

The Security Newsletter

In this issue

The news	
- The fight on AACs continues	2
- Leaking mail	2
- Update on iPhone hacking	2
- Net neutrality?	2
- Shamir's new attacks	3
Understanding Sybil attacks	3
Forensic authentication of audio recordings	4
P2P: new threats for TV business?	5

INTRODUCTION to NEWSLETTER



We already knew that too demanding security led to less efficient security. People would try to bypass the too constraining security mechanisms, which would result in security holes. A typical case is the extremely constraining rules imposed to define strong passwords. Inevitably, it ends up with robust passwords written down on a post-it on top of the monitor.

We also knew that users do not accept security that is not user-friendly. People will try to find alternate solutions. This is one of the announced reasons for the refusal of digital rights managements (DRM). Current DRMs are not interoperable, thus some consumers may look for DRM-free content on illegal distribution channels, such as peer-to-peer networks.

Recent studies seem to indicate that too much security may also frighten people and may lead to less business. Since their inception, on-line banking services and e-commerce are under the fire of attackers. Many techniques have been designed to steal account passwords



and credit card numbers: key loggers, phishing sites, etc. The banking industry has escalated its answers with more and more elaborated solutions such as one time credit card numbers (also called number fobs), dedicated card readers, and visual authentication. Increased complexity of security mechanisms highlights the feeling that online banking is dangerous and requires caution. This feeling may lead to people fearing and terminating this type of service.

Once more, we see that security is a complex trade-off between efficiency and user friendliness. The user is at the center of this delicate balance. Good security has to take the human factor into account.

Best wishes for a prosperous 2008!

Published Quarterly By:

Thomson Corporate Research
Part of the: **Technology Division**

Technical Editor:

Eric Diehl

Editors:

Gary Donnan
Natalie Hamrick
Sharon Ayalde

Contributors:

Patrice Auffret
Peter Baum
Eric Diehl
Oliver Heen
Mohamed Karroumi
Michel Morvan
Stephane Onno

SBU Technology Head:

Jean-Charles Hourcade

Mail and to subscribe:

security.newsletter@thomson.net

Copyright Thomson 2007

The News

The fight on AACS continues

In early October, two released Blu-ray titles¹ encountered playback problems. Customers complained that their Blu-ray players (Samsung BDP-1200 and LG BH100) were not able to play back these titles. Manufacturers announced the issue and began working on firmware updates.

Could these problems come from the use of BD+ copy protection [3]? These discs hold a folder named "BDSVM", where "SVM" stands for Secure Virtual Machine. BD+ relies on the use of a SVM. Furthermore, the two discs use a more recent version of the Processing Keys (master keys in AACS), denoted by MKBv4 [9].

By the end of October, SlySoft released - much sooner than expected - the latest version of its popular ripping tool called AnyDVD HD, that defeats MKBv4 [10]. This was verified on the latest HD DVD releases using MKBv4 (but not using BD+). However, the last AnyDVD HD version does not have the ability to duplicate the newest Blu-ray discs. BD+ seems to be effective. James Wong, development chief at SlySoft said: "We already found a way to crack BD+ and we have just turned to fine-tuning." According to him, a release circumventing BD+ is expected by the end of this year. Let's wait and see.

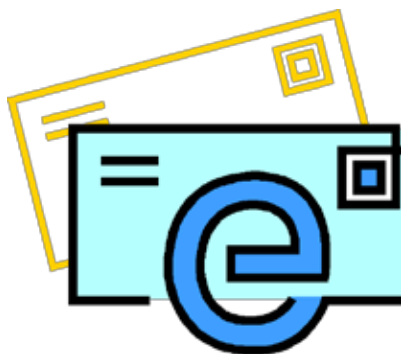
> M. KARROUMI

¹"Fantastic Four: Rise of the Silver Surfer" and "Day After Tomorrow"

Leaking mail

On September 15th, an archive of over 6,500 emails were spreading on BitTorrent. The archive belonged to MediaDefender [1]. MediaDefender is a company specialized in spoofing and decoying P2P networks.

This archive [2] revealed their decoying tactics and commercial practices. More interestingly, the archive acknowledged an old rumor. MediaDefender operated "miiwi", a site proposing fast downloads of copyrighted material. The decoys were redirecting towards this "honey pot" site.



MediaDefender attempted to stop the dissemination of this archive file by sending takedown notices to P2P sites without any success. Two days later, a phone conversation between MediaDefender and their attorney leaked. They used VoIP.

On September 24th, using the content of this archive, the Pirate Bay, a large P2P tracker site, filed legal complaints versus ten major media companies for sabotage.

This leak seems to have already cost MediaDefender \$825,000. The lesson for all: protect your email.

> E. DIEHL

Update on iPhone hacking

In the previous issue, we described evidence of the first software-based unlock of iPhones™. Meanwhile, on September 27th, Apple issued version 1.1.1 of its firmware. Unfortunately, unlocking hacks were updated with success by the hacking community ("TurboSIM" duplicates the SIM card; "SIMfree" modifies the Seczone memory image; "anySIM" modifies the baseband).



On November 8th, Firmware v1.1.2 patched flaws exploited by hackers (known as TIFF exploit). Hackers succeeded in upgrading the unlocked iPhone from v1.1.1 to v1.1.2. Since mid-November, Apple has proposed, for both the US and Europe markets, iPhones based on new bootloader (v4.6). This version defeats main software unlockers and

only the TurboSIM hardware solution seems to have the ability to resist.

Apple estimates that about 250,000 iPhones (17%) were sold for the purposes of unlocking. With such manipulations, people take the risk to make their iPhone useless with firmware updates.

> M. MORVAN

Net neutrality?

In August, TorrentFreak, a weblog bringing the latest news about BitTorrent, reported that Comcast, a major U.S. Internet Service Provider (ISP) has throttled BitTorrent downloads and uploads connections. Comcast is using a packet shaping application from the broadband management company Sandvine. Comcast sends a reset (RST) packet to the Comcast customer, impersonating the host at the end of the BitTorrent connection. This impersonation is illegal in many states.



Comcast still denies hampering the BitTorrent data flow. Last month, many customers sued Comcast for not being net neutral. They asked the Federal Communications

Commission to ensure that Comcast stop interfering with file

sharing. Some Comcast users reported that running BitTorrent with header encryption or encrypted tunnels such as SSH or VPN might eliminate the problems. BitTorrent is estimated to account for at least 30% of Internet traffic. Reducing BitTorrent traffic would save the bandwidth bill. Should ISPs continue to observe this pitfall or should they interfere with the net neutrality principle?

> S. ONNO

Shamir's new attacks

The C&ESAR 2007 conference was held on November 6, 7 and 8 in France. The subject "Cryptography: new stakes, new challenges" drew 200 participants from all over the world. Many hot topics of modern cryptography were debated including: security of hash functions, quantum cryptography, some attacks against content protection systems and credit card security.



During his keynote speech, Professor Adi Shamir (the S of RSA) disclosed new side channel attacks:

- One attack against RSA/CRT involves a carefully crafted entry containing positive and negative parts. Power analysis detects the use of multiply rather than square operation, which, in turn, reveals many secret bits.
- One so called "lunch attack" uses the USB port of a Personal Computer instead of an oscilloscope for power analysis.
- One "bug attack" against RSA assumes that a microprocessor fails the $x*y$ multiplication for some specific values of x and y . Shamir demonstrated how to craft an entry, based on x and y , whose encrypted value eventually reveals the secret key. The failure may be a design error or a malicious design decision.

> O. HEEN

Understanding Sybil attacks

A Sybil attack may exist as soon as a system, or a network, relies on identities to provide some functionality. Such systems are extremely common:

- Web ranking services like the one used by Google™.
- Voting and reputation systems like the one used by e-Bay™.
- Social networks like LinkedIn™, Viadeo™, MySpace™...
- Anonymizing networks, Peer-to-Peer networks and even online games.

