Trusted Computing Technology and Government Implants

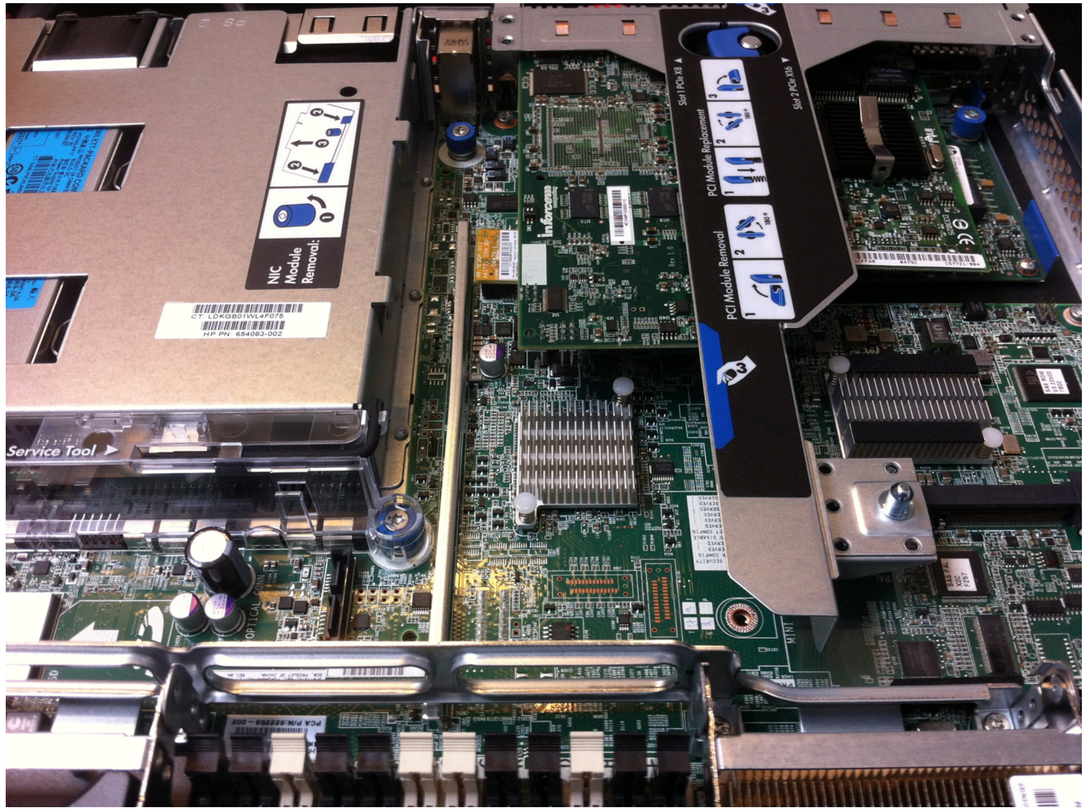
TrustyCon 2014

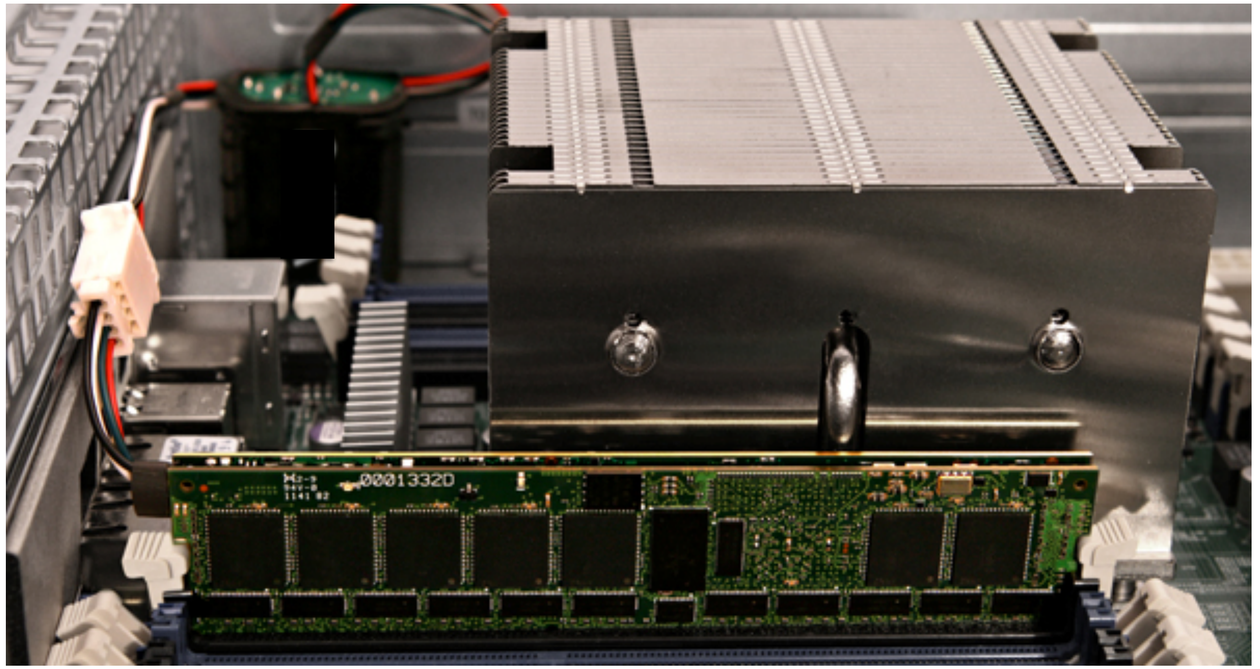
Steve Weis

Intro

- **Me:** Cryptographer, Co-founder & CTO PrivateCore, Google 2-factor, Keyczar, saweis.net, @sweis
- **Today's talk:**
  - Snapshot of NSA ANT hardware, firmware, & software implants
  - "Trusted Computing": What is it? Can it help? Can we trust it?
  - Defensive technologies on the horizon

Can you spot the implants?





