Physical Considerations for Designing Secure Networks

Senior Lecturer Răzvan Daniel ZOTA, Ph.D.
E-mail: zota@ase.ro

During the past ten years or so networks' vulnerabilities has increased continuously; the need for designing more and more secure networks it is a must in the present. One common security truism is that if you have physical access to a box, „all bets are off". If an attacker has physical access to any networking device, like a computer, switch, router, firewall and so on, the security options are considerably reduced. The purpose of this article is to present design considerations for secure networks at the physical level.
Keywords: *Networking, Security, Security design, Physical Access, Distributed systems, Network security.*

1 Introduction

It is well known that if an attacker gain physical access to a networking device, this fact may compromise dramatically the security options. Networking devices, with few exceptions, can have their passwords reset by attaching to their console port. Hosts can be booted with a special floppy disk or CD-ROM designed to circumvent most host security on the device. The article do not cover physical security in detail and topics like site selection or disaster recovery are not discussed. A network designer, however, must know where to rely on physical security to support overall network security. There are some general rules to follow in order to successfully manage the network security:

- Physical access control to facilities;
- Control physical access to data centers;
- Separate identity mechanisms for insecure locations;
- Prevent password-recovery mechanisms in insecure locations;
- Electromagnetic radiation;
- Physical PC security threats;
- Cable plant issues.

2. Physical access control to facilities

Effectively controlling physical access to the organization's facilities must be the single top concern for both physical security staff and the network designer. Most organizations utilize one of three mechanisms to implement physical security (presented in increasing order of security):

- Lock-and-key access
- Key card access
- Key card access with turnstile

Lock-and-Key Access

The most common physical security control, particularly in smaller organizations, is traditional lock-and-key access. For this method, individuals who need access to certain rooms or buildings are given keys for access. This option has the following benefits:

- Generally, this is the cheapest option for small organizations.
- No technical experience is required.
- Special keys are available to thwart key duplication.

However, there are also several drawbacks:

- If employees leave the company on less than amicable terms, they might "lose" their keys or might simply stop showing up for work. In such cases, it can be very costly to rekey the locks and redistribute keys to the valid employees.
- Unless coupled with an alarm system that augments the lock-and-key access, there is no mechanism to determine when employees with keys access a given physical location.
- Most keys can be easily duplicated at the local hardware store.
- Key authentication is *single-factor,* meaning the key is all a person needs to access locked areas.

Key Card Access

More common in larger organizations, key card access can alleviate some of the management problems associated with lock-and-

key access and can provide increased security measures. Key card access can take the form of a magnetic card reader or a smart card. All of these systems have the same basic pros and cons once you eliminate the technical differences of the technology. These are the benefits of a key card system:

- Access to multiple locations can be controlled with a single card.
- In the event that an employee leaves the company, the employee's card can be quickly disabled whether or not it is physically returned.
- Locks should never need to be "re-keyed."
- Facilities with multiple entrances are easily supported.
- Reports can be run to show when individuals entered specific locations.

The drawbacks to a key card system are as follows:

- Like lock-and-key access, key cards are single-factor security. Any individual with a valid key card could access the location.
- Key card systems can be expensive, and in the event of a failure in the central authentication system, all users can be denied access to a facility.
- The principal problem with key card access is tailgating. *Tailgating* is gaining unauthorized access to a building by following an individual with valid access. Oftentimes, if attackers are dressed in the appropriate clothing, they can simply follow legitimate individuals into a building without having to present a key card. Even if someone requests to see a card, an attacker can show an invalid card because it might not actually be scanned by the card reader.

Key Card Access with Turnstile

Although most often associated with ballparks and stadiums, turnstile access with a key card can be one of the most secure methods of controlling physical access to a building. For this method, a key card is used to activate the turnstile and allow one person into the building. These systems are most common in large multi-floor buildings, where access can be controlled at the ground floor. In the following list, you can see that this option has all the benefits of the previous option plus more.

- Tailgating is greatly diminished because only one person can enter per card.
- Access to multiple locations can be controlled with a single card.
- In the event that an employee leaves the company, the employee's card can be quickly disabled whether or not it is physically returned.
- Locks should never need to be "re-keyed."
- Reports can be run to show when individuals enter specific locations.

The drawbacks of a system such as this are as follows:

- Like the previous two systems, key card access with turnstile is a single-factor identity system. Any individual with a valid card could gain access to the building.
- This doesn't work well for facilities with multiple buildings and multiple entrances.
- This method generally requires a security guard to verify that individuals are not hopping over the turnstile or tailgating through an entrance designed for persons with physical disabilities that bypasses the turnstile.
- Turnstiles are not aesthetically pleasing.
- Turnstile access can be inconvenient for employees, escorted guests, or individuals using dollies for equipment.
- This method is more expensive than simple key card access and also has the same issues in the event of a failure in the key card authentication system.

Solving the Single-Factor Identity Problem

A second factor can be added to either of the previous key card authentication processes. The first option is to put a personal identification number (PIN) code reader at every location where there is a card reader. After using their key card, employees must enter a PIN to unlock the door. Another option is to use some form of biometric authentication. Biometric authentication could be used as either the second factor in a key card system or the principal factor in a biometric system. In the second case, users would enter a PIN after successful biometric authentication. Both of these alternatives add cost to the system and inconvenience for users.

3. Control Physical Access to Data Centers
Data-center access can utilize any of the preceding mechanisms in addition to PIN-reader-only access. The important difference with data-center access is that you are often dealing with a smaller set of operators, so issues around key management are somewhat reduced. In this context, *data center* refers to any location where centralized network resources are stored. This could include traditional data centers, wiring closets, coat closets, or someone's desk. It all depends on the size of the facility and the way it is organized. Exceptionally secure data centers utilize sets of cameras, key card access, biometrics, and "man-traps" to catch anyone illegally trying to gain access to the room.

4. Separate Identity Mechanisms for Insecure Locations
From the physical security perspective it is important to ensure that passwords in physically insecure locations are not the same as those used in secure locations. Often an organization will utilize common authentication mechanisms for the various systems that must access network resources. For example, SNMP community strings or Telnet / SSH passwords might be set the same on all devices. From a pure security perspective, it is preferable to use two-factor authentication, when available, for each user who accesses the network device.
Although this might be possible for users, it is often impossible for software management systems, which need to run scripts to make changes on several machines at once. For optimal security, different passwords should be used on each device, but this is often operationally impossible for large networks. Therefore, at a minimum, organize your common passwords so that they are never used on systems in physically insecure locations. For example, assume you have 3 main locations (with data centers) to your organization and 10 remote sites (considered insecure). In this case, only use your shared passwords on the main sites and ensure that the passwords for each of the remote systems are unique per site at a minimum and per device ideally.

5. Prevent Password Recovery Mechanisms in Insecure Locations
Some devices have controls to prevent the recovery of passwords in the event that an attacker has physical access to your system. For example, on some newer Cisco routers and switches, we enter the following command:
Router(config)# **no service password-recovery**
When the above command is entered on a router or a switch, interrupting the boot process only allows the user to reset the system to its factory default configuration. Without this command, the attacker could clear the password and have access to the original configuration. This is important because the original configuration might contain common passwords or community strings that would allow the attacker to go after other systems. This would be particularly useful in insecure branch offices or other locations where the physical security of a network device cannot be assured.

6. Electromagnetic Radiation
In 1985, the concerns of the paranoid among the security community were confirmed. Wim van Eck released a paper confirming that a well-resourced attacker can read the output of a cathode-ray tube (CRT) computer monitor by measuring the electromagnetic radiation (EMR) produced by the device. This isn't particularly easy to do, but it is by no means impossible. Wim van Eck's paper can be found here: http://www.shmoo.com/tempest/emr.pdf
This form of attack is now commonly called *van Eck phreaking*. Additionally, in 2002, Markus Kuhn at the University of Cambridge published a similar method of reading data off of a CRT, this time by measuring the changes in the amount of light in a room. Markus Kuhn's paper can be found here: http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf and an easy-to-read FAQ on the topic can be found here: http://www.cl.cam.ac.uk/~mgk25/emsec/opti

cal-faq.html
A simple way to mitigate van Eck phreaking might just be to change the type of font you are using. Ross Anderson and Markus Kuhn did some excellent research on the topic: http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf
Of course it is not recommended that all systems must address these sorts of security considerations, but it is good to know that such attacks are possible.

7. Physical PC Security Threats

Often, inexperienced network designers begin with an unacknowledged assumption that *all* the sensitive data within an organization is contained on servers. In reality, there is sensitive information about the company on the employees' laptops, as well as on the servers. Like most employees at my company, server resources are used when necessary, but often interesting information is stored locally.
Several physical security issues manifest when you operate under the preceding assumption:

- The first is that portable computer theft is a big problem, not just in the cost of replacing the computer but in the proprietary information that is stored on it. The best protection against having a lost portable computer turn into lost trade secrets is some type of file system encryption (some are built into modern operating systems).
- The second is that by compromising the data coming into and out of a PC, you can learn passwords, sensitive data, and so on. An attacker can achieve this through network sniffing, EMR emissions (discussed previously), remote control software (Back Orifice 2000), or novel devices that attach between the keyboard and the PC and record to flash memory every key typed. For more information, one may see this URL: http://www.thinkgeek.com/stuff/gadgets/5a05.shtml

8. Cable Plant Issues

In today's networks, there are two primary cable types: unshielded twisted pair (UTP) category 5 (or higher) and fiber optic. The risk of an attacker accessing your physical cabling is important to consider because that level of access often can bypass other security controls and provide the attacker with easy access to information (provided encryption is not used). UTP cable is very easy to tap, but it was thought years ago that fiber was immune to cable taps. We now know that this is not the case. The National Security Association (NSA) is rumored to have already tapped intercontinental network links by splicing into the cable; one may read about it at the following URL: http://zdnet.com.com/2100-11-529826.html.
It is also theorized that fiber cable could be bent far enough so that some light would escape if the outer layer of the cable is removed. With the right types of equipment, this information could then be read.
Additionally, if an attacker gains physical access to a wiring closet or the fiber cable as it runs in a cable tray above a drop ceiling, tapping the cable by installing couplers is another possibility.
All this being said, fiber is more secure than copper because the means to tap the signal are more expensive, difficult to execute, and often require interrupting the original flow of data to install. On the other hand, the means to tap a UTP signal can easily be purchased off of the Internet.

References:

1. Preston Gralla - *Next-Gen Nets Need Next-Gen Security*, networkingpipeline.bitpipe.com, 12 November 2004
2. Convery Sean – *General Design Considerations for Secure Networks* – Cisco Press, January 2004
3. Tanya Baccam - *Security Assessments: Reducing the Security Risk to Your Enterprise: What Different Types of Security Assessments Provide* – iQ Magazine, 2004
4. *Physical Security - What It's All About* - http://www.infosyssec.org/infosyssec/physical_security.htm
5. Robert L. Boque - *Lock IT Down: Don't overlook physical security on your network*, http://techrepublic.com.com/5100-6329_11-5054057-2.html
6. E.J. McGowan - *Security White Paper* - Intranets.com ABOUT,http://www.infosyssec.org/infosyssec/physical_security.htm