Meeting the Cybersecurity Challenge of Physical Security Systems

Αλέξανδρος Αυγερινός
Security Systems Engineer

SPACE

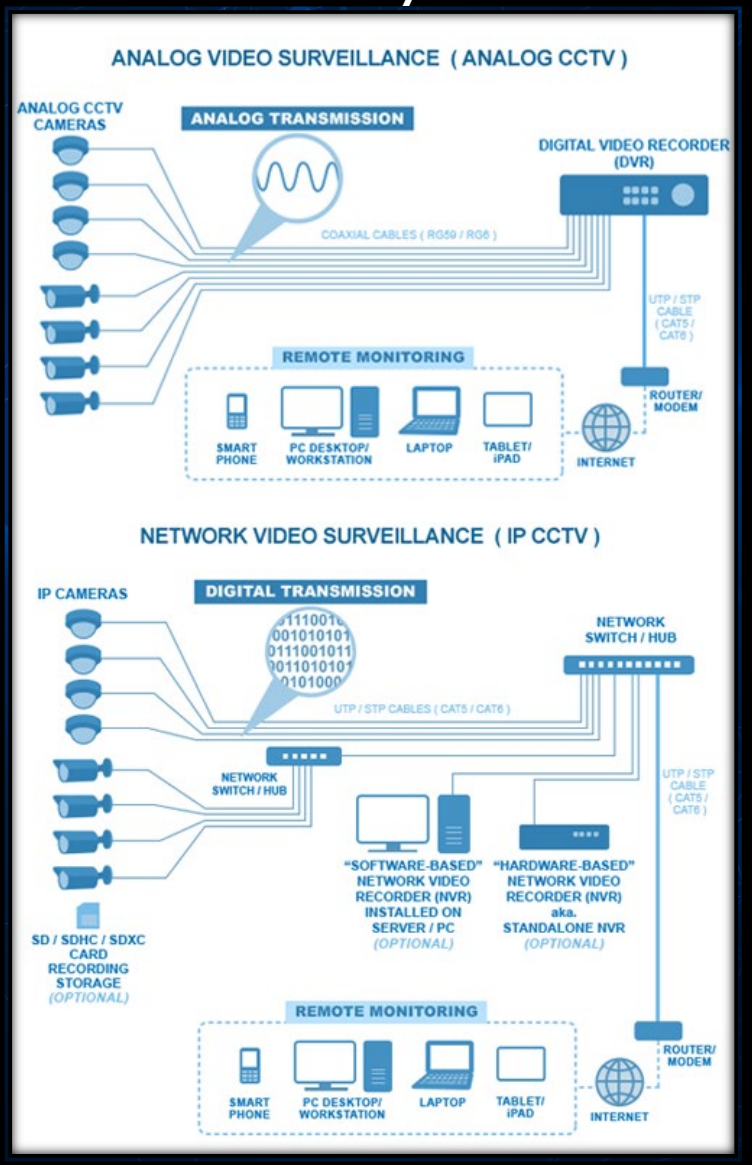
Classification ISO 27001: Public

www.space.gr

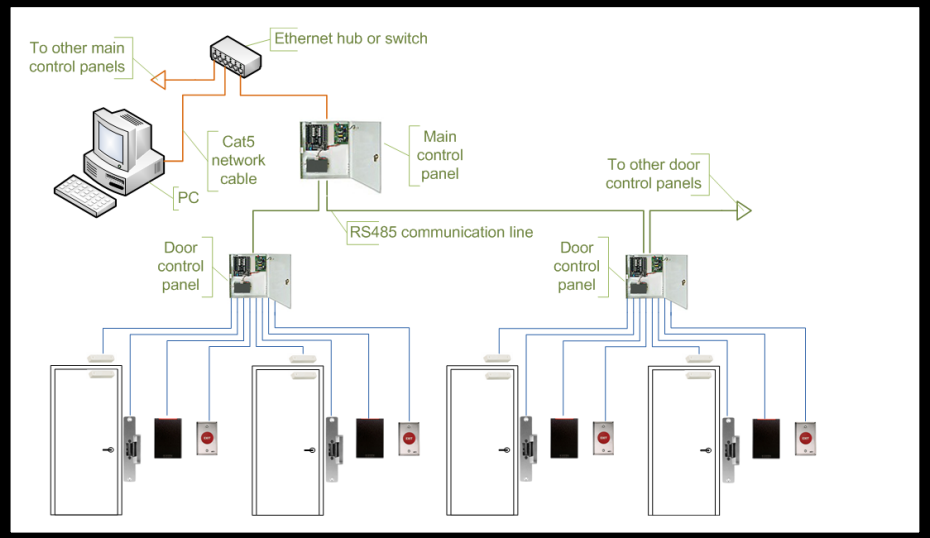
Classification: Public

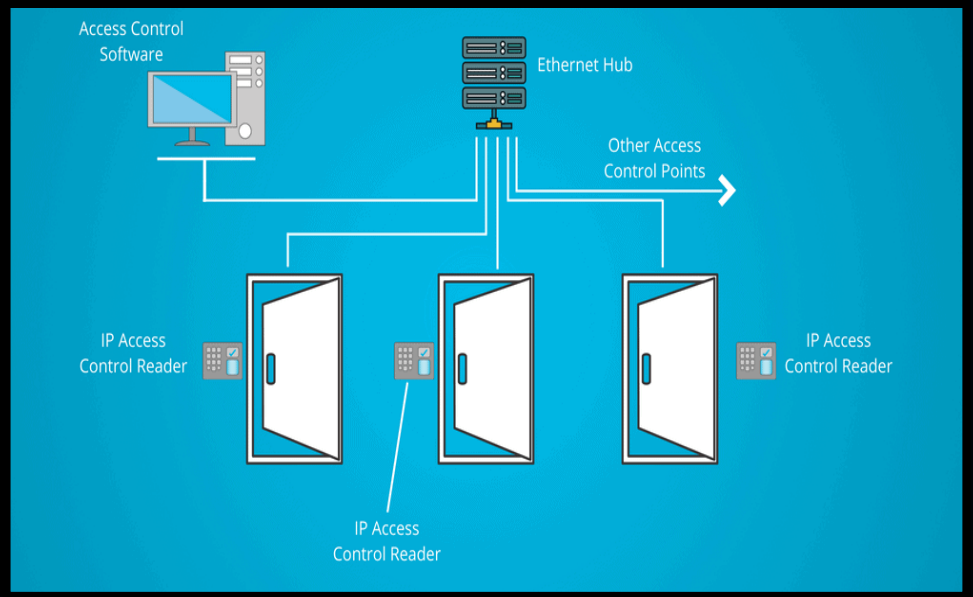
Physical Security Systems Migrating to IP Network

CCTV IP Systems



Access Control IP Systems





The physical security market migrates to IP-based systems for increased return on investment, the demand for stand-alone, proprietary security systems is declining. This creates a gradual integration of building systems and IT departments and promotes a unified approach to security and data infrastructures

Incidents involving cyber and physical Security

- Cyberattack on Physical Systems

  In March of 2021, more than 150,000 cloud-based Verkada physical security cameras were hacked. This incident provided the hackers with access to thousands of cameras through a broad cross-section of industries, from hospitals, schools, and corporate offices to police stations and jails.

- Physical Systems used in Cyberattacks

  Mirai was one of the most infamous botnet attacks in 2016 and was the first significant botnet to infect insecure IoT devices. The Mirai botnet resulted in a massive, distributed denial of service (DDoS) attack that left much of the Internet inaccessible on the east coast of the United States.

- Physical Security of cyber systems

  On April 21, 2017, Lifespan Corporation filed a breach report with OCR regarding the theft of a laptop when an employee's car was broken into. The laptop was unencrypted.

New Threats

- ## Physical Breaches Can Facilitate Hacking

  For many hackers, the easiest way to obtain your data is to access it in the physical world. While strong firewalls and other cybersecurity best practices may thwart hackers outside your business from entering the network, very often hackers will simply find a way into your building and plug into any IP connection.

- ## Hacking Can Create Physical Threats

  If your IP-connected physical security solutions are not properly hardened to cybersecurity threats, they can be compromised via the network. A hacker outside your building can access your network—through unsecured WiFi networks, a vulnerable Internet of Things (IoT) device, or another weakness—and can disable physical security devices such as surveillance cameras, access control systems or alarms.

- ## Physical Security Devices Can be Used as Attack Surfaces

  Any device on the IoT – from a smart fishtank to an elevator system – could be used by hackers as an entry point to the network. The same is true for physical security products from surveillance cameras to WiFi locks. The moment a device is connected to the network, it becomes a potential attack surface.

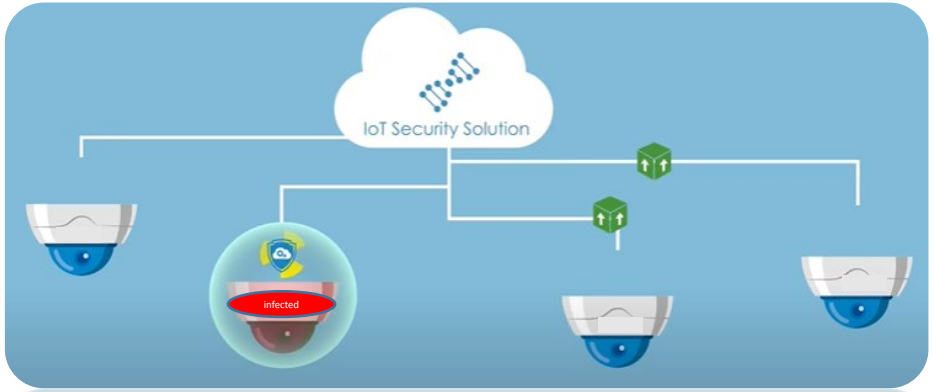
Secure CCTV Cameras

1. Secured connections supported
2. Password enforcement at setup
3. Unsecure ports disabled
4. Unsecure remote communication disabled
5. Protection against execution of untrusted and malicious code
6. Firmware updates only possible via manufacturer signed firmware files
7. Embedded Login Firewall. Prevention of Denial of Service (DoS) attacks
8. Software sealing to detect configuration changes
9. Built-in Secure Element with trusted chip functionality

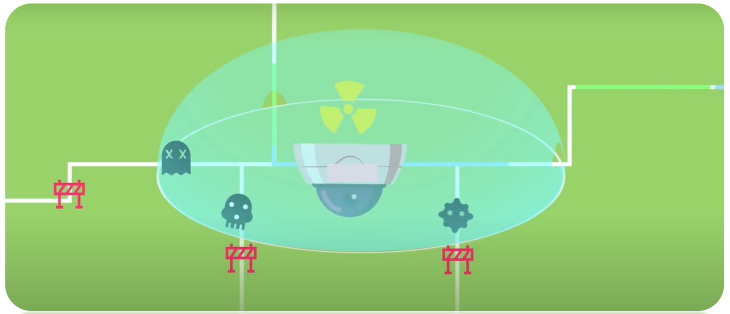
Secure Camera – Server IP Channel

Cabling out of Public Reach

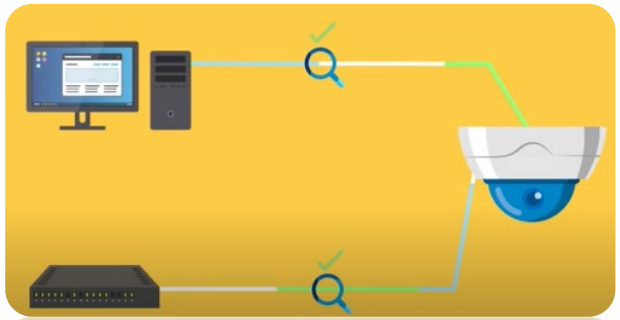
Damage Control



Detection & Prevention of Intrusion



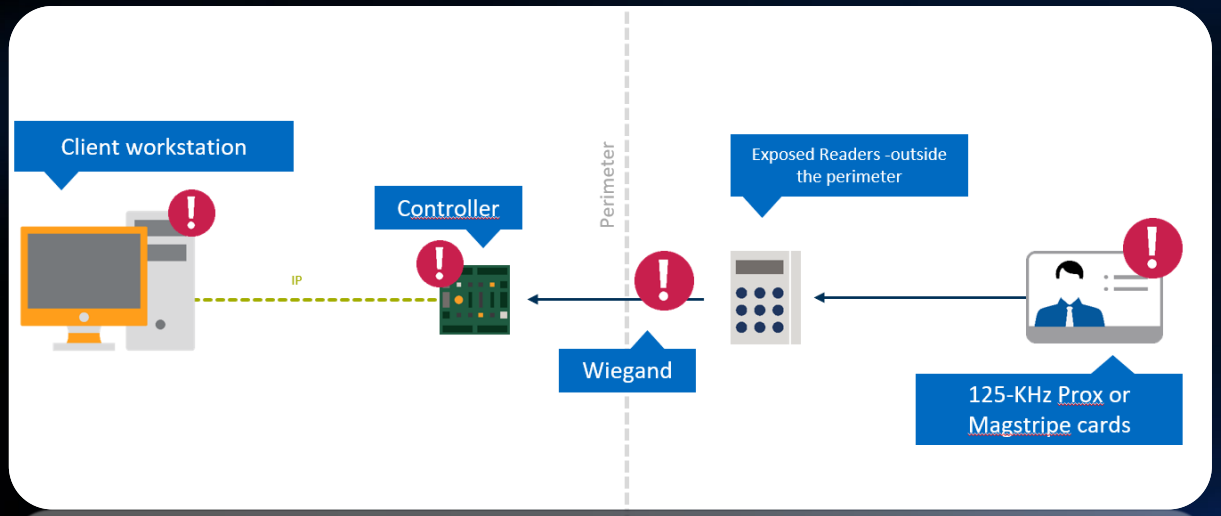
Block Brute Force Attacks

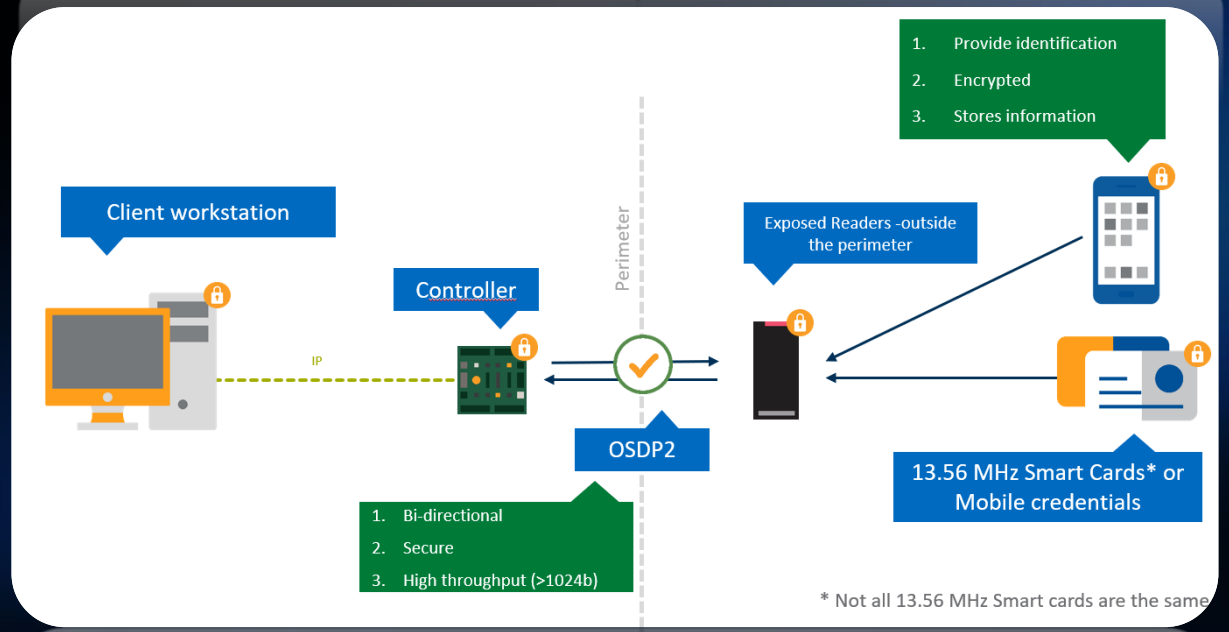


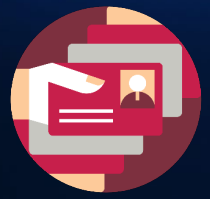
Secure Access Control Devices

- Employ Strong Credentials
- Implement Multi-Factor Authentication
- Authenticate Everything
- Manage the Credentialing Process
- Secure Users Outside of your Organization
- Harmonize with the Organizations' Objectives
- Protection against DoS attacks via Bluetooth Readers

Secure Reader – Controller – Server Channel







Skimming

attacker uses his reader to access information on the victim's access card without consent

Relay attacks

attacker possesses a "clone" of a token, thereby allowing him to gain the associated benefits

Tapping

attacker can recover the data sent between a reader and a controller

Secure Credentials

MIFARE DESFire EV2-3 smartcard platform, iClass SEOS technology, Mobile Credentials

Tampering Detection

Readers capable of detecting counterfeiting, tampering or hacking of the credential

Encryption Standards

Vendors adopting latest secure protocols. OSDP2 over Wiegand, TLS 1.2 standards between server and downstream hardware.

Secure end to end project

- High Technology System Integrator
- Compliance with Standards and Certifications
- End to End IT & Physical Security Design
- Trusted Vendor
- System Maintenance
- Trained Staff
- Control Room – Live handling of incidents (Both Physical & IT)

Strategic Activities & Competences

Communications & Networks	•Communication & Data Networks (wired, wireless, satellite) •Network Management
Telecom Services	•IP - MPLS - VPN (domestic and global connectivity) •Fixed & Mobile Telephony, Satellite Communications •Node Housing
IT	•Virtualization Platforms, Cloud Computing, Application Delivery •Data Management, Backup, High Availability and Disaster Recovery/BCP •IT Intelligence & Monitoring, Service Level Management, BSS/OSS
Information & IT Security	•Network Security •Information Security and Compliance •IT Security
Security Systems	•CCTV/IP HD Surveillance, Video Analytics, Number Plate Recognition, Biometrics, Perimeter Protection, Access Control, Intrusion Detection •Integrated Security Systems
Infrastructure	•Data Centre Infrastructure •Structured Cabling, Electrical and Mechanical Installations
Applications	•Unified Communications IP telephony, Video Conference Audio Visual Appls •Fleet/Asset Tracking & Management, Telemetry •Security Platforms, Training Simulators
Research & Development	•Applications Development & Systems Integration •National and International Co-funded Projects •Defense Projects

Facts Sheet

Presence

- HQ located in Athens
- Branches in Athens, Thessaloniki, Patra, Heraklion-Crete, Ioannina, Farsala and Nicosia-Cyprus
- Subsidiaries in Cyprus, Romania, Serbia, Malta & Jordan
- Activities in Europe and the Middle East

Human Capital

- Over 540 Specialized Employees
- Over 700 Certifications
- Accreditations: National . EU . NATO Secret
- Certified according to: ISO9001:2015 . ISO/IEC27001:2013 ISO14001:2015 . OHSAS18001:2007 ISO20000-2018 . ISO22301-2019

Growth & Stability

- Over 35 Years of Operations and Sustainable Growth
- Turnover: € 103.3 million (2021)
- Listed on the Athens Stock Exchange since 2000

Investments

Space Hellas Holds:

- **18.1%** of Mobics (Greece)
- **32.2%** of WEB-IQ (Netherlands)
- **35%** of AgroApps (Greece)
- **60%** of SingularLogic (Greece)
- **100%** of SenseOne (Greece)
- **40%** of Epsilon SingularLogic (Greece)

Space Hellas is the leading Digital Integrator and Service Provider in South Europe

SECURING

Your Digital Transformation Journey

Ευχαριστούμε για την Προσοχή σας

SPACE

Classification ISO 27001: Public

www.space.gr