

Internet Security Systems: a View on Global Cyber-Security

Two of the more notable characteristics of contemporary society are the vast amounts of available information and the growing demand for effective and continuous connectivity. It is therefore no surprise that usage of the Internet has grown incredibly over the last several years, some estimating that there are nowadays over 1.4 billion users worldwide, almost quadruple the number of users in 2002. However, as in many other fields which developed greatly over a very short time span, crime is not far behind, targeting the entire range of possible connected systems, from private computers to sensitive governmental networks, not skipping over corporate networks, etc. And indeed, damage ranges from millions of annual cases of online identity thefts, through countless corporate network breaches resulting in great financial damage, to attacks affecting national infrastructures, e.g. city power outages caused by cyber attacks.

What is on the Market

It therefore comes as no surprise that the computer security market is flourishing with countless security solutions such as firewalls, intrusion detection systems, intrusion prevention systems, VPNs, etc. Unfortunately, none of these solutions can guarantee complete security. Firewalls, for example, are hacked on a daily basis, while intrusion detection and prevention systems mainly identify (previously) known attacks and are vulnerable to "zero-day" attacks. Moreover, many IT security systems suffer from inaccurate configuration and lack of timely security patches and updates. While such risks may be reasonable as far as a home user is concerned, this is not the case when classified, commercially sensitive, or mission critical networks are at stake. In such scenarios a foolproof and future proof solution is mandatory, as the risks are otherwise simply too high.

Unidirectional Connectivity

Unidirectional connectivity is the only technology that can provide such guaranteed protection for computer networks. This novel security concept enables information to flow

strictly one-way, from network A to network B, and not vice versa. The solution thereby eliminates any possibility of online attack against the secured network or the possibility of unlawfully extracting sensitive data from it. A unidirectional communication system must enforce its absolutely unidirectional data flow by means of physical hardware, as opposed to software. This is realised by using a system which is comprised of two hardware components, physically capable of communicating one-way only: one component can only transmit to the other, and not vice versa. This is accomplished by connecting the two components via fiber optic cable, with the transmitting component having only a transmitter (e.g. laser LED) and the receiving unit having only a receiver (e.g. photoelectric cell). In such a way data is strictly restricted, at the physical layer, to flow only from the transmitter to the receiver. To facilitate reliable data transfer, a unique communication protocol must be implemented. This protocol also adds another layer of security by allowing transfer of the payload data (raw data) only, stripping it from other protocol fields, which are also known to facilitate certain forms of attacks.

Possible Scenarios

Critical National Infrastructure (CNI) Facilities

This security concept of unidirectional connectivity can serve in a large variety of scenarios. A typical situation where such connectivity is perhaps the most useful is when there is need for secure remote monitoring. For example, critical networks, such as those serving Critical National Infrastructure (CNI) facilities, are many times kept completely segregated from the outside world in order to maintain their security. However, most of the equipment residing on these networks must be remotely monitored from a control center or a 3rd party facility - this is the case in production related equipment, and today also in general network and IT products and appliances. This is where unidirectional connectivity is the optimal security solution, as necessary data can be transferred from the CNI network to the

remote control center, or any 3rd party facility, through a one-way link. Whereas the possibility of carrying out monitoring is thereby not impaired, there is no risk of online attacks against the CNI network from external sources, as the one-way link provides no inbound path to this network.

Disaster Recovery Plans

Similarly, deploying a unidirectional link would seem equally efficient when there is need for remote infrastructure management, for example in remote management of computer networks for verifying ongoing functionality or for carrying out a comprehensive backup scheme as part of a DRP (Disaster Recovery Plan) policy. Here too, data can flow one-way from the monitored environment to the remote management center, with no possible threat of online attack on the monitored network or data leakage from it.

Physical Security

A third typical remote monitoring scenario is that of physical security, i.e. remote sensors such as IP video surveillance cameras transmitting data to the control room. Whereas the communication infrastructure in such cases is often not the Internet, but rather a private network, the threats prevalent on the Internet are relevant here too, as is the concept of unidirectional connectivity as a foolproof security solution. One of the weaknesses in physical security remote monitoring systems is that the sensors, e.g. cameras, are by nature located outside the physical security perimeter, as they are viewed as "guards", and as such are relatively easily accessed. Consequently, a hacker connecting a laptop computer instead of such an exposed IP camera can thereby relatively easily gain access to the IP surveillance network, potentially causing great damage to the surveillance system and connected IT infrastructures. However, if cameras transmit data through the unidirectional gateway, a hacker gaining access to an IP camera will not be able to cause much damage beyond the local port he has accessed. First, he will not have access to other cameras as they will be located "behind" a unidirectional gateway. Second, he will not be able to carry out online attacks against the surveillance network, as no return link will be at his disposal: data will only be flowing from the cameras inwards to the surveillance network and not vice versa.

One-way File Transfer Systems

Unidirectional connectivity can also serve to enable secure connectivity in various scenarios other than remote monitoring. For example, a network may be connected to the Internet in order to download software updates for software packages used within it. However, this con-

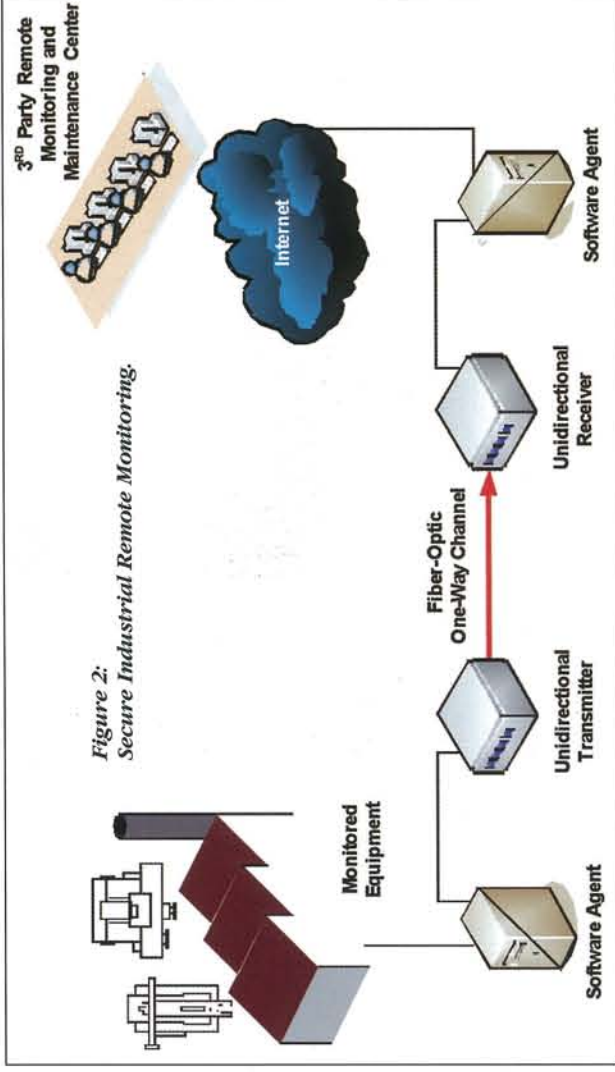


Figure 2: Secure Industrial Remote Monitoring.

nection will of course be bidirectional and will therefore expose the network to attacks from the Internet. A one-way file transfer system will enable the same functionality of carrying out automatic and timely software updates without risking online attacks or data leakage, as data will be flowing in a controlled manner only from the Internet into the secured network. Similarly, such unidirectional connectivity can

be used for the insertion of information collected from public websites into a secure network or for safe insertion of financial data, stock exchange data and banking transactions' statements into a bank's or investment-house's secure network. Of course, unidirectional connectivity can also serve to connect networks with different levels of security for the simple transfer of files or emails from one to the other,

Waterfall Solutions Ltd. is a leading provider of unidirectional connectivity solutions. For more information about the company please visit www.waterfall-solutions.com.

without exposing the higher-level security network to threats from its counterpart.

The Internet is a Two-edged Sword

Indeed, the Internet is a two-edged sword, on the one hand placing incredible amounts of data and remote connectivity at one's fingertips and thus providing excellent productivity, but on the other hand creating great risks by way of cyber attacks. The challenge is maximising the advantages which the network connectivity affords, while at the same time providing the necessary security. Unidirectional connectivity rises to this challenge precisely: in a great many scenarios it enables all the necessary connectivity, while at the same time providing sensitive, classified or mission-critical networks with foolproof and future proof security, which no other security solution can provide.

intersec

trade fair and conference

The focal point of security and safety. For the protection of life, property and assets, information and borders.

Conference: Fighting terrorism and serious organised crime

18 - 20 January, 2009
Dubai International Convention and Exhibition Centre, Dubai, UAE

www.intersecexpo.com

messe frankfurt

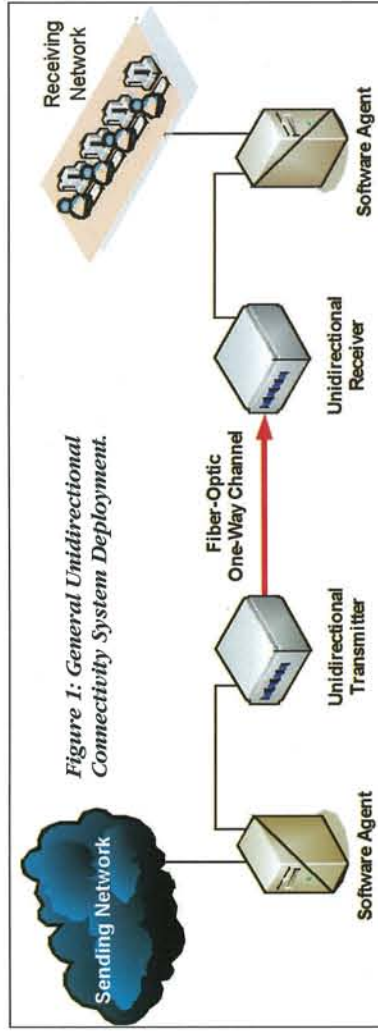


Figure 1: General Unidirectional Connectivity System Deployment.