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

Acoustic emissions must be reduced by at least a weighted sound reduction index of $R'_w = 52$ dB. This measure roughly corresponds to the Sound Transmission Class 50 listed in the IC Tech Spec-for ICD/ICS 705 as an enhanced rating for areas that provide for amplified conversations (Office of the National Counterintelligence Executive 2012, p. 66). We use this as a general minimum measure, because the IC Tech Spec is geared towards military and other government facilties that provide a large measure of security in depth (SID), meaning that only semi-trusted personnel ever get within earshot of the SCIF. Security in Depth is a multilayered approach, which effectively employs human and other physical security measures [like fences, walls, and guarded entry gates] throughout the installation or facility to create a layered defense against potential threats" (NAVFAC Northwest 2012, p. 20). Additionally, SID increases the probability of detection of nefarious activity because of continuous friendly-forces presence (Office of the National Counterintelligence Executive 2012, p. 3). These conditions cannot be guaranteed for all locations, especially in the corporate realm, so we strive to compensate reduced SID with a higher degree of sound insulation. When possible, $R'_w = 52$ dB should be exceeded.

R'_w represents the resulting sound insulation between two rooms, taking into account all sound transmission paths (Tichelmann, Pfau 2000, p. 26). This explicitly includes not only transmission through dividing components, but also so-called “flank transmission” over adjoining building components. In this phenomenon sound waves cause vibrations in flanking walls and then linearly travel through them into the other room (Möser 2009, p. 254). R'_w is a cummulative value calculated on the basis of the weighted sound reduction index of each component R_w (Tichelmann, Pfau 2000, p. 34).

R_w is calculated by measuring sound transmission from one room into the other in one-third octave or octave steps. White noise with the given bandwidth is used as test sound. A frequency response curve R is thus obtained in the so-called building-acoustics frequency range between 100 Hz and 3.15 kHz. The frequency response curve R is then compared to a reference curve B in order to derive a

single comparison value. In the comparison, the reference curve is shifted in 1 dB steps onto the frequency response curve until the sum of the undershoots S_U of the frequency response curve compared to the reference curve is less than 32 dB. (Möser 2009, pp. 256–257)

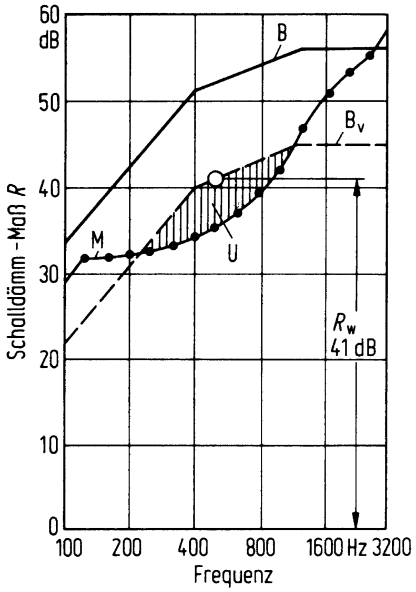

Figure 1: For the definition of the weighted sound reduction index R_w. B = Reference curve, B_v = Shifted reference curve, M = Measured values, U = Undershoots of M compared to B_v. Gösele, Schröder (2004)

From this diagram we can also see that for a $R_w = 52$ dB (the reference curve) the fundamental frequency of the male voice - 125 Hz - only undergoes a sound attenuation of ca. 35 dB. Given a 60 dB conversation sound-level the sound attenuation is not sufficient to protect from a close proximity attacker. Passive sound-attenuation measures should be specifically evaluated in the 125 Hz to 300 Hz range, and significantly exceed the reference curve's performance.

Airborne sound transmission via ventilation and structure-borne sound transmission via ducts, such as water and ventilation pipes, can significantly reduce sound insulation. In some cases they can even provide direct channels for an outside attacker to capture sound on. (Möser 2009, p. 276)

4.3 Electromagnetic/TEMPEST

Electromagnetic emissions should be reduced by the values defined in National Security Specification for Shielded Enclosures NSA 94-106. This specification sets forth an attenuation for 1 kHz - 1 MHz H (magnetic) Field of 20 dB @

1KHz, 56 dB @ 10 kHz 90 dB @ 100 kHz, and 100 dB @ 1 MHz. For 1 kHz - 10 MHz E (electromagnetic) Field it requires 70 dB @ 1kHz, and 100 dB at 10 kHz, 100 kHz, 1 MHz, and 10 MHz. For a 100 MHz - 10 GHz Plane Wave it also requires 100 dB attenuation.

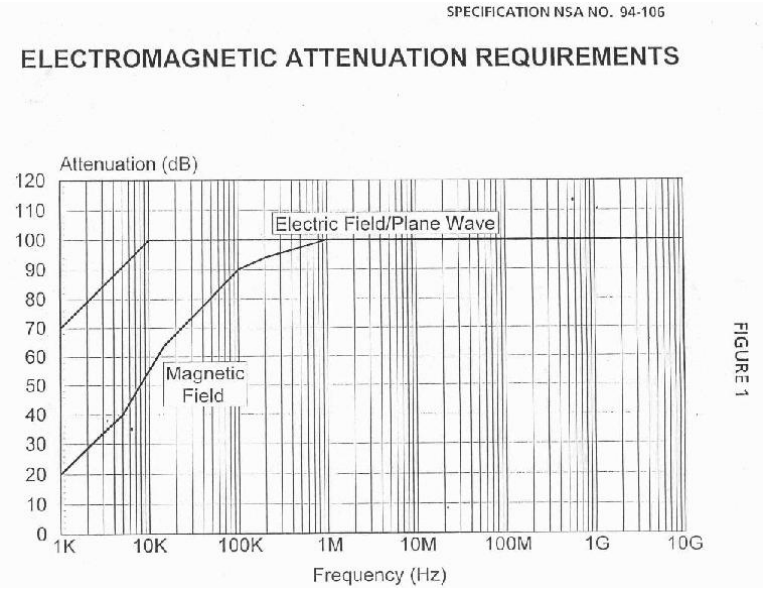

Figure 2: Electromagnetic Attenuation Requirements. U.S. National Security Agency (1994)

