Insurance Europe
Prevention Forum

Information for insurers — Smart systems

November 2017

1. Content

This paper will explore the current generation of so-called 'smart systems', sometimes referred to as 'home automation', although such systems are now finding their way into business premises, particularly small businesses. Such systems have a wide range of roles but this paper considers systems only in the context of the premises security application. Other applications, including detection of water leakage, automatic control of heating, gas and fire detection, etc., are of obvious interest to insurers and some of the issues explored impact these functions, too.

2. What is a smart system?

A 'smart system' is generally understood as a network within a premises linking 'smart' devices. Although a smart device may be capable of operating independently (such as a programmable light switch), such devices are generally intended to be included in a (generally wireless) smart system, usually controlled centrally by a 'hub' with a user interface. A smart device implies a device with a certain autonomy, capable, in combination with other devices in the system, of altering its environment or responding to events in a way that adds value for the user unavailable with individual 'dumb' devices. Conversely, there are other design philosophies which work on the basis that the deployed system devices are dumb and all the intelligence is in the hub.

The majority of these devices are powered by an on-board battery. The most popular devices are those controlling multi-media, lighting, temperature, security, CCTV, access and fire detection. 'Smart' operation is demonstrated when, for example, the system's software captures information from its network of sensors and then takes some type of action independent of human control such as preparing for the owner's homecoming by adjusting the temperature, activating lighting, opening the garage door, starting home entertainment, etc. Some systems will actually unlock the entry door if the owner is sensed as being "close by", these automatic operations having been pre-programmed in by the owner. Many devices require a certain degree of initial user interaction (setting preferences for heating, etc.) if they are to deliver something approaching an 'intelligent' function. In addition to convenience these systems can have an energy conservation benefit.

Another feature of the system may be control of devices in a convenient way from more than one point in the building and, remotely, through a smartphone, tablet, PC or laptop connected to the internet. An internet channel may also exist between the system and the 'host' – the supplier or manufacturer or their contractor, to collect data and/or send updates and/or provide 'cloud' data storage and/or connect with a response service.

The 'hub' generally takes the form of a separate component of the smart system performing a function very similar to the control and indicating equipment (CIE) of an intruder alarm system. However, the 'hub' could just as easily be incorporated into a product that is commonplace in a home or business but is participating in the system such as an air conditioning control box, a television receiver or even a refrigerator!

3. What issues arise?

The fact that these products and services have been developed in the so-called Internet of Things (IoT) arena is significant. They do not reach the market via the traditional fire and security system industry and, although the designers appear to have highly developed skills in designing "trendy" products, their skills do not seem to extend to security. Where security and privacy are at stake the basic security precautions recognised as fundamental elsewhere in the wider computer and network sectors seem not to be understood and/or neglected and/or badly implemented. In fact, the philosophy behind the IoT with which designers may be more familiar is that millions of everyday devices should be fully visible to each other and not sit behind cyber defences intended to isolate them.

Numerous market players are jostling to get their products out in front of the public as soon as conceivably possible to gain market share with apparently little appreciation of basic security principles in the design of a security product, not least, the need for fully developed cyber security controls. Some of the sales and marketing material for these products can be misleading for the public, for example the implication that information will be "relayed" to the police.

Another important feature of the smart system market, which now contains the highest profile names in internet services such as Apple, Google and Samsung, is that these "heavyweights" are keen to see the

market adopt their own proprietary operating protocol with the consequence that all the devices on the system must be compatible with that protocol. The utility companies (gas, power, etc.) are also in a particularly advantageous position to take full advantage of the technology, having huge resources with networks connecting every in their area of operation. However, in the absence of an agreed single international or industry standard for smart systems as such, the market is very fragmented through the interoperability problem at this point in its development.

This interoperability issue extends additionally to the system network technology which might employ traditional short range communication such as local mains borne (power-line), Wi-Fi or Bluetooth or one of a small number of new, low-power networks specifically developed for the limited amounts of data that need to be exchanged between the components of a smart system. This therefore adds another layer of potential incompatibility.

Some 'agnostic' smart system hubs allow the user or an installer to connect different brands of smart device provided, of course, these are all compatible with a local wireless network supported by the hub. These so-called 'Open Ecosystems' therefore form a rival market in competition with the proprietary systems in which all devices are from the same stable. A potential difficulty might be that as the various components making up the smart system have not been designed to be compatible, functionality might be lost and security vulnerabilities might be caused.

The designers in this sector attach great importance to simplicity in user adoption and operation (but frequently fail to achieve it). Perhaps this is largely accounted for by their wish that products should be suitable and attractive for the implementation either of a purchaser on a "do it yourself" (DIY) basis or a contracted installer, typically from the electrical or heating installation industries. It might be that certain devices conform to recognised national and international standards such as those in the EN 5013X series but, if so, they are a very small minority. Consequently, although it is thought that some smart system devices are in fact being installed by approved fire and security companies, in many countries this is likely to conflict with the rules of the sector inspection-control body if the components do not conform to the applicable fire/security standards. It follows that such systems do not qualify for insurance company approval if the insurer requires a system conforming to fire/security standards as a condition of insurance cover.

Furthermore, systems installed by non-approved firms are unlikely to receive any ongoing routine inspection or preventative maintenance and service personnel are unlikely to be properly vetted and trained in security. As it happens few manufacturers of smart systems appear to see the traditional fire and security field as their target market but, confusingly, some smart system providers offer the services of well known alarm receiving centres that, in the past, have contracted only with the providers of approved systems. There is potential here for insurers to be misled into assuming a smart protection system is entirely competent and to recognised standards simply through its association with an alarm receiving service familiar to stakeholders as operating in the traditional fire/security systems market.

Special note

Insurers and other stakeholders should not confuse the products described so far in this paper with the recent introduction of the smart phone applications becoming available from mainstream specialist fire and security system providers. These allow the user to remotely control and manage a system over the internet from a remote point and, provided the supplier can demonstrate that the application is adequately protected from cyber attack, and that false alarm control is built in, an insurer might be comfortable to accept this form of system operation which is rapidly growing in popularity with users. One way for a system provider to satisfy the user or his insurer that the application will be unlikely to represent a security vulnerability is to provide evidence of conformity to a recognised performance specification available from (e.g.) a recognised testing and certification organisation.

5. Specific security issues

Various papers and reports, some by authoritative and respected organisations, have found widespread security vulnerabilities in the current generation of smart systems and devices. Examples include:

- weak, single factor authentication
- systems that allow access to video streams by merely breaking into Wi-Fi
- weak password recovery mechanisms
- absence of a limit on failed login attempts
- insecure cloud and mobile interfaces
- elementary mistakes in security configuration
- lack of encryption e.g. with the result that security settings are exposed

The benefit of being able to monitor the security of the premises from afar becomes a serious security exposure if the owner is not the only one doing so – that is to say, if criminals have penetrated the communication channel.

Cyber vulnerabilities in devices and systems exposed by hackers quickly find circulation on the specialist websites. The vulnerabilities found in certain connected locks for example were widely circulated. A lock temporarily compromised by a hacker the purpose of a burglary might offer no clue to the property owner or insurer as to how the loss occurred. Merely hacking a humble thermostat potentially yields valuable information for an intruder as to whether a family appear to be at home or on holiday.

If security barriers are easily penetrated a wealth of information is usually available to a hacker such as whether a door is unlocked, a garage door open, etc. Personal information, including credit card details, can also be at risk. A device may connect automatically to the internet without the owner fully appreciating the significance. The user usually has no control over the type of information made available to the host.

Furthermore, as well as being able to extract data from it, the host may have the ability to control the hub in certain ways and might be able to terminate service (e.g. in the event of a dispute). If security is inadequate a hacker might be able to hijack these powers.

Understandably, new owners of connected household gadgets tend not to go online to set up a username and password for the device, even if they had understood the reasons for doing so. Consequently the first *botnets* consisting of hundreds of thousands of IoT gadgets bombarding a target with a blizzard of messages to sabotage have already been detected.

6. Looking forward

Smart systems are superficially seductive and those supplying them tend to be well resourced major corporations with ambitious growth targets in this sector. Innovation and marketing departments of traditional and conservative businesses such as utilities, national network providers, consumer electronics suppliers and insurers may see association with smart products as demonstrating a progressive approach to technology and innovative consumer benefits. The public are inclined to trust such institutions but will this be misplaced if their management have not understood the risks to the customer?

By exploiting vulnerabilities in home automation devices, attackers will gather information on targets, placing at risk their property, privacy and safety and observing their behavior patterns. It would be ironic if those encouraged to have smart security in fact found themselves more exposed to crime than if they had done nothing. There are expected to be 50 billion IoT devices in use by 2020 and potentially huge volumes of data concerning the behaviour of populations could be harvested.

On the commercial front businesses have long recognised the economic benefits in the heating, ventilation and air conditioning (HVAC) field of building management systems and fire and security detection has been bundled with these systems for several years. Most serious construction projects, whether purpose designed or speculative, are likely to show that intelligent building control has been built in. Is there a risk that the poor

security standards of the consumer products currently flooding the market in this sector contaminate the commercial market? At least in the new build market standards do exist and are employed, for the communication bus at least, such as EN 50090 Home and Building Electronic Systems. Meanwhile, smart systems have started to penetrate the small business sector.

Some insurers are believed to view smart systems as having the potential to improve results through better intelligence. Household insurers could have access to very large volumes of data from which they can form an accurate picture of the composition of their business and the behaviours of their customers. On an individual basis occupancy levels could be monitored, and policyholders rewarded for keeping their houses reasonably heated with humidity controlled and security in operation whenever the house is unattended. The challenge for insurers might be that in order to put themselves in the position of gaining these insights they may be inadvertently supporting the adoption of security systems that actually form a security threat.

Furthermore, policyholders tempted or encouraged to have a smart system now will be difficult to convince of the need for a proper system should the value of their property increase or they be unlucky enough to suffer a serious burglary.

7. Recommendations

Until there is better order in the home automation and smart system market, and secure products to recognised standards are more clearly differentiated, it is dubious that householders and small businesses should be allowed to assume that these systems necessarily provide good security protection and insurers should consider their options for sensitively communicating this to their customers.

Insurers should also consider warning policyholders of the dangers of self-installation of off-the-shelf smart systems if they involve work on electrical circuits, boiler controls etc.

Insurers should monitor developments as the market inevitably matures and, as influencers, encourage the adoption of proper performance standards in the smart systems field.

Publishing house: VdS Schadenverhütung GmbH Amsterdamer Str. 174 • D-50735 Cologne • Phone: +49 (0)221 / 77 66 - 0 • Fax: +49 (0)221 / 77 66 - 341