Privacy in the Digital Age of Encryption and Anonymity Online

Speech by ENISA Executive Director, Prof. Dr. Udo Helmbrecht

THE HAGUE

19TH- 20TH MAY, 2016

Good morning Ladies and Gentlemen

It is a great pleasure to be able to welcome you to this conference. I am really impressed by the collection of different sector actors represented in this event today and I would like to thank Europol and the European Institute of Public Administrations for giving me the chance to address you.

The underlying point of today's event is that everything is becoming digital, from cars to cities to services to the whole economy. Network infrastructure, available anywhere and at any time, is transporting a huge volume of information. An obvious and immediate conclusion would thus be that the integrity of this information is crucial to the functioning of this economy.

So let's start with this point.

Continuous growth of e-commerce

It is often stated that we depend increasingly on trustworthy network services.

For example in 2014, about 13% of all retail trade in the UK was online; for 2016, retail researchers estimate that this share will grow by more than 30%. This will be good for 71 bn Euros. For Germany the numbers are slightly lower (10% in 2014 and 13.5 expected for 2016)[1].1 But in essence, for a market that depends on habits of people this growth rates are tremendous.

While it is harder to find numbers for B2B, my gut feeling says that an even bigger share of B2B transactions are carried out online or is at least supported by electronic communication – just try to remember when it was the last time that you selected a product from a paper catalogue and sent a letter to order it for your work. The younger among this audience might not even understand this question.

As a matter of fact **an increasing part of our everyday life is moving online**: e-Governance, e-health, and social networks. Most evident here is the change in the media sector. Most young people use the internet as news, communications and entertainment source - printed newspapers market share is constantly declining. For example, quite recently the newspaper *The Independent* announced its last printed issue on 26 March 2016. It is likely that this was only the first very prominent victim of the change.

Crime also goes online

So it is a fact.

We do depend increasingly on trustworthy network services for business and social life. Unfortunately also criminals "go digital". Already in 2012 12% of internet users reported that they experienced online fraud, and 8% have fallen victim to identity theft[2]. I am quite sure that our host can confirm that this issue did not disappear in the last 4 years.

And, vulnerable digital services are not only a risk for the individual users; **vulnerable services might also lead to a general decline of the overall trust in information technology and the services offered**. However, the European Digital Agenda points out that **trust in information technology** is of uttermost importance for our economy. This is echoed in the recently published NIS Directive that is aiming to *"allow[..] the public and private sector to trust digital networks' services at national and EU level. By setting incentives to foster*

[1] http://www.retailresearch.org/onlineretailing.php
[2] http://europa.eu/rapid/press-release_IP-12-751_en.htm?locale=en

investments, transparency and user awareness, the strategy will boost competitiveness, growth and jobs in the EU."

In other words: **industry needs to be encouraged to provide trust trustworthy services**. They need to be asked to implement up to date technical protection measures. **It is our belief that in this, cryptography plays a key role.**

Is there a role for cryptography?

Cryptography is the essential tool to implement secrecy and integrity for electronic communication. It provides for electronic communication is the equivalent of the letter cover, seal and rubber stamp in the brick and mortar world. Hence, it is essential to protect IT services from criminal activities. However, the use of cryptography might also make law enforcement's investigations on crimes harder. For example, an investigator might have difficulties to intercept the communication of suspects. In such a scenario 'it is only natural' that under clear rules, law enforcement should be able to intercept suspicious communication. (As much as they can search a suspicious flat). However, it turns out that this is easier said than done.

Limited key size

Some legislators have proposed to limit the key size to facilitate law enforcement. This has been introduced under the assumption that these capabilities are used only for legitimate cause, and that criminal or terrorist organizations do not have access to the technology that would be necessary for abuse.

Now, this assumption might have been correct at the time, but technology moved much faster than expected and today, with computing power as a service and a tremendous drop in costs, they do not hold anymore.

Allow me here a short advertisement block: Later today there will be a panel on "Lawful Access and Security: A Transatlantic Perspective" organized by the EastWest Institute where I will comment on the issue of key sizes a bit more in detail.

Key escrow or recovery / back doors

Others proposed key escrow or recovery. Here, neither algorithms nor key sizes are limited. Instead, the investigator gets a (technical or organizational) mechanism provided to get the private key of the suspect. Here, key recovery means being able to reconstruct the key from the encrypted message itself, while key escrow means keeping a securely stored copy of that key. Back doors on the other hand, allow the investigator to intercept the communication without the knowledge of a key.

To my knowledge, ready to use implementations of these schemes do not exist. On the one hand, the deployment of such systems would imply fundamental changes of the telecommunication infrastructure. The design and development of such systems would require the involvement of several fields of expertise, namely cryptography, personal data protection and law enforcement.

My fear would be that such systems increase the complexity of protocols, which would in turn increase the attack surface, which than even might attract criminals; just imagine criminals or terrorist that got access to private keys or a law enforcement backdoor. Moreover, in the brick and mortar world, we do not deposit the key of our front door at the local police station; there is a process to require unlocking doors which only starts after crime investigations have started.

On the other hand, it will be an economic burden to software and service providers in our legislation. Creating an economic disadvantage for our industries, since providers outside of our legislative scope will be able to deliver more secure services at a lower cost.

But the worst for law enforcement might be my last consideration: anyone who obtains a private key, can perfectly impersonate the legitimate key owner. This might be a risk to the quality of evidence that is gathered by these means.

Bypassing

But let us set aside the considerations above, in the end this all is still a matter of balance.

Society might accept the costs for industry, the risks of abuse, etc. There is a more fundamental problem with the limitation of the use of strong cryptographic tools, namely, criminals can and, by the very nature of criminals, will easily bypass all this rules, and it is hard to detect if they do so.

The research community in the field has a long tradition of creating open access and open source crypto tools; a vast amount of tools is readily free available. Furthermore, the algorithms are publically available and well documented; hence, an average skilled programmer could implement them (and it would be naïve to assume, that criminals are any less intelligent than honest people.)

This leads to the following challenge: without contextual information, such as the deployed algorithm, it is complicated to distinguish a cryptogram from a malformed message that contains only random noise. So a ban on end-to-end encryption would pose the following difficulty for the potential investigator: How to prove that a suspect has used such a forbidden technology?

Moreover, even if the use of cryptography could be easily detected, malicious users have access to a vast body of steganographic protocols, that is to say protocols that allow the user to put a hidden message in a cover media such as a picture. An investigator will usually not have enough information about the potential steganogram to discover its mere existence, let alone to decrypt the content.

To conclude

We need cryptography as the **electronic equivalent** of the **letter cover, the seal or rubber stamp**, and **signature**. These electronic tools are necessary **to protect our assets** in a **highly computerized world**. However, these are **dual-use technologies**. Any advance in cryptography, will cause new problems for crime investigation.

1) Key escrow and recovery is theoretically possible. But, it would need a fundamental change of our communication infrastructure and joint development efforts of many experts.

2) The resulting infrastructure would be more complex, making it more vulnerable to attacks and less resilient to failures. Future advances in cryptology and computing power might turn any law enforcement mechanism into a vulnerability that can be exploited by criminal and terroristic organizations.

3) The economic impact of such mechanisms might be undesirable.

4) For individuals, it would be rather simple to bypass these systems (unnoticeable for law enforcement).

One more thing, all the above mentioned issues are mere examples of currently widely used protection measures; emerging privacy enhancing technologies might introduce even more challenges. To overcome these issues, ENISA is inviting the European Commission as well as Member States and competent EU bodies to increase their efforts in performing further R&D.

Concerning all what was said above, my advice only can be: do not weaken encryption on purpose; do not inhibit the use of tools for data protection and privacy: promote secure IT.
Thank you for your attention.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu