

Physical Security for Network Operators

Securing the Tangibles

Alan Hannan
CrowdStrike

Target Audience

5-200+ cabinets/site
colocated with a
data center provider

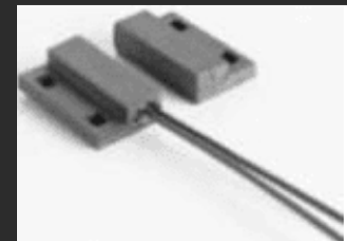
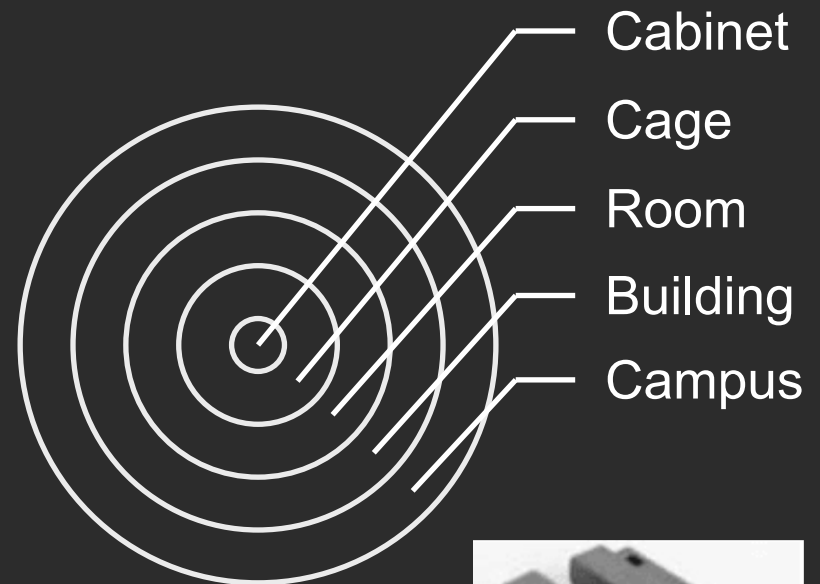
Security focused

Overview

1. Cage/Cabinet Access and Monitoring
2. Circuit Encryption
3. Encryption Key Management
4. Encryption at Rest
5. Vendor Access

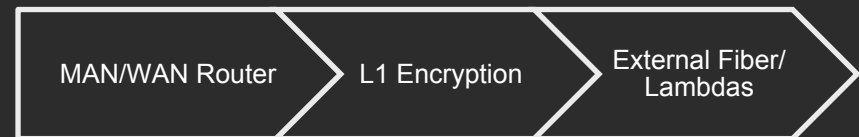
Cage/Cabinet Access and Monitoring

- Build with the approach of secure concentric enclaves within datacenter down to your cabinet
- Cameras everywhere – separate infrastructure by you and the DC
 - Store offsite
- Locked doors on cabinets within cages
- Key card every perimeter
- Door sensors everywhere in cage
 - Magnetic reed switches back to dry contact sensors w/ syslog or SNMP traps work great
- Audit logs
 - Trust but verify – have your vendors show you proof of records and video



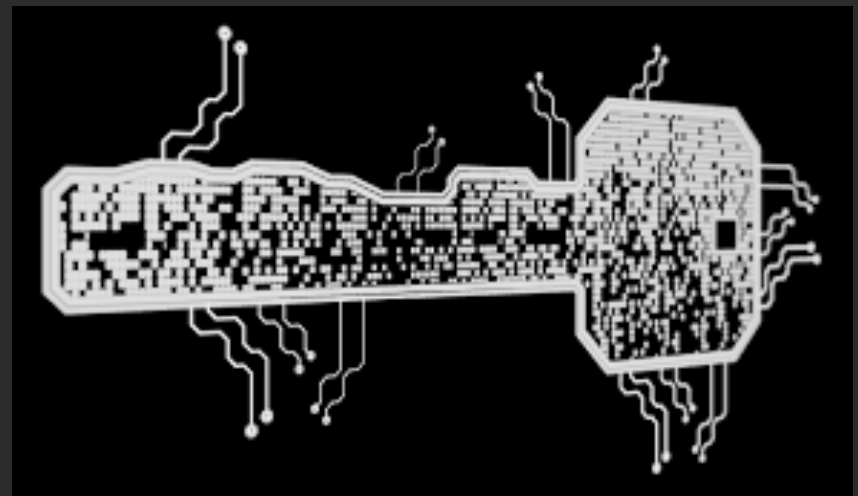
Circuit Encryption

- It's easy to do AES256 encryption at 100G or 10G today
- Arista, Adva, Others..
- IPSEC/Application Layer (TLS) everything else
- Consider encrypting every circuit outside of DC, and if risk requires, inside
- Special transport circuit types required for some(all?) encryption OTU4e



Encryption Key Management

- Roll your keys periodically
- Store canonical keys in HSM
- Require 2FA/MFA where plausible
- Store all keys encrypted; 1Pass; gpg, openssl, JCE
- Require N of M for changes/extraction
- Shamir's Secret Sharing Scheme is good
- Make it a priority to immediately change default passwords




Encryption at rest

- Many ways to ensure security of data
- All disk drives that store secrets, proprietary IP, PII, or Customer Data should generally be encrypted at rest; requiring explicit unlock at power on.
 - TCG/OPAL Protocols
 - Your choice depends on your threat model
- Can encrypt at many levels
 - Physical disk
 - Volume Level
 - Application Level
- A key management system relying on back-end HSM like StrongKey, Safenet, Thales or others can do this.
- Some data may require application encryption.
- If your strategy involves interacting with Government, review cryptography requirements in advance



Vendor Access

- Avoid it whenever possible
- Escort Vendor at all times
- Do not allow them to handle equipment or modify configurations
- Remote tech support through “View only”
- On-site tech support to inspect and advise, not effect change



You can get in anywhere with a ladder under your arm. [VIDEO]

Troy Kinne
Wimp.com - Dec 2, 2016

Sneaking in EVERYWHERE for FREE (Yellow Vest Experiment)

Yes Theory
YouTube - Nov 21, 2017

Thank you