Staying up-to-date with cryptology

Vlastimil Klíma

v.klima@volny.cz

Cryptologist
http://cryptography.hyperlink.cz
Prague

Abstract

This paper provides an overview of current cryptographic techniques, targeting management and focussing on applicability of cryptographic tools and on the level of their security. The paper shows real-life examples and latest developments in the area. It also brings recommendations that should help managers to understand the necessary basics, what is really important and how to manage cryptology.

Keywords: cryptology, management

1 Introduction

This paper should be of assistance to managers of information systems and security, and it should provide them with lessons and recommendations that would be of help in the course of their duties, especially when facing issues of applied cryptography.

Current cryptology is no science about secrecy, which was its role for four thousand years, now it is a science about mathematical methods of information security.

The early role of cryptology was designing and breaking ciphers. Its role these days is to design various methods of information security (cryptography) and also discovery of their weaknesses (cryptanalysis). And so the outcome of cryptographers can be not only a cipher, but also an algorithm for integrity protection, for non-repudiation of origin in case of transmitting digital document by e-mail, authentication protocol or key exchange protocol. Outcome of cryptanalysis can be a discovered encryption key or deciphered plaintext as before, but it is more likely to be a digital document with a faked electronic signature, or another proof of a cryptographic technique being more vulnerable than in the time of its first deployment. Cryptology can be viewed by many as an exceptional area of human interest, and *cryptologists often like their baby to be something exceptional*. Yet from management point of view there is no difference from other methods of information security. And we also overturned arguments that:

- too few people dedicate their attention to cryptology (really *theoretical and formal methods* of antiviruses, spam filters, etc. most likely attract attention of less people that cryptology does),
- cryptology is based on mathematical principles (cryptology relies heavily on heuristics, most likely more than antiviruses; used methods are often mathematical, but mathematics does not guarantee their absolute security, perhaps with one or two exceptions),
- the consequences of incorrect deployment or wrong choice of cryptographic methods will be more critical than consequences related to poor choices in other areas (*it is hard to say whether a wrong setting* of a spam filter that would bounce a mail leading to a new order that would provide business for the entire company for a year, or loss of a notebook with poorly encrypted data).

Here we would make a first conclusion for management:

Cryptology is just one of methods for information security; there is no need to dedicate more attention to cryptology than to other methods, like antiviruses, spam filters or firewalls.

The only difference that we found is the rich history of cryptography, and its impact documented even in many historical sources. Yet this can show other methods of information security in the following four thousand years too. On the other hand we agree that it is true that:

Cryptology is quite useful and often life critical, can provide for needed and important basic services of information security that have an impact on numerous other services.

These are:

- *confidentiality,*
- *authentication,*
- *integrity,*
- *non-repudiation.*

These cryptographic services can be achieved by various methods, algorithms, protocols and tools. The basic ones are:

- *symmetric cipher – block and stream,*
- *message authentication codes (MACs),*
- *hash functions,*
- *keyed message authentication codes (HMAC),*
- *random sequence generators and pseudorandom generators,*
- *asymmetric methods for digital signatures,*
- *asymmetric methods for encryption,*
- *asymmetric methods for key agreement,*
- *cryptographic protocols,*
- *etc.*

Each of these areas is served by many *algorithms* and also often by many respected *international formal standards and de facto standards*, which have different *parameters and properties*, fitting *different needs*. Particular *techniques (ciphers, protocols, modes, parameters)* grow in numbers, instead of getting simpler. There are many new *standards* that specify how to *implement, set, combine and use* these algorithms. These methods *have to be followed*. It has been often shown that „*home baking*" in *application of standards has fatal consequences*. Even though there are thousands of standards, their numbers decrease for particular application scenarios. *Standards are often expressing the experience of many experts in relevant areas, their applicability and security is scrutinized, and so they should be good guides for application of cryptographic methods, if they exist for a particular area*.

There is no shortage of cryptographic techniques, but *shortage of crypto engineers* who are able to *combine and implement* them correctly.

