Let's Get Physical

Network Attacks Against Physical Security Systems

Ricky "HeadlessZeke" Lawshae – Defcon24 – 2016

Intro

Intro

Who am I?

- Security Researcher at TippingPoint
- IoT (drink!) hacking enthusiast
- Occasional conference presenter
- Used to install physical security systems for a living

Intro

Physical Security

- Electronic or mechanical devices used for
  - Access control
  - Surveillance
  - Alarms
- Card readers, door controls, video cameras, DVRs, motion sensors, fire alarms, tamper switches, etc etc etc

Intro

Deployment

- Used by basically every organization of any size
- Piece by piece getting put on the network
  - Acknowledge alarms and watch cameras
  - Push schedule and access changes
  - Pull logs and reports
- Physical is becoming digital...IoT (drink!)

Intro

Embedded devices…

accessible via the network…

protecting valuable assets…

in every organization…

…Should be fine!

Access Control

Access Control

Overview

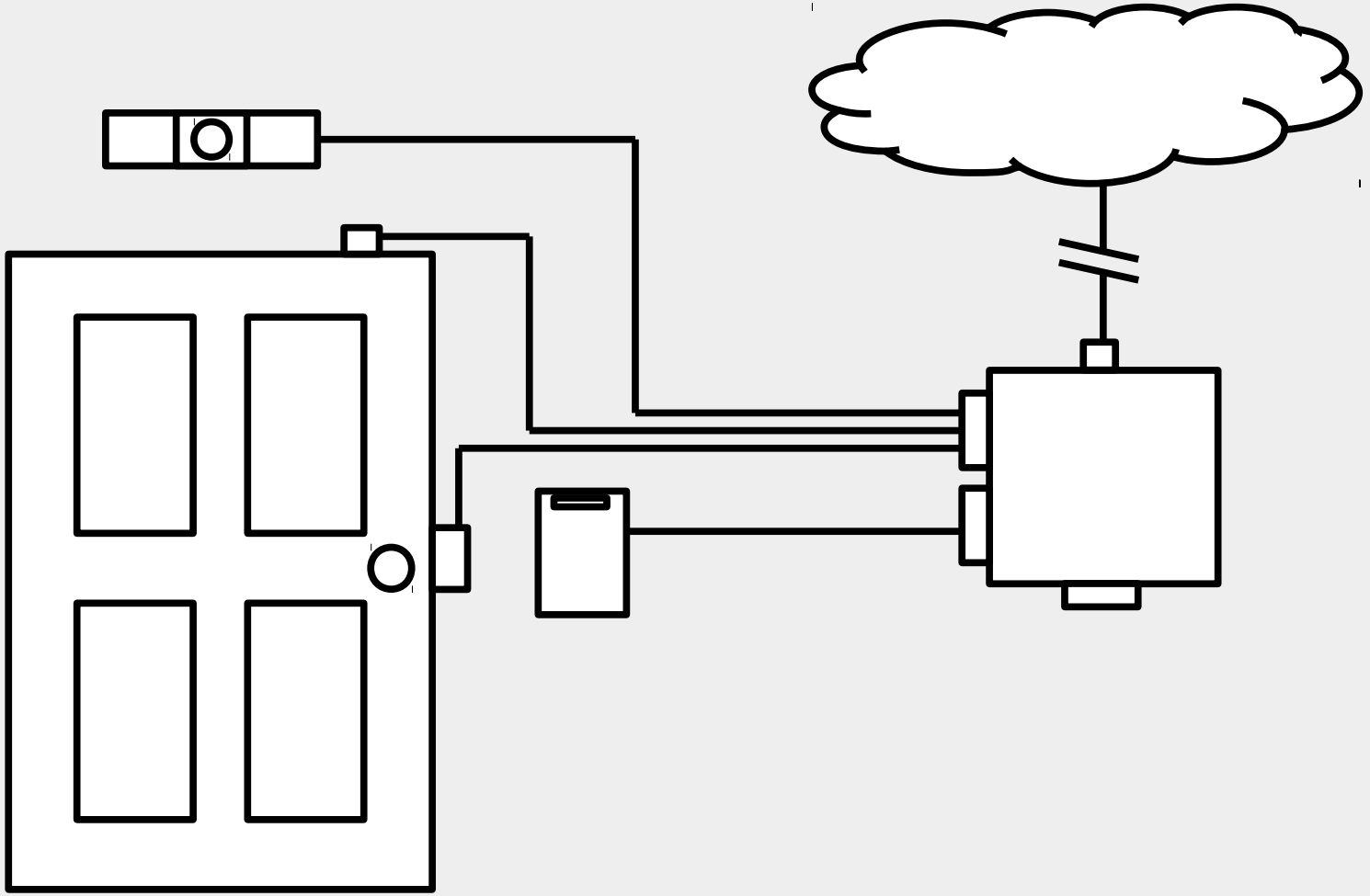
- Locking mechanism
- ID mechanism
- Sensors
- Management software
  - Monitoring
  - Access and schedule changes
  - Override lock states

