How Hackers Attack Physical Access Control Systems

Cameras

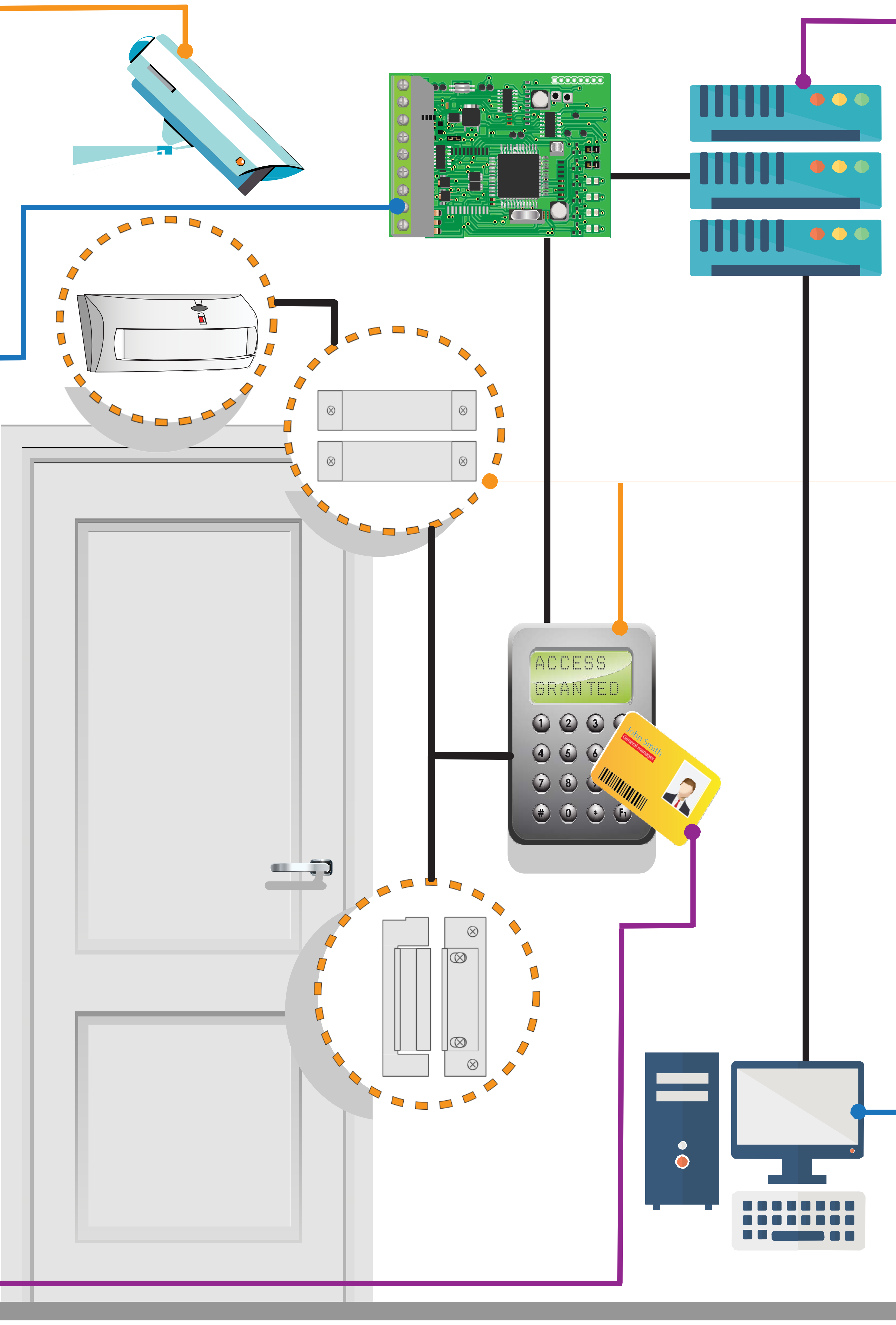
Security cameras can be accessed from the corporate network, and occasionally from the Internet. This gives attackers a 24/7 view of the facility.

Control panels

The control panel decodes credential data received from the access card reader, compares it to an access list, then grants or denies entry. The access list is sent to the control panel from the access software via a network connection. These panels are often easily accessible from the entire corporate network, and have little security features enabled.

Credentials

The most common credential is an access card. Inside the card is a small chip that contains a facility number and identification number. Hackers can obtain this information using a variety of attack methods.



Access Software

The master list of employees, credentials, and access areas is managed by access control software running on a server. If the server is improperly secured, it is possible to highjack the access control software -- allowing attackers to lock and unlock doors on demand.

Door controls

Electronic and physical door controls -- such as access card readers and request to exit devices can be defeated with technical and non-technical tools.

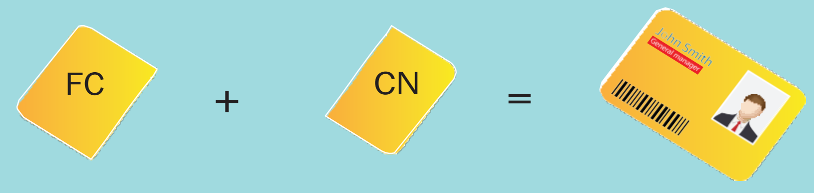
Workstations

Physical security personnel connect to the access control software from a workstation. By gaining access to a workstation, a hacker can also connect to the access control software.

Physical Access Control Systems (PACS) consist of several components working together to ensure that doors and turnstiles unlock when appropriate authentication credentials are presented. Many of these components require computer network access in order to function properly. Once installed and operational, they are often overlooked during cyber security assessments. This common situation leaves the PACS components exposed and mostly unmonitored, creating an ideal environment for an attacker.

Attack Chaining

A common misconception is that hackers obtain their goal with a single attack. After obtaining access to one component, an attacker can utilize information from the compromise to attack other PACS components.



Credential duplication is a significant threat to the integrity of the PACS environment. Most credentials consist of two key pieces of information -- the facility code and credential number. With these two pieces of information, it is possible to create duplicate credentials to gain or elevate access levels.

Next Steps

Securing a PACS implementation requires coordination between physical and cyber personnel. To aid in this process, Securicon has released a PACS Security Checklist designed to provide guidance in hardening the PACS environment from network and computer-based attacks. Scan the QR code to download.

Access control panels are high priority targets due to the useful information they contain. Each panel stores the access list for the areas it regulates, complete with credential numbers. Hackers will compromise panels to gather valid credential numbers and other configuration details.

Valerie Thomas (@hacktress09) is a Executive Information Security Consultant for Securicon LLC that specializes in social engineering and physical penetration testing. Her unique Defense and civilian background provides her with a solid understanding of intrusion detection, data loss prevention, and endpoint security. While some focus on cyber or physical security, she has chosen to exploit the weaknesses of the combination of the two.