

The security newsletter N°2

April 2006

Published Quarterly By
Thomson Corporate Research
part of the
Technology Division.

Editors:

Eric Diehl
Nicholas de Wolff

Contributors:

Jeffrey Bloom
Olivier Courtay
Alain Durand
Mohamed Karroumi
Frédéric Lefebvre
Nicolas Prigent
Dekun Zou

Corporate Research Head:

Patrick Baudelaire, Kumar Ramaswamy

SBU Technology Head:

Jean-Charles Hourcade, Willy Shih



Editorial

Welcome to the second edition of the Security Newsletter.

The proposed new version of the most recent General Public License (GPLv3) would ban any methods that might ensure software security. The clear objective is to prevent DRM from using GPLv3. Richard Stallman, the founder of the Free Software Foundation and co-author of the first draft of this license, claims that digital rights management “is a malicious feature and can never be tolerated, as DRM is fundamentally based on activities that cannot be done with free software.”

GPL currently rules many open source software programs such as Linux, MySQL, or gcc compiler. One of the potential consequences of adopting this new license would be that any platform implementing DRM could not use newer versions of Linux. Another consequence, as highlighted by Linus Torvalds, the creator of the Linux kernel, is that GPL software would be unable to properly employ cryptography, as it could not effectively hide the secret keys. Torvalds announced that he would not release newer Linux kernels under GPLv3. In any case, it seems that any bright future for Open Source DRM is growing increasingly dimmer. A hot debate is guaranteed...

This second issue of the Security Newsletter analyzes the promise of “new cryptography”, including high robustness and low cost, and discusses what its real impact may actually be. We also explore video fingerprinting, a technology that has many interesting applications, especially in content identification.

I hope that you will enjoy this second issue. We welcome your comments, questions and suggestions.

E. DIEHL

The news

DeAACS.com

Jon Lech Johansen, better known as “DVD Jon”, the author of the DeCSS program, announced early January on his blog [1] that he has registered the URL deaacs.com [2]. For the time being, deaacs.com is relatively light on content. A single sentence announces an estimated release date (namely winter 2006/2007). However, DVD Jon does not formally announce he will attack AACS [3]. AACS is the copy protection scheme of next generation DVD formats. DVD Jon has announced that he has not forgotten to register the relevant website, and is waiting eagerly for the first AACS products to be released.

This time, however, DVD Jon may well face several challenges. First, AACS security is far superior to CSS. For example, AACS allows single player revocation. Thus, the publication of a single key will not shut the whole system down. Second, even if DVD Jon manages to automate his attack to retrieve keys from many AACS instances, this program will work on only one single implementation from one single manufacturer. Other implementations will not be affected. Finally, DVD Jon will meet legal difficulties. He is now a US resident and thus subject to DMCA enforcement.

A. DURAND

Samsung & HDCP

Five studios are suing Samsung for developing and briefly selling at least one non-secured DVD model. Since February 2005, forums indicated that Samsung's HD841 could be easily dezoned and HDCP could be deactivated. An example easily found in a forum:

Press the ANGLE button
Press the numbers 4, 3, 2, 7
(You should see the message 'HDCP Free' appear in the upper left hand corner of your television screen)

Dezoning is not the real problem, however. Today, many DVD models can be dezoned. The main problem is HDCP deactivation. HDCP protects the DVI output. Thus, HDCP prevents digital copying of high-resolution images. Once HDCP has been deactivated, digital high-resolution content is freely available.

Studios probably want to give a strong message to manufacturers that they have to comply with the robustness rules. Their frustration is understandable. However, in publicizing this suit, and the underlying issues relating thereto, the studios may have also compounded their problems, at least in the short-term. Already hackers are identifying other models using the same core as the HD841. HD841 will soon become a highly prized collector's item...

E. DIEHL

TiVo® goes mobile

In January 2005, TiVo launched a new service called TiVoToGo™, which allows customers to transfer recordings from a TiVo Series2™ box to a computer or Windows Mobile-based Portable Media Center. Content is stored on the computer and requires a special code called a Media Access Key assigned to each user account for decryption and playback. Last November, TiVo announced plans to support Sony PSP and Apple iPod in the

TiVoToGo service. TiVo also announced its intention to use forensic watermarking technology to "enable tracking of the account from which a transferred program originated."

"If copyrighted programs show up on Internet file-sharing networks, entertainment companies, working with TiVo, will be able to use the watermark to identify the TiVo user from which it originated" (Wall Street Journal, Nov. 21, 2005). The details of the watermarking technology have not been released. Once deployed, this system will represent the largest real-world application of digital watermarking in video content copyright management. This is an indication that forensic watermarking has crossed a "maturity threshold".

Forensic watermarking serves as a complementary security feature to more traditional encryption-based Digital Rights Management or Conditional Access Management mechanisms. The encryption system provides the first level of protection, preventing unauthorized access to the content. However, if the incentives for unauthorized access are strong, there will be people eager to exploit any weaknesses in the implementation, protocol, or security infrastructure. In fact, there is already a tool available on the Internet that can extract a raw MPEG2 stream from an encrypted .tivo file. Once content is removed from its encryption envelope, DRM and CA systems can no longer control access. In this case, a digital watermark can provide another level of protection by working passively to provide forensic information and enabling the content owner to trace the pirate copy back to the source of leakage. Moreover, public knowledge that watermarking is used in this way can act as a deterrent to copyright infringement. It is expected that the use of watermark technology for forensic tracking will continue to grow.

D. ZOU, J. BLOOM

Security problems on Voice over IP

Voice over Internet protocol (VoIP) uses the existing Internet network for telephony. VoIP delivers, among other things, reduced telephone costs. Unfortunately, this transition brings some problems and more specifically security problems.

Users trust displays identifying the caller (caller ID). With standard phones, this trust is justified. The infrastructure is not shared with other applications and no one has access to the data. But, on the Internet network, third party access to this infrastructure (Internet) is relatively easy and VoIP protocol does not guarantee that the caller ID is the actual calling phone number. The problem has been known for a long time, but recently companies (e.g. www.spoofcard.com) started to develop business based on this problem. For a few dollars, anyone can select a CallerID alias to display during each call.

Changing one's Caller ID is legal. Nevertheless, this service can also be used for illegal activities. For example, Western Union uses Caller ID to authenticate the client before authorizing a wire transfer. A hacker can call Western Union with your Caller ID and authorize the cash transfer (this attack is often used on eBay).

Stuart Zipper disclosed another VoIP vulnerability. Communication billing uses a mechanism that requires an acknowledgment message confirming a connection with the correspondent. By blocking this message, the attacker has free calls. A possible lesson from this is that when porting an old service on an IP network, the security of the infrastructure should be extensively studied.

O. COURTAY

On the design of a low-cost cryptography

Recently Laszlo Kish, a physics professor from Texas A&M University, presented a scheme similar to "quantum cryptography" without the need for photon apparatus [6]. This security does not rely on mathematics but rather on physics engineering.

Both Alice and Bob have two resistors. Each one randomly chooses one of his/her resistors, and connects it to a circuit linking both resistors. The two resistors are in parallel, without any source of energy. Because these resistors are not null, current will nevertheless flow, due to thermal noise.

By measuring the current, anyone (Alice or Bob or an eavesdropper, Eve) can determine the total resistance of the circuit – A combination of the two resistance values. Alice knows her resistor's value, so she can extrapolate Bob's value (and vice versa). Eve just gets the combination of the two values and cannot guess Alice or Bob's values. Now Alice and Bob both know something that Eve does not, and that shared secret can be used to further secure communications. There are a few more steps involved in turning it into a communications system, but they are not critical. Note that with quantum cryptography, Eve would be discovered as soon as she sniffs bits. This is not the case here. Tery Bollinger's critique explains why it is not possible to detect (or keep out) Eve using classical physics [7].