Access Control

Door Components

- ID reader
  - Magstripe, RFID, biometric, pin pad
- Request to Exit (REX)
  - Signal that unlocks door and prevents force alarm
- Door contact
  - Magnet or switch that shows door state
- Lock or strike
  - Releases to allow door to open
- Door controller
  - Contains schedules and access rules

Access Control



Access Control

Attack Vectors

- ID reader
  - RFID spoofing, brute force, biometric forgery
- REX
  - Trigger PIR sensor, pull inside handle
- Management software
  - Vulnerable host, unsecured database
- Door controller
  - Network-connected embedded device
  - Has complete control over all door functionality

Access Control

Door Controller Attacks

- API exposure
  - Forge or replay remote unlock commands
    - Encryption? Authentication?
  - Physical Security Interoperability Alliance (PSIA)
    - Standard used by several manufacturers
    - Send HTTP PUT req to accessOverride URI with accessOverrideState set to ‘Unlatched’
    - Should be authenticated...individual implementations may vary

Access Control

Door Controller Attacks

- Vulnerabilities in running services
  - Onboard mgmt portal
    - Default creds or auth bypass
    - Cmd injection
  - Old, unpatched services
  - Proprietary services
    - Great targets for fuzzing
    - Not as often or thoroughly audited

Surveillance

Surveillance

Overview

- Video camera
  - Hard-wired or IP-based
- DVR
- Management/viewing software

Surveillance

Attack Vectors

- Management/viewing software
  - Same deal as before
- DVR
  - Modify or delete recordings, DoS to prevent recording
- Video camera
  - Disable or DoS camera
  - MitM video stream?

Surveillance

MitM Video Stream

- RTP or MJPG
- Usually UDP with no encryption
- Intercept frame, modify, then send it on
- Loop playback by capturing frames and reinjecting with modified timestamp/sequence number
- Replace stream with fuzzy static or a single image
- Use opencv to find and replace faces

Alarms

Alarms

Overview

- Fire
  - Smoke/fire detectors
  - Alarm panel
  - Suppression system
- Tamper sensors
  - Mainly simple switches and resistance measurement
- Motion sensors
  - Lots of variety, but mostly PIR and some MW

