More Security or Less Insecurity

Partha Das Chowdhury and Bruce Christianson

[1] Emotions Infomedia
partha.dc@gmail.com
[2] University of Hertfordshire
b.christianson@herts.ac.uk

Abstract. We depart from the conventional quest for 'Completely Secure Systems' and ask 'How can we be more Secure'. We draw heavily from the evolution of the Theory of Justice and the arguments against the institutional approach to Justice. Central to our argument is the identification of redressable insecurity, or weak links. Our contention is that secure systems engineering is not really about building perfectly secure systems but about redressing manifest insecurities.

1 Introduction

The purpose of authentication is to verify that a user is who he/she is claiming to be. The goal of authorization is to provide access for certain users to certain resources based usually on predefined rules. An audit trail links actions to principals retrospectively. Authentication, authorization and audit trail are three traditional concerns in building a privilege management infrastructure (PMI). Traditionally, authentication is strong (based on long term credentials linked to a stable identity) and authorization is linked to audit via the authentication mechanism (explicitly using the same long term credential and identity).

The traditional approach to PMI has variously been institutionalised in the form of PKI [17] or trust management engines [6] or Role Based Access Controls [14, 19] or ticket based access management services [18]. We observe the same trend of institutionalisation even by the proponents of privacy enhancing technologies [8–10, 7]. The temptation has always been to identify 'completely secure' systems without consideration of the actual societies and groups that would use such systems, i.e. the design process discounts[3] behavioural transgressions.

2 Case for Departure

We present a case for departure from the conventional theory of 'wholly secure' systems in this paper. We draw from the debate on 'Justice' where we see a clear conflict between a 'Wholly Just' approach based on Transcendental Institutionalism, and realization-based approaches which focus on the advancement or retreat of Justice [20].

[3] For example, by assuming them away, or by classifying them simply as attacks.

The thesis of this paper is that the pertinent question for systems engineering is not 'What would make our Security Perfect', but 'How can we be more Secure' in the context of our strong perceptions of manifest insecurities in our daily lives [3, 2, 5]. The identification of redressable insecurity is central to this thesis.

We first argue that institutionalism (in particular, the discounting of behavioural transgressions) often leads to weak links, which render the entire system more vulnerable; then we argue that just as institutions often tend to be indifferent to liberty and life, so institutionalism tends to give rise to systems which do badly at meeting legitimate aspirations of users.

2.1 Building in Weak Links

It has been reported widely in the literature that investigations into most frauds in the banking systems lead to an insider who has legitimate access to the system, and who knows his way around it [3, 2, 1]. In [1] the author clearly points out

> "Designers of cryptographic systems have suffered from a lack of information about how their products fail in practice, as opposed to how they might fail in theory. This lack of feedback has led to a false threat model being accepted. Designers focused on what could possibly go wrong, rather than on what was likely to; and many of their products are so complex and tricky to use that they are rarely used properly."

We can observe a clear similarity between this observation in [1] and the conflict between "institutional-focused' [20] approaches to Justice (initiated by the Thomas Hobbe's social contract model and pursued by Jean Jacques Rosseau, Immanuel Kant and John Rawls) which presume a well-ordered society; versus the "realization-based" comparisons which are required to include the actual behaviour of people rather than presuming ideal behavior. It is our contention that systems engineering should take into account the realised actuality rather than assuming compliance by all the stakeholders of the system.

Our case for taking realised actuality into account can be illustrated by the work in [11]. Presumption of ideal behavior would seduce us to think if A trusts B to be honest and competent and B trusts C to be honest and competent then A can behave as if A trusts C to be honest and competent. However it is argued in [11] and [15, 12] that such spontaneously transitive trust relationships can have negative consequences and are not always desirable. And yet institutionalised PKI forces exactly this assumption of transitivity upon the user[4].

The realised actuality in the case of banking systems can be users who are entrusted with protecting the system but do not have the incentives to do so [3], or for legislation like RIPA can be behavioural transgressions by errant officers [4]. We emphasise the fact that in [11, 1, 3, 2, 4] the authors were engaged in redressing manifest weak links (e.g. arguing for elimination of transitive trust relationships) which they, reasonably enough, thought could be overcome.

[4] This type of involuntary trust relationship is called 'Compulsive Trust' in [12].

2.2 Examining Realised Effects

Human life is as much about freedom as about utility [20]. The case for realisation-based understanding can be further strengthened by the observation that institutions tend to be indifferent to the lives of people [4, 5, 1, 3, 2].

Instances of *Matsyanyay*[5] are pretty common in applications such as banking security systems [2, 3] where users are helpless against big corporations [3, 2], and with laws such as RIPA [4].

As argued before [12, 11, 13, 15], institutionalised approaches to security often compel users to enter unwillingly into a trust relationship with large parts of the system infrastructure. In consequence, the user is left without any means to control the risks to which they are exposed. A realisation-based understanding would make it easier to identify redressable insecurities. For example in the practical world of law enforcement we observe century-old "orthodox" institutions adopting a feedback mechanism (exactly as argued in [1]) to obtain a better understanding of the realised actuality. In the recent initiatives by Kolkata Police[6] the focus is more on the realised actuality [21] of various policies and mechanisms. The intention is to identify instances of redressable insecurities and inequalities, and to build upon this realised actuality, rather than imposing a set of 'Principles and Mechanisms' on citizens in a manner which is effectively oblivious to the actual impact of these mechanisms on lives and liberty. Similarly campaigners against ID cards and crypto laws in the UK have been animated by the identification of the impact those systems or laws would have on life and liberty [16, 4].

We advocate an explicitly realisation-based approach to secure systems engineering which builds upon an identification of such redressable insecurities. The institutionalised approach effectively regards security policy as an input-only parameter to the design process, and asserts a single threat model which must be accepted by all stakeholders, thus forcing a rigid distinction between stakeholders and attackers. We advocate rather to look at the effects which a given system realisation will have upon the behaviour of its users, and the incentives which it provides for that behaviour. We can then identify and redress the weak links, i.e. the manifest insecurities which emerge, and allow for the effect of feedback on the security policies themselves.

3 Summary

The motion before this house is that when it comes to security the best is the enemy of the good. We endeavour to learn from the debates in the formulation

[5] The classical distinction in Indian Jurisprudence is between *Niti* and *Nyay*, two Sanskrit words for Justice. *Niti* stands for organizational propriety and behavioral correctness, *Nyay* stands for realised justice [20]. *Matsyanyay* (literally 'Fish Justice') refers to the default case, where small fish have little redress against being eaten by big fish.

[6] formerly Calcutta Police; Calcutta was the capital city of British India before Delhi.

of principles of Justice, and to draw an exploitable analogy to the world of security. The situation where a mentally ill man is subjected to injustice due to the incompetence of institutions is redressable. We advocate building on identification of redressable insecurities to address the question 'How can we be more secure'. Discounting social realizations as narrowly consequentialist (which is the current tendency in secure systems design) would lead us into developing mechanisms and institutions whose very insulation from the practical world makes them vulnerable.

References

1. Ross Anderson. Why cryptosystems fail. ACM Proceedings of the First Conference on Computer and Communications Security, 1993.
2. Ross Anderson. Security Engineering. Wiley, Inc, 2001.
3. Ross Anderson. Why Information Security is Hard — An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications Conference, page 358, 2001.
4. Ross Anderson. RIPA III: A legislative turkey comes home to roost. The tragic consequences of anti-crypto law. The Register, 2009.
5. BBC. Tax Records for Sale. Available at http://news.bbc.co.uk/1/hi/business/2662491.stm, 2003.
6. Matt Blaze, Joan Feigenbaum, and M. Strauss. Compliance Checking in the Policymaker Trust Management System. Proceedings of the 2nd Conference on Financial Cryptography: Lecture Notes in Computer Science Series, 1465:251–265, 1998.
7. Jan Camenisch and Els Van Herreweghen. Design and Implementation of the idemix Anonymous Credential System. Proceedings of the 9th ACM conference on Computer and Communications Security, pages 21–30, 2002.
8. David Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM, 24(2):84–90, 1981.
9. David Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, 28(10):1030–1044, 1985.
10. David Chaum. Achieving Electronic Privacy. Scientific American, pages 96–101, August 1992.
11. Bruce Christianson and William Harbison. Why Isn't Trust Transitive. Proceedings of the 4th International Workshop on Security Protocols: Lecture Notes in Computer Science Series, 1189:171–176, 1996.
12. Partha Das Chowdhury. Anonymity and Trust in the Electronic World. PhD thesis, University of Hertfordshire, 2005.
13. Partha Das Chowdhury, Bruce Christianson, and J.A. Malcolm. Anonymous Context Based Role Activation Mechanism. Proceedings of the 13th International Workshop on Security Protocols: Lecture Notes in Computer Science, 4631:315–328, 2005.
14. David Ferraiolo, Ravi Sandhu, Serban Gavrilla, Richard Kuhn, and Ramaswamy Chandramouli. Proposed NIST Standard For Role Based Access Control. ACM Transactions on Information and Systems Security, 4(3):224–274.
15. William Harbison. Trusting in computer systems. Technical Report 437, University of Cambridge, 1997.

16. Minutes of Evidence Taken Before Home Affairs Committee House of Commons. Inquiry into identity cards. http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm 2004.
17. Loren M. KohnFelder. Towards a practical public key cryptosystem. BS thesis, M.I.T., 1978.
18. B. Clifford Neuman and Theodore T'so. Kerberos: An Authentication Service for Computer Networks. IEEE Communications, 32(9):33–38.
19. Ravi Sandhu. Lattice Based Access Control Models. IEEE Computer, 26(2):9–19, 1993.
20. Amartya Sen. The Idea of Justice. Penguin, 2009.
21. Times News Service. Kolkata police set up blog for popular feedback. http://timesofindia.indiatimes.com/city/kolkata/Kolkata-Police-set-up-blog-for-popular-feedback/articleshow/5034239.cms, 2009.