This scheme would be extremely cheap. Indeed, only four resistances (few cents cost), a fast switch and a clock (a few dollars worth) would be required. Also, the key generation process is within the range of completely conventional PC abilities. When the paper was originally published, Bruce

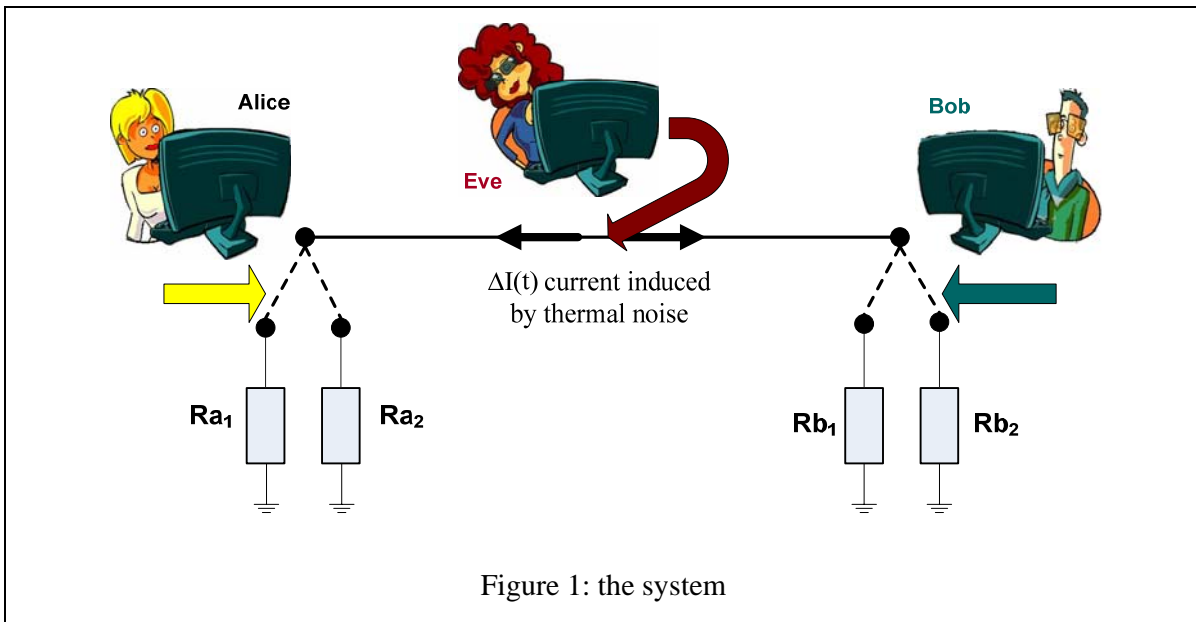


Figure 1: the system

Schneier of Counterpane Internet Security wondered, “How would you feel if you invested millions of dollars in quantum cryptography, and then learned that you could do the same thing with a few 25-cent Radio Shack components?” [8]. At the same time, journalists hastened to claim that it was a revolutionary system intended for people that cannot afford quantum technologies.

Is the scheme actually secure? In the paper, the author claims that it is absolutely secure, and answers an interesting key question: If Eve can find out the total resistance of the circuit, could she deduce which resistor is Alice and which one is Bob? His conclusion was no. Unfortunately, he was wrong. This scheme suffers from a lack of analysis of how attackers can use the physical laws of propagation. Two attacks were published on Bruce Schneier's blog site [9].

Attack 1: For Kish's scheme to work, both sides need to simultaneously change their resistance. This is not possible to achieve in practice. For instance, when Alice and Bob

connect their resistors, Alice may connect hers a few milliseconds before Bob. In that time, Eve can observe a glitch on the line from just Alice's end without Bob's contribution. She will thus know Alice's resistance value. In practice, end-to-end synchronization is challenging even if Bob and Alice had perfect timing, because Alice's information cannot go to Bob faster than the speed of light.

