December 2004

Rating Certificate Authorities: a market approach to the Lemons problem

James Backhouse
London School of Economics

John Baptista
London School of Economics

Carol Hsu
London School of Economics

Rating Certificate Authorities: a market approach to the Lemons problem

James Backhouse
London School of Economics
james.backhouse@lse.ac.uk

John Baptista
London School of Economics
j.m.Baptista@lse.ac.uk

Carol Hsu
London School of Economics
w.y.hsu@lse.ac.uk

ABSTRACT

This paper re-examines the problem of information asymmetry in the digital certificates market (Backhouse et al., 2003). It aims to discuss how market mechanisms such as rating systems may be more efficient than regulatory interventions in resolving the Lemons problem in this market. In this research, we discuss the concept of rating systems in the economics literature, and explore their value as signaling devices for overcoming asymmetries of information and promoting trust between certification authorities and relying parties. To operationalize this concept, we further suggest the use of semantic analysis as a method to signal the operational risk associated with each certificate authority. We also provide an example of how semantic analysis may be used as a technique to rate the operational risk of certificate authorities. The paper contributes to the current efforts seeking to resolve problems of trust in the digital certificate market, and provides some conceptual ideas for further research in this area.

Keywords

Economics of IS Security, Public Key Infrastructure, Interoperability, Rating Systems, Semantic Analysis.

INTRODUCTION

The value of using economics theory in research in the information systems field is well documented; see for example Malone, Yates and Benjamin (1987); Ciborra (1993); and Wigand (1997). Recently, economic theory has gained new importance for research in the information security field. This new approach in IS Security research complements the more predominant legal and technical rationales in understanding the dynamics that lead to a secure system. Research in this area has been greatly developed by researchers at Cambridge University[1] and by those who attend the annual Workshop on the Economics of IS Security[2].

The point of departure for this approach is the acknowledgment that economic interests underpin all implementations of security technologies. For example, suppliers of security systems are in business for profit maximization. Buyers also weigh costs and benefits before purchasing these products and services. These two sides, supply and demand, form the basis of markets. The study of their dynamics is important in order to grasp the essence of a secure system. We take this market approach to study the global market for digital certificates, where Certificate Authorities (suppliers) sell digital certificates (product) to a growing number of companies and individuals (demand) wishing to conduct trustworthy transactions over the internet. Our analysis arises from the complexities of global open e-commerce and does not directly apply to the more closed and mediated domains of e-commerce, such as the EDI networks. At the global e-commerce level, organizations tend to experience an increasing number of new commercial relationships with an greater number of unknown business partners from foreign domains. In this context, digital certificates are used as trust mechanisms between the different agents involved in commercial exchanges.

[1] www.cl.cam.ac.uk/~rja14/
[2] http://www.cpppe.umd.edu/rhsmith3/

This paper follows the work of Backhouse, et al. (2003), which applies the Lemons economic theory developed by Akerlof (1970) to examine the existence of quality uncertainty and asymmetrical information problem in the digital certificate market. In their research, they also examine the effectiveness of signaling countermeasures to this problem. The use of branding, licensing and guarantees are discussed as mechanisms to signal quality and overcome asymmetries of information.

Although we subscribe to the argument underlying the work of Backhouse et al. (2003), we consider an alternative signaling mechanism for addressing the Lemons problem in the digital certificates market. In contrast to more formal mechanisms based on governmental intervention or regulation, we put forward the concept of a rating system offered by private firms as a market solution for resolving the Lemons problem.

The organization of the paper is as follows. The paper commences with a brief description of the digital certificates market and the intrinsic sources of quality uncertainty. In the following section, we look at the concept of signaling as a countermeasure to this problem. We then propose a specific signaling countermeasure based on a rating system following the work of Thakor (1982). In the final section we present semantic analysis as method for the development of the rating system and sketch how this method may be used to rate certificate authorities according to their operational risk.

2. SOURCES OF QUALITY UNCERTAINTY IN THE DIGITAL CERTIFICATES MARKET

The design for the digital certificate market works as follow. A subscriber (individual or organization) acquires/buys a digital certificate from a Certification Authority (CA) for the purpose of exchanging confidential electronic messages or contracts with a relying party. Relying parties make a decision on whether to accept the certificate as an online trust token by balancing the risk (potential cost of a loss) and the perceived trust in the CA's technology, procedures and legal environment. However, not all CAs use the same technology or employ the same procedures in the issuance of digital certificates. Therefore, not all certificates are produced in quite the same way and hence there is no standard quality. The market is populated with digital certificates of widely differing quality.

In the digital certificates market, the quality of the certificates can be evaluated on the basis of the cryptosystems employed by the CA, by the procedures adopted to check identity and by the legal domain in which a CA is embedded. However, we argue that this information is not perfectly available to the relying parties, either because of their insufficient knowledge of law and technology or their inability to access information from the CA. This creates the problem of asymmetry of information. Some CAs may conceal the shortcomings in their procedures taking advantage of the inability of relying parties to assess the quality of the digital certificates. In this market, good quality digital certificates are not readily distinguishable from bad quality certificates. Thus, from an economic perspective, the market offers no incentive for the production of high quality digital certificates. Following the argument presented by Akerlof (1970), bad quality digital certificates would drive out good quality certificates and, in the long term, the market could cease.

Recognizing such a problem and adopting the countermeasures proposed by Akerlof (1970), Backhouse et al. (2003) discuss how effectively the signaling devices, i.e. guarantee, brand name and licensing, are working in the digital certificate market. In the analysis, they show the current status of different intervention mechanism and examine the difficulties related with the implementation of each method. For example, in terms of guarantees in the market, they identify that the Certificate Practice Statements from different CAs, exhibit differences in the sections on "limitation and warranty". Although similar texts are enforced by the industry "standard" (RFC 2527) many CAs have different policies. They contend that with no case law yet to establish precedent, it is unclear which laws might apply to digital certificates and how the courts might apply them.

In this paper, we share the view with Backhouse et al. (2003) regarding the contention that the digital certificates market inherits the problem of asymmetry of information. However, we propose a different solution to this problem. We argue that a market solution arising from a private initiative may be more efficient than guarantees, branding or licensing countermeasures. This point is argued by Steckbeck and Boettke (2001) who stated that *"what Akerlof's models tend to ignore is the dynamism of markets and the incentive mechanism driving entrepreneurs to discover ways to ameliorate problems associated with market exchange."* (Page 8). In the light of this argument and the inefficiency of current

institutional initiatives to overcome the vicissitudes in the take up of the digital certificates market, we are proposing the adoption of a market-oriented solution. We argue that this market approach will more efficiently deal with the underlying economic Lemons problem in the digital certificates market than the alternative initiatives described by Backhouse et al. (2003).

In the next section we discuss the concept of the rating system as a signaling device and review economic literature on rating systems. We then propose a specific method for how such an idea may be implemented in the digital certificate market. Section four shows how semantic analysis may be used as a method for rating certificate authorities according to their operational risk, thus signaling quality of the digital certificates they produce.

THE RATING SYSTEM

The existence of a Lemons problem in the digital certificate market described in the previous section can be remedied through the use of signaling countermeasures (Backhouse et al., 2003). The concept of signaling is based upon the idea that the Lemons problem can be prevented if *a priori* imperfectly informed buyers of a given product can somehow revise their initial conditional estimate of product quality (Thakor, 1982).

Signaling may be effected in three different ways. The first, presented by Spence (1973, 1974, 1977), Bhattacharya (1979, 1980) and Ross (1977), is based on the concept that the seller generates costly signals to the market to demonstrate product quality. The second and third are both based on the idea of having a Trusted Third Party in the market working as information providers. In the second case, proposed by Campbell & Kracaw (1980), a Trusted Third Party emerges in the market as an intermediary and sells information about the quality of the products to their buyers. In the third case, proposed by Thakor (1982), the Trusted Third Party emerges from the seller's interest in providing credible information to the market about their product quality. Thakor examines markets where this third signaling solution is present and demonstrates how market equilibrium is achieved in this model. In this paper we follow Thakor's economic model and propose the creation of a rating system where CAs pay for and supply information to another Trusted Third Party which assesses and rates the quality of the digital certificates produced. This Trusted Third Party will then freely release this information to the relying parties. Relying parties will then use the rating information to make decisions on whether to take the digital certificate as a trust token or not for any given purpose.

