

# The Security Newsletter

## In this issue

**The news**

- Silencing MBTA flaws 2
- The spy who hides in the phone 2
- Red Hat server compromise 2
- DNS weakness 2
- Bug attacks 3

**Lessons from BlackHat and Defcon** 3

**Unclonable chips** 4

**Fighting piracy** 4



Published Quarterly By:  
**Thomson's Corporate Research** - part  
of the Licensing, Research & Innovation  
Division

**Technical Editor:**  
Eric Diehl

**Editors:**  
Sharon Ayalde  
Natalie Hamrick

**Contributors:**  
Patrice Auffret  
Olivier Courtay  
Alain Durand  
Marc Éluard  
Marc Joye  
Frédéric Lefèbvre  
Yves Maetz  
Charles Salmon-Legagneur

**VP and Head of Corporate Research:**  
Gary Donnan

**LR&I Head:**  
Beatrix de Russé

Email and to subscribe:  
[security.newsletter@thomson.net](mailto:security.newsletter@thomson.net)

Copyright Thomson 2008

## INTRODUCTION



Current movie industry's business models are under fire, and two events illustrate this growing pressure. In September, RealNetworks launched its new application, RealDVD. This \$30 application creates a "backup" copy of any DVD on a computer. This saved copy is linked to one computer, i.e., it is not possible to copy it onto another computer. A user may register up to three extra computers (for \$20 each) in order to make additional copies. RealNetworks claims that RealDVD is legal because it does not crack the CSS that actually protects DVDs.

This, according to them, is not infringing the Digital Millennium Copyright Act. However, studios do not share this opinion. A judge ordered RealNetworks to halt sales of RealDVD in order to have time to study the problem. In turn, RealNetworks and Hollywood studios sued each other.

Summer season ends when the new seasons of TV series start. The first big hit was Prison Break's season four. According to Fox, the audience of the first episode exceeded 6.5 million viewers. According to TorrentFreak, about 1 million downloads of this episode occurred on BitTorrent one day after the first airing! Interestingly, Fox offered a free catch-up TV service, i.e., Internet users could watch it free on Fox's site. Nevertheless, many viewers used the illegal alternative. Thus, downloaders do not seek free downloads, but rather, availability. Fans that are outside the US cannot access Fox's catch-up TV service, so they face two choices: wait one year to legally watch the misadventures of their heroes, or immediately illegally download the episodes.

For many years, the motto of consumer electronics has been "anywhere, any time, and any how." Consumers want greater flexibility. Some consumers will take any solution in order to be granted this flexibility - legal or illegal, paying or free. Thus, new schemes of content protection have to embrace flexibility



Eric Diehl  
Domain Director, Security

## The News

### Silencing MBTA flaws



Three MIT students, Z. Anderson, R. Ryan and A. Chiesa, under the lead of R. Rivest (The R of RSA!), studied the security of the Massachusetts Bay Transportation Authority (MBTA) cards. They were able to reload the magnetic stripes card "Charlie Ticket" and store information in the electronic card "Charlie Card."

Unfortunately, it seems that the students did not disclose the information to MBTA. They were expecting to present these vulnerabilities at DefCon08. MBTA requested that the presentation be cancelled. The District Judge Douglas Woodlock granted a ten-day restraint. He reinforced his decision with the Computer Fraud and Abuse Act. This law targets hackers who "knowingly cause the transmission of a program, information, code, or command to a computer or computer system." In other words, according to this judge, presenting a paper disclosing weaknesses is equivalent to using software to penetrate a system.

Once more, the questions of when and how to disclose a vulnerability surfaced. Zero day exploits, i.e., exploits using vulnerability not yet disclosed, will be the subject of an endless debate. In any case, restraining information dissemination is not the right solution.