Every standard has to face the current state of cryptology, as cryptology is a vibrant area of science and attracts new and new attacks and with them also new countermeasures, which have to be continuously and promptly incorporated in the standards, same as for other areas of information security.

Examples:

- The most frequently used standard for application of the most frequently used asymmetric cryptosystem, PKCS#1.

  (The first attack has been shown by Bleichenbacher in 1998 [2], this attack has been extended in 2003, see [3]. In both cases there have been all critical applications patched, e.g. in the SSL protocol, quite soon after the publication of these attacks).

- IP encryptors.

  (They encrypt the IP protocol and have been constructed by valid, verified and mature IPSec standards. These devices are put in front of local networks or individual computers in the network, and they make sure that all traffic in between these is encrypted. And so there devices can be connected through any public network, e.g. via Internet. These expenses „hardware boxes" are typically set once, and then work and protect data for years, without much care. Yet application of recent cryptanalytical methods (see later for so-called side channel attacks) has shown that the communication can be easily decrypted. And then these devices have to been reconfigured or else they become uses pieces of metal scrap [1, parts 51 and 52].)

2 Latest developments

The topic of "recent developments in cryptology" was chosen for IS2 by a respected crypto expert Arjen Lenstra in 2001. And quite a few things have happened since. Let us review some of them:

- A new encryption standard AES was selected in an open world-wide competition and the US approved it for protection of information classified at the level TOP SECRET.
- Weaknesses have been discovered in the construction of almost all modern hash functions, including the widely used SHA-1 hash function, use of which (as a standardized algorithm) will end in two years and it should be replaced by another function at latest by then.
- A new hash function competition for SHA-3 is open world-wide, as in the case of AES.
- Collisions for the hash function MD5 were found, and their generation is a matter of seconds on a standard notebook.
- A possibility of breaking SSL protocol was demonstrated.
- A way to access the PGP private signing key was also demonstrated.
- A new revolutionary method of cryptanalysis, side channel analysis, was discovered. Its application leads to novel results and it is by all means the most effective cryptanalytical method.
- Cryptology and applied cryptology courses have appeared at many universities in the Czech Republic, and the Charles University opened even a new program in this area.

3 Interpretation and assessment of cryptologic news

Assessment of new discoveries in the areas of viruses, operating system or application patches is nothing new for a security manager, and related day-to-day duties are automated and left up to dedicated personnel. Yet assessment of news from the area of cryptology is left up to the security managers, and with the common absence of “company cryptologist" it is often left to the imagination of IT experts. Here we provide the *second management conclusion*:

Cryptology is nothing special, it is just one of information security methods, but it calls for at least the same level of attention like, e.g., antiviruses, spam filters, or firewalls.

Interpretation of cryptologic news is one of the major weaknesses of applied cryptology, and it is so even in countries with mature cryptology, where the crypto engineers are educated and trained by one generation longer than in our country.

4 Status quo

Cryptology provides very little certainty these days. Perhaps we are afraid that it is a volcano, where we do not know when the eruption could start.

The first critical issue in cryptology is that majority of its techniques are based on unproven security, as was discussed by A. Lenstra here in Prague in 2001 [4]. This has got a very important consequence as we have to work with the risk of the techniques getting broken. And if we ignore these risks, such discoveries can have fatal consequences. Imagine what would a new method of large (composite) number factorization mean for internet banking or electronic commerce world-wide? What all data, carefully encrypted in the past, could be open? What would be the consequence of a considerable advance in quantum cryptography that would enable all symmetric cipher decryption?

The second critical issue of current cryptology lies in the discrepancy between the theory and practice.

On one hand, there are encryption methods that cannot be deciphered even by the most powerful cryptanalytical services of the world and any ordinary citizen can use them. On the other hand, there are prominent instances of encryption deployment that are so terribly wrong. And while a widely deployed operating system includes strong encryption tools, hardly anybody uses them because of complicated use, fear of data (access) loss or backdoor existence. And while there are source codes of PGP and other software publicly available, they are so complicated that hardly anybody will vouch with their neck for the security of the entire product.

