A hard problem: Disclosing how to break public key cryptosystems ⋆

Audun Jøsang

Abstract. New results in cryptanalysis are constantly being presented in the academic community, and this process poses no problems. Paradoxically, the discovery of a method that would allow breaking for example an RSA key in the same time as it takes to encrypt a message with it, would have serious and disturbing impacts on sectors such as finance and defence, and would in fact be impossible to publish in a normal way. The transition phase from discovery to a complete technological adaptation to the new situation could be painful. This paper examines various ways of making such a discovery public, and their corresponding consequences.

1 Introduction

In it's first issue, CryptoBytes[1] bluntly prints an article by Gilles Brassard[1] that discusses the possible demise of the RSA public key algorithm. Brassard's conclusion is that neither progress in hardware performance nor development in number theory will ever increase the factoring speed enough to make RSA obsolete, and that only quantum computing has such a potential.

This may sound reassuring because quantum computing still is more a theoretical concept than a practical method for doing real computation. It does however leave open a realistic possibility of a total collapse of cryptosystems that are based on the difficulty of factoring large numbers.

The security of public key cryptosystems depends on trapdoor one-way-functions. A one-way-function is easy to compute but exceedingly difficult to invert. A trapdoor one-way-function allows someone in possession of secret information to compute the inverse easily. We will use the term *trapdoor penetration method* to denote a method for computing the inverse easily without the secret information, thus an efficient method for breaking public key systems, that for example would allow cracking an RSA key in about the same time as it takes to compute one encryption with it.

From the first proposals for using public key cryptography [2, 3] and the announcements of the first practical systems [6, 5, 4] it took at least 10 years before the scientific community considered it "safe" to implement public key cryptography in real applications for commercial or government use.

Public key cryptography is used in thousands of applications from private electronic communication to advanced military weapon systems, and now, only 20 years after its

⋆ Appears in S.J.Knapskog and T.Brekne, editors, Proceedings of the Third Nordic Workshop on Secure IT Systems(NORDSEC'98), NTNU, Trondheim, Norway, 1998.

[1] CryptoBytes is a scientific magazine published by RSA Laboratories

invention, seems indispensable. In some ways, however, its technological base is disturbingly narrow. As expressed by Whitfield Diffie ([7], p.166): "...virtually all surviving public key cryptosystems and most of the more numerous signature systems employ exponentiation over products of primes. They are thus vulnerable to breakthrough in factoring or discrete logarithms. [...] From the standpoint of conventional cryptography, with its diversity of systems, the narrowness bespeaks a worrisome fragility."

Assessing the likelihood of ever finding a trapdoor penetration method is not easy. The general rule for determining whether a cipher is secure is to present it at scientific conferences and invite experts attack it. The assumed strength of the cipher then increases as a function of the number of years passed without any successful attack being reported.

By this standard, the remaining unbroken public key systems can be described as strong after 20 years of being exposed to attacks. However, the risk involved does not only depend on the the perceived vulnerability of the cipher, but also on the asset values at stake. When considering that an increasing number of sectors of modern society depends on public key systems, the risk can in fact be increasing dramatically, despite public key systems being considered stronger.

We will not discuss the technical issues related to cryptanalysis of public key systems, but rather the consequences the discovery of a trapdoor penetration method would have on the IT security industry and on the society as a whole. Assume that a trapdoor penetration method has been discovered by an individual or small group of individuals. We believe that once this has happened, it will sooner or later be made public. This person or group then has a great responsibility to limit the potential damaging consequences, but as we indicate in the title, it can be a hard problem. The difficulty of handling such discoveries may never be a real problem to anyone, but it should at least be discussed, as long as it can not be excluded that public key systems will never suffer total breakdown.

In the following sections we first discuss some less desirable ways of handling the problem, and subsequently what we believe are good ways of dealing with the issue. In general there is no single best way of disclosing a trapdoor penetration method to the public, and each scenario has drawbacks and advantages.

Public key systems have the particular property of being useful only as long as no trapdoor penetration method is found. The discovery of for example an efficient method for factoring large numbers would certainly have considerable effects in many other areas of science and industry as well, but the scenarios presented below only focus on the direct and secondary consequences for IT security alone.