> E. DIEHL

### The spy who hides in the phone

If you have an Apple iPhone, you probably appreciate the pretty animation effects when navigating through the menus. Do you know that in order to display these effects the iPhone takes a snapshot of all navigated pages? Thus, the iPhone secretly keeps the history of its use. This includes text messages, web pages, emails, and even some confidential data.

Jonathan Zdziarski, a renowned iPhone hacker<sup>1</sup>, recently revealed this potential privacy leak. The snapshots are only stored temporarily. Nevertheless, any forensic specialist may recover them using techniques and tools for the recovery of deleted files. This weakness has already been used to gather evidence for criminal investigations<sup>2</sup>, but many other uses are possible.



Security is often a question of trade-off. The developers favored user-friendliness over privacy. Most Apple customers would probably approve this choice. In addition, will its major competitor, Google's new G1 phone, have these issues? We shall see in the coming weeks.

> Y. MAETZ

### Red Hat server compromise



Servers attacked by hackers are common on the Internet. Often, hackers take control of a web server, change the home page (defacing), or steal unprotected sensitive data. Last August an intrusion on a package server of Red Hat (a professional oriented Linux distribution) was detected. The package server is the source for Red Hat released software. This may be critical if hackers modified software. After an inspection, some critical software was actually modified: the OpenSSH server<sup>3</sup>. This corrupted software allows hackers to take control of any Red Hat-powered computer. Nevertheless, the attack could not work and no corrupted software was distributed.



In 2003, the same kind of attacks occurred against the source code server of the Linux kernel<sup>4</sup> ([kernel.org](http://kernel.org)). A hacker successfully inserted one vulnerability in the kernel to obtain administrator privilege. The modification was discovered by chance before the kernel's public release. Now, kernel developers use a distributed cryptographic system that spots any unauthenticated modification of the source code.

As updating and patching mechanisms become more robust, hackers will target the modification of the source, which is the next part to secure.

> O. COURTAY

### DNS weakness

DNS (Domain Name System) is one of the core Internet protocols. DNS converts human readable addresses (such as [www.thomson.net](http://www.thomson.net)) into computer addresses (80.231.198.188), called IP addresses.



Recently, Dan Kaminsky<sup>5</sup> proved how easy it is to exploit a major weakness of DNS protocol. This weakness had never been overlooked. The novelty is the extreme ease to exploit. DNS works as a request/response protocol. It relies solely on the unpredictability of the transaction ID to avoid spoofing vulnerability. This ID is only 16- bits long. An attacker needs only to send 65,535 spoofed replies to exploit the flaw.

Dan Kaminsky showed another method to exploiting DNS. Instead of spoofing a maximum of 65,535 replies, he forces the victim to look up many different hostnames, forcing them to send many DNS requests. Meanwhile, the attacker always spoofs replies

with the same transaction ID until the victim sends a DNS request matching this ID. The novelty is that the attacker's DNS reply answers the victim's requests, but also adds another answer. The victim host accepts it, and a new human readable address to IP address mapping is accepted. The attacker now has access to network communication from the victim to the spoofed domain name. This attack is a race between the attacker and the good DNS server.



DNS implementers try to fix it with software patches, but they just make the vulnerability somewhat harder to exploit. This highlights that security should be part of the initial design. The only efficient solution is wide deployment of DNSSEC.

> P. AUFFRET

## Bug attacks

At the last CRYPTO conference (Santa Barbara, August 17-21, 2008), Eli Biham, Yaniv Carmeli and Adi Shamir<sup>6</sup> presented what they call *Bug Attacks*. These are a variation of fault attacks<sup>7</sup>, but applied to another context.



Bug attacks assume that an implementation is buggy, i.e., the output of a computation may be incorrect. Ordinary fault attacks require that one must inject a fault, whereas bug attacks make use of a "fault" that is already present, but only shows up

for particular inputs. Consequently, bug attacks do not require the physical possession of the device under attack and can be mounted remotely.

