Cryptography between Wonderland and Underland

Moti Yung

Google Inc. and Department of Computer Science, Columbia University
moti@cs.columbia.edu

Abstract. Cryptography is a very broad field, interdisciplinary in nature, and connected to many other areas (in mathematics, computer science, computer systems and engineering). On the one hand, in theoretical cryptography many new notions have been defined, constructed and improved, especially new protocols and cryptosystems that are very powerful and surprising, including solving challenging and even seemingly paradoxical problems. On the other hand, cryptography is often required in actual computing systems, where the computing and communication infrastructure is very dynamic and evolves in a very fast pace. Thus, actual systems may need solutions that are highly constrained, non trivial, and not covered by merely combining existing cryptographic tools and protocols in a black-box fashion. These solutions are the subject of industrial development of specific cryptographic systems that are much less known than their theoretical counterparts. We discuss the interplay between theory of cryptographic protocols and actual industrial cryptographic systems, the differences in specifying, analyzing, modeling, designing and validating in each sub-area, as well as the similarity and the mutual influence between the two sub-areas.

A Tale of Two Sub-areas

Modern cryptography is famous for far reaching developments in many areas that are reported in theoretical and experimental papers. In particular, the area of designing public key cryptosystems and cryptographic protocol has been very fruitful, where amazing developments have been taking place. Working in this area, formalizing new problems, solving them and proving their security, then improving, refining and re-defining the problem is fascinating. Working this way, in fact, often feels like having an adventure in Wonderland (this is obviously said in an allusion to Lewis Carroll's "Alice's Adventures in Wonderland").

However, this area of cryptography is often criticized as being only theoretical. It is often believed by system designers that cryptographers finish their usefulness once they design ciphers and similar cryptographic functions (e.g., a hash function) and a few building block protocols (SSL/TLS, IPSEC). Systems researchers have said that these building blocks can then be deployed in systems by general system designers and essentially solve all problems. Ignoring the fact that it is typical to hear cross-field criticism among researchers, it is indeed the

H. Gilbert (Ed.): EUROCRYPT 2010, LNCS 6110, pp. 320–321, 2010.

case that for various tasks, standard general cryptographic solutions do work. However, standard components usually serve well typical standard systems (for which system researchers may not be needed as well). For more sophisticated systems (e.g., fast and safe cryptography on specific hardware platforms such as smartcards) cryptographers need to be heavily involved (and they are).

The thesis of this presentation is that cryptographic protocol design of special-purpose industrial solutions is not different, and it needs cryptographic sophistication as well. This area presents challenges that require understanding of the underlying system, the available technologies, the system's goals and specifications, involved costs and financial risks, the relevant business goals, as well as threats and their implications. However, to get secure and safe solutions it requires involvement of cryptographic protocol designers. Note that even though this area is less publicized and is based quite often on an oral tradition (given its industrial nature), it is, nevertheless, highly exciting to develop these types of solutions. These solution need to satisfy a large set of constraints, such as having the right performance parameters, providing right level of usability, being cost effective, having robust engineering, and assuring "the right level" of security given the underlying working environment. Contributing to lasting solutions that employ its underlying cryptography correctly is indeed a fascinating area, and working in this area often feels like having an adventure in Underland (this is said in an allusion to another series of fantasy novels: Suzanne Collins' "The Underland Chronicles").

Working in both areas of cryptographic protocol design (the theoretical and actual) gives one a large spectrum of appreciation of what is the state of the art and what is actually required in systems. When designing "a system that incorporates cryptographic subsystem," there are unique advantages to a team that is aware of the state of the art of the theoretical cryptographic literature. Further, the mode of thinking about problems from their specifications and security requirements, the formalization of threat as an adversary arguments, the careful design, and the need to scrutinize it, which dominates the theoretical work, are, all, applicable to working on actual systems incorporating cryptographic components. Yet, theory alone is not enough; specific system knowledge (as described above) is a must, and working closely with the entire engineering team is also a must for achieving successful contributions. This enables adapting the best solutions necessary to a specific setting, based on the full range of the specialized system goals and constraints.

The presentation will cover case studies of actual systems, designed for different purposes and facing different threats. The influence of "theoretical thinking" will be argued, as well as the added value of "specialized systems thinking" which is beyond theory. The general notions of transferring ideas from theory to systems, as well as turning systems ideas to subjects of new theoretical studies will be presented as well.