantaten sicherstellt, die für das BULLDOZER Hardware-Implantat in Systemen mit PCI-Bus konzipiert ist. Damit will NSA die Fernsteuerbarkeit von Windows-Systemen sicherstellen.

IRATEMONK: Ein Implantat, das sich in der Firmware von Festplatten der Hersteller Western Digital, Seagate Maxtor (wurde von Seagate übernommen) und Samsung verbirgt und den sogenannten Master Boot Record (MBR) der Festplatten ersetzt.

SWAP ist ein Bios-Implantat, welches das Nachladen von Steuerungssoftware der NSA für diverse Betriebssysteme (Windows, FreeBSD, Linux, Solaris) und Dateisysteme (FAT32, NTFS, EXT2, EXT3, UFS 1.0) auf PC ermöglicht.

WISTFULTOLL ist ein Software-Implantat, das die Windows-Management-Instrumentation-Schnittstelle (WMI) zum Ausleiten von Daten nutzt. Es funktioniert auch als Plug-in für die NSA-Spähprogramme UNITEDRAKE und STRAITBIZZARE.

HOWLERMONKEY ist ein Funksender und Empfänger, der zusammen mit einem anwendungsspezifischen Modul Daten aus IT-Komponenten schmuggelt, beziehungsweise es erlaubt, Geräte fernzusteuern.

JUNIORMINT ist ein frei konfigurierbares Hardware-Implantat für verschiedene Anwendungen, eine Art Computer im Kleinstformat.

MAESTRO-II ist ein Multi-Chip-Module (MCM) zum Einbau, eine Art Mini-Computer in der Größe einer Euro-Cent-Münze.

SOMBERKNAVE ist ein Windows-XP-Software-Implantat, das ungenutzte Wireless Interfaces (802.11) benutzt, um eine Verbindung zum Remote Operations Center der NSA aufzubauen und das Gerät so aus der Ferne steuerbar zu machen.

TRINITY ist ein frei konfigurierbares Hardware-Implantat für verschiedene Anwendungen, eine Art Mini-Computer im Format einer Euro-Cent-Münze.

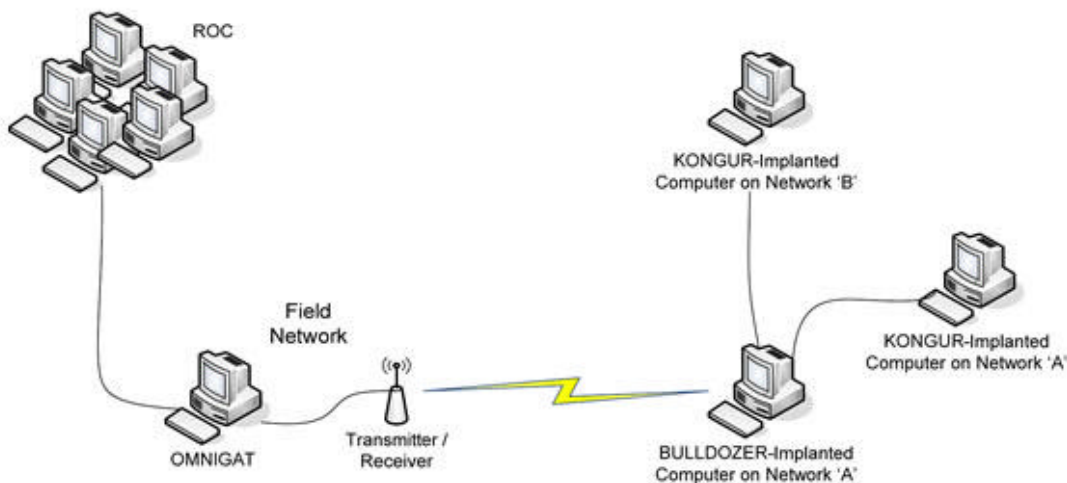


GINSU

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.

(TS//SI//REL) Through interdiction, BULLDOZER is installed in the target system as a PCI bus hardware implant. After fielding, if KONGUR is removed from the system as a result of an operating system upgrade or reinstall, GINSU can be set to trigger on the next reboot of the system to restore the software implant.