As an illustration, consider an RSA exponentiation, say  $y = x^d \pmod N$ , computed using Chinese remaindering. Let  $p$  and  $q$  be the two secret prime factors forming public modulus  $N$  and let  $e$  denote the public exponent corresponding to private exponent  $d$ . Lenstra<sup>8</sup> showed that if either the computation of  $y$  modulo  $p$  or of  $y$  modulo  $q$  (but not both) is faulty - we let  $z$  denote the resulting faulty output - then the computation of  $\text{GCD}(z^e - x \pmod N, N)$  will reveal the factorization of  $N$ , and thus the value of private exponent  $d$ . Lenstra's fault attack can be turned into a bug attack. The attacker must be able to choose an input  $x$  so that, for example, the value of  $x \pmod p$  gives rise to a bug, but that of  $x \pmod q$  does not. As a result, the computation of  $y$  modulo  $p$  will be faulty. A GCD computation simply recovers  $d$ . The authors suggest to choose an  $x$  giving rise to a bug, close to the square root of  $N$ , so that, assuming  $p > q$ ,  $x \pmod p = x$  and  $x \pmod q \neq x$ . Refer to this work for further adaptations of fault attacks.

In conclusion, developers of cryptographic applications should now consider the potential presence of bugs and implement appropriate countermeasures.

> M. JOYE

## Lessons from BlackHat and Defcon



In connection with BlackHat Europe 2008, the summer sessions held several tracks concerning reverse engineering. The new generation of debuggers was the star.

### Idapro superstar

Idapro, the professional disassembler from hexray proved to be a great success for several reasons: Its open architecture, customizable by scripts and plug-ins, invites everyone to enrich the tool with their own security bricks. Version 5.3 improved interoperability by supporting many language interpreters (perl/python/ruby). As a result, it stimulated the creativeness of the Defcon community. A plethora of tools around IDA was presented. One worth mentioning is the CollabREate idapro plug-in, a database wrapper.

### Stronger, faster

Although there was no big revolution in Reverse Engineering, the discipline slightly evolved and became more mature. Economically, reverse engineering is costly because it requires skilled people and time. The current goal is no longer to reverse engineer, but to react faster to threats and patch vulnerabilities against zero-days exploits. Ilfak Guilfanov presented a decompiler plug-in for IDA that correctly decompiles binaries to source code in 80% of the cases. This may increase the speed of the reverse up to 50%. Additional mature tools are also integrated, such as a Swiss army knife mixing all features together - as illustrated in the RETrace kernel debugger package.

### Close Encounters with debuggers of the Third Kind

One of the biggest challenges in reverse engineering is facing polymorphic viruses, as they change their code during execution. A static analysis of their code fails, as it is transiently in clear form only in run time. A dynamic analysis is also



inadequate. The big trend of the last few years is combining both approaches. Hypervisors and virtual machines offer new solutions. Two interesting demonstrations were shown: In the "malware analyst blue pill", a "super-debugger" running in the hypervisor supports both fine grain tracing and in depth investigation of the guest's operating system. VmWare presented a feature that replays the execution of a process in a Virtual Machine. Between live monitoring and static analysis, debugging takes a third way, similar to studying the rushes of a movie.

## A better land for DRM?



At Defcon, Jan Newger presented Reverse Engineering of Windows DRM. This, once again, illustrated the vulnerability of DRM clients on untrustworthy platforms. Although, protected by strong anti-RE techniques, an attacker could modify

user level dependant components (DLL) without tampering with the application. To protect itself from user-land attacks, some DRMs try to take advantage of secret features in kernel land, for instance, by tagging a process (DENY\_ATTACH) to disable debug tracing under MACOSX. Unfortunately, even those protections are vulnerable to attacks from root mode in virtual machines.

Tal Garfinkel (VmWare) explained the new "virtual time" concept: How can a DRM client insure the license date credentials if time and files can be rolled back inside a virtual machine? We should expect that DRM applications will migrate from kernel and user lands to more favorable lands within a virtual host.

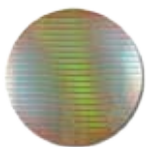
## Conclusion

Viruses are better armed against Reverse Engineering. This calls for better debuggers. The upcoming super debuggers, running in a virtual monitor, are not conceptually different from our actual kernel debuggers. However, they have some great advantages. Running beside and not inside the debugged OS, they are non-intrusive and allow more live debugging and monitoring of the OS.

> C. SALMON-LEGAGNEUR

## Unclonable Chips

A Physical Unclonable Function (PUF) is a function that is easy to evaluate, but difficult to characterize, and thus to duplicate or emulate.



Several years ago, Pappu Ravikanth, a MIT researcher, discovered the basic principle and applied it to optical elements<sup>10</sup>. The idea was to create a 3D microstructure by injecting small glass spheres into an epoxy coating.

Thanks to the randomness of the manufacturing process, each microstructure was different. When illuminated by a laser beam, each reflected the light differently and displayed a different pattern. Identifying one microstructure was done by simply recognizing the corresponding light pattern.

This principle can be applied to silicon<sup>11</sup>. Silicon components replace the glass spheres. Randomness comes from some variations of the components (wire delays, gate delays, quantum mechanical fluctuations) naturally produced by the manufacturing

process. These variations are unpredictable and out of the control of the manufacturer. It is not possible to produce two PUFs with the same characteristics.

However, the chip has a deterministic behavior. When fed with a specific challenge, a given chip always replies with the same response. Another chip answers differently. This uniquely identifies the instance of the chip.

This unique identification can differentiate mass-produced electronic devices using a PUF. This prevents the duplication and emulation of the device.

PUF-based systems use a two-step process. The enrollment step characterizes the PUF. This is done by sending challenges and recording the corresponding responses. The authentication step sends a chosen challenge to the PUF, gets the response, and verifies the matching with the enrolled value.

The principle sounds promising. Real world limitations may appear when implementing a PUF-based solution. There is a risk of insufficient diversification when addressing mass-production quantities or using PUF with too few gates. There is no guarantee that the process is collision free. Therefore, authentication should use a set of challenge responses instead of a single one. Such authentication systems would securely store the challenge response pairs and randomly use them to prevent replay attacks.

This promising PUF technology can be used in real applications. Verayo<sup>12</sup> recently announced the commercialization of the first PUF RFID chip (Vera X512H). The main applications targeted by Verayo are anti-counterfeiting, secure-IDs, and electronic ticketing.

> M. ÉLUARD, Y. MAETZ

## Fighting Piracy

Reducing content piracy uses several methods: increasing the legal offer and its attractiveness, protecting this legal offer using DRM, fighting professional pirates blocking early content leaks, etc. However, these measures are not sufficient. Valuable content is available on Peer-to-Peer (P2P) networks or User Generated Content (UGC) websites. Increasing legal offers are a good incentive for users to stop illegal downloading. Another possible approach is to actively deter users from accessing illegal content. Fingerprinting<sup>13</sup> is an efficient technique to prevent the uploading of copyrighted content on UGC sites. Preventing the exchange of illegal content on P2P networks is more difficult. Increasing the awareness of the public regarding associated risks is a first step. Nevertheless, targeting people who illegally download content is far more effective. Often, Internet users assume that they are completely anonymous, thus, they feel immune against legal

prosecution. Demonstrating to these users that this assumption is wrong can be a good deterrent.



However, this raises several challenges: How can decentralized networks be monitored? How can valuable content be identified? What type of information is relevant? For instance, the first step for sharing a video file on BitTorrent is to create a torrent file, which contains mainly metadata from the video files and metadata about the server (called the tracker). The tracker manages communication between peers sharing this file. It provides the location of the different video chunks. Once a user obtains an entire chunk, he is part of the peer set proposing this video. Other users can download chunks from him. The tracker regularly updates the list of peers. The peer is identified by its IP address.

The next challenge is content identification. In P2P networks, hash codes (MD5, SHA-1, etc.) identify a bit stream. If one bit changes, the whole hash code changes. Thus, a hash code cannot be used alone to identify content. A possible solution is digital fingerprinting. Valuable content is tracked on P2P networks (e.g., based on the movie name). Once identified, a digital fingerprint of the downloaded content is computed to confirm whether it is the claimed content. If so, all files with the same hash code (whatever the associated filename is) will be identified as copies of this movie.

Then, copyright holders or copyright agencies may monitor networks, identify copyrighted content, collect evidence and send a notice, (e.g., called the Digital Millennium Copyright Act (DMCA) takedown notice in the US), to the Internet Service Providers (ISP) that allocated the IP address of the infringer.

Still, there are two main issues/questions: What is the relevance of the IP address stored by the tracker? What is the relevance of the mapping between the IP address and the user? A recent publication<sup>14</sup> described some examples of the users that have been identified as infringers and receiving DMCA notices - although they never downloaded or uploaded any content. Another example is the notifications addressed to printers. These false positives were due to erroneous IP addresses in the trackers, mistimed reports (i.e., blaming a user that was allocated to the IP address at a different moment), or even to man-in-the-middle attacks or dedicated malwares.

While current monitoring systems to detect copyright infringement and pirates reach their limits to guarantee zero false positive, new technologies such as video fingerprint, machine fingerprinting, watermarking and human control bring some solutions. Fighting piracy is more a business and legal issue than a technical issue.

## The French graduated riposte

In June 2008, the French government published a project law deemed "Creation and Internet" to provide a legal framework for the so-called graduated riposte. This riposte identifies Internet users downloading specific content. At their first infringement, users would receive a mailed warning. At the second offense, they would receive registered mail. For the next offenses, their Internet connection would be suspended for three to twelve months. The enforcement of this law is expected to be under the control of an authority named HADOPI (Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet, literally high authority for content diffusion and copyright protection on the Internet). This authority would also be responsible for the follow-up of DRM interoperability. Identification of the infringers would be done with the collaboration of ISP.

Most content providers supported the project, although two major criticisms have been raised. The first one is that access to the Internet would be a fundamental human right, and thus its suspension is not acceptable. The second one is that the control of the law application should not be under the control of an administrative authority, but under judicial power. Concerns were also expressed about potential privacy issues when divulging the owner of an IP address by an ISP.

The European Parliament led this protest by voting two amendments to a European directive on telecommunications: The second one, amendment 138, voted at an overwhelming majority (573 against 74) on September 24th, forbids the suspension of civil liberties or fundamental rights, including access to the Internet, in the absence of judicial decision.

The text of the directive is not yet final since a second vote is expected in November. French President Sarkozy has already tried to influence this vote, asking the European Commission to withdraw the voted amendment. The European Commission rejected this request.

If amendment 138 is confirmed, the French government has to modify its project to comply with the European legislation. Possible tracks are to place the control of law application back under judge authority (at least for the Internet access suspension), or to modify the punishment, e.g., by reducing the bandwidth of the Internet access instead of suppressing it.

Many have surveyed the French case of graduated riposte and it may set a legal precedent, whatever the outcome.

## Where will we be?



- \* Colloque PRIAM (Les technologies au service des droits: opportunités, défis, limites), Grenoble, France, November 20, 2008  
Invited talk: Techniques de protection des contenus multimedia, by Teddy Furon
- \* 7th International Conference on Cryptology and Network Security (CANS 2008), Hong Kong, China, December 2-4, 2008  
Paper presentation: An efficient on-line/off-line signature scheme without random oracles, by Marc Joye
- \* 15ièmes Journées SSI du CELAR (C&ESAR 2008), Rennes, France, December 4, 2008  
Invited talk: Digital rights management, by Eric Diehl
- \* 1st International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems (MPIS 2008), Yilan, Taiwan, December 9-10, 2008  
Paper presentation: Laundering and repackaging of multimedia content in content distribution systems, by Marc Joye (joint work with A. Durand and M. Karroumi)
- \* IEEE International Symposium on Multimedia (ISM 2008), Berkeley, CA, USA, December 15-17, 2008  
Paper presentation: Secure and low cost selective encryption for JPEG2000, by Ayoub Massoudi (joint work with F. Lefèbvre, F.-O. Devaux, and C. De Vleeschouwer)
- \* SPIE/IS&T Conference on Media Forensics and Security XI (Electronic Imaging 2009), San Jose, CA, USA, January 19-21, 2009  
Paper presentation: Image and video fingerprinting: Applications, by Frédéric Lefèbvre (joint work with, A. Massoudi, B. Chupeau, and E. Diehl)  
Paper presentation: Binary Forensic Code for Multimedia Signals: Resisting Minority Collusion Attack, by W. Sabrina Lin (joint work with S. He, and J. Bloom)

## References

<sup>1</sup>Jonathan Zdziarski, iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets (O'Reilly Media, Inc., 2008)

<sup>2</sup>Kathryn Barrett, "Video now available - iPhone Forensics 101: Bypassing the iPhone Passcode - O'Reilly FYI Blog," O'Reilly FYI, September 17, 2008, <http://fyi.oreilly.com/2008/09/iphone-forensics-101-recording.html>

<sup>3</sup>"Critical: openssh security update," Red Hat Network, <http://rhn.redhat.com/errata/RHSA-2008-0855.html>

<sup>4</sup>Simoniker, "Linux Kernel Back-Door Hack Attempt Discovered," Slashdot, November 6, 2003, [http://linux.slashdot.org/article.pl?no\\_d2=1&sid=03/11/06/058249](http://linux.slashdot.org/article.pl?no_d2=1&sid=03/11/06/058249)

<sup>5</sup>Dan Kaminsky, "It's The End Of The Cache As We Know It," in , [http://www.doxpara.com/DMK\\_BO2K8.ppt](http://www.doxpara.com/DMK_BO2K8.ppt)

<sup>6</sup>Eli Biham, Yaniv Carmeli, and Adi Shamir, "Bug Attacks," in Advances in Cryptology - CRYPTO 2008, vol. 5157 of Lecture Notes in Computer Science, vol. 5157, pp. 221-240, Springer-Verlag, 2008.

<sup>7</sup>Dan Boneh, Richard A Demillo, and Richard J Lipton, "On the importance of checking cryptographic protocols for faults," in Advances in Cryptology - EUROCRYPT '97, vol. 1233 of Lecture Notes in Computer Science, pp. 37-51, Springer-Verlag, 1997.

<sup>8</sup>Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults," Journal of Cryptology 12, no. 4 (1999): 241-245

<sup>9</sup>Ravikanth Pappu et al., "Physical One-Way Functions," Science 297, no. 5589 (September 20, 2002): 2026-2030, doi:10.1126/science.1074376.

<sup>10</sup>Blaise Gassend et al., "Silicon physical random functions," in Proceedings of the 9th ACM conference on Computer and communications security (Washington, DC, USA: ACM, 2002), 148-160, doi:10.1145/586110.586132, <http://portal.acm.org/citation.cfm?id=586110.586132>.

<sup>11</sup>"Verayo :: Home," <http://www.verayo.com/>

<sup>12</sup>Frédéric Lefebvre and Michael Arnold, "Fingerprinting and filtering," Security newsletter 1, no. 4 (December 2006), <http://eric-diehl.com/newsletterEn.html>

<sup>13</sup>M. Piatek, T. Kohno, and A. Krishnamurthy, "Challenges and Directions for Monitoring P2P File Sharing Networks," University of Washington Technical Report UW-CSE-08-06-01. (June 2008), [http://dmca.cs.washington.edu/uwcse\\_dmca\\_tr.pdf](http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf)