

On the Socio-Economic Issues of Web and Application Certification

Pern Hui Chia

Centre for Quantifiable Quality of Service in Communication Systems (Q2S)
Norwegian University of Science and Technology (NTNU)
chia@q2s.ntnu.no

Identifying bad websites or applications is a daunting task for most ordinary users. While most users can recognize the established companies and trust them for reliable transaction or proper handling of sensitive data, one is usually more reserved when dealing with the less popular vendors such as the bulk of websites in the long-tail. The increasing number of third party applications on mobile platforms also presents a new dilemma for users. While many applications are interesting, there are risks such as misuse of personal information, when installing them. As of November 2010, there are more than 300K and 100K third party applications in the App Store and Android Market respectively, making it economically impractical for the application stores to conduct a thorough vetting process [1]. Indeed, Apple determines which applications can be marketed in the App Store through a much veiled (and presumably manual) process, while applications are distributed in the Android Market without a formal review from Google. Both Google and Apple have implemented a ‘kill-switch’ process on their respective operating system as a reactive measure to shut down applications that might have been inadvertently distributed through the application stores. In comparison, an *independent software testing* is needed for Symbian applications that require access to sensitive phone capabilities; however, the testing focuses on technical compliance and does not guarantee security.

Security is a trade-off [2]; a higher level of security often comes with a higher cost in terms of money and/or usability. While users are often blamed to be careless or naïve, it is not difficult to reason that they may be in fact being rational to act using on some simple rules, ignoring complex advices and improbable threats [3]. Heuristic reasoning by ordinary users is often guided by various assurance signals as summarized in Table I. Brand name, warranty, privacy policy and good visual design are examples of first party assurance signals suppliable by the website or application developers. First party signals, while valuable, are however less credible than signals provided by a trusted third party. Yet, third party assurance signals, such as online trust seals, certification or permission to distribute an application in the application store (which we regard as a form of *implicit certification*), is not without its own limitations. A survey of theoretical and empirical studies on quality disclosure and certification in the fields of education, health care and

finance can be found in [4]. There are relatively less research effort on the issues of certification for web and application security. We discuss in this article several directions that may be worth further investigation.

I. MORE INSIGHTS WITH THEORETICAL ANALYSIS?

Differentiating bad websites or applications from the good ones is challenging due to *information asymmetry* between the users and providers. In economics, two well-known problems due to information asymmetry are adverse selection and moral hazard. *Adverse selection* describes a situation in which private information is unknown ex-ante resulting in bad products (websites, applications) being more likely to be selected. *Moral hazard*, on the other hand, depicts the problem whereby one is unable to continuously monitor the ex-post actions such as to ensure the continuous good behavior of websites or applications after certification.

Early economic publications suggest to rely on certification intermediaries to approach the problems of information asymmetry. Biglaiser and Friedman showed that middlemen could attenuate the moral hazard problem by policing product quality assuming that they are quick to identify defects and switch to selling other products without extra cost [5]. Albano and Lizzeri showed that if quality is endogenous, the existence of a certification intermediary will improve product quality [6]. If quality is exogenous, an intermediary will also improve welfare by not certifying unsafe products [6]. However, it has also been shown that a monopolistic certifier will be keen to disclose only minimal information to induce trade [7]. Indeed, many certification schemes today specify only whether a product (website, application) has met a minimal set of requirements.

Further analysis on the incentives of a certifier to provide honest report on web or application security, in the presence of competition from other certifiers, can yield useful insights. Indeed, vendors can now (choose the easiest route to) obtain certification from different certifiers, such as TRUSTe.com, BBBOnline.org, Trust-Guard.com, buySAFE.com, WebTrust.org, TrustedShops.com and so on.

II. DO USERS VALUE CERTIFICATION?

It is well known that many anti-phishing techniques such as security toolbars, HTTPS indicators and site authentication images fail to be effective as they are often ignored

Table I
VARIOUS WEB AND APPLICATION ASSURANCE STRATEGIES

Type	Strategy
First party	Brand name
	Warranty
	Voluntary disclosure (e.g., privacy policy)
	Design and visual appearance
Third party	Trust seal or certification
	Permission-to-distribute in application store
Crowd	Community-based reputation or recommendation
Regulation	Mandatory policy (e.g., EU's Data Protection Directive)

by the users. Through a survey, Chia et al. [8] found that majority subjects (78%) seldom check for digital signatures or certificates when installing an application. There is also little awareness for even the more prominent certifiers such as TRUSTe and BBBOnline. Several studies have evaluated the effectiveness of various trust seals, but produced mixed conclusions on their values for website owners and users. A recent field test conducted by Ozpolat et al. [9], however, found that the presence of a trust seal does help to increase the completion rate of purchase. Having too many trust seals on a website, nevertheless, adversely reduces trust.

