How to Bypass the Wassenaar Arrangement: A New Application for Watermarking

Franck Leprévost
Institut Fourier BP 74
F-38402- Saint Martin d'Hères
Cedex, France
leprevot@math.tu-berlin.de

Raphaël Erard
EPFL, DE-LTS
Ecublens
CH-1015 Lausanne
Raphael.Erard@epfl.ch

Touradj Ebrahimi
EPFL, DE-LTS
Ecublens
CH-1015 Lausanne
Touradj.Ebrahimi@epfl.ch

ABSTRACT

The scope of this article is to clarify the current legal and political situation related to electronic surveillance on the one hand, and to export regulations for encryption software on the other hand. We will look at different international agreements, such as the UKUSA agreement and the Wassenaar arrangement, and elaborate on current encryption techniques falling under these regulations. This discussion is then followed by introducing the basic concepts of steganography and digital watermarking which could be used for secret communication. As a consequence, we propose an original way to legally bypass the international export regulations using these technologies. To this end a new watermarking technique is proposed, which is robust to JPEG2000 compression and provides a good channel capacity. The efficiency of the proposed technique is analyzed by means of simulations to allow for secure communications.

Keywords

Wassenaar Arrangement, watermarking, cryptography, steganography

1. INTRODUCTION

In the digital age, the need to rely on secure communications is an important matter not only for diplomatic or military purposes, but also for business purposes such as e-commerce, marketing strategies and financial secrets. Moreover, various agencies increasingly focus on the collection of sensitive information such as in corporate espionage.

In Section 2, we recall the UKUSA agreement and the ECHELON network, both cited officially for the first time in a survey [22] in the context of technologies of political control. This triggered the European Parliament to ask for a more in-depth study on the development of surveillance technology and the risks of abuse of economic information ([3], [5], [17], [4]).

As explained in [17], one obvious solution against these risks would be to use cryptography, on which we concentrate in Section 3.

In Section 4 we look at the legal aspects, related to the export restrictions on cryptographic software which have been recently introduced under the leadership of the USA. The focus is on the Wassenaar Arrangement ([21]) on *Export Controls for Conventional Arms and Dual-Use Goods and Technologies* which is the successor of COCOM (Coordinating Committee for Multilateral Export Controls). The goal of the arrangement is to restrict movements of potentially dangerous technologies such as biological, nuclear, and chemical weapons, missiles, artillery, and, since December 1998, encryption software. We will show that the security of the "free-exportable" cryptoproducts is not guaranteed. Therefore the question arises, if you want to communicate in a secure manner, do you have to break law? Not quite!

A technical and legal solution is provided by steganography and digital watermarking which we will review in Section 5.

Finally, section 6 provides an overview of the technique used in this article for hiding additional information in a video sequence and will report some of the performance results.

2. THE UKUSA AGREEMENT AND THE ECHELON NETWORK

In 1947 ([2]) the governments of the United States, the United Kingdom, Canada, Australia and New Zealand signed a national security pact known as the United Kingdom - United States (UKUSA) agreement. The intention of the agreement was to seal an intelligence bond in which a common national security objective was created. The UKUSA agreement standardized terminology, code words, intercept handling procedures, arrangements for cooperation, sharing of information, and access to facilities. The more impressive realization of the UKUSA agreement is the ECHELON network. It was exposed in detail for the first time in 1996 in Nicky Hager's book [9]. All written communications such as telex, fax, and e-mail are intercepted at the Waihopai station and then fed into computers. The computers automatically search through everything as it arrives at the station with the help of a dictionary program. This program picks out

To appear in the 8th ACM International Multimedia Conference on Multimedia and Security, November 2000, Los Angeles, California

all the messages containing target keywords and numbers. Thousands of simultaneous messages are read in 'real time' as they pour into the station, as the computer finds intelligence needles in the telecommunications haystack. Encryption is an appropriate counter-measure to fight the spooks operating at satellite tracking stations run by the NSA – in Australia (Geraldton), England (Morwenstow), the U.S. (Sugar Grove and Yakima) and other places.

3. CRYPTOGRAPHY

3.1 Secret-key cryptography

Without any doubt, the most widely used block cipher is the Data Encryption Standard (DES, [7]). Acknowledged as FIPS 46 in 1977, DES uses a secret key of length 56 bits, while the blocks have a length of 64 bits. Because of the existence of the DES-cracker constructed by the Electronic Frontier Foundation ([8]), symmetric algorithms using secret keys of length ≤ 56 bits should no longer be considered as secure.

