Preventing Your Physical Access Control System From Being Used Against You

Valerie Thomas @hacktress09, Executive Consultant, Securicon
• Executive Security Consultant for Securicon
• 15+ years in Information Security
• Coauthor of *Building A Security Awareness Program*
• Social Engineering trainer
• Physical access “enthusiast”
• Why this topic is essential for the ICS/SCADA world
• Topology of a physical access control system (PACS)
• Why PACS deployments are insecure
• Attack surfaces and trending attacks
• Common misconfigurations
• Roadmap to locking down existing implementations
Why This Topic Is Essential For ICS/SCADA

- Many legacy systems are vulnerable to attacks that require local area network, or physical access
- Firewalls and various forms to controls are implemented to reduce the likelihood of a successful attack
- Many cyber defenses can be bypassed with physical access
- Attackers want to gain physical access to attack cyber assets
- The ultimate goal is to obtain access and stay there unnoticed
Whose Responsibility Is It Anyway?
Attack Surfaces and Exploits

- Access cards
- Readers
- Request to exit devices
- Access control panel
  - Cameras
  - Workstations
Access Cards

Low Frequency
- 125kHz
- Small amount of data
- Unencrypted

High Frequency
- 13.56 MHz
- Large amount of data
- Sometimes encrypted

Multi-Frequency
- 13.56 MHz and 125kHz
- Large amount of data
- Partially encrypted
Access control panel

- Decodes binary data
- Compares card data to an access list, then grants or denies entry

(Facility Code) 12 34281 (Card Number)

In Chip (in card):

5031782 297038582818496992981839006

When read by controller against format:

5031782 297038582818496992941839106
Tastic RFID Thief

- LCD Screen
- Any RFID Badge Reader
- Power
- MicroSD Card
- CARDS.txt
- TXT
• Inserted in-line with the reader
• Records card data and sends via Wi-Fi
• Replays data
• Reader Denial of Service
Reader attacks - ESPKey
Most vendors print the card number on the card.

And on the box:

- S/O: 181518
- Job: 174878
- Part Number: 1386LGGMN
- Card Range: 06365 – 06564
- Quantity: 200
- Format: H10301
- Facility Code: 0
Request to exit device attacks
• Many controllers have features to simplify configuration
  • Embedded web servers
  • FTP
  • SNMP
• Access is generally open or protected with a weak default password
• Many allow anonymous FTP
• Metasploit modules available
Access Servers

- Usually not as obvious as controllers
- Majority are Windows Servers
- Can often obtain the IP from a controller
- DNS search is a fairly reliable method
Once Server Access Is Obtained

Grants the attacker the ability to:

• Obtain card numbers for all employees
• Obtain card configuration
• Add card configuration (Maybe)
• **Modify members of access groups to grant or deny entry**
• Release door/turnstile/gate locks temporarily
The New Ransomware?

Attacker

Locates Admin User

Admin Access

Workstation

Attacks Admin User

User Access To Software
ALL YOUR BUILDING ARE BELONG TO US
Camera Access

• Provides attackers with a 24/7 view of the facility
• Zoom feature can be used to view keystrokes, labels, post-it notes
• This also provides the opportunity to take down a video feed if they need to physically access a certain area
• Most cameras are not centrally controlled and have default/weak passwords
• Changing the passwords could create a denial of service to the owner
• Also Metasploit modules available
Once Physical Access Is Obtained
Target The Human
Many of the misconfigurations discussed are preventable

Understanding your system architecture is vital to attack prevention

Lock down access to attack surfaces
  • Internally or with an outside security company

Educate employees on credential protection

Educate your staff on attack vectors
Caution Areas

- Multi-technology access cards
- Multi-technology readers
- Third-party monitored access control or cameras
- Improper network segmentation
- Software misconfigurations
Resources

Free PACS security resources available – contact us!

Valerie.Thomas@Securicon.com
@Hacktress09
@Securiconllc