Security vulnerabilities, exploits and attack patterns: 15 years of art, pseudo-science, fun & profit

Iván Arce

Core Security Technologies
Humboldt 1967 2do Piso
Buenos Aires, Argentina
(+54-11) 5556-2673
www.coresecurity.com

.prolog

Who is this guy?!

CTO and co-founder of Core Security Technologies (http://www.coresecurity.com)

- Founded 1996 in Buenos Aires, Argentina

Involved in security research and vulnerability discovery ever since

- Early adopters and pioneers of the public diclosure process for software bugs
- 50+ security advisories, papers and technical articles published
- Several hundredths of bugs reported
- Coordinated bug report with Microsoft, Cisco, Sun, SGI, IBM, Digital, HP, all Linux vendors, BSD, etc.

Develops and sells the first commercial software package for automated network penetration testing that includes real exploit code

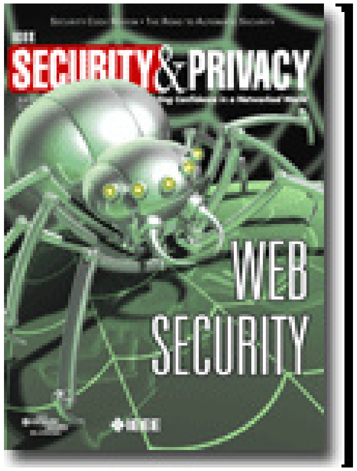
- CORE IMPACT ($)

Provides security consulting services: Network/Application penetration testing, source code security audits & training

Does research, development and maintainance (...barely...) of a handful of defensive/offensive security OSS projects

- Core Force, Core Wisdom, Secure Syslog, Modular Syslog, Pcapy, Impacket, Uhooker, crypto systems, attack simulation & modeling, software rights protection, webapp privacy & security....

But also...



Editor for IEEE Security & Privacy magazine

- New Vulnerabilities and Attack Trends department
- Mental note: *check out IEEE S&P magazine* http://www.computer.org/portal/site/security

Un-graduated Electronic Engineering student at UBA

- At 4 out of 7 years to degree
- A more respectable way of saying “college dropout”

Former head of R+D at Computer Telephony Integration startup in Argentina

- Dealt with early day CTI HW & SW
- Had to work with PBXs, CO swtiches, PSTN, signalling systems, SS7, MFCR2, CCITT 5
- Force to understand non-IP data networks and protocols: X.25, SNA, IPX, propietary
- Forced to deal with “obscure” systems: MVS/TSO/CICS, Tandem NonStop, VMS, Prime OS, HP RTE
- Forced to write, break and fix mission critical/security sensitive apps.

Basically, a monkey with a keyboad (and a low budget)

Why is any of this relevant ??

Speaking @ the 15th USENIX Security Symposium

10. I felt honored by the invitation. I accepted

20. I realized I had nothing really deep, new or interesting to talk about

30. Somebody made a terrible mistake. What were they thinking?!

40. So now I need to talk my way out of here (hopefully alive)

What is this talk about then?

Speaking @ the 15th USENIX Security Symposium

The only thing I am somewhat authoritative about

But how to do that without being:

Arrogant

Boring

Content-free

Blame it on others!

1991-2006: 15 years in the infosec industry

The generation that came to the infosec world in the 1990s

Hackers, crackers, phreakers, virus writers, game developers, hardware manglers

Self-perceived and often called

- Computer artists
- Greedy new business men
- Pseudo-scientists
- Half-baked engineers (hey, don’t look at me!)
- Dangerous criminals
- Treacherous cyber-terrorists
- Technological anarchists
- Progressive thinking libertarians what will save the world, the whales and our precious bodily fluids

What does it mean to the information security discipline?

The information security avant garde

I looked it up on Wikipedia

http://en.wikipedia.org/wiki/Avant-garde

> *Avant-garde in French means front guard, advance guard, or vanguard. People often use the term in French and English to refer to people or works that are experimental or novel, particularly with respect to art, culture and politics.*
>
> *According to its champions, the avant-garde pushes the boundaries of what is accepted as the norm within definitions of art/culture/reality.*
>
> *…proponents of the avant-garde argue it is relevant to art because without these movements art itself would stagnate and become dormant and merely craft, repeating the same style over and over…*

So… did it meant any improvement?

My first computer

~1982 The birth of a computer user

My first computing experience

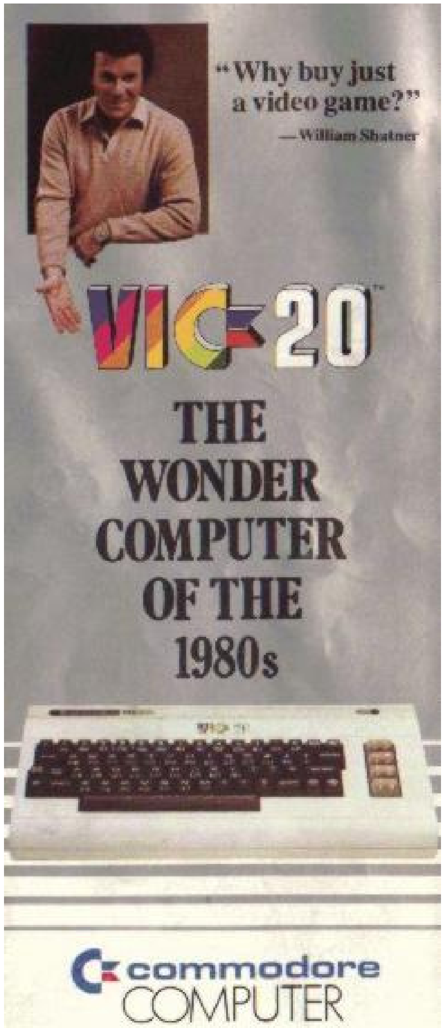
- Commodore VIC-20
- ~4KB RAM, MOS 6502 1Mhz CPU
- 22 column x 23 row color display (RF out to TV)
- ROM BASIC
- ~ $300USD

http://oldcomputers.net/vic20.html

Seen as a toy to experiment and play with

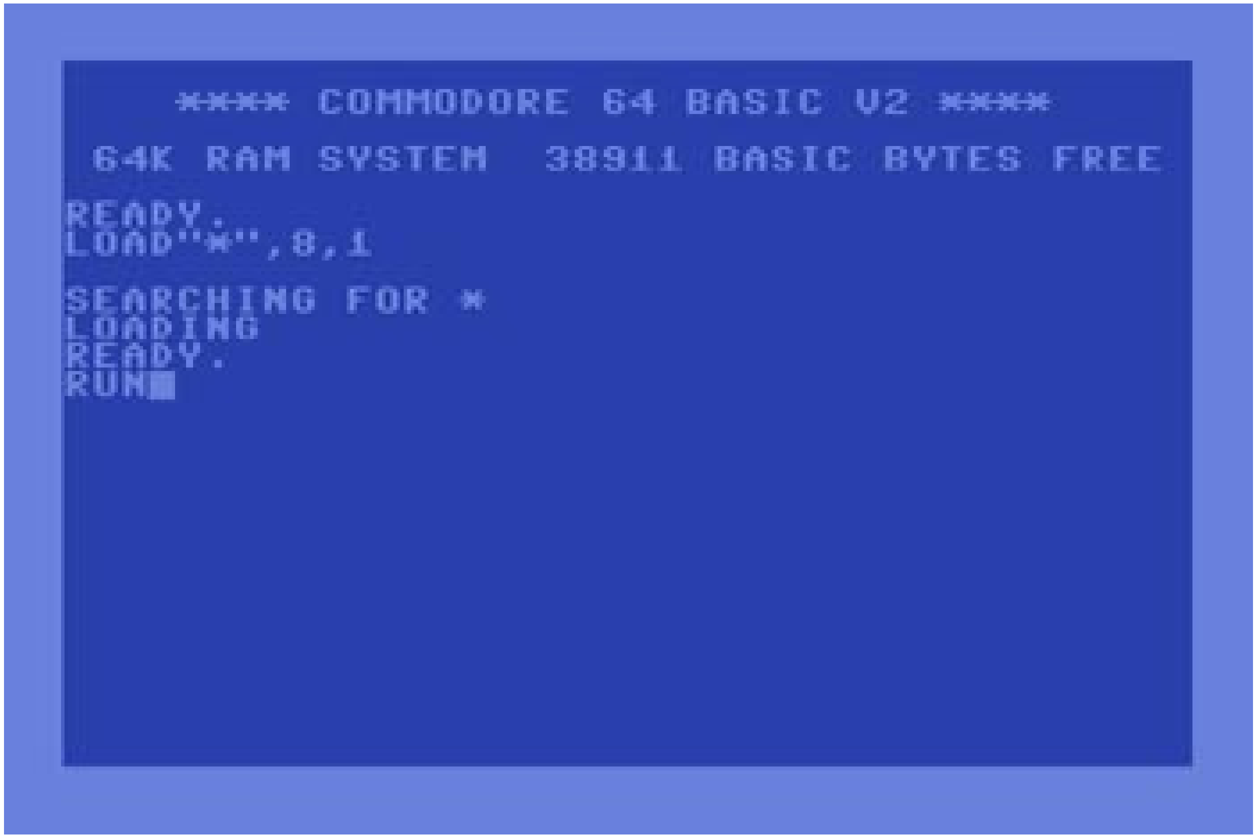
- Installed the notion of computers (and eventually computer security) as a game rather than a tool for formal education or work
- Hence the difference: Adversary vs. Enemy
- Experimental, self-centered, bound by its physical limitations