Pr. J. Douceur from Microsoft Research first described the Sybil attack in 2002 [10]. Since then, more than 100 papers were published [15]. The idea is to simulate many identities for gaining more prescription power within the system. Just imagine thousands of fake identities voting for you! The Sybil attack is in

fact a generalization of the ID spoofing attack. The name Sybil comes from of a woman suffering multiple personality disorders [5].



To understand the transposition to computer science, we must define the concepts of entity and identity. An entity is a physical principal like a human or a computer. An identity is an informal abstraction of an entity, like a string or an IP address. As soon as one entity can acquire multiple identities, there is potential for a Sybil attack. Thus, in a Sybil attack, an entity uses many identities to gain some benefits. The attacked system assumes that each identity is linked to a different entity.

Some reputation functions are inherently vulnerable to Sybil attacks. For instance, CHENG [11] exhibited a formal construction of a Sybil attack against reputation functions (that are invariant under a renaming of the nodes in the function graph). In practice, only a few defense mechanisms will be genuinely efficient.

Some possible consequences

Search engines often use reputation systems for evaluating the popularity of web pages. For instance, with Google's PageRank, a hyperlink between pages counts as a vote. The higher the reputation of the linking page, the stronger the vote for the linked page. By creating multiple pages and judiciously setting hyperlinks, one can intensively vote for a page and thus raise its popularity. A famous example happened in 2003: the result for the search of "Miserable Failure" in Google was – erroneously – a page with the biography of George W. Bush.



A first defense mechanism involves a central authority. This authority knows all registered entities in the system, and can make the correlation with all identities. This solution works well, but brings a single point of failure, fragile against denial of service attacks.

Another mechanism is to challenge identities, to check if they represent the same entity. Pr. J. Douceur studied the case of challenging resources like computational power, storage capacity, or bandwidth. For example, one can send a computational challenge to a remote identity and measure how long it takes to solve it. Another identity may not solve the same challenge exactly in the same time. Thus, when two different identities

solve the challenge in exactly the same time, this might be an evidence of a Sybil attack. This solution brings the problem of measurement uncertainty.



One general defense is to raise the cost of creating identities so that it would be unaffordable for an attacker to launch an efficient attack. This will not avoid an entity to create multiple identities, but will severely limit the number.

Unfortunately, raising the cost of acquiring an identity may cause users not to make use of the system. This is particularly a problem in P2P networks, where a large number of users are required to be efficient.

On large P2P networks, the combination of using a central authority and a high cost on creating an identity may be a winning combination. This will not stop an attacker to write a Trojan horse for taking control of the user's computer, and thus its identity. Proper defense is still an open research topic.

> P. AUFFRET, O. HEEN

Forensic authentication of audio recordings

Introduction

The ultimate goal of forensic authentication of audio recordings is to provide evidence that can be presented to the court in civil or criminal cases. Possible questions, for example, are: Has the recording been edited? Is the recording a concatenation of multiple recordings? Have parts of the original recording been removed? When has the recording been done? Where has it been done? Grigoras proposed a methodology based on the electric network frequency, which might answer all these questions [12].

The electric network frequency

The utility frequency is the frequency at which alternating current is transmitted from a power plant to the end user. It is 60 Hz in most parts of America and 50 Hz in most parts of the rest of the world. Many countries share different networks to provide a reliable power supply. The electric network frequency (ENF) is not constant [4], but varies over time (Figure 1). This variation is due to time varying power consumption and production. It is the same for the whole network. A variation of plus or minus 50 mHz is considered normal. The electronic network is regarded as impaired without major risks if the variations are between 50 and 150 mHz. Above this limit, serious countermeasures prevent a collapse of the system.