Modern cryptanalysis can change the encryption device into the executor of attacker's calculations.

This is a consequence of revolutionary development of cryptanalysis. Cryptanalysts never had such options in the history. This also led to the decryption of SSL protected communication in 2003 [3].

Cryptanalysis is in the stage of exponential growth in terms of breadth, depth and importance of new discoveries, in both positive and negative ways. This leads to many practical problems as new results are not comprehended and existing know-how not incorporated into cryptographic products and systems. Cryptology brings new exciting options to both defenders and to attackers. And there is a lack of experts who could follow this development and incorporate appropriate countermeasures. *We face both a wide scale of applications, tools and systems that truly excel, as well as elementary mistakes at all levels*, including those with severe impact. And even worldwide used security products have critical holes that open these products to attackers. Pressure of the market and competitors is at the root of this. Functionality has got much higher priority than security. And products come to the market often in such a way that functionality is not complete and security is added at the very last minute or even "sometimes later". *And cryptology is often put in by application programmers rather than cryptologists or crypto engineers.* But security cannot be added on later, it must be included in architectural considerations right since the start, and often can cause some user discomfort. And here we see another lesson:

The area of applied cryptology often sees more unwanted risk than really necessary.

5 Interpretation of marketing materials

As we have seen, it is necessary to validate statements about cryptographic products

Typical mistakes of marketing materials are insufficient specification of techniques, use of poor quality RNG, application of old standards, application of wrong encryption mode or improper technique, weak authentication, key backup and recovery that is poorly thought through, poor key generation, protection of keys not provided through their entire lifecycle (including reliable deletion), problems with cryptographic service configuration and updates.

Good starting advice for evaluation of marketing materials include:

- verification and cooperation of the supplier to verify that the product implements the given technique in a way it advertises,
- tests of real behaviour of a product in trials,
- evaluation of properties by an independent expert,
- verification that the product really has the certificates it declares (very often the certificate was issues for another version of the product).

6 Basic theses

The basic thesis of this paper is:

Cryptology is just one of methods for information security; pay the same attention to it as to other methods, like antiviruses, spam filters, patches of operating systems and applications of personal, process of physical security.

It is hard to find a security manager that would analyze the logics of algorithms for antiviruses and spam filters, or to set a firewall. So why would managers have to understand cryptologic methods? Yet they are often asked for decisions how long should the certified keys be, or whether the company network encryption should be provided by product X or Y, or what do media news about broken electronic signatures mean for the company. The point is that the IT industry lacks the layer of crypto engineers that should provide the inputs for the managers to make a qualified decision. Decisions without sufficient information now cause problems to managers. And so the next advice is:

Grow your own cryptologists

Grow your own expert that will take care of cryptology and will follow the developments, educate herself or himself, inform you and prepare inputs for you to make decisions. And as most companies and institutions will not want or afford own expert, and will probably ask somebody to take care of these tasks part-time. Ideally, it should not be anybody from the IT department so that you get impartial inputs. The current state when managers

have to attend various seminars to understand the technical problems of cryptology (that often are presented at a very superficial level and so are little effective) is conceptually wrong.

7 Quest for speed

Commercial cryptography is in the trap of quest for maximal speed and minimal price.

The world is not asking for secure functions, but for fast functions that have no known weaknesses.

This is a consequence of market economy that put functionality on the prime position. Electronics gets faster, memory bigger, processors quicker, data sizes bigger. This requires higher transmission speeds. And the consequence is then in quest for fast stream ciphers, fast block ciphers, fast hash functions, fast asymmetric cryptosystems. For example, the new hash function standard SHA-3 will quite likely have to be not only more secure than the old one, but also faster. These requirements are usually in a direct contradiction, but the reality is just like that. This puts enormous pressure on research and leads to *increased* risks of such cryptographic tools getting broken (we emphasize the increase here as some risk exists even now, given the fact that proofs of security are not provided for most cryptographic tools). And since this trend will prevail, security managers have to react by modular development of new systems or by purchasing and using such products in a way that broken or weakened cryptographic algorithms can be replaced by a simple update of software of firmware.

