



The Security Newsletter

N°3

Fall 2006

In this issue

Be our guest	2
The news	3
Xbox hacked	3
CP that reboots	3
WEP: The lengthy burial procession	4
Is selling illegal advice illegal?	4
Internet Armageddon will start on Feb. 27, 2010 at 07:30AM5	
Fingerprinting cameras	5
Digital watermarking	6

Published By
Thomson Corporate Research
Part of the
Technology Division

Technical Editor:
Eric Diehl

Editors:
Nicholas de Wolff
Elizabeth Marx

Contributors:
Jeffrey Bloom
Olivier Courtay
Olivier Heen
Mohamed Karroumi
Frédéric Lefebvre
Benoît Macq (UCL)
Philippe Nguyen
Nicolas Prigent

SBU Technology Heads:
Jean-Charles Hourcade, Willy Shih

Mail:
security.newsletter@thomson.net



Am I an “evildoer”? This was my recent existential question. According to the EFF (Electric Frontier Foundation), I am an accomplice to three evil super heroes [16]; based on an editor’s opinion, I am designing CRAP (Content Restriction Annulment Protection), better known as DRM [14]; and according to an author, I am destroying the creativity of the new generation [4]. Sounds somehow evil to me...

After some home-brewed therapy, I thought, why does game protection raise only a few objections? Except for some minor cases, where game system protection has caused havoc (see the news), customers tolerate it. Then why not content protection? A possible answer is that customers have much higher expectations regarding the usability of their content. The obvious but difficult challenge is the interoperability of content protection systems. Of course, there are many other rationales. Security must also integrate the societal and sociological parameters in its designs. There is always a trade-off between the conflicting interests of all the participants of various systems. A balanced position would reduce piracy.

I am pleased to introduce a new section, Be our guest starting this issue. Each quarter we will invite a famous security researcher to share views on security and offer forecasts for the future of our field. Our first guest is Benoit MACQ from Université Catholique de Louvain (UCL). Benoit is well known in the watermark community. Also in this issue, Jeffrey BLOOM and Philippe NGUYEN present a solid introduction of digital watermarking.

Oh, do I still feel like an evildoer? I am still here, so guess the answer.

E. DIEHL, Technical Editor

Attending IBC, September 8-12th?



Do not forget to visit the Thomson Content Security Booth 11.550, Hall 11.

Be our guest

Images and beyond: the target of Thomson technologies. When dealing with security, the objects to protect in this domain are manifold: images and sounds produced in camera; processed and post-produced in studios; formatted for distribution and delivered to devices for producing a visual experience to consumers.

Security of the whole chain may not be restricted to a simple secure digital communication problem. When dealing with media, the final experience is delivered by the projection of light on to the screen and in acoustic waves from loudspeakers. Even if the cryptographic security were to be perfect, it could only protect *bits* from the source to the destination. In the end, the light projected on the screen can be re-digitized and re-distributed illegally.

To combat efficient redistribution, forensic watermarking is the only technological tool that allows tracing the usage of a particular distribution of a movie. Watermarking modifies the waveforms imperceptibly to embed robust messages in the waveform. It is the ultimate protection of the intrinsic *wave* of the contents, independent of their various potential binary representations. Watermarking, in combination with trusted devices, has been envisaged for copy control, but not very successfully up to now.

(Con’t)

The security of the distribution chain requires that distant devices share trusted information, like ciphering keys. Trust between the processing units of the distribution chain requires trusted devices, resistant to tampering. For that purpose, one needs devices that include tamper-resistant processing units, where the *atoms* conveying critical information are physically protected.

The first European project we had at UCL, when Jean-Jacques Quisquater and I arrived as professors, was the ACCOPI project. It was a small project combining conditional access, including the use of tamper-resistant smart cards and watermarking techniques. Our German partners were E. Koch and J. Zhao [currently part of Thomson's Security business management team – Ed.]. Their algorithm is a reference in the domain and has shown to be useful in many video applications.

Today we are launching a very ambitious research project on Digital Cinema, the ED-CINE project, funded by the European Commission, with the security experiments handled by Thomson and UCL. The goal is to provide tools beyond the DCI (Digital Cinema Initiative) specifications. All the initial ingredients are there. Ciphering mechanisms will provide protection of bits. Forensic watermarking will protect waves. And atoms will be protected in a list of Trusted Devices.

Being back with the Thomson team on these topics with keynote researchers we have known for a long time is an exceptional opportunity for academic research in the field. Our team is very excited about future security research for images and beyond.