Figure 1: Variation of the electric network frequency over time [7]

The ENF variation does not follow any predictable pattern and is therefore purely random [12], [7]. This means that a specific recording of some seconds length of the network frequency defines unambiguously the time and date at which the recording was done. With a granularity of an electric network even the location can be determined. It is, for example, possible to distinguish recordings made in Dublin, London, Paris and Stockholm, since all belong to different electric networks. The same is true for the US, where different networks are applied as well.

Authentication using ENF

This theoretical knowledge becomes practically relevant, since electromagnetic fields oscillating exactly with the ENF surround all AC-powered lines or devices. These fields are captured by standard audio devices, leaving a (usually unwanted) 50 Hz (or 60 Hz) "hum" signal in the recording. This is even the case if the recording device is battery powered, but not too distant from a power line [7].

With this methodology, Grigoras proved in court that a recording of two speakers A and B, did not take place at the date claimed by speaker A, but at the date claimed by speaker B. Furthermore, he convinced the court that the recording had been edited (i.e. words and expressions were removed), which was indicated by several major discontinuities of the ENF trace [13]. With the same principle, it is also possible to detect whether a recording is a mix of several recordings made at different dates, since the mixed

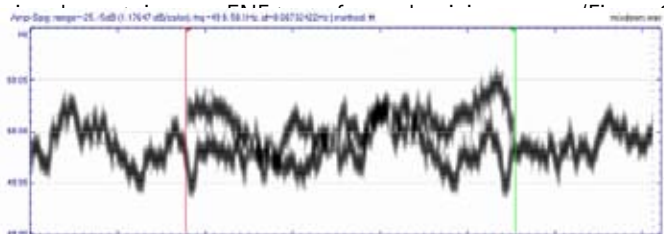


Figure 2: Two recordings partly mixed together [7]

Summary

The electric network frequency methodology allows forensic authentication of audio recordings. It permits the determination of the date and time of the recording, detects editing points and, to a certain extent, the location and where the recording was conducted. This can be interesting for the Media and Entertainment Industry, not only in the area of forensic tracking or of pirated copies, but also, for example, to uncover fake news recording.

> P. BAUM

P2P: New threats for TV business?

Introduction

For a decade, Peer-to-Peer (P2P) systems have been employed for a variety of applications such as file-sharing and VoIP. Recent deployment of P2P TV application proves that P2P could also address live streaming. P2P TV is an Internet TV-based application that enables live content distribution from anywhere, to anyone, at any time.

Watching P2P live TV is fast and straightforward. First, the user installs a P2P live TV application, for instance, Sopcast or Tvants. Then, the user browses the worldwide "electronic program guide" portals that propose related TV schedules. One example is www.myp2p.eu - this proposes all kind of sports. When a user clicks on such dedicated URLs (i.e. respectively `sop://..` or `Tvants://`), the application recognizes the format of the stream and invokes the right player application. After 40 seconds, the video is visible with a playback lag of about three minutes. The average streaming rate is between 300 and 400 Kbit/s for Sopcast. On a standard residential connection, we observed video at about 750 Kbit/s with Tvants. The video quality was good enough to be displayed in a full screen mode.

Technical overview and challenge

The P2P streaming application is a mesh-pull based Internet overlay based on BitTorrent protocol. The P2P application uses a tracker server that provides streaming channels and peer and chunk information for each peer node of the network. A channel stream server converts the media content into small chunks of video. All the peers cooperatively exchange chunks of data among themselves via their streaming engine. A streaming engine, depicted in Figure 3, downloads video chunks from other peer nodes or from the channel-streaming server. The key element is the buffer map that indicates the available data chunks. The streaming server reassembles chunks into the original media content and streams them to the media player.

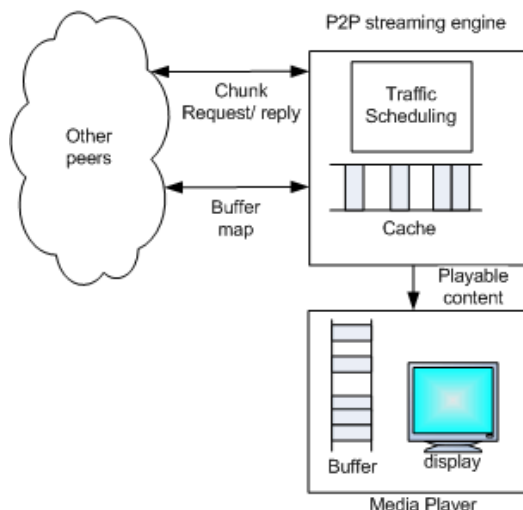


Figure 3: Streaming engine overview [14]

P2P live TV faces many new challenges compared to traditional P2P. Large scale deployment involves thousands of users simultaneously connected. Performance requires high bandwidth expectations. Real-time constraints require timely and continuously streaming delivery. Thus, data chunks have a limited lifetime. On the other hand, the more important the event, hence, valuable and attractive, the higher the quality, thanks to the P2P mass effect.

New TV experience for users

Other than the convenience, the P2P application offers additional benefits. Anyone with a broadband connection could access virtually any TV channel. There are no more geographical constraints. An end-user could also generate live content for a worldwide attendance. Channels could be user-centric and could target small audiences. However, these benefits also create new threats, especially for copyright issues.

Security concerns

P2P live TV is more vulnerable to "Denial Of Services" attacks than traditional file-sharing P2P. Attacks on content, such as impersonation or defacing (i.e. one content is replaced by a fake one), could also occur. No such attacks have yet been reported.

The rebroadcast threat

Like normal P2P, the P2P live TV technology is not evil. However, some uses may be illegal. The major threat is illegal rebroadcast. Two types exist: Free-to-air and Pay-TV.

Content owners grant local rights to Free-to-air broadcasters. However, P2P live TV also enables receiving such local channel everywhere, thus infringing the granted rights. For the Pay-TV case, while malicious users watch live content on his set-top box or computer, he captures and rebroadcasts the clear content. Most of the Pay-TV channels are available in the clear on P2P live TV (at least for major live events).

Implementing watermarking technology inside the player may prevent the latter threat. The watermark would identify the subscriber. Thus, it is possible to trace back to the infringer and, for instance, terminate his subscription. This assumes that the Pay-TV system is not hacked.

This solution is less efficient for Free-to-air channels. There is no subscription and back tracing may be difficult. In this case, IP addresses of the main source of illegal re-broadcasting content could be detected. Tackling this former threat is much more challenging. In any case, these threats are serious and already exist. We were able to view most of the Free-to-air and Pay-TV channels through P2P live TV with reasonable quality.

Impact on the TV business

"Open" overlay networking: P2P live TV application takes advantage of ISP's infrastructure to spread live content over the world without paying a fee. It could harm traditional broadcast

and broadband TV business. Will Internet service providers remain neutral regarding these issues (see Net neutrality? in this issue)?

The “broadcast perimeter” has vanished: Until recently, a dedicated network could be perceived as a “broadcast perimeter protection.” This protection is gone. Content owners will have to reconsider the problem.

Prosumer trends: P2P live TV application brings the same breakthrough for live content as YouTube did for downloading content. Broadcasters may lose the tight control on what consumers watch. Users will create their own personal TV channels with all the associate copyright issues.

Conclusion

P2P live TV application may be a killing application. It enables a shift from regular broadcast TV to IP-based TV, which allows more flexibility and interactivity. P2P live TV is for live content on what file-sharing P2P is for pre-recorded content. Unless regulations or ISP measures are taken, users will be able to watch illegal and free live TV. A new deal on the current TV business is ongoing. New countermeasures are also set to be designed and implemented.



> S. ONNO

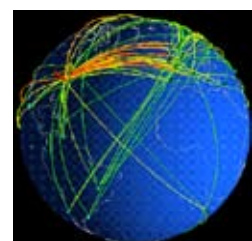
Where will we be?

Security, Forensics, Steganography, and Watermarking of Multimedia Contents X ([IS&T/SPIE Electronic Imaging 2008](#)), San Jose, California, USA, January 27-31, 2008

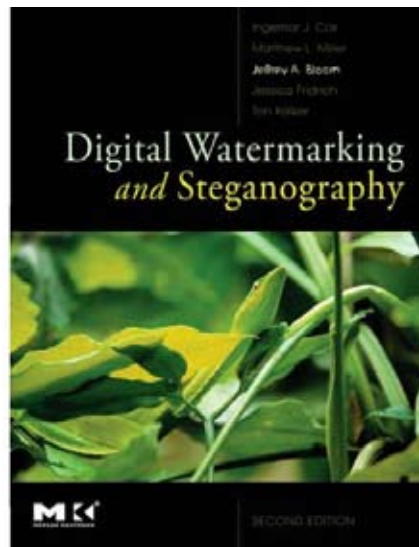
Paper presentation: In-theater piracy: Finding where the pirate was, by Bertrand Chupeau

Third International Conference on Availability, Reliability and Security ([ARES 2008](#)), Barcelona , Spain, March 4-7, 2008

Paper presentation: A federated physical and logical access control enforcement model, by Stéphane Onno



Authors



The second edition of this popular book was published by Morgan Kaufmann this November. As has been the case with the first edition, it is expected that this book will be widely used in both academia and industry. Thomson's Jeffrey Bloom and his co-authors have updated many of the chapters to reflect recent developments in the field. The highly

related field of steganography has been added to the book with the two new chapters dedicated to the topic and other chapters updated. In addition, the topic of informed watermarking has been expanded to two chapters with an emphasis on dirty paper coding. This book presents the fundamental principles underlying all modern digital watermarking and steganography technologies.

Strengthening hardware AES implementations against fault attacks

Marc Joye, Pascal Manet, and Jean-Baptiste Rigaud in *IET Information Security* 1(3):106-110, 2007

References

- [1] <http://www.mediadefender.com/>
- [2] <http://www.mediadefender-defenders.com/>
- [3] <http://forum.slysoft.com/showthread.php?t=8982>
- [4] <http://www.ucte.org>
- [5] http://en.wikipedia.org/wiki/Sybil_%28book%29
- [6] BLOOM J., SPDC forensic stream marking, in The Security Newsletter, Issue 7, fall 2007, THOMSON
- [7] BRIXEN B., Techniques for the Authentication of Digital Audio Recordings, Presented at the AES 122nd Convention, Vienna 2007
- [8] BRIXEN B., Further Investigation into the ENF Criterion for Forensic Authentication. Presented at the AES 123rd Convention, New York 2007
- [9] COURTAY O., KARROUMI M., AACs under fire, in The Security Newsletter, Issue 4, spring 2007, THOMSON
- [10] DOUCEUR J., The Sybil Attack, Microsoft Research, 2002 at <http://www.cs.rice.edu/Conferences/IPTPS02/101.pdf>
- [11] CHENG A., FRIEDMAN E., Sybil proof Reputation Mechanisms, Cornell University at <http://www.sigcomm.org/sigcomm2005/paper-CheFri.pdf>
- [12] GRIGORAS C., Forensic analysis of digital recordings – The Electric Network Frequency Criterion. Forensic Science International, 136 (Supp. 1), (2003)
- [13] GRIGORAS C., Applications of ENF Analysis Method in Forensic Authentication of Digital Audio and Video Recordings. Presented at the AES 123rd Convention, New York 2007
- [14] HEI X. et al., A Measurement Study of a Large-Scale P2P IPTV System IEEE Transactions on Multimedia, Volume 9, Issue 8, Dec. 2007
- [15] LEVINE B., SHIELDS C., MARGOLIN N., A Survey of Solutions to the Sybil Attack at <http://prisms.cs.umass.edu/brian/pubs/levine.sybil.tr.2006.pdf>





Contact us to join our newsletter mailing list:
security.newsletter@thomson.net