SCIF Research Working Title

diyscif

2021-01-01

Abstract

This paper will examine the different constructive 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, and propose various passive and active countermeasures to reach these limits. Finally it will present an example module that reaches these specifications measurably.

Note, this paper is limited in scope to constructive 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 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.

2 Information Sources

There are various information sources that can leak from the secure facility and be intercepted. These include

- Visual
- Acoustic
- TEMPEST

For each practical usecase only a subset of these information sources must be isolated.

3 Limits

Set limits on information sources that should be available to an outside observer.

4 Information Leak Countermeasures

4.1 Passive Countermeasures

Passive countermeasures are preventive and use physical construction to secure an area against intrusion and information source leaks.

4.2 Active Countermeasures

Active countermeasures use interference to obscure and render useless information source leaks.

5 Physical Security

5.1 Intrusion Resistance

5.2 IDS

5.3 Access Control

5.4 Locks

6 During Construction

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.

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 (~ 12 x 2.5 x 2.5 m) module to reach the quantitative limits on information source leaks defined above.