While the salience of an assurance signal may depend on multiple factors such as UI design, measuring user awareness and valuation of certification schemes in practice is important as it can have profound effects on the profitability and the potential gaming behaviors of certifiers, such as to lower the requirements to induce sales.

III. ARE CERTIFICATION SCHEMES TRUSTWORTHY?

Indeed, when the certification criteria are lenient, costs for certification will be indifferent, causing the separating equilibrium and a reliable signal to diminish. Edelman showed that, in 2006, TRUSTe-certified websites were more likely to be untrustworthy compared to non-certified websites [10]. Continuous efforts to probe the reliability of different online trust seals would be important to safeguard the users. It would be also interesting to study the implications due to the fierce competition between different mobile platform vendors to attract third party developers, often by lowering the bar of developing and publishing an application in the respective application store.

IV. THE ROLE OF MANDATORY REGULATION?

While it appears that regulation may help to mitigate the risk of manipulation by certifiers or to ensure a sufficient security assurance in the different application stores, mandatory regulation may introduce undesired effects such as encouraging gaming behaviors and being socially excessive [4]. Tang et.al. [11] showed that when the expected loss due to online privacy violation is moderate, self-regulated certification schemes is socially optimal compared to mandatory regulation. Indeed, regulatory actions would also be hard to implement as the Internet is global.

V. SOURCING FOR CROWD BASED SCRUTINY?

A plausible strategy is to crowdsource inputs for web and application security. PhishTank and Web Of Trust are two global-community based systems for web security. There have been also innovations to employ personalized community for anti-phishing purposes (e.g., Net Trust). Inputs from personalized community can be more relevant, catering to groups with different perception on web or application appropriateness. Social ties within a personalized community can also increase the motivation of contribution [8]. Potential challenges of a crowd based system are the limited user capability in security evaluation, noise in collected inputs and the problem of public good provisioning. Future work to address these challenges will be very interesting.

REFERENCES

- [1] P. McDaniel and W. Enck, "Not so great expectations: Why application markets haven't failed security," *IEEE Security and Privacy*, vol. 8, pp. 76–78, 2010.
- [2] B. Schneier, "The psychology of security," in *AFRICACRYPT '08: Proceedings of the 1st Int'l Conference on Cryptology in Africa*. Springer-Verlag, 2008, pp. 50–79.
- [3] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *NSPW '09: Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 2009, pp. 133–144.
- [4] D. Dranove and G. Z. Jin, "Quality disclosure and certification: Theory and practice," National Bureau of Economic Research, Inc, NBER Working Papers, Jan. 2010.
- [5] G. Biglaiser and J. Friedman, "Middlemen as guarantors of quality," *International Journal of Industrial Organization*, vol. 12, no. 4, pp. 509–531, 1994.
- [6] G. L. Albano and A. Lizzeri, "Strategic certification and provision of quality," *International Economic Review*, vol. 42, no. 1, pp. 267–83, February 2001.
- [7] A. Lizzeri, "Information revelation and certification intermediaries," *RAND Journal of Economics*, vol. 30, no. 2, pp. 214–231, 1999.
- [8] P. H. Chia, A. Heiner, and N. Asokan, "Use of ratings from personalized communities for trustworthy application installation," in *NordSec '10: Proceedings of 15th Nordic Conference in Secure IT Systems*. Springer (to appear), 2010.
- [9] K. Ozpolat, G. Gao, W. Jank, and S. Viswanathan, "The Value of Online Trust Seals: Evidence from Online Retailing," *SSRN eLibrary*, 2010.
- [10] B. Edelman, "Adverse selection in online "trust" certifications and search results," *Electronic Commerce Research and Applications*, vol. In Press, Corrected Proof, 2010.
- [11] Z. Tang, Y. J. Hu, and M. D. Smith, "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems*, vol. 24, no. 4, pp. 153–173, 2008.