Standard-Making in Information Security: A Literature Review

Kalle Räisänen
Örebro University School of Business, kalle.raisanen@oru.se

Follow this and additional works at: http://aisel.aisnet.org/wisp2012

Recommended Citation
http://aisel.aisnet.org/wisp2012/31

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Standard-Making in Information Security: A Literature Review

Kalle Räisänen
CERIS – Centre for Empirical Research in Information Systems, Örebro University School of Business, Örebro University, Sweden

ABSTRACT

Information security standards have an important role in the development of organizational information security. They are seen to represent best practices in the field and act as a starting point for creating procedures that are implemented in organizations. As with every artifact information security standards are the result of design processes; actors participate in a negotiation process when designing artifacts and actors are not equal in the power they exercise in these processes.

This paper presents a review of information security literature, investigating the nature and extent of information security standard-making research, to find in which, if any, ways the design processes of information security standards, the making of information security standards, have been researched.

Of 924 papers published between 1985 and 2013 mentioning information security and standards, only eight were found to deal specifically with standard-making, and only one of those studied methodically the processes of negotiation underlying information security standards; the other papers dealt only with formal or technical aspects of standard-making. Thus, there is little research on information security standard-making, and what research is done is to a large part descriptive rather than analytical.

1 Corresponding author. kalle.raisanen@oru.se +4619301106
This lack of research into the negotiation and power processes of information security standard-making represents a large gap in the field, with consequences for both researchers and practitioners: while information security standards are important and widely touted in the field, their making is as yet unstudied, the underlying processes of that making as yet not understood, and thus the claim that standards correctly reflect best practices as yet unfounded. Practitioners cannot be sure that standards represent the best practices of their field, and consequently cannot place their trust in them.

Future work in the field should investigate much closer the negotiation processes that underlie information security standards, for example through case studies following standards as they develop in standardization organizations such as ISO and its national constituents. This research must take into account both the technical and social factors which influence standards and their making.

**Keywords:** information security, standard-making, standardization, literature review

**INTRODUCTION**

**Background**

Information security standards have an important role in the development of organizational information security. They act as a starting point for creating procedures that are implemented in organizations. In the case of information security there is a long tradition of standards, both national and international. The most commonly discussed today is probably the ISO-27000 series (ISO, 2005a, 2005b, 2008). Although there is a large body of research on information security policy (e.g. Doherty, Anastasakis, and Fulford, 2009; Cresson Wood, 1995;
Siponen and Iivari, 2006; Lindup, 1995; Knapp, Franklin Morris Jr., Marshall, and Byrd, 2009; Doherty and Fulford, 2005, 2006), and much consensus can be found with regard to the importance of information security policies, the use of information security standards has been criticized, since they do not take into account differences among organizations (Baskerville, 1993; Baskerville and Siponen, 2002; Dhillon and Backhouse, 2001).

This criticism of information security standards seems relevant, but does not say much about the goals and values that organizations inject into their businesses through the use of standards. As with every artifact an information security, a standard is the result of a design process (Friedman, 2003), and earlier research in the field of information systems has shown that such processes inscribe different actors’ goals and values (e.g. Hedström, 2007; Karlsson and Ågerfalk, 2009). Hedström (2007) has also shown that actors participate in a negotiation process when designing artifacts, and that actors are not equal in the power they exercise in these processes. It means that power relations between the participating parties affect the final design.

There is therefore a need for a better understanding of the development process of the information security standards that are used as starting point for so much information security work in organizations.

This paper tries to add to that understanding through a review of information security standard-making literature, and is organized as follows: in the present section I lay out the background of the paper, give an overview of general information systems standard-making research, and present the aim and research questions upon which the paper is based. In section 2, I present the method used to conduct the literature review. Next, I present the results of the literature review in section 3. Finally, in section 4, I discuss the implications of those results,
draw conclusions about their consequences for research and practice, and give suggestions for future research.

**Related work**

That the social and socio-technical processes underlying standard-making in information systems (IS) have received increasing focus is evidenced by MIS Quarterly’s special issue on information systems standard-making in 2006 (Lyytinen and King, 2006), in which standard-making was described as “a critical research frontier”.

This socio-technical focus is characterized by problematization of standard-making and an emphasis on issues of negotiation and power. This includes investigating how actors influence or try to influence standard-making—e.g. how firms “ambush” standard-making through patents (Hemphill, 2005), how a countries try to gain control of standards (Lee and Oh, 2006), or how established actors become entrenched (Grøtnes and Kristoffersen, 2010). Other research focuses on how standardization bodies and their standards shape and are shaped by their members—how the politics of the engineers responsible for creating Internet technologies influenced Internet standards (Russell, 2006), how standards with open standard-making processes “defeat” competing standards with more closed processes (Russell, 2006, 2012; Jain, 2012), or how the features of standardizing bodies replicate themselves in the standards they make (Werle, 2001; Graham, 2011).

The focus of standard-making research on negotiation and power is reflected also in the theories used, e.g. institutional theory (Werle, 2001; Graham, 2011), critical theory (Russell, 2012), Actor-Network Theory (Hanseth, Jacucci, Grisot, and Aanestad, 2006; Grøtnes and Kristoffersen, 2010; Lee and Oh, 2006).
Aim and research questions

This paper presents a review of information security literature, with the aim of investigating what research has been done on information security standard-making, and what the nature of that research is. The review is guided by the following research questions:

1. How much research has been done on information security standard-making?
2. What is the nature of that research?, i.e. What are the research questions, methods, and theoretical frameworks used?

METHOD

This paper uses a concept-centric literature review, per Webster and Watson (2002), to investigate the extent and nature of research into standard-making within the field of information security: The extent (RQ1) of the research is found through simply counting how many papers there have been dealing with information security standard-making; the nature (RQ2) of the research is found by analyzing which research questions, research methods, and theoretical frameworks the papers purport to use.

Selection of papers

Articles were found using the article search engine Scopus², using the search phrase “{information security} standard”. I chose these keywords to cast a wide net and try to gather as many papers as possible dealing with information security and standards. The search yielded a

²http://www.scopus.com/
total of 930 papers\textsuperscript{3}, of which six were duplicates, for 924 unique papers, published between 1985 and 2013.

I read through the titles, abstracts, and keywords of those papers, selecting the ones which professed to cover the development processes of information security standards. Note that, as evidenced by the choice of keywords, I rely on the papers’ own definitions of “standard” and of “information security”; if a research paper claimed to study standardization and information security, it was included. After excluding duplicates, this first selection yielded 62 papers.

**Analysis**

To analyze these papers, a concept-matrix was inductively constructed by having three researchers (the author and two further researchers) jointly classify 15 randomly selected papers from the data set, looking for recurring themes in how standards and standard-making were studied, in terms of, e.g., research objects and methods. The resulting matrix had the following headings:

1. Author and year.
2. Aspect of standardization studied in paper. These categories can overlap, so one paper can study standards in several ways. This heading helps answering \textit{RQ1}, not only by finding the number of papers dealing with standard-making, but also by giving a comparative measure of what other aspects of standards are studied. The aspects of standardization studied that we found were:
   (a) Standard-making: The formal and informal processes that result in a standard.

\textsuperscript{3}Search conducted August 20, 2013.
(b) New standard developed: The paper proposes a new standard or modification of an existing standard, without explicitly studying the standard-making process.

(c) Use or implementation: The paper discusses using standards or implementing standards-based systems.

(d) Evaluation: The paper evaluates standards based upon practice or theory.

(e) Overview of standard: The descriptive presentation of one or more standards.

(f) Literature review: The paper presents a literature review.