- And hinted at many undocumented and hidden features


"Why buy just a video game?"
—William Shatner
VIC-20
THE WONDER COMPUTER OF THE 1980s
commodore
COMPUTER

My 2nd computer. Commodore C-64

~1982 The birth of a computer user



```
    **** COMMODORE 64 BASIC V2 ****

 64K RAM SYSTEM  38911 BASIC BYTES FREE

READY.
LOAD"*",8,1

SEARCHING FOR *
LOADING
READY.
RUN
```

Apple II, TRS-80, TI-99/4A, Sinclair ZX80, Timex/Sinclair 1000, Atari 400/800

How the toys went wrong

Programing with home computers

VIC-20 Programmer’s reference guide (http://www.geocities.com/rmelick/prg.txt)

“VIC-20: An all-purpose reference guide for the first-time computerists as well as experienced programmers!”

“The great thing about a computer is that you can tailor the machine to do what you want it to - you can make it calculate your home budget, play arcade - style action games - you can even make it talk! And the best thing is, if your VIC 20 does only ONE of the things listed below, it's well worth the price you paid for it.“

“*In the future, being able to "speak" a computer language will give you a tremendous advantage over those who can't...not because you can write a computer program, but because you'll have a better understanding of what a computer is and does, and you'll be able to make better use of computing at school, on the job and at home…”*

The misterious “Machine Language”

Programming with home computers

VIC-20 Machine Language programming guide:

> *WHAT IS MACHINE LANGUAGE? At the heart of every microcomputer, there is a central microprocessor, a very special microchip which is the "brain" of the computer. The VIC 20's microprocessor is the 6502 chip. Every microprocessor understands its own language of instructions, and these instructions are called the machine language instructions of that chip. To put it more precisely, machine language is the ONLY programming language that your VIC 20 really understands. It is the native language of the machine.*
>
> *WHAT DOES MACHINE CODE LOOK LIKE? You should be familiar with the PEEK, and POKE commands in the CBM BASIC language for changing memory locations. You will probably have used them for graphics on the screen, and for sound effects. The memory locations will have been 36874, 36875, 36876, 36877, 36878 for sound effects. This memory location number is known as the "address" of a memory location. If you can imagine the memory in the VIC 20 as a street of houses, the number on the door is, of course, the address. Now we will look at which parts of the street are used for which purpose…*

BYTE magazine and my first “security incident”

…10 YEARS LATER

Home computer users become professionals

INFORMATION SECURITY 1990

Post RTM worm

No public discussion and research about security

- UNIX security list: ~450 subscribers (1989)
- Zardoz security list (1989-1991)
- Core security list (1990-1991)

No TCP/IP stack on Windows

No Linux

No “web”

No Google (only “archie”)

Security information flowed from technical journals, BBSes and underground publications (Phrack et al.)

