White paper

Cybersecurity

Concepts and Terminology

AXIS COMMUNICATIONS

Table of contents

1. Introduction 3
2. Cybersecurity 3
3. Risk assessment 3
4. Threat landscape 4
5. Threat actors and their motivation 4
6. Attack value and costs 5
7. Common organization types and threats 5
8. Risk 6
9. Security controls 6
10. Vulnerabilities and exposures 6
11. Vulnerability scanning 7
12. IP filtering 7
13. Network isolation (network segmentation) 7
14. Network encryption – HTTPS 8
15. Certificate Authority (CA) 8
16. Network access control – 802.1X 8
17. SNMP 9
18. Syslog server 9
19. More information 9

1. Introduction

This document provides a broad overview of cybersecurity concepts and terminology. The content is based on simplified descriptions, models and structures. The target audience are individuals and organizations that want to understand the fundamentals of cybersecurity, with a focus on physical security systems. The document is a terminology and definition reference for other Axis cybersecurity-related documents.

2. Cybersecurity

There are several definitions of cybersecurity. Wikipedia's description refers to Computer Security:

> *Computer security, also known as cybersecurity or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.*

There is no single way to keep yourself safe online. Digital security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats. To become more secure, you must determine what you need to protect and whom you need to protect it from. Threats can change depending on where you're located, what you're doing, and whom you're working with. Therefore, to determine what solutions will be best for you, you should conduct a threat modeling assessment.

3. Risk assessment

The process of risk analysis in cyberspace is like risk analysis in physical protection. In the physical world, it is typically physical things, buildings, and people that need protection. In cyberspace, the asset is information/data and the resources are services. A physical breach is easier to detect, and theft and damage are more noticeable.

Five basic questions when doing risk assessment:

1. What do you want to protect?
2. Whom do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go to in order to try to prevent those consequences?

The ISO 27000 information protection standard talks about asset **Confidentiality, Availability** and **Integrity** (a.k.a. the CIA-triad).

What is the impact if you cannot access your data or services, if your data has been destroyed or if your data is disclosed to unauthorized parties? To assess the impact, data must be classified, because different types of data may differ in value.

ISO classifies data and services as R**estricted, Private** or **Public**. As an example, one video system may classify video system resources in the following way:

> Live video is classified as public. This could mean to the general public, or it could mean to the public within an organization. If the live video is exposed to the public, the harm is limited.

> Recorded video may be classified as **private**, only accessible to a specific organizational unit, because some recorded incidents may be sensitive.

> System configurations, accounts and passwords are classified as **restricted**, only accessible to selected individuals within the organization.

4. Threat landscape

There is always an underlying reason that someone exploits a vulnerability and attacks a system. Attacks can be categorized as either opportunistic or targeted. In cybersecurity, attackers are also referred to as **adversaries** who may either have malicious intent or unintentionally (or accidentally) cause harm to assets.

The clear majority of attacks today are opportunistic attacks: attacks in which there is a window of opportunity. In many cases, opportunistic attackers do not know who the victim is. These attackers will use low-cost attack vectors such as scanning for open networks, services and ports, trying default or common passwords, finding unpatched services, and sending phishing emails. Opportunistic attackers do not have the determination to spend time or resources on a failed attack; they will move along to the next victim. Applying a standard level of protection will mitigate most risks related to opportunistic attacks.

It is harder to protect against targeted attacks, ones that are directed at a specific system and have a specific goal. Targeted attacks use the same low-cost attack-vectors as opportunistic attacks. However, if the initial attacks fail, these attackers are more determined and are willing to spend time and resources to use more sophisticated methods, depending on how much value is at stake. Target attackers often use sophisticated social engineering and spear phishing (a well-crafted email targeting a specific recipient) to gain access to the system. If those fail, they will analyze the system, software or processes to find alternative exploitable vulnerabilities.

5. Threat actors and their motivation

By having some understanding of which actors are the ones most likely to attack, you can gain insight into their probable motives and how much time, resources and determination they are willing to spend, as well as what vulnerabilities they are likely to target.

> **Near and dear** who may want to pry into your personal life.

> **Employees**, or those who have legitimate access, who engage in accidental or deliberate misuse.

> **Pranksters** who find interfering with computer systems an enjoyable challenge.

> **Hacktivists** who wish to attack organizations for political or ideological motives.

> **Cybercriminals** interested in making money through fraud or from the sale of valuable information.

> **Industrial competitors** interested in gaining an economic advantage for their companies.

> **Cyberterrorists** trying to carry out an attack designed to cause alarm or panic with ideological or political goals.

> **Nation-states** (foreign intelligence services) acting to gain economic/political mileage or to inflict damage on critical information systems.

> **Individuals**, a specific person or group acting on their own, where the motivation may differ from the ones listed above. Examples could be an investigating journalist or a white hat hacker. White hat hackers (ethical hackers) may pose a threat if you spend your resources on hiding your flaws and vulnerabilities instead of on fixing them.

6. Attack value and costs

The value of an attack depends on the benefits of a successful breach relative to the cost of the attack. The goal in cybersecurity is to make the cost of an attack outweigh its benefits, thus reducing the value of the attack (value = benefits – cost). To apply an appropriate protection level (establish the attack cost), it is important to know what the plausible threats are. Though every system may be subject to any threat actor or any intention, some threats are more plausible than others. Understanding which threats are more plausible helps identify where to focus security measures (which vulnerabilities are likely be exploited).

7. Common organization types and threats

The negative impact of an attack will typically depend on what type of organization the victim is.

Organization type	**Examples**	**Plausible attackers**	**Impact**
Small organizations	> Consumers > Family business > Non-profit	> Near and dear > Pranksters > Opportunistic hackers	**Individual** level > Privacy > Integrity
Business organizations	> Industries > Corporations > Retailers	The above plus: > Employees > Hacktivists > Organized criminals > Competitors	**Business** level > Money loss > Downtime > Trust > Intellectual property > Competitive edge
Critical infrastructure organizations	> Energy/water > Bank/finance > Telecom > Transportation > Public health > Police/military	The above plus: > Nation-states > Cyberterrorists	**Public** level > Safety > Supplies > Panic

8. Risk

People may have different definitions of the term "risk". RFC 2828 Internet Security Glossary defines risk as:

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

The shorthand version used in many situations is risk = *probability * impact.* This formula is used to prioritize different types of threats. The RFC definition includes the word "particular" to describe threat, vulnerability and harmful result. Each threat should be examined individually, starting with the one that is most plausible and has the highest negative impact.

For each protection type (confidentiality, availability and integrity), it is important to have some understanding of the negative impact of the threat. This task is hard: estimates are in many cases subjective, and the impact is often underestimated. Using the ISO 27000 impact types (**Limited, Serious, Severe** or **Catastrophic**) can help you get a quick overview to help you prioritize. You can think of the impact type as related to the time it would take to recover. Limited = hours/days, Serious = weeks, Severe = months, Catastrophic = years, if at all.

9. Security controls

The process of adding security controls is called hardening. Security controls are safeguards or countermeasures employed to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Compensating controls are alternative safeguards that can be employed when it may not be possible to apply the preferred security control or when the preferred protection may be too costly.

Restricting access and reducing exposure will decrease the system's usability. Striking a balance between system usability and system protection often requires difficult compromises between the needs of the system's users and the needs of those in charge of protecting it. If there is too much restriction, users may find ways to bypass the protection and thus introduce new vulnerabilities. The desired balance between usability and protection needs to be defined by the system owner.

10. Vulnerabilities and exposures

Vulnerabilities provide the opportunities for attackers to gain access to a system. They can result from flaws, features, or user error; attackers may look to exploit any of them, often combining one or more to achieve their end goal.

Research shows that more than 95% of all successful breaches can be ascribed to three factors: human errors, poorly configured systems, and poorly maintained systems. These typically are a result of a lack of adequate policies and defined responsibilities.

A device API (Application Programming Interface) and software services may have flaws that can be exploited in an attack. No vendor can ever guarantee that products have no flaws. If the flaws are known, the risks may be mitigated with compensating security controls. If an attacker discovers unknown flaws, on the other hand, zero-day exploits may occur, not giving the victim any time to protect the system.

Non-critical vulnerabilities are ones that either have low impact or, though the potential impact may be serious, are very hard to exploit. Exploiting a critical flaw may require a number of conditions to be fulfilled; these include having access to the network and the resources it provides.

Common Vulnerability Scoring System (CVSS) is one way to classify the severity of a software vulnerability. It uses a formula that looks at how easily the vulnerability can be exploited and what the negative impact may be. The score is a value between 0 and 10, 10 being the most severe. You will often find the CVSS number in a published Common Vulnerability and Exposure (CVE) report. Axis uses CVSS as one of several measures to estimate how critical an identified vulnerability in the software/product may be.

Exposure also plays a role in determining the risk of a vulnerability. How easy is it for an attacker to exploit the vulnerability? This depends on the infrastructure, service exposure and daily operation.
Example: The risk of a vulnerability may be classified as severe on a public web server serving an enterprise business portal. The same vulnerability could be classified as limited when used in cameras on a local protected network.

11. Vulnerability scanning

Vulnerability scanning is an automated or manual audit of a software or product. There are several such scanning tools on the market. Vulnerability scanning tries to identify services with known vulnerabilities. Such a service could possibly be exploited if exposed to an attacker.

Vulnerability scanning can only find known vulnerabilities. The results are not a good measure of how secure a product is. A new critical vulnerability may be discovered tomorrow. Vulnerability scanning is sometime confused with penetration testing. Penetration testing is when you actively try to bypass security controls. Vulnerability scanning will only identify potential vulnerabilities.

12. IP filtering

IP filtering acts like a local firewall in the camera. In a professional video system, the Video Management System (VMS) is the center of the system. Video clients will not access video directly from the camera: live and recorded video will be supplied to clients via the VMS services. This means that the only computer/server that should be accessing the cameras during normal operation is the VMS server. If the video system is on a non-isolated network where non-video clients may have network access to the cameras, IP filtering can be applied as additional protection. With IP filtering, a camera will not respond to requests from any IP address that is not defined in the whitelist. The whitelist should include the VMS server, the Axis Camera Manager (ACM) server and other PCs (if any) that may be used for troubleshooting and maintenance.

13. Network isolation (network segmentation)

Network isolation is a way to separate critical network resources from each other to reduce the risk of one of them having a negative impact on another. Isolation is particularly relevant for resources that do not need to (or should not) interact with each other. Network segmentation can be virtual (VLAN), which requires infrastructure of managed switches; networks can also be isolated with different cabling and network gear. The type of segmentation to use depends on cost, infrastructure and policies.

A good overall protection is to isolate the physical security network from other (domain) network resources. A firewall between the two segments can be added if video clients on one network need to access the VMS server on the other segment. The firewall should open only traffic between clients and the VMS server, not traffic to cameras.

14. Network encryption – HTTPS

Network encryption protects the communication between the client, VMS, and the camera. It prevents information being extracted by network traffic sniffing, and it prevents data being altered during transfer. Network encryption does not necessarily increase the protection for the camera, VMS, or clients.

Axis cameras supports HTTPS (HTTP over a secure SSL/TLS tunnel). The client (for example, VMS) also needs to support HTTPS. HTTPS will encrypt all administrative traffic (normal HTTP traffic) but may not necessarily encrypt video, as this is transferred over RTSP (Real-Time Streaming Protocol). Encrypting video requires that the VMS also support requesting RTSP tunneled over an encrypted TLS tunnel. Not all VMS supports this: check with the VMS vendor. Before HTTPS can be established, the camera needs to have a certificate (self-signed or CA-signed) and HTTPS policy needs to be set.

15. Certificate Authority (CA)

Whether self-signed or CA-signed certificates are used makes no difference to the encryption level. The difference is that self-signed certificates do not protect against network spoofing (situations where an attacking computer tries to impersonate a legitimate client or a server). CA-signed certificates add a trustpoint for a client to authenticate that it is accessing a trusted camera. CA-signed certificates are used for both HTTPS (**server certificates**) and 802.1x (**client certificates**).

Public vs. Private CA

Publicly trusted CA, such as Comodo and Symantec (prev. Verisign), is typically used for public services such as public web sites and email servers. The CA root certificate for publicly trusted CA is pre-installed in most operating systems (Windows, Linux, Mac) and browsers.

A private CA is a trustpoint for internal/private network services. A private CA is a software/server (typically Active Directory/Certificate Service) that is used to issue certificates for all internal clients and servers. The private CA root certificate needs to be installed in all clients that access private resources. The certificate deployment can be manual or automated, depending on available tools and infrastructure.

16. Network access control – 802.1X

IEEE 802.1X is a standard designed to prevent unauthorized network devices from accessing the local network. Before a device is allowed access to the network (and its resources), it needs to authenticate itself. There are different authentication methods that can be used, such as MAC address (MAC filtering), user/password, or client certificate. The system owner decides which method to use; the appropriate choice depends on threats, risk and cost.

Operating an 802.1X infrastructure is an investment. It requires managed switches and additional servers, typically a RADIUS (Remote Authentication Dial-In User Service). Using client certificates requires a CA (private or public) that can issue client certificates. In most cases the infrastructure needs personnel to maintain and monitor it. If the end user does not already have 802.1X infrastructure in place, it is unlikely that this will be added when a network video/security system is added. A compensating control that can provide an alternative to 802.1X is network isolation to reduce exposure of different critical network resources.

17. SNMP

SNMP (Simple Network Management Protocol) is used for collecting and organizing information about managed devices on IP networks. Using SNMP to monitor cameras may help detect camera malfunction as well as disconnects that may indicate a possible attack.

18. Syslog server

All cameras have an internal log that logs all operations in the camera. This log may be lost if the camera is rebooted or be wiped or modified by the attacker when an intrusion attack is successful. A remote syslog server can collect all camera log messages during daily operation. Having a remote syslog server secures the logs; this may simplify troubleshooting or forensic investigation to find abnormalities and traces of intrusion.

19. More information:

www.axis.com/support/product-security

> AXIS Vulnerability Policy

> AXIS Hardening Guide

> Security advisories (CVE)

> White papers

www.axis.com/learning/online-courses

> AXIS Academy training on cyber security

www.axis.com/blog/secure-insights/category/cyber-security

> Various topics on cyber security

70711/EN/R1/1706

About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

Axis has more than 2,700 dedicated employees in more than 50 countries around the world, supported by a global network of over 90,000 partners. Founded in 1984, Axis is a Sweden-based company listed on NASDAQ Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.

AXIS COMMUNICATIONS