B.MACQ (Université Catholique de Louvain)

The news

Xbox hacked

Only four months after the release of the Xbox 360, a hacker called "TheSpecialist" disclosed an attack that allowed running illegal copies of games. In fact, the hack was merely an adaptation of an older Xbox v2 hack.

Xbox 360 uses many protection layers such as signature of playable files, a so-called "mediaflag" on the disc that identifies bootable media, and a unique 128-bit secret key embedded in authorized DVD drives.

Unfortunately, the DVD drive firmware code is not cryptographically signed. Thus, TheSpecialist replaced it with firmware that plays any recordable media. Bit-to-bit copies of legal titles would now play. The Xbox was in essence "tricked".

Microsoft corrected the error. The hack now only works for the earlier Xbox 360 using the "Hitachi-LG GDR-3120L DVD-ROM" drive.

A well-known lesson: "A chain is as strong as its weakest link". This is especially true when considering third-party equipment and subcontractor code such as firmware.

O. HEEN, M. KARROUMI

CP that reboots

In our first issue (December 2005), we highlighted Sony's copy protection system; so intrusive it was considered malware. This time another copy protection system is facing challenges from the marketplace, the Starforce™ system [15]. Starforce provides solutions to game editors like Ubisoft™. When it detects illegal access to the content, the Starforce system immediately reboots the computer. Any unsaved data is lost

(cont'd)

during the reboot. Unfortunately, the detection is not perfect and has false positive detections (the system confuses attack and normal use). In response, a boycott against all Starforce protected products launched on the Internet [18]. Ubisoft has decided not to use this protection anymore.

O. COURTAY

WEP: The lengthy burial procession

WEP (Wired Equivalent Privacy) was the initial proposal to secure 802.11. It uses a shared-key mechanism. To communicate on a given 802.11 network, one has to know the 40 bits-long WEP key. This key is used in conjunction with a 24 bit-long Initialization Vector (changed at each message for diversification) as an input to the RC4 stream-cipher. The resulting key-stream is XOR-ed with the clear frame to encrypt it, and XOR-ed to the encrypted frame to decrypt it. To ensure integrity, WEP computes the CRC-32 checksum on the clear-text and appends it to the message before encrypting them altogether.

Numerous attacks against WEP have been disclosed. First, the very small IV space (2^{24} possible values) requires that the IVs be reused after a few hours on a same network [1]. Thus, different frames are encrypted with the same key-stream. If clear-text is known for one of the frames (which may happen under reasonable hypotheses), the attacker can compute the key stream for this IV and decrypt all the other messages that use it. Second, even without knowing the clear-text message, the use of CRC-32 allows modification of any encrypted message by tuning the encrypted CRC to obtain a legitimate-looking message [1]. Third, the key-space itself (2^{40} possible values) is too small and makes brute force or dictionary attacks possible. WEP2, with 104-bit keys, is

designed to counter these attacks. Unfortunately, research has shown [4][11] that certain “weak IVs” lead to leakage about the key, whatever its length: About 10^6 frames suffice to recover the WEP key.

Nevertheless, many networks still use WEP. A recent attack [2] may be the “last nail in WEP’s coffin”. It injects encrypted frames of arbitrary length without knowing the key. It uses the fragmentation function of 802.11. Like in IP, the source may split a frame into smaller frames. The destination handles these frames and returns the original frame. First, the attacker seeks for encrypted frames containing ARP messages. They are easily distinguishable due to their size and MAC destination, and have easily guessable clear-text. The attacker then knows the key-stream for the IV of these frames and can inject 36 bits long messages. Using fragmentation, he or she can inject arbitrary messages.

This new attack demonstrates that WEP should no longer be used. While WPA still allows fragmentation, its dynamic re-keying mechanism prevents IV reuse, uses a much more secure algorithm for integrity, and is thus preferable to WEP.

N.PRIGENT

Is selling illegal advice illegal?

The answer is yes. In May 2006, the Federal Trade Commission (FTC) sentenced Cashier Myricks [17]. His website proposed, for \$24.95, a “100% legal” method to download copyrighted material. In fact, he sold a tutorial for using current free P2P file sharing software.

Myricks will have to refund his 611 customers. The FTC will not sue the lured customers for copyright infringement.