A new round for the security disclosure debate

THE CORE SECURITY LIST

http://securitydigest.org/core/archive/101

Date: Sat, 23 Jun 90 14:49:30 PDT

From: neil (Neil Gorsuch)

Subject: WELCOME to core

> *Welcome to the core security mailing list! THIS IS NOT THE ZARDOZ SECURITY MAILING LIST! The core list is a small subset of the zardoz security list. The core list is much more difficult to join, and the membership is limited to a small select group of people. The zardoz list exists for these reasons: 1. To notify system administrators and other appropriate people of serious security dangers BEFORE they become common knowledge. 2. Provide security enhancement information. The core list shares those goals, and in addition is meant for the open discussion of NEW and UN-FIXED security holes. The members of the core list are expected to be actively finding and FIXING new security holes. Any new holes that are found to be "pluggable" by the vast majority of binary-only sites that they affect, will have only the directions for "plugging" them forwarded to the zardoz list after about a 2 week delay by me. NO "COOKBOOK" DIRECTIONS for duplicating the holes will leave the core list. If the directions for plugging the holes make the nature of the hole obvious, a brief description of the hole will also be sent to the zardoz list. After an additional 3 or 4 week delay, I will post some even more abbreviated "plugging" directions to the news group alt.security. I will take whatever steps I can to keep the core list from falling into the wrong hands, but you can make my job immensely easier by not keeping archives of the list. One of the primary reasons that the core list was formed is because enough copies of the zardoz list's archives were on enough internet systems, and enough internet systems were being broken into, that a lot of the "serious" crackers ended up getting copies on a fairly regular basis. I would also appreciate it if the members of the core list would refer to it (publically, at least) as the "holes" list or the "inner" list. I don't want crackers grepping mail spool directories for "core", as they have in the past for "zardoz"….*

A new round for the security disclosure debate

THE CORE SECURITY LIST #2

Date: Thu, 28 Feb 91 23:22:40 PST

From: neil (Neil Gorsuch)

Subject: core list change

> *[The core list was formed to be a forum for exchanging information about newly found security holes and other areas of concern and is as safe as I can reasonably make it for such information. As of now, I am implementing a new policy that was suggested by another person that, like me, is tired of seeing people gather information without contributing any. Except for a few exceptions, anyone not submitting a security "report" at least once a year will be dropped from the list. Exceptions are organizations like cert and a few other obvious destinations. The exceptions do not include certain large computer companies that announce security holes in various places without posting the details here 8-). - neil]*

Date: Tue, 5 Mar 91 11:33:07 PST

From: neil (Neil Gorsuch)

Subject: more on core list change

> *[The "reports" that are now required at least once a year for most members to remain on this list may consist of any of the following: 1. An explanation of a new security hole, with COOKBOOK DIRECTIONS on how to exploit it if it's not obvious. 2. A clarification of an announced, but not explained, security hole. In the words of someone else, "meat, we need meat". Neil]*

A string of bugs in rdist to make a point.

http://securitydigest.org/core/archive/120

RDIST BUG

Date: Wed, 11 Sep 91 13:08:52 PDT

From: Brad.Powell@Corp.Sun.COM

Subject: one for the inner core.