3. Theoretical framework used—e.g. Actor-Network Theory, Circuits of Power, etc.

4. Research question.

5. Research method—e.g. case study, literature review, action research, etc.

This matrix was validated by having the same three researchers independently classify 10 further randomly selected papers. Comparing the classifications of the three researchers, we found that they agreed fully upon the classifications of seven of the papers, and partially on the remaining three papers; differences in classification concerned the boundary between “Evaluation” (2D) and “Use or implementation” (2C). These differences were resolved through stricter definitions of the two categories. Given the high degree of agreement among coders, the concept matrix was considered validated, and it was then used by the author to deductively analyze the content of the remaining 37 papers.

Given the aim of this paper, the papers belonging to the category 2A, i.e. those papers explicitly dealing the the standard-making process, were most interesting to analyze further. Thus, I focused my analysis upon those papers.
RESULTS

A total of 62 papers were included in the final analysis. The full list of papers is presented in Appendix A, while the results for the papers concerned with standard-making are presented in this section.

Table 1. Aspects of standardization studied (overlapping).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>26</td>
<td>3</td>
<td>7</td>
<td>23</td>
<td>3</td>
</tr>
</tbody>
</table>

The aspects of standardization studied in the papers are summarized in Table 1. While nearly half of the papers (26 out of 62) propose new, or modifications of existing, standards (2B), only 8 papers (no overlap with 2B) concern the standard-making process (2A). The theoretical frameworks, research questions, and research methods of the eight papers studying standard-making are presented in Table 2.
Table 2. Research framework, question, and method.

<table>
<thead>
<tr>
<th>Author, Year</th>
<th>Theoretical framework</th>
<th>RQ</th>
<th>Research method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anon, 1988</td>
<td>N/A</td>
<td>Who shall be responsible for standards-development (on a national level)?</td>
<td>N/A</td>
</tr>
<tr>
<td>Backhouse et al., 2006</td>
<td>Circuits of Power</td>
<td>“We aim at establishing the influence of exogenous contingencies for the creation of a standard and theorize about the power mechanisms required for a standard to evolve from an idea into an obligatory passage point for organizations and agencies”</td>
<td>Case study</td>
</tr>
<tr>
<td>Dent, 2010</td>
<td>(Standard model)</td>
<td>“This article will investigate the methodology that is used produce these standards and their meaning for an organisation who wishes to implement public-key”</td>
<td>N/A</td>
</tr>
<tr>
<td>Krull, 1996</td>
<td>GSSP (Generally-Accepted System Security Principles)</td>
<td>“Is there a need for standards? How detailed should standards be? When do standards make sense? When don’t standards make sense? Who enforces standards?”</td>
<td>N/A</td>
</tr>
<tr>
<td>Manning, 2006</td>
<td>N/A</td>
<td>“This paper uses the example of information security to consider ways of ensuring that standards development matches evolving market needs within appropriate timeframes.”</td>
<td>N/A</td>
</tr>
<tr>
<td>Pounder, 2001</td>
<td>N/A</td>
<td>What is the EU’s role in standardization</td>
<td>N/A</td>
</tr>
<tr>
<td>R. Ross et al., 2005</td>
<td>N/A</td>
<td>“This paper includes a discussion of NIST’s FISMA risk management framework (RMF) and the suite of related standards and guidelines being developed by NIST to help federal agencies comply with FISMA requirements (i.e., the FISMA suite of documents)”</td>
<td>N/A</td>
</tr>
<tr>
<td>Williams, 2006</td>
<td>N/A</td>
<td>“suggests that a more holistic approach is taken to the development of standards, in which standards and associated context specific guidelines are developed”</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Of those eight papers, only one (Backhouse et al., 2006) has an explicit theoretical framework (namely, “Circuits of Power”), while the remaining papers were either purely argumentative, or technically focused (e.g., Dent (2010), who discusses the motivations behind key lengths in cryptography standards; though one could argue that Dent’s theoretical framework is standard model cryptography). Backhouse et al., 2006 was also the only paper to use a specific research method (case study), while the other papers are primarily based upon argumentation or description. Three of the papers (Anon, 1988; Pounder, 2001; R. Ross et al., 2005) discuss public sector involvement in standardization – Anon, 1988 whether US standard-making should be led by the National Security Agency or the National Bureau of Standards, and Pounder (2001) discusses EU involvement in standardization, while R. Ross et al. (2005) describe the impact of the Federal Information Security Act on NIST standardization activities. A further three papers (Krull, 1996; Manning, 2006; Williams, 2006) discuss how to improve standard-making in general and formal terms. Krull (1996) discusses the need for standardization, Manning (2006) discusses making standards adaptive to quickly-changing markets, and Williams (2006) argues for “a more holistic approach” in standardization. Of the remaining two papers, Dent (2010) deals with lengths of cryptographic keys in standards and how they are chosen, while Backhouse et al. (2006) looks at how the standard-making process is shaped by circuits of power.

