Just how secure is your video surveillance?

Why do I need video surveillance ?

What methods are currently used?

Or:

Why we should pay more attention to security in video networks.

Do I need video security? What methods are currently used?

Or: Why we should pay more attention to security in video networks.

We constantly observe during visits to our client sites that users have taken no security precautions in their video networks. We see standard passwords, DHCP settings, unprotected open networks and much more. It should not take the recent large failure at the German Telekom to reveal that an inadequately protected IP network is exposed to risks.

No professional IT network is run without virus scanners and firewalls. IT departments have learned, at times to their own high cost, just how important security in IT networks is. However, we seem to consider ourselves to be very secure in the area of video over IP. Existing security settings are simply disregarded and not configured. Security updates on cameras are ignored and service contracts that could seal precisely these gaps continue to remain rare in German IP networks.

It can often be misleading to believe we enjoy security – something we want to explore in greater detail in this brief report.

There is a wide variety of methods for attacks on camera systems. The most common problem – and the one that is easiest to remedy – refers to unchanged password settings.

Effects of unchanged standard passwords

The internet page https://www.insecam.org alone offers more than 600 exposed cameras with live video transmission in Germany. These transmissions include everything from views of companies, city surveillance, private residences, horse stables, garages, offices, shops, etc.

Estimates claim that the standard password has not been changed for more than 60% of all video cameras. This shortcoming makes them very easy to manipulate.

As original examples from the Internet demonstrate, the IP cameras can be seen by anyone and can be directly accessed over the internet .

For example, cameras that survey a public area without explicit permission can be accessed over the internet. The video data can then be legally viewed on the web, the user can in the worst case even be targeted for large penalties by lawyers for filming in the public arena.

Any potential offender can see exactly when offices in a company are vacant and, in the easiest possible manner, discover through spying on habits and working hours practised in a company or shop, or the regular behaviour in private residences; in this way exploit the best time for carrying out a burglary or raid with minimum risk.

Cameras may even show on the internet the precise location of alarm areas covered by the cameras. Lurking offenders then know exactly in what area of the camera image an alarm is generated and, even more importantly, where they are not triggered.

These are only a few example of how careless video security is treated in some cases today.

Even more critical are instances of video data from the private sphere (from apartments, gardens, swimming pools, etc.) becoming public. Nobody wants to be filmed when at home on the couch or when engaged in other private matters.

And there are even further gaps in security that can be exploited.

What happens if unauthorised individuals obtain access to a video camera?

A variety of scenarios are possible. First of all, a security camera should of course increase the security in areas requiring protection. If a stranger now obtains unauthorised access to the camera, it can be switched off, manipulated or transmit misinformation and the interloper can carry out attacks on the entire network through the camera link.

This problem was very unlikely to occur in the "old" analogue world since we already had a high level of security provided by separate networks (generally in the form of coaxial cables or two-wire connections) and tapping and manipulation of data was (and is) very difficult.

The ever-growing proliferation of IP cameras makes the need to protect camera systems and the underlying network more and more important as knowledge regarding attack methods is becoming easier to obtain, especially over the internet. Similar developments were and can still be observed for some time now in the case of PCs and smartphones. Moreover, extended analysis and evaluation applications on cameras are making them more and more crucial in the control of processes, machines and alarms (for example, in monitoring for occurrences of smoke, entry control systems, etc.).

Possible effects on IP cameras:

1. They can be attacked over the IP network
2. The IP access on cameras can be used to infiltrate the IP network
3. Wireless LAN cameras can be attacked through the WLAN (wifi) network
4. Video data can be manipulated
5. Network-relevant data can be read out (IP addresses, gateways, server data, databases, domains, etc.)
6. Cameras can be equipped with so-called backdoors that enable manufacturers, security agencies or hackers to access them and consequently also to the network

Who is interested in such data?

We regularly hear from our clients that they believe their video cameras are of little relevance to outsiders and that therefore there is no danger associated with the IP cameras. However, it should be noted that cameras can indeed also indirectly provide vital information. The following proverb comes to mind – opportunity makes the thief! Attacks do not necessarily always have to be planned. Information could also leak to the outside world by chance, thereby facilitating attacks.

In this way, unprotected cameras provide the opportunity to very easily research local conditions from the anonymous internet without having the person to be actually present at the site.

Information from a camera	Conclusions from the information
People still in the building	When is the best time to break in? When is the security staff in the building? Are there times when it is less risky to break in? (the person goes to work from ... to ...)
Shop monitoring – Shelves	Where will I not be recorded when stealing? Where are there gaps in the surveillance network?
Shop monitoring – Cash desks	How can cameras be manipulated in such a way that they cannot record possible fraud?
Warehouse monitoring	Are loading bays and ramps monitored? Call all areas be viewed? Where can goods be brought outside without being seen (e.g., unsupervised doors)?
Outside area	Is the entire entry area monitored? Where are the most open entry areas? Can cameras be moved to record false information? Manipulation of the camera during security circuits
IT area – Server room	When is staff present in the computer centre? Can important access information be viewed by the video camera (e.g., what systems are used, reading passwords when entered, information on servers using applied IP address, passwords, etc.)

Examples of how hacked cameras can be used

Danger does not always have to arise directly from the anonymous internet or from globally connected secret services. Unfortunately, it is often the case that frustrated employees or former staff members are persons wishing to take revenge on a company for perceived bad treatment. Or information may be relayed to customers, suppliers, contracted service staff, etc., etc.

There are also other hacking opportunities exposed by IP cameras:

Every IP camera is a client in the network

Since cameras are located in the network just like any PC or client and have their own IP addresses, they also represent possible points of attack on the local PC network. Each camera must be considered to be a client or user in a network and can, like any other device in the network, be attacked. This means that attacks on every server, PC or user in the network are possible from here.

Errors in a camera's operating system

IP cameras are nowadays miniature high-performance processors with their own operating systems and software for image processing. Potential software errors and security gaps in the software of a camera can be exploited to launch attacks on the camera. For example, it was only recently discovered that a software error (or was it a deliberate mechanism?) for a well-known camera manufacturer allowed control of the camera to be hijacked.

Backdoors through video cameras

Backdoors (also known as *trapdoors*) refer to parts of software (often introduced by the author) that enable users to avoid the standard access security control to obtain access to a computer or IP camera or to an otherwise protected function of a computer application – e.g., video management systems (VMS).

It only emerged recently that the world's largest manufacturer of IP video cameras is alleged to have built a backdoor in its' cameras that enables the manufacturer, and also the national secret services, to access any of the manufacturer's cameras anywhere in the world (provided it is located in a network with internet access).

See (article from 24 November 2016 newsgram):
http://www.newsgram.com/imagine-a-world-whereeveryone-can-be-tracked-is-the-worlds-biggestsurveillance-camera-maker-sending-footage-to-china/

Manipulation of video images

Access to camera technology of course means that the associated video data can also be manipulated and altered. For example, presets (specified views that can be configured by a camera for security circuits) can be changed and areas completely removed from surveillance, activated alarms may no longer be transmitted and image data can be altered (e.g., blurred). Generally speaking, it takes some time until changes of this nature are noticed by users since the camera continues to function normally. However, this can already be too late.

Attacks on management software/recording solutions

Video management systems implemented as software solutions are becoming more popular since only a simple, cost-effective PC/server is required. The software is often also offered free of charge for small expansion stages of up to 15 to 20 cameras, meaning that a functional system can be obtained at a very attractive price.

Management of the system is very easy as the know-how for server-based systems (usually Windows or Linux) is available in the user's own IT department. Unfortunately, the security system will also have become more susceptible to hacking since security flaws in the operating systems are often published on the internet and can be easily exploited by perpetrators. Decentralised systems (i.e. recording takes places in branch offices) also encounter the following issues:

- They are not equipped with the appropriate security software.
- Updates are only performed inadequately or never.
- Compatibility conflicts with the monitoring software may occur in the case of automatic backups that then go undetected.
- There may be no or only insufficient backup processes.
- Some processors may be integrated into the corporate network, thereby facilitating direct access to all key company data.
- Different applications might run in some cases on the same system.
- The applications and video data are stored on one processor.

What needs to be changed to obtain a secure video network?

Protective measures are always essential in video monitoring systems and should be urgently incorporated if they have not already been planned in advance to the appropriate level.

Unfortunately, the vast majority of camera manufacturers, specialist companies and integrators are today not equipped to deal with all possible threats and also fail to inform their customers adequately.

- For example, video data continue to be almost always transmitted in unencrypted form over the network.
- Access by unauthorised processors, persons, etc. is not detected.
- Changes in the network structure, camera configuration, video image data, etc. cannot be detected or only too late.
- Encryption methods are not offered at all or only in OpenSSL form.
- Passwords remain in their default setting or are entered in simple form like "1234" or "Admin/admin".
- Video data are stored in unencrypted form, making access easy and enabling the data to be manipulated or deleted.
- An absence of virus protection means that viruses, trojans and other malware are not detected.
- Security updates are not adequately carried out.
- Cameras run for years without updates and as a result open up gaps in security.

Our recommendation

1. Immediately change the standard password when setting up a camera.
2. Notify users of update options or agree to a service contract that includes the necessary regular software and security updates.
3. Encrypt all data transferred between camera, recorder and VMS.
4. Install a virus scanner in all video systems to detect changes in the network without delay (install scanners in all other IP systems too, of course) in order to detect and eradicate possible threats.
5. Check the firewall policies, open ports, etc., also in regard to your video systems.
6. Use data verification to detect changes in your network.

What can i-PRO offer you for video security?

We at **i-PRO** have been considering for many years how we can offer our customers a solution to safeguard their security systems and to detect and eliminate possible deficiencies.

With the latest generation of our camera systems customers now have the opportunity – at no extra cost – to protect their security network against dangers in the network.

i-PRO provides the following features:

1. New cameras are configured with password protection that no longer allows the cameras to be operated with the default password.
2. Data transfers between cameras, recorders and the VMS are fully encrypted.
3. Certificates are supplied to customers who have encapsulated source code (refer to the list) that enables very fast data encryption (17 ms in comparison to OpenSSL with 43 ms).
4. Recorders with a hardened operating system are used that does not automatically download the latest software version during Windows updates, but can instead act independently of Windows and Linux systems.

Advantages of the i-PRO encryption:

Application	OpenSSL	i-PRO SSL	Strengths
Source code	open	close	safe – cannot be attacked
ROM	1,310 KB	162 KB	approx. 1/8 of data volume
RAM	2,400 KB	40 KB	approx. 1/60 of data volume
Encrypt	43 ms	17 ms	approx. 2.5 times faster
decrypt	1450 ms	683 ms	approx. twice as fast

Comparison between OpenSSL and i-PRO SSL encryption

Features offered free of charge in cameras and systems by i-PRO:

1. Data encryption
2. Encrypted communication between cameras, recorders and video management systems
3. Monitoring for changes in data networks
4. Analysis of weaknesses in networks

Very secure communication of IP video surveillance is made possible in this way, giving hackers no capability to access your data.

Akihiro Nawata

Manager, SoC Module Development

The Power of Truth

4-1-62 Minoshima, Hakata-ku, Fukuoka-shi, Fukuoka, 812-8531 Japan

i-pro.com/corp/jp/