Regulating Cryptography is harder than you think

so the Government experiences

Bert-Jaap Koops

Tilburg University
Eindhoven University of Technology

Encryption is essential for information security, but it can also be used by criminals to circumvent wiretaps and searches. Governments are thinking hard how to address this problem. The options - key deposits, commanding decryption, using other measures to gather information - all have their drawbacks. For the near future, the Dutch government is not likely to adopt a restrictive regulation of cryptography.

Introduction

Encryption is an essential part of information security, and thus it is an increasingly important tool in the information society. It can be used to protect the authenticity, integrity and confidentiality of information. Banks, businesses, governments, and individuals use it widely, for instance, in electronic transactions, business negotiations, private e-mail, smart card protection, cellular telephones, and cryptofax machines. However, not only good guys use it. Criminals and terrorists are discovering the potential of robust cryptography to shield their data: that way, they will remain out of reach of wiretapping and searching police officers.

Because of the potentially evil use of cryptography, governments are looking for ways to regulate it. On the one hand, they want to stimulate its use for information security, while on the other hand, they want to keep strong cryptography away from criminals. These conflicting concerns make regulating crypto harder than governments at first sight would think.

In this article, I will go into the reasons why governments want to regulate encryption, and I will describe the possible alternatives for a crypto regulation, focusing on the situation in the Netherlands. I conclude with a tentative view into the future, indicating potential consequences for businesses.

Why regulate crypto?

Cryptography is not a recent invention. The Greeks and Romans already used secret writing, and through the ages, cryptography has been an important part of diplomatic and intelligence work. In the Second World War, crypto machines encrypted all communications, and states employed thousands of people to crack the enemies' machines and messages. During the Cold War, cryptography remained a classified and obscure field of study, which was restricted mainly to government applications. Through all this time, governments restricted the export of cryptography, to protect foreign enemies from using it.

The advent of modern cryptography in the late seventies changed the field. The invention of public-key cryptography (like RSA) opened the way for large-scale application, and the automation of fast conventional encryption (like DES) made encryption easy to use.

Since then, cryptography has become widespread. Still, the classification of cryptography as a potentially harmful weapon that should be kept from foreign states and terrorists continues on: the export of cryptography is still widely restricted - for instance, through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which classifies cryptography as a "dual-use" good with both military and civil applications. Increasingly, businesses protest against these restrictions; especially US businesses argue that they are being hampered, as they cannot incorporate strong cryptography in hardware or software for the foreign market. Despite a recommendation by the National Research Council [3] to gradually relax export controls, the US government has shown no real intention to substantially relax the current export restrictions. In Europe, export controls are generally less restrictive than in the US, but in most cases, licenses are still required to export strong cryptography.

The invention of public-key cryptography (like RSA) opened the way for large scale application.

However, export controls are not the only issue. Apart from the fear that foreign states or terrorists will use strong encryption to thwart national intelligence agencies, governments increasingly worry about criminals using it to remain out of reach from law-enforcement agencies [2].

To show how cryptography can hamper law enforcement, I will describe how "automated" criminal investigation takes place in the Netherlands. First, during a search, the police can turn on a computer to see what it contains; they can copy the hard disk for later investigation, or they can seize the computer or diskettes. If the computer is access-protected, the police can command someone to undo the protection; this command can not be given to a suspect, as suspects can not be required to incriminate themselves. In 1993, when the Dutch Computer Crime Act was enacted, it was realized that encryption could thwart the search in computers. Therefore, a provision was added that when the police encounters encrypted information during a search, they can require someone who is likely to know the means of decryption, to decrypt it. Again, the command can not be given to suspects.

A second major investigation measure is wiretapping. The police can intercept telecommunications - (mobile) telephone, fax, or computer communications. Wiretapping is considered by many law- enforcement officials as an essential tool in combating, in particular, organized crime. After all, criminal organizations have a large need for communicating, and so, intercepting their communications is an excellent way to gain knowledge of who is involved in which activities.