E. DIEHL

Internet Armageddon will start on Feb. 27, 2010 at 07:30AM

“Security is 20% technology, and 80% people and process”

Worms such as Code Red, Witty or Nimda regularly plague the Internet. They cause massive unavailability, data loss, and web site defacement. The efficiency of a worm attack is related to several factors: the infection vector (mail, applications, and documents); the exploited vulnerabilities of targets; and the reaction delay before the first workarounds and corrections appear. This last factor is critical. The longer the reaction is delayed, the wider the proliferation.

Before carrying out an appropriate defensive action, several human actions must take place. First, someone has to understand what is going on, then catch the worm and reverse engineer it. Once the vulnerabilities exploited by the worm are understood, a specific patch can be developed and distributed. Only then are administrators able to test and apply the patch.

The duration of this causal chain is determined by human availability. Therefore, the optimal moment to release a worm is when nobody is available!

From this statement, Fries et al. managed to determine the longest non-working periods for the next four years [7]. They first collected information about working-time in the 50 most Internet connected countries. This information includes standard business days and hours, daylight saving times, national and religious holidays. Then an algorithm systematically scanned the database and determined **February 27, 2010 07:30 to February 28, 2010 20:00** as the longest non-working period worldwide. During those 36.5 hours, few people will be at work to detect and fight back a worm proliferation.

Restricting the geographical zone led to interesting results. North America will go across an 82.5 hours non-working period from December 23, 2006 3:30 to December 26, 2006 2:00; this is due mostly to Christmas Day falling on a Monday. Taiwan and Turkey have the longest nationwide non-working period during the next four years: 159 hours (almost one full week). Knowing this, a hacker may release worms in these areas at the worst moment.

Conversely, software editors may use the same algorithm to determine the best moment to release a patch: during long working periods. At that time, more administrators will be available to correctly test and apply patches.

O. HEEN

Fingerprinting cameras

There is a growing need for security and forensic methods in an ever-expanding range of applications [12]. Forensic methods for digital camera applications include:

- Metadata in the image header
- Watermarking
- Fingerprinting

The first technique concerns the Exchange Image File (EXIF) containing metadata such as date, serial number of the camera, and camera references. However, metadata is

not persistent in the case of post-processing and file conversions. Watermark technology requires embedding of a watermark algorithm inside the camera device. Only a few manufacturers are ready to include this feature in their high-end devices.

(cont'd)

Fingerprinting is a new technique largely used to track and trace content by extracting representative and unique features from the content.

Lukas, et al. propose to trace information back to a digital camera device by only using its output [10]. They put forward an innovative solution to identify the sensor that generated the images. This so-called “biometric device” links a digital image to its digital camera. It extracts unique and robust image features from the sensor. Each sensor generates a specific noise or imperfection, also called sensor fingerprints that the authors try to uniquely link to the digital camera.

The sensor noise is divided into fixed pattern noise (FPN) and photo response non-uniformity noise (PRNU). FPN is in the dark frame that is sensitive to exposure and temperature. PRNU is present in all natural frames. Non-uniformity of noise is due to variable sensitivity of pixels to light, optical lens characteristics and light refraction on dust particles. Optical lens and light refractions on dust particles are of low frequency and are independent of the sensor.

The authors focused their research on pixel non-uniformity (PNU) which is the sensitivity of pixels to the light. This noise is mainly due to the heterogeneity of silicon wafers and imperfections during the manufacturing process. Thanks to image processing, the authors remove non-representative pattern noise and extract representative features from average residual noise. Authentication or identification is done by inter-correlation between the fingerprint of the candidate sensor and the fingerprint of the reference sensor. Experimentation with nine different sensors highlighted good selections and showed robustness against classic attacks: JPEG compression, gamma correction, re-sampling and long-term stability.

This sensor fingerprint technology suffers from same security weaknesses against “copy attack” [7] as do some watermark algorithms. If anyone can create a sensor fingerprint from 50 images (according to the authors) taken by digital camera A, then an adversary can copy and paste the sensor fingerprint from camera A into a new image. A malicious adversary can also remove the sensor fingerprint from an image taken by camera A and paste a new sensor fingerprint from camera B into a new image. M. Kuhn, computer security researcher at Cambridge University, pointed out that manufacturers make efforts to reduce sensor noise. If the sensor noise is removed, is a sensor fingerprint still valid? Does the sensor fingerprint survive sophisticated image processing?

“The biggest potential application is in court,” said J. Fridich [19]. The FBI is currently evaluating this sensor fingerprint technology as an investigative tool [21]. According to B. Schneier it is “an investigative technique, but not as court-admissible evidence” [20].

The topic is promising but the technology needs improvement.

F. LEFEBVRE

Digital watermarking

In 1995, a breakthrough in digital watermarking led researchers to believe that this technology could be used to prevent unauthorized copying of multimedia works; to resolve ownership disputes; and to track unauthorized copies back to the source of the piracy and to distinguish authentic content from tampered content. When the Copy Protection Technical Working Group (CPTWG) started to consider using watermarking as part of a DVD copy management approach, the R&D community redoubled its efforts and a number of commercial efforts took root.

Applications of Watermarking

There are two flavors of watermarking technology. The first are “robust watermarks” designed to be recoverable even after the marked work has been subjected to processing (compression, filtering, even analog capture via camcorder or microphone). The other flavor, “fragile watermarks”, are designed with exactly the opposite goal: they become unrecoverable at the slightest modification of the marked work. Thus, they provide an indicator of processing. Most of the described applications use robust watermarking.

Watermarking can be used whenever someone wishes to attach metadata to a work so that it will not be removed during a change in format or when the work must travel through a legacy channel that does not support metadata. Below we give a short description of a number of applications. For more information about applications or watermarking technology in the standard book by Cox et al. [4] and in an overview book edited by Davoine and Pateux [5].

Two applications that drove early development of watermarking technology are *Owner Identification* and *Proof of Ownership*. These target content owners who would like to provide owner identification information to potential customers; search a database or network looking for content they own; or settle a dispute regarding the ownership of a digital work.

The application considered by CPTWG in 1995 was *Copy Control*. This application is still under consideration today by the DVD-CCA. Here the watermark provides a format independent channel for copy control information. This channel is designed to survive the D-A-D conversion and thus offers the ability to close the *analog hole*.

The application receiving the most attention in the literature today is *Forensic Tracking*. Here, the watermark carries information

about the legitimate path the work has taken. In other words, it indicates to whom the work was legitimately distributed. If a copy is redistributed contrary to the wishes of the content owner, the watermark provides forensic evidence to help the content owner understand and manage the problem. Recently, the Digital Cinema Initiative (DCI) proposed that digital cinema content be marked during exhibition with a location identifier and a time stamp. Recovery of this information from a pirated copy of the movie may help the content owners track down and stop camcorder piracy.

There are applications, particularly in surveillance, criminal justice, and insurance, where the authenticity of a work must be established. Cryptography offers hash functions and digital signatures that can be used to insure a work has not been altered. A signature, embedded directly into the work as a watermark, provides an authenticable work that then can be stored and transmitted on legacy devices and channels.

While all of the applications discussed so far relate to security, watermarking can also be used for non-security purposes. These applications require an extra communication channel within the context of legacy systems and networks. Before the watermarking age, design of composite video from B&W video and stereo FM from mono FM were responses to the same kind of situation. Recently, watermarking techniques were used to provide automatic audio/video synchronization (to resolve lip-sync error); to perform remote triggering for local advertisement; and to convey specific information for the deaf [1].

Watermarking technologies

There are a number of standard approaches to the watermarking of works of art (audio, still

(cont'd)

images, and moving pictures). All involve subtle changes to the sample values (pixel colors or audio samples). The changes are subtle enough to be imperceptible, yet give the work unique statistical properties detectable later. Combinations of changes can be used to encode a payload of metadata.

Two important aspects of watermarking technology are fidelity and robustness. Fidelity describes the imperceptibility of the watermark. A work marked with a high fidelity mark cannot be distinguished from the original unmarked work. The other, robustness, is the ability of the watermark to be recoverable after the watermarked work has been subjected to additional processing.

The most common technique is spread spectrum watermarking. The name comes from an analogy to spread spectrum communications. Each bit of payload data is spread over many samples. This is done by defining a reference sequence or pattern that has the same dimension as a frame of audio or imagery.

The reference pattern is designed to have very low amplitude and be uncorrelated with the samples of the audio or imagery. The low amplitude means it can be added to the work without introducing too much distortion. More advanced techniques use a perceptual model to attenuate the reference pattern in areas where it would introduce visible or audible artifacts and increase the reference pattern in areas where it is well masked. The low correlation with the work makes it easy to distinguish between works with the pattern and works without the pattern.

While this approach could be applied directly to the samples, it is often applied to other features (i.e., signals derived from the samples). Initially this approach was applied to a collection of DCT coefficients. It has also been applied to sets of block DCT coefficients, sets of wavelet coefficients, phase signals derived from audio clips,

luminance signals extracted from image sequences, and many other derived signals.

