(C//REL) Internet Anonymity 2011

- NSA (S31323)
- [redacted]
- [redacted]
- [redacted] NSTS

(C//REL) What is Internet Anonymity?

- (U) Many Possible Meanings/Interpretations
  - (S//REL) Simply Not Using Real Name for Email
  - (S//REL) Private Forum with Unadvertised Existence
  - (S//REL) Unlocatable Endpoint on Internet
- (S//REL) This Talk Concerns Endpoint Location
  - (S//REL) The Network Address (IP Address) is Crucial
  - (S//REL) It is Not Always Sufficient, However
    - (S//REL) Dynamic IP Address
    - (S//REL) Mobile Device

(C//REL) What is Internet Anonymity?

- (S//REL) Anonymity Is Not Simply Encryption
  - (S//REL) Encryption Can Simply Hide Content
  - (S//REL) Anonymity Masks the MetaData and hence association with user
  - (S//SI//REL) Importance of MetaData to SIGINT post-2001 can not be overstated
  - (S//REL) There is also anonymity specifically for publishing information
    - (S//REL) Beyond the Scope of this Talk!
- (U) Anonymity is the antithesis of most business transactions (but encryption may be crucial)
  - (U) Authentication for monetary exchange
  - (U) Marketing wants to know customer well
  - (U) The same goes for Taxing Authorities :-)

(C//REL) Who Wants Internet Anonymity?

- (U) All Technology is Dual-Use
  - (U) Nuclear Weapon to Plug Oil Well
  - (U) Homicide by Hammer
- (U) Internet Anonymity for Good
  - (U) Anonymous Surveys (Ex: Diseases)
  - (U) Human Rights Bloggers
  - (U) HUMINT Sources

(C//REL) Who Wants Internet Anonymity?

- (U) Internet Anonymity for Bad (Semi to Really)
  - (U) Copyright Violators (File Sharing)
  - (U) Internet Scam Artists
  - (U) Pedophiles
  - (C//REL) Foreign Intelligence Agents
  - (S//REL) Terrorist Actors (Our Concern)
- (U) Both Cases Use Internet Anonymity Technology (IAT)

(S//REL) Internet Censorship: A "Dual"

- (U) Different Scenario
  - (U//FOUO) User IP Address known
  - (U//FOUO) User Blocked from accessing certain site IP Addresses
  - (U//FOUO) Users get around it with Circumvention Technology – Mostly the same as Internet Anonymity Technology (IAT)

(C//REL) Types Of IAT

- (S//REL) Single Hop Proxies
  - (S//REL) Web Site Proxies
  - (S//REL) HTTP/SOCKS Proxies
    - (S//REL) Browser Configured to Access
  - (S//REL) Proxy Aggregator Sites for Both
  - (S//REL) May support SSL/TLS
    - (S//REL) HTTP Sites: Only User ↔ Proxy
    - (S//REL) SSL Sites (HTTPS)
      - (S//REL) Transparent (Just Pass the Bits)
      - (S//REL) Man-in-the-Middle (MITM)

(C//REL) Types Of IAT: HTTP Proxies/Aggregators

- (S//REL) Web-Site Proxy Aggregator sites
  - (S//REL) May list thousands of proxies
    - (S//REL) Taxonomy may be country where hosted
    - (S//REL) Taxonomy may be ego/business related
    - (S//REL) Taxonomy may be proxy software related
    - (S//REL) Taxonomy may be provider related
  - (S//REL) Proxy Information IS Temporal
    - (S//REL) Requires active confirmation
    - (S//REL) Requires revisits

(C//REL) Types Of IAT: HTTP Proxies/Aggregators

- (S//REL) Web Proxy Sites (and Aggregator sites) – Info We Want
  - (S//REL) Domain Name (obvious :-))
  - (S//REL) Associated IP address(es)
    - (S//REL) Can get live (*nslookup*, *host*, *dig*, etc)
    - (S//REL) Can maybe get internally (*Foxtrail*, *NKB*, etc.)
  - (S//REL) "Exit" IP address (where does user appear?)
    - (S//REL) Obtaining manually easy (*http://checkip.dyndns.org*)
    - (S//REL) How to Automate?
      - (S//REL) *Proxy Discoverer* (Originally S31323)
  - (S//REL) Other miscellaneous (cookie modification, SSL support, etc.)

(C//REL) Types Of IAT: HTTP Proxies/Aggregators

- (S//REL) Web Proxy Aggregator sites Analysis
  - (S//REL) *Proxy Discoverer*
    - (S//REL) Scrapes Aggregator (ie www.proxy.org)
    - (S//REL) For each proxy, GET www.checkip.dyndns.org
      - (S//REL) Iterate over software, variations
      - (S//REL) *Glype, PHProxy, CGIProxy, ASP.NET, cURLProxy, Surrogafier, Zelune*
      - (S//REL) Try multiple times
      - (S//REL) Aggregator may give software hints
      - (S//REL) Failure may indicate site down, or proxy SW modification
  - (S//REL) Results from *Proxy Discoverer* must bridge low->high
  - (S//REL) Operationalized by *NAC/RONIN* with *NTOC* support (project *PONTENTPOTABLES*)
    - (S//REL) See *SDC2011:* [redacted]

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Provider may offer multiple servers
    - (S//REL) Different Sovereign Nations
    - (S//REL) Different Bandwidths
    - (S//REL) Most fee based: Can vary on time/number of servers
  - (S//REL) May offer multiple VPN protocols
    - (S//REL) *PPTP* (No client software)
    - (S//REL) *SSH*
    - (S//REL) *OpenVPN*
    - (S//REL) *L2TP/IPSEC*
    - (S//REL) *SSTP*
  - (S//REL) Communications User ↔ Server Encrypted

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Plethora of providers (I found about 200)
    - (S//REL) *12VPN, Ace VPN, Air VPN, AlwaysVPN, Ananoos, AnoCentral, Anonine, Anonyproz, AnonymityNetwork, Anonymizer, Anti-Hadopi, Arethusa, ArtofPing, Astrill, BananaVPN, BeeVPN, BlackLogic, BlackVPN, BolchVPN, BuyProxyService, Change-Mon-IP, Cienen, ClearVPN, ConnectInPrivate, ConnectionVPN, CrackIP, Cryptline, Cryptocloud, CyberGhostVPN, DarknetVPN, DrakkerVPN, DoubleVPN, ExpressVPN, Eztun, FBVPN, FlashVPN, FQVPN, Freedur, FreeVPN, GateVPN, GoldenFrogVyprVPN, GoTrusted, HappyVPN, HideIPVPN, HideMyAss, Hideway, High-Speed-VPN, HostSpotVPN, HotspotShield, IAPSSecurityStore, ibVPN, IdealVPN, InvisibleBrowsing, iOpusiPig, IPJET, Ipredator, ItsHidden, Ivacy, IVPN, Ksecure, KeyVPN, Kryptnet, LamniaVPN, LeVPN, LibertyVPN, LifeVPN, Linkideo, Loki, MadVPN, MetroPipe, MicroVPN, MonkeyVPN, Mullvad, MyOpenGateway, MyVPN, Overplay, oVPN, PacketIX, PC-Streaming, PerfectPrivacy, Privacy.io, Privacy.li, PrivacyTunnel, PrivateInternetAccess, PrivateVPN, PRQtunnel, PublicVPN, PureVPN, Relakks, RemoteVPN, RoadWarriorVPN, RootPanama, RoxNetworks, SaferSurf, SecretsLine, SecureNetics, SecureSwiss, SecureTunnel, SecureVPN, SlickyProxy, SmallVPN, SofanetSofaLINK, SteganosInternetAnonymVPN, StrongVPN, SuperVPN, SurfBouncer, SurfoNym, SurfRescue, SwissPVN, SwitchVPN, TheSafety, Tiggerswelt, tonVPN, Trackbuster, trilightzone, TorrentFreedeom, Tunnelr, TUVPN, UkiVPN, UltraVPN, UnblockVPN, USAIP, VIPAccounts, VIPVPN, VPN4ALL, VPNDeutschland, VPNDog, VPNGates, VPNMaster, VPNonline.ru, VPNPrivacy, VPNProNet, VPNSeek, VPNSteel, VPNSwiss, VPNtraffic, VPNTunnel, vpntunnel.se, VPNSecure, VPNod, VPNout, VPNWorld, VyprVPN, Witopia, WorldVPN, WOWVPN, XeroBank, xtra-vpn, YourFreedom, YourPrivateVPN*

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Range of Sovereign Nations/Localities in this set huge!
    - (S//REL) Multiple Cities in more popular countries
    - (S//REL) Most fee based: Can vary on time/number of servers
      - (S//REL) Most notable exception: *Hotspot Shield* (Provider *AnchorFree*)
        - (S//REL) Advertising supported
        - (S//REL) Multiple OSINT reports of "most popular"
      - (S//REL) About a half dozen others claim they are free
    - (S//REL) Package deals (Europe, any 3 servers, etc.) sometimes available
    - (S//REL) Poster child for location selection: *IAPS* (*www.intl-alliance.com*)
      - (S//REL) *AE, AG, AI, AM, AN, AQ, AT, AU, AW, BB, BD, BG, BM, BR, BS, BZ, CA, CH, CL, CN, CO, CR, CU, CY, DK, DO, EE, EG, FJ, GB, GD, GI, GL, GR, GT, HK, HU, ID, IE, IL, IN, IR, IS, JM, JO, JP, KN, KP, KR, KW, KY, LC, LI, LU, MA, MC, MH, MK, MN, MT, MX, MY, NI, NO, NP, NZ, OM, PA, PE, PF, PG, PH, PK, PR, PS, PY, QA, RO, RU, SA, SB, SC, SE, SG, SI, SK, SN, TC, TH, TR, TV, TW, UA, US, UZ, VA, VE, VG, VI, VU, ZA*,

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Search of SIGINT Forensics Lab Holdings for *OpenVPN*
    - (S//REL) Using SNAPE Portal
    - (S//REL) *OpenVPN* specifically because a client is required
    - (S//REL) Listing is just name of IAT provider
      - (S//REL) *HotSpot Shield*
      - (S//REL) *Steganos Anonymous VPN*
      - (S//REL) *Securenetics*
      - (S//REL) General references to using *OpenVPN* products
      - (S//REL) Several references to IP address only: Need more products in *RONIN*!

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) What "we" want
    - (S//REL) Server enumeration
      - (S//SI//REL) SIGINT: Obvious – target using such a service
        - (S//SI//REL) One hop, so enough coverage means success!
      - (S//SI//REL) Compliance: FAA – Is target in US is important!
    - (S//REL) Exploiting User ↔ VPN traffic
      - (S//SI//REL) Very case by case
        - (S//SI//REL) Coverage (may need 2 sided collection)
        - (S//SI//REL) Protocol (may or may not have vulnerabilities)
        - (S//SI//REL) Settings (implementation important)
        - (TS//SI//REL) "Collateral" - NCSC, TAO, FISA, etc.
        - (S//SI//REL) Request sent to CES if important

