(U) Air-Gapped Network Threats

Jump to: navigation, search

Contents

[hide]

[edit] (U) Background

(S//NF) An “air gap” is the physical separation of a network from other networks. For example, classified computer networks typically are air-gapped from the Internet or other networks of lower classification. Even if a high-value network is designed to be isolated from the Internet, an adversary could try to circumvent an “air gap” by finding computers inadvertently connected to both the Internet and the isolated network.

(S//NF) Since August 2003 and March and August 2004, viruses infected computers on classified military networks, apparently through unauthorized connections from the Internet, according to military reporting.[1] The viruses did not target classified systems, but the incidents illustrate the potential for inadvertent connections to bridge what should have been a secure air gap.[2]

(S//NF) Growing interconnectivity between secure and non-secure networks combined with current adversary intrusion trends suggest that threats against sensitive DoD networks are growing. There are fewer and fewer actual air-gapped systems. There are some older systems where one has to transfer large sets of data between classification levels, but that technology is going away and being replaced by cross-domain guards. In some cases, for security reasons, they may always keep the air gap, such as for cryptographic key generation. There may be other compartmented networks that are totally air-gapped still. (Some say air-gapped refers to all connections and others are using it to apply to just the Internet. A series of guards from the Internet to the network is technically not air-gapped but those threats should be addressed as well.)

[edit] (U) Key Findings

- (TS//SI//REL TO USA, FVEY) The MAKERSMARK W37B implant poses a significant threat to U.S. and allied classified networks if policies and procedures covering removable media are not adhered to. [3]
- (S//NF) To attack the air-gapped system, the adversary must implant devices through direct physical attack, through a trusted insider (possibly unwittingly), or through attacking the supply chain to the network.
- (S//NF) The most successful attack against an air-gapped system would contain elements of an insider attack with implants that can be triggered remotely at a later time. For example, a thumb drive or other implant may be inserted by a trusted insider that enables a previously inactive wireless port that is

connected to a defeated cross domain solution via supply chain interdiction. The greater the complexity of a compound attack, the more unlikely the probability of success, and the lower the threat. Therefore, the likelihood of a successfully completed attack is low.

- (S//NF) There may be weaknesses that are exploitable remotely through a cross domain solution, but the damage possible due to a remote attack without physical implant is much less than a remote attack combined with a physical attack.

[edit] (U) Recent News and Reporting

click column headers to sort

Agency	Feed
Open Source	Failed to load RSS feed from [redacted]
CIA	Failed to load RSS feed from [redacted]
DIA	Failed to load RSS feed from [redacted]
NSA	Failed to load RSS feed from [redacted]
State Department	Failed to load RSS feed from [redacted]

[edit] (U) Threat from Physical Implants

(S//NF) In 2004, US Air Force personnel portraying computer infiltrators during an exercise used fabricated credentials to enter opposing forces' headquarters and installed a device bridging two physically separated networks to enable later access from the Internet, according to military reporting.[4]. In 2005, an unidentified intruder broke into a US Government contractor's office building and stole computers containing employees' personal information, according to a press report.[5] Also in 2005, cleaning staff at Sumitomo Mitsui Bank in London attached hardware bugs to computer keyboards, according to a press report. The bugs captured computer passwords, which criminals then used to access Sumitomo systems in an attempt to steal about $300 million.[6]

(S//NF) In April 2006, U.S. press reported that Afghan nationals working as cleaners and garbage collectors at the U.S. base in Bagram had stolen flash memory "thumb drives" containing classified information and sold them at the local bazaar.[7]

[edit] (U) Supply Chain Attacks

(S//NF) A few intelligence services reportedly have stealthily penetrated computer networks by subverting the supply chain—the people and companies who supply hardware and software. The complexity of hardware and software makes detecting a subversion extremely difficult, but an adversary would find it difficult and expensive to acquire the skills and tools to create a subtle subversion. Moreover, an adversary would need to plan carefully to ensure that a subverted product makes its way into a chosen high-value target network.[8]

(S//NF) An adversary could subvert a supply chain by recruiting or inserting a programmer or hardware

engineer, setting up a front company, or replacing legitimate hardware or software with a subverted version during distribution or routine maintenance. Subversions could include “back doors” that permit covert access or control, code that silently steals data, or disruptive “logic bombs.[9] A supply chain attack to a CDS guard could be very effective. The U.S. government has had problems in the past buying fraudulent computer equipment that luckily was not an attack from a foreign intelligence service.

