Security industry standards – a research agenda

Weaver, Benjamin

2013

SRC 14 / LXM-BW4: Security industry standards – a research agenda

Benjamin Weaver

October, 2013

The traditional security industry: analog and fragmented

The electronic security industry is an interesting sector for the study of standards. In terms of technology, security systems encompass everything from electromechanical locks to complex IT and software. As modular components such as locks, card readers, sensors, detectors and cameras, are combined into integrated security systems, standardization of hardware and software interfaces is crucial to enable interoperability between products from different vendors.

The security industry value chain is highly fragmented – both upstream in terms of the number of brands and manufacturers in most product classes – and downstream in terms of the number of local installers and integrators that sell to the end-user. Despite this fragmentation, traditional security vendors have typically relied on proprietary interfaces in combination with legacy *de facto* technology standards carried over from other industries such as building automation (for e.g. access control) and television (for CCTV).

The lack of interoperability that follows from this fragmentation has allowed vendors to lock in customers to specific brands and systems. Many installers and integrators have also benefitted from the same customer lock-in effect, as they have become the preferred and certified supplier of a particular vendor's products in a local market.

Over time, security end-users have been accustomed to the single vendor, one-stop-shopping model, as it has proven an effective way to ensure that "everythings works". However, the absence of multi-vendor interoperability has often led to security sub-systems (e.g. video surveillance and access control) being installed in a stand-alone and non-integrated fashion. As organizations and facilities grow, it is also not uncommon to see several different generations of interoperable systems installed in conjunction or on top of each other. Servicing and maintaining such systems quickly become complex and costly, as each legacy installation needs its own specialist technician or vendor-certified integrator to run properly.

While siloed, non-integrated systems may have been tolerable – and sometimes even preferred – in the past, they run counter to the preferences of most current end-users who are increasingly calling for increased IT-driven integration, not only of the security systems under their control, but also between security and other corporate systems such as building automation and human resources.

SRC

The Standardisation Research Centre (SRC) promotes and organizes research about standards and the standardisation process. Examples of industrial objects of study are telecom, automotive, food, information technology software and hardware, energy, packaging and other consumer-related products. In addition, the operation of national and international standardisation bodies, which continue to be highly instrumental in the development and upholding of standards, are an important object of study.

www.srclund.org

LUSAX

Lusax is a multidisciplinary research project focusing on the transformation of the global security industry, with a an emphasis on the shift from analog to digital technology platforms, and its consequences for corporate strategy, global demand and supply, market expansion, and organizational management.

www.lusax.ehl.lu.se

Why the security industry has lacked standards

Security vendors are not unique in their use of proprietary interfaces to create customer lock-in. However, as a result of end-user network effects, most technology markets tend to consolidate towards a few dominant product platforms and companies over time.[1] Yet such platform consolidation has not historically been evident in the security industry. Several factors, which will be outlined and discussed below, have contributed to sustained fragmentation and lack of standards in the security industry:

- Absence of network effects
- End-user heterogeneity
- Low barriers of entry
- Security as a locally procured service
- Lack of price transparency
- Fragmented industry associations

Absence of network effects: From an end-user perspective, security systems exhibit an absence of network effects (also referred to as "network externalities" or "demand-side economies of scale") relative to many other technical systems. Some demand-side network effects – e.g. brand recognition and reputation – are in place for almost all product categories, including security. But by their very nature, security systems are supposed to be closed to the world outside the end-users organization. Hence, the utility a particular end-user derives from a security system, does not increase as other end-users adopt the same system. In fact, negative network effects could be said to exist, in the sense that a high degree of standardization of security systems would make them more vulnerable to breaches.

End-user heterogeneity: End-user needs and preferences across and within different vertical markets tend to be heterogeneous, with regards to the degree and type of sub-system integration. In a corporate office building, for example, integration of security systems and building automation systems is often desired, whereas in a retail setting, the integration of video surveillance and point of sales (POS) systems is more typical. The plethora of security use cases inhibits standardized solutions, and has led to vertical specialization both upstream and especially downstream in the security value chain, where smaller integrator firms focused on a specific vertical (e.g. retail or education) are common.

Low barriers of entry: Most security systems are composed of products that are highly modular and commoditized at the component level. Due to fragmented market share and the relatively small size of the total market for security prod-

Main takeaways

The security industry has traditionally been highly fragmented and vendors have opted for proprietary standards that induce customer lock-in. Several factors – including absence of network effects, end-user heterogeneity and low barriers of entry – have contributed to the dearth of standards.

The shift to digital product platforms did not initially change the structural dynamics that inhibit standards within the industry. However, as the security industry breaks away from vertical integration and is coming to resemble the modular IT industry, the need for increased interoperability has become a critical issue.

In recognition of the need for standards and interoperability, some of the industry's leading players decided to take matters into their own hands, launching tow industry-led consortia in 2008. By today, thousands of products that conform to standards issued by these consortia have been shipped. Through voluntary industry collaboration, a lot of progress has thus been made in a short period of time. Security industry standardization is however still in its infancy, and the competitive dynamics that will follow from these early efforts have just been set in motion.

[1] See for example: Cusumano, M. (2010). Technology Strategy and Management: The Evolution of Platform Thinking. Communications of the ACM, 53(1) and Henderson, B.

ucts, very few pure play security companies are able to fund innovation and R&D on critical components on their own. Instead, the security industry relies on innovation spillover from sectors such as consumer electronics and ICT, where companies such as Sony innovate at the critical component level (e.g. image sensors, and smart card chips[2]). With components as well as software widely available on the global market, a generic modular product such as a surveillance camera or an access control reader is not difficult or costly to design and OEM, leading to a profusion of brands and smaller players entering the security product market.

Security as a locally procured service: Security services have traditionally been procured and provided locally and regionally. The firms that install security systems have thus tended to be small and local. Lacking the resources necessary to develop high level, multi-vendor integration capabilities, local security firms usually rely on proprietary and "pre-integrated" products from a few known brands.

Lack of price transparency: The traditional security distribution channel has always been closed to outsiders, making it difficult for end-users to discern the product markups applied by downstream resellers and integrators. With hardware prices increasingly becoming available online, some installers seek to protect their margins by turning to lesser-known vendors that maintain a tighter control of their distribution.

Fragmented industry associations: Industry associations are typically important actors in standards setting efforts. Mirroring the industry they represent, security industry associations tend to be fragmented and have a national bias.[3] Having been built up in a previous era, they typically cater mainly to the vested interests of security incumbents, while largely ignoring the effects of recent digitalization. This may explain why recent industry association standardisation and interoperability initiatives have gained little traction at an industry-wide global level.

The shift to digital: the lure of IT interoperability

During the past decade the security industry has slowly but surely been undergoing a shift from analog and mechanical technology to digital and IT-based product platforms. During this transition, traditional vendors – and their vertically integrated product silos – have been disrupted by a new breed of IT-based security companies. As a result, the security industry is structurally starting to break away from vertical integration and coming to resemble the modular IT in-

[2] In contrast to the security sector, the markets for critical components, such as camera sensors and smart card chips tend to be dominated by a few companies.

[3] In Europe, the standardisation efforts of national industry associations are consolidated at the EU level, facilitating the creation of international standards.

dustry, where systems integrators create best-of-breed systems sourced from specialized hardware and software vendors.

In terms of standardization and interoperability, the digital era has nonetheless turned out to be worse than the old analog days in many ways. The fragmentation and the structural factors that inhibit standards have not changed, but rather increased as new digital players have entered the market. Where the old guard security incumbents aimed for customer lock-in, new digital vendors are trying to fight off commoditization from generic, low-cost manufacturers by leveraging proprietary technology and product features. As an example, ever since CCTV recording started to migrate from analog VHS cassettes to digital media, law enforcement in the UK and elsewhere have found it significantly more difficult to collect and play back recorded video material, due to the proprietary digital video codecs used by different vendors.

So while the industry's leading players continually tout the openness of IP-based networking and call for increased interoperability, they are also acutely aware that standardization is double-edge sword that may accelerate commoditization in what is a very price-sensitive market.

Towards a new era of security standardization

The situation outlined above has gradually led to an increased awareness within the industry that something has to be done. Despite hopes that a new era of digitalization and IT-fication would favor the adoption of open standards, the lack of interoperability have largely been carried over from the "old" analog to the "new" digital security industry. If left unabated, this situation could ultimately mar the industry's reputation, block the diffusion of new technology and hamper profitability and growth.

With standards initiatives from national security industry associations and formal standards bodies moving at a slow pace and struggling to keep up with new technological developments, some of the industry's leading players decided to take matters into their own hands. Hence, in 2008 two separate and partly overlapping industry-led consortia – ONVIF and PSIA – where launched to solve the problems of interoperability across vendors and between product classes.

By today, hundreds of companies have joined these organizations, and thousands of products that conform to the interface standards proposed by ONVIF and PSIA have already been shipped. Through voluntary industry collaboration, a lot of progress has thus been made in a short period of time. Security industry standardization is however still in its infancy, and the competitive dynamics that will follow from these promising early efforts have just been set in motion.

A security standards research agenda

The discussion above highlights many of the factors that make the security industry an interesting case and a fertile ground for empirically driven research on standards and standardization.

The security industry standards project aim to combine and integrate insights from the LUSAX and SRC research programs to investigate topics such as:

- Standards setting through consortia vs. formal standards bodies.
- Structural factors affecting standardization in an industry.
- Negative network effects and standardization.
- The role of standards in analog to digital technology migration.
- Standards and consequences for firm level competitive strategy.
- Interoperability, standards and dynamics of innovation.