# The Future of Information Security Research: Cryptology and Beyond

Bart Preneel(✉)

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

**Abstract.** This paper reflects on the state of the art in cryptology and information security. It considers the main achievements and shortcomings of research and identifies the major challenges for the future. It explores which research approaches have a high potential to evolve from academic ideas to practical solutions. The paper concludes by discussing how the deployment of more secure and reliable IT systems requires a complete re-engineering including new architectures; it also sketches the broader societal context of such a redesign.

As scientific discipline, cryptology was born during World War II with the seminal work of Shannon. In the 1970s, the academic research in the area took off, with the invention of public-key cryptology by Diffie and Hellman. During the last four decades, cryptology has developed into a mature scientific discipline with sub-disciplines focusing on foundations, cryptographic algorithms and protocols, and secure and efficient implementations. The dramatic reduction in cost of hardware and communication and the development of the Internet have resulted in the processing and storage of huge amounts of personal data; this has motivated the mass deployment of cryptology during the past two decades.

In spite of these successes there are major challenges ahead. While cryptographic theory has developed solid foundations, most of this theory deals with reduction proofs, that show that a cryptographic primitive is secure if a certain problem is hard. It has been noted that some of these proofs have shortcomings in the sense that the model used is not realistic, or that the reduction is not tight. However, it seems that the main issue is that as a community, we don't know which problems are hard; even for problems we believe to be hard it is very difficult to make reliable estimates for the difficulty of concrete instances.

Symmetric cryptographic algorithms seem to be rather mature: the block cipher AES and the hash function SHA-2 are widely deployed and one can expect that SHA-3 (Keccak) will find its way into products quickly. For stream ciphers, the field is more diverse but the eSTREAM competition has resulted in several promising designs. The short term challenges are how to phase out many older and weaker algorithms (such as A5/1, E0, Keeloq, MD2, and MD5), the design of more efficient and versatile schemes for authenticated encryption, and the further reduction of cost of these algorithms (a.k.a. lightweight cryptography).

W. Jonker and M. Petković (Eds.): SDM 2013, LNCS 8425, pp. 23–27, 2014.
DOI: 10.1007/978-3-319-06811-4_5, 

The long term question is whether we can find novel techniques to cryptanalyze the current schemes or whether we can start building evidence (or even proofs) that these constructions offer long term security.

One particular threat to the currently widely deployed systems is the development of quantum computers. Twenty years ago, these we considered to be exotic objects; today it is clear that substantial progress has been made. It remains an open question whether or not quantum computers will be able to break realistic key lengths for public-key algorithms in the next twenty years. However, if they can, public-key algorithms – and thus our information security infrastructure – will be in deep trouble. Moreover, it should be realized that changing a global infrastructure can take 10–20 years (or even more); and some data such as medical, financial, or government data requires confidentiality for 50 years or more. In view of this, more resources need to be spent on the development of concrete proposals for public-key algorithms that resist quantum computers. There has been some excellent research in the past decade in this area, so this topic is no longer "new" or "hot." On the other hand, interest for this issue in the industry is low, as the time horizon of this research lies beyond 2020.

In addition to the risks created by novel computers, the open cryptographic community learned in the past decades that, even if cryptographic systems are mathematically secure, their implementations can be vulnerable. One potentially weak element are the Application Programming Interfaces (APIs) to software libraries and hardware modules. Attackers can also exploit physical phenomena, such as side channels (timing, power, electromagnetic radiation) or active attacks such as the deliberate injection of faults in the hardware (e.g. by voltage glitches or laser pulses). There has been a large body of research on securing implementations by masking or hiding information and by verifying calculations to detect injected faults; there also have been initial ideas on how to create implementations with a security proof (under the name leakage-resilient implementations). However, the models considered in theory are far from practice and even the best *ad hoc* solutions are too inefficient. This means that cryptographic implementations have to switch to "security by obscurity": while the algorithm used is known, the details on how it is implemented have to remain secret – revealing the (limited) countermeasures against implementation attacks that are present would allow to break the system. There is no doubt that further research is needed to create better models and more secure implementations.

It took about 20 years for the breakthrough research on public-key cryptology of the late 1970s to become widely deployed. This required a major engineering effort. Since then, at cryptology conferences an ever growing number of more complex protocols is being presented. The challenge is to understand how one can build up a large body of schemes and study how their security relates. But few of those schemes make it to implementations – either because there is no need for them or because the application developers do not understand the benefits. The broader research agenda however that is being pursued is highly relevant: while historically cryptography was developed to secure communication channels and later on to protect local storage, cryptography is much

more powerful. With advanced cryptographic tools, one can replace a central trusted party by a distributed system. The use of centralized trusted parties seem to have been essential for modern societies and the advent of information technologies has only exacerbated this trend: in application such as auctions, search, recommendation systems, road pricing, e-commerce, and in many security systems centralized parties play a key role. However, a properly designed cryptographic protocol allows to create a completely different design, that is fully distributed and in which no central party needs to be fully trusted. The system optimally protects the interests of each party and works if the majority of the players is honest. As there is no central party, this kind of design can be much more robust against attacks either by hackers or by governments. While the first designs brought enormous overhead in terms of communication and storage, there has been tremendous progress and some proofs of concepts and even real deployments have materialized. One can compare this approach to peer-to-peer distribution versus centralized distribution, with as difference that much stronger security guarantees are provided and a broader range of applications can be covered. It is clear that implementing such systems will be extremely hard: the technological challenges are daunting and one will always pay a performance penalty compared to fully centralized systems. One can also question whether cryptographers can ever convince society that such an approach is indeed better. Moreover, the large incumbents and several governments have nothing to gain by such an approach that undermines their power.

While cryptology is essential for information security and privacy, it is only a very small part of the very complex security puzzle. There has been a substantial amount of excellent work on information security, but the discipline itself seems to lack maturity. This may be because information security is much broader than cryptology; moreover, it is more closely coupled to the ever changing information infrastructure that is deployed with minimal or no security. In this environment new programming languages, frameworks, and system architectures are deployed continuously. As an example, browsers have evolved from simple viewing programs to sophisticated software that is more complex than an operating system from the 1980s. On the one hand, innovative security ideas are being incorporated, but each new development opens up a plethora of new weaknesses. The situation can be summed up with a quote from A. Shamir: "In information security, we are winning some battles but losing the war."

While security and privacy by design are a common mantra, very few systems have been designed with security or privacy as dominating factors: it is well understood that deployed systems are driven by economic factors, and in most cases it is preferred to have a successful but not so secure system that can be patched later, over a much more secure system that arrives one year too late in the market. Once a system or infrastructure is successful, updating its security is extremely difficult – this has been compared to changing the wheels on a bicycle while one is driving it. The overall solution is to patch the most blatant holes, have centralized detection and monitoring to go after abusive attacks and keep fingers crossed that no disastrous attack will happen. This approach has worked

rather well for the first two decades of the Internet as a mass medium, but we are now witnessing its limitations. In particular, as more and more of our critical infrastructure goes online (very often with very limited or even no protection) and the Internet and cyber world are developing as the theater not only for crime but also for terrorism attacks and war, one can question whether the past approach that seemed adequate for e-commerce and business infrastructure is sufficient to build an information society on.

If the answer is no, the discipline of information security and privacy engineering should be further developed to create solid long term solutions. This is only possible if we start re-thinking the way we architect, develop, and evolve systems: security and privacy considerations should be one of the key drivers of an infrastructure that is too big to fail. It is important to keep in mind that "architecture is politics": the choice of an architecture is not a purely technical decision, but it is determined by and determines power relations in the information society. The best way to avoid huge privacy breaches is by stopping to collect massive amounts of personal data. For reliability and correctness, we can learn from the aviation and space industry, that have developed advanced methods to create reliable and complex systems (in spite of this, it seems that they use insecure communication channels). Of course we would need a more cost effective approach that can deliver similar results.

It is not within the scope of this position paper to give more concrete answers, but some of the elements that are needed are obvious: the only systems we can make secure are simple systems; hence we need a better understanding of how to reduce complexity and how to put together secure systems from well understood and simple building blocks. This approach has been used in the past, but probably deserves more attention. Another element that needs more attention is modularity: so far we have failed to deliver on this, as upgrading a cryptographic algorithm or protocol is much more complex than it should be. Finally, we should question the current approach of extreme centralization, where all the data and control of a system are brought to a single place: we have learned that eventually these systems will be compromised with dramatic consequences for both privacy and security.

The above problems are well understood by the security community, but somehow we have failed to make progress. On the one hand, research tends to focus on the "find a hole and patch it" game, that brings short term success. On the other hand, there are very few drivers to start from scratch and develop systems that are more robust, secure, and reliable. Moreover, this would require a large scale international collaboration effort between industry and academia, which is complex to manage.

It would be very interesting to study how society can be transformed to deal in a more effective way with large scale risks and vulnerabilities that are created by the information infrastructure.[1] This is a complex problem with economical, psychological, sociological, political and legal dimensions. While there is an

[1] The same applies of course to our financial infrastructure and to the problems of energy supply and global warming.

understanding that liability could play a role as the key driver to align the market players, it seems very difficult to conceive how one could assign liability in a complex system in which billions of subsystems interact. Moreover, for privacy the problem is even more challenging, as some of the damage by revealing sensitive personal data can create irreversible harm. Overall this would require a thorough redesign of the complete architecture of our ICT systems to make them more robust and distributed; distributed cryptography could play an important role here. But it seems likely that society will only be prepared to pay the price for this after a major disaster.

**Acknowledgements.** This work was supported in part by the Research Council KU Leuven (GOA TENSE/11/007), by the Flemish Government (FWO WET G.0213.11N and IWT MobCOM), and by the European Commission through the ICT programme under contract FP7-ICT-2013-10-SEP-210076296 PRACTICE.