(S//NF) As of October 2005, the German Federal Intelligence Service (BND) had established a few commercial front companies that it would use to gain supply chain access to unidentified computer components, according to information obtained during an official liaison exchange. Beginning in 2002, the French external intelligence service (DGSE) delivered computers and fax equipment to Senegal’s security services and by 2004 could access all the information processed by these systems, according to a cooperative source with indirect access. In 2000, the Iraqi regime executed or jailed a number of people connected to technically compromised computers intended for use by the Iraqi Government. According to a source with good access and London-based media reports, Baghdad blamed Israeli intelligence for the operation.[10]

(S//NF) Russia has experience with supply chain operations, but we do not have a firm grasp of the current Russian supply chain threat. Russian software companies have set up offices in the United States, possibly to deflect attention from their Russian origins and to be more acceptable to US Government purchasing agents. We have no indication that these companies have ever served as platforms for Russian computer network operations; however, a well-run front company would not present direct indicators. The next attacks may be attempted while the product is part of the supply chain, or by a trusted insider outside of the supply chain.

See also: Supply Chain Cyber Threats

[edit] (U) BIOS Implants

(TS//SI) A Basic Input/Output System chip (BIOS) is used to load and start an operating system. It is stored on a read-only memory chip on a computer motherboard. The main reason for introducing malware into an expansion card (or BIOS) is to maintain a persisting presence through typical methods of system rebuilds. In addition to being immune to hard disk reformatting and OS reinstallations, some BIOS implants can survive a flashing of the BIOS by hiding in the BIOS’s free space. A BIOS implant cannot be detected by traditional security mechanisms based on an operating system’s software because the BIOS resides outside the operating system. BIOS implants are unaffected by hard drive wipes and can trick forensics tools into thinking the BIOS is operating normally or has been properly reflashed.[11]

(TS//SI) Recent reporting corroborates the tentative view in a 2008 national intelligence estimate that China is capable of intrusions more sophisticated than those currently observed by U.S. network defenders. DIA assesses China’s basic input/output system (BIOS) computer network exploitation capability reflects a qualitative leap forward in exploitation that is difficult to detect.[12] There still needs to be a path to the Internet to exfiltrate data from an implanted machine. A DOS attack is easier to achieve but still requires activation to be used in a timed coordinated computer network attack.

See also: BIOS Threats

[edit] (U) Implants in KVM Switches and Peripherals

(U//FOUO) KVM (keyboard/video/mouse) switches are used to allow access to multiple computers, usually connected to different networks, with a single set of interface hardware. The switch necessarily makes an electrical connection between the interfaces and all the computers, which introduces the risk that someone with access to a low level system will be able to obtain data from a higher level system using this

connectivity.

(U//FOUO) If the switch is programmable it may be possible for someone with electronic access to an unclassified system to reprogram the switch to copy data being typed on a classified system to the unclassified system. If the switch has memory, it may be possible for data that was entered while switched to a classified system to be transferred to an unclassified system. A device that electrically connects classified and unclassified systems is an ideal place for an implant. This attack requires physical access to the KVM switch, which may be either before or after the switch has been delivered and installed.[13] Some call the KVM switch a CDS and require strict protocols for their acquisition for this reason. A supply chain or insider attack on a single KVM switch could be very damaging if successful. Though, it is not likely to produce unfettered access to an air-gapped network.

(U) The U.S. attempted to use a supply chain attack to place implants in printers to perform a DOS attack on the Iraq C2 network during the OPERATION DESERT STORM. It is unknown whether the trigger was wireless, timed, or through Internet guards.[14]

[edit] (U) Enabled Wireless and Other Emanations

(U) Since the CDS attacks mentioned later are difficult, enabling a rogue wireless access point may be the easiest way to access an air-gapped network. Graphic, sound, and network card firmware could provide further hiding places for malware. Graphic cards have been subverted to support distributed brute-force password breaking since they are essentially many parallel processors like a mini-supercomputer. Network cards could be used to create covert channels to exfiltrate data as in the following example.[15]

(U) In 2005, an Israeli man was convicted of stealing about $90,000 from the Postal Bank in Haifa by breaking into a bank branch and installing a wireless access device, then accessing the bank's internal network from a nearby office using the implanted wireless signal, according to Israeli press reporting[16] TEMPEST]] countermeasures should guard against this possibility, and this is why they are still very necessary.