Status: Released / Deployed. Ready for Immediate Delivery

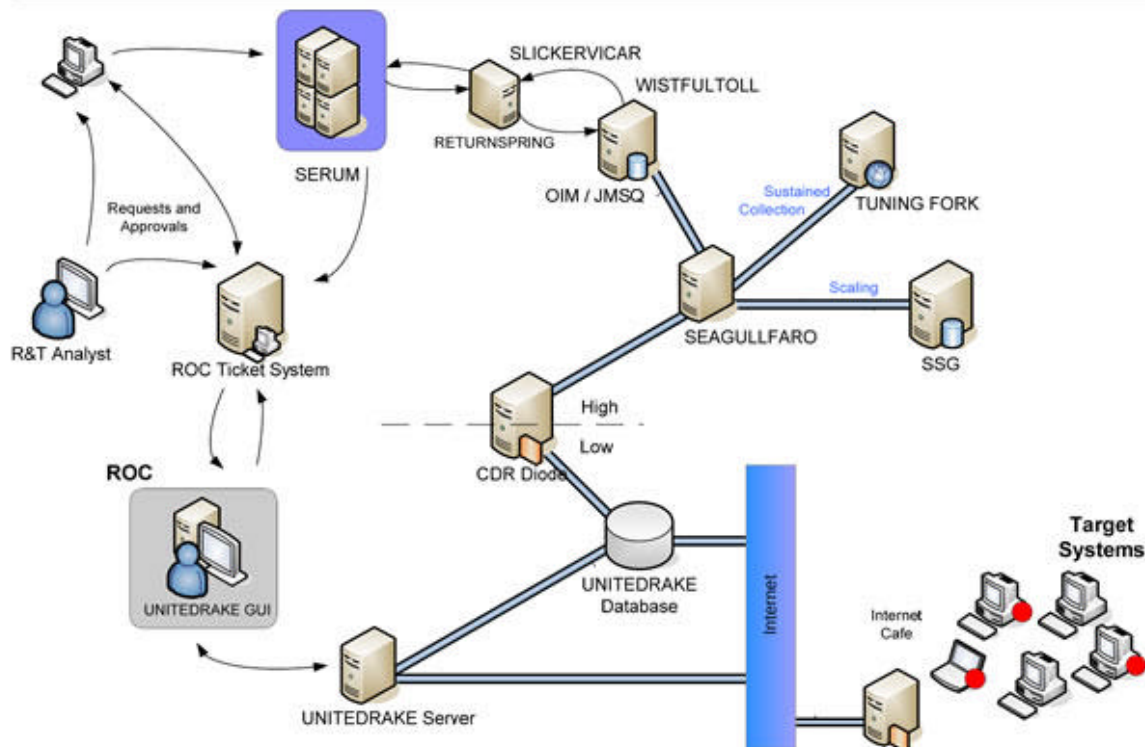
Unit Cost: \$0

POC: [REDACTED], S32221, [REDACTED], [REDACTED]@nsa.ic.gov

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

ANT Product Data

06/20/08



(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.

Unit Cost: \$0

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

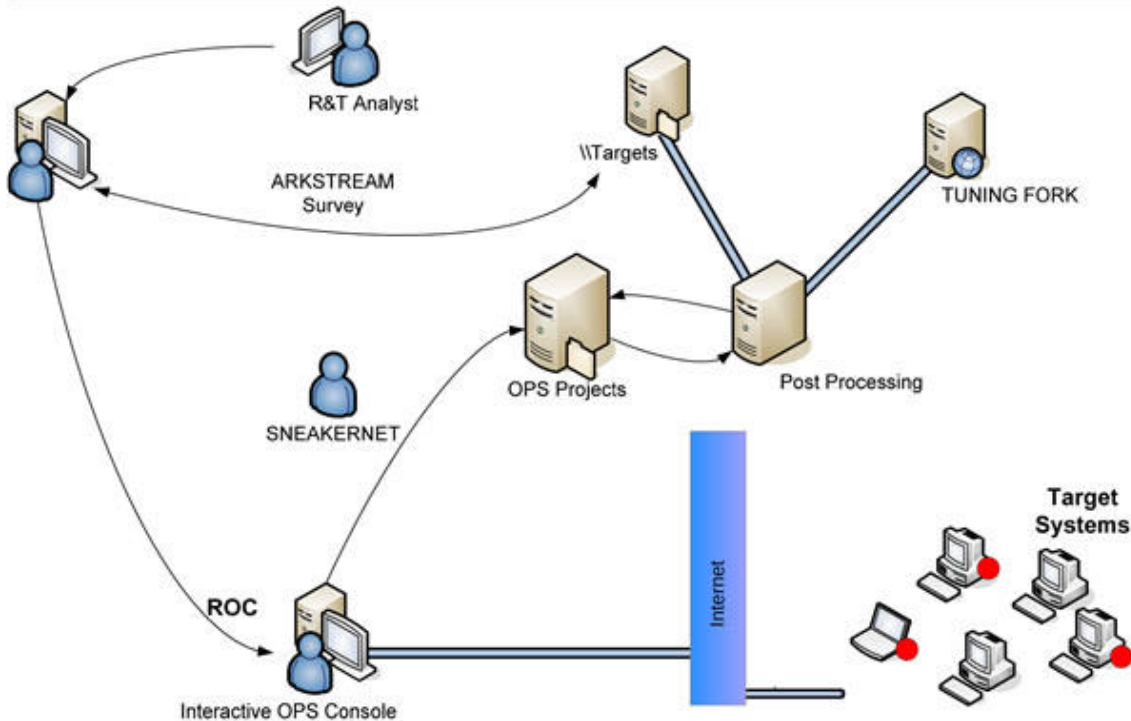


SWAP

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

(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

POC: [REDACTED] S32221, [REDACTED], [REDACTED]@nsa.ic.gov

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

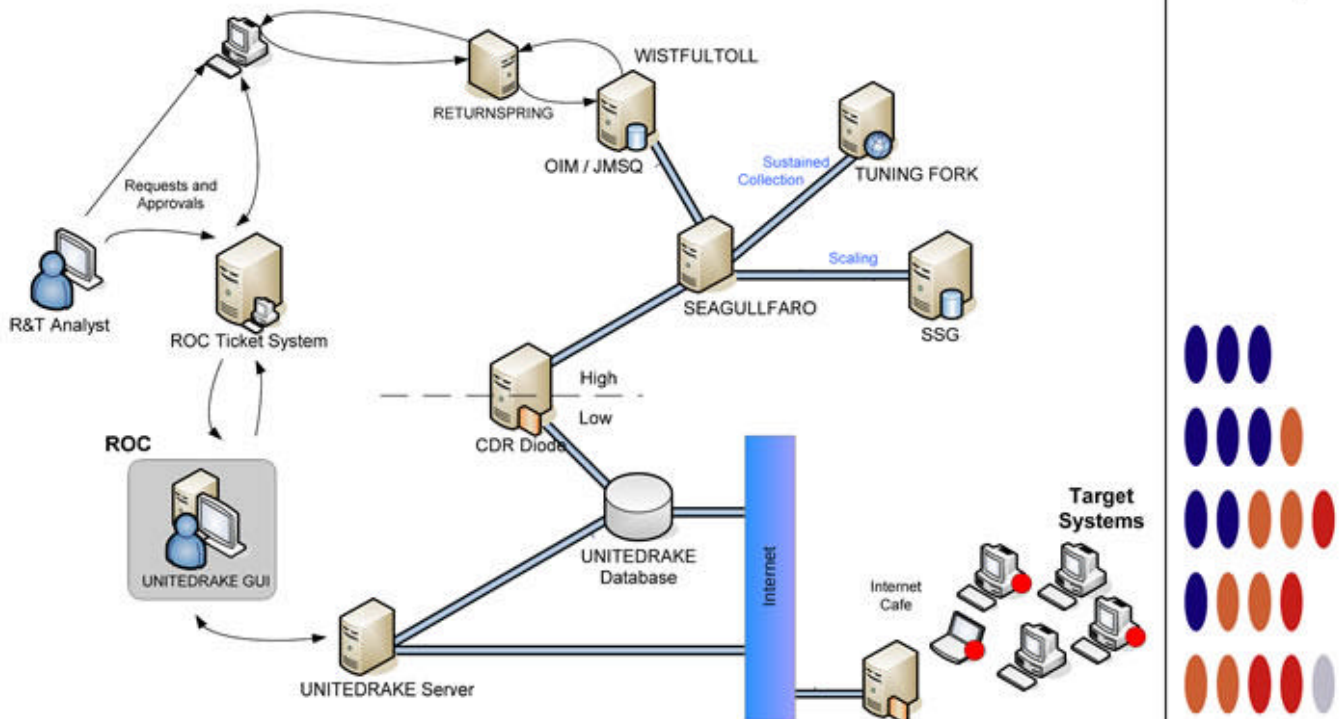


WISTFULTOLL

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) WISTFULTOLL Extended Concept of Operations

(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.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: \$0

POC: [REDACTED], S32221, [REDACTED], [REDACTED]@nsa.ic.gov

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



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



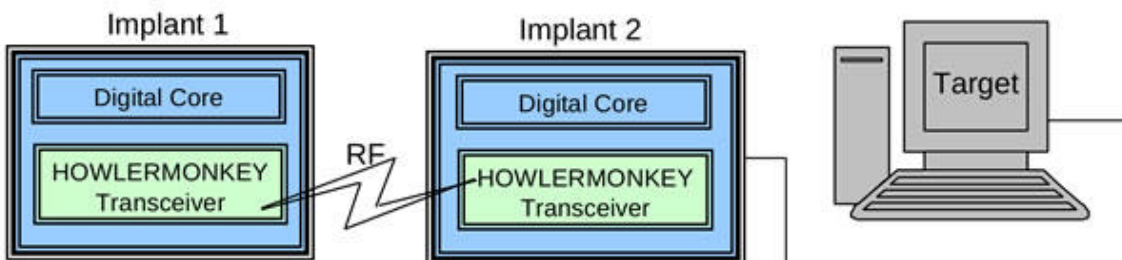
1.20" (30.5 mm)
x 0.23" (6 mm)

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.



Status: Available – Delivery 3 months

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

POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

ALT POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

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



JUNIORMINT

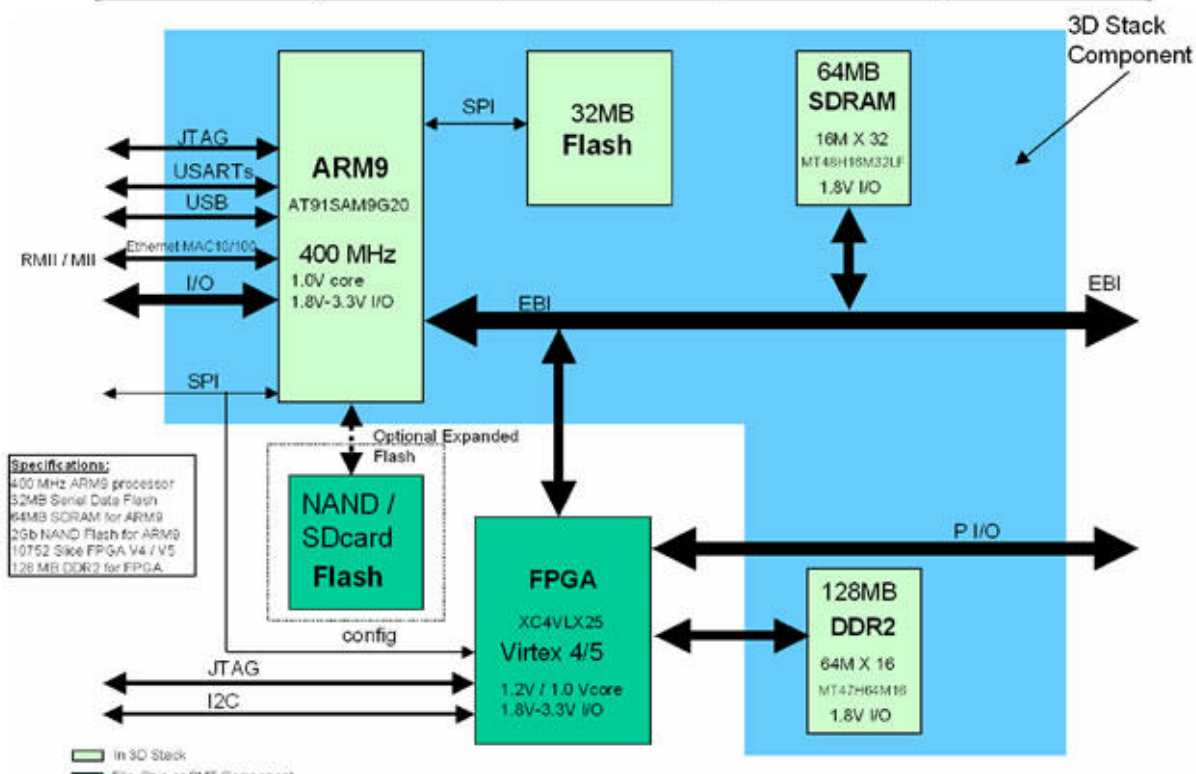
ANT Product Data

(TS//SI//REL) JUNIORMINT is a digital core packaged in both a mini Printed Circuit Board (PCB), to be used in typical concealments, and a miniaturized Flip Chip Module (FCM), to be used in implants with size constraining concealments.