3.2 Public-key cryptography

Public key algorithms are usually based on one of the following mathematical problems:

- Integer factorization problem (IFP): RSA and Rabin-Williams.
- Discrete logarithm problem (DLP): DSA, key exchange of Diffie-Hellman, coding methods of El Gamal, digital signature of El Gamal, of Schnorr, and of Nyberg-Rueppel.
- Discrete logarithm problems for elliptic curves over $\mathbf{F}_p$ or over finite fields of characteristic 2 (ECDLP): these are analogous to the algorithms mentioned above.

A standard [11] provides a reference for specifications of a variety of techniques from which applications may select. The draft [11], which started as the "Standard for Rivest-Shamir-Adleman, Diffie-Hellman, and Related Public-Key Cryptography", became a IEEE-standard in the first half of 2000. It includes in particular elliptic curves cryptosystems, which offer the highest strength-per-key-bit of any known public-key system. For example, with a 112-bit modulus, an elliptic curve system offers the same level if cryptographic security as DSA or RSA with 512-bit moduli.

4. LEGAL ASPECTS

Although very secure secret-key and public-key cryptosystems do exist, it does not mean that privacy and corporate secrets are protected. One has to pay attention to legal aspects (see [13]). On November, 1993 in The Hague, the representatives of the 17 member countries of COCOM decided to dissolve COCOM and rethink its function into the post cold war era. This decision was confirmed in Wassenaar (Holland), and effective on March, 1994. At this date, 33 countries, including the countries of the EU and - partly overlapping - of the UKUSA agreement, are participating states of the Wassenaar Arrangement. Concerning information security, very important changes were made during the last meeting of the representatives in Vienna on December, 1998 ([21]). They concern the category 5, part 2, entitled Information Security. In short, the part 5.A.2 specifies that are under control the systems, equipments and components using (directly or after modification):

1. a symmetric algorithm (like DES) employing a key length in excess of 56 bits for niche markets and 64 bits for mass market applications ; or
2. an asymmetric algorithm where the security of the algorithm is based on any of the following:
   - Factorization of integers (like RSA) in excess of 512 bits;
   - Computation of discrete logarithms in a multiplicative group of a finite field (like DSA) of size greater than 512 bits; or
   - Discrete logarithms in a group other than mentioned above in excess of 112 bits.

Unfortunately, the security-level of the free-exportable public key cryptoproducts is obsolete: Shamir [20] described a hardware based method to factorize very quickly RSA-512 bits. Also, as pointed out in [16], the level of security offered by a 64-bit symmetrical encryption is roughly equivalent to the protection offered by 768-bit RSA. It would be therefore logical to set the limit for RSA keys to be at 768 bits in the Wassenaar Arrangement, although considered as breakable since 1995 (see [16]).

5. USING DIGITAL WATERMARKING TO BYPASS THE WASSENAAR ARRANGEMENT

To our knowledge, two solutions exist to bypass legally the Wassenaar Arrangement. Rivest's Chaffing and Winnowing's method ([19]) relies on digital signature, and as such involves some techniques that are usually included in cryptography area. We focus here on a complementary although different approach: steganography and digital watermarking.

Two main goals of encryption are secrecy and privacy. That is, a non authorized party should neither be able to read the information, nor should it be possible to identify a secret communication. Steganography [1] and digital watermarking [10] are two related technological concepts, both providing a similar functionality as encryption. However, the difference with encryption is that the message to be transmitted is not encrypted, but hidden in the cover data under use of a secret key, resulting in the stegano data. In the recovery process, the message is extracted from the cover data under use of the same secret key. In some cases, especially in digital watermarking applications, the original data is also required in the watermark detection process.

From a functional point of view, steganography and watermarking are equivalent, that is both methods hide a message in the cover data and allow for the recovery of the message given the stegano data. Furthermore, both methods have the requirement of transparency which says that the stegano data should not be perceptually different from

the cover data. However, the difference between the two approach is related to the robustness of the hidden message. Robustness in this context describes the behavior of the system if the stegano data has been modified. In steganography, it is usually not possible to recover a message from the modified stegano data. However, in digital watermarking, message recovery is possible, even if the stegano data has suffered from distortion, for example through modifications such as lossy compression, filtering or geometrical transformations. Of course, for increased robustness the user has to pay a price, which is in general a reduction in the channel capacity. In other words, in digital watermarking applications the message is usually shorter than in steganographic methods.

6. A WATERMARKING ALGORITHM TO BYPASS THE WASSENAAR ARRANGEMENT

Existing watermarking techniques (see [6], [10], [15]) are designed with image authentication and/or copyright protection in mind. Thus, they provide fair robustness against specific kind of attacks: geometrical distortions, image compression, noise addition, filtering, etc. A steganographic use of a watermarking technique will not benefit from a robustness to all of these attacks, because the host image is simply used as a *container*. Only a resistance to image compression is required, to enable transmission of the watermarked image using standard image compression techniques (lossy JPEG or JPEG2000 [12] for example).

Our watermarking scheme provides data hiding and retrieval with the use of a secret key; the unmarked image is not required to retrieve the hidden information and the method provides an integrity check on the embedded data. A secret key is used to generate a binary random sequence, which is is mixed with the actual watermark before the embedding process. Without the key, it is not possible to extract the watermark; it's even not possible to prove the existence of a watermark hidden in an image. The integrity of the retrieved watermark is asserted using a simple but efficient CRC-16 checksum [18]. This checksum is useful, because we can not tolerate a single bit error in the retrieved information. Our watermarking technique doesn't require the original (unmarked) image to retrieve the watermark. This is possible by embedding a redundant watermark, hence introducing some known correlation in the host image. Our technique is based on the *amplitude modulation technique*[14]: in summary, the wavelet decomposition of the blue channel of the image is computed, and each of the wavelet coefficients is modified to embed a single bit of the watermark:

$$C_i^{'} = C_i \left(1 + (-1)^{b_i + r_i(\sigma)} \alpha\right), \qquad (1)$$

where C_i is a wavelet coefficient, $C_i^{'}$ the modified wavelet coefficient, α is the strength of the embedding process, b_i one bit to embed and r_i a random number based on the key-seed σ.

To estimate the capacity of this method, and its resistance to the upcoming standard JPEG2000, we've performed a series a simulations. First, the length of the watermark is set (for instance 256 bits). Then, different strength values α are taken. Because our main goal is capacity and because the host image will be highly compressed with the JPEG2000 lossy coder, it does not matter if the watermark is slightly visible after choosing a high value for α. Then, given the length and the strength of the watermark, 200 different embedding steps are performed on 4 different test images (lena, bike, cafe and woman, 512×512 pixels), using random hidden data and secret keys. The 800 covers images are then compressed with the JPEG2000 coder at various target bitrates. Finally, we determine the minimum bitrate that still allows the complete recovery of the watermark from our 800 covers images after the compression. The results are depicted in Fig. 1. Statistically, the probability of watermarking recovery error having chosen a compression ratio given by Figure 1 is less than $1/800 = 0.125\%$.

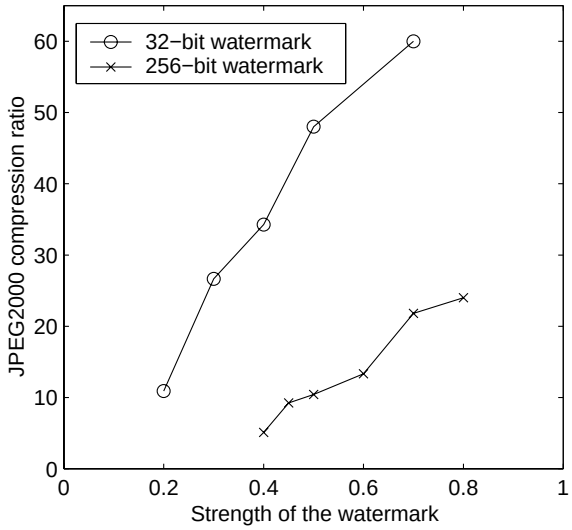

Figure 1: Given the watermark length (32 or 256 bits) and the strength of the watermark, this graph gives the minimum JPEG2000 compression ratio that still allows full recovery of the watermark from the JPEG2000 compressed host image.

We can of course generalize the method to a video sequence coded with MotionJPEG2000 (each frame of the video is coded with JPEG2000). With 256 bits, it is possible to to encode 34 characters of plain English. Of course, this capacity can be expanded if we entropy encode the secret message. Through a simple calculation, we can see that a 30-seconds video sequence (25 frames per seconds) can hide more than 25 000 characters (equivalent of 3 pages of text) and be relatively robust up to a compression of 10:1.

7. CONCLUSION

The introduction of legal barriers on export of cryptosoftware is officially a way to counter terrorism and organized crime. Although these two threats have to be very carefully considered by ad-hoc organizations, this article shows that these measures in reality do not provide a valuable help against them, for at least two reasons:

- The first one is technical: This article presents a simple

and efficient algorithm to hide a secret message inside a compressed image sequence, and provides some proof of efficiency. Hence using digital watermarking makes possible to bypass those restrictions.

- The second one is common sense: which terrorist or criminal would ask for a permission to use crypto-software? Moreover, such softwares could be downloaded from the Internet, or even developed by moderately well-founded organizations.

The measures described in the part 4 of this article indeed have perverse consequences: From a technical point of view, they facilitate eavesdropping (see section 2) and hence may constitute a handicap for "honest" people and corporations.

8. ADDITIONAL AUTHORS

Additional authors: Martin Kutter, Ch. des Combes 17A, CH-1802 Corseaux, email: `martin.kutter@kutter.ch` and Diego Santa Cruz, EPFL, DE-LTS, Ecublens, CH-1015 Lausanne, email: `Diego.Santacruz@epfl.ch`.

9. REFERENCES

[1] R. Anderson and F. Petitcolas. On the limits of steganography. *To be published in a special issue of IEEE J-SAC*, 1998.

[2] J. Bamford. *The Puzzle Palace: A Report on America's Most Secret Agency*. Viking Penguin, September 1983.

[3] N. Bogonikolos. *Developpement of surveillance technology and risks of abuse of economic information. Part 1/4: The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception*. European Parliament, Directorate General for Research, Directorate B, STOA Programme, 1999.

[4] D. Campbell. *Developpement of surveillance technology and risks of abuse of economic information. Part 4/4: The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadland multi-language leased, or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition*. European Parliament, Directorate General for Research, Directorate B, STOA Programme, 1999.

[5] C. Elliot. *Developpement of surveillance technology and risks of abuse of economic information. Part 2/4: A concise survey of the principal legal issues and instruments under international, European and national law*. European Parliament, Directorate General for Research, Directorate B, STOA Programme, 1999.

[6] R. A. F. Petitcolas and M. Kuhn. Information hiding – a survey. *Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Information*, 87(7):1062–1077, July 1999.

[7] FIPS 46. Data encryption standard. Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977. (revised as FIPS 46-1: 1988).

[8] E. F. Foundation. *Cracking DES, Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly, 1998.

[9] N. Hager. *Secret Power-New Zealand's Role in the International Spy Network*. Craig Potton Publishing, 1996.

[10] F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proceedings IEEE:Special Issue on Identification and Protection of Multimedia Information*, 87(7):1079–1107, July 1999.

[11] IEEE. P1363 draft, version 13. http://grouper.ieee.org/groups/1363/index.html.

[12] JPEG Committee. JPEG 2000 web site. http://www.jpeg.org.

[13] B.-J. Koops. Crypto-law survey. http://cwis.kub.nl/∼frw/people/koops/lawsurvy.htm.

[14] M. Kutter, F. Jordan, and F. Bossen. Digital watermarking of color images using amplitude modulation. *Journal of Electronic Imaging*, 7(2):326–332, Apr. 1998.

[15] M. Kutter and F. Petitcolas. A fair benchmark for image watermarking systems. In *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, volume 3657, pages 226–239, Jan. 1999.

[16] A. K. Lenstra and E. R. Verheul. Selecting cryptographic key sizes. *PKC2000*, 2000.

[17] F. Leprévost. *Developpement of surveillance technology and risks of abuse of economic information. Part 3/4: Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues*. European Parliament, Directorate General for Research, Directorate B, STOA Programme, 1999.

[18] W. H. Press. *Numerical Recipes in C: The Art of Scientific Computing*, chapter 20, pages 896–901. Cambridge University Press, 1992.

[19] R. L. Rivest. Chaffing and Winnowing: Confidentiality without encryption. *CryptoBytes (RSA Laboratories)*, 4(1):12–17, Summer 1998.

[20] A. Shamir. Factoring large numbers with the twinkle device. *Preprint*, 1999.

[21] Wassenaar Arrangement. http://www.wassenaar.org.

[22] S. Wright. *An Appraisal of the Technologies of Political Control*. European Parliament, Directorate General for Research, Directorate B, STOA Programme, 1998.