The Future of Cryptography

Bart Preneel

KU Leuven and iMinds
Dept. Electrical Engineering-ESAT/COSIC,
Kasteelpark Arenberg 10 Bus 2452, B-3001 Leuven, Belgium
bart.preneel@esat.kuleuven.be

Abstract. We reflect on the historic role of cryptography. We develop the contrast between its success as an academic discipline and the serious shortcomings of current cryptographic deployments in protecting users against mass surveillance and overreach by corporations. We discuss how the cryptographic research community can contribute towards addressing these challenges.

Since its early days, the goal of cryptography is to protect confidentiality of information, which means that it is used to control who has access to information. A second goal of cryptography is to protect authenticity of data and entities: this allows to protect payment information, transaction records but also configuration files and software. Cryptography also plays a central role in the protection of meta data: in many settings it is important to hide the identities and locations of the communicating parties. In modern cryptography much more complex goals can be achieved beyond protection communications and stored data: cryptographic techniques are used to guarantee the correctness of the execution of a program or to obfuscate programs. Multi-party computation allows parties to compute on data while each one can keep its input private and all can check the correctness of the results, even if some of the parties are malicious. Sophisticated techniques are being developed to compute on encrypted data and to search in the data. Even in a domain as challenging as e-voting progress is being made.

Until the late 1980s, cryptographic devices were expensive, which means that the use of cryptography was limited to military, government, and diplomatic applications as well as a few business contexts such as financial transactions. In the early 1990s the cost of cryptography dropped quickly as the increased power of CPUs made it feasible to implement crypto in software. This resulted in the crypto wars, in which government key escrow schemes were proposed and defeated. One decade later commodity cryptographic hardware started to appear, resulting in a cryptography everywhere. The fast dropping cost of cryptography combined with a rich cryptographic literature leads to the conclusion that today cryptography is widespread.

A quick count shows that there are about 30 billion devices with cryptography. The largest volumes are for mobile communications, the web ecosystem, access cards, bank cards, DRM for media protection, hard disk encryption, and

applications such as WhatsApp and Skype. It is remarkable that very few of those mass applications offer end-to-end confidentiality protection; moreover, those that do typically have some key management or governance issue: the specifications or the source code are not public, or the ecosystem is brittle as it relies on trust in hundreds of CAs.

The threat models considered in cryptographic papers can be very strong: we assume powerful opponents who can intercept all communications, corrupt some parties, and perform expensive computations. Since the mid 1990s we take into account opponents who use physics to eavesdrop on signals (side channel attacks) or inject faults in computations. However, the Snowden revelations have shown that our threat models are not sufficiently strong to model intelligence agencies: they undermine the standardization process by injecting stealthily schemes with backdoors, they increase complexity of standards, break supply-chain integrity, undermine end systems using malware, obtain keys using security letters or via malware, and exploit implementation weaknesses, to name just a few.

By combining massive interception with sophisticated search techniques, intelligence agencies have developed mass surveillance systems that are a threat to our values and democracy. In response academic cryptographers have started to publish articles that consider some of these more advanced threat models. Industry has expanded its deployment of cryptography and increased the strength of deployments, e.g., by switching to solutions that offer forward secrecy. However, their efforts are sometimes limited because of the business models that monetize user data and business plans to exploit Big Data at an ever larger scale.

In terms of protection of users, progress is still very slow. The cryptographic literature has plenty of schemes to increase robustness of cryptographic implementations, but few are implemented. The reasons are cost, the lack of open source implementations, and the misalignment with business objectives that are driven by the Big Data gold rush. Moreover, in response to the modest advances made by industry, law enforcement is reviving the early 1990s crypto wars.

Overall, this complex context brings new opportunities for cryptographers: we have the responsibility to help restoring the balance of power between citizens on the one hand, and governments and corporations on the other hand. We can invent new architectures that give users more control and visibility and that avoid single points of failure. We can propose new protocols that are more robust against local compromises by malware, backdoors or security letters. And we can contribute towards developing or analyzing open implementations of these protocols to facilitate their deployment.