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Server enumeration
    - (S//SI//REL) Manual work with Covered Internet (Linux/Windows)
      - (S//SI//REL) Sometimes info derived from documentation
      - (S//SI//REL) Sometimes need to access service
      - (S//SI//REL) May be a trial version to get “seed”
      - (S//SI//REL) Even if paid may only get some servers
      - (S//SI//REL) Some providers give you the works, YMMV
      - (S//SI//REL) Try to minimize work!
      - (S//SI//REL) Try to extend seed(S//REL)
      - (S//SI//REL) DNS “Pattern”, ex. *vpn01.hidegood.net*
      - (S//SI//REL) Use scripting/free Linux tools to exhaust space (try nslookup on *vpn01.hidegood.net*, *vpn02.hidegood.net*, etc.)
      - (S//SI//REL) Open source DNS enumeration scripts (brief look)
      - (S//REL) Where do results go? (Again, See NAC/RONIN talk)

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Server enumeration
    - (S//SI//REL) Use the XKEYSCORE, Luke – AKA Fun with X.509
      - (S//SI//REL) Prompted by *Hotspot Shield (HSS), the free service for which server lists are NOT readily available (Software Reverse Engineering required)*
      - *(S//SI//REL) OpenVPN, as well as SSL/SSTP, send a server x.509 certificate to client as part of setup*
      - *(S//SI//REL) XKEYSCORE sees a LOT of traffic worldwide*
      - *(S//SI//REL) XKEYSCORE fingerprints aren't too hard*
        - *(S//SI//REL)* Need unique string, usually *CN* and/or *DN*
        - (S//SI//REL) Check for valid X.509 certificate
      - (S//SI//REL) Query safe: Traffic encrypted (still do 1-side defeat)

(C//REL) Types Of IAT

- (S//REL) VPN Anonymity Providers
  - (S//REL) Server enumeration
    - (S//SI//REL) Use the XKEYSCORE, Luke – AKA Fun with X.509
      - (S//SI//REL) Prompted by *Hotspot Shield (HSS), the free service for which server lists are NOT readily available (Software Reverse Engineering required)*
      - (S//SI//REL) ***fingerprint('encryption/hotspot_shield/x509') = $pkcs and $udp and 'metrofreefivpn';***
      - (S//SI//REL) ***fingerprint('encryption/easy_hide_ip/x509') = $tcp and from_port(8881) and ('\x06\x09\x2a\x86\x48\x86\xf7\x0d\x01\x01\x01'c) /*RSA*/ and'***www.easy-hide-ip.com***';***
      - (S//SI//REL) ***fingerprint('encryption/comodo_trustconnect/x509') = $tcp and from_port(443) and ('\x06\x09\x2a\x86\x48\x86\xf7\x0d\x01\x01\x01'c) /*RSA*/ and 'ComodoVPNS-';***

(C//REL) Types Of IAT

- (S//REL) Proprietary Multi-Hop Networks (Usually Circumventor Motivated)
  - (S//REL) *Freegate*
  - (S//REL) *Ultrasurf*
  - (S//REL) *Gpass*
  - (S//REL) *Garden*
  - (S//REL) *Haystack* (by Austin Heap – ruled bogus by community)
- (S//REL) Movement to Secure US Government Support to Providers (Congress)
  - (S//REL) US Dept of State
  - (S//REL) Broadcasting Board of Governors (Independent USG Agency)
    - (S//REL) Has instructions for "Getting around Internet Blockage" on Radio Free Asia (RFA) and VOA Persian news sites

(C//REL) Types Of IAT

- (S//REL) Anonymous Remailers (Multi-Hop)
  - (S//REL) Most Secure
  - (S//REL) Main examples: *Mixmaster* and *Mixminion*
  - (S//REL) Extremely High Latency (Random Delays)
    - (S//REL) Only useful for email, other store and forward communications
    - (S//REL) Not much use
    - **(S//REL) NOTE 1: Usability and Anonymity are Foes!**

(C//REL) Types Of IAT

(S//REL) Miscellaneous IAT Technologies (Single Hop)

- (S//REL) *PSIPHON*
  - (S//REL) Discussed in Censorship Circumvention Circles
  - (S//REL) Technology for known associate to setup in appropriate place
  - (S//REL) Access via knowing obscure URL and Username/Password w/HTTPS
- (S//REL) Miscellaneous Multi-Selectors
  - (S//REL) Some are just "HTTP and/or Socks Proxy Aggregators"
    - (S//REL) *EasyHideIP.com*
    - (S//REL) *Real-Hide-IP.com*
      - » (S//REL) Found researching this presentation!
    - (S//REL) Both of these yield list with HTTP GET!
    - (S//REL) Postprocessing: Shell/PERL/etc. script to extract another to check w/Covered Internet (simple proxy option to *wget*)
    - (S//REL) NAC/RONIN will track these

(C//REL) Types Of IAT

(S//REL) Miscellaneous IAT Technologies (Single Hop)

- (S//REL) Miscellaneous Multi-Selectors
  - (S//REL) Proprietary Proxy Provider/Chooser
    - (S//REL) Paid product, Client Software
    - (S//REL) Usually involves obfuscation and/or encryption
    - (S//REL) *GHOSTSURF*
      - (S//REL) First analyzed 2006 – uses obfuscaton
      - (S//REL) Server list has changed but all else same
    - (S//REL) *Easy-Hide-IP*
      - (S//REL) Analyzed in 2011 – uses TLS on port 8881
      - (S//REL) Over 400 servers in 7 countries
    - (S//REL) *Hide-IP*
      - (S//REL) Analyzed in 2006 – New product now
      - (S//REL) Need to re-analyze

(C//REL) Types Of IAT

(S//REL) Miscellaneous IAT Technologies (Single Hop)

- (S//REL) Bot-Based Proxy Networks
  - (U//FOUO) Kudos to [redacted], NGA, for pointing this out in her Intelink-TS blog, Sphinx1121 (Pointer to *krebsonsecurity.com*)
  - (S//REL) Bot owners drop socks proxies on compromised computers
  - (S//REL) Said proxies are then rented out to "customers" for anonymity
  - (S//REL) OSINT indicates a "product" called *XSOX* available on underground forums as a C&C for such a network
- (S//REL) General Note for IAT analysts: Details IMPORTANT
  - (S//REL) Proof by example: *EasyHideIp.com* NOT the same as Easy-*Hide-IP.com* (Of course domains are not case sensitive)

(C//REL) Types of IAT

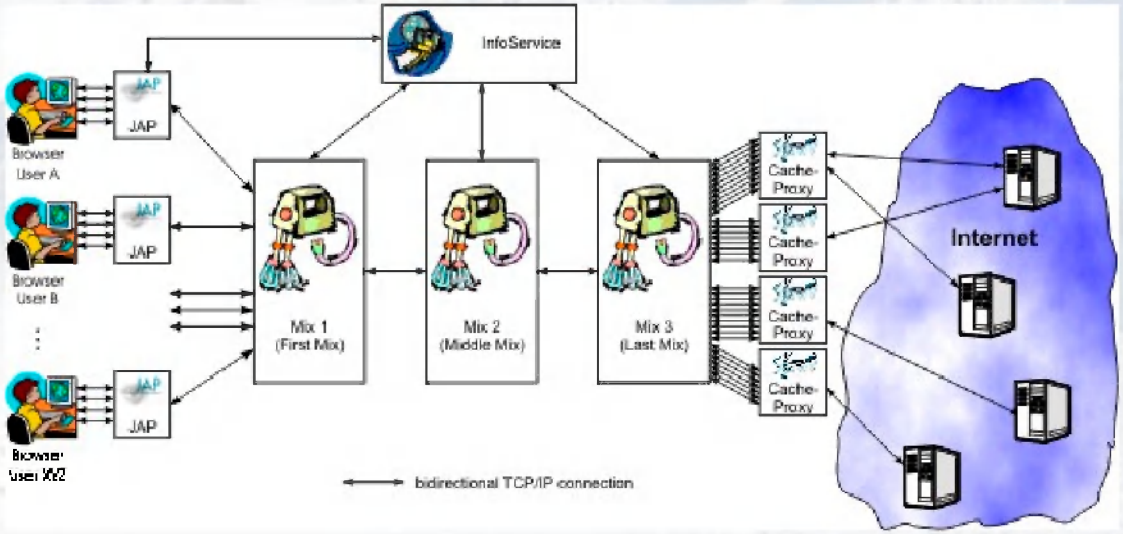
- (S//REL) Open Source Multi-Hop Networks
  - (S//REL) Jondo Anonymous Proxy (JAP)
  - (S//REL) Championed by German University (Dresden)
  - (S//REL) (Mostly?) Open source software – some Docs in German
  - (S//REL) Uses a technology known as *Cascades*
    - (S//REL) Each cascade is set of 2 or 3 *Mixes*
    - (S//REL) All internal traffic encrypted
    - (S//REL) Free service *AN.ON*: 5 Cascades
    - (S//REL) Premium service *JonDoNym*: 10 Cascades
      - (S//REL) Countries: BG, CA, CH, CZ, DE, DK, FR, GB, IT, LU, US,
      - (S//REL) Less than 50 mixes total

(C//REL) Types of IAT

- (S//REL) Open Source Multi-Hop Networks
  - (S//REL) *Jondo 'Anonymous Proxy (JAP)*
  - (S//REL) Comparison with *Tor*
    - (S//REL) Not nearly as well studied
    - (S//REL) Much smaller contained development community
    - (S//REL) More centralized structure (all mixes centrally approved)
    - (S//REL) Not as diverse geographically or scalable
    - (S//REL) Not as well used or publicized
  - (S//REL) Not analyzed in great detail here at NSA (or FVEY?)
  - (TS//SI//REL) Much better chance for Global Adversary (SIGINT :-))
    - (TS//SI//REL) Sessionization of DNI still would be a problem

(C//REL) Types of IAT

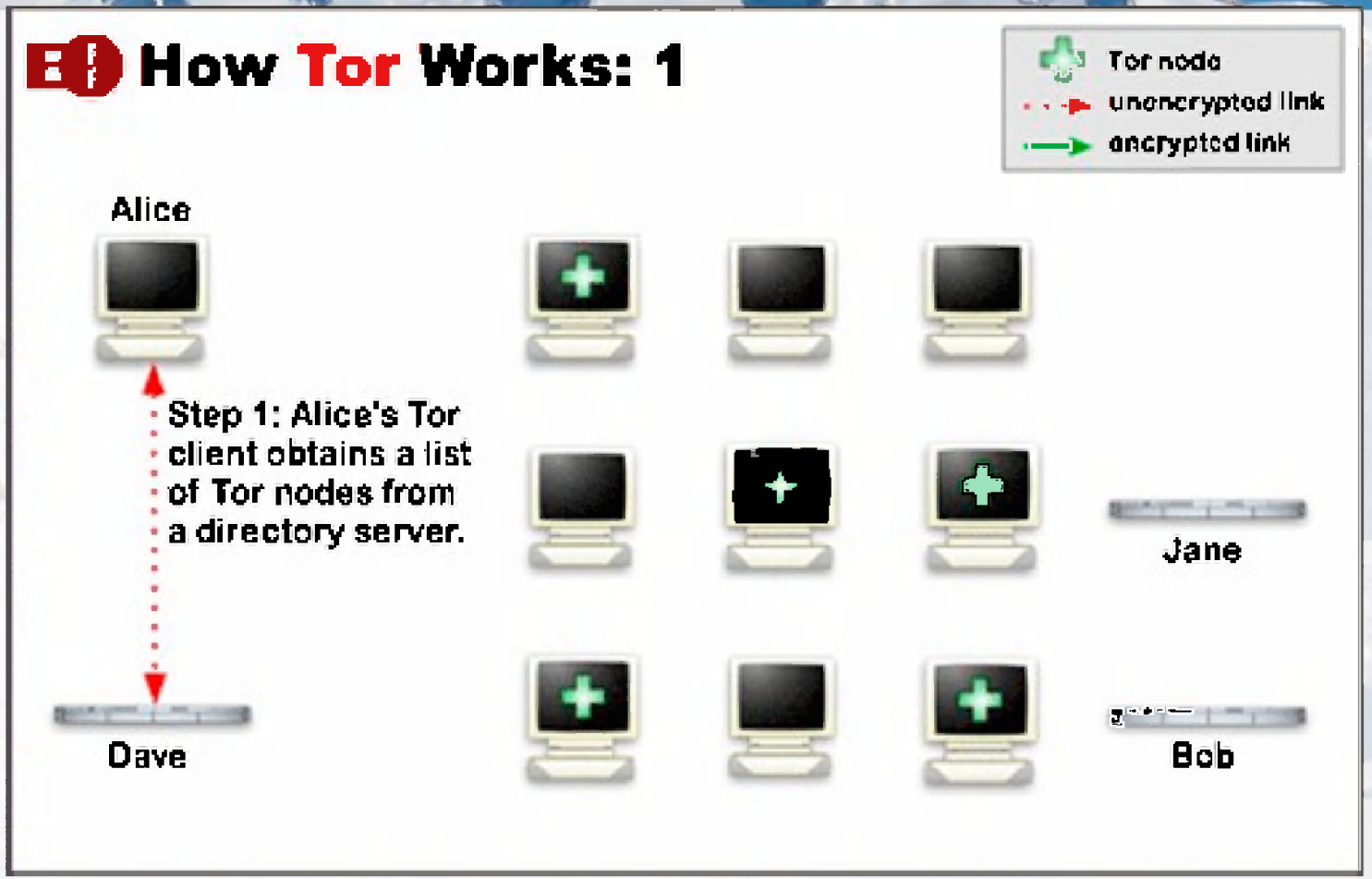
- (S//REL) Open Source Multi-Hop Networks
  - *(S//REL) JonDo /Anonymous Proxy (JAP)*



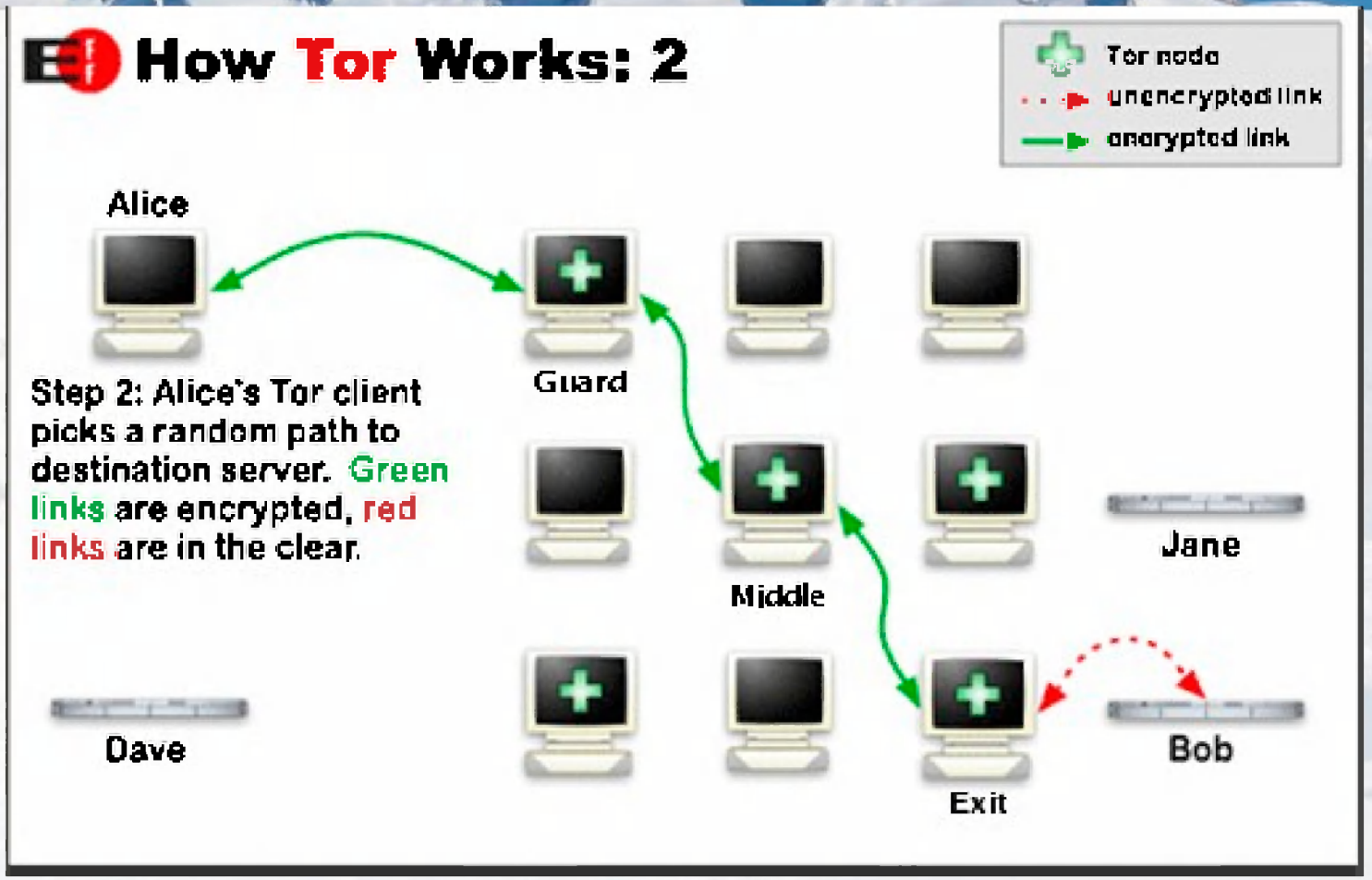
(C//REL) Types of IAT

- (S//REL) Open Source Multi-Hop Networks
  - (S//REL) *Tor*
  - (S//REL) Very widely used worldwide
  - (S//REL) Open Source
    - (S//REL) Active Development
    - (S//REL) Mitigates Threats
  - (S//REL) Very Secure
  - (S//REL) Low enough latency for most TCP uses
  - (S//REL) Still the King of high secure, low latency Internet Anonymity
    - (S//REL) There are no contenders for the throne in waiting