Attack 2: One assumption made in this paper is that there is only one measurement point (tap) on the wire. Let Eve have two taps with significant distance one from the other. Each tap records the resistance values using very small time-frames. Resistance difference leaves room for guessing resistor values. When comparing the two taps there will be a slight time delay in the changes of resistance at either tap. The time delay and its direction identify which is Bob's resistor and which is Alice's. So Eve can almost guess Alice and Bob's resistors values, with near perfect certitude.

These two attacks show that the system is not secure. The proposed scheme relies on

simplified assumptions that are wrong. The lessons are various. It is extremely difficult to design a secure scheme. Side channel attacks are devastating. Serious security requires multidisciplinary skills. However, Kish's scheme opens an interesting research field that may deliver cheap quantum-like cryptography one day. The media hype around this paper shows that the telecom and media entertainment industries have a real interest in such fields of research...

M. KARROUMI

Secure routing in ad hoc networks

Ad hoc networks are wireless networks of mobile devices that use no infrastructure to communicate. This technology allows easy opportunistic network deployment, even in uncontrolled areas. Ad hoc networks are currently used mainly for military and emergency rescue applications. Many new applications are foreseen such as easy network deployment in SOHO (Small Office/Home Office) and homes, and entertainment-related networking.

In ad hoc networks, two devices that are in each other's radio range communicate directly. If they are not within mutual range, they rely on other devices to forward their messages. This process is called routing, and follows the same principles as Internet routing. As devices are mobile, the communication path between two of them evolves organically. In other words, the devices that forward their messages will not always be the same. Consequently, routing information must be automatically updated when the topology of the network evolves. To that end, each device manages its own routing information in a fully distributed way. Each device exchanges routing information with its neighbors, such as what

other devices it can reach, the number of hops necessary to reach a given device, etc. Based on this information, each device computes and maintains its own routing table that provides the information required to transmit messages correctly to their destinations.

Attacks against routing intend to prevent messages from traveling correctly from source to destination by corrupting the routing information of legitimate nodes. Among other effects, attacks against routing can have the following practical objectives:

- Isolating a given node by preventing it from receiving any messages.
- Positioning the attacker's device on the path of all messages.
- Making devices consume more energy than necessary by using a longer path to transmit messages, possibly creating loops that may also prevent messages from reaching a destination at all.

The objective of security is to prevent an attacker from disrupting routing, which is the case when the following properties are ensured:

- If a path made of legitimate devices exists between two nodes, then these two nodes should be able to communicate.
- If there is a shorter path made of legitimate devices, then this one should be used.

In practice, attacks against routing use messages that provide wrong routing information. Simply said, the attacker lies.

Two kinds of lie exist:

- Lies about the device's identity, in which the attacker pretends to be a device it is not.
- Lies about the link, in which the attacker pretends to be in the radio range of a device while it is not, or to

have a shorter path to a given node than it actually has.

To combat identity lies, solutions apply authentication. Each device authenticates the routing messages that it sends. A device that receives a routing message first checks that it is legitimate.

To prevent links lies, solutions apply proofs of promiscuity. Device *A* collects proofs of promiscuity from all its neighbors. The proof of promiscuity issued by device *B* is a time-stamped certificate assessing that device *A* is in device *B*'s neighborhood. Device *A* later uses the received certificate in its routing messages to prove its proximity to device *B*.

Both security measures require distribution of keys to all the legitimate devices. Initial key distribution and trust management is currently the main outstanding problem. Indeed, most of the proposals of secure routing assume that all the initial keys have been previously correctly distributed. This hypothesis invalidates one of the main advantages of ad hoc networks: simple auto configuration. Moreover, most of the proposed key distributions only handle trusted devices and non-trusted devices. These key distribution schemes work in military and emergency applications, for which it is easy to differentiate friends from foes. These schemes are not suited to civilian entertainment applications, for which the separation between "well-behaved" and "badly-behaved" entities is not obvious.

