Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-97

Standards for Cyber Security

STEVE PURSER
European Union Network and Information Security Agency (ENISA)

Abstract. Standards play a key role in improving cyber defense and cyber security across different geographical regions and communities. Standardizing processes and procedures is also essential to achieve effective cooperation in cross-border and cross-community environments. The number of standards development organizations and the number of published information security standards have increased in recent years, creating significant challenges. Nations are using standards to meet a variety of objectives, in some cases imposing standards that are competing and contradictory, or excessively restrictive and not interoperable. Other standards favor companies that are already dominant in their field. The European Union, with the support of ENISA, has started to include standards in its strategies and policies, but much remains to be done. The development and use of standards is necessary, timely, and requires the involvement of public and private sector actors working in tandem.

Keywords. Cyber security standards, national security strategies, European Union, cyber resilience, standard development organizations, standardization process.

Introduction

This paper explains why standards are important for cyber security, and especially for customers with stringent security and resilience requirements, such as defense organizations. Because they are so important, it is critical to consider both the benefits associated with adopting cyber security standards and the many challenges they present. This paper reviews some of these challenges before offering an overview of several key European Union (EU) initiatives in this area, and a short summary of the work that the European Union Network and Information Security Agency (ENISA) has carried out since 2009 on standardization. The paper concludes with a number of recommendations for enhancing the effectiveness and efficiency of cyber security standardization.

1. Background

In the recently published Cyber Security Strategy of the EU, 'the EU reaffirms the importance of all stakeholders in the current Internet governance model'[1] and reiterates its support for a multi-stakeholder governance approach. This is critical because the multi-stakeholder approach is fundamental for the development of successful standards, particularly in the area of cyber security, where private sector service providers are extensively involved in carrying out the implementation of public sector requirements.

A number of EU governments are now advocating a wider adoption and use of open standards. The UK government, for example, recently published a set of open standards for data and document formats and software interoperability for the government's IT specifications.[2] Open standards also play an important role in the EU's Digital Agenda. As stated by the European Commission's Vice President Neelie Kroes: 'Open standards create competition, lead to innovation, and save money.'

What is valid at the governmental level and in the EU often applies to other countries as well. The virtual world does not observe national borders, has no uniform legal system, and does not have a common perception of security and privacy issues. It is however, relatively homogenous in terms of technology.

The standardization activities of the private sector in the area of network and information security (NIS) tend to be driven by areas of work that are in line with the core interests of product developers or service providers (i.e., authentication, billing, etc.). Aligning public sector goals with standardization priorities of the private sector remains challenging.

Despite the difference in standardization priorities, both public and private sector information security practices can be improved by identifying and responding to evolving risks and technology developments. In particular, the time lag between the appearance of a new technology or technically driven business model and the availability of applicable standards is still too long.

2. Importance of Standards in Information Security and Cyber Defense

There are many reasons why standards play an important role in improving approaches to information security across different geographical regions and communities. Some of the more important reasons include:

- Improving the efficiency and effectiveness of key processes;
- Facilitating systems integration and interoperability;
- Enabling different products or methods to be compared meaningfully;
- Providing a means for users to assess new products or services;
- Structuring the approach to deploying new technologies or business models;
- Simplification of complex environments; and
- Promoting economic growth.

Standardizing processes and procedures is an essential part of achieving successful cooperation in a cross-border or cross-community environment. In the absence of standardization, both processes and communication can be rendered ineffective. An illustrative example is provided by the way in which different countries would react to a significant cyber incident. Here, in line with the principle of subsidiarity and the need to preserve sovereign state control, decision-making is made in a distributed environment and the processes that support this procedure must be optimal. Standardization would help ensure that various countries can interact with each other according to one set of procedures.

Similarly, standards such as ISO 27001[3] encourage the adoption of a standard organization structure, which makes it easier for customers to understand how processes work, and reduces the costs of auditing and due diligence. This is largely due to the fact that these organizational standards provide a blueprint for setting up a

management system for security, but also a blueprint for auditing and checking compliance of an organization to security best practices.

Standards play a key role in ensuring that security products can be put together into systems capable of detecting and responding to real events. In particular, standard interfaces and protocols make systems integration much simpler and allow products to interoperate in heterogeneous environments. Standardization of testing methods also makes it possible to compare security products in a meaningful manner ('benchmarking') and provides a means for the end user to assess new products or services. For instance, the level of compatibility of cryptographic modules with the FIPS 140-2 standard[4] (which is used to accredit such products) is used to assess the ability of such products to meet certain security requirements.

