

# Are CCTV Cameras Secure?

Athira Dinesh Mangaparambil (40258046)

*Concordia Institute for Information Systems Engineering*

## Abstract:

The report discusses security concerns and solutions for closed-circuit television (CCTV) systems, serving as private surveillance systems for real-time monitoring and safety enhancement. It explores camera classifications based on specific criteria. However, these systems face susceptibility to various attacks, as outlined. To mitigate these risks, multiple methods are recommended to uphold security and integrity, preventing unauthorized access and potential vulnerabilities. Additionally, it discusses a security tool that aided in detecting the Mirai malware attack. Overall, the report provides insights into safeguarding CCTV systems against security threats.

## Introduction:

CCTV, also known as closed-circuit television, is a surveillance system utilized for security purposes through private monitoring, without the public broadcasting of video signals. Its primary function is to enable real-time monitoring of specific areas, enhance safety, and detect criminal activities. CCTV operates by strategically positioning cameras in certain spots and then monitoring the captured footage on screens situated somewhere. The cameras transmit their footage to monitors or recording devices through either cables or wireless connections. The term "closed-circuit" indicates that only authorized individuals or entities have access to this footage. In essence, CCTV serves as a private surveillance system designed for security purposes, ensuring that only authorized individuals can access the recorded material [1].

## Types of Security Cameras:

Security camera technology is rapidly evolving to meet diverse security needs in various contexts, from locations without WiFi or power sources to specialized areas like front doors, backyards, and driveways. However, navigating the different types of security cameras can be challenging, and selecting the right camera type is crucial for optimal functionality and application.

Below are the classifications of security cameras based on certain parameters.

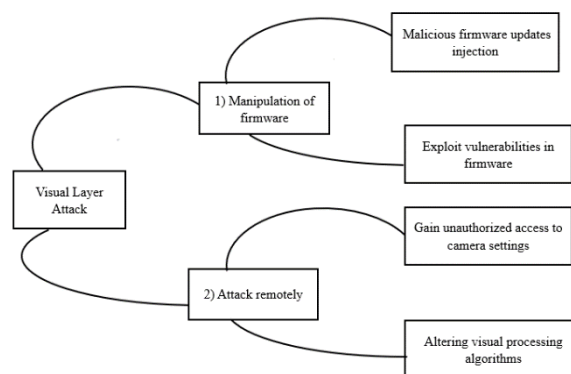
- **Classification Based on Connectivity:** Based on their connectivity technology, security cameras fall into two categories: Analog and IP cameras.
  - **Analog Cameras:** These capture video signals in analog format and transmit them over coaxial cables to devices such as Digital Video Recorders (DVRs). While they provide basic video recording functionality, they lack advanced features like motion detection, two-way audio, or video analytics.
  - **IP Cameras:** IP cameras use digital technology to encode and transmit video data over IP networks like the Internet or local networks. They often store footage onboard or on network-attached storage devices, eliminating the need for a separate DVR.
- **Classification Based on Area of Placement:** Security cameras are classified based on their installation locations into three types: Indoor Security Cameras, Outdoor Security Cameras, and Video Doorbells.

- ***Indoor Security Cameras:*** Designed for monitoring indoor environments such as homes, businesses, and retail stores. Most variants are compact and capture video and sometimes audio within interior spaces.
- ***Outdoor Security Cameras:*** Built to withstand rain, snow, and extreme temperatures. Most outdoor cameras have a high IP rating, indicating greater tolerance to harsh external environments.
- ***Video Doorbells:*** Combining a doorbell, camera, and intercom system to monitor and communicate with guests remotely.
- **Classification Based on Wiring:** Security cameras can be categorized into two types based on their wiring options: Wired Security Cameras and Wireless Security Cameras.
  - ***Wired Security Cameras:*** Connected to recording or monitoring systems via physical connections such as Ethernet (Cat5e or Cat6) or coaxial cables, which transmit power and video signals.
  - ***Wireless Security Cameras:*** Transmit data wirelessly via WiFi or other communication protocols, eliminating the need for physical cables.
- **Classification Based on Recording Methods:** Different cameras employ various recording methods:
  - ***NVR (Network Video Recorder):*** Records video directly from network-connected cameras via Cat5 or Cat6 Ethernet cables with RJ45 plugs. NVRs are compatible with IP cameras, including PoE NVRs and WiFi NVRs.
  - ***DVR (Digital Video Recorder):*** Processes uncompressed videos from analog cameras and compresses them into a digital signal before transmission.
  - ***Cloud Recording:*** Allows users to store recorded video and photos in the cloud, a remote server, or an Internet-connected data center without the need for a central administration device.
- **Classification Based on Shape:** Different camera types are categorized based on their shapes, including Bullet cameras, Dome cameras, Turret Cameras, and Fisheye Cameras.
- **Latest Innovations in Security Camera Types:** Advancements in technology have introduced distinctive security camera types:
  - ***Floodlight Cameras:*** Combine high-intensity floodlights with integrated security cameras to provide outdoor security.
  - ***Dual-Lens Cameras:*** Use two lenses to capture multiple angles simultaneously, improving video quality and night vision.

- **Solar-Powered Cameras:** Utilize solar panels to harness the sun's energy, providing long-term power for isolated areas [2].

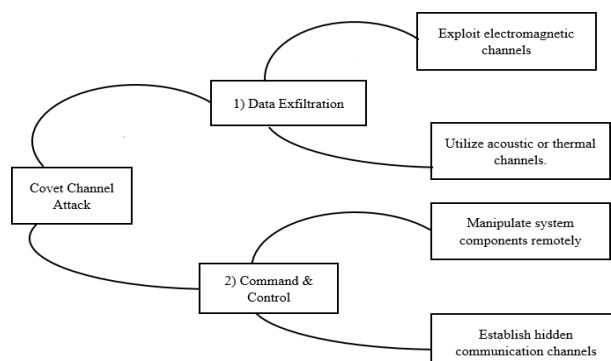
## Attacks on Video Surveillance Systems:

- **Visual Layer Attacks:** Visual layer attacks exploit the image processing capabilities of surveillance systems. Malicious components, which can be introduced locally or remotely through methods such as firmware updates, are triggered by specific visual inputs captured by cameras. For example, attackers can manipulate camera inputs to blur specific faces or disable critical functionalities like video recording. These attacks take advantage of the system's reliance on visual data processing.



## Defenses:

- Monitoring video frames for suspicious processing patterns can help identify malicious activities. However, identifying hardware-based assaults is complex and expensive.
  - To prevent attacks, introducing random or key-based pixel noise can disrupt malware's ability to interpret video images. Another strategy is to use adversarial image techniques to alter images in ways that affect detection and classification. However, these methods have disadvantages, including the risk of interfering with valid video analysis and tampering with vital information.
  - To provide enhanced malware protection, a robust cryptographic system using a multi-party key-sharing approach could be implemented to ensure safe, secure, and private video feeds.
- **Covert Channel Attacks:** Covert channel attacks have been the subject of recent research, focusing on methods like electromagnetic, acoustic, thermal, and optical pathways, especially in isolated environments. Researchers have identified new and existing covert channels within video



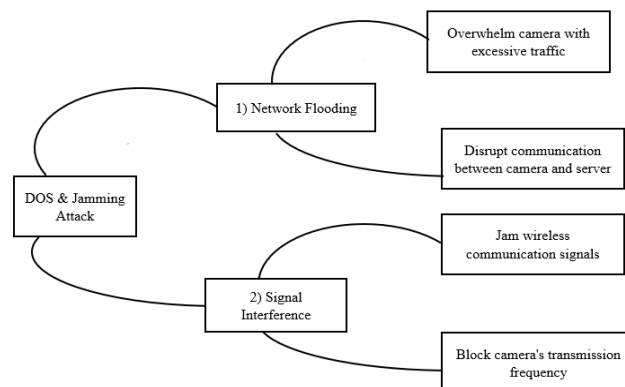
surveillance (VSS) and CCTV systems, enabling data exfiltration or distributed command-and-control functions through compromised components.

Furthermore, researchers propose using smart screens linked to VSS systems to employ techniques such as *VisiSploit* for data exfiltration. Another method that attackers may exploit is *steganography*, which involves using digital images typically accessible from VSS systems.