The field test is carried out with a parallel setup. A continuous wave source generates a wave in the range of 1 KHz to 10 GHz. Two antennas are placed, one on either side of the shielding. One antenna acts as a transmitting (TX) antenna and the other as a receiving (RX) antennas. The antennas are separated by a distance of 61 centimeters plus the wall thickness. The signal from the RX antenna is fed back into a reciver. Attenuation levels can then be read from a spectrum analyzer. Magnetic field, electronic field, and plane wave attenuations are then measured at various specified frequencies. Attenuation tests are performed around the entire door frame, air ducts, filters and through any accessible joint or penetration. (U.S. National Security Agency 1994)

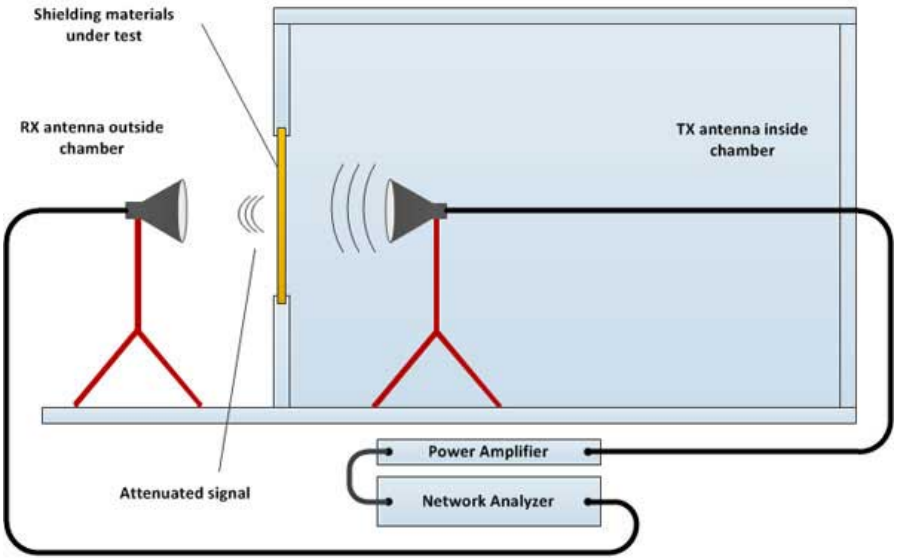

Figure 3: Test setup for NSA-94-106. EMCTEST Technologies (2018)

No comprising emanations should exit the SCIF on power lines and data connections.

5 Attacks

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

5.1 Visual

The goal of all visual attacks is to place cameras inside the SCIF. These cameras allow an attacker to gain valuable insights into the sensitive information being handled or processed inside the enclosed area. Cameras can be inserted by someone who gains physical access to the space, inserted through HVAC ducts, or drilled through the perimeter.

Another attack avenue is taking over installed CCTV cameras. The video feed from these cameras could allow insights into the SCIF's comings and goings, and, with badly placed cameras, even into the information processed. This attack can also target the built-in cameras of information processing equiptment like laptops.

Cameras transmit video feeds to the outside using radio/electromagnetic waves or wired connections. Wired connections could be specially installed for the attack or hijack existing lines, either directly or as emanations along unshielded lines.

5.2 Acoustic

An attacker may also attempt to place a microphones within the SCIF. To do this he can either physically insert a new microphone or hijack one of the built-in microphones of devices already included in the room. Acoustic information is usually most sensitive, especially in conference rooms or discussion areas.

Avenues for placing a microphone are again physical entry, HVAC ducts, and hole drilling. In order to exfiltrate information the attacker again utilizes either radio/electromagnetic waves or wired connections, existing or specially placed. Another attack would be finding a weak spot in the sound attenuating shell and placing a microphone directly on it.

An attacker could also seek to weaken the sound attenuation measures by tampering with the sound masking, destroying insulation or purposely creating sound bridges.

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

EMCTEST TECHNOLOGIES, 2018. *NSA 94-106 Effectiveness Testing RF Shielded Enclosures*. 2018. https://www.shieldingtests.com/?standard=NSA-94-106.

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.

GÖSELE, K. and SCHRÖDER, E., 2004. Schalldämmung in Gebäuden. In: *Taschenbuch der Technischen Akustik*. Berlin, Heidelberg: Springer-Verlag.

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.

MÖSER, Michael, 2009. *Technische Akustik*. Berlin, Heidelberg: Springer-Verlag.

NAVFAC NORTHWEST, 2012. *Physical Security of Sensitive Compartmented Information Facilities (SCIF)*. November 2012. https://www.washingtonpost.com/news/politics/wp-content/uploads/sites/11/2017/02/navfac_scif_ho.pdf.

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.

TICHELMANN, Karsten and PFAU, Jochen, 2000. *Entwicklungswandel Wohnungsbau: Neue Gebäudekonzepte in Trocken- und Leichtbauweise*. Wiesbaden: Vieweg+Teubner Verlag.

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

U.S. NATIONAL SECURITY AGENCY, 1994. *NSA 94-106 National Security Agency Specification for Shielded Enclosures*. 1994. http://cryptome.info/0001/nsa-94-106.htm.

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