Electronic Design

By CHRIS KRUELL, Director of Marketing, DIGISTOR,
a CRU Data Systems company, https://digistor.com

Air-Gapped Networks (Part 1): Air-Gapped Madness

It's not enough to have an air-gapped network—that network must be located in a secure facility, too.

There's an old saying along the lines of: "If more than one person knows something, it's no longer a secret." This point of view was certainly promoted by the Dutch linguist and cryptographer Auguste Kerckhoffs, who is best known today for two essays he published in 1883 in *le Journal des Sciences Militaires* (*Journal of Military Science*) entitled *La Cryptographie Militaire* (*Military Cryptography*).

The problem arises when multiple people must work together on tasks where they share information while keeping the shared information secure from others. Everything is exacerbated in today's digital era, where information is created, processed, and stored on humongous computer networks that potentially involve thousands of clients (end-user computers), servers, and storage devices.

One part of the solution involves using an "air-gap network" (also "air-wall network") or "disconnected network." This refers to a secure computer network that's physically isolated ("air gapped") from any unsecured networks, such as an unsecured local area network (LAN) or the public internet.

Confidential, Secret, Top Secret, and Sensitive Compartmented Information

For the purposes of the U.S. Government, information may be classified as Confidential, Secret, or Top Secret (TS).

Confidential information is information or material of which unauthorized disclosure could reasonably be expected to cause **damage** to the national security. Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **serious damage** to the national security. Top Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to the national security.

The term Sensitive Compartmented Information (SCI) refers to classified information concerning or derived from sensitive intelligence sources, methods, or analytical processes. SCI isn't a classification, per se. Although SCI clearance has sometimes been called "above Top Secret," information at any classification level may exist within an SCI control system.

SCIFs and SAPFs

Having a secure, air-gapped network is one thing, but limiting access to only people with appropriate "need to know" credentials and security clearances is another. The solution is to implement the network inside a secure facility in the form of a Sensitive Compartmented Information Facility (SCIF) or a Special Access Program Facility (SAPF).

A SCIF is a high-security facility designed to secure information and communications. SCIFs come in various shapes and sizes, including portable units designed to be shipped to any part of the world.

For the purposes of these discussions, however, we will consider only SCIFs that are enclosed areas located inside a larger building or facility, or SCIFs that are buildings in their own right. These types of SCIFs are physically hardened constructions with steel frames, steel cages, multiple layers of drywall, soundproofing, and radio-frequency (RF) blocking. Entry to an SCIF is via a steel door with special hinges and locking mechanisms reminiscent of a bank vault. In fact, these facilities are more secure than bank vaults!

Meanwhile, a SAPF is a U.S. Department of Defense (DoD)-specific "SCIF-Plus" facility used to store, process, and analyze intelligence information associated with Special Access Programs (SAPs). Ranging from so-called "Black Projects" to routine but especially sensitive operations, SAPs

involve security protocols that provide highly classified information with safeguards and access restrictions exceeding those for regular (collateral) classified information. As part of this, only one or a limited number of SAPs will be associated with each SAPF.

SCIFs and SAPFs can both be used to process and store Classified, Secret, TS, and SCI materials, However, only SAPFs can be used for SAP materials and materials designated as Handle via Special Access Channels Only (HVSACO).

Almost every federal government agency will have its own SCIFs and/or SAPFs. These can be located at facilities such as the Environmental Protection Agency (EPA), the Department of Homeland Security (DHS), military bases, and the Pentagon.

Many of the programs that employ SCIFs and SAPFs are not publicly acknowledged. (While this article is focusing on SCIFs and SAPFs, the most commonly deployed method to protect classified information is known as a collateral vault.) A few examples of programs that are publicly acknowledged include:

- GE F-35 Replacement Engine
- Northrop Grumman B-21
- DARPA's HAWC (Hypersonic Air-breathing Weapon Concept)
- Lockheed Martin's Next Generation Interceptor

Who are All of the Players?

If you happen to find yourself working with sensitive information in a SCIF or a SAPF, then you will quickly discover that many people have security-related roles. Below is a brief introduction to these roles.

Let's start with the Special Security Office (SSO), which is a function within multiple arms of the U.S. federal government and armed forces. Its mission is to provide a reliable and secure means to receive and disseminate SCI and SAP to authorized recipients in the U.S. government and military organizations.

Per facility:

- Each SCIF and SAPF will have a Special Security Officer (SSO) assigned to it.
- Each SCIF will have a Special Security Representative (SSR) who reports to the SSO in charge of the facility.
- Each government SAPF will have a Program Security Officer (PSO), contractor SAPFs will have a Contractor Program Security Officer (CPSO), some facilities will have a Program Security Representative (PSR). In each case, they will report to the SSO in charge of the facility.