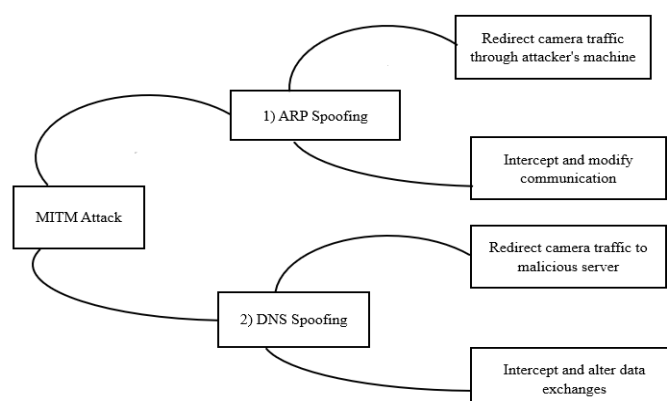
Moreover, cameras equipped with *Pan-Tilt-Zoom (PTZ)* functionality can encode data into movement, providing yet another covert communication method. Attackers can increase data exfiltration rates by integrating compromised cameras into a Collaborative Group (CG) and performing coordinated PTZ movements.

Finally, the audio capabilities of VSS systems can be used as command-and-control channels using techniques such as hidden voice instructions. These diverse strategies highlight the challenges in securing modern surveillance systems from covert communication tactics.

- **Denial-of-Service (DoS) and Jamming Attacks:** These pose major risks to video surveillance systems. These attacks are especially important to address because uninterrupted operation of surveillance systems is critical for monitoring and documenting significant actions such as crimes. Even a brief interruption caused by a DoS attack could cause these systems to miss key events like fast-paced crimes or incidents with serious implications. Unlike DoS assaults on home routers, which may cause minor inconveniences, DoS attacks on video surveillance systems have severe consequences that must be carefully considered during system design, assessment, and testing [3].

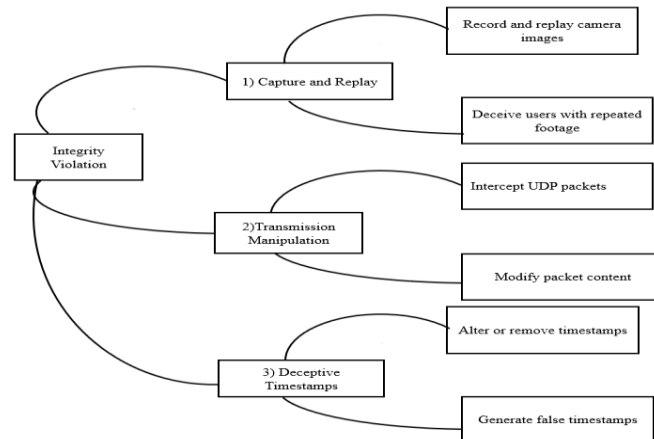


- **Man-In-The-Middle Attack:** The camera system's susceptibility to a potential security flaw exposes it to Man-in-the-Middle (MITM) attacks. By exploiting Address Resolution Protocol (ARP) spoofing, attackers can intercept traffic between the camera and other network-connected



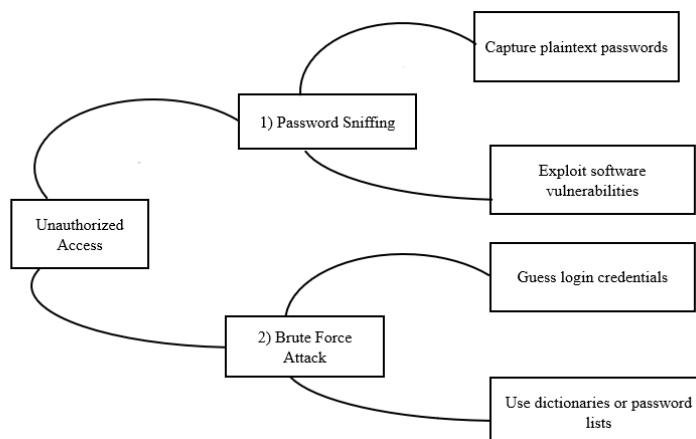
devices. Manipulating the ARP table allows the attacker to reroute communication through their own device, serving as an intermediary between the camera and its intended destination. This enables the attacker to eavesdrop on or tamper with transmitted data without detection.

- **Violation of Integrity:** In cases of integrity violation, attackers employ a deceptive tactic beyond simply blocking camera data transmission. They manipulate victims by repeatedly sending a



sequence of photos, creating the illusion of continuous live footage. However, this approach has limitations, including flickering visuals and detectable timestamps, which may alert the victim to the deception.

- **Unauthorized Access:** This security concern arises during the authentication process between the target PC and the camera. Despite the existence of authentication methods, passwords are often transmitted in plaintext, particularly in surveillance applications. This vulnerability is alarming, especially since it affects cameras compliant with the ONVIF (Open Network Video Interface Forum) standard, which aims to ensure interoperability and security in video surveillance systems [4].



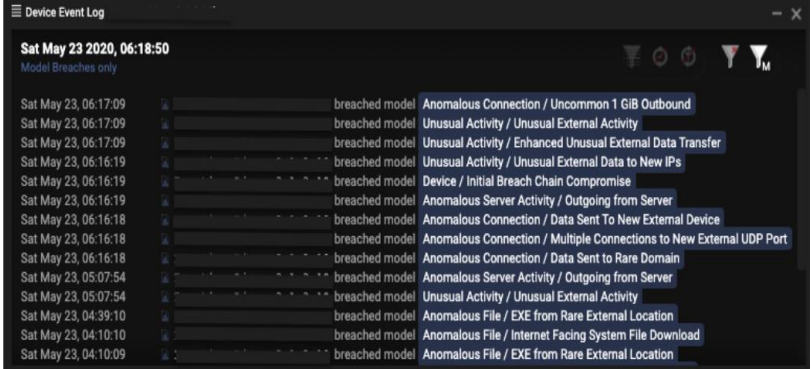
- **Mirai (Malware) Attack and how it is detected (real-time example):**

Darktrace, a cybersecurity company, recently found a major cyber-attack aimed at an internet-connected CCTV camera. This attack was caused by a variation of the Mirai malware, a well-known threat that targets weaknesses in Internet of Things (IoT) gadgets. IoT devices, like internet-

connected cameras, are becoming more common but are tough to secure. They're attractive to cybercriminals due to their easy integration into digital networks.

Even though IoT devices are on the rise, traditional security measures struggle to keep up with new threats. That's where advanced cybersecurity tools like Darktrace's Cyber AI Platform come in handy. In May, Darktrace spotted the Mirai malware infecting a DVR camera owned by a Canadian logistics firm. Although the firm was testing Darktrace's security tool, Antigena, it wasn't fully set up, letting the attack go further than it should have.

When the attack started, regular methods of spotting threats, like open-source intelligence (OSINT), couldn't figure out how the Mirai botnet was structured. But Darktrace's smart AI algorithms noticed odd activities, like strange file downloads and data transfers to unusual places on the network (as seen in the image on the right-figure1).



The screenshot shows a 'Device Event Log' window with a title bar. Below the title bar, it says 'Sat May 23 2020, 06:18:50' and 'Model Breaches only'. The log contains a list of events, each with a timestamp, a status icon, a 'breached model' label, and a description of the breach. The breaches include anomalous connections, unusual activity, and data transfers to rare domains and external locations.

Timestamp	Status	Breached Model	Description
Sat May 23, 06:17:09	breached model	Anomalous Connection / Uncommon 1 GiB Outbound	
Sat May 23, 06:17:09	breached model	Unusual Activity / Unusual External Activity	
Sat May 23, 06:17:09	breached model	Unusual Activity / Enhanced Unusual External Data Transfer	
Sat May 23, 06:16:19	breached model	Unusual Activity / Unusual External Data to New IPs	
Sat May 23, 06:16:19	breached model	Device / Initial Breach Chain Compromise	
Sat May 23, 06:16:19	breached model	Anomalous Server Activity / Outgoing from Server	
Sat May 23, 06:16:18	breached model	Anomalous Connection / Data Sent To New External Device	
Sat May 23, 06:16:18	breached model	Anomalous Connection / Multiple Connections to New External UDP Port	
Sat May 23, 06:16:18	breached model	Anomalous Connection / Data Sent to Rare Domain	
Sat May 23, 05:07:54	breached model	Anomalous Server Activity / Outgoing from Server	
Sat May 23, 05:07:54	breached model	Unusual Activity / Unusual External Activity	
Sat May 23, 04:39:10	breached model	Anomalous File / EXE from Rare External Location	
Sat May 23, 04:10:10	breached model	Anomalous File / Internet Facing System File Download	
Sat May 23, 04:10:09	breached model	Anomalous File / EXE from Rare External Location	

Figure1: Detections of Darktrace[5]

The attack lasted three days, during which Darktrace's AI kept an eye on network behavior, flagging anything suspicious. Through careful investigation, Darktrace's Cyber AI Analyst found the Mirai Botnet-related file, showing that the infected IoT camera didn't have antivirus protection.

Even though the client noticed slower network speeds, they didn't realize the seriousness of the attack until Darktrace alerted them. Acting fast, they disconnected the compromised DVR camera, stopping the attack in its tracks.

While Darktrace's security tool Antigena wasn't fully operational at the time, it could have helped by blocking connections to malicious endpoints if it had been fully set up.

Overall, Darktrace's AI-powered cybersecurity platform did a great job detecting and responding to the Mirai virus attack on the IoT camera. This incident highlights the urgent need for modern security solutions to safeguard IoT devices from ever-evolving cyber threats [5].

## Solutions to Enhance Security:

**Button for Resetting Factory:** This button enables the restoration of a video surveillance system to a predetermined secure state stored on a non-writable memory chip. In case of any system issues or security concerns, pressing this button can reset it to its initial, secure configuration.

**Protected Scan Chains:** Protected scan(or)Secure scan techniques ensure that the surveillance system may be debugged and tested safely, with no risk of possible attackers gaining unauthorized access to debugging features. This method adds an extra layer of security during system maintenance.

**External Validation Process:** External Validation Process (or) Remote attestation is a method for ensuring the integrity of critical code running on the surveillance system. It checks trusted roots to ensure that the system has not been tampered with or corrupted.

**Formal Validation and Confirmation:** Formal proof and verification methods ensure thorough testing and validation of hardware designs, firmware implementations, and security mechanisms. These methods ensure that all surveillance system components meet security standards and operate as expected.

**Adherence to Standards:** Video surveillance systems can improve their security by adhering to software and hardware security standards such as DO-254 and DO-178B (commonly used in aviation). These standards establish guidelines for design, development, and testing to effectively mitigate cybersecurity threats.

**Graphical Interface:** While defending against visual layer attacks is challenging, techniques such as remote attestation and secure firmware upgrades may reduce the necessity for specific visual layer defenses. These broader security measures can address underlying vulnerabilities targeted by visual layer defenses [3].

## **Conclusion:**

In conclusion, this report underscores the crucial importance of addressing security concerns in closed-circuit television (CCTV) systems. While CCTV serves as a vital tool for real-time surveillance and safety enhancement, it remains vulnerable to various attacks, including visual layer attacks, covert channel attacks, and denial-of-service attacks. To tackle these threats effectively, solutions such as factory reset buttons, secured scan chains, and adherence to security standards are paramount. Moreover, the recent Mirai virus attack on an internet-connected CCTV camera highlights the urgent need for modern security solutions to safeguard IoT devices from emerging cyber threats. Overall, by implementing robust security measures, we can enhance the reliability and integrity of video surveillance systems, thereby ensuring their capability to uphold security and safety.

## **References:**

- [1] "What is CCTV (closed circuit television)? - Definition from WhatIs.com," WhatIs.com. <https://www.techtarget.com/whatis/definition/CCTV-closed-circuit-television>. (accessed Mar.20,2024)
- [2] "Types of Security Cameras: A Complete Overview," reolink.com. <https://reolink.com/blog/cctv-camera-types/> (accessed Mar. 31,2024)
- [3] Costin, Andrei. (2016). Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. 10.1145/2995289.2995290.
- [4] K. Boyarinov and A. Hunter, "Security and trust for surveillance cameras," *2017 IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, NV, USA, 2017, pp. 384-385, doi: 10.1109/CNS.2017.8228676.
- [5] "Mirai malware infects CCTV camera | Darktrace Blog," darktrace.com. <https://darktrace.com/blog/mirai-malware-infects-cctv-camera> (accessed Apr. 20, 2024)