[Received this today. My own testing results: as expected, Suns and Solbournes have the hole, as does Ultrix 4.2 on a DECstation. The NeXT seems to be safe. The IBM 6000 doesn't have an on-line manual page for rdist and I can't get rdist to work on it. - neil]

*Neil- I turn to you, since this bug seems to be in BSD UN*X as well as AIX for that matter. We are working out a fix now, but others will need to also. We have had a fix suggested to us, and are evaluating now. The fix description is at the end. Brad Powell Sun Microsystems Software Security Coordinator.*

SENSITIVE INFO FOLLOWS:

SUMMARY Users can gain root access with rdist(1) as shipped with BSD 4.x And probably all systems derived thereof (SunOS 4.X included)

DESCRIPTION Rdist(1) is a program that updates files on remote machines. At the end of the update it does a chmod on the file (under certain circumstances). The pathname used is the pathname of the temporary file. The chmod(2) is done as root. During the transfer of a file there is a window of opportunity in which the user can replace the temporary file by a symbolic link to a system executable. (It also does a chown(2), but chown(2) doesn't follow symlinks, but chmod(2) does.)

Yet it did not seem to work back then...

http://www.security-protocols.com/textfiles/advisories/8lgm/8lgm-01.txt

ANOTHER RDIST BUG

This advisory has been sent to:

comp.security.unix
INFOHAX infohax-emergency@stormking.com
BUGTRAQ <chasin@crimelab.com>
CERT/CC cert@cert.org

===

[8lgm]-Advisory-1.UNIX.rdist.23-Apr-1991

PROGRAM: rdist(1) (/usr/ucb/rdist or /usr/bin/rdist)

VULNERABLE OS's:

SunOS 4.1.2 or earlier (Patch-ID# 100383-06 fixes this), A/UX 2.0.1, SCO 3.2v4.2 BSD NET/2 Derived Systems Most systems supporting BSD rdist

DESCRIPTION: rdist(1) uses popen(3) to execute sendmail(8) as root. It can therefore be made to execute arbitary programs as root.

*[**exploit code deleted**]*

FIX:

1. *Contact your vendor for a fix. Sun's latest rdist patch (Patch-ID# 100383-06) fixes this hole in SunOS. **Some vendors closed this hole while fixing an unrelated problem** published by CERT in their advisory: CA-91:20.rdist.vulnerability.*
2. *2. In the meantime, restrict access to rdist.*

SHELLCODE

Discovery of the shellcode

SHELLCODE EVOLUTION

1974- “Multics Security evaluation: Vulnerability Analysis” (pp.22+)
Paul Karger, Roger Schell
http://csrc.nist.gov/publications/history/karg74.pdf

1989- Buffer overflow exploit for fingerd in RTM Worm
“The Internet Worm Program: An Analysis”
Eugene H. Spafford
http://homes.cerias.purdue.edu/~spaf/tech-reps/823.pdf

?

1995- ”Vulnerability in NCSA HTTPD 1.3”
Thomas Lopatic
http://archives.neohapsis.com/archives/bugtraq/1995_1/0403.html

1996- “Smashing the Stack for Fun and Profit”
Aleph1, Phrack Magazine issue 49
http://www.phrack.org/phrack/49/P49-14

Stack smashing-> monolitic shellcode

Common software engineering practices applied

EXPLOIT CODE & SHELLCODE

Build re-usable components

- “LSD Win32 Assembly components”
- http://www.milw0rm.com/shellcode/
- http://www.metasploit.com/shellcode.html

“Functional refactoring”

- Attack vector
- Control of execution flow
- Payload

Some components

- Enconding/(Un)Marshalling
- Connection methods for command and control
- “Stagers”

“Techniques”

- Stack overflow, FP, Heap oveflow, SEH,
- Return-into-libc, signal handlers, GOT, PLT, vpointers, DEP, etc...

