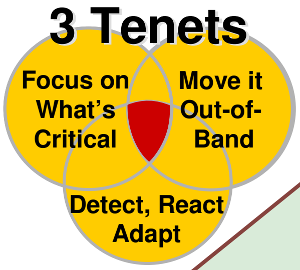
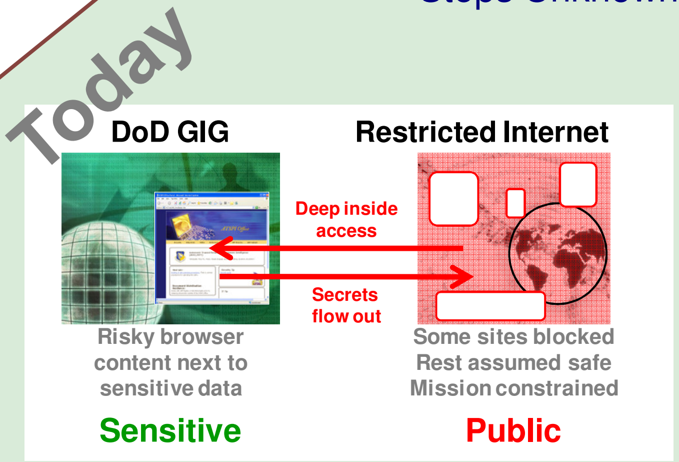
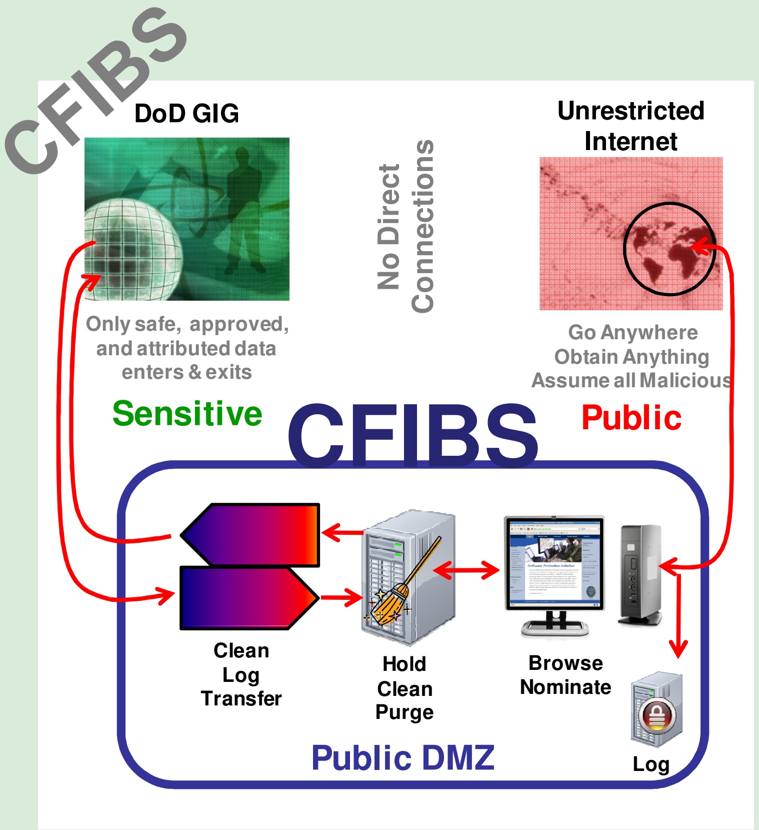
CFIBS

Cross Fabric Internet Browsing System



- Safe Desktop Browsing
- Safe File Transfers
- Stops Unknown Exfiltration
- Any Website, Any Content
- Push-plus-Pull Transfers
- DIACAP Type Accreditation


Today
DoD GIG
Restricted Internet
Deep inside access
Secrets flow out
Risky browser content next to sensitive data
Some sites blocked Rest assumed safe Mission constrained
Sensitive
Public



The Dangerous But Necessary Internet

The DoD's Net-centric doctrine, corporations, and users alike depend upon the Internet. But even the best-managed, locked-down PCs on restricted networks are exposed to risks from malicious Internet content through the easily-exploited browser. In 2008, Symantec reported 95% of cyber attacks were against the browser. Why? It's the easiest path for criminals and adversaries to obtain sensitive data. How? Untrusted web data in the browser executes on a well-known OS deep inside the network.

Poor Alternative 1

Today, most enterprise network solutions attempt to mitigate Internet risk by blocking / scanning risky sites, protocols, and content. Attackers simply corrupt "good" websites and infect content faster than we can change our blacklists and definitions. Patches arrive weeks to months <u>after</u> exploits are realized. These "solutions" interfere with legitimate activities yet do not stop data leaks, Advanced Persistent Threats, or honest user accidents.

Poor Alternative 2

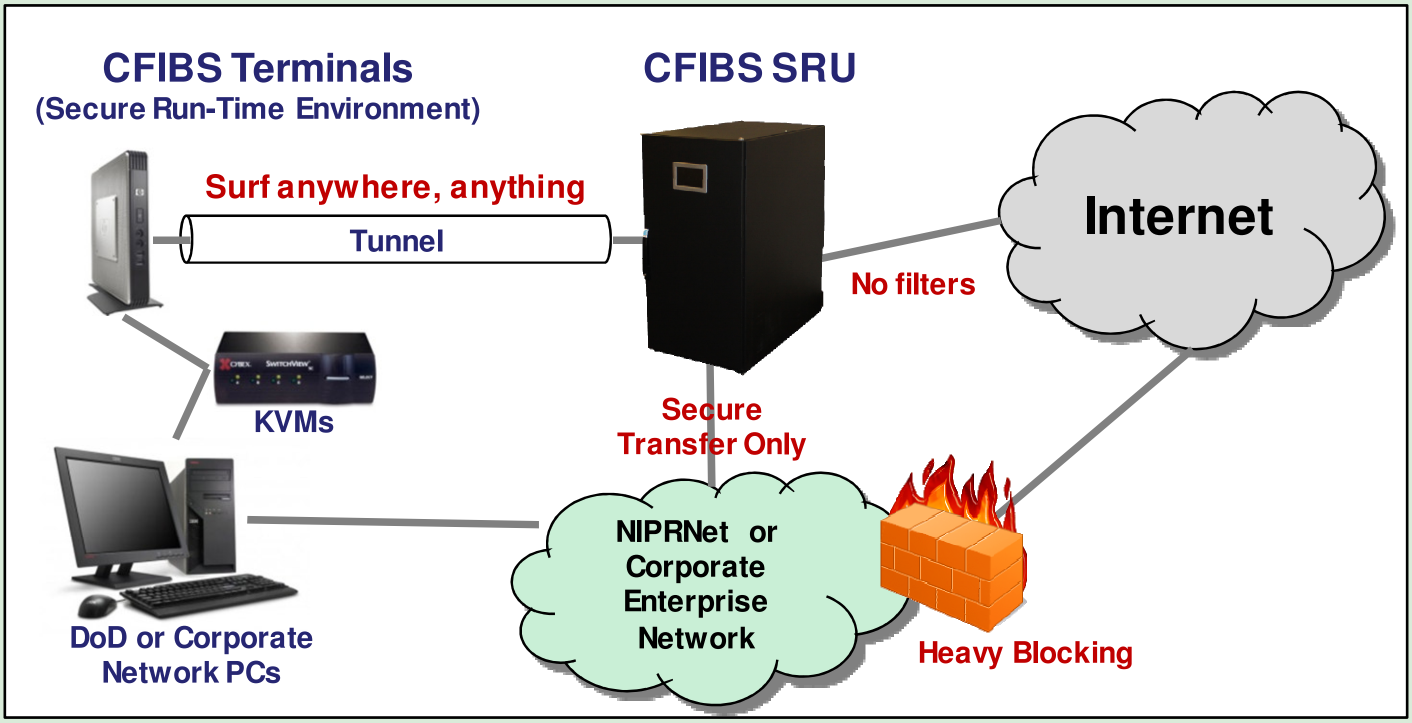
A common but very risky alternative is a standalone PC with a commercial ISP connection. Why risky? The PC is still malware-susceptible; each system is unique and difficult to support; each connection requires a GIG Waiver; malware is easily transferred even by CD; bots can still exfiltrate data; and there is little accountability / attribution of data transfers.

Safe, Unfettered Internet Browsing Solution

The Cross Fabric Internet Browsing System (CFIBS) provides unlimited safe Internet browsing and controlled file transfers within a corporate or government network. CFIBS protects networks from the Internet. View any video or malware site. Social network and cloud compute safely without restriction. CFIBS technically prevents both remote and insider exploitation.

Separation of data and simplification of tasks are key to security. CFIBS strictly holds activity in the public Demilitarized Zone (DMZ) between the public Internet and your private, restricted network (e.g. DoD's NIPRNet). Attackers cannot get a foothold on CFIBS much less access the network. CFIBS does not depend upon updated browsers or anti-virus scanners. Protection is provided by hardware. CFIBS tightly controls transfer of filtered and cleaned data with the primary network. A human user on the primary network must 'pull' all transfers. As shown above, CFIBS separates and then tightly controls various user actions related to browsing and moving files.

Software Protection Initiative. A DDR&E program managed by AFRL/RYT protecting DoD intellectual property in the cyber domain. Learn more at **spi.dod.mil.**



A Unique Solution

CFIBS was designed per ATSPI's novel 3 Tenets security methodology to mitigate vulnerability. All Internet content and activity stays in the DMZ on a unique combination of COTS, GOTS, and custom hardware/software contained within just two components. A Terminal sits adjacent to a user's PC and shares its keyboard and monitor via a KVM switch. Users switch to the Terminal to freely surf the Internet and nominate files for transfer. Terminals provide safe access to <u>any</u> public web site and viewing of <u>any</u> content. The System Resource Unit (SRU) rack handles data transfers between public and private networks yet offers no direct connections. Remote attackers cannot exploit CFIBS to gain unauthorized access to the primary network. CFIBS imposes robust attribution of all activity.

Type Accredited, MAC III, Public

CFIBS is a DIACAP Type Accredited, Mission Assurance Category III (routine), Confidentiality Level: Public system designed for any enterprise network environment. (AF accredited.) CFIBS does not contain or process any sensitive data. CFIBS is built, configured, and documented for each host site's particular network, users, and mission needs. Content cleaning schemes are customized for each host site's data transfer requirements.

CFIBS' Tough Components

In CFIBS, multiple, anti-tamper, thin-client Terminals run an immutable, burned-in-silicon, run-time environment (no operating system, no shells) hosting only a Firefox browser and select add-ons. Even if the browser were cracked, an attacker cannot reach the Terminal much less the network. CFIBS uses physical separation, not virtualization. Terminals connect to the SRU via existing infrastructure. Located in the data center, the SRU breaks the command-control loop with many layers and unique protection technologies. The SRU (a half rack) has dedicated input and output communication channels and intermediate repositories. Pre-determined content types are transferred only after 1.) user nomination (push), 2.) multiple cleanings and filtering, and 3.) multi-factor authentication plus Captcha approval from the primary network (pull). CFIBS may transfer files via email or shared drives. All Internet traffic and file transfer activity is recorded and fully auditable in multiple locations to reveal misuse. Additional design, security, and accreditation details available upon request.

Available Now

To learn how CFIBS can greatly increase both your Internet access and enterprise network security, contact the Software Protection Initiative.

Software Protection Initiative

The Software Protection Initiative (SPI) protects critical DoD intellectual property against nation-state class threats by taking an alternative approach to security based on the 3 Tenets - 1) Focus on What's Critical, 2) Move it Out-of-Band, and 3) Detect, React, Adapt. SPI researches, designs, develops, tests, and deploys protections to prevent piracy, tampering, and reverse engineering of critical software code and data. SPI builds cost effective, adoptable, strong defenses from today's commercial components. The Air Force Research Laboratory's ATSPI Technology Office manages SPI for the DDR&E via the High Performance Computing and Modernization Program.

Software Protection Initiative
AFRL/RYT, Wright-Patterson AFB
ATSPI_outreach@wpafb.af.mil
(937) 320-9095 x150

spi.dod.mil

Approved for Public Release: 3 March 2010, 88 ABW-10-0952