# On Some Conjectures in IT Security: The Case for Viable Security Solutions

Jan Zibuschka, Heiko Roßnagel

Fraunhofer IAO
Nobelstraße 12
70569 Stuttgart
jan.zibuschka@iao.fraunhofer.de
heiko.rossnagel@iao.fraunhofer.de

**Abstract:** Due to the increased utilization of computers and the Internet the importance of IT security has also increased. Naturally the field of IT security has grown significantly and has provided many valuable contributions in recent years. Most of the work is concerned with the design of systems offering strong technological security. With regard to behavioural factors, researchers build their work on assumptions about human behaviour that are prevalent in the field of IT security without considering the results and insights of related disciplines. In this contribution we challenge some of these widely held conjectures and offer alternative interpretations based on the results of neighbouring disciplines. Based on this analysis, we suggest new directions for the design of security solutions that support the inclusion of insights from reference disciplines during the design process.

## 1 Introduction

Since the series of cyber-attacks in the first half of 2011 against leading, international corporations like Sony, Citigroup, Lockheed Martin, Google, and Apple [Pau11], it should be obvious that IT security is more important than ever before. With the increased utilization of computers and networks for mission-critical applications in recent years, their reliability and security has also become essential. As a result the field of IT security has grown significantly and has provided many valuable contributions. However, as the recent successful attacks also illustrate, not all of these advances have been utilized in practice and systems remain vulnerable to attacks that are not very sophisticated. For example, a recent study by SANS Institute lists SQL injections and unpatched known vulnerabilities as the predominant threat vectors [DDEK09]. Security technologies that could protect companies or users against these attacks do exist. The problem is that these technologies are often simply not bought, not used or not configured correctly. Therefore, several authors have argued that human factors might be the biggest threat to security in practice [Sas03, JEL03]. At the same time, researchers in the IT security field rely on assumptions about human behavior to guide both the designs of individual systems, and the direction of the discipline as a whole. Examples include conjectures about how humans form trust

on the internet, theories concerning market failure, and opinions about user awareness and education. However, the field of IT security lacks the tools or methods to provide anything but anecdotal evidence to support those conjectures. Neighboring disciplines, especially information systems (IS) and marketing, have amassed a significant amount of knowledge about human behavior with regard to factors such as trust, diffusion of innovative systems, and what constitutes a market failure. Those results at times contradict the conjectures applied in the security domain. However, this body of kernel theory is seldom applied by researchers when designing secure systems [SO07]. In this paper, we will challenge some of the most commonly held conjectures from IT security publications, and present alternative interpretations based on evidence from neighboring disciplines. As this evidence casts doubt on some of these conjectures, we will further argue that those misconceptions are at least partially responsible for the missing market success and utilization of security solutions. In addition, we will outline a framework for the design of secure systems that allows collecting and including relevant evidence concerning behavioral aspects during the planning and specifically feasibility analysis stages, using the information systems and marketing fields as reference disciplines. Especially IS has now collected a significant body of knowledge, especially with regard to the development of innovative yet viable systems [Nam03].

## 2 Common Conjectures in IT Security

In this section we present three common conjectures that are prevalent in the field of IT security. We will challenge these widely held beliefs and present alternative theories that are supported by inputs from kernel theory from the proposed reference disciplines.

### 2.1 "More Security = More Trust"

One of the most widely held beliefs in IT security is that increasing the security of a system, and thus its trustworthiness, will eventually also lead to an increase in trust towards the system [RIS09, GRSS04, Ran00]. On first glance, this reasoning seems to be quite logical. A system that is more secure than others should be more trustworthy and therefore people should trust it more, which in turn should lead to a higher intention to use or buy the system. However, both trust and intention to use are behavioral aspects, involving human beings, and thus are subject to beliefs and behavior of those involved. Therefore, methods of behavioral science are needed in order to be able to measure whether trustworthiness of systems translates into trust of users towards the system or their intention to use it. IT security research does not possess these methods, and cannot provide strong evidence answering the question scientifically. Therefore, researchers in this field should consider the results of related disciples. Trust has been subject of various disciplines, such as sociology, psychology, and economics. As a result there a many different definitions, which often reflect the disciplinary perspectives, but today most researchers see it as a multidimensional and context-dependent construct [LPF06]. When considering the results