8 How will we encrypt in the year 2100?

Cryptology in general provides little assurance and simple tools for information technologies today. The problem is that mathematical methods of information security cannot be simply and effectively implemented in current information technologies since there technologies are not built for security, do not have the right architecture in place. And when information technologies will be designed in such a way that they can be made secure or security can be provided for them in a meaningful way, cryptology will sure come with simple and effective tools. This is witnessed by professional products for protection of classified data, where security is one of the core elements of their architecture. And if the development will take the path of security being requested, then the cryptology of the future will be part of the basic structure of information technologies, will not bother us and most likely we will know only very little about its existence.

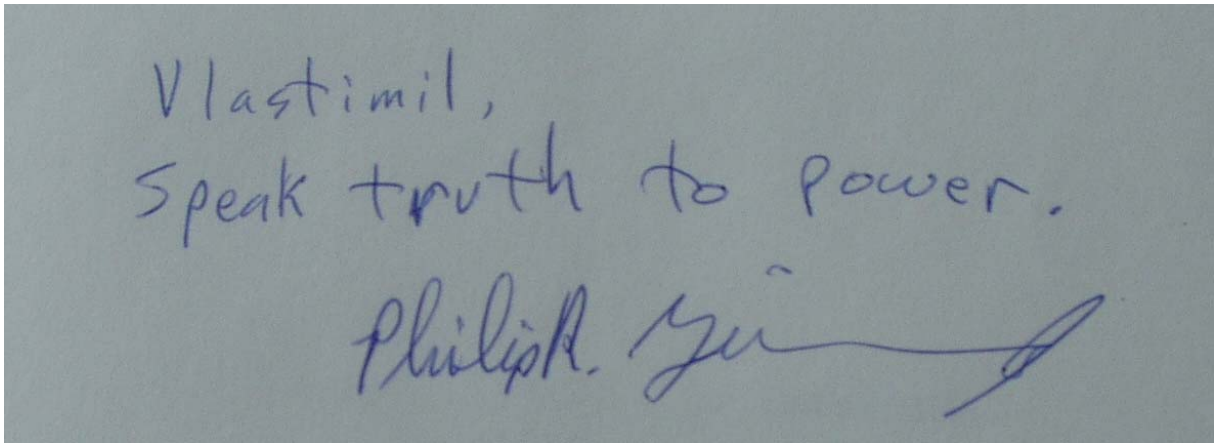

Fig. 1: Advice of PGP father: "speak truth to power"

9 Conclusions

I tried to review the current state of cryptographic developments, analyze this and make some conclusions. A basic management conclusion is that cryptology is nothing special, just one of the methods of information security, And this implies how to treat it: not to ignore it, not to overestimate it, delegate the direct responsibility to an expert and take care of its qualified management.

10 Acknowledgements

I would like to thank Pavel Vondruška and Vashek Matyáš for valuable comments and discussions, and to Vashek Matyáš also for the English translation of my paper.

Literature

[1] Vlastimil Klíma, Tomáš Rosa: Archive (56+...) of articles from the series Cryptology for practice (*Kryptologie pro praxi*), published in the magazine Sdělovací technika, and made available at http://cryptography.hyperlink.cz/, http://crypto.hyperlink.cz/

[2] Daniel Bleichenbacher: Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, CRYPTO '98, pp. 1 - 12, Springer Verlag, 1998,

[3] Vlastimil Klima, Ondrej Pokorny, Tomas Rosa: Attacking RSA-based Sessions in SSL/TLS, CHES 2003, pp. 426 - 440, Springer Verlag, 2003, http://eprint.iacr.org/2003/052.pdf,

[4] Arjen Lenstra: Recent developments in cryptography, Information Security Summit 2001, Prague, May 30-31, 2001.