Data Transmission in local wired computer networks (p. 3)

Krystyna Szczepaniak

Risk Related to IP Technology and Active Attacks on Network Devices

Tomasz Polus *(tpolus@polvision.com.pl)*

The future belongs to network technologies. The future of CCTV systems is connected with IT technologies. Network cameras have their own operating systems, built-in IP servers, signal processing software, and operating memory; they are real network devices – just like computers. It sounds fantastic, but are we really aware of what will come after implementing IP technology?

These are just a couple of quotes from recent TWIERDZA issues to support the assertion that IP technology is the inevitable future. In these articles I found mainly delight and admiration for IP and I generally agree that we should spread this magnificent technology and not only within the CCTV industry and security systems. However, I cannot ignore the impression I have that people who encourage others to use these solutions are not fully aware of how complicated and sometimes expensive the path is which they lead their customers down.

Technical support for network devices

Reading such articles can bring a small pitying smile to the face of someone who has administered advanced IP devices on a day-to-day basis for a couple of years. Frequent mistakes related to basic IP issues arouse suspicions that companies offering these solutions lack proper technical, IT-related support. A good example of this is an article on some network devices that can be remotely managed with the use of a special application. This application is supposed to work: “on the basis of standard management protocols (SNMP, HTML or TelNet)”. SNMP and Telnet are indeed standard management protocols, somewhat obsolete, but popular and well known to computer intruders... But what about HTML? This is a language describing a WWW page layout, not a management protocol! Perhaps the authors meant HTTP (Hyper Text Transfer Protocol) and these are just two small typos... Fine, but why are those typos repeated so often in the article?

Being interested in this topic, I began an intensive search for substantial information on the security of IP solutions and most of all on the security of the proposed network devices. I found nothing except some magic phrases, such as “data encryption”, “virtual private networks”, “firewalls”, which when applied to the IP security environment mean something similar to “access control” in the physical security environment.

What’s worse, none of these articles contained reliable information about technical support for network devices... If network cameras do have: “their own operating systems, built-in IP servers, signal processing software, and operating memory;” and they are “real network devices – just like computers”, then they will soon require technical support similar to that needed by typical servers and computer network devices. The more so because companies which offer these devices boast about (and recommend) integrating them with the existing IT infrastructure, for example with enterprise computer networks (but nobody mentions that they should be connected to separate networks for security reasons!). In the IT environment everyone knows perfectly well that a computer system (and especially a network system) cannot work unaided by qualified technicians. Sooner or later, for different reasons, a system failure occurs and searching for the cause may require specialist knowledge of the field of

Fig. 1. Message reporting serious error in operating system kernel.

data transmission in IP networks. Resetting network devices is usually enough, it is true. But which devices..? In advanced network systems there are such complicated devices as managed switches, routers, bridges, VPN servers, complex network cameras, digital recorders (as we know, most of them are just normal computers with suitably large disks and special software). Who can determine which of these devices is responsible for the lack of signal from an IP network camera? Maybe resetting the camera will help? Its operating system might be suspended – as we know, all software contains some errors and, as one of the most complex and demanding parts of a computer system, it doesn't always follow the programmer's intentions...

All these devices have their own operating systems, working on different hardware platforms, which require expert administration (not control) knowledge. It's not so bad if all the devices used in a network come from the same manufacturer, because manufacturers usually implement only one type of operating system, whose hallmark is a uniform user interface. In such a situation the training of an administrator of the system is not very expensive or time consuming. Unfortunately, from what I can see in the offers and articles, it's clear that there is a lack of generally accepted standards – almost every manufacturer offers their own devices and software. In practice, this means that a customer without technical, IT-related support or without at least one trained network administrator, will be left alone in the event of a failure and won't be able to repair such a complex infrastructure. It also means additional high costs for that customer. For the same reason big companies maintain their own IT departments which employ and train many administrators, but what about small and medium-size ones?

Security of IP network devices

One should remember that the big possibilities offered by IP technology are connected with high risks. It is generally the same sort of risk we face dealing with IT systems. If network cameras are small computers with their own operating systems (IP servers), and if digital recorders are not very far from being typical computers and the whole security system is managed by one main computer, then I can see unlimited possibilities for computer intruders. The knowledge of all types of attacks, server intrusion techniques and of IT in general will soon be useful in a new field – in security systems and monitoring based on IP technology. The future – now to be seen only in the movies – when an intruder, armed with advanced knowledge of the system and a laptop with special software... will tackle all sorts of electronically controlled means of physical protection – is not as distant as it may seem... "The future belongs to network technologies" – yes, this is unavoidable: but it is worth holding on and trying to realize what waits for us beyond these new technologies and what threats are inseparable from them.

In the first part of this article I tried to present the details of the most important processes and definitions related to data transmission in local wired computer networks, especially those concerning transmission security issues. The aim of the second part was to lift the discussion to a higher level about understanding the potential threats that result from using network technologies based on IP protocols, as well as to present the most important and most dangerous sniffing methods. This portion of information was followed by some recommendations concerning issues related to protecting an IP network from being sniffed by intruders. I'm afraid, however, that making practical use of these tips would require much more technical knowledge than I have been able to pass on in these few pages. That's why, in this part of the article, I decided to spare the readers any complex and – in fact – boring details of various methods of network attacks. In my opinion, if a company places its hopes on the high security level of its IP network, then it is necessary that they employ an experienced network administrator (having experience in securing data transmission with the use of IP protocols is extremely important), or hire a company which will secure the network and data transmission (for example by installing and configuring crypto accelerators at important network nodes), choose the right devices (and proper software), provide technical support and, the most important thing, keep computer intruders at bay.

Active and passive attacks

In network security terminology sniffing is called a passive attack, which means that it is not used to get direct access to the system. It is more like gathering as much information about the system as possible, without interfering with its functionality. For that reason passive attacks are much more difficult to track, in comparison to active attacks.

The definition of an active attack assumes a much broader range of the intruder's activities. It encompasses so-called "denial of service" attacks, spoofing and taking control of system and network resources, i.e. operations finally leading to a compromise of the system's security.

Attacks through software vulnerabilities

Software vulnerabilities are detected mainly in network services (for example in WWW servers, just like in some network cameras) and in network operating systems (just like in digital recorders). The most common vulnerabilities allow attacks through buffer overflow. For example, a programmer allocates 100 characters for a username, assuming that it will never be longer. An intruder tries to predict what will happen to the program if he enters a longer username. It turns out that if the programmer didn't obey the fundamental rules of secure programming, then, after sending more than 100 characters, the system may incorrectly execute the operation of authentication, executing also the commands included in the excess data, and reset the device or constantly use the entire processor resources, blocking any other operations of the device. If the intruder is incessantly sending the same data to the device, the constant resetting and blocking will make its normal operation impossible.

Another time, an intruder may also supply incorrect data to the application program servicing the device and make it work in a way that is different to how its maker ever expected. It would be a typical vulnerability to input incorrect data. Some programs are written in such a way that incorrect data is rejected and corrected. Unfortunately, programmers often forget about the necessity to add a special code to block the incorrect data, which means that the vulnerability remains.

One example of a lack of security tests and of the rules of secure programming being ignored was the software previously used in a network camera supplied by one of the leading manufacturers. In the first half of 2003, the company dealt with two serious vulnerabilities of their software. The first allowed an intruder to get full access to the administration panel of a device, by using a very simple password “pass”, while the second resulted in the same outcome without any password, just by adding a second slash in the camera network address (see fig.2).

WWW servers are the network services which are most vulnerable to those kinds of attacks (and the most frequently attacked). Providing an appropriate security level is a good topic for a separate publication. Many providers boast about their devices, equipped with built-in IP servers (it is usually a WWW server, based on a specially adapted Linux operating system), which may be controlled via a normal internet browser... Fantastic and very comfortable, but why there is no information about the risk that is inseparable from this comfort?

Creating secure software will remain a dream until someone finds new programming methods (if indeed they ever do). In the case of software destined for PCs,

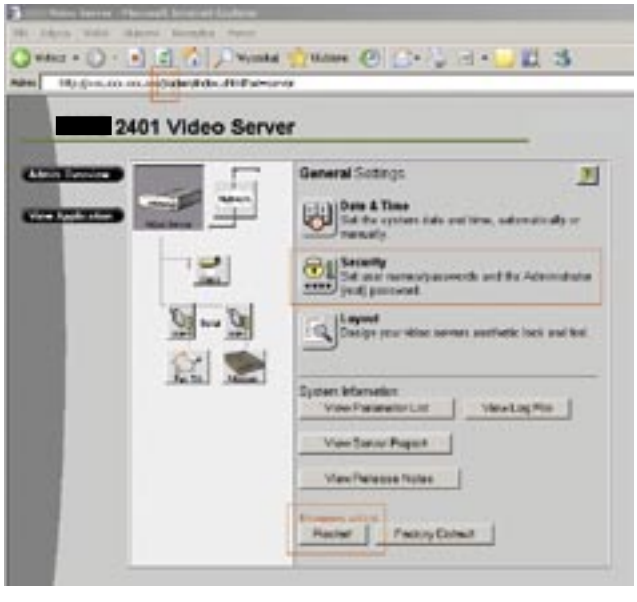

Fig. 2. Screenshot of the administrating panel of a network camera, illustrating a vulnerability which was discovered in 2003 and promptly eliminated by its maker. It was found that it could have been accessed without logging on, by adding a slash in a network address. The options, then accessible from the screen, are marked: the possibility to manage user accounts and to reset the device.

Fig. 3. Intercepted user logon session to network camera WWW server and a fragment of HTTP protocol session from the intruder’s point of view (marked user name, password and WWW server name).

most providers prepare and offer free software updates, which can be downloaded from the Internet and installed on the system, in order to eliminate vulnerabilities found in the application’s security subsystem. The same can be achieved by deleting application programs or system components, containing a dangerous vulnerability. Of course it’s only possible under the condition that they are not necessary for the system to work... In the case of network devices, the problems are that usually all the components of the installed software are necessary for its proper operation, and that this software might never be updated by its provider. Sometimes, if a company is extremely serious about the security of its products, then, shortly after the vulnerabilities are detected, it creates special updates and makes them available from the company website. An excellent example of this was the way that the company mentioned earlier in the article immediately equipped their customers with updates following the detection of the previously mentioned vulnerabilities. But there are many companies that don’t care so much about security, so watch out...

However, even if the manufacturers of these devices make the updates to their products publicly available, it usually means that a special program, which allows the user to get access to the read-only memory of a device in which an operating system is found, also becomes publicly available. Unfortunately, an intruder can use the same program to modify the system, not necessarily according to the manufacturer’s recommendations...

Let’s imagine a situation where someone buys a popular network camera, tests it for a very long time in a private laboratory and, in the end, finds a vulnerability in its software (it is only a matter of time, as there is no functional software which is entirely free from vulnerabilities). That person doesn’t inform anyone about their discovery and possesses a powerful weapon, allowing them, once they’ve got access to the IP network, to attack all devices of this type in their own way, causing results that are difficult to foresee, but surely adverse from the point of view of network security.

"Denial Of Service" attacks

The number of operations, which may be processed by a network device, is always limited by factors such as the amount of random-access memory, computing power, disk space, connection capacity, as well as the capabilities of the installed software. Making use of these obvious facts, intruders have worked out a special method of attack called Denial Of Service (DoS). Such an attack is an automated, long-lasting process of sending the same information to a network device, time and time again: for example, an instruction to read or search for the same data, or to write some new bogus data. If the number of requests is high enough, the device's resources will run too low and it will stop servicing other requests from legal users and devices installed in the network. The aim of DoS attack is to prevent normal operation of services in the network, for example to quickly fill up the recorder's hard disks or to significantly slow down the work of an IP camera so that it is not able to transmit video in real time.

A very dangerous type of DoS attack are those aimed at important IP network nodes, for example routers or switches, because to stop them it is necessary to block some parts of a network.

One of the most common DoS attacks is resetting a connection. The operation consists of constantly sending false network packets, containing information about the termination of the connection, to both its participants, e.g. a network camera and a computer. This way an intruder can constantly block the communication between the operator and the camera, making them unable to receive video signals or to send control signals.

Network devices are usually designed to simultaneously service as many clients as possible. They are equipped with powerful processors, large amounts of memory, large disks, high capacity network connections etc. If an intruder is not equipped with the latest technology and if the capacity of his network connection is not higher than that of a victim, the "blockade" is practically impossible.

Unfortunately an intruder may also perform another, more dangerous type of DoS attack – a so-called DDoS (Distributed Denial Of Service) attack. The difference is that DDoS attacks are not carried out from single computers (whose network connection and hardware resources are usually too weak when compared to the resources of the attacked network device), but from many computers simultaneously. Involving a suitable number of previously compromised computers, intruders are able to block any network device, preventing it from servicing normal requests.

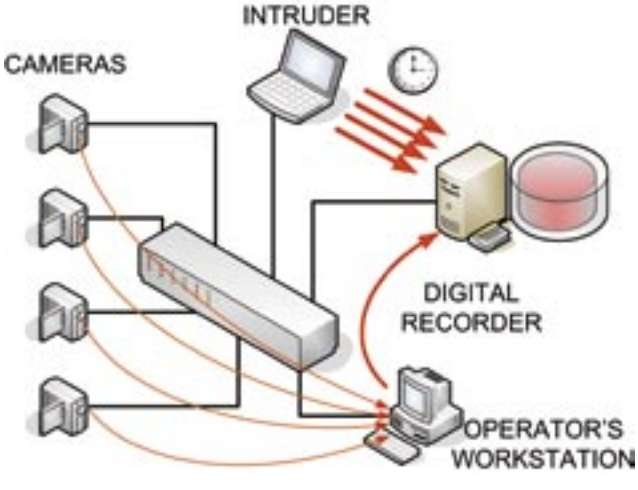

Fig. 4. „Denial Of Service" attack means constantly sending large amounts of data to be written to the digital recorder's media in order to fill them up and to block archiving processes.

Let's imagine a situation when an intruder starts sniffing an IP network, recording all communication. After some time they know the protocol used for communication between the network devices and for recording the video data to a digital recorder. The intruder prepares a special application, which may be used to automatically send data to the recorder, in compliance with the transmission protocol. The program will automatically generate data and send it on in a loop, so after some time all the hard disks of the digital recorder will be full. Taking into account the capacities of today's hard disks (for example 250 GB), and assuming that they use intensive transmission via a 100 MBit/s network, that kind of storage media may be filled up in a couple of hours. Even if the recorder automatically deletes the old data, there will be no proper archive, so its usefulness will be equal to zero...

Brute force attacks

In network devices equipped with network software, the access control at user level is usually realized by logon mechanisms using such credentials as username and password. What's more, network devices are usually installed with passwords already set by the manufacturer (or even without any passwords) to make the first configuration possible. Of course, these passwords should be changed immediately after the installation, but not everyone complies with this recommendation, because it makes access to the device more difficult. However, even if the administrator has defined new passwords after the installation, they can be cracked.

In the IT environment one of the most popular and effective methods of cracking passwords is the brute force method. An intruder tries to log on, using different combinations of alphanumeric and special chars until a password is accepted.

The efficiency of the "brute-force" method is highly dependent on the password complexity. Assuming that the password consists of 6 chars, which can be capital letters (26), small letters (26) or digits (10), then there are 62 possibilities for every char of the password and 626 possibilities for the whole password. A computer equipped with a 500 MHz processor (today popular PC computers, even laptops, have 2 – 3 GHz processors), cracks that kind of password in 3 months. If the string additionally contains some special keys (for example ~, @, #, <, >) (22 altogether), cracking that kind of password would take about 2 years. In spite of this, the brute-force approach is still one of the most popular methods of cracking passwords. The main reason is the fact that users think of simple passwords, using the names of their spouses, birth dates or telephone numbers. Yet they shouldn't be blamed for this situation. If they lack the necessary knowledge to choose an appropriate password – it is the security officer's fault.

Fig. 5. Intercepted user password and a fragment of a Telnet protocol session from the intruder's point of view.

Sessions hijacking and spoofing other devices

"Sessions hijacking" and "spoofing other devices" – these terms must sound unreal for someone who has no experiences with IP network security. They are real, though. In the world of computers and IP protocols everyone can put on a mask, hide, spoof their identity, and take over control... The good news is that these operations are very complicated – only experienced intruders are able to carry out such attacks. They must have extensive knowledge of network protocols and skills to create their own software, adjustable to the task of attacking a particular system. The bad news is that there are many new specialist tools which are designed for automatic session hijacking and spoofing, and compatible with the previously mentioned management protocols: SNMP, Telnet or HTTP. It is common knowledge that, because of the full availability and simplicity of these tools, even a beginner can pose a serious threat to the security of the system. Yet the final success of such attacks mainly depends on the level of the intruder's experience on one hand and on the level the of IP network security on the other.

It's obvious what can be achieved by spoofing other devices and hijacking session, but let's have a look at an example. Network access control is often based on the verification of IP addresses of communication partners. For example, if a computer's IP address is not registered on a network camera's list of authorized client devices, the connection will not be established. Yet even in such situations intruders are not helpless – they must make a lot of extra effort to spoof their identity and disguise themselves as an authorized device, that is, to start using its IP address. The simplest method would be to use the same IP address that is set on an authorized device. This, however, due to some characteristics of IP and ARP protocols (see the earlier part of this article, TWIERDZA 6 (31) / 2004) would in practice mean recurring communication problems, as the authorized device would either lose its network connection or the responses from the camera would go to this device instead of to the intruder's device. Moreover, it could be quickly detected in the network, because the victim's device would terminate its normal network operation. There is, however, another method (also described in the previous part of this series). An intruder can assume the role of a mediator in communication between two legal devices, so that the whole network traffic between them is directed by the interfering device. The traffic, as a whole, remains unimpaired in the sense of the system's operation, but it can be modified on a real time basis, by a specially prepared application, in a way that depends on how a given protocol is implemented. For example, while maintaining full communication between the authorized device and the camera, the intruder can add their own commands to the data stream, in order to supplement the list of authorized devices stored in the network camera's memory with a new network address. Then, the attacker can use this new address unseen by the system operators and without the need to disguise themselves.

Another example can be hijacking a Telnet protocol session, which can be used to manage network devices in many systems. Telnet is based on TCP protocol, unlike SNMP, which is based on UDP protocol.

The logic of TCP protocol makes hijacking sessions a difficult task. The reason is that it is, by intent, a reliable protocol, which means that no data is supposed to get lost in the network. Consequently, a special mechanism, designed for confirmation of TCP segments transmission, was built in the protocol, which, combined with sequence numbers, makes it very difficult to spoof computers participating in communication, or to hijack sessions. Nevertheless, everything is possible in IT, so, if there are programs able to "sniff" network transmissions, nothing stands in the way of using the data, gathered in this way, in order to hijack a session.

If the sequence numbers of TCP segments get captured, it is likely that a Telnet session will be hijacked when a user has already been authenticated by the device's operating system. This way the intruder would take over all the privileges granted to this user, which usually means taking full control of the device.

UDP, on which, among other things, the operation of SNMP protocol is based, isn't assumed to be reliable, which means that it is a very simple type of protocol. Forging UDP packets in order to hijack sessions and to spoof identities is, unfortunately, a lot easier than in the case of TCP...

Summary

I hope the readers have found the series, which is concluded by this article, to be a graspable account of processes occurring in network devices, during data transmission performed over a wired computer network, based on Ethernet and IP standards. I would also like to emphasize that I am not against using IP technology – on the contrary, I believe that this is the only proper direction for research and the further development of CCTV, security systems and more. I am intent, however, that the providers and users of IP network devices, who benefit from IT solutions, be aware of the threats related to the potential misuse of these technologies by intruders.