In conclusion, routing protocols in ad hoc networks are at risk if not correctly secured. While solutions have been proposed to protect them, they all rely on key distribution schemes that are well suited to military and emergency-related applications,

but that do not fit civilian opportunistic networks deployment.

N.PRIGENT

Digital Fingerprints: designed to track and identify content.



Identifying content is often required in content security. Watermarking is one possible solution. It requires pre-release embedding. Often, this is not possible. The crudest identification method compares two contents bit by bit. In P2P networks, hash codes (MD5, SHA1...) identify versions of different bit streams. If one bit changes, the whole hash code changes. Thus, any content manipulation (legitimate or malicious), such as analog to digital conversion, compression, frame removal or addition generates a content detection failure for bit-to-bit comparison or hash code. Fingerprinting, insensitive to natural distortion, solves this issue. Fingerprinting design extracts discriminating characteristics, called fingerprints, from each piece of media content. It is often called multimedia DNA [11].

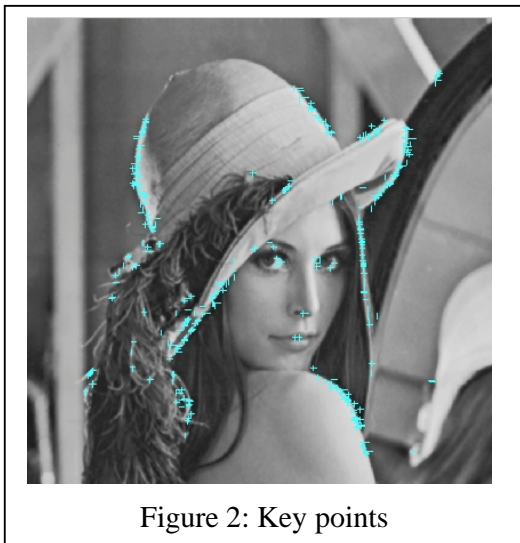
How does it work?

Fingerprinting techniques automatically extract representative, unique and relevant features from media content. There are two types of feature: semantic characteristics and non-semantic ones.

Semantic characteristics are high level. For instance, in soccer content: goals, penalties and corners are the main semantic features. In the sport context, semantic features are largely used to sum up a match. However,

semantic features suffer from some weaknesses such as non-universal interpretation or difficulty to compute.

Non-semantic characteristics are low level. They are usually based on signal analysis and the Human Perceptual System to be less sensitive to natural distortion. The fingerprinting system is divided in two processes: a detection process selects a set of key points (Figure 2), and a description process provides a strong, representative and compact description of the key points. In image context, the luminance distribution is usually used to characterize the whole image. The major drawback to this global approach is the lack of robustness against occlusion, incrustation (logo) or cropping. The solution is to characterize independent regions of the image with interesting features such as high contrast, edges, or corners [16].



Theory to practice: applications

Fingerprinting is largely used to search content in large multimedia databases [10]. In audio context, CDDDB [12] algorithm calculates a (nearly) unique disc identifier (ID). This disc ID is compared to a disc ID

database and the database search engine provides disc information such as artist, CD title... In freeCDDDB [12], the computation of the disc ID (fingerprint) is based on a CD's table of contents in minute second frame form. This technique is robust against compression, but not against track removal, track incrustation, concatenation of tracks, or voluntary attacks.

More recently, Philips proposed a new audio fingerprint system for automatic music recognition. The fingerprinting system [13] combines a fingerprint extraction algorithm and a fingerprint database. The fingerprint extraction algorithm segments the audio signal into frames. For each frame, a spectral representation is computed. These extracted representations are mapped into a more compact representation and characterize a sub-fingerprint. The set of all sub-fingerprints is the fingerprint of the audio signal. Contrary to the CDDDB process, this audio fingerprint recognizes music even if frames are removed or added. According to Philips, "a 3-second fingerprint on any piece of audio is sufficient to uniquely identify it, even if it is heavily degraded by compression or environment noise". Gracenote® integrates Philips' technology to propose a new Mobile MusicID™ service. The consumers can use their cellular phones to identify music playing on the radio or anywhere else.