(S//REL) Tor Operation (1)



(S//REL) Tor Operation (2)



(S//REL) Mom: Where Do *Tor* Relays Come From?

- (S//REL) Recall there is (well actually more than 1) *Tor* Directory server?
  - (S//REL) This is the pool
  - (S//REL) Choices made in terms of advertised capabilities:
    - (S//REL) Bandwidth
    - (S//REL) Uptime
    - (S//REL) Supported Protocols
  - (S//REL) *Tor* client has total final say

(S//REL) Mom: Where Do Tor Relays Come From?

- (S//REL) Pool is still currently about 1500
  - (S//REL) Many countries represented
    - (S//REL) Most in DE
    - (S//REL) Second most in US
  - (S//REL) Anyone can set one up and register it
  - (S//REL) Exit nodes are scary (Kiddie Porn)
- (S//REL) How about a private pool? (heh-heh)
  - **(S//REL) Note 2: Private Resources and Anonymity are foes!**

(S//REL) Bridges: Special Tor Relays

- (S//REL) Having the set of relays public makes it easy for government censors
  - (S//REL) Just block access to all relays from that country
- (S//REL) Tor Project staffed with smart people!
  - (S//REL) Introduce new concept: Bridge Nodes
    - (S//REL) Unadvertised Entry Nodes distributed “out-of-band”
    - (S//REL) Project will hand out three at a time (weekly)
      - (S//REL) Email or surf *bridges.torproject.org*
  - (S//SI//REL) SIGINT: Use Tor Against Itself! (Bridge requests from exit nodes)
  - (S//REL) Circa April 2011: Tor Project claims around 600 Bridges

(S//SI//REL) Tor and NSA Targets

- (TS//SI//REL) Sophisticated CT Targets use TOR to access Terrorist Web Forums
  - (TS//SI//REL) Web Forums: *al-Faloja*, *CEMF*, *al-Hisbah*, *shumukh*, *TRSC*
  - (TS//SI//REL) Persona: *DLW*, *Song of Terror*, *Time of Terror*
- (TS//SI//REL) Visible exit traffic allows for “All except the Client IP” SIGDEV
- (TS//SI//REL) Solving (attempting to solve :-( ) this IP address problem was the work of NSA PARTNERSNIPPET team
- (S//SI//REL) Also 80+ CT email selectors who have used Tor

(S//SI//REL) Passive Traffic Analysis

- (S//SI//REL) For Normal SIGINT flow, need to identify *Tor* traffic!
  - (S//SI//REL) Only outer TLS layer visible → How to Distinguish?
  - (S//SI//REL) *Tor* developers attempt to remain anonymous by blending in with myriad other TLS traffic
  - (S//SI//REL) *Tor* TLS has changed over the years
  - (S//SI//REL) There ARE some server → client features which are recognizable *NOW*

(S//SI//REL) Passive Traffic Analysis (2)

- (S//SI//REL) Tor TLS (server → client) startup features
  - (S//SI//REL) Certificate: Specific Diffie-Hellman (DH) Modulus (just string match)
  - (S//SI//REL) Certificate: Issuer and Subject random names of same form – ex: *CN=www.ofzgkdjxvjrss.net (regex match)*
  - (S//SI//REL) Certificate: Always 2-hour lifetime (ASN.1 format → more intensive computation)
- (S//SI//REL) Several XKS fingerprints and a plugin implemented

(S//REL) *Tor* Project Recent Activity

- (S//REL) Driven by Censorship Circumvention, Hide Signature
  - (S//REL) New bridge nodes blocked in China
  - (S//REL) Researching better bridge distribution strategies
    - (S//REL) Claim by *Tor Project* is 8000 requests/day for <1000 total
  - (S//REL) Around Feb 2011, changed the *TLS* handshake
    - (S//REL) Signature more like *Apache* web-server
      - (S//REL) Different DH Modulus
      - (S//SI//REL) New XKS Signatures address this
  - (TS//SI//REL) Proposed eventual change will kill identification!
    - (S//REL) Each *Tor* node will generate randomish signatures in a volatile way specifically designed to look like normal website TLS traffic!

(S//REL) *Tor* Project Recent Activity

- (S//REL) *Tor* on non-traditional platforms
  - (S//REL) *ORBOT*, *Tor* for *Android* smartphones
  - (S//REL) *Tor* Router Project
    - (S//REL) Modified Linksys Router – everything over *Tor*
  - (S//REL) *Hide-My-IP-Address*
    - (S//REL) Proprietary replacement for *Tor Browser Bundle*
    - (S//REL) From "*WCCL Network*" not part of *Tor* Project
    - (S//SI//REL) Looked at based on reference by CT target
  - (S//REL) Tor Project working on better strategies to distribute bridges
  - (S//REL) *Tails*: Complete Bootable OS on CD for anonymity
    - (S//REL) *Tor* is a crucial component