08/05/08

(TS//SI//REL) JUNIORMINT uses the TAO standard implant architecture. The architecture provides a robust, reconfigurable, standard digital platform resulting in a dramatic performance improvement over the obsolete HC12 microcontroller based designs. A mini Printed Circuit Board (PCB) using packaged parts will be developed and will be available as the standard platform for applications requiring a digital core. The ultra-miniature Flip Chip Module (FCM) will be available for challenging concealments. Both will contain an ARM9 microcontroller, FPGA, Flash, SDRAM and DDR2 memories.

uController	Flash	SDRAM	FPGA	DDR2
ARM 9 400 Mhz	32 MBytes	MT48H16M32LF 64 MBytes	XC4VLX25 10752 Slice	MT47H64M16 128 MBytes



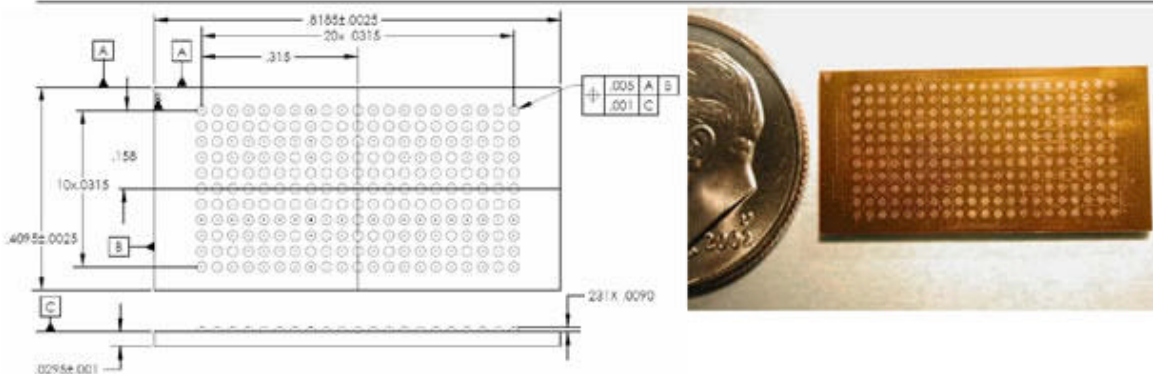


MAESTRO-II

ANT Product Data

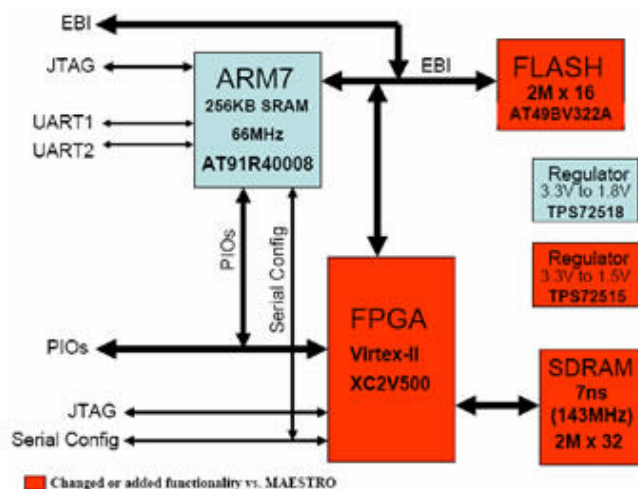
(TS//SI//REL) MAESTRO-II is a miniaturized digital core packaged in a Multi-Chip Module (MCM) to be used in implants with size constraining concealments.

08/05/08



(TS//SI//REL) MAESTRO-II uses the TAO standard implant architecture. The architecture provides a robust, reconfigurable, standard digital platform resulting in a dramatic performance improvement over the obsolete HC12 microcontroller based designs. A development Printed Circuit Board (PCB) using packaged parts has been developed and is available as the standard platform. The MAESTRO-II Multi-Chip-Module (MCM) contains an ARM7 microcontroller, FPGA, Flash and SDRAM memories.

uController	Flash	SDRAM	FPGA
ARM 7 66 Mhz	AT49BV322A 4 MBytes	MT48LC2M32 8 MBytes	XC2V500 500k gates