(U) A microphone could be used to capture the audio sound produced from dot matrix printers, then evaluated to discover what exactly was printed on the device. By examining the sound wave, length, height, intensity they were able to correctly identify the text printed with a 65% accuracy.[17] Since this only worked from 2 meters away, an additional channel would be needed to exfiltrate the signal. Security researchers have shown that sound cards can be controlled by malware to emit frequencies beyond normal hearing range designed to exfiltrate data.[18] Again, TEMPEST shielding helps guard against this threat. It was shown that an iPhone can use its accelerometer to reconstruct up to 80% keyboard activity when placed next to keyboard. [19]TEMPEST Would not guard against this threat.

(TS//REL TO USA, FVEY) Radio Frequency (RF) Flooding, a form of close-access collection, can recreate and display data from a smartphone, or a nearby monitor. An example of RF flooding is when a smartphone is placed next to a classified information processing system. The RF signals from the smartphone can unintentionally couple with the video signal on the classified computer monitor. The smartphone signal, which includes the coupled monitor signal, can then be collected on a listening post such that the original classified monitor signal can be reconstructed, displayed, and exploited by the adversary. For these reasons the battery of the phone must be removed if the phone is brought in proximity to an air-gapped network.[20]

See also: Technical Surveillance Countermeasures

[edit] (U) Infected Removable Media

(U//FOUO) One attack that is known to "jump the gap" between networks can be successfully achieved through the insertion of removable media into a computer on the Internet, before and/or after placing it in a higher classification computer. While the media is connected to an unclassified network, malware is downloaded onto the media. After the media is inserted into a higher classification computer, the malware then implants the "high-side" with a callback or beacon to the attacker's computer, permitting passive collection of data, or active accessibility by a hacker to that domain. (This also may be achieved by disconnecting an entire computer, connecting it into the Internet, and then later reconnecting it to the higher classification network.) This is actually a bypass of the CDS, which is a security violation that occurs regularly. It is not certain if most of these events are an intentional breach of security or acts of negligence, but can never the less result in infection with malware, and data exfiltration. NTOC has no evidence of any targeted attacks that were successful using this method.

(S//REL TO USA, FVEY) According to previous reporting, an OPSEC incident involving the transfer of malware between unclassified and classified networks occurred in July 2008. The malware, called Agent.BTZ by antivirus vendors, existed on an unclassified computer. An authorized user placed a thumb drive into the unclassified computer and then into the SIPRNet, thus infecting the classified network with the virus. See SIPRNet Threat Assessment. The malware is a Trojan with worm capabilities. It can locate any physical or logical drive and then copy itself to that drive. The next time the media is inserted into the unclassified box, a callback occurs and network topology information is attempted to be exfiltrated to the person who initiated the exploitation. The incident caused multiple infections in unclassified and classified DoD networks, but there was no evidence that an actor was able to gain control of a DoD classified host. Subsequent orders were given to prevent the use of removable media to transport data between networks. However, it is apparent that such orders are easily ignored. Agent.BTZ was attributed to the MAKERSMARK (MM) intrusion set, sponsored by Russia's Federal Security Service (FSB) to collection of military, diplomatic, economic and science and technology data.[21]

(TS//SI//REL TO USA, FVEY) There are many variations to this implant such as the W37B. The MM W37B implant is a lightweight, stand-alone implant used primarily for propagation and survey. This particular implant is also the only known implant to possess the capability to create a communications bridge between infected hosts on the Internet and air-gapped networks if infected removable media is continuously used between the two. This capability poses a significant threat to U.S. and allied classified networks if policies and procedures covering removable media are not adhered to.

(U) Disabling network ports and removable media like universal serial bus (USB) ports and CD and floppy drives cuts off a simple way that insiders could bring unauthorized software into a network or take information out.

[edit] (U) Threat from Remote Attacks

[edit] (U) Cross-Domain Solutions

(S//NF) The only way to get to an air-gapped system remotely is through a cross domain solution (CDS). A possible method of attack would be tunneling from a network of one classification to a network of a different classification. If the CDS guard is not properly configured or if it fails to an unsecure state, then it may allow malicious code through. It is theoretically possible for an insider or supply chain attacker to make a trapdoor in the guard. (This would have a similar effect as when someone accidently connects a SIPRNet machine to the Internet, which happens often.) If it is a one way up guard, an attacker can get code to the high side if

they have used reconnaissance to determine an address to go to. But that path is virus scanned. In most cases, they only let certain highly formatted messages in. That makes an attack very difficult – assembling parts of malcode on the inside to prepare for an attack. This would be difficult to do without help from an insider. If the CDS guard works as indicated, properly configured with all controls in place, then it would be very hard to make this attack work. It is possible for a guard to be poorly installed such as when a router or firewall is left with a default password. But this is very unlikely on a classified network with many controls in place.

