Commercial Solutions for Classified (CSfC) Threat Prevention

Commercial Off-the-Shelf (COTS) products are essential and ubiquitous across National Security Systems (NSS) CSfC networks. The CSfC Program develops Capability Packages in order to provide customers with ready access to the information needed to use COTS in their daily operations and protect their data against today's threats that aim to exploit NSS networks.

Capability Packages (CP)

The NSA's CSfC Program Management Office (PMO) leads Customers, National Information Assurance Partnership (NIAP), Trusted Integrators, Vendors, Independent Laboratories, and internal entities to create, maintain, and improve CSfC CPs.

Customers create systems by following the product-agnostic guidelines in the CPs and selecting products from the CSfC Approved Products List. Customers can create systems that are afforded threat protection through the Top Secret level.

This Threat Prevention Paper is based on the high-level CP designs, and makes no assumptions regarding the use of specific products for the defined components. For a deeper understanding of the threats to each design, please contact the NSA's Client Contact Center via your Client Advocate.

Passive Threats

Passive Threats refer to attempting to gain information from the network without changing the state of the system. Passive Threat actions include collecting or monitoring traffic (e.g., traffic analysis or sniffing the network) passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting Data in Transit (DiT) across Public Black networks is provided by the layered encryption of two independent tunnels (Inner and Outer) using a specific selection of security protocols as instructed in each CP. The two independent Encryption Components provide confidentiality and high-level assurance for the solution, because the adversary should never be able to exploit a single cryptographic implementation to compromise both tunnels.

Two layers of Data at Rest (DAR) Commercial National Security Algorithm (CNSA) encryption are employed to provide confidentiality and mitigate passive attacks of stored data. The DAR components are independent in a number of ways to mitigate the ability of an adversary to exploit a single cryptographic implementation to compromise both layers.

Users with End User Devices (EUDs) that access classified information outside of a secure physical environment open the possibility that an adversary in the immediate environment could use surveillance techniques to obtain classified information. The user agreement must provide methods of usage and storage to mitigate this threat.

Active Threats

Active Threats refer to cyber adversaries gaining unauthorized access and conducting actions that threaten the system or network. Threat actions include: inserting viruses, malware, or worms with the intention to compromise the network; exfiltration of data; degradation of the availability of the system or network; or analyzation of the design of the network or system for future attacks.

Additional threats to CSfC Solutions include: Denial of Service (DoS); Distributed DoS (DDoS); traffic injection attacks; replay attacks; social engineering attacks to assist adversaries with gaining additional access to and compromising information systems; and brute force attacks.

One requirement for preventing unauthorized access is having both encryption layers apply a form of user authentication. This ensures that the data residing on the EUD will still be protected with one layer of encryption if an adversary is able to access the other layer in the solution. Users must also adhere to the password policy established by the Authorizing Official (AO).

Insider Threats

Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track. This threat includes employees or escorted personnel who have the means and desire to gain elevated privileges on the network and who may be poorly trained, curious, disgruntled, or dishonest.

Threat actions include insertion or omission of data entries that result in loss of data integrity; willingly changing the configuration of an EUD; unwillingly or unknowingly introducing malware; cross-contaminating an EUD with data from a higher classification to a lower classification (e.g., secret data to unclassified device); or malicious or unintentional exfiltration of classified data.

To mitigate insider threats, logging and auditing of security critical functionality is required. Intrusion Detection Systems (IDS) can help identify unusual or suspicious traffic that could result from a failure, misconfiguration, or attack on solution components. Additionally, outbound filters are configured to block traffic leaving the internal network that does not go through the Encryption tunnels.

Finally, strong authentications of the Security Administrator, Auditor, and EUD user are required to ensure accountability of these individuals. Additionally, organizations concerned about users misbehaving when connected remotely may wish to restrict the use of EUDs to those deemed sufficiently trustworthy.

Supply Chain Threats

The Supply Chain Threat refers to an adversary gaining access to a vendor, retailer, reseller, or shipper and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a customer in an effort to gain information or cause operational issues.

Such adversary actions include inserting faulty or counterfeit parts or components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow adversaries easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of data. This threat also includes the installation of malicious software on components of the solution.

Since vendors build products containing components manufactured by subcontractors, it is often difficult to determine where different pieces of components are built and installed within the supply chain. It is imperative that every AO perform due diligence and that all organizations use the guidance available in the "Supply Chain Threat" section of the NSA CSfC website.

Integrator Threats

Integrator Threats refer to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. Actions of integrators with nefarious motives may not be detectable through normal tests, scans, and security countermeasures. This is why the CSfC PMO recommends selecting a Trusted Integrator (TI) for this process.

To mitigate the threat, TI's are required to be cleared to the highest level of data protected by the solution(s). A customer may wish to use multiple integrators, such that no one integrator has access to all elements of the solution.

The NSA's list of TIs can be found on the NSA CSfC Website on the "Trusted Integrator List" page.

Preventive Measures

If the CSfC PMO finds a security problem in an approved solution, we will promptly issue new or revised guidance as necessary to resolve the identified deficiencies. Customers must implement resolutions as soon as they receive this guidance and report their actions to the CSfC PMO over SIPRNet.

Customers who have concerns or questions about any threat described in this document or a possible threat that is not covered here can contact the CSfC PMO over SIPRNet. To report a concern over the phone, please call the Information Assurance Capabilities Officer (IACO) at the National Security Operations Center (NSOC).

For all other generic questions that remain unclassified, send those remarks to the CSfC PMO's unclassified mailbox.

Contact Information

For Classified threat inquiries:

✉ CSfC@nsa.smil.mil
☎ IACO at (301) 688-3495

For general CSfC inquiries:

✉ CSfC@nsa.gov

To obtain a Classified Risk Assessment for each CP:
Please contact your NSA Client Advocate or visit the SIPRnet CSfC site for information.