of information systems and economics, we find several research contributions that provide evidence that trust indeed positively affects intention to use or buy, especially in the E-Commerce environment [Gef00]. However, when looking into the relationship between technological trustworthiness and trust, it becomes apparent that the relations are much more complicated than a direct implication. Trust is influenced by many different factors. Security technology certainly is one of those factors, but not the only one. McKnight et al conducted a large-scale meta-study on trust formation in electronic commerce, and found that the most important influences on trust in an e-commerce site are institutional trust — the trust in the operator of the site — and individuals' general predisposition to trust [MCK02]. Furthermore, technical measures providing trust through security are dominated by user interface issues: a user may distrust even a secure system because it is very complicated to use, it appeals less to him visually, or it produces errors during usage. Those influences have an impact that is at least as strong as technical security across all user groups [LT01]. Even the color of the web site has been identified as a statistical significant influence on trust [LSR10]. These results cast a serious doubt on the assumption that improved security will automatically lead to an increase in trust. Some IT security researchers have acknowledged, that trust is a social construct that is mainly influenced by the interacting parties, and is hardly influenced by preventive technologies that the user cannot even observe [And01] and have expressed skepticism whether trust can really be managed or influenced by technical means [JKD05]. Consequently, this implies that trust and trustworthiness are separate constructs that are determined by different requirements and influences. Therefore, they should also be addressed separately during system design.

### 2.2 "We need to educate the users"

One possible conclusion that may be drawn from the disparity of theoretical trustworthiness and actual trust is that users need to be educated, enabling them to identify trustworthy systems. This argument is quite compelling. Once users recognize the technological superiority of the more secure product they will naturally choose the better solution. However, several problems arise with regards to this argument. Flinn and Lumsden surveyed users' security knowledge and practices, and specifically the impact of educational measures. They find *"that the benefits of modest education may not be as dramatic as we would hope"* [FL05]. User education is inefficient as the problems associated with security are highly complex. But even if we assume that user education does work, research in related disciplines especially marketing suggests that educating users will not necessarily make them buy more secure products. When confronted with purchasing decisions users need to make choices regarding different product features and the price of the overall product. The security of the product is only one product feature that will be weighed against other features and the costs associated with it. Since more secure solutions often also come with higher costs (including non monetary costs such as reduced performance or high complexity) they might not offer the highest consumer surplus to prospective customers, who are generally perceived as being careless and unmotivated with regard to security [VCU08]. Even when users do exhibit a significant willingness to pay for security, much of this

willingness to pay vanishes if the guaranteed security level is anything less than 100% [MPLK06]. This common underestimation of risks is further reinforced by the tendency of users to assume that negative events are less likely to happen to them than to others and that positive events are more likely to happen to them than others [Wei89]. Therefore, educating users about the trustworthiness of products is not sufficient by itself. It has to be combined with raising the awareness of user about the risks of using unsecure systems. However, given the prominence of the recent security incidents it remains doubtful, that users are still unaware of these risks in general. Furthermore, raising awareness about specific risks can even undermine trust in the systems due to privacy and security salience [JAL11]: the mention of security risks may reduce users' intention to use a service as they are made aware that breaches are possible. In addition, the users' criticized security behavior can be seen as entirely rational [Her09]: contemporary systems are asking too much of users in terms of both cost and complexity and offer too little benefit in return.

### 2.3 "There is a market failure, and we need regulation"

Many information security practitioners share this assessment, and call for the government to intervene and regulate computer security [Lau96, BHRR07]. A common reasoning is that the problems of security solutions in the market indicate a market failure, caused by incomplete information — a lemon market problem [Ake70], an asymmetric information distribution that results in a vicious circle where price is the dominant factor for success, and high quality systems suffer. Of course, we cannot disprove market failure for all security systems in their specific markets in general here; this has to be discussed for each market individually. However, we can say that in some cases where regulation has been made based on observations of market failure have not gone as had been hoped; in analyses following the implementation of the regulation, economic factors such as high costs, network externalities, unfair incentive distributions and lacking applications have been identified as problems e.g. in the case of the German electronic signatures [Roß06]. Speaking of a market failure of security systems in a sense that regulation was needed might be understood as implying that the situation in the market was not Pareto optimal, meaning that the situation of the users might be improved by forcing them to use highly secure systems. Vidyaraman et al. [VCU08] proposed to persuade users to improve their security practices by designing systems in a way that would artificially make insecure practices less desirable. They warned that there would be a backlash from the users, making the approach of imposing security on the user impractical where practices cannot be enforced by an overarching organization, as users would not adopt a solution threatening disciplinary measures to enforce secure practices voluntarily. As we stated in the last section, users valuate systems based on a number of factors, including but not limited to security. If they need to be forced, this would not be an improvement in the sense of Pareto optimality. We feel, in such cases we need an alternative to calls for regulation that would persuade users to use security systems they would not employ by choice. Classical information security aims at developing systems with high complexity (which is a problem with regards to diffusion [Rog03]) and offering the highest possible level of security (which users can-

not observe [And01]). Under those circumstances, the explanation of market failure may apply in some cases, i.e. where a lemon market problem is the main hindrance, but all in all is not necessary to explain why security systems often have no success in the market. Our idea, as an alternative to this, is to find methods for a new design process that would take market compliance factors into account early in the system design.