Per network (there may be multiple air-gapped networks in a facility):

- Each network inside a SCIF and SAPF will have an AO (Authorizing Official), a DAO (Delegated AO), or an AODR (AO Delegated Representative). These are the people who have approval authority on the creation of, and any changes to, the network.
- Each network has an ISSM (Information System Security Manager) who is responsible for the security of the network, the users, the IT (Information Technology) administrators, and the IS (Information Security) staff.
- Each network will have a SCA (Security Control Assessor), sometimes known as a SCAR (SCA Representative) who helps the AO review the ISSM's work and the structure of the network.
- Each network has ISSOs (Information System Security Officers) who audit the network and report to the ISSM.
- Each network has ISSE (Information System Security Engineers) who modify security settings with the IT administrators and report to ISSM. These are the people responsible for implementing zero-trust tools and architecture (e.g., Splunk, Sentinel One, Nessus).
- Each network has privileged users and general users. Privileged Users are typically IT staff and DTAs (Data Transfer Agents). General users are the end-users.
- Each network has an ISO (Information System Owner). This is usually the Commander of the unit or head of the organization. The ISO is subject to the standard operating procedures put in place by the ISSM and SSR or PSO associated with their network and facility.

Ingress and Egress

There are, of course, strict rules as to who and what is allowed to go into and come out of a SCIF or a SAPF. Personnel must employ individual multifactor authentication (MFA) to enter the facility, and they will be obliged to leave all bags, cameras, phones, and any other electronic equipment (e.g., USB data sticks outside). Any electronic equipment will be stored in RF-blocked lockers. (Since lack of a signal can cause cell-phone batteries to quickly drain, these lockers may be equipped with charging facilities.)

Even IT personnel must follow strict rules with respect to bringing hardware and software into a SCIF or SAPF. As one example of a problem that can arise with hardware, consider what happened to the Taiwan Semiconductor Manufacturing Company (TSMC).

TSMC's fabrication plants are completely isolated from the internet and connected only to each other. Standard operating procedure is for any new equipment to be scanned for viruses by the IT department before being connected to the plant's intranet. Unfortunately, in 2018 a junior operator connected a new piece of equipment before it had been cleansed. The machine was infected by the WannaCry ransomware cryptoworm, which quickly spread throughout the network, eventually costing TSMC weeks of time and $200 million.

And an example of a problem that can arise with software, consider what happened to Danish shipping giant A.P. Moller-Maersk, which controls almost 20% of the world's shipping capacity. In 2017, a finance executive for Maersk's Ukraine operation asked his IT administrators to install an accounting package he had acquired. This infected package bypassed the company's cybersecurity defenses and—within a matter of hours—Maersk's worldwide operations were shut down. Once again, it took the company weeks of time and $200 million to recover from the attack.

All of this means that, in the case of SCIFs and SAPFs, it's not possible to use off-the-shelf commercial software. One solution is for the organizations to create their own software. However, this simply isn't realistic in the case of high-end applications that may have taken commercial companies the equivalent of hundreds or thousands of human-years to create.

The problem is that many of these applications make use of "trusted" industry-standard libraries. These libraries have so many levels that no one really knows what may lurk in the lower levels. The solution is for the SCIFs and SAPFs to establish teams at the software companies, where these teams sanitize the software, removing third-party libraries and replacing them with custom-created equivalents (I'm making this sound much easier than it really is).

Although there are trash cans in SCIFs and SAPFs, these are not to be used for paper. Instead, special cross/cut shredders are used to convert any wastepaper into—what is essentially—dust.

Similarly, in the case of a hard-disk drive (HDD) or solid-state drive (SSD) that needs to be replaced for some reason, it's not sufficient to simply "wipe" the drives by overwriting them with random data or (in the case of HDDs) subjecting them to an intense magnetic field.

Instead, the drive must be physically destroyed by shredding it into small particles, where this process must be observed by two witnesses holding special security clearances. Furthermore, a signed certificate must be issued confirming that the drive was indeed destroyed. In the case of a SAPF, this same process also must be used for any computers or other equipment that needs to be retired for any reason.

What Happens Next?

To be honest, we've only scratched the surface of the multiple aspects associated with maintaining security in SCIFs and SAPFs. But there's an elephant in the room and a fly in the soup, which is what happens when there's a legitimate reason to transfer information into or out of one of these facilities.

For example, let's suppose that the people working in a SCIF located at a defense contractor have designed a next-generation fighter aircraft. How can this design data be securely transferred out of the SCIF and transported to where it needs to go? This will be the topic of my next article in this 4-part series on air-gapped networks.

Chris Kruell joined DIGISTOR, a CRU Data Systems company, in 2012. Since then, his leadership in product marketing has driven the company's e-commerce to 10% of the company's overall revenue. As director of marketing, he develops and manages the corporate brand and go-to-market strategy for three major product lines across multiple industries and channels.