NSA ANT

SPIEGEL ONLINE

Shopping for Spy Gear: Catalog Advertises NSA Toolbox

By Jacob Appelbaum, Judith Horchert and Christian Stöcker

WIRED

NSA Hackers Get the 'Ungettable' With Rich Catalog of Custom Tools

BY KIM ZETTER 12.30.13 4:11 PM

The New York Times

N.S.A. Devises Radio Pathway Into Computers

By DAVID E. SANGER and THOM SHANKER JAN. 14, 2014

NSA Observer https://nsa-observer.laquadrature.net/

AGILEVIEW
AGILITY
AIGHANDLER
AIRGAP/COZEN
ALTEREGOQFD
ANCHORY
ANGRYNEIGHBOR
ANTOLPPROTOSSGUI
AQUADOR
ARCA
ARKSTREAM
ARTEMIS
ARTIFICE
AUTOSOURCE
BANANAGLEE
BANYAN
BEACHHEAD
BELLTOPPER
BINOCULAR
BLACKFOOT
BLACKHEART
BLACKMAGIC
BLACKPEARL
BLARNEY
BLINDDATE
BLUEANCHOR
BLUEZEPHYR
BOUNDLESSINFORMANT
BROKER
BRUNEAU
BSR
BULLRUN
BULLSEYE
BYZANTINEANCHOR
BYZANTINECANDOR
BYZANTINEHADES
CADENCE
CARBOY
CASPORT
CCDP
CDRDIODE
CHALKFUN
CHEWSTICK
CHIMNEYPOOL
CHIPPEWA
CIMBRI
CINEPLEX
COASTLINE
COBALTFALCON
COMMONDEER
CONJECTURE
CONTRAOCTAVE
CONVEYANCE
CORALINE
COTRAVELER
COTS
COTTONMOUTH-I
COTTONMOUTH-II
COTTONMOUTH-III
COURIERSKILL
CREST
CROSSBEAM
CRUMPET
CRYPTOENABLED
CTX4000
CULTWEAVE
CUSTOMS
CW
CYCLONE
DANCINGOASIS
DANDERSPRIT
DANDERSPRITZ
DANGERMOUSE
DARKTHUNDER
DAYTONA
DECKPIN
DEITYBOUNCE
DIKTER
DISHFIRE
DISTANTFOCUS
DIVERSITY
DOCKETDICTATE
DOGCOLLAR
DRAGONFLY
DROPMIRE
DRTBOX
DRUID
DYNAMO
EBSR
EGOTISTICALGIRAFFE
EGOTISTICALGOAT
ENDUE
ENTOURAGE
EPICFAIL
ERRONEOUSINGENUITY
EVENINGEASEL
EVILOLIVE
EWALK
FA
FACELIFT
FAIRVIEW
FALLOUT
FASCIA
FASTSCOPE
FEEDTROUGH
FERRETCANNON
FET
FINKDIFFERENT
FISHBOWL
FLUXBABBIT
FLYINGPIG
FOXACID
FOXSEARCH
FOXTRAIL
FRA
FREEFLOW
FREEZEPOST
FRIEZERAMP
FRONTO
FUNNELOUT
GAMUT
GARLICK
GENIE
GENTE
GEOFUSION
GHOSTMACHINE
GILGAMESH
GINSU
GODSURGE
GOPHERSET
GOURMETTROUGH
GREATEXPECTATIONS
GTE
HALLUXWATER
HAMMERMILL
HAWKEYE
HC12
HEADWATER
HEMLOCK
HIGHLANDS
HIGHTIDE
HOMEBASE
HUSHPUPPY
INDIA
INDRA
INTELINK
INTERDICTION
IRATEMONK
IRONCHEF
IRON SAND
ISHTAR
JACKKNIFE
JETPLOW
JUGGERNAUT
JUNIORMINT
KAMPUS
KEYRUT
KLONDIKE
KONGUR
LADYLOVE
LANDSHARK
LEGION-JADE
LEGION-RUBY
LEMONWOOD
LFS-2
LHR
LIFESAVER
LITHIUM
LONGHAUL
LOPERS
LOUDAUTO
MADCAPOCELOT
MAESTRO-II
MAGNETIC
MAILORDER
MAINCORE
MAINWAY
MARINA
MAUI
MESSIAH
METTLESOME
MIDDLEMAN
MINERALIZE
MJOLNIR
MOCCASIN
MONKEYCALENDAR
MONKEYROCKET
MOONLIGHTPATH
MOONPENNY
MTI
MULLENIZE
MUSCULAR
MUTANTBROTH
NEBULA
NEWTONSCRADLE
NIGHTSTAND
NIGHTWATCH
NUCLEON
OAKSTAR
OCEAN
OCEANARIUM
OCELOT
OCONUS
OCTAVE
OCTSKYWARD
OILSTOCK
OLYMPUS
OLYMPUSFIRE
OMNIGAT
ONIONBREATH
ORANGEBLOSSOM
ORANGECRUSH
OSMJCM-II
PACKAGEGOODS
PARCHDUSK
PATHFINDER
PBD
PEDDLECHEAP
PHOTOANGLO
PICASSO
PINWALE
POWELL
PPM
PREFER
PRINTAURA
PRISM
PROTOSS
PUZZLECUBE
QFD
QFIRE
QIM/JMSQ
QUANTUM
QUANTUM INSERT
QUANTUMBOT
QUANTUMCOOKIE
QUANTUMCOPPER
QUANTUMNATION
QUANTUMSKY
QUANTUMTHEORY
QUICK
QUICKANTQFD
RADON
RAGEMASTER
RAGTIME
RAMPART
RC-10
REMATION-II
RETROREFLECTOR
RETURNSPRING
ROCKYKNOB
RONIN
ROYALCONCIERGE
SCALPEL
SCHOOLMONTANA
SCISSORS
SCS
SEAGULLFARO
SEASONEDMOTH
SEMESTER
SENTINEL
SERUM
SHARKFIN
SHARPFOCUS
SHELLTRUMPET
SHENANIGANS
SHIFTINGSHADOW
SHOALBAY
SHORTSHEET
SIERRAMONTANA
SILVERZEPHYR
SKYWRITER
SLICKERVICAR
SNEAKERNET
SNICK
SOLIS
SOMBERKNAVE
SOUFFLETROUGH
SOUNDER
SPARROW-II
SPECULATION
SPINNERET
SPOTBEAM
SSG
SSP
STEELFLAUTA
STEELKNIGHT
STELLAR
STELLARWIND
STORMBREW
STRAITBIZARRE
STRIKEZONE
STRONGMITE
STUCCOMONTANA
STUMPCURSOR
SURLYSPAWN
SURPLUSHANGAR
SUTURESAILOR
SWAP
TALENTKEYHOLE
TARGETPROFILER
TAWDRYYARD
TEMPEST
TEMPORA
THINTREAD
TIMBERLINE
TLN
TOTECHASER
TOTEGHOSTLY
TRAFFICTHIEF
TRAILBLAZER
TREASUREMAP
TRINITY
TUMULT
TUNINGFORK
TURBINE
TURBOPANDA
TURBULENCE
TURMOIL
TUSKATTIRE
TUTELAGE
TWDRYYARD
TWISTEDKILT
TYPHONHX
UAV
UMBRA
UNITEDRAKE
UPSTREAM
VAGRANT
VALIDATOR
VIEWPLATE
WAGONBED
WATERWITCH
WEALTHYCLUSTER
WEBCANDID
WHITETAMALE
WINDSTOP
WINTERLIGHT
WISTFULTOLL
WRANGLER
XCONCORD
XKEYSCORE
YACHTSHOP
YELLOWPIN
ZESTYLEAK