(S//REL) *Tor* Hidden Service URLs

- (S//REL) *Tor* Hidden Services (HS) for anonymous publishing
  - (S//REL) Not real reliable, but *Tor Project* research continues
  - (U//FOUO) I said outside scope, sorry
  - (S//REL) Tor HS accessed via Tor only by http://xxxxxx.onion
  - (S//REL) There is the *tor2web.com* site which is a HTTP to *Tor* proxy
    - (S//REL) Loses some anonymity but easy to use
    - (S//REL) Good tool for Covered Internet research
  - (S//REL) Site on WikiInfo to document Tor HS URLs
    - (S//REL) "The Onion Realm" - [redacted]
    - (U//FOUO) Kudos to CES/CTSO (S314) for populating this

(S//REL) Public IAT Resources Inside

- (U//FOUO) General IAT
  - (S//REL) [redacted]
- (S//REL) *Tor*
  - (S//REL) [redacted]
  - (S//REL) [redacted]

(S//REL) References to IAT in SIGINT

- (S//REL) "Grep" in SIGINT reports for relevant phrases (ex anonymity)
  - (S//REL) Most is FVEY (cited here) Majority US, also UK, CAN
  - (S//SI//REL) Format is TOPI / Type of Info
    - (TS//SI//REL) CT / Discuss *Tor* (6 reports)
    - (TS//SI//REL) CT / Use *Tor* or another proxy
    - (TS//SI//REL) CT / Create modified *Tor*
    - (TS//SI//REL) CT / Mandate use of *Tor*
    - (TS//SI//REL) CT / *Tor* for Censorship Circumvention
    - (TS//SI//REL) CT / Use *Tor* and a VPN (*UltraVPN*)
    - (TS//SI//REL) CT / Instructions for using *Tor* and other US Proxy
    - (TS//SI//REL) CT / Discuss us of (non-specified but non-US) VPN
    - (TS//SI//REL) CT / Discuss *Tor* and HTTP Proxies for anonymity
    - (TS//SI//REL) CT / Discuss *Tor* and *RealHideIp* (previously unknown IAT)
    - (TS//SI//REL) CT / Discuss use of *Kproxy.com* (HTTP Proxy)

(S//REL) References to IAT in SIGINT

- (S//REL) "Grep" in SIGINT reports for relevant phrases (ex anonymity)
  - (S//SI//REL) Format is TOPI / Type of Info
    - (TS//SI//REL) CT / Use of *PimpMyIp* (HTTP Proxy)
    - (TS//SI//REL) CT / Use of (masked US Company) VPN (L2TP protocol) for anonymity
    - (TS//SI//REL) CT / Instructions for use of VPNs for anonymity
    - (TS//SI//REL) CT / Use of VPN (*HotSpotShield*) and SSH tunnels
    - (TS//SI//REL) CT / Use of *Tor* and an unspecified VPN
    - (TS//SI//REL) CT / Use of *Easy-Hide-IP* (Socks proxy chooser)
    - (TS//SI//REL) CT / Use of unspecified anonymizing proxy
    - (TS//SI//REL) CT / Instructions on use of *Tor* and name-masked US program
    - (TS//SI//REL) CT / Use of VPN (*Cyberghost*)
    - (TS//SI//REL) CT / Use of unspecified HTTP proxy
    - (TS//SI//REL) CT / Questions on whether *Tor* is compromised
    - (TS//SI//REL) CT / Questions on whether associated compromised by IAT non-use

(S//REL) References to IAT in SIGINT

- (S//REL) "Grep" in SIGINT reports for relevant phrases (ex anonymity)
  - (S//SI//REL) Format is TOPI / Type of Info
    - (TS//SI//REL) Iran / Use of *Freegate* and *Ultrasurf*
    - (TS//SI//REL) India / Use of unknown proxy for anonymity
    - (TS//SI//REL) India / Use of *Tor* to access a webmail account
    - (TS//SI//REL) India / Use of *Tor* for hacking (2 reports)
    - (TS//SI//REL) India / Provision of list of socks proxies to use
    - (TS//SI//REL) Iran / Provision of list of socks proxies to use
    - (TS//SI//REL) India / Use of unknown proxy for anonymity
    - (TS//SI//REL) Cuba / Use of unknown proxy for anonymous research
    - (TS//SI//REL) Turkey / Use of *Tor*

(U) Backup Slides

- (S//REL) From Last years SDC *Tor* Talk

(S//REL) Tor (The onion router)

- (S//REL) Development originally NRL funded
- (S//REL) Original developers from Anonymous Remailer Research Community
- (S//REL) Project now a US non-profit (www.torproject.org)
- (S//REL) User to Internet site interaction uses 3 hops through Tor “Relays”
  - (S//REL) Entry
  - (S//REL) Middle
  - (S//REL) Exit

