Protecting people, property, business and the environment
FPA
Fire Protection Association

IPCRes guidance

InFiReS
Insurers' Fire Research Strategy funding scheme

Alarm signalling using the internet protocol

Part 1: An overview

Fire Protection Association
Protecting people and property

London Road
Moreton-in-Marsh
Gloucestershire GL56 0RH

Insurers Property Crime Research (IPCRes) working group

This guidance document has been developed by the IPCRes working group of InFiReS. IPCRes publications continue the tradition of providing authoritative guidance on crime prevention topics which was established by the Crime Panel of the Association of British Insurers.

Important notice

This document has been developed through the Insurers' Fire Research Strategy scheme ("InFiReS") and published by the Fire Protection Association ("FPA"). InFiReS membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various InFiReS Steering Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA have made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing However, the FPA make no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA make no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state of the art technologies current at the date of this document.

Use of or reliance upon this document or any part of its content is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude) entirely or in part mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it or any use of or reliance placed on the content of this document or any part of it.

First published by
The Fire Protection Association
London Road
Moreton-in-Marsh
Gloucestershire GL56 0RH
Tel: 01608 812 500, Fax: 01608 812 501
E-mail: fpa@thefpa.co.uk, Website: www.thefpa.co.uk

ISBN 1-902790 37-5

Copies of this document may be obtained from the publications department of the FPA, at the above address, or by calling 01608 812 500 or e-mailing *sales@thefpa.co.uk.*

Printed in Great Britain by Modern Colour Solutions. 2.0/1.06

Contents

Scope

This report is aimed at those seeking an introductory understanding of different methods of transmitting security alarm data over local area network (LAN) and wide area network (WAN) infrastructures using internet-based protocols.

It investigates and reports on internet protocol (IP) signalling designed to be used to transmit intruder, hold up and other critical signals from a monitored location to an Alarm Receiving Centre (ARC). It reviews, in particular: security; signal path; bandwidth; duplication; impact of multiple end users; and choice of protocol.

IPCRes will produce a second, more technical report designed to give insurers a clear understanding of what to look for when investigating IP alarm signalling.

From here on, refer to the Abbreviations/Glossary section, page 12, for explanations of abbreviations.

History

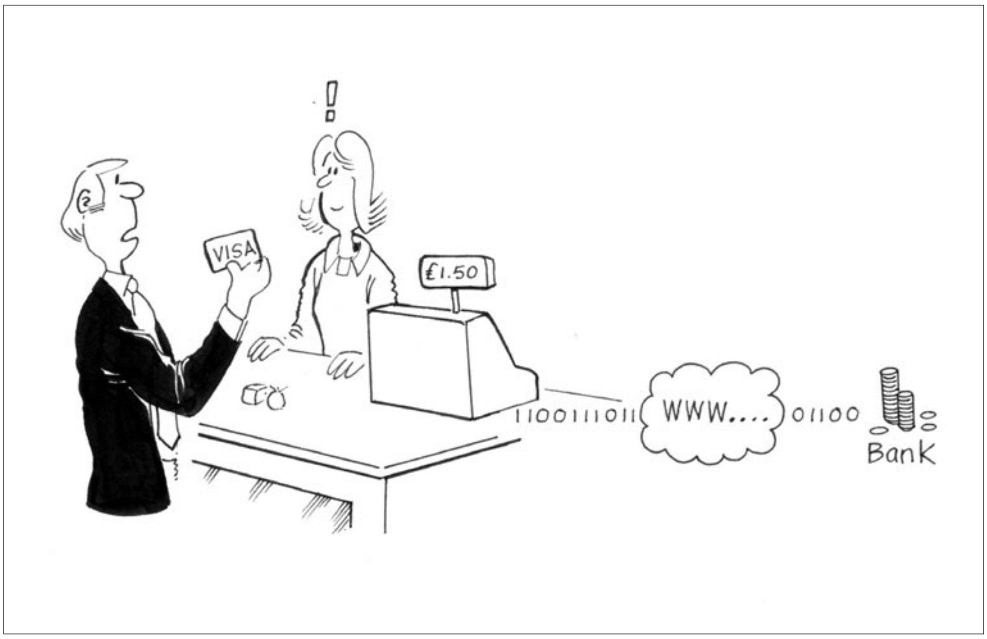
The security industry has seldom been at the forefront of technology and has typically adopted and re-engineered technologies designed primarily for other industries.

As with PSTN and ISDN technology, the security industry is a late adopter of IP technology and, as a consequence, the security industry is now asking questions about IP signalling that have not only been asked by the IT industry but have been already solved by the IT industry.

Equivalent problems and solutions in the IT industry

Most people today use computers connected to the internet for sending emails, purchasing goods online, checking bank accounts etc. Even people who don't have a PC often use cash machines and pay for goods and services at tills which use LAN, WAN and the internet to process transactions.

'Is it safe?'



Billions of such transactions are carried out securely and quickly every day. In spite of the perception that the internet is insecure, if basic security principles are followed then such transactions are completely secure. If this were not the case whole economies would collapse.

Since the IT industry has developed secure methods of data transmission over IP networks, it only remains for the security industry to identify and adopt the best practices of the IT industry to secure alarm data for transmission over the internet.

Protocols

There are a number of communication protocols used for sending and receiving data over the internet. The two most widely used are TCP/IP (transmission control protocol/internet protocol) and UDP/IP (user datagram protocol/internet protocol).

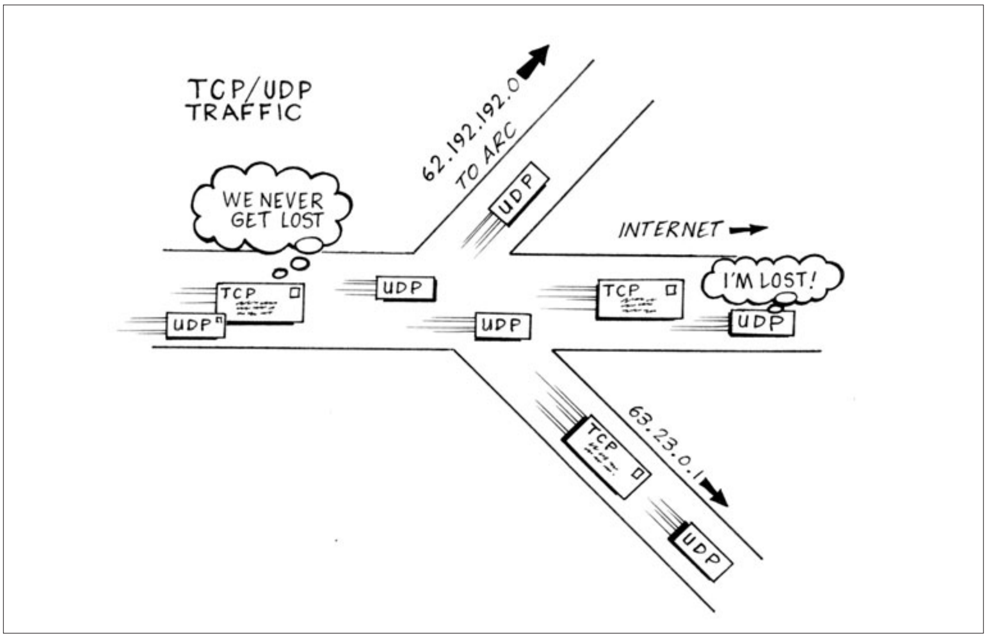
TCP v. UDP

The simplest way to compare TCP and UDP is to use the analogy of posting a letter. TCP could be seen as recorded delivery and UDP as ordinary mail

When a recorded delivery letter is posted, you get a receipt of posting, the letter is tracked internally by the mail company and the recipient will sign for the letter on receipt; proof that the letter was received. With ordinary mail you simply post the letter and rely on the postal infrastructure to ensure safe delivery of the letter.

In simple terms TCP confirms delivery, UDP doesn't.

'Help, I'm lost.'



On the face of things it would seem that TCP should be the protocol of choice for delivery of alarms over IP.

However, TCP/IP data packets are much bigger than UDP packets and more susceptible to time outs on slower network connections such as satellite, GPRS and GSM dialup etc which the security industry often uses as backup to IP signalling. UDP data packets are smaller and quicker and handle slower bandwidth connections better than TCP and, as with ordinary mail, delivery is successful most of the time. (See Timeouts and Bandwidth in Abbreviations/Glossary, page 12.)

TCP confirms delivery but is slower than UDP. UDP is quicker but there can be some data loss.

This has prompted a number of alarm panel manufacturers to investigate UDP for alarm data transmission.

How to transmit UDP securely 100% of the time

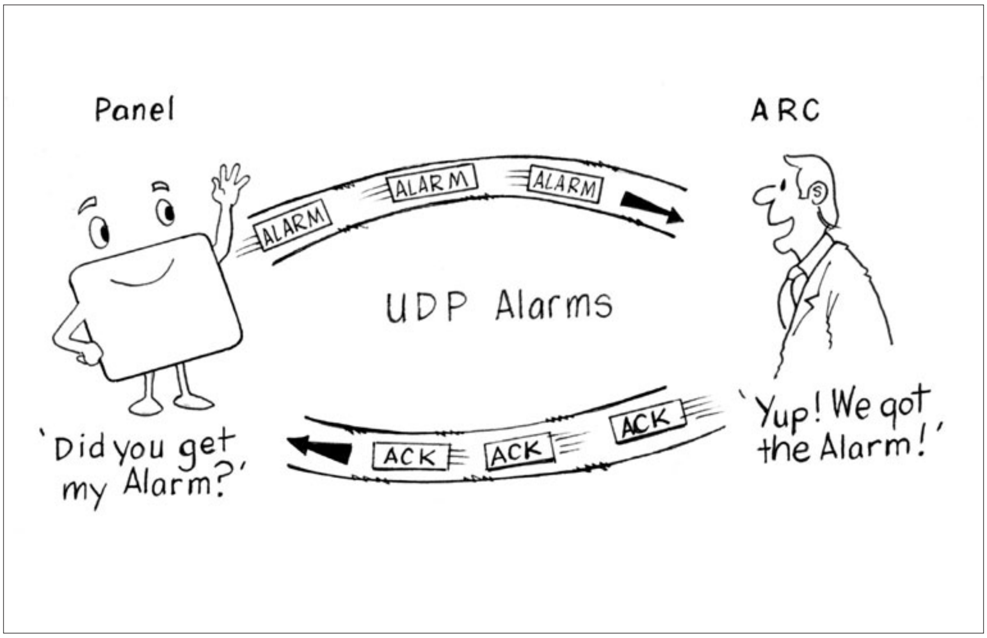
Take the letter delivery analogy, this time the letter requests the recipient to acknowledge (ACK) the receipt of the letter and, if acknowledgement is not received within a given time frame (time out), then the sender will post the same letter again. This process will repeat (retries) until the sender receives a letter back from the recipient acknowledging the letter (kiss off).

In this way it is possible to guarantee that a UDP data package is sent and received. The majority of UDP data packets will get there first time. Those that don't will be re-sent until the transmitting panel receives an ACK or exceeds the number of retries; in which case the alarm does not receive the final kiss off from the ARC.

At this point the UDP alarm data could be sent via an alternate path if one exists, otherwise the alarm remains unacknowledged in the alarm panel.

In terms of traffic volume, speed and flexibility UDP has won favour over TCP with some panel manufacturers.

'Alarm alarm alarm!!!'



The method of repeatedly sending an alarm until an acknowledgment is received would work just as well for TCP alarm data.

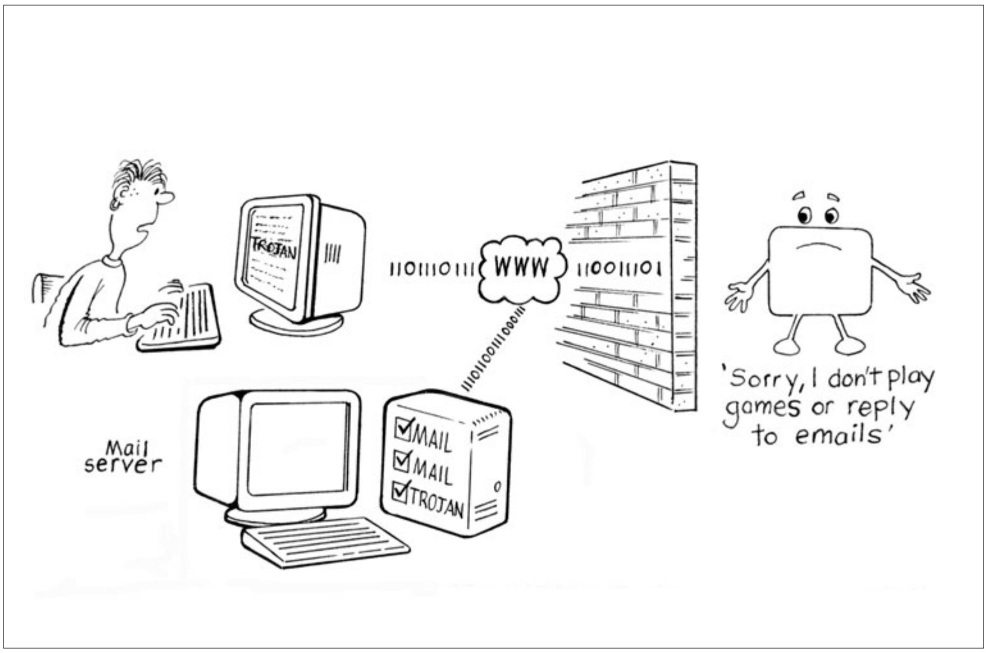
Security

To prevent automated (brute force) login attacks, alarm panels and alarm receivers should employ a 'three strikes and out' policy. If the user doesn't login correctly after three attempts, login is aborted and the user has to reload the login page. This approach makes automated login attacks virtually impossible. Multiple failed login attempts should also raise an alarm to the ARC.

Alarm panels don't have the same vulnerability as a PC since they run a minimal operating system with little for hackers to exploit, unlike a PC that has a complex operating system running multiple applications, such as e-mail, ftp, telnet etc, many of which have vulnerabilities that can be exploited.

Much of the traffic on the internet today relies on applications that run on servers, such as mail severs and web servers. Internet monitoring utilises very small and efficient message packets that travel on the internet backbone, bypassing other internet servers that run vulnerable applications. Additionally, because panels and receivers are single-purpose devices, they cannot download applications or run scripts that would put them at risk of acquiring a virus or make them susceptible to a hacker. It would be extremely difficult for a hacker to break into a panel or central station receiver through the internet. Hackers would need several pieces of unfamiliar information and would have to sort through an astronomical number of possible combinations. Listed below are the odds of success if a hacker knew different levels of information to gain access to an encrypted alarm panel:

Hacker v. Panel



Panel protocol only: 1 in 463,070,916,161,327,503,017,132,890,625

Panel protocol, IP address: 1 in 429,483,618,205,163,775

Panel protocol, IP address, Port number: 1 in 6,553,499,934,465

IP address only: 1 in 1,078,203,909,375

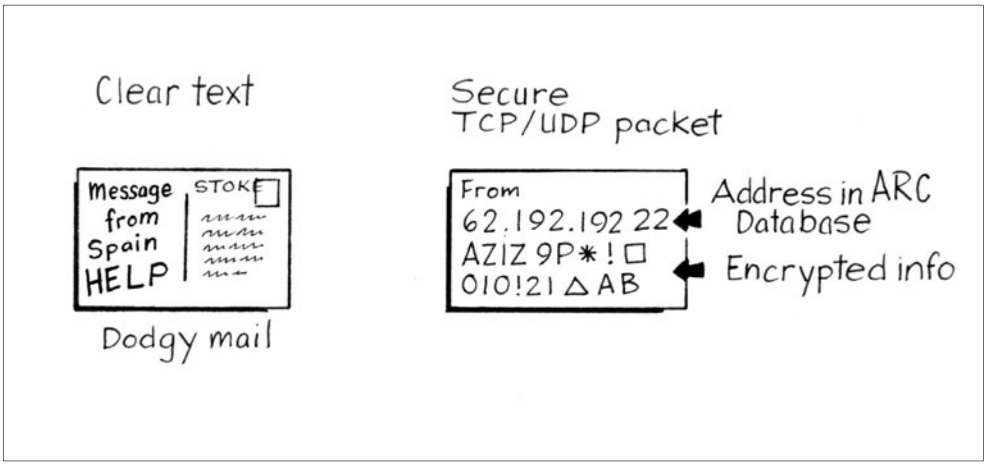
Panel protocol, IP address, Remote key: 1 in 4,294,836,225

How to verify the origin of the alarm data

As with letters, most TCP and UDP traffic is easily read since information is sent in clear text and many network applications can read TCP and UDP traffic. For alarm signals to be sent securely, the data must be encrypted and the sender must be verified so that alarm signal substitution cannot take place

Using the mail analogy it is possible to check the origin of a letter before you act on the contents. Mail has a postmark that is not easily substituted, indicating where the letter originated. If you receive a postcard from Spain with a postmark of Stoke-on-Trent, it is very likely that the card didn't originate in Spain. IP traffic has an originating IP address which can be checked before action is taken on the alarm information. If the originating IP address is not in the ARC's database then the message will be ignored or flagged for further investigation as possible alarm data substitution.

'Who am I?'



A panel can also transmit a unique panel ID to verify the origin of the alarm. This, combined with IP address verification and encryption of data by the panel, means that substitution would be extremely difficult.

Some manufacturers' panels can work without a fixed IP address (DHCP), the panel 'alarms in' to the ARC. As long as this incoming alarm has the correct encrypted data and panel ID and is in the ARC database then it is treated as a valid alarm from a know location.

One advantage of a fixed IP address is that firewalls can exclude an unknown IP address from connecting to the ARC software, providing an additional layer of security.

One disadvantage of a fixed IP address is that most ISPs will charge a monthly rental for this service.

I don't trust you, you don't trust me, and we don't trust anyone!

How can I post my letter to you and ensure that only you read the contents?

First I need to place the letter into a container and padlock it; I keep the key and post the padlocked parcel to you.

You then put your padlock onto the parcel (keep your key) and post the parcel with both padlocks back to me.

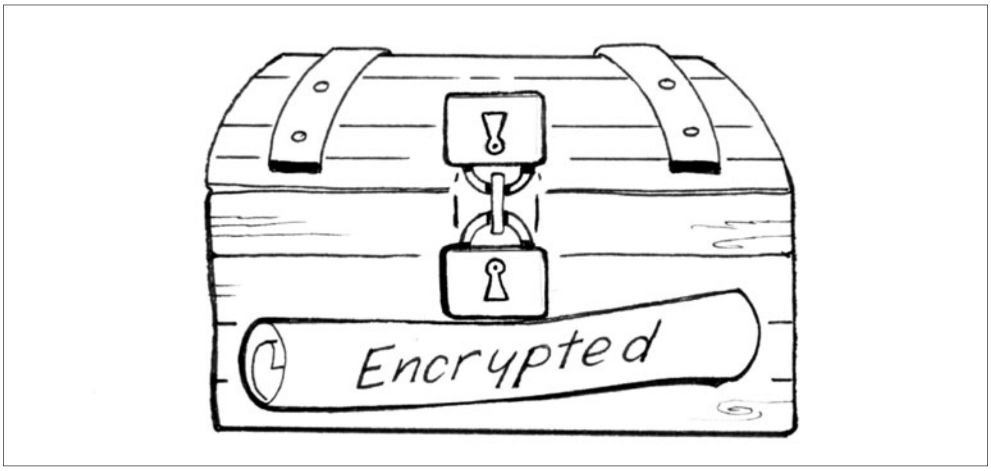
I remove my padlock, leaving only your padlock on the parcel and post it back to you.

You now have the parcel with only your padlock on; which you remove and read the letter inside.

Although simplistic, this is the basis for data encryption using public and private keys.

When an encrypted communication is received, the key is used to convert the garbled signal into its original state. Typical encryption programs have a 1024 bit format, and 128 and 256 bit AES (advanced encryption standard) as used in applications like WinZip, PGP (Pretty Good Privacy) and other commercial encryption packages.

Secure encrypted data



What if I am on the internet?

Because networks work on packet data, TCP and UDP packets share the network with other data that is being transmitted at the same time. This means that many computers and hardware devices can use the internet simultaneously.

At the post office I can post my single letter and know it will be delivered, even though there are many millions of letters per day, although at times of peak traffic like Christmas the post slows. It is the same with network traffic; when there are high demands data delivery slows but seldom stops completely. Most broadband users' data is being downloaded from the internet, whereas the alarm data is being uploaded to the internet. There is far less traffic going up to the internet than comes down to the users' PCs, so alarm packets are not competing for bandwidth.

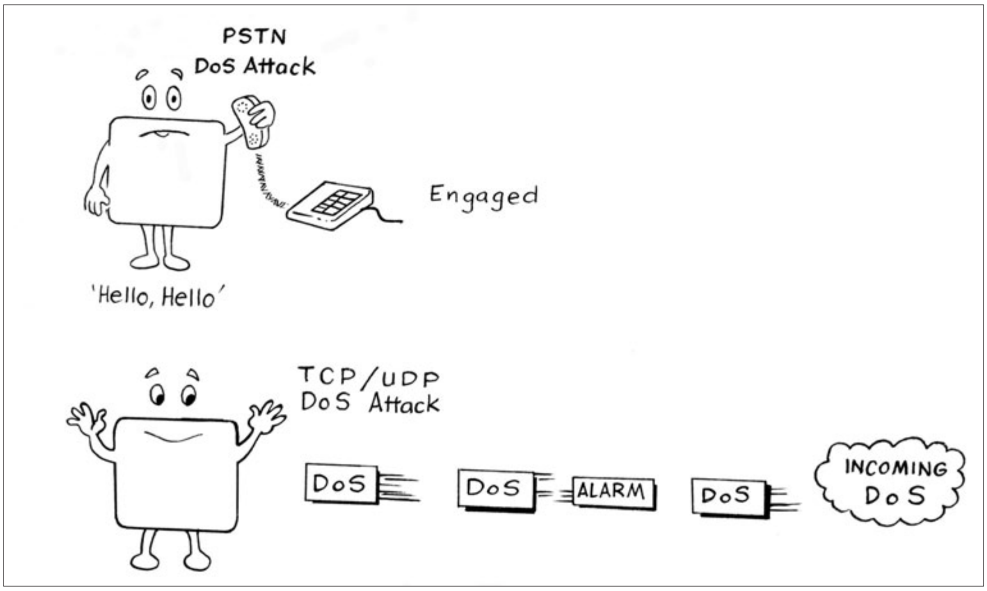
Denial of service (DoS)

This is a form of internet attack in which the targeted address is overloaded by incoming malicious IP traffic (ARC or panel). Many routers now have built in DoS protection turning such attacks back on to the originating servers.

Alarms sent via PSTN to an ARC create a form of self-inflicted DoS as each alarm connection ties up an incoming line. At peak periods an ARC can run out of available PSTN lines. With IP data it takes many tens of thousands of connections to perform a successful DoS attack on a network connection and because of the packet nature of IP, the 1k alarm packet can still get through.

As with PSTN lines, routers can be configured not to accept incoming connections, so a connection to the ARC can only be originated by the panel.

'Nobody listens.'



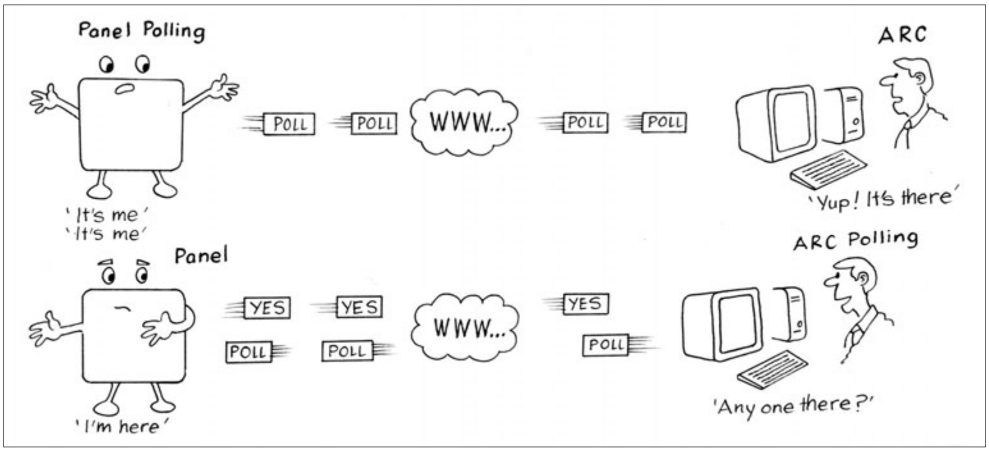
Polling

PSTN and ISDN telephone lines can be polled to ensure that the communications path is uninterrupted.

Since broadband connections are always on, the remote panel can poll the ARC on a regular basis confirming that the alarm equipment and communications are working. On the face of it, this is a better service than simply checking the availability of the line.

Some alarm panels poll the ARC on a regular basis, if the ARC doesn't receive the poll, an alarm is generated in the ARC. If the alarm panel cannot connect to the ARC then alternate routes such as PSTN, GSM and GPRS can be used.

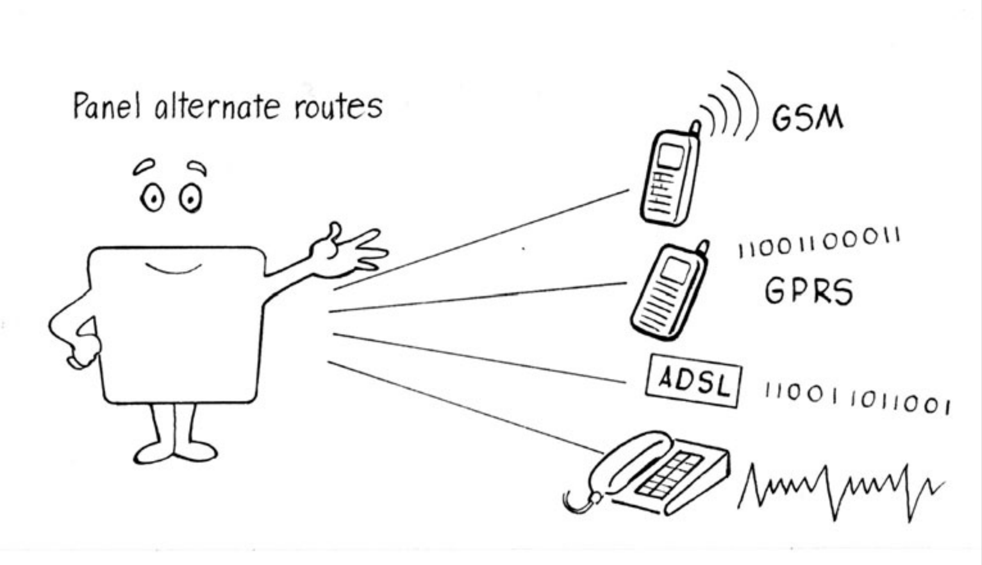
'Anyone there?'



Signal path

ADSL circuits require the use of an analogue PSTN line. This can provide an alternate signalling path since the PSTN and ADSL services are separate. If the ADSL service fails the PSTN line continues to work. If there is a line cut, however, then both PSTN and ADSL services will fail and a GPRS/GSM backup will be required.

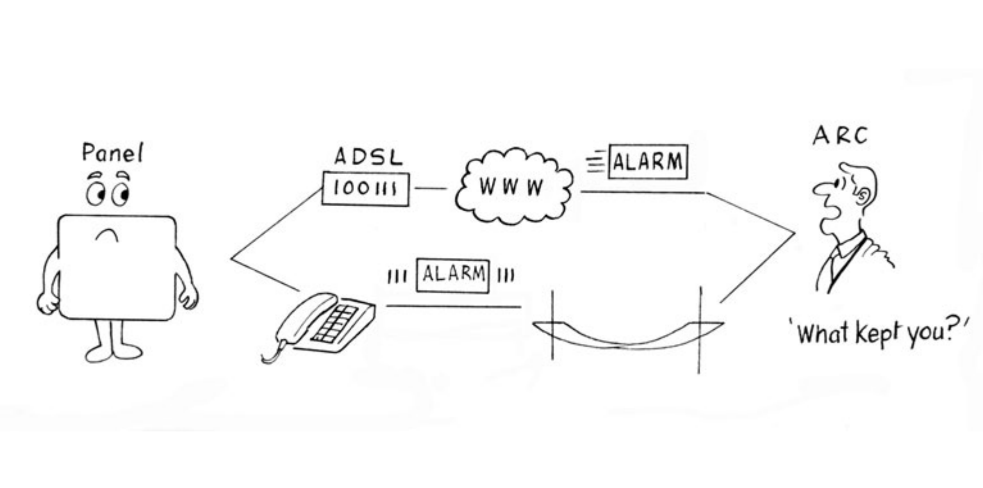
'Take your pick. There's a lot to choose from.'



Speed

Any alarm signal sent over LAN (local area network) or WAN (wide area network such as internet), whether via TCP or UDP is going to get to the receiving centre much quicker than signalling over PSTN or ISDN (most ISDN modems used the slow Hayes AT commands). A typical alarm message is around 700 bytes (less then 1kb). As most broadband packages offer upload speeds of around 256kb per second, the alarm traffic represents a fraction of available bandwidth. A typical UDP alarm packet can be delivered from London to Sydney in under a second whereas a dial up alarm connection can take from 5s to 45s to ACK and disconnect.

'Every second counts.'



Network alarm signalling reduces the time a signal takes to get to the ARC and increases the availability of the ARC to handle alarms, thereby improving service delivery, and when every second counts, such as in personal attack alarms, improves customer service. Network data also has a fixed cost whereas dial-up usually has a cost per use.

Hardware

To take advantage of modern network communications, the panel must support an NIC (network interface connection) usually an RJ45 connector. This is the standard network connection used on your laptop or PC. Some panels also support wireless connections (802.11b), using wireless encryption. The panel must also support interface card connection to PSTN, GPRS, serial data port for GSM, and alarm connector allowing retro fitting to older dial-up panels. The panel firmware will support encryption.

Practical problems and pitfalls

Since most companies have existing computer networks it would seem the logical choice to use the existing network for alarm traffic (lower costs, infrastructure in place, etc).

However, existing PSTN alarm systems don't share a company switchboard to route alarm traffic and for good reasons.

For those same reasons IP network systems should not use the company infrastructure. Instead, design and install a new standalone IP system using a dedicated ADSL circuit. This will ensure that the IP alarm system can be a standalone, with dedicated UPS – an independent IP based security system.

If an IP based panel with reverse polling loses its primary IP connection and starts a PSTN, ISDN, GSM or GPRS poll, then the dialup/data cost could be considerable. If there is a large IP failure, such as happened with the Manchester cable tunnel fire in the spring of 2005, when the north of England lost broadband, there is a potential with reverse polling to swamp an ARC with dialup connections as polls re-route through dialup connections.

ARCs will have to invest in new hardware and software to receive alarms over IP, staff will need training in the basics of TCP/IP, key staff will require in-depth knowledge of TCP/IP and network communications.

Future systems

Ultimately, telecommunications companies (telcos) will develop their own products for line monitoring over IP networks. Arguably they already exist at a basic level. Take your mobile phone as an example; the GSM network knows when your phone is connected to the network and moves from cell to cell.

Telco ISPs know when your IP ADSL router is connected to their network; this is achieved without the necessity of polling equipment.

The future will probably contain a combination of services, telcos providing the line monitoring and panel manufacturers and ARCs monitoring individual pieces of equipment. This will result in a more secure and resilient system.

Even when the telcos start providing such connection monitoring services, it is far better to have the encryption done within the panel and the decryption done within the ARC, and a polling service that confirms that equipment is working.

Conclusion

TCP and UDP protocols can be used for the secure transmission of alarm data. To achieve this, alarm panels must encrypt the data before transmission. To use the mail analogy, the protocol is just the postman carrying encrypted information to a known address. The panel should support alternate communication routes and be capable of polling the ARC or responding to polls from the ARC. Sending alarms over IP does not present any great technical challenges, the infrastructure is in place, the protocols are tried and tested, the encryption is well proven, and the choice of alternate routes are many; the security industry is simply taking what was transmitted over PSTN, encrypting it and sending it over IP.

Abbreviations/Glossary

ADSL: Asynchronous Digital Subscriber Line
A technology for transmitting digital information at high bandwidths on existing phone lines. Unlike the regular dialup phone service, ADSL provides a continuously-available connection. ADSL is asymmetric in that it uses most of the channel (512kb) to transmit downstream to the user and only a small part to receive information from the user (256kb). ADSL simultaneously accommodates analogue (voice) information on the same line. ADSL is generally offered at downstream data rates from 512kbps to about 6Mbps.

ARC: Alarm Receiving Centre

Bandwidth
A measure of the capacity of data that can be moved between two points in a given period of time. Most network managers consider 50% bandwidth usage to be the maximum data throughput. Any higher data throughput usually requires more bandwidth.

DHCP: Dynamic Host Configuration Protocol
Dynamic Host Configuration Protocol is a communications protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organisation's network. DHCP allows devices to connect to a network and be automatically assigned an IP address.

DoS: Denial of Service
A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks.

Ethernet
A computer network cabling system designed by Xerox in the late 1970s. Originally transmission rates were 3Mbps via thick coaxial cable. Media today include fibre, twisted-pair (copper), and several coaxial cable types. Rates are up to 10Gbps or 10,000Mbps.

FTP: File Transfer Protocol
A standard method for sending files from one computer to another on TCP/IP networks such as the internet. FTP is also the name of the command used to initiate transfer of files. Anonymous FTP is a common practice which permits users to access some parts of an FTP site without needing an account and password for the site. Access usually is gained by using the username 'anonymous' or 'ftp'. By convention, the user should enter their e-mail address as the password.

GSM: Global Systems for Mobiles
Global System for Mobile Communication. Originally developed as a pan-European standard for digital mobile telephony, GSM has become the world's most widely used mobile system.

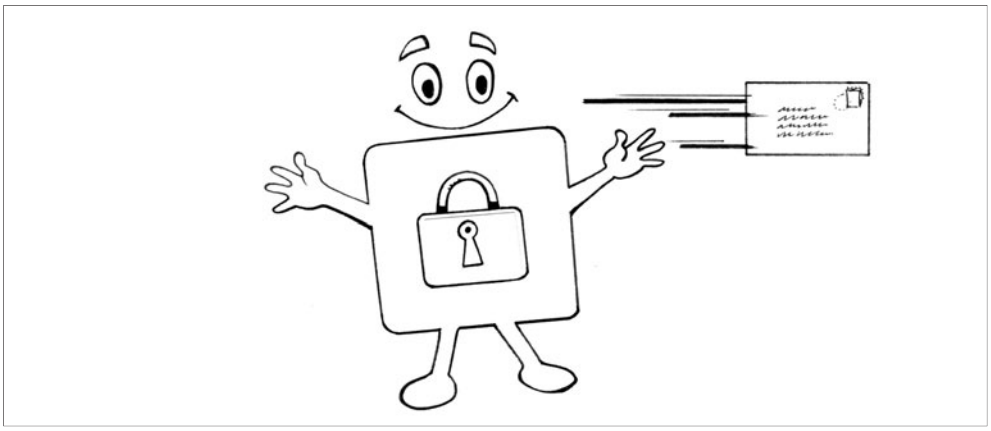
GPRS: General Packet Radio Service
Short for General Packet Radio Service, a standard for wireless communications which runs at speeds up to 115kbps, compared with the current GSM (Global System for Mobile Communications) rate of 9.6kbps. GPRS, which supports a wide range of bandwidths, is an efficient use of limited bandwidth and is particularly suited for sending and receiving small bursts of data, such as e-mail and Web browsing.

IP: Internet Protocol
Part of the TCP/UDP/IP protocol suite. The layer three protocol used in a set of protocols which support the internet and many private networks. IP provides a connectionless datagram delivery service for transport-layer protocols such as TCP and UDP.

ISDN: Integrated Switched Digital Network
Digital network with higher speed than found on the traditional telephone network. Even though ISDN uses existing phone lines, it does require specialised equipment. Because the network is all digital it can easily send voice, data, and video over the same line simultaneously.

ISP: Internet Service Provider.
An ISP provides access to the internet for others via some connectivity service(s). This might be in the form of dial up services, ADSL, web hosting services or a combination.

'Secure Fast Resilient TCP/UDP.'



IT: Information Technology

LAN: Local Area Network
A local area network (LAN) is a computer network covering a local area, like a home, office or small group of buildings such as a college.

PC: Personal Computer

POTS: Plain Old Telephone System
Conventional analogue telephone service delivered over copper wire.

Ports
A network-attached device can have up to 65,000 ports, each of which can be used to send and receive data.

PSTN: Public Switched Telephone Network
Also know as Plain Old Telephone System, this refers to the world's collection of interconnected public telephone networks designed primarily for voice traffic.

Remote key
A type of PIN (personal identity number) provided by the panel manufacturer.

SMS: Short Messaging Service
Available on digital GSM networks allowing text messages of up to 160 characters to be sent and received via the network operator's message centre to your mobile phone, or from the internet, using a so-called 'SMS gateway' website. If the phone is powered off or out of range, messages are stored in the network and are delivered at the next opportunity.

TCP/IP: Transmission Control Protocol/Internet Protocol
A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard internet protocols.

Telnet
Telnet is a utility program and protocol that allows anyone to connect to another computer on a network. After providing a username and password to login to the remote computer, users can enter commands that will be executed as if entered directly from the remote computer's console.

Timeout
Usually the time allotted for a task to complete, when the time to complete has been exceeded, the task times out.

UDP/IP: Universal Datagram Protocol / Internet Protocol
Provides unreliable but low-latency transport for small data packets.

UTP: Unshielded Twisted Pair
Unshielded Twisted Pair is a type of networking cable that combines four pairs of wires insides the same outer jacket. Each pair is twisted with a different number of twists per inch which cancels out electrical noise from the other twisted pairs.

WAN: Wide Area Network
A wide area network or WAN is a computer network covering a wide geographical area, involving vast array of computers. The best example of a WAN is the internet.

IPCRes **guidance**

InFiReS

Insurers' Fire Research Strategy funding scheme

Alarm signalling using the internet protocol

Part 1: An overview

London Road
Moreton-in-Marsh
Gloucestershire GL56 0RH

Fire Protection Association
Protecting people and property