Looking at the research questions of the eight papers, one of them papers has a clear focus on issues of power and negotiation (Backhouse et al., 2006) similar to that found in the general IS field, while the others are concerned primarily with formal (Pounder, 2001; Anon, 1988; R. Ross et al., 2005) aspects of standard-making or technical issues (Dent, 2010). The ones whose research questions approach the negotiation aspect—Krull, 1996; Manning, 2006;
Williams, 2006—are still focused solely on the technical and formal aspects of standard-making in their methods and results.

DISCUSSION

In this section, I will go back to the research questions, and—based upon the results presented above—answer them one by one:

RQ1. How much research has been done on information security standard-making?

Of 924 papers published between 1985 and 2013 mentioning information security and standards, only eight were found to deal specifically with standard-making. Thus, there has been little work done on information-security standard-making.

RQ2. What is the nature of that research?

Only one of the eight papers dealing with information-security standard-making (Backhouse et al., 2006) has an explicit focus on the negotiation process underlying standard-making; the other seven papers dealt only with formal or technical aspects of standard-making. In addition, when looking at RQ2—which research questions, methods, and frameworks the papers use (Table 2)—we see that only one (again Backhouse et al., 2006) is concerned with investigating the negotiation processes behind standard-making, rather than simply describing its technical or formal features. Even if the others have power and negotiation implicit in their research—e.g. the issue of regulators influence on standard-making in Pounder, 2001, R. Ross et al., 2005, and Anon, 1988—none of them deal with it explicitly or systematically. Thus, what research is done is to a large part descriptive rather than analytical, and there is a distinct lack of
focus on the social part of the socio-technical processes which create standards, as compared to general IS standard-making research.

**Conclusions**

According to Andrew L. Russell, “stories about standards are necessarily about power and control” (Russell, 2012, p. 80), which is a view we have seen is echoed in much standard-making research, but not in the information-security standard-making research studied in this paper. The results of this review echoes the state of the general information systems field a decade ago; as reported by Lyytinen and King (2006), in 2002 only 2 per cent of published journal articles dealt with standards, and most of that work was descriptive and content-focused, not focused on the processes underlying standard-making. A situation very much similar to the one in information security research today, as represented in the literature reviewed in this paper.

This lack of research into the negotiation and power processes of information security standard-making represents a gap in the field, with consequences for both researchers and practitioners: while information security standards are important and widely touted in the field, their making is as yet unstudied, the underlying processes of that making as yet not understood, and thus the claim that standards correctly reflect best practices as yet unfounded. This means that practitioners cannot be sure that standards represent the best practices of their field, and consequently cannot place their trust in them.

**Future work**

Future work in the field should investigate much closer the negotiation processes that underlie information security standards, for example through case studies following standards as
they develop in standardization organizations such as ISO and its national constituents. This research must take into account social factors of negotiation and power which influence standards and their making.

ACKNOWLEDGEMENTS

This research was funded by the Swedish Civil Contingencies Agency through the SECURIT (Information Security Culture) project, and by the research school Management and IT.

REFERENCES

References marked with an asterisk indicate papers included in the literature study.