Rather than add a signal to the features, another common approach is to add a signal by manipulating the relationships between features. There are many different features used and numerous relationships. The choice of features and relationships will dictate the fidelity and robustness of the watermark.

An example of this kind of watermark is SysCop [12]. Here the features are block-DCT coefficients and the process of watermarking enforces a *greater than or less than* relationship. Pairs of coefficients are selected and the payload bit dictates which pairs should have greater amplitude. The marking process changes the coefficient values so that the desired relationships hold. A second example is the introduction of echo in an audio signal. The relationship that encodes the data is the time delay between the first appearance of a peak and the appearance of its echo. The delay time is always short enough that the echo cannot be heard.

Both spread spectrum watermarking and the approach of using relationships between features to represent data, introduced in the mid 1990's, form the basis of most current commercial offerings. However, new techniques are currently being developed in research labs. One approach based on quantization is receiving a great deal of research attention. Work is transformed into some feature space and those features are quantized. The data is represented by the choice of whether to round up to the next higher quantization level or to round down to the next lower quantization level. The claim is that this approach has the potential to offer significant improvements in fidelity and robustness.

(cont'd)

Last but not least, a comment about the security of watermarks. Different applications require different kinds of security. Authentication requires that an adversary is unable to embed a valid watermark. Copy control requires that the adversary is unable to remove the watermark. Forensic tracking requires that the adversary is unable to remove or change the watermark. As with most security technologies, watermarking requires serious key management.

J. BLOOM, P. NGUYEN

References

- [1] BAILLY G. et al. "ARTUS : calcul et tatouage audiovisuel des mouvements d'un personnage animé virtuel pour l'accessibilité d'émissions télévisuelles aux téléspectateurs sourds comprenant la Langue Française Parlée Complétée", Handicap'2006, Paris, June 2006
- [2] BITTAU A., HANDLEY M. and LACKEY J., The Final Nail in WEP's Coffin, in *Proceedings of IEEE Symposium on Security and Privacy 2006*, may 2006
- [3] BORISOV N., GOLDBERG I. WAGNER D., Intercepting Mobile Communications: The Insecurity of 802.11, in *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking (MOBICOM)*, July 2001.
- [4] COX I., MILLER M., and BLOOM J., Digital Watermarking: Principles & Practice, San Mateo, CA: Morgan Kaufman, 2001.
- [5] DAVOINE F., PATEUX S., Tatouage de Documents Audiovisuels Numériques, Hermes – Lavoisier, 2004.
- [6] FLUHRER S., MANTIN I. SHAMIR A., Weaknesses in the Key Scheduling Algorithm of RC4, *Lecture Notes in Computer Science*, vol. 2259: 1-24, 2001.
- [7] FRIES N., VOGT R., AYCOCK J., Timing is everything Computers and Security, vol. 24, No. 8
- [8] KUTTER M., VOLOSHYNOVSKIY S., HERRIGEL A., "The Watermark Copy Attack", *Electronic Imaging 2000, Security and Watermarking of Multimedia Content II*
- [9] LASICA J.D., Darknet Hollywood's war against the digital generation, Wiley, 2005
- [10] LUKAS J., FRIDRICH J., GOLJAN M., Determining digital image origin using sensor imperfections- in *Proceedings of SPIE*, 2005
- [11] STUBBLEFIELD A., IOANNIDIS J., RUBIN A., Using the Fluhrer, Mantin and Shamir Attack to Break WEP, In *Proceeding of the 9th Network and Distributed System Security Symposium (NDSS'02)*, 2002
- [12] ZHAO J., KOCH E., "Embedding robust labels into images for copyright protection", Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, August 1995
- [13] IEEE transactions on INFORMATION FORENSICS AND SECURITY, march 2006, Editorial.
- [14] http://news.zdnet.com/2036-2_22-6035707.html
- [15] www.star-force.com
- [16] <http://www.eff.org/corrupt/>
- [17] <http://www.ftc.gov/os/caselist/cv057013/cv057013.htm>
- [18] <http://www.glop.org/starforce/>
- [19] http://www.newscientisttech.com/article.ns?id=dn9046&feedId=online-news_rss20
- [20] http://www.schneier.com/blog/archives/2006/04/digital_cameras.html
- [21] http://www.technologyreview.com/read_article.aspx?id=16446&ch=infotech