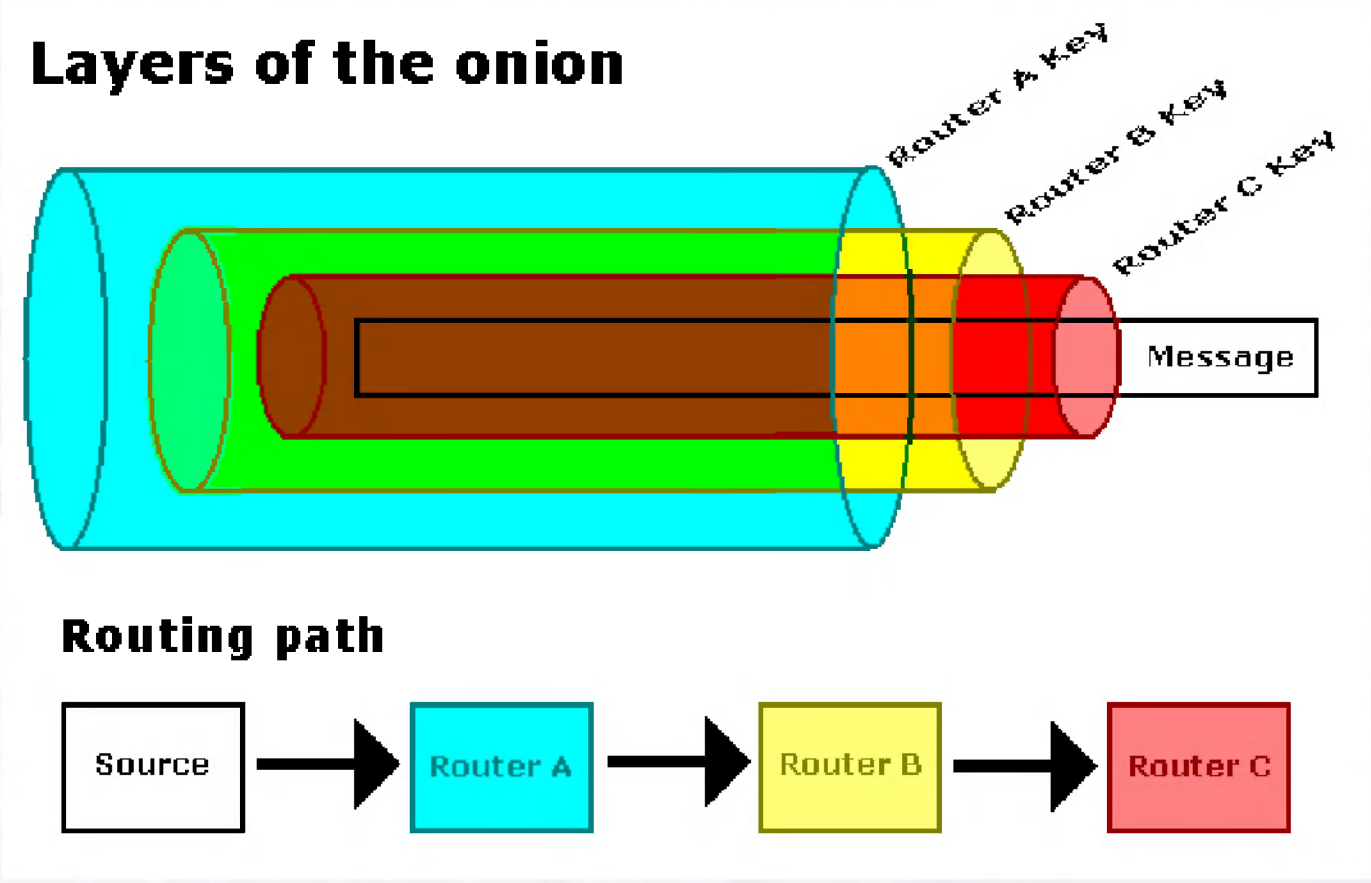
(S//REL) Tor Security

- (S//SI//REL) As you can see from the diagram, everything except for final hop is encrypted.
- (S//SI//REL) The final hop may be also in the case of Bob being an SSL site.
- (S//SI//REL) Two-layer TOR encryption: Pipe between any 2 nodes TLS encrypted (Only thing seen externally).
- (S//SI//REL) Inside the TLS is the Onion Routing (see following diagram):

(S//REL) Tor Security (2)

- (S//SI//REL) So each node can only decrypt data between its predecessor and itself and only knows about its predecessor and successor.
- (S//SI//REL) The exit node can read the final traffic if it is not SSL.
- (S//SI//REL) The user Tor client is in control of everything
  - (S//SI//REL) Setting up keys for cryptography
  - (S//SI//REL) Choosing the Entry, Middle, and Exit
- (TS//SI//REL) Tor is very good – No passive exploitation :-(

(S//REL) Tor Onion Encryption



(S//SI//REL) Passive Traffic Analysis (3)

- (S//REL) NSA Network Analysis Center (NAC) data source GOLDENFORTIN
  - (S//REL) *Cisco Netflow* Records
    - (U) From IP Address
    - (U) To IP Address
    - (U) Time Up
    - (U) Time Down
    - (U) Number of Bytes
    - (U) Number of Packets
  - (S//REL) Heavy Representation of Tor Relays

(S//SI//REL) Passive Traffic Analysis (4)

- (S//SI//REL) How to use Tor network data?
  - (S//SI//REL) Attempt to work back from known exit traffic of interest all the way back to client user
    - (S//SI//REL) This is “Circuit Reconstruction”
    - (S//SI//REL) Requires great coverage
    - (S//SI//REL) Geography might be your friend sometimes
  - (S//SI//REL) Attempt to correlate known exit traffic to a small set of putative client traffic
    - (S//SI//REL) Client Geographical Assumption Required
  - (TS//SI//REL) No smoking gun yet :-(Optimism still lives!

(TS//SI//REL) Active: Traffic Shaping

- (S//SI//REL) This primarily means deny/degrade to date
  - (TS//SI//REL) If target is behind a choke point to Internet
    - (TS//SI//REL) Block all or a major subset of Tor Relays
    - (TS//SI//REL) Block all Tor TLS handshakes
  - (TS//SI//REL) Try to force target to use alternate communications means
- (S//SI//REL) Always the (potential) Exploit vs Attack Tradeoff

(TS//SI//REL) Active: Implants

- (S//SI//REL) *TorButton*: A Thorn in the side of SIGINT
  - (S//REL) One of the components of *The Tor Browser Bundle* – AKA “Tor for Dummies”
  - (S//REL) Firefox browser plugin – on/off switch for *Tor*
  - (S//REL) Locks down browser REAL good (disables all active content things, sandboxes state, etc.)
- (TS//SI//REL) No current bypass methods for CNE Exploits
- (TS//SI//REL) Only hope is implanting web server with poisoned content document intended for target

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu