



**THOMSON**

# The security newsletter N°1

December 2005/January 2006

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

**Editor:**  
Eric Diehl

**Contributors:**  
A Durand  
O Heen  
S. Lelievre  
O. Courtay  
C. Salmon LeGagneur

**Editorial Advisor:**  
Nicholas de Wolff

**SBU Technology Head:**  
Jean-Charles Hourcade, Willy Shih

**Corporate Research Head:**  
Patrick Baudelaire, Kumar Ramaswamy

## Editorial

Welcome to the first edition of the Security Newsletter. This quarterly newsletter will provide you with analysis from the experts in THOMSON Security Laboratories on the latest developments in the field of security. The newsletter will mainly focus on content protection, and infrastructure protection.

Each quarter, THOMSON Security Laboratories will explore the latest industry goings-on, extracting the most relevant news, and presenting short articles thereon. Each issue will also feature a more in-depth article that will either examine a special event in detail, or present a specific technology. The objectives will always be to be educational, and to separate practical information from “buzz”.

This quarter’s event is of course Sony BMG’s rootkit misadventure. We will explain what a rootkit is, describe the system in question, and highlight the unforeseen consequences. The main lesson of this disaster may be that content protection designers have to act ethically. A “sine qua none” condition for consumers to accept content protection is the respect of such fundamental rights as privacy, and ownership. It would be unforgivable if the content protection community fell prey to the same pitfalls as the IT security industry, with the gray borders of ethical hacking.

This first issue also demystifies the latest progress in cryptanalysis. Numerous attacks and exploits have been disclosed. What does it mean for actual applications? Are we in danger?

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

*Eric DIEHL*

## The news

### Improved attack on SHA-1

Last summer, at the “CRYPTO 2005” conference, XIAOYUN Wang, the Chinese researcher who first cracked SHA-1 [5] announced that she improved the performance of her previous attack [6]. The break consists in finding a collision (two different messages with the same hash). Hash functions, like SHA-1, are designed to make it computationally difficult to find such collisions. The previous attack generated a collision after  $2^{69}$  computation steps (instead of  $2^{80}$  for a brute force attack). The new attack requires only  $2^{63}$  steps. It is 64 times faster than the previous one. The attack now becomes feasible. We expect some teams to cooperate to exhibit the first collision on SHA-1 within the next few months. The demonstration of such collision will not be a disaster. The required computation power is still too high to endanger current applications. They can still be seen as safe for the next few years. These attacks show however that SHA-1 no longer offers a good security margin. It is highly recommended, for future developments, to use more robust hash functions (e.g. SHA-256). NIST has actually published a note [7] announcing that they would phase out SHA-1 by 2010.

*A. DURAND*

### French Parliament to vote the “DADVSI”

France is one of the last European Union countries that have not yet transcribed the EU CD (European Union Copyright Directive, equivalent to American Digital Millennium Copyright Act) into its national law. The French Parliament will review by



20<sup>th</sup> and 21<sup>st</sup> of December 2005 the DADVSI (“Droits d’Auteur et Droits Voisins dans la Société de l’Information”, copyright and neighboring rights in the information society bill). The project includes the following measures: prohibition of circumventing techniques (creation, detention, usage, selling, advertising – status of research publication is unclear), including encryption and watermarking, exception for private copy ... We will report on the final text in our next edition!

A. DURAND

## The End of Anonymous Surfing?

Attacking a computer via the Internet often starts with *information gathering*. Many techniques already exist: operating system fingerprinting, port scanning, banner grabbing... The ultimate goal is to obtain unique characteristics of the computer: a kind of *physical fingerprinting*. Accurate enough, this would allow detection of one specific computer among other Internet computers. Physical fingerprint has legitimate usage, but may also be used for “malware”. Malicious applications are numerous: recognition of web clients by servers (literally the end of anonymous surfing), tracking of a specific computer despite IP address and location change (so long to privacy), early detection of honeynets...

Kohno et al. [3] recently published a realistic physical fingerprinting method. It is close to the operating system fingerprinting method previously co-published by Thomson Security Lab and France Télécom Security Lab [1]. The idea is based on the following observation: no two-computer clocks are the same; no two clocks have exactly the same *time skews*. The most innovative part lies in the way clock skews are measured: through the Internet, using

very common protocols, TCP and ICMP, and generally without target awareness.

### How does it work?

One easy application of this technique is when a web server physically fingerprints its clients. For each received TCP message, the server records the reception times and TCP Timestamps (RFC 1323). Once it has collected sufficient data, it computes the average deviation between both series. This is a good approximation of the time skew. Then, if a fingerprinted computer comes back to the server even from another location, its time skew will be recognized as soon as the server has received enough packets.

O. HEEN



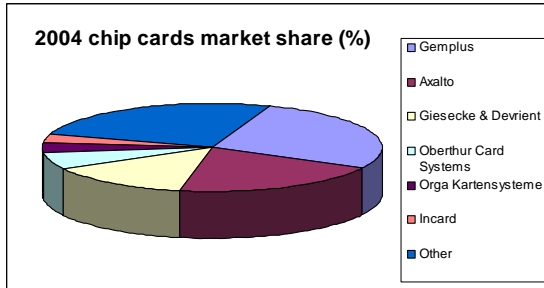
## GEMPLUS + AXALTO = GEMALTO

After many months of rumor and gossip, the news is confirmed: the two leading smart card manufacturers, Gemplus and Axalto will merge to form [Gemalto](#). A giant in the smart card industry is born! [8]

Gemplus is a leading provider of smart card enabled technologies, products and services for secured wireless communications and transactions. Gemplus is active in the telecommunications, financial and security service sectors.

Axalto is a card manufacturer and a major supplier of point-of-sale terminals. Axalto is active in the telecommunications, finance, retail, transport, entertainment, healthcare, personal identification, information

technology, and public sector markets. Axalto is the former smart card division of Schlumberger. It spun off from the group in 2004.



With respectively 27% and 20% market share, Gemplus and Axalto dominate the smart card market. This market is mainly driven by the telecom sector (SIM cards for mobile phone). However, the banking, identity and security markets are clearly emerging. The EMV migration for banking cards, the deployment of e-passport or the development of national ID card projects are considerable growth opportunities.

Cards shipment (Millions of units - Mu)		
	Memory card	Microprocessor cards
Telecom	244	605
Financial Services, Retail, Loyalty	12	158
Government, Healthcare	7	21
Transport	32	12
Pay TV	0	22
Corporate security	10	7
Others	5	6
<b>Total</b>	<b>310</b>	<b>831</b>
<b>Total First Semester 2005</b>	<b>1141</b>	

The new entity will be composed of 11,000 employees in 65 countries. It will represent almost 50% of the market share (between 35% and 40% for the banking cards and

SIM cards) and should be able to face increasing competition from Asian manufacturers with renewed confidence.

Some analysts predict that this merger will dwarf the other players in the smart card industry. Smaller players may become a target for companies looking to enlarge their smart card operations.

The new entity is being presented as a "Global leader in Digital Security". It may become a key partner in the development of many future projects. Content security is one of the new markets that Gemalto is eager to address.

S. LELIEVRE

## New records in computations over large numbers

Since May 2005, two records of RSA modulus factorization and four records of discrete logarithms computations (respectively) have been announced.

The problems of integer factorization (on which RSA relies) and discrete logarithm computation (on which rely DIFFIE-HELLMAN or DSA) are the foundations of modern asymmetric cryptography. Such cryptosystems are based on large numbers and can thus use variable key size. In today's applications, the current selected size for both types of algorithms is 1024 bits. When RIVEST, SHAMIR and ADLEMAN first presented RSA in 1978, they recommended to use a size of 320 bits for the modulus. Factorization performances have since constantly been improved, as shown in the table on the following page [9].



number	digits	bits	date
RSA-100	100	333	Apr. 1991
RSA-110	110	366	Apr. 1992
RSA-120	120	399	Jun. 1993
RSA-129	129	429	Apr. 1994
RSA-130	130	432	Apr. 10, 1996
RSA-140	140	466	Feb. 2, 1999
RSA-155	155	515	Aug. 22, 1999
RSA-160	160	532	Apr. 1, 2003
RSA-576	174	576	Dec. 3, 2003
RSA-150	150	499	Apr. 16, 2004
RSA-200	200	665	May 9, 2005
RSA-640	193	640	Nov. 4, 2005
RSA-704	212	704	open
RSA-768	232	768	open
RSA-896	270	896	open
RSA-1024	309	1024	open
RSA-1536	463	1536	open
RSA-2048	617	2048	open

The above table shows that the progression has been of 300 bits within 15 years. This could be interpreted in (at least) two ways: If you are optimistic and you bet that the progression will stay roughly linear, then in 2020, the record will be roughly 970 bits. This means 1024-bit keys will be secure till roughly 2015. If you take a more pessimistic view (the default POV here at Security Laboratories), and you consider that the modulus size doubled in 15 years, then 1024-bit modulus would be factorized around 2014. In that case, it would be safer not to use 1024-bit keys after 2010.

Techniques used to compute discrete logarithms are similar to those used to factor integers. However, there is a difference between records for discrete logarithms computation and integer factorization as shown in the next table:

Field	digits	bits	date
GF(p), p prime With 130 digits	130	432	Jun. 18, 2005
GF(2 <sup>613</sup> )	185	613	Sep. 22, 2005
GF(65537 <sup>25</sup> )	121	401	Oct. 24, 2005
GF(370801 <sup>30</sup> )	168	556	Nov. 9, 2005

This table teaches us several facts: First, it is easier to compute discrete logarithms over GF(2<sup>m</sup>) than over other GF(p<sup>m</sup>) (with m greater than 1 and p prime greater than 2) that are themselves easier to compute than the ones over GF(p) (with p a large prime). Although calculus are more efficient over GF(2<sup>m</sup>), one should prefer GF(p) as a base field when using a cryptosystem based on the discrete logarithm problem.

Second, there is a huge difference between records in integer factorization and discrete logarithms computations. At least three explanations exist. First, as asymmetric cryptography based on discrete logarithms is less deployed than systems based on RSA, it remains of less interest to researchers. Antoine JOUX, the researcher responsible for the 4 records (together with Reynald LERCIER), publicly declared that he restarted computing discrete logarithms because the gap with RSA had grown too wide (previous record was made in 2001!). Second, less computation power is dedicated to break discrete logarithm records than integer factorization records. Finally, one step of the discrete logarithm makes the global complexity of the calculus higher than the one of integer factorization. This difference is usually estimated at roughly 80 bits. This means that, deploying the same computation power as RSA, one would probably be able to compute discrete logarithms over GF(p) with a p of 580 bits. This slight difference of complexity does not justify however using smaller key size with cryptosystems than for RSA, based on discrete logarithm problem.

A. DURAND



## Sony's twisted path toward copy-protection

Bruce SCHNEIER once said "digital files cannot be made uncopyable, anymore than water can be made not wet" [4]. Current PCs do not provide a trusted environment, thus copy protection is not inherent to PCs. Sony's arduous experience shows that it is a complex and difficult task with many trade-offs.

November 2005, Sony BMG sold 2 million music CDs (around 50 titles) embedded with a controversial copy protection system, called Extended Copy Protection, or XCP (see box). Like many other existing solutions, XCP requires playback of content using a provided media player. For that purpose, XCP installs a permanent hidden driver on the host PC. The stealthy ability of this driver contributes to the self-protection of the whole copy protection system. The user, ignorant of the driver, should not be able to remove XCP.

XCP software is intrusive. To remain hidden to the user, and intercept copy requests or play back actions from the user, the software needs a rootkit (see box) to be installed on the PC. Rootkits evolved from piracy techniques used by malware writers. They alter the core operating system, degrade performance and raise instability. According to malware experts, XCP may also act as a spyware application, by contacting online sites during a playback sequence (which may lead to user privacy issues).

Sony BMG, to counter piracy, employed the bad techniques of pirates, like cloaking, rootkits, and spywares. In the same spirit, EULA did not mention that XCP installs hidden files on a user's computer. Furthermore, the installation, obviously, did not provide tools to uninstall the rootkit.

XCP is a perfect example of security by obscurity. Security by obscurity never works. On 31 October 2005, Mark RUSSINOVICH, a rootkit expert, discovered an installed rootkit on his PC. After analysis, he identified the source: the XCP copy protection of Sony BMG. The detailed analysis also highlighted that XCP infringes Gnu Public License (GPL). It includes a source code portion written by the (in)famous hacker DVD Jon.

### Rootkit

When a hacker gains access to an Operating System (OS), often he wants to maintain stealth access. Thus, the hacker installs a specific program called a Rootkit. The rootkit has the capability to hide itself from the user of the operating system and to provide a hidden "back door" to the hacker.

Operating Systems have a kernel, many applications and the user. A Rootkit is very close to the kernel. It permanently monitors communication between users, applications and the kernel. Thus, the Rootkit can intercept queries that may disclose its presence, and replace data with a fake answer.

A Rootkit may be useful to hide a process or an open point used by the hacker to control the computer. For instance, XCP's rootkit hides files with the name containing the pattern "\$sys\$".

A Rootkit can only intercept predefined queries. Thus, there are always specific queries that permit discovery of a Rootkit. Its response does not match the expected one. This difference of behavior permits use of a Rootkit detector. Rootkits and Rootkit detectors are now arm-wrestling, like anti virus.

Unfortunately, this was only the beginning of a long list of problems. A few days after the rootkit discovery, some hackers exploited the stealth ability of the already installed rootkit to install their hidden “malware” (similar to a Trojan horse). Facing this disaster, Sony BMG provided a patch to uninstall the rootkit. Unfortunately, it came with its very own problems. This patch was written too fast. It generates stability problems on any computer to which it is applied. Furthermore, this patch creates a new security flaw if the customer visits web sites controlled by hackers. The hackers can install malicious programs using the resident Sony BMG’s deactivation tool.

### XCP

XCP is a CD copy-protection system provided by a company called First4Internet. CD copy protection is very difficult because it has to comply with Philips’s “Red book”, in order to avoid compatibility issues (e.g. the CD does not play on car radio). XCP is a “Red book” compliant system. The CD has a standard behavior on non-Windows system like car radio, or HiFi audio system. The same is true for Mac OS or Linux system. No copy protection is activated on these systems. On Windows systems, XCP installs three programs (this is a simplified view). The first one controls the CD drives; the second one is a Sony player; and the last one is the rootkit that hides the first program, and obviously itself. The program controlling the CD drive impairs the audio stream unless it is played by Sony’s player. The Sony player allows three copies on the hard disk of the same PC.

In addition to technical and image problems come legal problems. Several lawsuits have been filed against Sony BMG. The Electronic Frontier Foundation (EFF) is attacking Sony for endangering consumers through a flawed copy-protection system. A class action was filed in California, New York and Texas for use of a spyware application against consumers.

Protecting digital content against piracy is legitimate in a context where peer-to-peer networks allow unlimited copies of music tracks. Unfortunately, Sony BMG has gone too fast and too far in the anti-piracy race.

From the point of view of security, we learn some lessons. Once more, security by obscurity produced a flawed design. This has been common knowledge for more than a century [2]. A PC is an extremely complex and hostile environment. To be efficient, security needs a minimal set of assumptions to be trusted. Current PCs do not offer the right environment. Existing PCs need the addition of a trusted and/or tamper resistant kernel. Today, using secure tokens, such as smart cards, or USB tokens, offers one solution. In the future, the Trusted Platform Module (TPM) may provide another stable ground.

*O. COURTAY, C. SALMON LEGAGNEUR*

### References

- [1] COURTAY O., HEEN O., VEYSSET F., Cron-OS, SSTIC 2003, <http://home.gna.org/cronos>
- [2] KERCKHOFF A., La cryptographie militaire, Journal des sciences militaires, vol 9, January 1883
- [3] KOHNO T. et al., Remote Physical Device Fingerprinting, 2005 IEEE Symp. on Security & Privacy.
- [4] SCHNEIER B., The futility of digital copy prevention, in CRYPTOGRAM may 2001, available at <http://www.schneier.com/crypto-gram-0105.html#3>
- [5] XIAIOYN W., HONGBO Y., YIQUN L. Y., Finding Collisions on Full SHA-1, CRYPTO 2005, <http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf>
- [6] XIAIOYN W., Recent Progress on SHA-1, Rump session, CRYPTO 2005, available at <http://www.iacr.org/conferences/crypto2005/r/2.pdf>
- [7] *NIST brief comments on Recent Cryptanalytic attacks on SHA-1*, available at <http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf>
- [8] [http://www.axalto.com/Company/press/pdf/gemalto\\_PR\\_en.pdf](http://www.axalto.com/Company/press/pdf/gemalto_PR_en.pdf)
- [9] <http://www.rsasecurity.com/rsalabs/node.asp?id=2092>