Standardizing the approach to deploying new technologies and business models helps reduce the complexity of the business environments that deploy them, which in turn makes it easier to secure the resulting environment. Although there is also an argument against such standardization, notably that any vulnerabilities associated with such systems would also be 'standardized,' opening the door for rapid, large-scale attacks. The usual way of dealing with this, however, is not to avoid standardization but rather to ensure that the defenses used to protect information systems are not critically dependent on a single system or type of system – this is the principle of defense in depth.

Last but not least, the use of standards encourages information exchange between developers and is likely to result in greater competition between companies developing products.

All these factors have a great impact on the overall preparedness of governments to counter the cyber threat. Standardized technologies and approaches enhance harmonization among cooperating countries, and ensure a larger pool of available experts and a higher level of knowledge of systems deployed.

3. Standardization Challenges in Cyber Security

Despite the fact that an appropriate use of standards is clearly beneficial in achieving a strong approach to security in a cross-border environment, there are also many challenges to achieving this in practice.

3.1. Organizational Challenges

Over the last ten years, a plethora of standard development organizations (SDOs) has been created. These organizations have been mostly initiated by industry (Oasis, W3C, Open Data Center, IETF, Adobe, ITIL and many others). This was partially an industry reaction to the large investment in terms of time and people required by 'traditional' SDOs[5] (such as the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU)), and partially the result of convergence where standardization traditionally focused on a specific sector (e.g. IEEE, MPEG, etc.) found applicability in many others. The number of SDOs and the number of published standards has increased, which can be a source of confusion for end-users.

3.2. Areas of Standardization

Industrial interests in standardization activities in the area of NIS tends to be driven by areas of work that are in line with the core interests of service providers (for example, authentication, billing, etc.). Although an increased general interest in the area of privacy is observed, specific interest of industry is expected to diminish, as privacy-enhancing technologies are perceived as being in conflict with commercial expectations.

At the time of writing, there is no single, continuous 'line of standards' related to cyber security, but rather a number of discrete areas which are the subject of standardization:

- Technical standards;
- Metrics (related mostly to business continuity);
- Definitions; and
- Organizational aspects.

Some areas are potentially over-standardized. There are several standards on information security governance and risk management.

In some areas standards are lacking, for example there are relatively few standards that address compliance with privacy and data protection legislation. Similarly, there are not many standards covering service levels, or more broadly, service agreements and service contracts, terms of use and conditions, etc. A quick look across the different offerings of cloud providers shows that every provider has a different (often long) legal text describing the terms of use and exceptions to obligations.

3.3. Lack of Agility

Designing and agreeing on standards is a lengthy process which is measured in months (in the best cases) to years. The information technology (IT) landscape, on the other hand, evolves rapidly. In order to remain useful, standards need to evolve at a comparable pace. Failure to do so will result in standards that are either obsolete or only partially applicable to real life environments.

One solution to this issue may be to use 'good practice' documents as precursors to standards. Such documents would be subject to change control procedures that are much less stringent than those applied to candidate standards and could therefore be developed to maturity more quickly. Good practice documents that are sufficiently mature could then be used as a basis for a corresponding standard.

3.4. Competing Sets of Standards

In some areas of information security there are several different groups of standards that are defined. To some extent, these standards are competing with each other for adoption and it is often difficult for the end user to judge which is best for their particular requirements. Occasionally, it is necessary to mix and match standards from different families in order to achieve the goal. For instance, when implementing Public Key Infrastructure (PKI), it is not unusual to see organizations adopt a combination of standards (for example X.509 (ITU) for the certificate format, PKIX (IETF) standards for core PKI and PKCS (RSA) standards for interfacing to secure devices).

3.5. Economic Considerations

Although some providers see their use of recognized standards as a unique selling point, there are also many cases of companies with a dominant position, who insist on their own proprietary standards and fail to constructively support and implement standards for their products. For instance, the fact that every mobile phone vendor uses different charger plugs is annoying for consumers, and wasteful in terms of resources. In order to resolve this situation, the EU had to take action to force vendors to adopt a single standard universal mobile phone charger plug.

Companies with a dominant position have few incentives to adopt interoperable standards, because it would only reinforce the position of their competitors. For a dominant vendor there are advantages to using proprietary standards, because they lock the customer in. This lock-in means that:

- The customer cannot buy or integrate compatible products from competitors, which generates more revenue for the provider.
- It is hard for customers to switch to another supplier, because they cannot easily move their data and processes to a competitor.

3.6. Lack of Awareness

Despite the clear disadvantages associated with the use of proprietary standards, there are still many examples of cases where customers (also in government organizations) fail to demand open standards. This may well be due to a lack of awareness.

4. EU Initiatives

4.1. The EU Cloud Strategy

Last year, the European Commission (EC) published its cloud strategy, entitled 'Unleashing the Potential of Cloud Computing in Europe.'[6] The strategy aims to improve the adoption of cloud computing in Europe so as to drive innovation and reduce costs in the EU's digital market. The main issue the cloud strategy is trying to address is the fact that the digital market for cloud services in the EU is currently fragmentized. In different countries public procurement processes use different requirements. On one hand, this means that it is hard for government bodies to get what they need because cloud providers do not change their offerings for small, individual customers. On the other hand, this fragmentation hinders the development of a EU cloud industry catering to Europe's need, because it is hard for providers to build one service and sell it to government bodies in different countries. A second goal of the strategy is to leverage the combined value of public procurement in the EU to improve adoption of cloud computing in the private sector as well. The cloud strategy has three key actions:

- Better use of Standards—the goal of this action is to gain a better understanding of the existing cloud standards landscape, and foster the adoption of standards and the development of voluntary certification schemes. As part of this activity, ETSI is asked to prepare a detailed map of standards,

and ENISA is asked to support the development of voluntary certification schemes.

- 'Safe and Fair Contract Terms and Conditions'—the goal of this action is to address issues with the legal framework around cloud computing, for example in regard to data protection, and derive more standardized and simpler contract terms and conditions for cloud computing services.
- 'Establishing a European Cloud Partnership to drive innovation and growth from the public sector'—the general idea is to agree on common requirements for procurement and use them to improve market offerings and speed up public procurement of cloud computing. Security and privacy requirements play an important role here.

All three actions are closely related to standardization of technology, requirements, and procurement processes.

ENISA is currently contributing to the EU cloud strategy action that maps existing cloud standards, and is also supporting the EC in deriving a list of certification schemes as a first step to supporting voluntary certification schemes as a way to improve trust in cloud computing services.

4.2. Open Standards in Information Communications Technology (ICT)

In June 2013, the Commission published the guide 'Against lock-in: building open ICT systems by making better use of standards in public Procurement.'[7] Although not specifically related to security, this recent EU communication underlines the need for a wide user of open standards in ICT. Open standards prevent lock-in of customers, and in this way both reduces costs and fosters competition and innovation in ICT. The communication argues that open standards could save an estimated one billion euros a year.

4.3. Cyber Security Strategy of the European Union

The European Commission published the Cyber Security Strategy of the European Union (EU CSS) on February 4, 2013.[8] This strategy provides a harmonized framework for the evolution of three different aspects of cyber security, which until recently had been evolving independently. In so doing, the Commission recognized and responded to the need to bring different communities together to improve the approach to cyber security across the EU, and laid the foundations for a more coordinated approach. The Cyber Security Strategy of the EU also includes a proposal for a Directive on Network and Information Security (NIS), which would require Member States (MS) to have minimum NIS capabilities in place, and cooperate and exchange information within a dedicated network, and demand the private sector to adopt NIS enhancing actions. The Strategy contains the following assertions:

- The EU reaffirms the importance of 'commercial and non-governmental entities, involved in the day-to-day management of Internet standards.'
- 'A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establishing voluntary EU-wide certification schemes building on existing schemes in the EU and internationally.'

- The Commission will support the development of 'security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing.'[9]

Under strategic objective four, the Commission asked ENISA to 'develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardization bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.'

This is a timely recommendation as the new ENISA mandate provided the Agency with a more proactive role in this area. The new ENISA regulation in this area tasked ENISA to 'support research and development and standardization, by facilitating the establishment and take up of European and international standards for risk management and for the security of electronic products, networks and services.'[10]

There are also recommendations for public and private stakeholders. In particular, the Commission encouraged public and private stakeholders to:

- 'Stimulate the development and adoption of industry-led security standards, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers;' and equip 'new generations of software and hardware with stronger, embedded, and user-friendly security features.'
- 'Develop industry-led standards for companies' performance on cyber security, and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market.'

