Cyber Threats in Physical Security

Understanding and Mitigating the Risk

Synopsis

Over the last few years, many industrial control systems, including security solutions, have adopted digital technology. Components of these systems, which were physically separated just five to ten years ago, are now linked together over networks, making them remotely accessible and thus open to cyber threats.

This document focuses on cyber threats to physical security networks, analyzes the specific threats and opportunities, and proposes viable, affordable solutions.

Background

In the past, physical security assumed that the exclusion of potential "enemies" from a critical site was enough to protect physical and intellectual properties. Typical security solutions consisted of several layers, such as:

1. Intrusion prevention (perimeter security)
2. Access control
3. Monitoring (mostly by CCTV)
4. Optional (additional security layers around specific onsite assets)

The digital era is challenging past assumptions. Today, systems consisting of processors, memory, software, and communication networks are making it possible to penetrate a site remotely with minimal risk and leaving almost no trace.

Emerging Vulnerabilities

Let's take, for example, a standard security system for a typical seaport.

The system would likely include smart fences, cameras, main gate access control, and a security management system (SMS), all networked and operated over a regular PC. Networking could be done either traditionally over dedicated networks via proprietary protocols, or more commonly, over a standard IT network with TCP/IP switches, routers, servers, and PCs, and may incorporate cellular or wireless elements. Almost all new security equipment is IP-based: surveillance cameras, access control panels, fiber optic cables, IP and PoE door locks, and fire detectors.

A network like the one described above is vulnerable to cyber threats as a result of some fundamental characteristics:

- **Physical exposure** – Many of the security devices are installed outdoors and are close to perimeters, leaving them physically accessible

- **Lack of awareness** – Most security managers believe that their networks are separated and thus safe.[1]
- **Lack of skills** – Most traditional security managers, consultants, installers and manufacturers lack knowledge and skills in IT technology, let alone cyber security.
- **Division of responsibility** – In many organizations cyber security and physical security are managed separately, so no one sees the full picture.
- **Market fragmentation** – The security equipment market is extremely fragmented[2]. Therefore, most of the players are very small and are less likely to invest in ruggedizing their system to meet the emerging cyber threats.

So, the paradox is that investment is being made in physical and cyber security separately, yet the connection between the two is being overlooked.

The result is that despite the proliferation of cyber threats to physical security systems, we still face a lack of standards and slow adoption rates[3] of requirements and solutions to protect them.

The Hybrid Cyber/Physical Threat

Intruders likely prefer committing a cyber or a mixed cyber/physical intrusion, rather than a pure physical one. Instead of taking the risk of actively penetrating through a fence or gate, a common hacker can undertake a number of actions that are just as effective, such as:

- **Neutralizing alerts** - blocking or saturating alarms from the smart fence.
- **Creating false perceptions** - freezing video of digital (IP) cameras or streaming recorded footage to the guard’s monitor.
- **Creating fake identities** - remote production of an access card.
- **Hacking onsite operational systems** - creating a direct outage or damage to power, elevators, fire alarms, and even damage production systems.

These cyber attacks can go completely unnoticed and leave no trace. When no one is aware an attack has occurred, no steps are taken to further secure systems, continuing to leave them vulnerable.

[1] In most cases security officers have limited tools and lack the skills to monitor their network separation or verify the exclusion of WiFi bridges, etc.

[2] As an example, we estimate there are more than 150 perimeter intrusion detection manufacturers worldwide. Likewise, the 10 leading access control players share less than 50% of the market.

[3] It took the security installers and system integrators more than a decade to migrate from analog cameras and dry contacts into digital networks. Although most of them already deploy complex networks, it will probably take quite a while before they become cyber savvies.

It’s Not All Doom and Gloom

Fortunately, the fundamental characteristics of security networks (as well as similar operational networks) provide hope for affordable solutions.

Unlike IT networks, which are extremely dynamic, security networks are mostly static:

- **Subscribers are very stable** - Changes to the network architecture seldom occur, and when they do, it’s almost always in a planned rollout.
- **Information flow is very routine** – Camera #1 streams information from point A to node B and to Server C.
- **Limited known protocols** – A given security network uses a limited and well defined number of protocols – Access reader #17 uses serial communications over a 485 serial protocol to node #18; Camera #1 streams H.264 VoIP in multicast mode to switch A, etc.
- **Limited external connectivity** – Security systems are usually closed within the protected site and external communication, if there is any, is limited to a couple of well-defined points.

