Privacy Respecting ELECTRONIC IDENTITY MANAGEMENT and Forensics

Dr. Udo Helmbrecht

Executive Director

ENISA (European Network and Information Security Agency)

European Security Round Table Working Group ESRT

Brussels, 27th November 2009

Check against Delivery. The **spoken word applies.**

Ladies and Gentlemen,

New developments in communications and information technology have changed our societies, our economies and our everyday life. Most private companies and public institutions now heavily rely on communication networks for their daily business. For most of us, e-mail has become an important means of communications and our mobile devices, laptops and phones have become woven into every aspect of our lives.

But - there are also threats in today's virtual world. The rapid advancement of technology has created new means and new opportunities for criminals to attack and defraud companies and citizens. Every day these crimes result in significant financial losses to consumers and businesses. According to the 2008 Global State of Information Security Study[1], a significant percentage of companies who cite negative business impacts from security breaches point to financial losses and theft of intellectual property as the most severe damages. Theft or misuse of personal data was the number one concern of end users in an Internet context according to a recent ENISA survey[2]. As an example remember the massive theft of credit card information some weeks ago. Other privacy and security issues - such as behavioural marketing and leakage of corporate secrets - are on the rise.

We are already exploring the next generation of technologies that will transform our lives in many ways. When we create policies and legislation for these technologies, we have to think about how to preserve and

[1] PWC, Safeguarding the new currency of business, Findings from the 2008 Global State of Information Security Study, http://www.pwc.com/en_GX/gx/information-security-survey/pdf/safeguarding_the_new_currency.pdf

[2] ENISA Survey of end-user attitudes to security-related issues among Web 2.0 users, http://www.enisa.europa.eu/act/it/oar/web-2.0-security-and-privacy/enisa_survey_web2.pdf/view

protect the personal privacy and civil liberties that we enjoy as European citizens. ENISA will actively support the Member States and the Commission in this process. This is fully in line with our role of providing advice to political decision-makers on important trends and developments in the IT security area.

--

The title of today's workshop is “Privacy Respecting Electronic Identity Management and Forensics”. Why is privacy so important when it comes to electronic identities and identity management?

An electronic identity card, or eID card, is a gateway to personal information. Any unwanted disclosure of personal information constitutes a violation of the citizen’s privacy rights. Apart from considerations of fundamental rights, this is also a serious obstacle to the adoption of national eID card schemes and to their cross-border interoperability.

European projects and initiatives such as the eIDM roadmap[3] or the STORK project, and its successor ELSA, aim at the development of a European federated and privacy-respecting eID infrastructure. Electronic authentication is an essential part of a system's security architecture and it has to interoperate smoothly with the other parts. Internet services should be available to citizens of European countries, using the authentication means favoured by the governments of those countries. An interesting question in this context is whether whether public identifiers, or even biometric information stored on eID cards, such as a facial image or a

[3] A Roadmap for a pan-European eIDM Framework by 2010, http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf

fingerprint, should be used for private applications and what are the requirements in terms of liability. A coordinated approach combining the benefits of all approaches will be needed in future years.

ENISA is working in a collaborative way with these European projects, the member states and the industry towards common goals through organizing events and the publication of white papers and reports[4].
But we need to remember: We're only at the beginning. There are fundamentally different approaches to privacy in Europe, let alone the differences between Europe and the other continents. The challenges to be overcome before harmonization can be achieved are numerous and complicated. They include various political issues.

Unique identifiers like tax IDs, for example, are handled and looked upon in completely different ways across the member states. In some countries, for example, every citizen is allocated to a unique number which remains the same for their whole life. In other parts of Europe this approach generates considerable legal problems. A common work-around, which has been discussed in many fora and white papers, is the idea of *domain-specific* unique identifiers where the identifier of one person is only valid within a certain domain, e.g. only for banking or e-government purposes. In simple terms, the domain-specific identifier is calculated by cryptographically hashing the unique identifier of the citizen (or the serial number of an ID card) and an identifier of the domain. Applied to customer IDs this strategy may, for example, prevent the merger of customer databases by large industry branches.

[4] ENISA's reports on electronic identity, http://www.enisa.europa.eu/act/it/eid/

Identity cards are in general a controversial issue all over Europe; in some countries heavily opposed, in other countries well-advanced and currently being integrated into many existing applications. Privacy-enhancing technologies, so-called PETs, exist but they are not yet widely deployed. However, in 2007 the Commission adopted a Communication[5] to consider the benefits of PETs and to promote these technologies by supporting the development of PETs and their use.

In one of last year's position papers ENISA investigated privacy features of European eID Cards[6]. A lot of very practical techniques exist to protect the citizen's privacy and, from the survey of available techniques in this paper, it was possible to identify a set of best practice guidelines for the protection of personal data in national eID card schemes. However, European eID card specifications are very diverse in terms of their implementation of the privacy features that were identified. They are by no means universally implemented and where they are implemented, they are not always technically interoperable.

Besides domain-specific identifiers, which I already mentioned before, there are other PETs which will play an important role in future applications, not only in combination with eID cards. One of them is anonymous age-verification - proving that you are above a certain age

[5] Communication from the Commission to the EuropeanParliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

[6] ENISA Position Paper, "Privacy Features of European eID Card Specifications", http://www.enisa.europa.eu/act/it/eid/eid-cards-en/

without disclosing your name or even your date of birth. This could become an interesting feature for future social networks.

Social networks, by the way, pose interesting challenges for the designers of privacy-enhancing systems. Imagine that your teenage kids are using a social network service. You certainly would like to be assured that their 'virtual friends' are not criminals. One way of doing this is though a validation of their names and, for example, the serial number of their ID cards, against a criminal register. However, if somebody else wants to check your kids' names and ID cards against that register, you prefer that they stay anonymous. Can you see the paradox? You want full disclosure from everybody else but refuse any kind of disclosure on your side.

This brings us to the relation between different types of eIDs and the security context in which they are being used. For example, the type of eID used to authenticate to your social network provider (chosen username and password) is a totally different security context to that used to authenticate to your bank. Citizens often use the same information - the same passwords, the same PINs - to secure credentials of greatly different security context, which is problematic. Figures about cyber crime trends in the first half of 2009 indicate that Internet users are far more susceptible to phishing and malware scams that use social media sites as a lure[7].

There are mechanisms that address these issues. Besides numerous scientific papers there are also several industrial products that provide unlinkable credentials for privacy-respecting applications. Revocation

[7] Washington Post, Brian Krebs, Spike in Social Media Malware, Phishing Attacks, http://voices.washingtonpost.com/securityfix/2009/11/spike_in_social_media_malware.html

plays an important role here. Sound revocation mechanisms of ID cards and certificates are fundamental and might jeopardize the entire scheme if not properly taken care of. In particular when deploying new technologies, like domain-specific UIDs or pseudonymous authentication, it is important 'to have revocation in mind' when designing the infrastructure.

This is, amongst others, one of the findings of a recently published position paper on the security of web authentication using eID cards[8]. ENISA will continue to work with experts from government, industry and academia in order to review the current situation and to develop guidelines addressing the needs of policy-makers and European initiatives.

I would like to make the point here that authentication is *not* trust. It tells us who we are dealing with. The trust comes from exactly what is checked by the registration procedures, which can differ greatly from service to service.

So, within the context of the 2010 Work Programme, ENISA has established a so-called 'Preparatory Action' on Trust and Privacy in the Future Internet. One of the objectives of this activity is to perform stock-taking exercises on authentication and privacy mechanisms, as well as existing security models of electronic services. By doing so, ENISA intends to assess the balance between privacy and accountability, consent and tracking. Today's online application environments are characterised by a plethora of "customized" security models tailored to various classes of applications in which they operate. There is a need to examine how users should use different types of electronic services.

[8] ENISA Risk Assessment Report, " Privacy and Security Risks when Authenticating in the Internet with European eID Cards", http://www.enisa.europa.eu/act/it/eid/eid-online-banking

For this reason, in 2010 ENISA will study security models of electronic services and their performance in highly distributed environments, such as today’s Internet. In addition, ENISA will investigate various ways of assuring privacy and accountability in the Internet, review the most prominent methods used, study their mapping to the underlying architectures, assess their level of effectiveness and performance and the impact on existing and future standards. With its international team of IT security experts, ENISA is well-equipped for these tasks and ready to become a key player in Europe's eID arena.