Rational Protocols

Christian Cachin

IBM Zurich Research Laboratory, CH-8803 Rüschlikon, Switzerland
cca@zurich.ibm.com

1 Introduction

Security research continues to provide a plethora of new protocols and mechanisms; these solutions patch either existing vulnerabilities found in practical systems or solve hypothetical security problems in the sense that the problem is often conceived at the same time when the first solution is proposed. Yet only a very small fraction of this research is relevant to ordinary users in the sense that they are willing to actually *deploy* the technology.

Users choose their security technology according to their incentives: if there is no loss or no threat, be it real or perceived, then they don't care about investing in new protection methods (users may be individuals or corporations, they behave similarly in this respect). Hence, the adoption of information security technology has largely been driven by the real and perceived threats.

One can observe this behavior in many cases [1, 5]. The deployment of data encryption for storage solutions in the recent years is a good example. Transparent encryption for a file system has first been demonstrated almost 20 years ago. The required methods have been around for much longer, it only takes standard block ciphers or stream ciphers and simple public-key methods for key management (that are not even used often). But it was new regulations (for example, the *Sarbanes-Oxley Act* or *California SB 1386*) and some highly visible security breaches starting in 2002 that triggered their widespread deployment. Nowadays every vendor in the storage market offers encryption for its products and many file systems come with integrated encryption.

2 Rational Protocols

Over the last years, economists and security engineers have started to address this problem together. A *Workshop on the Economics of Information Security* (`http://www.econinfosec.org/` is held annually.

Today's networked computing systems are controlled by many different agents, all of which have their own interests and possibly conflicting goals. Existing security methods protect the participants only in a very small number of the possible interactions among these agents.

Cryptography, for example, simplifies the design of secure communication methods by assuming a worst-case "malicious" adversary whose goal is to break the protection method and who will invest in this goal up to its own limits. In contrast, the protocol participants are assumed to be "good" and never deviate from the protocol. The cryptographic methods in a security infrastructure are usually its most secure part today, and

J. Camenisch and D. Kesdogan (Eds.): iNetSec 2009, IFIP AICT 309, pp. 93–94, 2009.

any sensible attacker does not even try to subvert the system by breaking the cryptography. But the cryptographic model fails to capture the richness of all security-relevant interactions on the Internet today; the strict separation between "all-good" and "all-bad" participants is not detailed enough to understand a system with many participants that do not share *one* common goal, but have sometimes conflicting incentives.

A more sophisticated point of view is given by the rapidly expanding field of *algorithmic game theory* [4]. Its main purpose is to provide an understanding of computational systems with the tools and language of game theory, whose goal is to analyze systems of several agents with partially conflicting interests. Researchers have made initial steps towards designing protocols in which no party gains by deviating from its specification [3]; in other words, a participant is free to choose its actions and it will do so according to the given incentive structure, but the incentives are designed so as to protect the interests of all participants. This field is known as *algorithmic mechanism design*. One part of it deals with analyzing and designing protocols for distributed systems, called *rational protocols*. Promising initial results in the area contribute protocols to solve tasks for which only cryptographic formulations have been known so far; a survey of initial results was produced in the EU-funded ECRYPT project [2].

We expect to expand this line of research, to gain insight in the structure that motivates the behavior of agents interacting on the Internet, and to develop new forms of interaction that eliminate security problems *by design*.

References

[1] Anderson, R., Moore, T.: The economics of information security. Science 314, 610–613 (2006)

[2] Nielsen, J.B. (ed.): Summary Report on Rational Cryptographic Protocols. Deliverable D.PROVI.7. ECRYPT IST-2002-507932 (January 2007)

[3] Nisan, N., Ronen, A.: Algorithmic mechanism design. Games and Economic Behavior 35, 166–196 (2001)

[4] Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V.V. (eds.): Algorithmic Game Theory. Cambridge University Press, Cambridge (2007)

[5] Ozment, A., Schechter, S.E.: Bootstrapping the adoption of internet security protocols. In: Proc. 5th Economics of Information Security (2006), `http://weis2006.econinfosec.org/docs/46.pdf`