The rating literature is vast and closely related to the bonds market rating literature. The role of the rating agencies (such as Standard&Poors or Moody's) in the bonds market is perhaps the most important application of rating systems as signaling devices working to overcome asymmetries of information. Pogue and Soldofsky (1969) describe the history and importance of the rating systems in financial markets. They explain how rating systems emerged in financial markets, *"Corporate bond ratings were developed prior to World War I in response to a commercially viable need for independent and reliable judgment about the quality of corporate bonds"* (Pogue and Soldofsky, 1969: page 203). Rating services have, therefore, emerged as a countermeasure to quality uncertainty and asymmetrical information in the bonds market. Rating agencies emerged to exploit commercially this business opportunity. We theorize that the bonds market solution to the Lemons problem is a good model and a solid basis for the development of a similar solution in the digital certificates market.

The establishment of successful rating system relies upon the credibility of the Trusted Third Party and its ability to fairly rate the quality of the products in the market. This is a high barrier to enter this market; rating agencies have to develop good reputation and have recognizable credibility (Campbell and Kracaw 1982). We suggest that existent rating agencies in the financial markets such as Standard&Poors and Moody's may be in a better position than new businesses to provide this service in the digital certificates market. These agencies could extend their expertise and reputation in the financial rating industry to rate certificate authorities' operational risk and the quality of the digital certificates in the market. Rating agencies such as Standard&Poors and Moody's have great expertise in rating bonds in financial markets; however, to exploit the new market for rating CAs, they would need specific techniques to rate CA's operational risk. Therefore, one of the critical issues in the development of this solution will be the creation of the appropriate method to be employed by the rating agency to rate CA's operational risk. In section four we show how semantic analysis may be employed for this purpose.

Ang and Patel (1974) review and compare the effectiveness of the rating techniques employed by the rating agencies for predicting the quality of bonds. More recently, Crouhy, Galai and Mark (2001) have also reviewed the techniques employed by the two leading rating agencies, Moody's and Standard&Poors. These techniques aim at assessing the financial risk of each bond and to distinguish those with high risk from those with low risk so that investors can manage the balance between risk and return. It is important to note that the rating system does not intend to bar low quality products (bonds) from the market, unlike other governmental interventions such as licensing. Instead, by signaling quality (high risk and low risk), it allows for the existence of niche markets for a range of quality levels.

We argue that the development of a model based on the existence of a Trusted Third Party to assess and rate certificate authorities supports four main benefits. First, assessing the operations of certificate authorities requires considerable investment in specialized tools and expertise: only a large organization aiming to sell this information will find justification for the necessary investment. A sole relying party would scarcely be able to develop these techniques by itself. Secondly, this approach complements the formal and legal solutions which have so far had only limited success in overcoming asymmetries of information. Third, relying parties would get quick, free and clear information about the quality and risk involved in accepting a digital certificate as a trust token, something that would otherwise be difficult to obtain. Finally, the rating system might trigger an improvement in the overall quality of digital certificates in the market, as a result of the additional motivation for the CAs to achieve higher ratings.

The rating system here proposed will work as a signaling mechanism which will overcome the Lemons problem as presented by Spence (1973). However, as shown by Campbell and Kracaw (1980) merely resolving market information asymmetries does not necessarily lead to market equilibrium solutions. This means that the signaling method proposed has to work in such a way that all parties involved in the production and consumption of the ratings reach market equilibrium. One may contend that the rating system is reiterative, in the sense that the Trusted Third Party which assesses and rates the CAs also itself needs to be checked by another entity and hence there is no logical end to this cycle. This issue is discussed in detail by Backhouse (2002). We argue that this cycle may only terminate when the market is prepared to accept and recognize a signal as a legitimate source of reliable information. The best example of this is the rating agencies in the bonds market such as Standard&Poors and Moody's. These agencies, have, through time, been institutionalized and legitimized in the financial markets, as the source of reliable information about the true quality of the bonds. A new "guardian", apart from the public eye and stringent regulatory environment, is not necessary because the ratings are not questioned and they are generally accepted as reliable. This is the reason why we believe that these agencies are the natural candidates for the provision of the rating services in the digital certificates market. Market participants presently do not enjoy the necessary reputation and legitimation as reliable sources of information.

This paper will not focus on the business model under which the Trusted Third Party will sell their rating services to the CAs. We will focus on the tools and techniques upon which this rating system may be developed. In the next section, we propose semantic analysis as a method to evaluate the operational variances between CAs according to their operational risk.

MEASURING OPERATIONAL VARIANCES

In the preceding section we argued that, in addition to institutional risk, the rating scheme should also incorporate the evaluation of operational risk. We reason that the digital certificate quality is completely dependent on the quality of the procedures, identity checks and technology employed. These are all operational characteristics that need to be assessed for an overall quality rating. Within the current rating techniques, there are no appropriate techniques yet to evaluate these operational differences. Hence, we propose the use of semantic analysis as a as a useful tool to highlight these operational variances and by doing that, measuring operational quality.

Semantic analysis is a technique for specifying the information requirements of an organization or business. By defining the business in terms of what actions and behaviors are afforded by its environment, the technique deals directly with the vexing problem of differences in meaning. It starts from the precept that agents create the world in which they operate. All social and

physical environments afford certain ways of acting or behaving, and these affordances are the primitives of this semantic modeling. The affordances have to be arranged in a manner whereby the dependency of one affordance upon the prior existence and realization of others is detailed. The ontology of these dependencies is charted to create a map of behaviors that illustrates graphically the prior actions that the agents must realize in order to instantiate any particular action. The semantics of any term employed are indicated by the actions that are needed to realize the concept in practice: the ontology charts demonstrate the behaviors that must be realized first. Of course the analysis needs to reveal who are the agents that take responsibility for determining when any behavior has been fully realized. In place of "objective" truth there is responsibility. A logic of behavior replaces the formal semantics of a closed system. In the field of information systems, Backhouse and Dhillon (1996) have demonstrated the value of semantic analysis in mapping responsibility structure in British National Health Service Hospital.

Creating an ontology, or rather a set of ontology charts, for the certification area has a number of advantages. The different CPSs clearly diverge in how they articulate their procedures. If it were just a problem of mapping linguistic elements on to one another, it would be a simple matter of developing a thesaurus of terms and aliases and leaving it at that. Unfortunately we cannot expect that the terminological diversity will all be reconciled to a single set of actions and behaviors, that just happen to have different terms with which to refer to them. In reality the issue is not about modeling language but about modeling the behavior to which the language refers. The method draws the analyst to investigate the substantive behavior identifying the various agents or entities with an interest in the operation of the PKI and then mapping their relationships. The mapping elucidates norms of behavior so that areas of risk can be identified where in a particular situation there may be a departure from the norm.

Ontology charts represent the behaviours, or affordances, that agents are afforded by the context presented in the analysis. Agents themselves are special types of affordances, i.e. those with power to act, that are found in any context. Charts are normally read from left to right: agents are able to realise affordances shown as nodes to their right. Each realization then opens up further behaviors or affordances – again shown as nodes to the right. However, reading from right to left, the emphasis is on necessity, in that behaviors depicted on the right may only exist whilst their ontological antecedents, to their left, continue to exist: if the subscriber ceases to exist then the certification status ceases also. Reading from left to right the accent is on possibility – possible behaviors that the context affords the agents as more behaviors in turn are realized. Some affordances are joint, having two affordances as required ontological dependents and these might typically be relationships e.g. the CA certifies the legal person and, in general, role-names apply to the two parties while they are in the relationship. In this case the legal person certified is referred to as "Certificate Holder" or "subscriber" and these are role names that apply but only while the relationship exists. Norms result when the behaviors realized by one or more agents trigger off other behaviors. An example might be that once the Verifiable Subscriber Information on the certificate application has been indeed verified, the affordance of certification is realized and applies to the applicant. In such an example the relationship between the behaviors is normative, not ontological. The norms derive from the agents concerned and in this case are set out in the relevant Certificate Policy or Practice Statement.

To demonstrate the application of semantic analysis in examining CPS, we take a section "authentication and certification" on class 1 certification as stated in Verisign's CPS[3] and developed the respective ontology charts (see Figure 1). Having analyzing the text, we have considered the notion of a Distinguished Name as an affordance that has two ontological antecedents: Subject (generic name for subscribers) and Domain. The Distinguished Name relies on the existence of the Subject and the Domain to be realized. Norm 3.1.1b, indicated by the arrow, stipulates how the components or parts of the Distinguished Name should be structured. This norm set out below as an overlay on the ontology chart indicates that when issuing class 1 certificates, for example, email addresses are used to provide values as components within the Distinguished Name.

[3] Verisign's CPS is publicly available at http://www.verisign.com

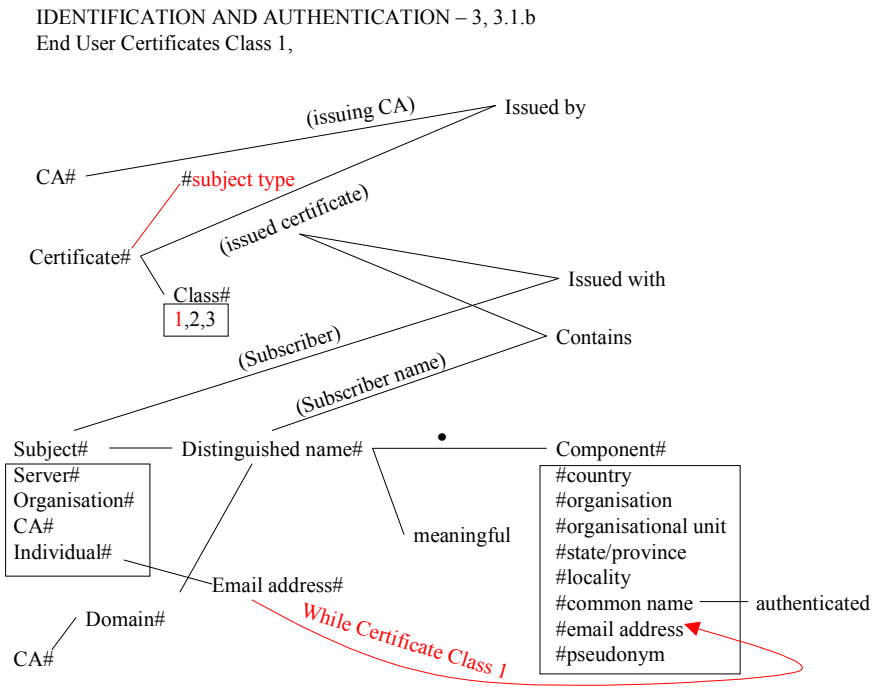

Figure 1: Norm and ontology chart for Class 1 certificate

The visual representation of this simple definitional norm consists in the combination of the underlying ontological structure and the overlaid arrow normative structure. Realizing the behavior in the condition part triggers the realization of the behavior in the consequent part. The group norm is essentially an expression of a pattern of behavior. These structures permit the researcher to view the "shape" of the norm and by extension it should be possible to compare the "shape" of the equivalent norms of other CAs. We might hypothesize that where there are similar "shapes", the commonalities between the policies are higher. Where the shape is not similar, the potential for commonalities is lower.

In future research, the mapping of several CPSs using semantic analysis and ontology charting enables the development of a reference model which is based on the best practices of the various CPSs. A new "ideal" CPS could be modeled based on the best norms found on these policies. This reference model could then be used as a benchmarking tool, against which any new policies could be compared against by using ontology charting. Ontology charting enables comparison between policies and the analysis of completeness, commonalities and variances. It is then possible to create a rate that could be used as a signal for the operational quality of a given CA.

CONCLUSION

In this paper, adopting an economics perspective, we review the argument put forward by Backhouse et al. (2003) that the digital certificates market is suffering from a Lemons problem (Akerlof 1970). In contrast to the suggested countermeasures of branding, licensing and guarantees, here we propose the idea of a rating system as an alternative solution. We discuss the concept of a rating system and the benefits of this system for the stakeholders in the digital certificates market. In the development of the rating system, we consider that there are two dimensions of analysis: institutional and operational. While the institutional dimension has an established methodology, the operational element is very specific for this market and requires the use of a new methodology to capture the operational variances existing among CAs. Although only in outline, we show empirically how semantic analysis can be a useful tool for achieving this aim.

The contributions of this paper are twofold: first, given the ineffectiveness of the formal and regulatory approaches, the proposal of a rating system can be seen as a market solution for ameliorating the effect of the Lemons problem in the digital certificates market; second, we demonstrate how semantic analysis can be applied as tool to facilitate the measurement of CA's operational quality. This is exemplified by using semantic analysis and ontology charting to analyze six certificate practice statements of six CAs well-established in the market.

We recognize that this work is at an early stage of development and further research is required in the development of the overall rating system. We also suggest as further research the development of a reference model against which new CPS could be compared against. We envision that with the development of semantic analysis as a tool and the reference model, it will be possible to build a software system that automatically analyses the operational quality of a given CA.

ACKNOLWEDGEMENTS

Funding support from grant number L142251004, the ESRC/DTI Management of Information LINK programme is gratefully acknowledged.

REFERENCES

1. Akerlof, G. (1970) "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", Quarterly Journal of Economics, 89 pp. 488-500.
2. Ang, J. and K. Patel (1974) "Bond Rating Methods: Comparison and Validation", The journal of Finance, 30 (2), pp. 631-640.
3. Backhouse, J. (2002) "Assessing Certification Authorities: Guarding the Guardians of Secure E-commerce", Journal of Financial Crime, 9 (3) pp. 217 - 226.
4. Backhouse, J. and G. Dhillon (1996) "Structures of Responsibility and Security of Information Systems", European Journal of Information Systems, 5 (1), pp. 2-9.
5. Backhouse, J., C. Hsu, J. Baptista and J. Tseng (2003) "The Key to Trust? Signalling Quality in the Pki Market". in European Conference of Information Systems 2003, Naples,
6. Bhattacharya, S. (1979) "Imperfect Information, Dividend Policy, and the "Bird in the Hand Fallacy"", The Bell Journal of Economics, 10 pp. 259-270.
7. Bhattacharya, S. (1980) "Nondissipative Signaling Structures and Dividend Policy", Quarterly Journal of Economics, 95 pp. 1-24.
8. Campbell, T. and W. Kracaw (1980) "Information Production, Market Signaling and the Theory of Financial Intermediation", The journal of Finance, 35 pp. 863-882.
9. Campbell, T. and W. Kracaw (1982) "Information Production, Market Signaling and the Theory of Financial Intermediation: A Reply", The journal of Finance, 37 (4), pp. 1097-1099.
10. Ciborra, C. (1993) Teams, Markets, and Systems : Business Innovation and Information Technology, Cambridge University Press, Cambridge [England] ; New York.
11. Crouhy, M., D. Galai and R. Mark (2001) "Prototype Risk Rating System", Journal of Banking & Finance, 25 pp. 47-95.
12. Malone, T. W., J. Yates and Benjamin R.I (1987) "Electronic Markets and Electronic Hierarchies", Communications of the ACM, 30 (6), pp. 484-497.
13. Pogue, T. and R. Soldofsky (1969) "What's in a Bond Rating", The Journal of Financial and Quantitative Analysis, 4 (2), pp. 201-228.
14. Ross, S. (1977) "The Determination of Financial Structure: The Incentive Signaling Approach", The Bell journal of Economics, 8 pp. 23-40.
15. Spence, M. (1973) "Job Market Signaling", Quarterly Journal of Economics, 87 (3), pp. 355-374.
16. Spence, M. (1974) "Competitive and Optimal Responses to Signals: Analysis of Efficiency and Distribution", Journal of EconomicTheory, 7 pp. 296-332.
17. Spence, M. (1977) "Consumer Misperceptions, Product Failure and Producer Liability", Review of Economic Studies, 3 pp. 561-572.
18. Steckbeck, M. and P. Boettke (2001) "Turning Lemons into Lemonade: Entrepreneurial Solutions to Adverse Selection Problems in E-Commerce". in Third annual conference of the Association of Historians of the Austrian Tradition in Economic Thought, Pisa - Lucca,24-26 May,
19. Thakor, A. (1982) "An Exploration of Competitive Signaling Equilibria with "Third Party" Information Production: The Case of Debt Insurance", The journal of Finance, 37 (3), pp. 717-739.
20. Wigand, R. (1997) "Electronic Commerce: Definition Theory and Context", The Information Society, 13 pp. 1-16.