An important part of the Cyber Security Strategy is the proposal for a Network and Information Security (NIS) Directive. This Directive asks the Member States to support standardization in the area of NIS:[11]

- 'Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.'
- 'Standardization of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at the EU level. To this end, it might be necessary to draft harmonized standards.'

Additionally, article 16 on standardization states the following:

- '…Member States shall encourage the use of standards and/or specifications to networks and information security.'
- 'The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.'

4.4. Cyber Security Coordination Group

In 2011, following a request of the Commission, the Standards Development Organizations CEN, CENELEC, and ETSI created the CEN–CENELEC–ETSI 'Cyber Security Coordination Group' (CSCG) to provide strategic advice in the field of IT security, Network and Information Security (NIS), and cyber security (CS). The main objectives of the CSCG are to:

- Establish a European standardization roadmap in the above mentioned areas.
- Act as the main point of contact for all *questions* by EU institutions related to standardization issues.
- Define and propose to the Commission a cooperation strategy between the EU and the US for the establishment of a framework, relating to standardization of cyber security.

ENISA has participated in and contributed to the activities of CSCG since its launch. Currently, the members of CSCG are working towards creating a first white paper addressed to the Commission, with strategic advice on priorities for R&D of EU funded research in this area, and ways to optimize EU research with mandates for cyber security standardization.

5. ENISA & Standardization

One of the tasks of ENISA, as put forward in its founding regulation, is to 'track the development of standards for products and services on Network and Information security.'[12]

Since 2009, ENISA has been identifying and elaborating on the work performed by standardization bodies (such as ISO, ETSI, ITU, CEN, CENELEC) relevant to its areas of work. One of the first deliverables in this area was a review of the state of standardization on the resilience of communications networks,[13] which at that time was not being addressed by the key standards development organizations other than as guidance for management processes. The report summarized and presented a number of findings covering the importance of correctly defining resilience in the context of standardization, the identification and presentation of the major activities undertaken by SDOs in security, and identification of key areas where further work is necessary.

Among other issues, the report also highlighted the lack of a consistent taxonomy for cyber security that identifies the role of resilience. ENISA therefore followed up on this initial report with a second one that provided an ontology of resilience alongside and embedding a taxonomy of resilience.[14] This study introduced two tools for understanding resilience as a network design target, and the output of those tools when applied to resilience. The tools introduced were classification using taxonomy, and relationship modeling using ontology with taxonomy at its core. This work was taken on board by the Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN) group of ETSI for possible future inclusion in a standard.

In addition to the work on specific areas, ENISA also facilitates cooperation between relevant EU actors (SDOs, EU organizations, industry), in order to address the shortcomings of standardization efforts. One way to achieve this would be through the promotion of best practices at the level of EU Member States through SDOs. In this particular case, ENISA would act as the interface between private and public sectors as well as interfacing with the SDOs.

ENISA has established working collaborations with SDOs and specific working groups (WG), such as ISO SC27 (collaboration agreement), ETSI (memorandum of understanding), CEN and CENELEC (collaboration agreement), and ITU SG17 (informal collaboration). These agreements allow for, among others:[15]

- 'ENISA's participation as observers in, and if appropriate, chairing of identified technical committees, their working groups, and workshops to support the preparation of European standards'.
- Evaluation of relevant ENISA research results by SDOs 'and their transfer to standardization activities'.
- 'The dissemination and promotion of information on publications, results, meetings, and seminars'.
- 'The provision of mutual support on promotional activities and in establishing industrial contacts and research networks for network and information security standards-related tasks'.
- 'The organization of topical workshops, conferences, and seminars addressing technology and research issues related to network and information security standardization activities'.
- 'The exchange of relevant information on topics of common identified interest.'

Finally, ENISA has also responded to the World Wide Web Consortium's (W3C) call for comments on the final draft of the HTML 5 specification by performing a security analysis of the standard, and making specific recommendations regarding security flaws and the security and privacy of APIs in the standard.

Recommendations and Conclusions

The following general recommendations on development and the use of standards can help NATO Member States in many areas critical to cyber security and cyber defense. These range from standardization processes and enforcement of regulations, to definition of effective practices for verification of security in national security relevant systems, to identification of standards for specific R&D areas. Recommendations are as follows:

1) Policy-makers should continue to encourage vendors to agree on the use of standards, and encourage both private and public sector organizations to include references to these standards in procurement processes.
2) Governments should incorporate standardization as part of their national cyber security strategies. Emphasis should be given to improving the coordination between policy and operational levels, and enhancing the role of public-private partnerships in standardization processes.
3) National Regulatory Authorities should make greater use of standards as a point of reference in enforcing regulations.
4) Public institutions involved in the funding of research and development should identify consistent sets of standards for different research areas. Where appropriate, publicly funded research should require compliance with these standards.
5) Standards Development Organizations should work together to identify ways of speeding up the standards development process for cyber security related standards. This might be achieved by a 'fast track' mechanism.
6) Governments of cooperating countries should work together to define a broad certification scheme allowing end users to verify that services or products upon which they rely comply with security standards.

Specific recommendations targeting resilience against cyber threats:

7) Work items should be actively promoted in the SDOs (e.g., through a mandate) to support the specification of metrics, and supporting test and validation criteria to be used in resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis).
8) Work items should be actively promoted in the SDOs (e.g., through the means of a mandate) to support the development of taxonomy for resilience.
9) SDOs should ensure that resilience aspects are addressed systematically in ICT-related standards.

References

[1] European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final). Brussels: European Commission. [online] Available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> [Accessed 17 November 2013].
[2] UK Cabinet Office, 2012. Open Standards Principles – for software interoperability, data and document formats in government IT specifications. [online] Available at: <http://ofti.org/wp-content/uploads/2012/12/46907_Open-Standards-Principles-FINAL.pdf> [Accessed 17 November 2013].
[3] International Organization for Standardization, 2005. ISO/IEC 27001 Information technology. Security techniques. Information security management systems. Requirements. [online] Available at: <http://www.iso.org/iso/catalogue_detail?csnumber=42103> [Accessed 28 October 2013].
[4] National Institute of Standards and Technology, 2001. FIPS PUB 140-2 Security Requirements for Cryptographic Modules. [online] Available at: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf> [Accessed 28 October 2013].
[5] Investments required by SDOs are usually very demanding in terms of time and human resources. The development of a standard, indeed, can require years of discussions, multiple drafts, and various work meetings. It is almost impossible to quantify the exact time spent developing a standard, but ISOs usually spend an average of 6 years to issue a standard, and ETSIs about 4.
[6] European Commission, 2012. Unleashing the Potential of Cloud Computing in Europe (COM(2012) 529 final). Brussels: European Commission. [online] [Accessed 17 November 2013]. Available at: ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf>
[7] European Commission, 2013. Against lock-in: building open ICT systems by making better use of standards in public procurement (COM(2013) 455 final). Brussels: European Commission. [online] Available at: <http://www.austria.gv.at/DocView.axd?CobId=52046> [Accessed 17 November 2013].
[8] European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final). Brussels: European Commission. [online] Available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> [Accessed 17 November 2013].
[9] Ibid. Cybersecurity Strategy of the European Union.
[10] Council of the European Union, 2012. Proposal for a Regulation of the European Parliament and of the Council concerning the ENISA. Council of the European Union. [online] Available at: www.statewatch.org/news/2012/oct/eu-council-enisa-position-14865-12.pdf> [Accessed 17 /11/2013]
[11] European Commission, 2013. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final). Brussels: European Commission. [online] Available at: <http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf> [Aceessed 17 November 2013].
[12] ENISA, 2004. REGULATION (EC) No 460/2004 of the European Parliament and of the Council [online] Available at www.enisa.europa.eu/?came_from=http%253A//www.enisa.europa.eu/activities/res-old/technologies/std/std> [Aceessed 17 November 2013].
[13] Gorniak, S., Saragiotis, P., Ikonomou, D., Cadzow, S., de Couessin, C., Mueller, A. and D'Antonio, S., 2009. Gaps in standardisation related to resilience of communication networks, ENISA study. [online] Available at: <http://www.enisa.europa.eu/publications/archive/gapsstd> [Accessed 28 October 2013].
[14] Vlacheas, P., Stavroulaki, V., Demestichas, P., Cadzow, S., Gorniak, S. and Ikonomou, D., 2011. Ontology and taxonomies of resilience, ENISA report. [online] Available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/ontology_taxonomies> [Accessed 28 October 2013].
[15] European Unition Network and Information Security Agency (ENISA), 2013. Cyber Security Collaboration Agreement Between ENISA and European Standardisation Bodies, CEN and CENLEC. [press release] Available at: <http://pr.euractiv.com/pr/cyber-security-collaboration-agreement-between-enisa-european-standardisation-bodies-cen-and> [Accessed 17 November 2013].