System Taxonomy Recap

Software	**Hypervisor, Operating System, Applications**
Firmware	**BIOS, SMM, Option ROMs, SINIT ACMs**
Hardware	**Processor, Memory, Storage, Devices, Buses**

DEITYBOUNCE

ANT Product Data

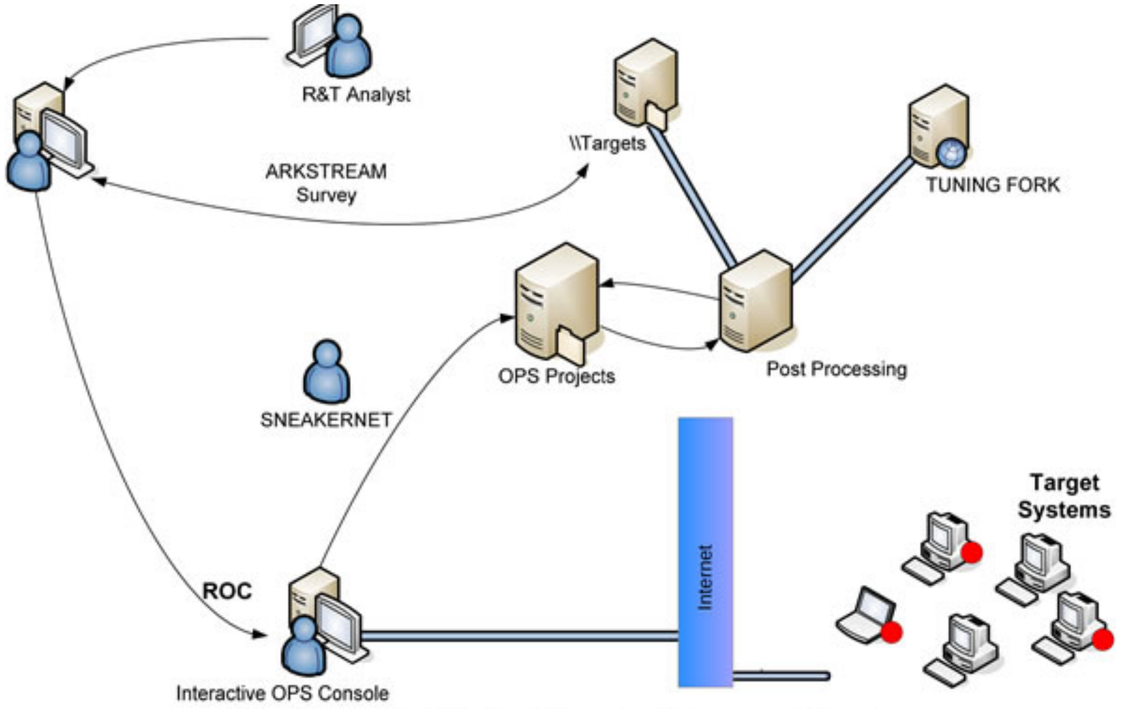
(TS//SI//REL) DEITYBOUNCE provides software application persistence on Dell PowerEdge servers by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to gain periodic execution while the Operating System loads.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS on a target machine to implant DEITYBOUNCE and its payload (the implant installer). Implantation via interdiction may be accomplished by non-technical operator though use of a USB thumb drive. Once implanted, DEITYBOUNCE's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

06/20/08

Status: Released / Deployed. Ready for Immediate Delivery

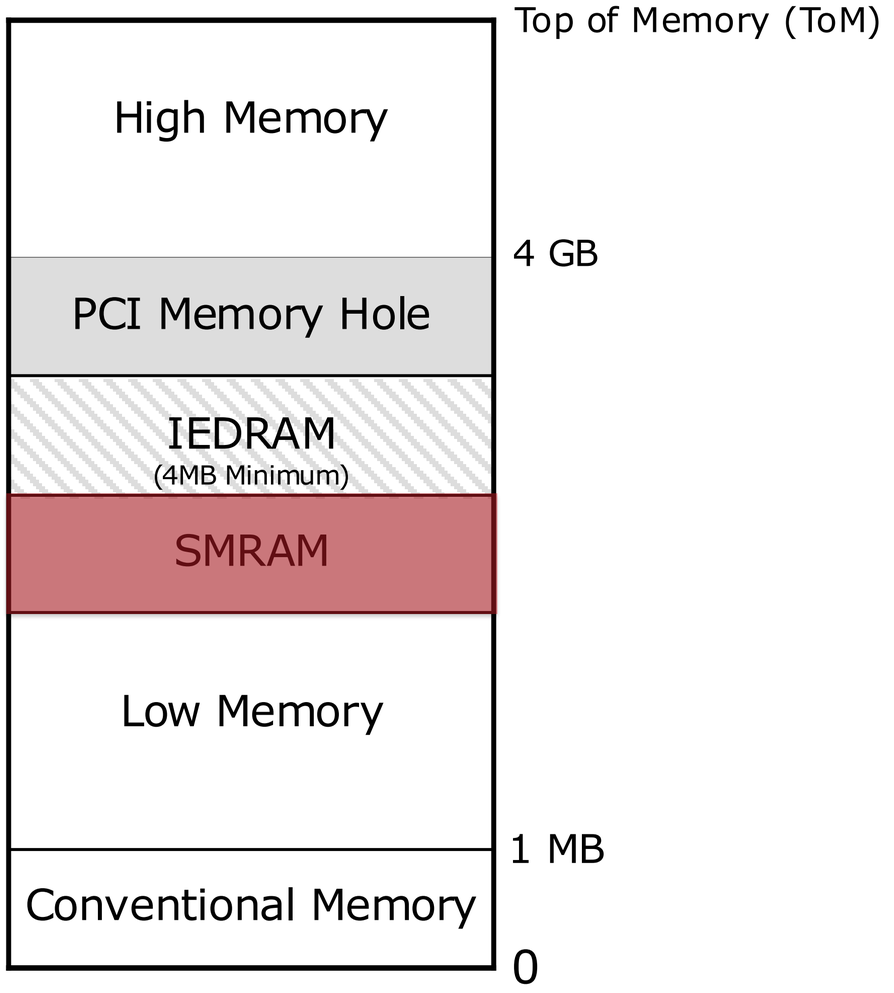
Unit Cost: $0



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

Why attack BIOS and SMM?

- **Basic I/O System (BIOS)**: Persistent firmware that runs first before the OS.
- **System Management Mode (SMM)**: Special mode of operation that runs with highest privileges, which is installed by BIOS and invisible to OS.



GOURMETTROUGH

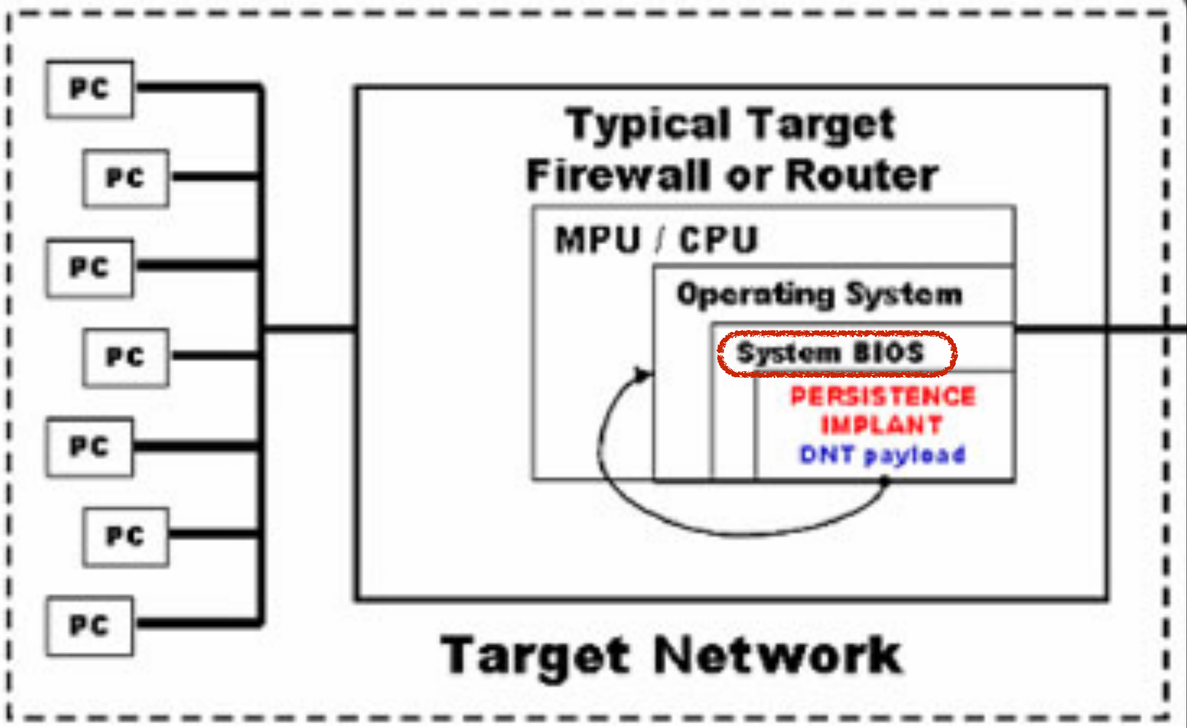
ANT Product Data

(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

Status: GOURMETTROUGH is on the shelf and has been deployed on many target platforms. It supports nsg5t, ns50, ns25, isg1000(limited). Soon- ssg140, ssg5, ssg20

Unit Cost: $0



IRATEMONK

ANT Product Data

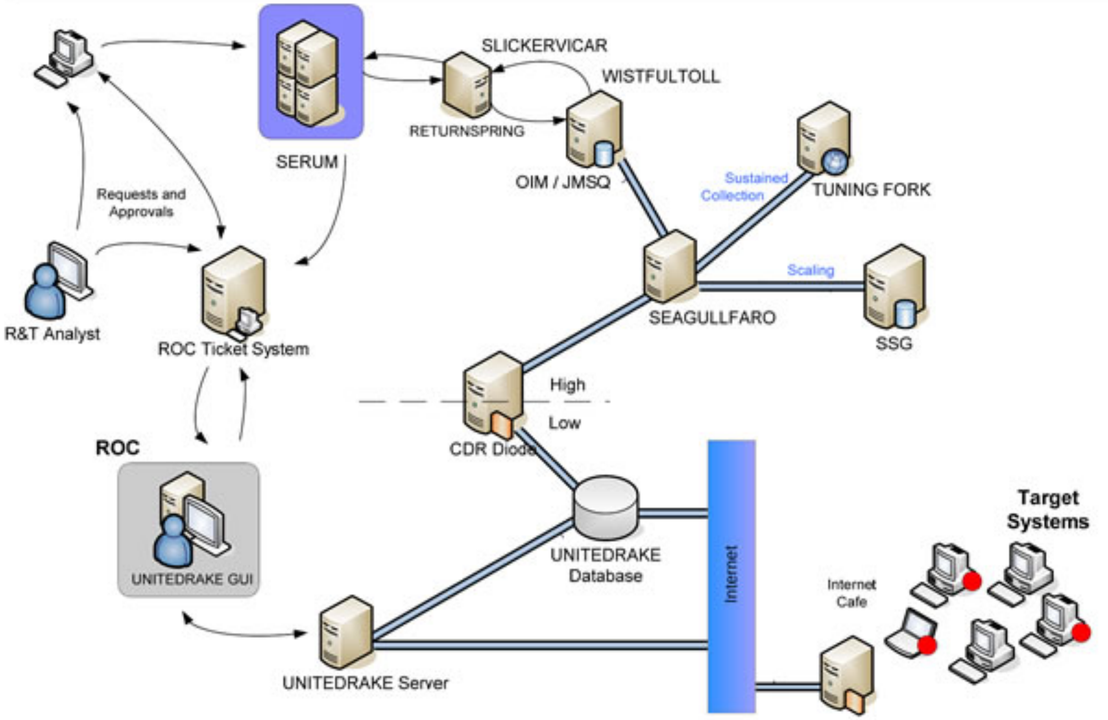
(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

(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.

06/20/08

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0



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

IRONCHEF

ANT Product Data

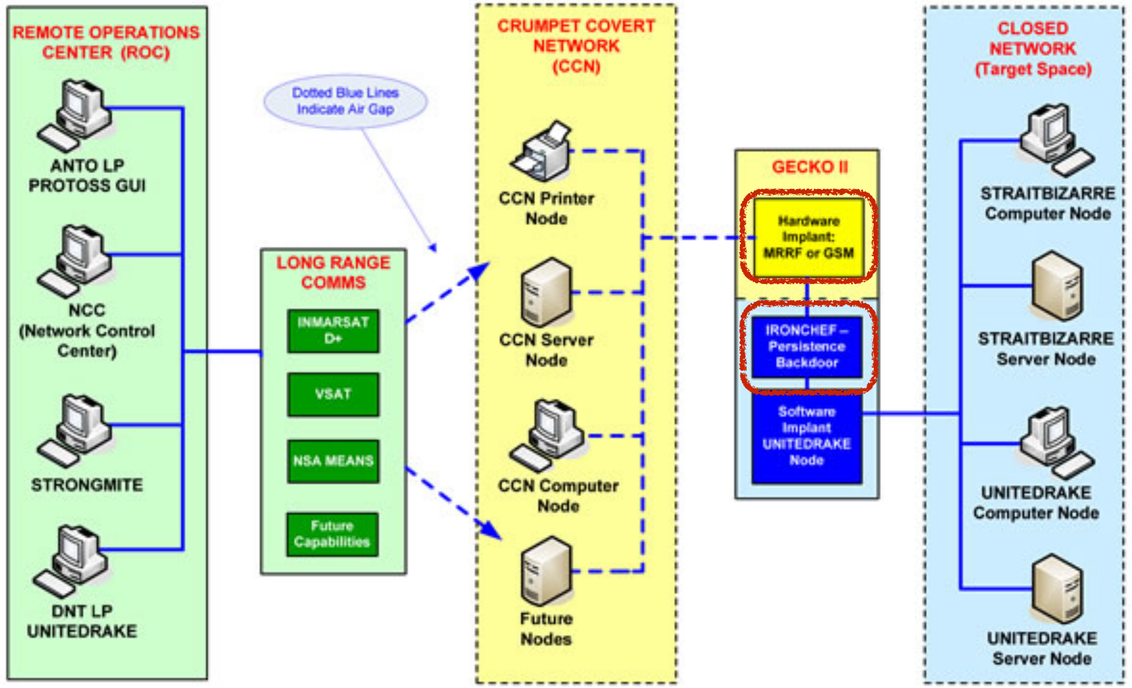
(TS//SI//REL) IRONCHEF provides access persistence to target systems by exploiting the motherboard BIOS and utilizing System Management Mode (SMM) to communicate with a hardware implant that provides two-way RF communication.

(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.

07/14/08

Status: Ready for Immediate Delivery

Unit Cost: $0

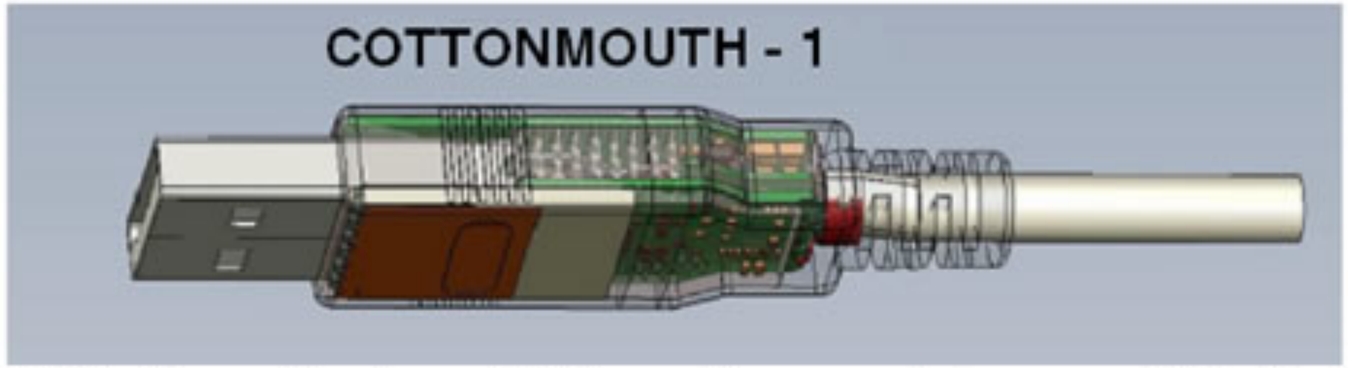


(TS//SI//REL) IRONCHEF Extended Concept of Operations

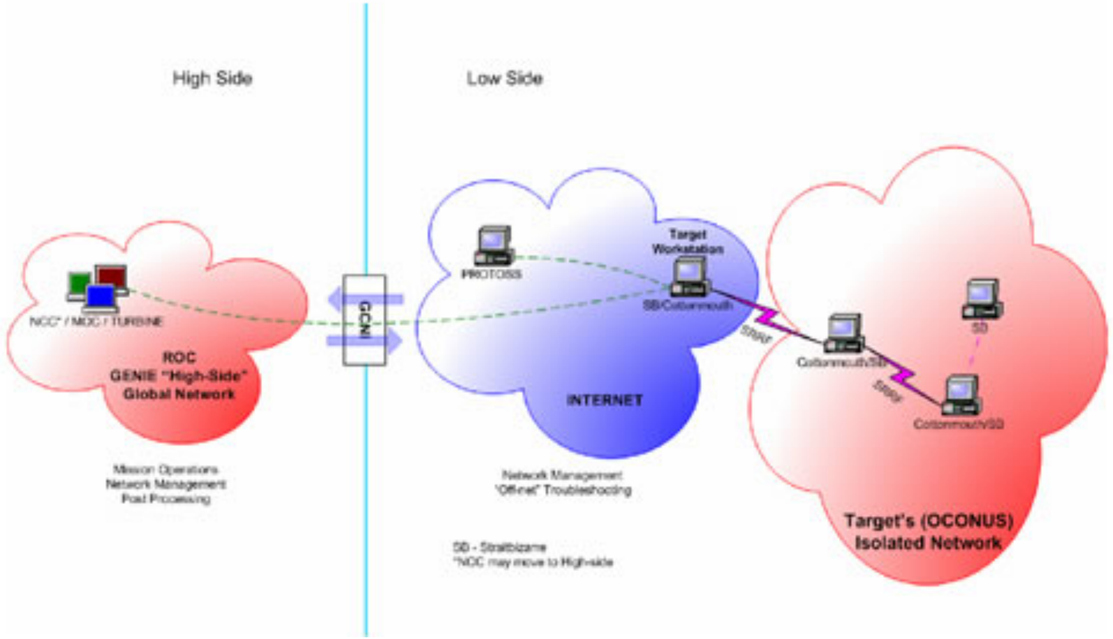
COTTONMOUTH-I

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.



(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.



Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

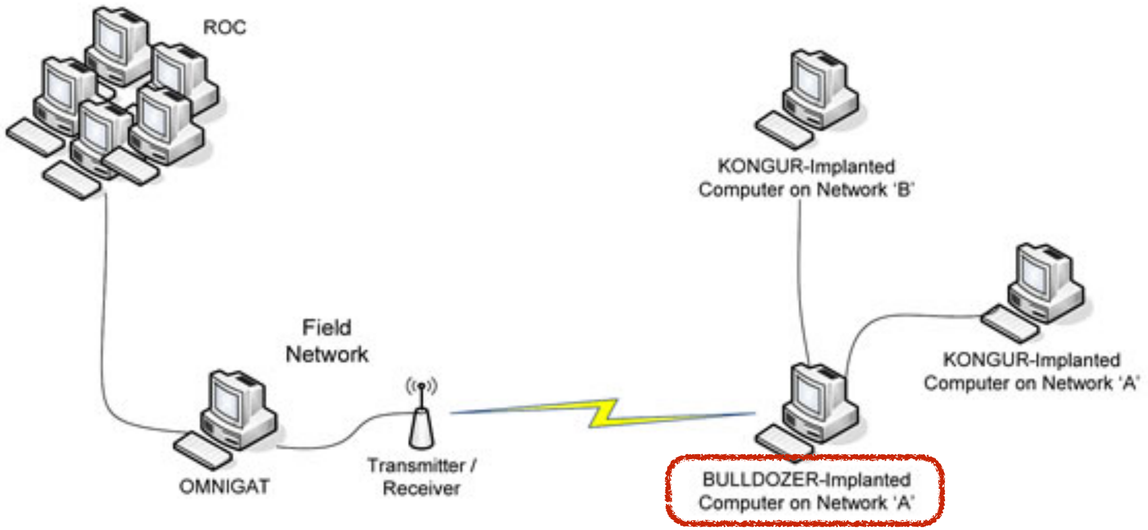
GINSU

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.

(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.



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

06/20/08

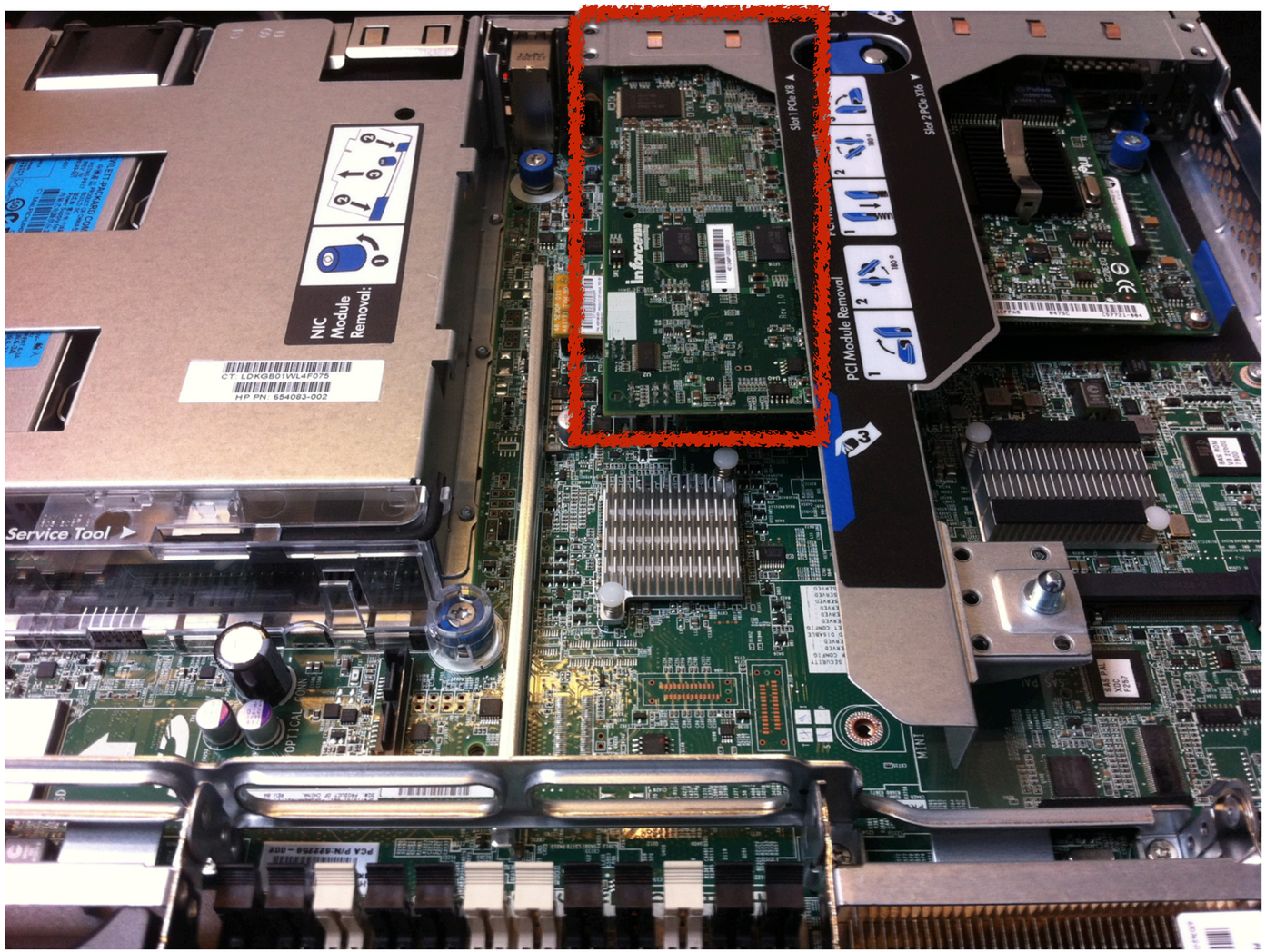
Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

Do-it-Yourself Implants

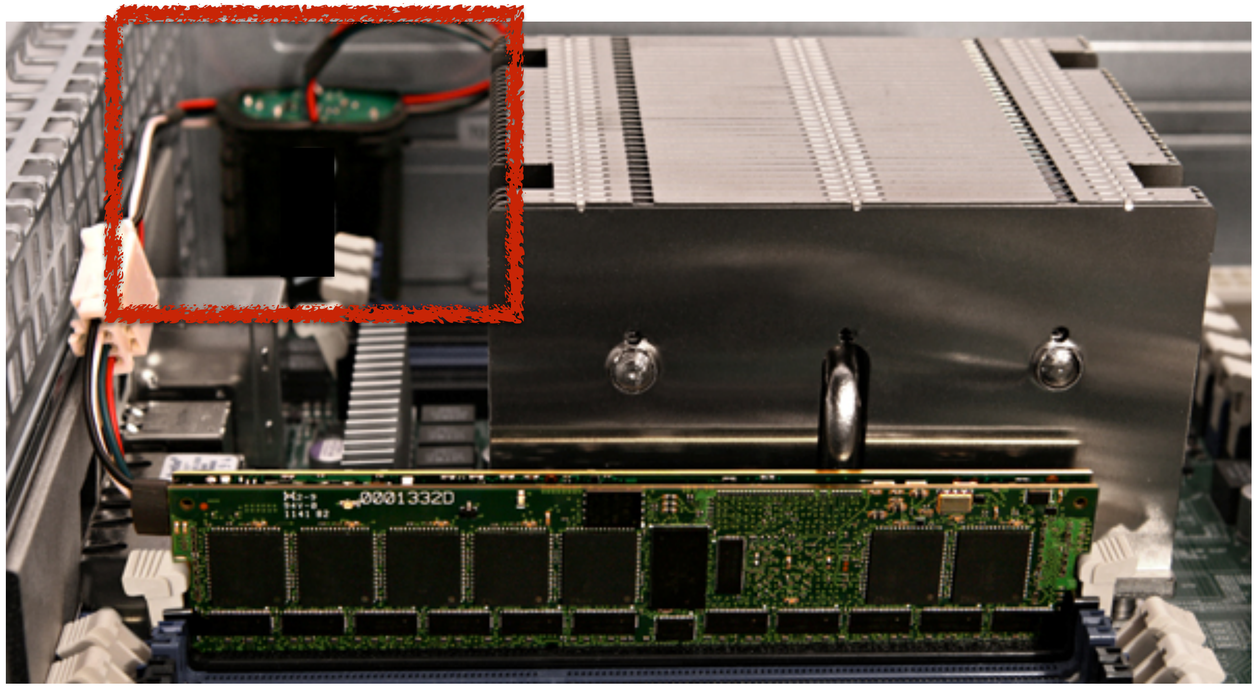
Can you spot the implant?

- PCI attack device
- Implemented with off-the-shelf hardware
- Boots independently of host
- Exfiltrates data over the network



Can you spot the implant?

- Non-volatile RAM (NV-RAM)
- RAM contents are saved to flash memory on power loss.
- Attackers can capture crypto keys from preserved memory contents
- Several non-volatile memory technologies are in the pipeline



Trusted Computing

Ensure _____’s software is running on _____’s computer.

Trusted Computing for DRM

Ensure a content owner's software is running on your computer.

Trusted Computing for You

Ensure your software is running on your computer.

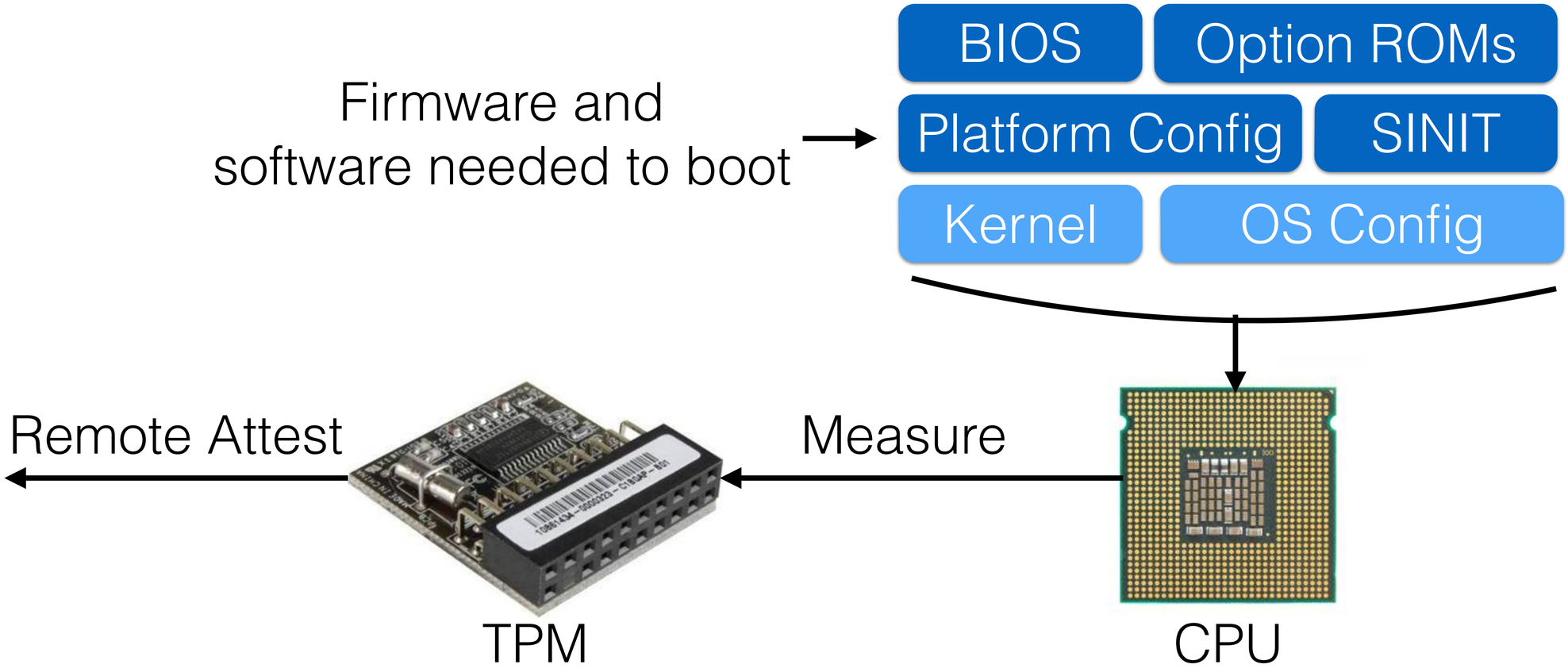
Trusted Platform Module

The Coming Civil War on General Purpose Computing:
"*A TPM is a nub of stable certainty: If it's there, it can reliably inform you about the code on your computer.*"

- Cory Doctorow

- Public-key encryption and signatures
- Random number generation
- Persistent key storage
- Special "Platform Configuration Registers" (PCRs)

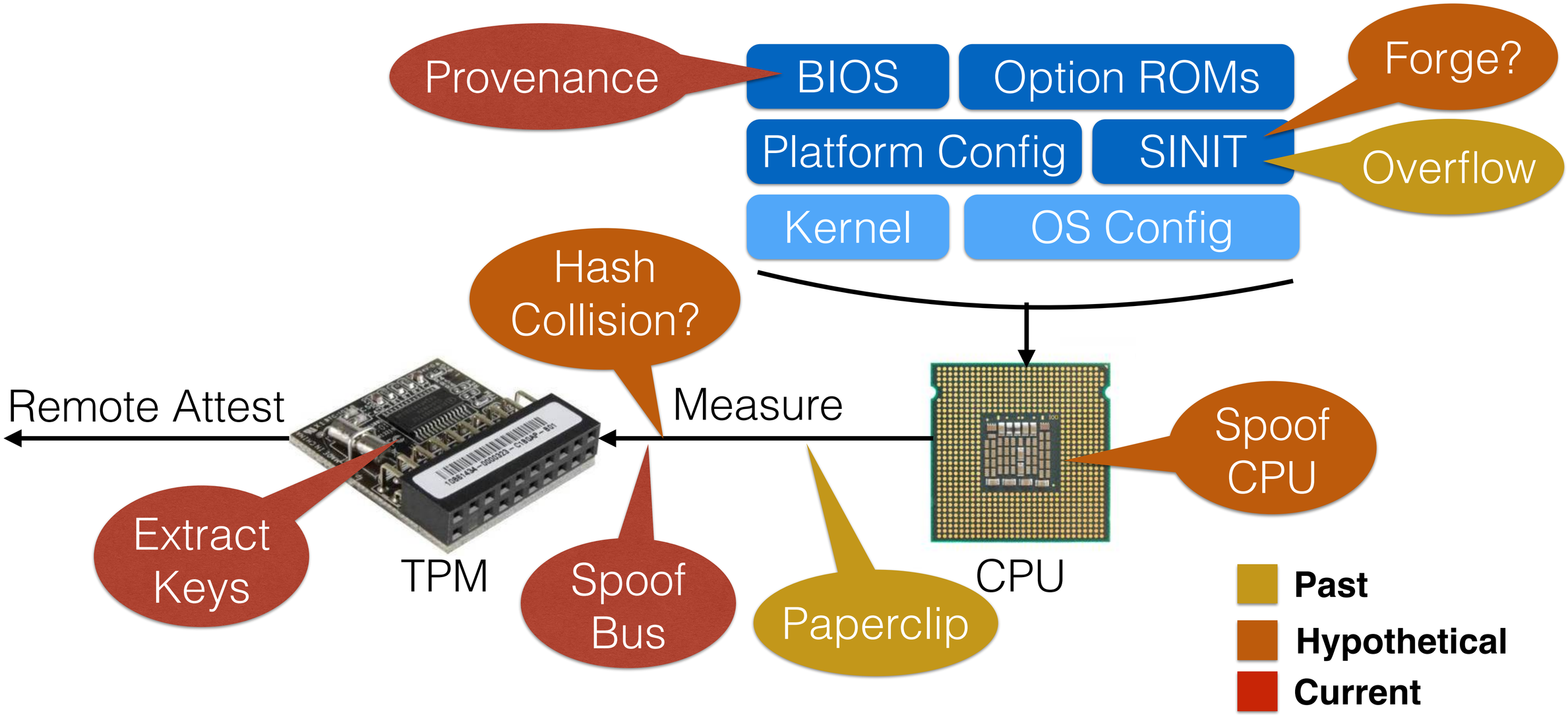
Trusted Execution Technology



Suspension of Disbelief

- What about physical attacks and hardware implants?
- Why do we trust the TPM? Where did it come from?
- Why do we trust the CPU for that matter?

Attack Vectors



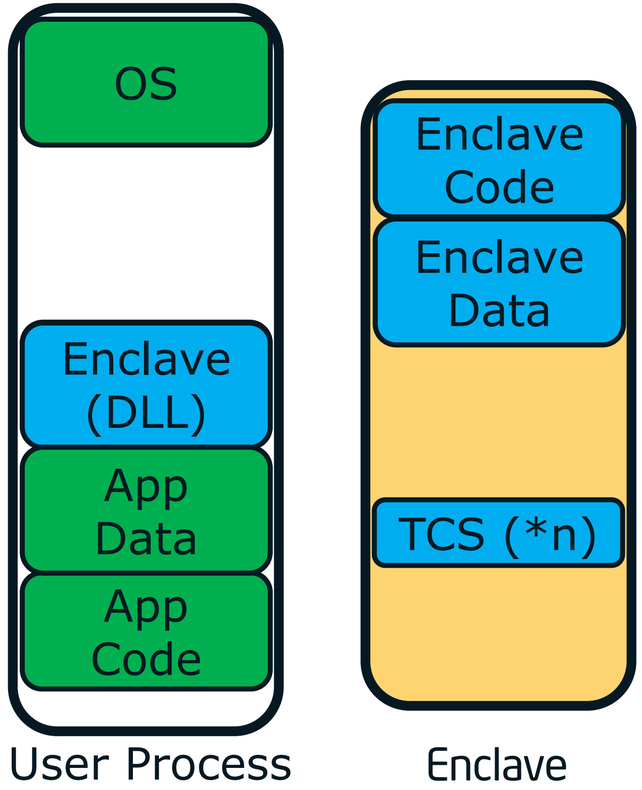
Where does this leave us?

- State-sponsored actors can circumvent trusted computing.
- Trusted computing still offers protection, although we ultimately have to trust the CPU and TPM.
- In the next 1-3 years: New hardware and platform security features
- Beyond: Practical applications of cryptographic protocols for security computation, e.g. fully homomorphic encryption.

Upcoming Technologies

Software Guard Extensions (SGX)

- Secure “enclaves” protected from other code.
- Enclaves are attested and won’t run if modified.
- Enclaves are backed by fully-encrypted memory.
- Potentially could make DRM hard to circumvent.



Enhanced Privacy ID (EPID)

- Provides ability for CPU to anonymously sign data.
- Could authenticate CPUs as real, without leaking identity.
- Caveat: Rooted in globally unique key material in CPU hardware.

Trusted Platform Module 2.0

- TPM 1.2 is deprecated and banned in several countries.
- TPM 2.0
  - More algorithms and functionality
  - Support for alternate cryptographic suites
  - Better management
  - Easier on-boarding

Summary

- NSA ANT implants target software, firmware, and hardware.
- Trusted computing helps against firmware and software attacks, but not against state sponsors.
- New technologies like SGX and EPID can work for us or against us.


Thank you!