Relatable® is another main actor. Their technology, TRM™, is also called Universal Barcode for Music. The audio extracted features are based on audio acoustical properties. MusicBrainz uses Relatable technology to offer services similar to CDDDB.

For the past few years, Microsoft [14] has been developing its own audio fingerprint technique, called RARE, to identify and

clean up duplicated audio files on a computer.

Fingerprinting is also a technical issue for the detection of illegal copies and streaming monitoring. Snocap (created by Shawn Fanning, Napster's developer), Audible Magic[®] and Advestigo filter music to manage and control the usage and payment of all music on file sharing networks.

In a video context, Advestigo's technology calculates sub-fingerprints to detect full pirated copies or a fragment of a pirated copy in P2P networks. The global identification scheme combines hash functions with digital fingerprinting to recognize and identify video content. The French INA monitors TV streams, using digital fingerprinting.

In a tracing context, fingerprint matching gives a model of distortion and can even provide the position of a camera in a projection room. This fingerprinting application is also called co-registration.

Conclusion and Perspective

Fingerprinting is an efficient solution to identify content, manage multimedia files in P2P networks, register two contents (detect the position of a camera in a theater), or detect malicious distortions such as frame deletion. Robustness is one of the weaknesses of fingerprinting. A new field of research, the perceptual hash [15] aims at solving this. Perceptual hash presents cryptosystem-like constraints (one-way property, fixed output bit length). A perceptual hash function computes a unique constant condensed version of the content, called perceptual digest. A small change in the content leads to a small change in the perceptual digest.

F. LEFEBVRE

(The opinions expressed in this newsletter do not necessarily reflect those of Thomson or its subsidiaries.)

References

- [1] <http://nanocrew.net/2006/01/08/deaacscom/>
- [2] deaacs.com
- [3] www.aacsla.com
- [4] http://www.technologyreview.com/TR/wtr_16484_323.p1.html
- [5] <http://www.accessintel.com/cgi-bin/press/show.cgi?1130972376>
- [6] L. Kish, "Totally Secure Classical Communication Utilizing Johnson (-like) Noise and Kirchoff.s Law", Arxiv preprint server, last revised September 19, 2005:
<http://arxiv.org/ftp/physics/papers/0509/0509136.pdf>
- [7] T. Bollinger, "On the Impossibility of Keeping Out Eavesdroppers Using Only Classical Physics," January 23, 2006:
<http://www.terrybollinger.com/genencrypt/BollingerCritiqueOfKishPaper-2006-01-31.pdf>
- [8] B. Schneier, "Hold the Photons!", Wired News, December 15, 2005:
<http://www.wired.com/news/privacy/0,1848,69841,00.html>
- [9] B. Schneier's weblog:
<http://www.schneier.com/blog/>
- [10] L. Amsaleg, P. Gros, S. Berrani, "Robust Object Recognition in Images and the Related Database Problems." Special issue of the Journal of Multimedia Tools and Applications, 23:221-235, 2004.
- [11] E. Batle, et al., "Recognition and analysis of audio for copyright protection : the RAA Project", Journal of the American society for information science and technology, 55(12):1084-1091,2004
- [12] <http://www.freecddb.org/>
- [13] J. Haitsma, T. Kalker, and J. Oostveen, "Robust Audio Hashing for Content Identification", Proc. of the Content-Based Multimedia Indexing, 2001.
- [14] Burges C. et al., "Using audio fingerprinting for duplicate detection and thumbnail generation", IEEE Conf. on Acoustics, Speech, and Signal Processing, 2005 Philadelphia, PA.
- [15] F. Lefebvre, "Message digests for Photographic Images and Video Contents", Thesis report, UCL, 2004
- [16] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints"