Securing Personal Data: ENISA guidelines on Cryptographic solutions

ENISA is launching two reports today. The "Algorithms, key size and parameters" report of 2014 is a reference document providing a set of guidelines to decision makers, in particular specialists designing and implementing cryptographic solutions for personal data protection within commercial organisations or governmental services for citizens. The "Study on cryptographic protocols" provides an implementation perspective, covering guidelines regarding protocols required to protect commercial online communications containing personal data.

"Algorithms, key size and parameters"

This report provides a set of proposals in an easy to use form, with a focus on commercial online services that collect, store and process the personal data of EU citizens. It provides an update of the 2013 cryptographic guidelines report on security measures required to protect personal data in online systems. Compared with the 2013 edition, the report has been extended to include a section on hardware and software side-channels, random number generation, and key life cycle management, while the part on protocols, for 2014 is extended and is a stand-alone study on cryptographic protocols.

The report explains two aspects of cryptographic mechanisms:

- whether a given primitive or scheme can be considered for use today if it is already deployed
- whether a primitive or scheme is suitable for deployment in new or future systems.

Long term data retention issues are analysed along with a number of general issues related to the deployment of cryptographic primitives and schemes. All the mechanisms discussed in the report are standardised to some extent, and have either been deployed, or are planned to be deployed, in real systems.

"Study on cryptographic protocols"

The second report focuses on the current status in cryptographic protocols and encourages further research. A quick overview is presented on protocols which are used in relatively restricted application areas, such as wireless, mobile communications or banking (Bluetooth, WPA/WEP, UMTS/LTE, ZigBee, EMV) and specific environments focusing on Cloud computing.

The main emphasis of the report is on guidelines to researchers and organisations in the field, which include:

- Cryptographic and security protocols to be designed by cryptographic protocol experts rather than networking and protocol experts to date. Additionally, researchers need to simplify the analysis and enable automated tools to provide strong computational guarantees.
- More attention is required to automated verification so the implementation of a protocol can meet given security goals, and examine how automated tools can guarantee correct implementation of a protocol design.
- Small insignificant changes in protocols can result in invalidating the guarantee proofs.

- Future protocols should be designed using solid and well-established engineering principles, ease of formal security analysis, and in conjunction with the development of formal security proofs, designed in cryptanalysis of their constituent primitives.
- Future protocols should not be any more complex than they need to be.
- More work needs to be performed on verifying APIs for application protocols.

Udo Helmbrecht said of the reports: *"What is highlighted is the need for certification schemes in all phases of the technological life-cycle. 'Security by design or by default' built in processes and products, are basic principles for trust. Standardising the process is an essential element in ensuring the correct application of the data protection reform in the service of EU's citizens and its internal market. ENISA's guidelines strive to provide the correct framework in securing online systems."*

The EC Regulation 611/2013 references ENISA as a consultative body, in the process of establishing a list of appropriate cryptographic protective measures for personal data protection. ENISA's cryptographic guidelines should serve as a reference document. Within this scope, the provided guiding principles are rather conservative based on current state-of-the-art research, addressing construction of new commercial systems with a long life cycle.

For the full reports: "Algorithms, key size and parameters" & "Study on cryptographic protocols"

For interviews and further information: press[at]enisa.europa.eu