Trends in Cybersecurity

How cybersecurity can impact your security, surveillance, and emergency communications systems

I am Brian Denmeade.

I have a passion for helping secure the world through physically- and digitally-secure devices.

We are Ganz.

Keith Sowa
DIRECTOR OF PRODUCT DEVELOPMENT
Q & A

Alisa Watlington
MARKETING COMMUNICATIONS SPECIALIST
Moderator

Outline

1. What Cyber Attacks are NOT
2. Actual Threats
3. Common Practices Today
4. Types of Cyber Attacks
5. Data Security
6. Common Cybersecurity vs. Proper Cybersecurity
7. Insider Threats
8. Cybersecurity Practices Checklist

What Cybersecurity Attacks are NOT

Let’s start with the myths

Top Myths

- Hackers are hacking into our webcams to watch us in our homes
- Hackers are trying to spoof video streams e.g., to rob a bank

Actual Threats

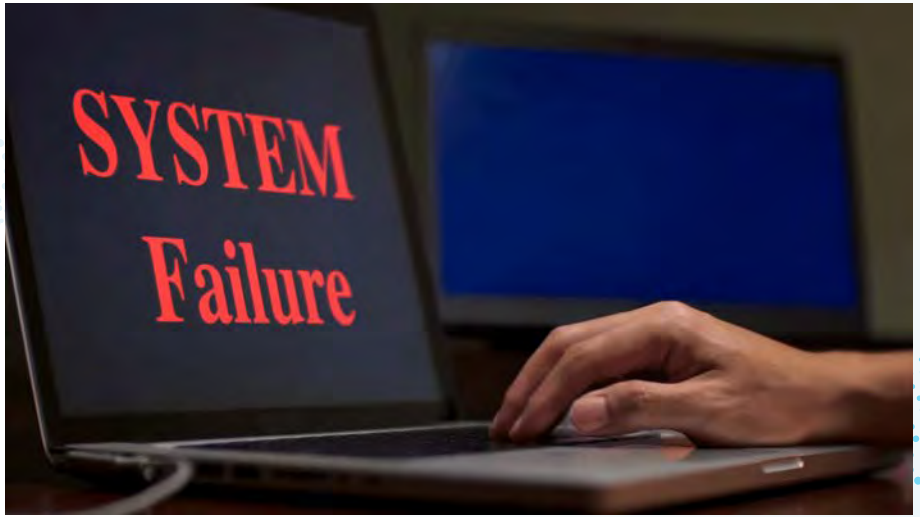
The most common types of cyber attacks on security systems are edge device **botnets** & **ransomware.**

Actual Threat: Botnets

- A botnet is a number of Internet-connected devices, each of which runs one or more bots. They can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. The word "botnet" is a blend of the words "robot" and "network".

Actual Threat: Ransomware

- Ransomware is a software used by cybercriminals to encrypt or "lock up" files on computers or servers with the goal of making those items inaccessible



Actual Threats, cont.

- Ransomware gangs are now using Ransomware as a Service and are more aggressive in negotiations by doubling down with distributed denial-of-service (DDoS) attacks.
- Timed attacks on critical infrastructure: IoT installations require due diligence, particularly those that connect to transportation systems, public facilities, & utilities

Common Practices

The Most Common Measures Security Managers Employ

Common Practices

- Ensure the system does not respond to Ping requests
- Change the IP port that is used to access the unit over the Internet
- Change the password over the system
- Configure your router's Firewall
- Check and install firmware updates

These are not actual cybersecurity measures.

Types of Cyber Attacks

The Most Common Threats

Types of Cyber Attacks

An infected edge device turned into a bot

- Behaves as usual, streams video, and has all the TLS certificates in place
- Can start DDos attack at a certain time point
- Can spam intranet with phishing emails
- Can spoof its index webpage, especially if it requires plugins
- Can distribute ransomware-infected screenshots if it can email such alarm notifications

These devices are Linux-based

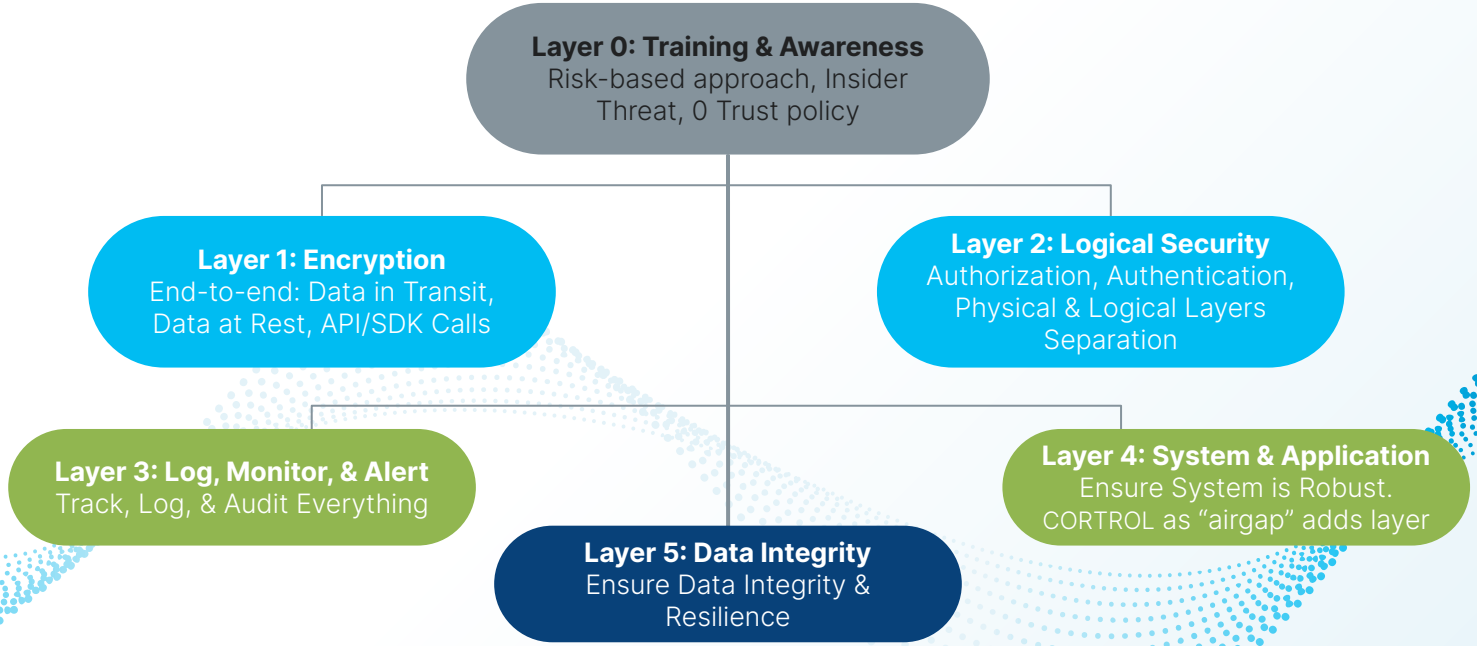
Large arrays of devices are most likely to be targeted

Data Security

Data Security

- Security of your video data can and should be a priority
- Older technology cannot keep up with evolving risks
- A casual collection of loose measures cannot provide an adequate cyber barrier
- There has to be a **consistent framework** to implement *multiple* cyber defense layers to ensure the system will be secured all-around

CORTROL Data Security Layers

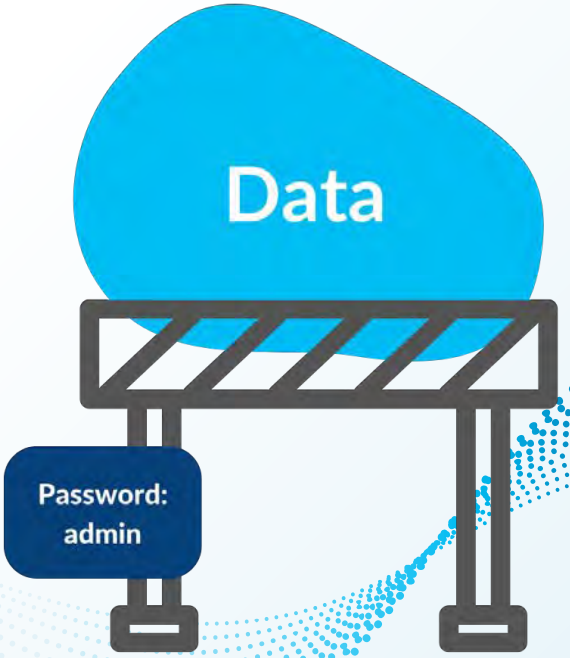


Data Security Authentication

Basic, HTTPS Basic, Digest, HTTPS Digest

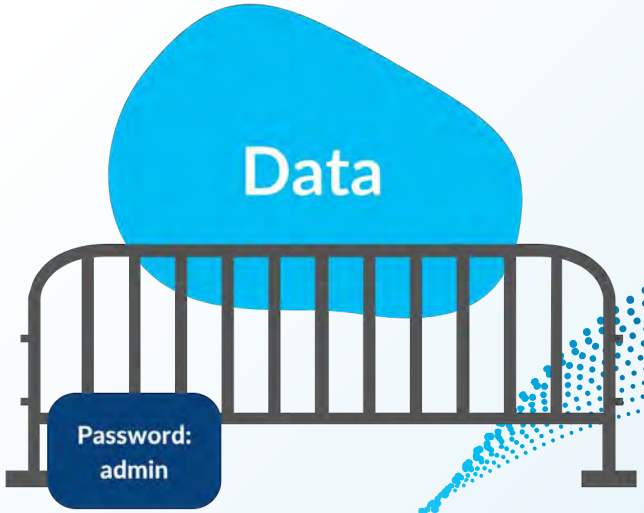
Basic Authentication

- **No Transport Layer Security**
  - All messages are visible
- **No Data Security**
  - Unencrypted data
- **No Password Security**
  - Unencrypted passwords
  - Password sent with each message
- **Attack Surface**
  - Any–no security in place
- **Attack Complexity**
  - None



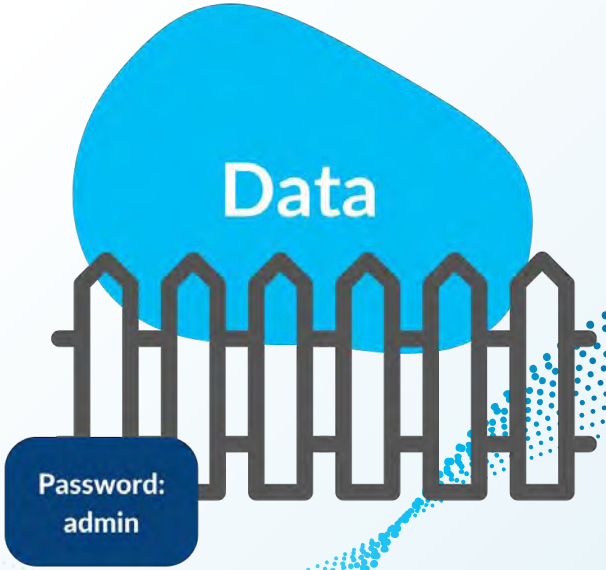
HTTPS Basic Authentication

- **Transport Layer Security - HTTPS**
  - Encrypted Transmission Channel
- **No Data Security**
  - Unencrypted Data
- **No Password Security**
  - Unencrypted passwords
  - Password sent with each message
- **Attack Surface**
  - Limited. Open to Middleware, Forged Certificates, API, DoS attacks
- **Attack Complexity**
  - Moderate



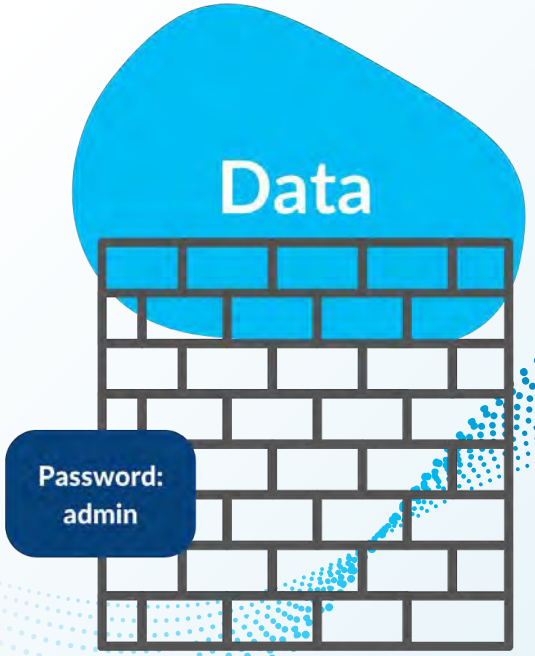
Digest Authentication

- **No Transport Layer Security**
  - All messages visible
- **Data Security**
  - Encrypted data
- **Password Security**
  - Encrypted Password sent just once
  - Session Token sent with each message
- **Attack Surface**
  - Limited. Can be vulnerable to Man-in-the-Middle, Insider (HA1 leakage) attacks.
  - Sensitive to quality-of-protection server policy.
- **Attack Complexity**
  - Moderate



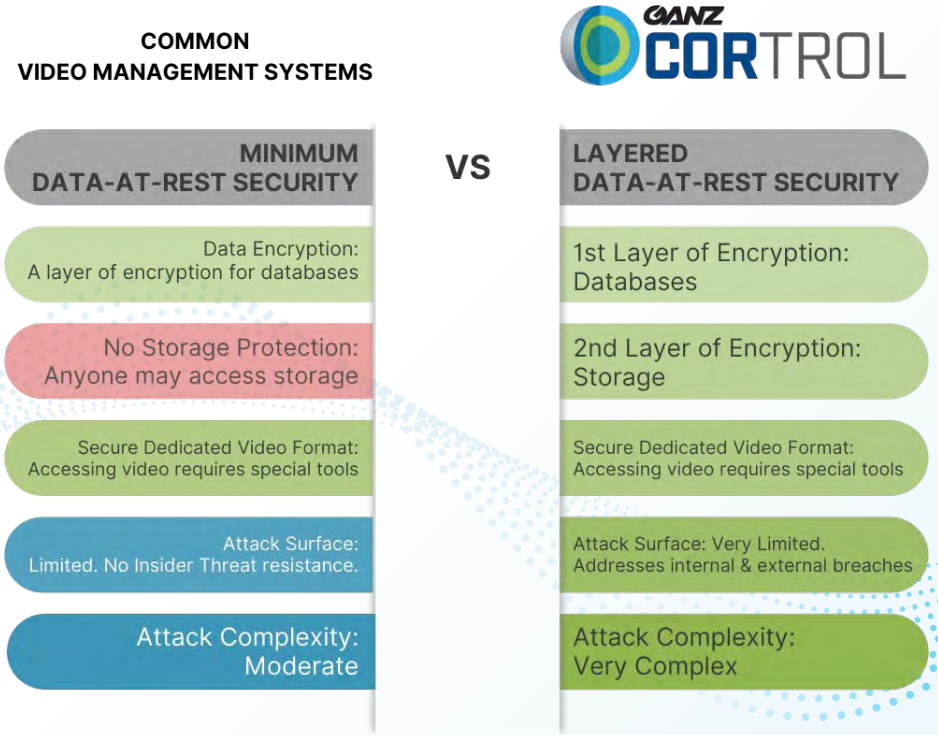
HTTPS Digest Authentication

- **Transport Layer Security - HTTPS**
  - Encrypted Transmission Channel
- **Data Security**
  - Encrypted data
- **Password Security**
  - Encrypted Password sent just once
  - Session Token sent with each message
- **Attack Surface**
  - Very Limited
- **Attack Complexity**
  - Very Complex



Data-at-Rest Security

Data-at-Rest Security Comparison



Data-at-Rest Security Checklist

Encryption

- ❑ Encrypted System Databases
- ❑ Encrypted Archive Databases
- ❑ Encrypted Storage

Storage Protection

- ❑ Restricted Storage Access
- ❑ User-defined Password (no root or admin-level access)

Secure Video Data Format

- ❑ Dedicated Secure Video Format
- ❑ No open-source or Generic Formats

Data-on-the-Move Security

Data-on-the-Move Security Checklist

Transport Layer security

- ❑ Self-signed Security Certificates

Password Encryption

- ❑ Hashed password transfer
- ❑ Password transferred only once

Data Security

- ❑ Data encryption
- ❑ Hashed messages

Session Security Tokens

- ❑ Time-limited session-specific tokens

The Safest Option

For Your Video Management System
& Centric Security Solution

Ganz CORTROL enhances data protection and cyber resiliency with advanced authentication and end-to-end data encryption technologies at all levels:

- Database encryption by default, plus an **extra user password layer**
- **End-to-end data flow encryption** server-server, server-client, camera-server
- Digital certificates: self-signed or customer's own (issued by authority)
- Encrypted session tokens + DoS attack prevention
- Strict "**No Basic Authentication**" policy for all API/SDK calls
- Enhanced security and faster archives with Proprietary format
- Multi-database architecture as an **extra layer against data corruption**

Download our free demo at: ganzsecurity.com/cortrol

GANZ CORTROL

GANZ D2PD POWERED BY Go²Blu

- With CORTROL as your video surveillance system, Ganz D2PD is an easy add-on **emergency communications system**
- In ¼ of 1 second, you can reach the police via physical panic button or computer program
- Securely chat directly with the police on any enabled laptop
- Utilizes the secure Amazon Cloud for its servers
- No data privacy threats based on app stores

Insider Threats

Ganz CORTROL Insider Threat Policy

- Physical Layers
  - Users
  - Configs
  - Databases
  - Cameras & Devices
  - Storage
- Logical Layers
  - Video Footage
  - Operator Tools

Good Cybersecurity Practices

Cybersecurity Practices Checklist

Transport Layer Security (HTTPS)

- ❑ Self-signed Security Certificates
- ❑ Custom Security Certificates

Practice Makes Perfect

- ❑ Conduct tabletop exercises and drills to understand how to respond and recover from an attack.

Communicate

- ❑ Establish lines of communication to make it easy for all entities affected by an attack to share information across countries & organizations.

Data Security

- ❑ Data Encryption
- ❑ Hashed Messages

Password Encryption

- ❑ Hashed Password Transfer
- ❑ Password transferred only once

Session Security Tokens

- ❑ Time-limited Session-specific Tokens

Thanks!

Any questions?

bdenmeade@cbcamerica.com

Learn more about CORTROL **VMS** | Learn more about D2PD **Emergency Communications System**

GANZ CORTROL

GANZ D2PD POWERED BY Go²Blu

Sources

Sources

- https://www.techrepublic.com/article/cybersecurity-worries-at-the-olympics-range-from-personal-phones-to-public-water-supplies/
- https://www.securitymagazine.com/articles/96781-top-15-cybersecurity-predictions-for-2022?oly_enc_id=3736C5780601H5X
- https://www.forbes.com/sites/bernardmarr/2021/12/17/the-five-biggest-cyber-security-trends-in-2022/?sh=7e9fdebe4fa3
- https://en.wikipedia.org/