Status: Available – On The Shelf

Unit Cost: \$3-4K

POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

ALT POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

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



SOMBERKNAVE

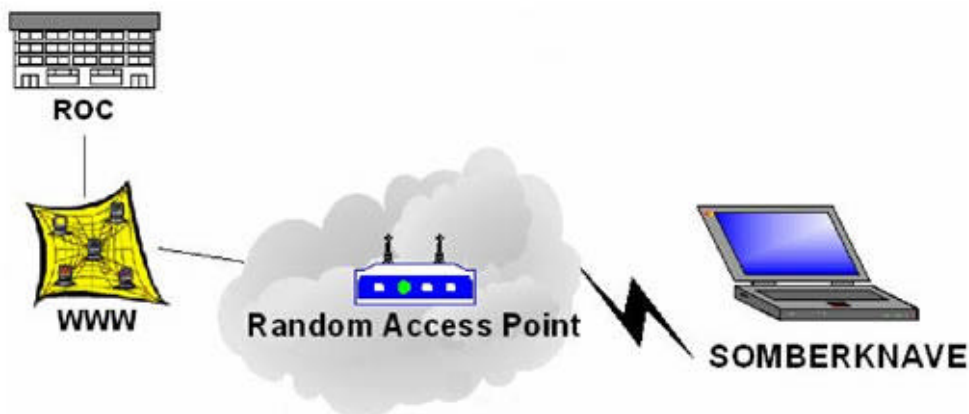
ANT Product Data

(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.



Status: Available – Fall 2008

Unit Cost: \$50k

POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov
 ALT POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

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

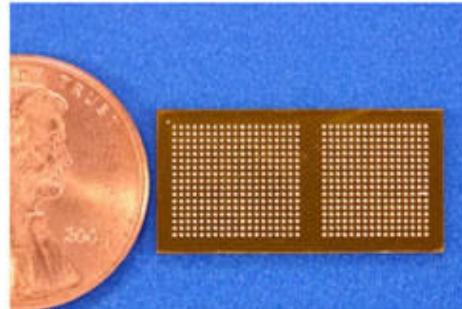
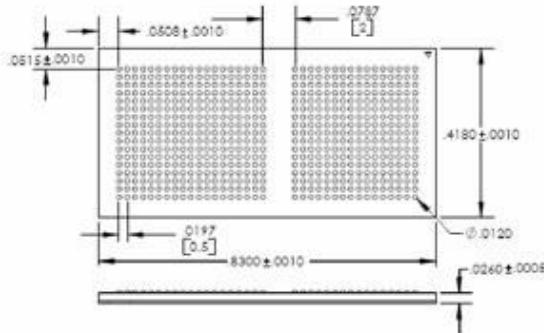


TRINITY

ANT Product Data

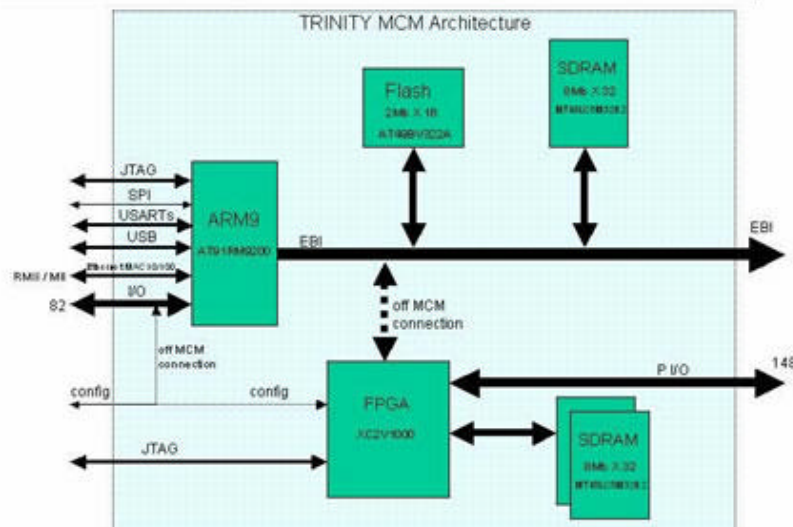
(TS//SI//REL) TRINITY is a miniaturized digital core packaged in a Multi-Chip Module (MCM) to be used in implants with size constraining concealments.

08/05/08



(TS//SI//REL) TRINITY uses the TAO standard implant architecture. The architecture provides a robust, reconfigurable, standard digital platform resulting in a dramatic performance improvement over the obsolete HC12 microcontroller based designs. A development Printed Circuit Board (PCB) using packaged parts has been developed and is available as the standard platform. The TRINITY Multi-Chip-Module (MCM) contains an ARM9 microcontroller, FPGA, Flash and SDRAM memories.

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



Status: Special Order due vendor selected.

Unit Cost: 100 units: \$625K

POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

ALT POC: [REDACTED], S3223, [REDACTED], [REDACTED]@nsa.ic.gov

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108