Obviously, if criminals store incriminating information in their computers in encrypted form, the police stands powerless. All they can do at present is require someone to decrypt - but in almost all situations, the only one to know the key will be the suspect, who cannot be addressed with this command. Likewise, if criminals communicate through encryption, wiretapping will yield gibberish. It is unclear how many criminals use encryption presently - the Dutch police seem to have encountered unbreakable encryption in only a few cases, so far. However, the general expectation is that this will soon change. Cryptophones can be bought at affordable prices - if cost would be an obstacle at all for criminals. Robust cryptography is available through the Internet, often for free. Moreover, the interfaces are becoming increasingly user-friendly. What is more, encryption will be built-in in web browsers, mail programs, and operating systems, and once such programs feature on every computer, encryption will be a seamless part of data storage and communications. Therefore, governments have good reason to worry about their future ability to gain information and evidence through computer searches and wiretaps.

What to do?

Suppose the police encounter encrypted data, what can they do? They can try to break it. In many cases, this will not be feasible - modern cryptography is generally too robust to break through exhaustive key search. In some circumstances, the police may find the key somewhere; after all, criminals are fallible like all humans, and they may be careless with their keys. However, this requires a good deal of luck, and the police can not rely on this. With current investigation measures, the police will often stand defeated by encryption.

What alternatives are available for trying to overcome crypto use by criminals? Prohibiting cryptography is not an option, given its necessity for information security - one remembers the public outcry in the Netherlands when the pre-draft law to regulate encryption through a licensing system leaked out. One could consider protocols to ensure the police can access encryption keys. The US Clipper chip, launched in 1993, is an example of a crypto system with built-in government access to keys [1]. The Clipper chip has not gained acceptance, but other systems for "key recovery" are being proposed instead. One can market crypto systems of which the keys have been deposited beforehand

with Trusted Third Parties (government or licensed private bodies). An alternative is a system such as RecoverKey International by TIS, which ensures the police can access session keys, without master keys having to be deposited. Both systems, however, will meet with resistance by businesses, since they will be reluctant to give others access to their encryption keys. Procedures and protections should be excellently dealt with before enterprises will consider this an option. Even then, the overhead will be significant, and the yield is doubtful. One can not expect criminals to use these systems if they know the police can access their keys. The only gain for law enforcement will be that the vast majority of communications can be regularly intercepted and read, so that they can focus on the small part of messages they cannot easily read. Still, it is a far-reaching measure, and it requires several hurdles yet to be taken before governments can realistically consider it. Especially liability issues and international cooperation need to be addressed, and I estimate that these issues are too complex to overcome.

The Clipper chip has not gained acceptance.

What then? One may consider infringing the principle that suspects are not required to incriminate themselves. In that case, one could command a suspect to decrypt information, and if he refuses, he may be either convicted for not complying with this command, or his refusal may be taken as evidence that he has something to hide, so that he could be convicted more easily for the crime he is being suspected of. The principle of non-self-incrimination, however, is an internationally recognized fundamental right, which can not be set aside easily. Indeed, governments must have compelling reasons to infringe upon it. And even then, would it really help? It would be disproportionate to punish non-compliance with a decryption command with a grave sentence of ten or more years, yet otherwise, if it is only punishable with a few years, criminals will have an easy job choosing a minor sentence. For the time being, many lawyers would consider the option of requiring suspects to decrypt disproportionate.

If the police has no option to access encryption keys, they will simply not be able to decrypt the information. They will have to use other means to gather information. The government has long been considering the possibility of "direct eavesdropping", through directional microphones or perhaps through bugs. With such devices, the police could gain direct knowledge of conversations - before they are being encrypted over the phone. Perhaps data mining and data warehousing can give the police new insights in criminal organizations. Such alternative investigation measures merit study, as they could circumvent criminal crypto use. However, such methods, if they are practicable at all, also infringe upon people's privacy, often in a very grave way, and one must question whether the infringement of the constitutional right to privacy is outweighed by the potential advantages.

What next?

The analysis of possible alternatives shows that governments have a hard job in addressing the crypto problem. The current stance of the Dutch government is to experiment with a Trusted Third Party (TTP) pilot, in which the police should somehow have access to keys. Government officials stress that they prefer to address the issue through self-regulation: voluntary projects with TTPs should do the trick. Of course, it will not solve the entire problem, because criminals will continue to use other forms of cryptography.

Another Dutch policy line is the intention to extend the current decryption command to telecommunications: the police will ask communicating partners to give the key to intercepted encrypted communications (if this is possible). This is likely to be a futile option, because in most communications, session keys are discarded immediately after the conversation. Only an obligation to store session keys could yield some effect, but that would create too much overhead to consider it an option.

Can the Dutch government expect support from international organizations? The OECD has been developing guidelines for a crypto policy, and it was hoped that these would give guidance to states in drafting a national crypto policy - with such guidelines, at least to a certain extent, international harmonization could have been effected. That is a necessary condition for a crypto policy to really work, given the international nature of the information society - and of criminal organizations. However, the OECD has not been able to come to some form of guidance: the guidelines, which are to be accepted by the Council of the OECD in April 1997, only indicate important principles to take into account - mainly, privacy protection and law enforcement access - while stating that these principles are interdependent and should be taken as a whole. The guidelines fail to indicate *how* the balance between these principles should be found, and they leave ample room for national interpretation. The United States, then, can continue with its "key recovery" policy, whereas Scandinavian countries will stress the protection of privacy and stimulate crypto use.

The Dutch government will therefore have to find its own way. If they continue along the present pol-

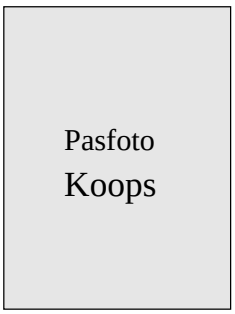
icy lines, businesses will not experience much hindrance. Voluntary TTP projects will not likely find a large support basis, and decryption commands will remain restricted to few criminal investigations. The problem of criminals using cryptography to remain out of the police's scrutiny will not be solved by these initiatives. In a few years time, when the extent of the problem of criminal crypto use in practice will be clearer, the government will likely reassess its policy, and look again at the alternatives. By that time, however, cryptography may be built-in in major programs and have become so widespread, that a regulation involving cryptography in general will likely be disproportionate, leaving only the options of requiring suspects to decrypt and alternative investigation measures. In that respect, businesses can steer the future: the more they will adopt cryptography, the harder it will be for the government to restrict cryptography at large. □

References

[1] Hoffman L.(ed.), *Building in Big Brother*, Springer Verlag, New York, 1995.

[2] Koops B-J., *Crypto Law Survey*, http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm.

[3] National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press, Washington, 1996.



Drs. Bert-Jaap Koops studied mathematics and general and comparative literature. He is working as a Ph.D. student at Tilburg University and Eindhoven University of Technology, researching judicial and private concerns with respect to encryption.

Hot News

SAI

On May 1st, the Stan Ackermans Institute (SAI) has formed a new management consisting of

> Prof.dr. J. (Jack) van Lint as director (0.5 fte) and Dr.ir. M.L.P. (Marloes) van Lierop as adjunct director (0.8 fte)

The appointment of Marloes van Lierop as adjunct director of SAI forces her to leave as OOTI Programme Manager. Beside her newly accepted employment, she will partly continue her activities at OOTI *until* the successive OOTI Programme Manager has mastered all details of the job. The new OOTI Programme Manager is not recruited yet.

In addition, a new model of executive management at the SAI is defined; the former management comprising all chairmen of the ten technological designer programmes has been abolished, and a different management is formed consisting of a member of the board of directors (CvB) of EUT who will act as chairman, two EUT-professors, and five representatives of industry. Currently, only the chairman is known: rector Prof.dr. M. (Martin) Rem.

One of the most important changes concerns the funding of the technological designer programmes. Departments used to be financed by SAI based on the number of students attending the programme. Henceforth, the SAI will more directly manage the finances by judging programmes on quality. The coupling of funding and quality has barely any consequences for OOTI; the department of Mathematics and Computing Science already knew how to manage SAI-funding taking into account quality criteria.

Design award

Peter Foliant is nominated for the UFE design award contest. The prizes are presented at the diesnatalis of EUT on April 25th. Each technological designer programme is allowed to nominate only one candidate.

New OOTI students

On March 1st, two new OOTI students started. They studied Mechanical Engineering before joining OOTI.

Turkey Trip

XOOTIC goes to Istanbul, Turkey from May 9th until May 13th. We hope that the stay will not retract people too long from daily work, otherwise it will be a 'cold turkey trip'. □