SCIFs - State of the Art and Future Considerations

diyscif

2021-01-01

Abstract

This paper will examine the different constructive and technical measures employed by governmental, non-governmental, and corporate actors to protect their secret communications in the physical realm. It will define the target ideal state of “information security”, identify information sources that must be controlled to reach this state, set up quantitative limits on these information sources discoverable externally, provide example attack techniques, and propose various passive and active countermeasures to reach these limits and defend against these attacks. Finally it will present an example module that achieves these specifications measurably.

Note, this paper is limited in scope to constructive and technical measures and does not focus on IT or organisational security measures, like encryption, security-related review/monitoring of employees, and classification levels. It also does not dwell on specific countries bureaucratic protocols, but instead aims to present a unified picture of the global state of the art.

Contents

1 What is a SCIF?

Sensitive compartmented information facility (SCIF) is a term used by U.S. military and intelligence organizations to describe secure, enclosed areas designated for handling sensitive, classified information. They come in many different shapes and sizes, each designed for a specific mission demand. They can be installed permanently in buildings, designed as mobile units, set up temporarily, and even built aboard aircraft and naval vessels. What unites these different variants is the common goal of creating a designated space with rigorous security practices that thwarts all plausible passive outside observers and active attackers.

SCIFs are by no means exclusive to U.S. government instituations. They are used internationally by a wide variety of actors, from other governments to international organization to corporations and NGOs. The term is simply the most common and will be used in this paper to refer to all structures specifically built to achieve the above aim.

Most countries classify their specifications for these secure facilities. The United States, in contrast, have published comprehensive information on their engineering practices under Intelligence Community Directive (ICD) 705 “Sensitive Compartmeneted Information Facilities” and its associated technical specifications. This information can be supplemented by private contractors’ informational material, documents released under the Freedom of Information Act (FOIA), leaked documents, and scientific literature.

The U.S. national security community has over time developed its own jargon that is difficult to understand in the context of a more unified, global perspective. Therefore, this paper will strive to use more neutral, publisher agonstic terms for general concepts. Consequently, what is referred to in the ICD as the “protection of Sensitive Compartmented Information (SCI)” (Office of the National Counterintelligence Executive 2012) can be more generally subsumed under the term information security.

2 Information Security - Ideal State

A communication link or room is considered secure if information travelling through it cannot be intercepted by unauthorized parties. This is a theoretical ideal state that *cannot* be reached. However, one can employ various countermeasures to secure a communication link or room to such a degree that it can be practically considered as secure against an attacker with certain resources.

Both we and our attackers are constrained by limited resources. Viewing attack techniques from a resource perspective allows us to determine whether they are reasonable, given the threat level, and if countermeasures must be deployed against them. Resources are best expressed in terms of cost, time, and technical skill required. Taking into account these parameters, we are then able to develop a mission-specific threat model that allows us to employ our *limited* resources effectively to defend against the most likely and serious attacks.

The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, p. 20) does this by using country-level threat ratings derived from the Department of State’s (DoS) Security Environment Threat List (SETL). The ICD establishes appropriate construction criteria based on the host country’s technical threat rating. Other possible criteria from which to derive a threat level include value of information handled and named/identified threats.

It is highly unlikely that an attacker will expend more resources to carry out an attack than the objective value of the attainable information.

3 Information Source Leaks

There are various information sources that can leak from the secure facility and be intercepted. These can generally be grouped into visual, acoustic, and electromagnetic informaiton source leaks. A passive observer can use different sensors to capture and analyze these leaks.

3.1 Visual

Visual leaks are any direct view of sensitive information, captured by the outside passive observer on camera, or surface whose reverberations can be captured with a laser and then translated into usable information. For example, when speaking, glass panes or mirrors in a room are set into vibration. When there is visual insight into the room (e.g. from the neighboring building), a laser beam can be directed onto these reflecting surfaces and the reflected beam can be received again. The reflected beam is modulated by the oscillations. By demodulation, the conversation can be made audible. (Wolfsperger 2008, p. 463)

Barring holes in the SCIF perimeter, like propped-open doors, visual leaks can only be captured through windows.

3.2 Acoustic

Acoustic leaks are sound waves that escape the enclosed areas, either directly or through structure-borne sound transmission. These can be captured with directional microphones, contact microphones, and well placed conventional microphones. An example of such an advantageous placement would be in an unmuffled ventilation or heating duct. Digital sound processing software can further be used to reconstruct, clarify, and analyze sound recordings.

3.3 Electromagnetic/TEMPEST

Compromising electromagnetic waves unintentionally emitted from information processing equipment, like computers, screens, and even printers are another source for information leaks. These radio or electrical signals, sounds, and vibrations can be captured with antennas, microphones, and other sensors, and allow inferences to be made about the information processed, sometimes even allowing its complete reconstruction (Liu, Samwel, Weissbart, Zhao, Lauret, Batina, Larson 2020). They can also serve as a side-channel for attacks on cryptography (Genkin, Pachmanov, Pipman, Tromer 2015). The techniques for extraction and analysis of compromising electromagnetic emanations fall under the commonly used U.S. National Security Agency codename TEMPEST (U.S. National Security Agency 1972).

4 Limits

This section will set quantitative limits on information sources available to an outside passive observer.

4.1 Visual

No visual information should be accessible to an outside passive observer. Visual information source leaks are the easiest to avoid and should therefore be wholly prevented. Even observation of the entrypoint could provide insights into the comings and goings of authorized personnel and should therefore be obscured as much as possible.

4.2 Acoustic

4.3 Electromagnetic/TEMPEST

5 Attacks

Apart from passively observing information source leaks from outside the secure facility, an attacker can also actively attack the space to place sensors inside it and transmit sensitive information to the outside.

5.1 Visual

5.2 Acoustic

5.3 Electromagnetic/TEMPEST

6 Countermeasures

6.1 Physical

6.1.1 Construction Security

Later passive and active countermeasures are completely ineffective if the SCIF is breached during construction. Therefore meticulous preparation of and adherence to a Construction Security Plan is required.

6.1.2 Intrusion Resistance

6.1.3 Intrusion Detection Systems

6.1.4 Access Control

6.1.5 Locks

6.1.6 CCTV

6.2 Visual

6.3 Acoustic

6.3.1 Sound Attenuation

6.3.2 Sound Masking

6.3.3 Microphone Jamming

6.4 Electromagnetic/TEMPEST

6.4.1 Electromagnetic Shielding

6.4.2 System Monitoring

6.4.3 Signal Jamming

6.5 Bug Sweeping

7 Example Module

This section will propose an example solution for a Sensitive Compartmented Information Facility (SCIF). It will employ the above passive and active countermeasures in a shipping container sized (~ 6 x 2.4 x 2.7 m) module to reach the quantitative limits on information source leaks defined above.

7.1 Physical

7.2 Visual

7.3 Sound

7.4 Electromagnetic/TEMPEST

References

GENKIN, Daniel, PACHMANOV, Lev, PIPMAN, Itamar and TROMER, Eran, 2015. Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation. *Tel Aviv University.* February 2015.

LIU, Zhuoran, SAMWEL, Niels, WEISSBART, Léo, ZHAO, Zhengyu, LAURET, Dirk, BATINA, Lejla and LARSON, Martha, 2020. Screen gleaning: A screen reading tempest attack on mobile devices exploiting an electromagnetic side channel. *Radboud University*. November 2020.

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, 2012. *Technical specifications for construction and management of sensitive compartmented information facilities version 1.2 - ic tech spec-for icd/ics 705*. 2012. https://fas.org/irp/dni/icd/ics-705-ts.pdf.

U.S. NATIONAL SECURITY AGENCY, 1972. *TEMPEST: A signal problem*. 1972. http://www.jproc.ca/crypto/tempest.pdf.

WOLFSPERGER, Hans A., 2008. *Elektromagnetische schirmung: Theorie und praxisbeispiele*. Berlin, Heidelberg: Springer-Verlag.