Comments to the Green Book "La protection juridique des services cryptés dans le marché intérieur"

Dr. Josep Domingo-Ferrer Ricardo X. Sánchez del Castillo

Escola Tècnica Superior d'Enginyeria
Universitat Rovira i Virgili
Autovia de Salou s/n, E-43006 Tarragona, Catalonia
E-mail: jdomingo@etse.urv.es
Tel.: +34-77-559657
Fax.: +34-77-559621

1 Introduction

This document contains comments to the Green Book "La protection juridique des services cryptés dans le marché intérieur" (Brussels, 06.03.96). We answer in this way to the public request for comments contained in the Green Book.

In the following sections, questions Q1 to Q5 raised on page 45 of the Green Book are dealt with. We are university professors and have no commercial interests. We contribute as experts in information security and cryptography.

2 Q1: Supplementary information to analyze national regulations in more detail

Encryption/decryption mechanisms were created as a technical solution in order the ensure the exploitation of a given service (in this case an information broadcasting service).

The fact that the technical solutions used failed to achieve their security target should not be a reason to create new regulations. A technical solution that does not

fulfill its function should not be "patched" by specific regulations, but replaced by a better technical solution (which is available nowadays).

On the other hand, encryption is a means and is not an end in itself. Therefore, regulation (if needed) should be done at a more general level such as the information broadcasting level.

As a guideline, the European Commission should consider the appearance of new technologies whose use is more and more affordable. The technological development in information security and cryptography can lead to simplifying or even eliminating many regulations. For example, if an author or service provider can *technically prevent* unauthorized use of the service he/she provides, is legislation necessary? A better thing to do is to *certify that a given technology meets its security target*. The European Commission has already worked on this useful issue (see *Information Technology Security Evaluation Criteria (ITSEC)* and *Information Technology Security Evaluation Manual (ITSEM)*).

3 Q2: Restrictions and restrictive effects other than those identified in chapter 4 of the Green Book

We are in a free-market economy. Encrypted service providers are standard companies, and it is up to them to look after their own profitability. Technology is available that can protect them against abuse (and this technology *is* affordable).

Therefore, it is our opinion that the European Commission should not get involved in a problem which is common to all kinds of companies: how to succeed and avoid failure.

4 Q3: Need for a harmonization at the Community level

The European Commission should concentrate its efforts in *simplifying* and homogenizing national regulations that try to

- Ensure a fair relationship between authors, service providers and consumers.
- Characterize the rights and duties of the user of broadcasted information.

5 Q4: Possible harmonization instrument

New legal instruments should *not* be created. At most, a recommendation to simplify (or even abolish) certain national regulations should be issued.

If some harmonization is needed, it is in order to minimize regulations and propose a list of certified technologies to enforce protection of authors' and service providers' rights.

6 Q5: Application of a possible harmonization instrument

As stated in the previous section, we do not recommend to create such a harmonization instrument. In order to justify our position, we discuss the subquestions of question Q5 raised in the Green Book

i. Application field:

a. No regulation is needed neither for broadcasting services nor for any other encrypted services. Protection provided by current encryption techniques is more than enough and can be afforded by companies.

b. As we say, regulation should be minimized, not maximized. States or the European Commission should not spend their efforts and resources at helping some *private* companies to get paid by the people using their services. If the European Commission feels that this is a part of its duty, then such help should be extended to all sorts of private companies. Unfortunately, the difficulty in getting paid is shared by most companies in the Union. Regarding the opportunity of legal protection against unlawful reception of any conditional-access service, we definitely think that it makes no sense. If bad access control services are to be supplemented by legislation, one could go as far as forbidding unlawful reception of clear (unencrypted) broadcasts. Again, the solution is to use better (certified) encryption algorithms.

ii. Possession of unauthorized devices:

If an individual buys a decoding device, then he/she is not responsible for the device being authorized or not. Further, one cannot pretend that the consumer be able to distinguish authorized devices from "forged" functionally equivalent devices. Thus, buying unauthorized devices cannot be regarded as an offence.

Even building or selling unauthorized devices is not a clear offence; it just proves that the encryption algorithm used is weak and should be improved.

7 Conclusion

To summarize, we recommend that weak encryption techniques do not be "patched" by regulations. Instead, stronger techniques available nowadays should be used. We are surprised by the European Commission being so concerned about profitability of encrypted service providers. In our opinion, setting up the technical security mechanisms to protect themselves against abuse is part of the business of such companies. Anyway, if the European Commission is concerned by the cost incurred by service providers to improve their technology, then perhaps the efforts and resources allocated for producing regulations should be redirected toward helping companies to keep the pace with modern technology.