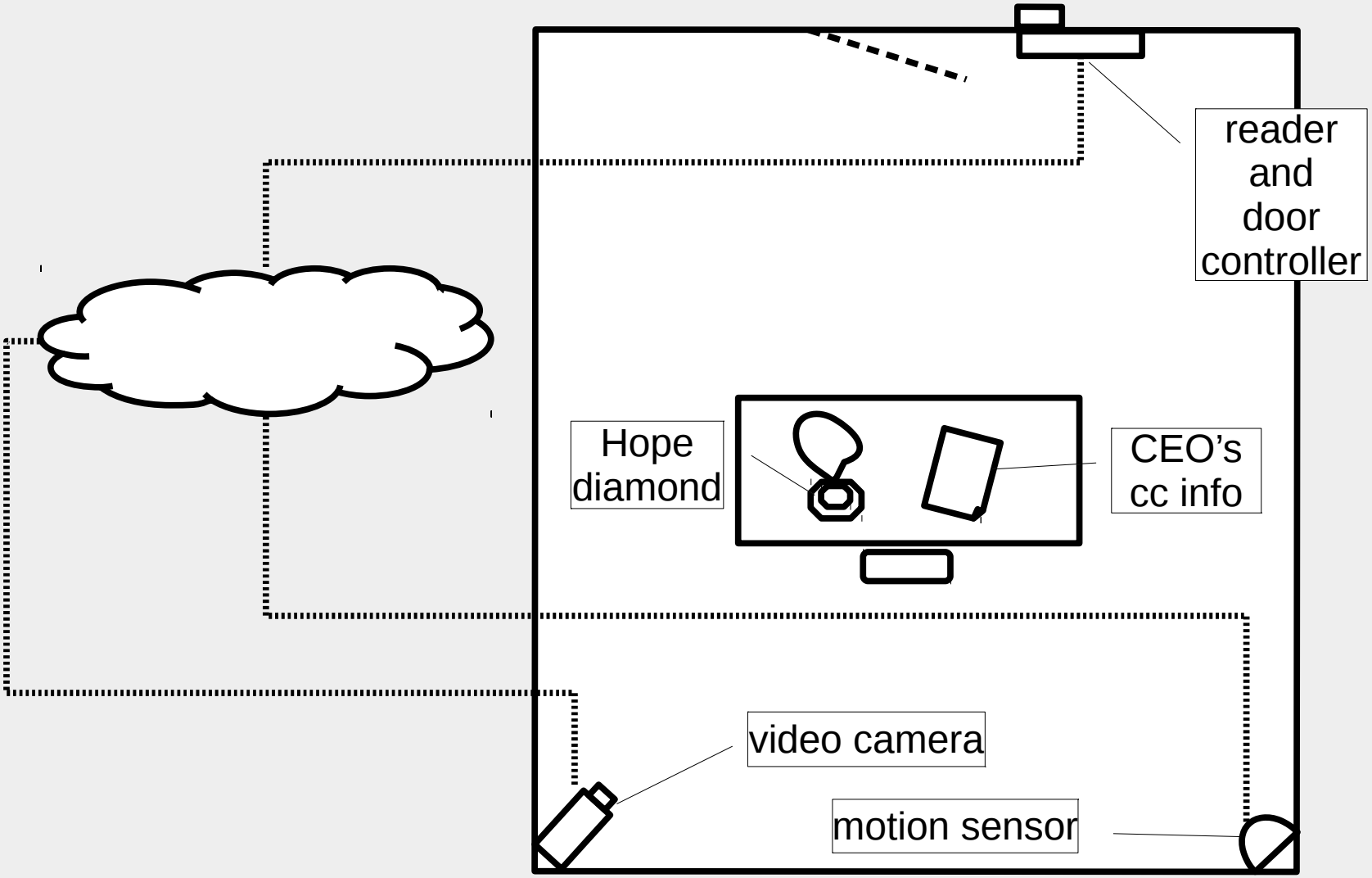
Alarms

Attack Vectors

- Fire
  - Use vuln panel as pivot point
  - Cause false positive as a distraction
- Motion sensors
  - DoS the sensor to prevent reporting
  - Spoof any heartbeats

The Heist

The Heist


reader
and
door
controller
Hope
diamond
CEO’s
cc info
video camera
motion sensor

What Can Be Done?

What Can Be Done?

Defense

- Network segmentation
  - VLANs and firewalls
  - Monitor networks for anomalous activity
- Firmware updates
  - Clearly define who owns what
  - Manufacturers need to be more open
- Think before you link
  - Do you really need an IoT (drink!) motion sensor?

What Can Be Done?

Offense

- Hack yourself
- Audit devices before deploying
  - 3rd party resellers are a good resource for devices and firmware
- Think before you link (yes, again)
  - If you can think like an attacker, they'll be less likely to surprise you later

Questions?

ricky_lawshae@trendmicro.com – twitter.com/HeadlessZeke