## 3 Engineering Viable Security Systems

We propose an alternative approach, a stakeholder requirements driven analysis in the very early stages of security system design. As Greenwald et al. observe [GORR04], user acceptance is underrepresented in security systems design. While we recognize that security systems should offer the highest feasible level of security, we feel this feasibility is limited by market compliance, as we need to build systems that are not only trustworthy in theory, but also trusted. It is a condition for the design of such systems that all involved stakeholders would still voluntarily use them. Where related approaches like Karyda et al.'s Viable Information Systems [KKK01] are concerned with the question how much security an information system needs to be successful, we consider the design of IT security systems, and ask how to make them more viable from a market compliance perspective. One very relevant approach is the viable security model [ZR11], which illustrates important factors influencing the impact of a given security solution on the overall security of deployed information systems [ZR11], including how market-compliant a security infrastructure needs to be to succeed on the market, and how effective it is in comparison with the currently deployed state of the art. Those two aspects mirror the earlier discussion of the trustworthiness of effective security systems, and the market compliance reached by creating trust in users. An effective security solution that is not market-compliant will not lead to an increase in security in practice, while a solution that is market-compliant but not as least as secure as what is currently deployed might even harm the overall level of security [ZR11]. The question of effectiveness is widely discussed in information security and related fields of computer science. Technical soundness is the core requirement of information security research in computer science, and the requirement that computer scientists can analyze using the methods of computer science. There have also been quite some efforts to increase the usability of security systems in recent years [JEL03]. Human-computer interaction experts have a comprehensive set of methods for designing and evaluating user interfaces [JEL03]. Factors like task-technology-fit have received less attention, but require a very specific combination of implemented system and concrete task, which makes them not directly applicable to system design. Hevner et al. [HMPR04] recently made the case for design science in information systems, where artifacts such as reference architectures or design theories are developed and then evaluated using behavioral methods, as a promising vector for research that contributes both to the scientific knowledge base (the research is rigorous) and to practice (it is also relevant). While this approach brought the information systems domain, which had been focused on behavioral studies, closer to the subjects classically addressed in computer science, we propose a paradigm shift that would bring the IT security domain closer to IS. While performing an iterative design, as described

by Hevner and usually applied in Software Engineering and security system development, we keep an IT security and computer science perspective, implying direct applicability to the technical design of such systems, but also regularly evaluate the market compliance of the designs based on reference disciplines such as IS or marketing that have methods for assessing market compliance. Hevner et al. [HMPR04] also make a strong argument for evidence-based evaluation. Several methods from the field of information systems can be applied to assess market compliance in the early stages of the design process. Methods such as stakeholder analysis [Pou99] and analyses based on diffusion theory [RZ12] have been applied in the IS field. They are tailored towards qualitative results, but can easily be applied by engineers as part of the design process, and are capable of digesting non-monetary impacts of e.g. privacy [Pou99]. Choice-based conjoint analysis from the marketing field [DRC95] offers quantitative results in the form of measuring stakeholders' willingness to pay for several system configurations, but requires expertise for designing a valid survey instrument.

## 4 Related Work

As mentioned earlier, our approach builds directly on the design science approach by Hevner et al. [HMPR04]. An argument that is very similar to ours has also been made by Fenton et al [FPG94] in the software engineering domain. There, they argue, that a lot of new technologies are developed which claim to lower development effort needed and make software more readily adaptable or maintainable, without giving a sound evaluation. Fenton et al. argue that more empirically sound evaluation is needed to address this. There have been several initiatives in information systems research focussing on the design of viable, secure information systems. Those include the Viable IS approach by Karyda et al. [KKK01], as well as the approach proposed by Siponen and Baskerville [SB02]. On the computer science side, Jürjen's UMLSec [Jür02] has provided a similar contribution, building on UML. Recently, Heyman et al [HYS+11] have proposed an iterative approach similar to the one proposed by Hevner, alternating between requirements and architecture, but lacking Hevner's focus on evaluation and contribution to theory. There are also a wider range of security requirements engineering approaches [FGH+09].

## 5 Conclusion

From our point of view, security systems designs should take into account both technological trustworthiness and socio-economic trust aspects. We build on findings from reference disciplines including information systems and marketing, but derive a framework for engineering secure systems targeting specifically the IT security domain. To achieve a viable security solution, designers have to make sure that their solution provides an effective security improvement and is compliant with market demands. We listed several methods that can be applied to assess market compliance already in the early stages of the design

process. Even though our reference disciplines are influenced by economics, our aim is not to maximise profit. Neither do we want to attack basic research in the area of security, which is of course needed to provide the underpinnings of a more secure future IT infrastructure. Our aim is to provide engineers designing security systems with tools enabling them to increase the practical impact of their solutions by designing solutions that are not only trustworthy but also trusted, effective as well as market-compliant. We see this as important contribution, as earlier work regarding system design has focused on trustworthiness/effectiveness, which, as the viable security model illustrates, is only one aspect of a larger problem. This contribution may also be applicable to field beyond IT security, Fenton et al. [FPG94] make a similar argument for software engineering tools, but we feel it is of special interest in the case of IT security due to the difficulties of many products in the market, said to be due to human factors [Sas03], and the underrepresentation in earlier works. We do not feel this contribution, specifically regarding the details of the design process, is final yet. However, we want to once again point to Hevner et al.'s design science [HMPR04], which provides a very solid meta-framework for a scientific design process with evidence-based evaluation concerning human factors.

## References

[Ake70] George A. Akerlof. The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, August 1970. ArticleType: primary_article / Full publication date: Aug., 1970 / Copyright 1970 The MIT Press.

[And01] Ross Anderson. Why Information Security is Hard - An Economic Perspective. In *Computer Security Applications Conference*, pages 358–365, Las Vegas, 2001.

[BHRR07] P. Bramhall, M. Hansen, K. Rannenberg, and T. Roessler. User-Centric Identity Management: New Trends in Standardization and Regulation. *IEEE Security & Privacy*, 5(4):84–87, August 2007.

[DDEK09] R. Dhamankar, M. Dausin, M. Eisenbarth, and J. King. The top cyber security risks. *SANS Institute*, http://www.sans.org/top-cyber-security-risks/, 2009.

[DRC95] Wayne S. Desarbo, Venkatram Ramaswamy, and Steven H. Cohen. Market segmentation with choice-based conjoint analysis. *Marketing Letters*, 6(2):137–147, March 1995.

[FGH+09] Benjamin Fabian, Seda Gürses, Maritta Heisel, Thomas Santen, and Holger Schmidt. A comparison of security requirements engineering methods. *Requirements Engineering*, 15:7–40, November 2009.

[FL05] S. Flinn and J. Lumsden. User perceptions of privacy and security on the web. In *The Third Annual Conference on Privacy, Security and Trust (PST 2005)*, 2005.

[FPG94] N. Fenton, S.L. Pfleeger, and R.L. Glass. Science and substance: a challenge to software engineers. *Software, IEEE*, 11(4):86–95, 1994.

[Gef00] D. Gefen. E-commerce: the role of familiarity and trust. *Omega*, 28(6):725737, 2000.

[GORR04] Steven J. Greenwald, Kenneth G. Olthoff, Victor Raskin, and Willibald Ruch. The user non-acceptance paradigm: INFOSEC's dirty little secret. In *Proceedings of the 2004 workshop on New security paradigms*, pages 35–43, Nova Scotia, Canada, 2004. ACM.

[GRSS04] Dirk Günnewig, Kai Rannenberg, Ahmad-Reza Sadeghi, and Christian Stüble. Trusted Computing Platforms: Zur technischen und industriepolitischen Situation und Vorgehensweise. In *Vertrauenswürdige Systemumgebungen*, pages 154–162. Verlag Recht und Wirtschaft, 2004.

[Her09] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, Oxford, United Kingdom, 2009. ACM.

[HMPR04] A.R. Hevner, S.T. March, J. Park, and S. Ram. Design Science in Information Systems Research. *MIS Quarterly*, 28(1):75–105, 2004.

[HYS+11] Thomas Heyman, Koen Yskout, Riccardo Scandariato, Holger Schmidt, and Yijun Yu. The Security Twin Peaks. In Úlfar Erlingsson, Roel Wieringa, and Nicola Zannone, editors, *Engineering Secure Software and Systems*, volume 6542, pages 167–180. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[JAL11] Leslie K. John, Alessandro Acquisti, and George Loewenstein. Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research*, 37(5):858–873, February 2011.

[JEL03] J. Johnston, J. H. P. Eloff, and L. Labuschagne. Security and human computer interfaces. *Computers & Security*, 22(8):675–684, December 2003.

[JKD05] Audun Jsang, Claudia Keser, and Theo Dimitrakos. Can We Manage Trust? In Peter Herrmann, Valérie Issarny, and Simon Shiu, editors, *Trust Management*, volume 3477, pages 93–107. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[Jür02] Jan Jürjens. UMLsec: Extending UML for Secure Systems Development. In Jean-Marc Jézéquel, Heinrich Hussmann, and Stephen Cook, editors, *UML 2002 The Unified Modeling Language*, volume 2460 of *Lecture Notes in Computer Science*, pages 1–9. Springer Berlin / Heidelberg, 2002. 10.1007/3-540-45800-X_32.

[KKK01] Maria Karyda, Spyros Kokolakis, and Evangelos Kiountouzis. Redefining information systems security: viable information systems. *Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge*, page 453468, 2001. ACM ID: 510799.

[Lau96] Kenneth C. Laudon. Markets and privacy. *Communications of the ACM*, 39:92–104, September 1996.

[LPF06] H Lacohee, A Phippen, and S Furnell. Risk and restitution: Assessing how users establish online trust. *Computers & Security*, 25(7):486–493, October 2006.

[LSR10] S. Lee and V. Srinivasan Rao. Color and store choice in Electronic Commerce: The explanatory role of trust. *Journal of Electronic Commerce Research*, 11(2):110–126, 2010.

[LT01] M.K.O. Lee and E. Turban. A trust model for consumer internet shopping. *International Journal of electronic commerce*, 6(1):7591, 2001.

[MCK02] D. Harrison McKnight, Vivek Choudhury, and Charles Kacmar. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *INFORMATION SYSTEMS RESEARCH*, 13(3):334–359, September 2002.

[MPLK06] Milton L Mueller, Yuri Park, Jongsu Lee, and Tai-Yoo Kim. Digital identity: How users value the attributes of online identifiers. *Information Economics and Policy*, 18(4):405–422, November 2006.

[Nam03] Satish Nambisan. Information Systems as a Reference Discipline for New Product Development. *MIS Quarterly*, 27(1):1–18, March 2003.

[Pau11] Ian Paul. IMF Hacked; No End in Sight to Security Horror Shows, PCWorld. http://bit.ly/jTpgAp, June 2011.

[Pou99] A. Pouloudi. Aspects of the stakeholder concept and their implications for information systems development. In *System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on*, page 7030, 1999.

[Ran00] Kai Rannenberg. Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet. *WIRTSCHAFTSINFORMATIK*, 42(6):489–498, 2000.

[RIS09] RISEPTIS. Trust in the Information Society: A Report of the Advisory Board RISEPTIS. www.think-trust.eu/downloads/public-documents/riseptis-report/download.html, 2009.

[Roß06] H. Roßnagel. On Diffusion and Confusion Why Electronic Signatures Have Failed. In *Trust and Privacy in Digital Business*, pages 71–80. Springer, 2006.

[Rog03] Everett M. Rogers. *Diffusion of Innovations, 5th Edition*. Free Press, original edition, August 2003.

[RZ12] Heiko Roßnagel and Jan Zibuschka. Assessing Market Compliance of IT Security Solutions A Structured Approach Using Diffusion of Innovations Theory. In *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions*. IGI Global, 2012.

[Sas03] Martina Angela Sasse. Computer security: Anatomy of a usability disaster, and a plan for recovery. In *Proceedings of CHI 2003 Workshop on HCI and Security Systems*, 2003.

[SB02] Mikko Siponen and Richard Baskerville. A New Paradigm for Adding Security into is Development Methods. In Jan H. P. Eloff, Les Labuschagne, Rossouw Solms, and Gurpreet Dhillon, editors, *Advances in Information Security Management & Small Systems Security*, volume 72, pages 99–111. Kluwer Academic Publishers, Boston, 2002.

[SO07] Mikko T. Siponen and Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *SIGMIS Database*, 38(1):6080, February 2007.

[VCU08] S. Vidyaraman, M. Chandrasekaran, and S. Upadhyaya. Position: the user is the enemy. In *Proceedings of the 2007 Workshop on New Security Paradigms*, pages 75–80, New Hampshire, 2008. ACM.

[Wei89] ND Weinstein. Optimistic biases about personal risks. *Science*, 246(4935):1232 –1233, December 1989.

[ZR11] Jan Zibuschka and Heiko Roßnagel. A Structured Approach to the Design of Viable Security Solutions. In N. Pohlmann, H. Reimer, and W. Schneider, editors, *Securing Electronic Business Processes*, pages 246–255. Vieweg, 2011.