(TS//SI//REL TO USA, FVEY) [redacted], BYZANTINE CANDOR actors participated in activities which could indicate an interest in CDS systems. The actors exfiltrated a file which contained instructions on how to change the password on the low side C2 Guard queue manager, as well as how to change the root password on each UNIX server for both the test bed and high side. The file contained weak, clear text passwords for what are believed to be CDS that transfer Global Decision Support System (GDSS) data from NIPRNet to SIPRNet through C2 Guards. Access to GDSS queue managers could allow BYZANTINE CANDOR to attack the C2 guards that act as security filters that process data that is passed between NIPRNet and SIPRNet. Fortunately, we have no reports of this being successfully carried out.[22] SIPRNet IP addresses, including SIPRNet to NIPRNet CDS hosts, are available via open source IP repositories and have been probed.[23] Most would not call SIPRNet an air-gapped network but it is disturbing nevertheless that sophisticated adversaries could gain access to SIPRNet if successful with these types of attacks.

(S//NF) NTOC does not have reporting of exploitation of networks via the CDS. NTOC does have extensive reporting of procedural violations that bypass the use of the CDS mechanisms, and the violations have endangered classified materials, and network services.

See also: Cyber Threats to Cross-Domain Solutions

[edit] (U) Virtual Private Networks

(U) A Virtual Private Network (VPN) refers to two or more separate networks logically or virtually and securely joined, generally over an untrusted network such as the Internet. Both government and commercial entities rely heavily on VPN technology for secure communication. Classified networks rest on unsecured Internet backbone with only the protection of VPN encrypted communication.

(U) Hackers and criminals have exploited VPNs and unprotected modems to find easily concealed and plausibly deniable access paths. An adversary could compromise a computer used for telecommuting and then hijack the trusted VPN to gain access to the target network.[24] Most VPN attacks occur through phishing and gaining access to a box connected to the Internet and then acquiring the VPN access from that box to the private network. VPN networks not connected to the Internet would not be exploitable in this way.

(C) In 2003, a computer virus specifically targeted bank employees' computers and captured VPN passwords, apparently to enable later operations against the banks' VPNs. The identities of the author and releaser of the virus are unknown.[25]

(U) In December 2004, an audit by the Department of Homeland Security's Inspector General found 20 unaccounted-for modems by war dialing and discovered that about 8,000 VPN and dial-in passwords, including administrator passwords, were easily guessed.[26]

(U) The DOD community relies on VPN for secure communication. That is what makes these attacks worth the effort it would take to find the few vulnerabilities wherever they may exist.

See also: VPN Threats

[edit] (U) References

1. ↑ (S) DOD-CERT Situation Awareness Report 2004-SA-0011, Netsky on SIPRNet, March 2, 2004.
2. ↑ ((S) DOD-CERT Situation Awareness Report 2004-SA-00311, Malicious Activity on SIPRNet, August 11, 2004.
3. ↑ (TS//SI//REL TO USA, FVEY) DIRNSA, 3/OO/521496-09, Information Operations/MAKERSMARK: Latest Version of W37B Implant (version 2.10) Deploys; Small Group of Initial Victims Consistent with Previous Targeting from 11 August 2009, 21 August 2009. Extracted information is TS//SI//REL TO USA, FVEY.
4. ↑ (S//NF) NSA, RED TEAM "QUICK-LOOK" FOR EXERCISE TERMINAL FURY 05 (TF05), Defensive Information Operations (DIO) and Fleet Information Warfare Center (FIWC) RED TEAMS, December 2004.
5. ↑ (U) Griff Witte, "Break-in at SAIC Risks ID Theft", Washington Post, February 12, 2005.
6. ↑ (U) Peter Warren and Michael Streeter, "Mission Impossible at the Sumitomo Bank", The Register, 13 April 2005.
7. ↑ (U) Watson, Paul, "U.S. Military Secrets for Sale at Afghan Bazaar", Los Angeles Times, April 10, 2006.
8. ↑ (U) CIA, Penetrating High-Value Computer Networks: A Look Inside the Enemy's Playbook, July 20, 2006. Extracted information is S//NF.
9. ↑ (U) CIA, Penetrating High-Value Computer Networks: A Look Inside the Enemy's Playbook, July 20, 2006. Extracted information is S//NF.
10. ↑ (U) CIA, Penetrating High-Value Computer Networks: A Look Inside the Enemy's Playbook, July 20, 2006. Extracted information is S//NF.
11. ↑ (S) Louchard, B., et al, (S) DIA, Defense Intelligence Digest: BIOS: China's Covert Cyber Capability, October 14, 2010 (A-Space required. Extracted information is TS//SI.)
12. ↑ (S) DIA, Defense Intelligence Digest: BIOS: China's Covert Cyber Capability, October 14, 2010 (A-Space required. Extracted information is TS//SI.)
13. ↑ (U//FOUO) [redacted] C43 Informal Technical Note, C43-023-00, A Look At The Risks of KVM (Keyboard/Video/Mouse) Switches with Multilevel Systems, 6 July 2000.
14. ↑ (U) Crawford, George, Information Warfare: New Roles for Information Systems in Military Operations, Air and Space Power Chronicles quoting from "Computers: Chip Shot," in U.S. News & World Report, Vol. 117, No. 23, December 12, 1994.
15. ↑ (S//NF) USCYBERCOM, J2 Bulletin 10-03, Hardware-Based Malware Demonstrates Resistance to Standard Security Practices, June 30, 2010.
16. ↑ (U) David Rudge, "Hacker cracks bank's computer code", Jerusalem Post, April 6, 2005.
17. ↑ (U) Acoustic Side-Channel Attack on Printers, USENIX Security Symposium, Washington D.C. 2010.
18. ↑ (S//NF) USCYBERCOM, J2 Bulletin 10-03, Hardware-Based Malware Demonstrates Resistance to Standard Security Practices, June 30, 2010.
19. ↑ (U) Terrazas, M.; Georgia Tech Turns iPhone into Spiphone; 17 Oct 11
20. ↑ NTOC, Z-T/OO/NTC/1137-09; 14 Dec 09; NTOC Threat Assessment: Threats to BlackBerry Server/Network Infrastructure, August 2006-July 2009
21. ↑ (TS//SI//REL TO USA, FVEY) NTOC, SUBSTANTIVE REVISION: NTOC THREAT ASSESSMENT: Foreign Threat to the Secret Internet Protocol Router Network, February 2010, 3/OO/NTC/0297-10, March 2010. Extracted information is S// REL TO USA, FVEY.
22. ↑ (TS//SI//REL TO USA, FVEY) NTOC, Information Operations/BYZANTINE CANDOR:

BYZANTINE CANDOR Views, Records, and Exfiltrates the Contents of Cleared Defense Contractor Files Associated with USTRANSCOM Mission Critical Mobility Systems, July to November 2009, 3/00/533505-09, December 2009. Extracted information is TS//SI//REL TO USA, FVEY.

23. ↑ (S//REL to USA, FVEY) NTOC, NTOC ADVISORY: Suspicious Activity May Be Targeting SIPRNET Cross-Domain Solutions, S/OO/NTC/0206-09, April 2009. Extracted information is S//REL to USA, FVEY.
24. ↑ (U) CIA, Penetrating High-Value Computer Networks: A Look Inside the Enemy's Playbook, July 20, 2006. Extracted information is S//NF.
25. ↑ (U) Symantec, "W32.Bugbear.B@mm",http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.b@mm.html, October 27, 2004.
26. ↑ (U) DHS Office of the Inspector General, "DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data (Redacted)", OIG-05-03, November 2004.

Retrieved from "http://[redacted]"
Categories: Cyber Threat Assessments | Russia Cyber

TOP SECRET//SI//NOFORN

- This page has been accessed 1,103 times.
- 6 watching users
- This page was last modified 19:44, 6 July 2012 by [redacted]. Most recent editors: [redacted].

Personal tools

- [redacted]
- My talk
- My preferences
- My watchlist
- My contributions
- Log out

Namespaces

- Page
- Discussion

Variants

Views

- Read
- Edit
- Page history
- Watch

Actions

- Rename/Move
- Tag this page

Search

Search | Search

- Main Page
- Recent changes
- Help
- Random Article
- Sandbox
- Guidelines
- Recent files
- Top categories

interaction

- Featured articles
- Announcements
- Collaboration requests
- Tutorial
- Bulletin Board
- Metrics
- Acronyms
- People Finder

social software tools

Toolbox

- Privacy policy
- About Intellipedia
- Disclaimers
-

[redacted]

Use of this U.S. Government system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution.
Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse actions.
This page contains dynamic content -- Highest Possible Classification isTOP SECRET//SI/TKSecurity BannerTerms of Use