

A White Paper for securityXML

A new approach to Integrated Security Systems

Peter Manolescue © September 2000

1.0 Where are we now and why?

1.1 The myth of Integrated Systems

For at least the last ten years companies in the security industry have been talking about 'Integrated Systems'. This 'holy grail' is in fact an illusion as it covers many different concepts. Companies who market such systems are usually pushing their own technology and obliging other suppliers to fit into their vision of what constitutes an integrated system.

1.2 Hardware solutions

Because most of the engineers in the security industry have a hardware background they have been looking for a hardware solution. A good example of this is the Echelon initiative which basically says 'Put a neuron chip in everything and hook it all up to an Lon-bus with a bit of LonWorks software and 'Voila' - integration. The basic problem is that this requires everyone to follow the same standards which are proprietary to the Echelon Corporation. This is another form of 'lock-in' which is great for the supplying company but very limiting for the industry. The Echelon approach has been around for at least 8 years and it has not achieved ubiquity yet.

Another solution is to start from a particular technology from a major supplier such as CCTV or Electronic Access Control (EAC) and then 'strap-on' other elements as they are needed. Once again the customer is locked-in to the original systems supplier and the products he supports. This can work fine for an individual installation but add-ons and upgrades are expensive. Also if the original designers and engineers have moved on then maintenance can prove difficult or impossible.

1.3 Software solutions

Many of the problems afflicting the hardware solution also apply to software solutions. The software controlling big CCTV and EAC installations is bespoke to one company so starting there always produces 'lock-in'.

Another approach is to produce a generic Windows-based user interface with software links to all the major manufacturers' products. However every time a new element is added a driver must be written. This quickly becomes unwieldy with the management of hundreds of drivers. Manufacturers of security equipment are notorious for example, with network installation companies for changing the specification of their products so driver update is a nightmare.

Because software is becoming increasingly important within security, developers have looked to advances in IT to provide solutions. One such approach is CORBA. This is a truly powerful tool but it can only be used on big systems with a lot of computing 'horsepower'. In many ways it is ideal for the connection of large legacy systems where it is not economic to rip out and start again. But for small systems which need to connect to grow it is over-kill.

2.0 What is happening around us?

2.1 Internet standards are pervasive

Even top executives have heard of TCP/IP. The most visible part of the Internet at the moment is the .com revolution with B2C and B2B investment soaring. However what is less obvious is that a world-wide technical standard has been imposed that can be built on without 'lock-in' to any one company.

2.2 Embedded processors everywhere

The average home now has many invisible small computers (embedded processors) in all kinds of devices (answer-phones, printers, toasters etc). These devices cost just a few dollars and are getting cheaper and more powerful every year. With the new Internet protocol IPv6 it will be possible for every device now matter how small to have its own unique address and be connected to the Internet.

2.3 Communication costs are crashing

High-speed data links are everywhere and this is now being reinforced by ubiquitous wireless communication at low cost. New technology such as GPRS and UMTS will give faster links and the ability to have 'always on' links with customers just paying for the data transferred rather than for the time of connection at present.

2.4 Open standards development is proving very productive

The most public example of this is Linux which was not produced by a giant corporation but by a group of interested and committed individuals. More recently, the XML standard has arisen. Even Microsoft has learned its lesson here. With its new .NET strategy it is committed to XML but is happy for the standard to be driven by non-affiliated industry-wide groups.

3.0 Where do we want to be?

3.1 The need for 'plug and play'

The dream of integrators is to be able to take any product from any manufacturer and simply plug it into a system with minimum fuss. This requires that the product can 'converse' with the rest of the system in a way that they both understand. Within a specific technology this already happens. A PIR knows how to signal to a control panel and a CCTV camera knows how to send its image to a monitor. But if you plug a PIR into a CCTV monitor the results can be unpredictable!

3.2 The need for open standards

In order for 'plug and play' to become a reality, manufacturers and users need to agree on common, open standards to which all will subscribe and adhere. For communication the obvious standard is TCP/IP. The choice of software 'carrier' standards is equally easy. The Internet has made HTTP the clear leader of choice. However, on top of this another standard is required. Security systems need a common language for communication that reflects the needs of the industry. For example, systems need a common expression for concepts such as 'alarm', 'request to exit' and 'pan left'.

In current systems, these messages are usually hardware encoded but in a distributed world they must be represented in software protocols. For integration to be 'plug and play' these protocols must be universally accepted. However to avoid 'lock-in' the protocol standard must be developed in an open environment that does not favor any one company.

3.3 The need for standards-based flexibility

As well as being universal, any industry-wide protocol must also be compatible with larger systems into which the security system may be embedded (such as a building management system) with enough flexibility to enable backward and forward compatibility with legacy systems and those yet to be developed. Indeed the protocol set itself must be open to future development without compromising earlier products and installations.

4.0 How are we going to get there?

4.1 An open forum

A open site (www.securityxml.org) will be set up for all interested parties. This not-for-profit forum will be open as a discussion group for developing the securityXML DTDs and exchanging information and ideas.

4.2 The role of the customer

Because of developing needs, security systems often end up being many times the size of the original system that was envisaged. By specifying securityXML protocols in their requests for tender, consumers of security will ensure that any system they buy will be expandable in the future even if they have little idea of what direction their needs will take them. Demand for inclusion of securityXML protocols will add pressure to manufacturers to obey standards and contribute to their development.

4.3 securityXML

securityXML responds to all the above requirements. It is:

Based on XML, an IT industry standard, owned by no single company yet supported by major corporations like Sun, IBM and Microsoft. Indeed XML is the core technology of Microsoft's new .NET strategy

An open standard which is developed in public by contributions from individuals and corporations

Scalable from small systems to large without the need for massive development investment

Simple to implement on new or legacy systems as securityXML is based on simple text rather than complex IT codes which are understandable to even non-IT users.

For example these three messages are typical of what a securityXML system would produce:

```
<alarm type='intruder' source='main office' time='11:43' date='4-Sep-2000' /> or
```

```
<cardswipe door='main entrance' time='8:32' date='12-Oct-2000' />
```

```
<camera position='lobby' panleft='8 degrees' />
```

Conclusion

There is a great deal of work to be done. Timing will be vital. The initiatives coming from such big players as OASIS and Microsoft's UPnP development will drive the gradual implementation of XML itself. The acceptance of the concept of securityXML will require persuasion and education. But it will happen.