2 What not to do

Those possessing the knowledge of a trapdoor penetration method will in fact have obtained considerable power by their discovery, at may want to use the knowledge to their own advantage. Depending on the interests of the discoverers, some parties may gain at the cost of others. In this section we describe less desirable ways of using or disclosing the knowledge, as seen from a the point of view of the global community.

2.1 Publish the details without warning

Disclosing the details of a trapdoor penetration method without prior warning to the rest of the scientific community would make thousands of security systems worldwide insecure instantly. This would probably destabilise important sectors of the industrialised world such as finance and defence, and in general produce unpredictable results. This is therefore the worst imaginable scenario.

2.2 Publish it anonymously

In addition to the effects described above, anonymous publishing is equivalent with giving away the discovery without getting any credit for it. However, a very strong psychological incitement for doing research is to gain recognition for results and achievements.

Publishing the results anonymously so that the discoverers at a later stage are able to prove that they did it would then be desirable. This in itself is an interesting cryptographic problem which for example could be solved with digital signatures. Paradoxically, by publishing the trapdoor penetration method, it may be impossible to use cryptographic methods for this purpose.

2.3 Exploit the method privately

The discoverers may decide to use it for their own benefit and keep the method secret. It is however difficult to imagine how a trapdoor penetration method can be exploited privately in a legal way. The purpose of cryptography is to produce security services such as confidentiality, integrity and authentication. The discoverers may be able to break the confidentiality and integrity of data belonging to others, and may be able to masquerade as others, but that will hardly ever be legal.

Illegal exploitation can naturally produce huge profits, and it is then only a question whether the discoverers' power of judgement is sufficiently strong to resist the temptation.

2.4 Exploit the method strategically

Military and government research agencies often keep results confidential because it can give their country a technological advantage over other countries. The knowledge of a trapdoor penetration method would however be difficult to exploit strategically.

It would be too risky for the government in possession of the knowledge to use public key systems themselves. The reluctance of the government to use public key systems is likely to be noticed by others and thereby create a suspicion that the government possesses the knowledge it tries to hide. If such rumours become sufficiently credible, everyone will stop using public key systems.

It is for example assumed by the open scientific community that governments with large research resources are able to factorise much larger numbers than the ones which are factorised by the academic community. How much larger those numbers are can only be subject to speculations.

The above observations lead to game theoretical considerations. A government would normally not want to admit how large numbers it can factorise, in order not to scare other nations to use larger numbers than it can break. On the other hand, if a government does not want others to use public key systems at all, it only needs to make it seem as if it has the technology to break them. Although playing such games can produce strategic advantage, it is also likely to create huge disadvantages for allied countries as well as the domestic industry.

2.5 Sell the method

Private organisations would not be able to exploit the knowledge of a trapdoor penetrating method commercially without becoming criminal. Governments can avoid being labelled criminal because they to a certain degree can decide what is legal and what is not. When the goal is to get military and strategic advantage over other countries, the term criminal no longer applies, because there are no relevant laws regulating such relationships.

Only government or criminal organisations would want to buy the knowledge of the trapdoor penetration method while keeping it secret for others. By selling the knowledge to a criminal organisation, the discoverers themselves become criminal. In addition the discoverers must consider that they may be seen as a threat to the buyer who therefore may want to have them eliminated.

Selling the knowledge to a government organisation will almost per definition be legal, but the discoverers will probably have to accept strict terms of secrecy, and may have their freedom of movement and participation in civil activities restricted.

2.6 Submit to a scientific conference

This procedure which is adequate for publishing ordinary research results would be a very bad choice for making a trapdoor penetration method public. Primarily, it would leave the programming committee in a delicate situation, in fact putting the burden of responsibility to the committee. Secondly, because of political implications, the submission will not be treated as an ordinary submission anyway, and thereby making this option meaningless.

The submission process itself is usually not very secure, and it can not be assumed that the knowledge has been kept confidential. This is something the committee would have to consider when deciding further actions. In any case, by considering all the parties involved in printing the proceedings of a conference, it will not be possible to simply include the paper in the proceedings without leaking the details, and thereby causing very unpredictable results

2.7 Do nothing

If a trapdoor penetration method is found, the discoverers will probably make considerations similar to the above, and can conclude that neither publishing nor exploiting would be worth the trouble, and therefore decide that keeping it as a secret is the best thing to do. This is maybe the simplest option, but also an unbearable one.

Simply knowing that the method exists will make it seem very likely that others will discover it sooner or later, or have already discovered it, so that it can not be expected to remain a private secret forever. Simply knowing that global financial systems and national security may be compromised can be unbearable, especially since it would have been possible to do something about it.

3 What to do

In this section we describe what we believe are correct ways of dealing with the discovery of a trapdoor penetration method, whether the discoverers are private citizens or belong to a government organisation.

3.1 Issue a warning

Because of the destabilising effect a disclosure without prior warning would have on society, the best thing is to issue a warning well in advance of publishing the details of the method. The problem of credibility of the warning is easily solved by responding to trapdoor challenges issued by sceptical parties.

The period immediately after issuing the warning will be critical, as it can be difficult to trust those possessing the knowledge for not misusing or exploiting it. Important considerations will be whether applications that depend on public key systems can be used at all. If not, thousands of IT services will have to be disrupted immediately, resulting in everything from consumer inconvenience to shifts in military balance.

Eventually, industry and society will adapt to the new situation, and it is important to allow enough time for this process to complete before the details of the trapdoor penetration method are disclosed.

3.2 Tell your government

If the discoverers are not already in a government organisation, a natural choice would be to tell the government. The consequences of this will of course depend on the government's intentions, and can therefore be somewhat unpredictable.

As described above, the government may want to use it to their own strategic and military interest, for example by tapping foreign telecommunication traffic, or even own domestic civil traffic. On the other hand, a government can take a responsible attitude by issuing a warning to the international community, and leading the efforts to adapt to the new situation. The discoverers' attitude to their government regarding these issues may then determine whether they want to share the knowledge with the government or not.

The total breakdown of public key systems can be called a global crypto disaster, and should maybe be handled by an international organisation. Both governments as well as private organisations have the responsibility to take the necessary steps to ensure that the knowledge is handled in a responsible way.

3.3 Patenting

Patenting the method will of course not stop people from using it. All public key systems would immediately become obsolete and useless. We therefore do not see how a trapdoor penetration method could be exploited commercially in a legal way in the area IT security. As already mentioned in the introduction, the method may however be very useful in other areas, so a patent can be valuable.

Keeping a patent secret is possible in some countries, such as in the USA where a special patent arrangement has been established to make sure that classified research eventually can be openly recognised. NSA is allowed to apply for a patent and then block its issuance. If at some later stage, the classification is downgraded or removed, for example because the same results have been obtained in the open community, the patent is finally issued.

4 Conclusion

By observing that public key systems have become indispensable in many sectors of modern society, it is worrying to admit that a total breakdown of those cryptosystems can not be excluded. The severity of the disaster will depend on the way in which the cryptanalytic know-how is handled. This again will depend on the discoverers' intentions and power of judgement.

We have described some less desirable scenarios and proposed what we believe are safe and responsible ways of handling the knowledge. Our main thesis is that a warning should be issued well in advance of disclosing any details, so that industry has time to adapt to the new technological reality.

An issue for further consideration is crypto disaster contingency planning. Many companies and governments probably have such plans, but in case of public key systems this becomes a global issue.

References

1. Gilles Brassard. The impending demise of RSA? *CryptoBytes*, 1(1):1–4, Spring 1995.
2. Whitfield Diffie and Martin E. Hellman. Multiuser cryptographic techniques. In *Proceedings of AFIPS National Computer Conference*, pages 109–112, June 1976.
3. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.
4. Robert R. McEliece. A public key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Laboratory, Jan.–Feb. 1978. DSN Progress Report 42–44.
5. Ralph Merkle and Martin E. Hellmann. Hiding information and signatures in trap door knapsacks. *IEEE Transactions on Information Theory*, IT-24:525–530, September 1978.
6. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signature and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
7. G.J. Simmons. *Contemporary Cryptology*. IEEE Press, 1992.