Therefore, providing an adequate level of cyber security, even for a large and complex security system, is possible and affordable.

Principles of the Core Solution

The solution is to monitor network flow, detect abnormalities and respond immediately to any suspected attack.

This can be achieved by a managed switch embedded with cyber security capabilities which acts like a flow guardian and enforces the security policy.

At first, when installed, the switch learns the network’s normal behavior (base-lining). Once triggered to hunt, the switch detects deviations from the base-line and reacts accordingly. A few examples of abnormalities that can be detected:

- Fiber: tapping[4], cutting, bending[5]
- Cable change: disconnecting, length change
- Connecting a new network element or disconnecting an existing one[6]
- MAC address change[7]
- IP address change[8]
- Session / Protocol change

[4] Examples – intrusion into a connection between sites or into the network’s backbone within a secured airport

[5] Advanced tapping techniques enable the use of bent cables to monitor leaks in information

[6] Copper wiring can be routed into some intermediate equipment for undetected monitoring

[7] New MAC address may indicate new hardware like recorders, computers, etc.

[8] IP address abnormality may indicate illegal new user taking control of existing equipment, Trojan horses, etc.

- Data flow / direction change[9]
- Abnormal bandwidth consumption[10]
- Abnormal PoE consumption[11]

The switch can also detect Layer2 and Layer3 cyber attacks such as:

- CAM overflow[12]
- ARP spoofing[13] or poisoning
- IP address spoofing[14]
- Stream and video hijacking[15]
- Spanning-Tree[16]
- Protocol manipulation[17]

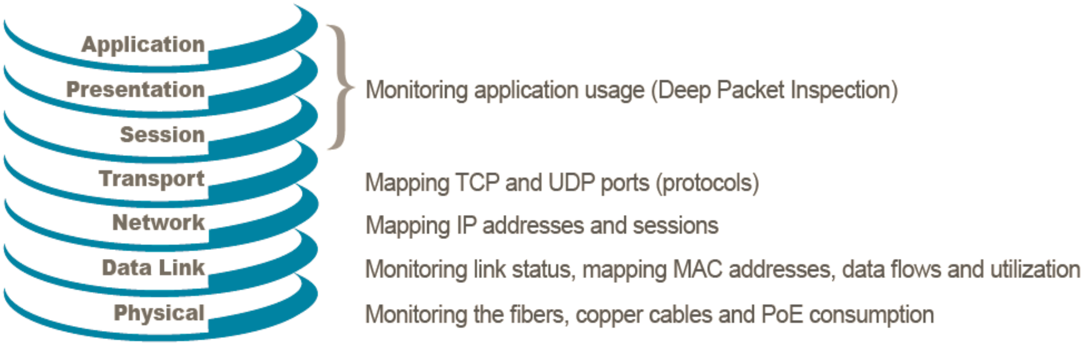
In detecting the above attacks, the switch can be configured to respond in three ways:

- Alert only
- Alert and enable manual intervention
- Alert and automatically execute a proactive intervention

Interventions include:

- Turn on / off port PoE
- Turn on / off port link
- Disable / Enable the alerted exception

ACTIVE AT EVERY LAYER



Monitoring application usage (Deep Packet Inspection)

Mapping TCP and UDP ports (protocols)

Mapping IP addresses and sessions

Monitoring link status, mapping MAC addresses, data flows and utilization

Monitoring the fibers, copper cables and PoE consumption

[9] Examples - Suddenly video is streamed to the wrong target or through a different path; or a camera receives commands from an unauthorized network component

[10] Examples - a camera starts to send files or emails; or a controller starts to bombard and saturate the network

[11] This is especially valuable if an advanced attack has managed to sneak under the cyber radar and thus only a change in the power consumption may expose some new consumer/s

[12] CAM = Context Addressable Memory - inflation of addresses may collapse the hole switch, network and flow behavior

[13] ARP = Address Resolution Protocol – manipulating the network's distribution list enables malicious routing of specific data to unauthorized addresses

[14] This may indicate an attempt to completely take control of the network

[15] This technique enables unauthorized user to subscribe to restricted type/s or sources of data

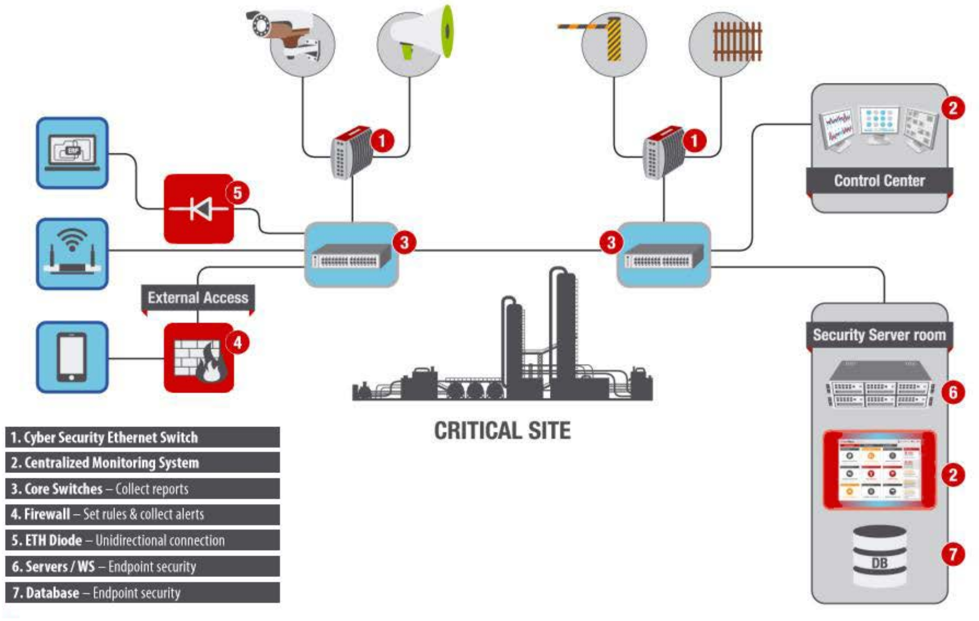
[16] This type of attack may completely crash the direction of the data flow within the network

[17] This may exploit back door holes in equipment and use innocent looking data packages to carry instructions beyond their permitted scope

The Complete Solution

At a minimum, any solution must include, beyond the switch described above, a centralized monitoring system (CMS) in order to collect and classify alerts, enable real-time human interaction, set-up / commission the rules, and more. The CMS is the central brain of the full solution which may also include:

- Wireline firewall, which should enforce the security policy regarding external communication.
- Diodes between critical networks, such as between the access control and the ERP.
- Local cyber agents for servers and databases that detect evolving abnormalities, even before these are manifested to the network.
- Local cyber agents on terminals that can detect policy breaches, such as virus import through disk-on-key and unauthorized bridging between the main wired network and wireless links (such as WiFi or Bluetooth).
- And last but not least – critical sites should also be protected from hacking of their cellular and wireless devices; otherwise the proliferation of smart-phone applications may open a back door into their core operational systems.


ERP
5
1
1
2
Control Center
3
3
External Access
4
CRITICAL SITE
Security Server room
6
2
7
DB
1. Cyber Security Ethernet Switch
2. Centralized Monitoring System
3. Core Switches – Collect reports
4. Firewall – Set rules & collect alerts
5. ETH Diode – Unidirectional connection
6. Servers / WS – Endpoint security
7. Database – Endpoint security

The Way Forward: Integrated PSIM with CMS

Most organizations separate the management of cyber and physical security to distinct systems, departments and people.

For critical sites this may be the wrong approach, since hybrid cyber and physical attacks may be the preferred approach for terrorists, crime organizations, hactivists and even frustrated employees.

Integration of Physical Security Information Management (PSIM) and CMS systems is the natural evolution for better situation awareness and efficient use of common resources (24/7 guards, cameras, communication and escalation procedures).

Although cyber attacks pose a new kind of threat to industrial control systems, a holistic strategy that considers both cyber and physical security is definitely achievable.

Senstar Cyber Security Product Line

Senstar's new line of solutions can protect security systems from cyber threats.

Tungsten is an industrial Ethernet Switch featuring unique protection for different network components against cyber attacks. Specially designed as the ultimate solution for physical security networks, SCADA-based systems, and safe city applications, Tungsten provides ironclad security with full control and customized networking capabilities.

Rubidium is a centralized monitoring system for security rooms (CMS). This appliance is an all-source cyber situation awareness apparatus with the enhanced ability to facilitate operational responses to cyber security events.

For more information about Senstar's cyber products, visit senstarcyber.com.

Senstar, the trusted innovator safeguarding people, places and property, has been manufacturing, selling and supporting the world's largest portfolio of perimeter intrusion detection sensor technologies for more than 30 years. Senstar is also a leading provider of life safety / emergency call solutions, as well as of a new line of solutions that protect security networks against cyber threats.