Avoid detection and prevention

- Polymorphism, metamorphism, fragmentation, multiple enconding
- StackGuard/Shield/Propolice/ASR/Syscall throttling/API hooking/etc
- Syscall proxying and other multi-purpose agents, stealthness, *rootkits*

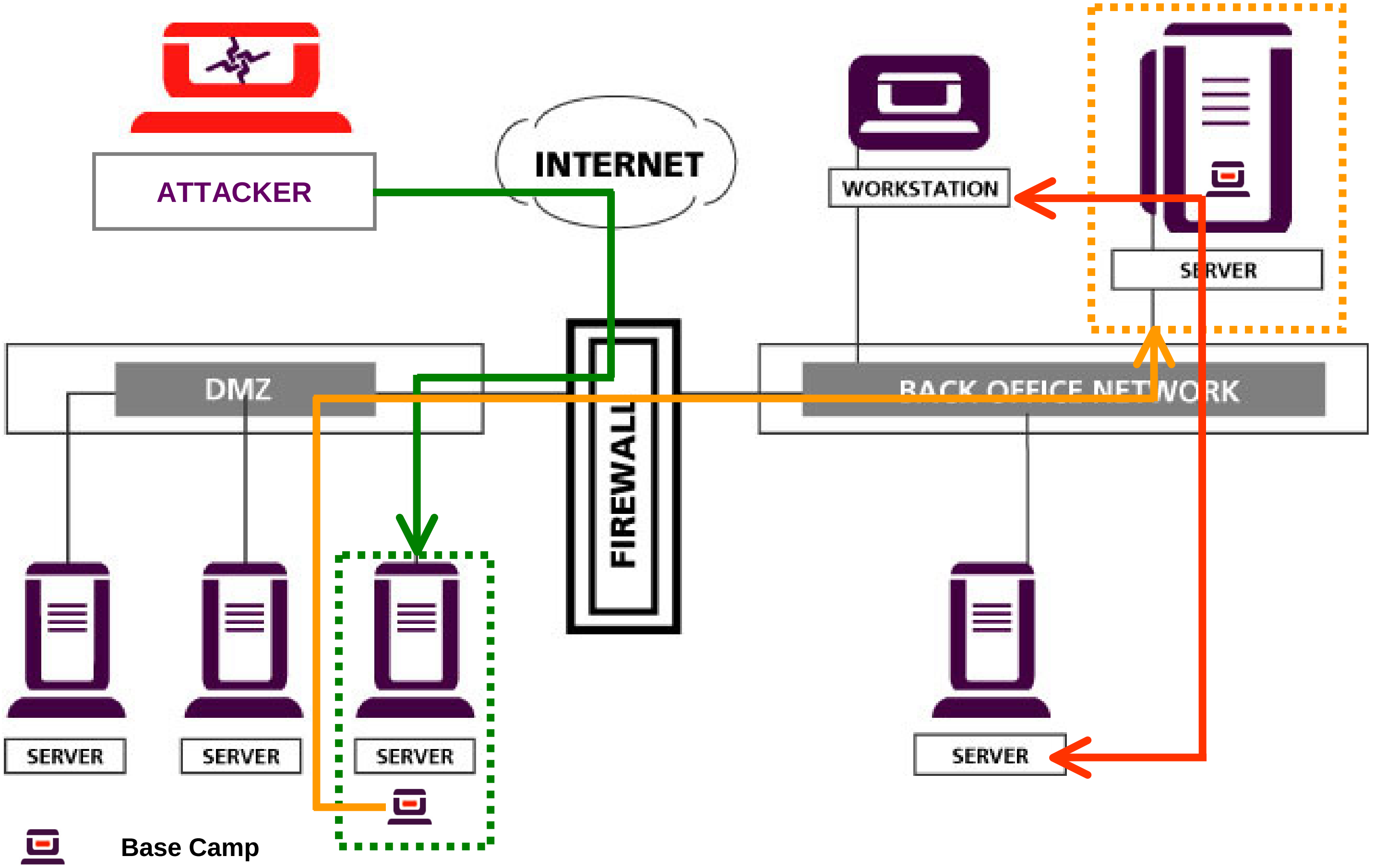
A new generation of shellcode experts?

"The Shellcode Generation" - IEEE S&P magazine vol.2 no.5

EVOLUTION OF ATTACK PATTERNS

The attack of the firewall era (1990-2001)

ANATOMY OF A CLASSIC ATTACK



💻 Base Camp

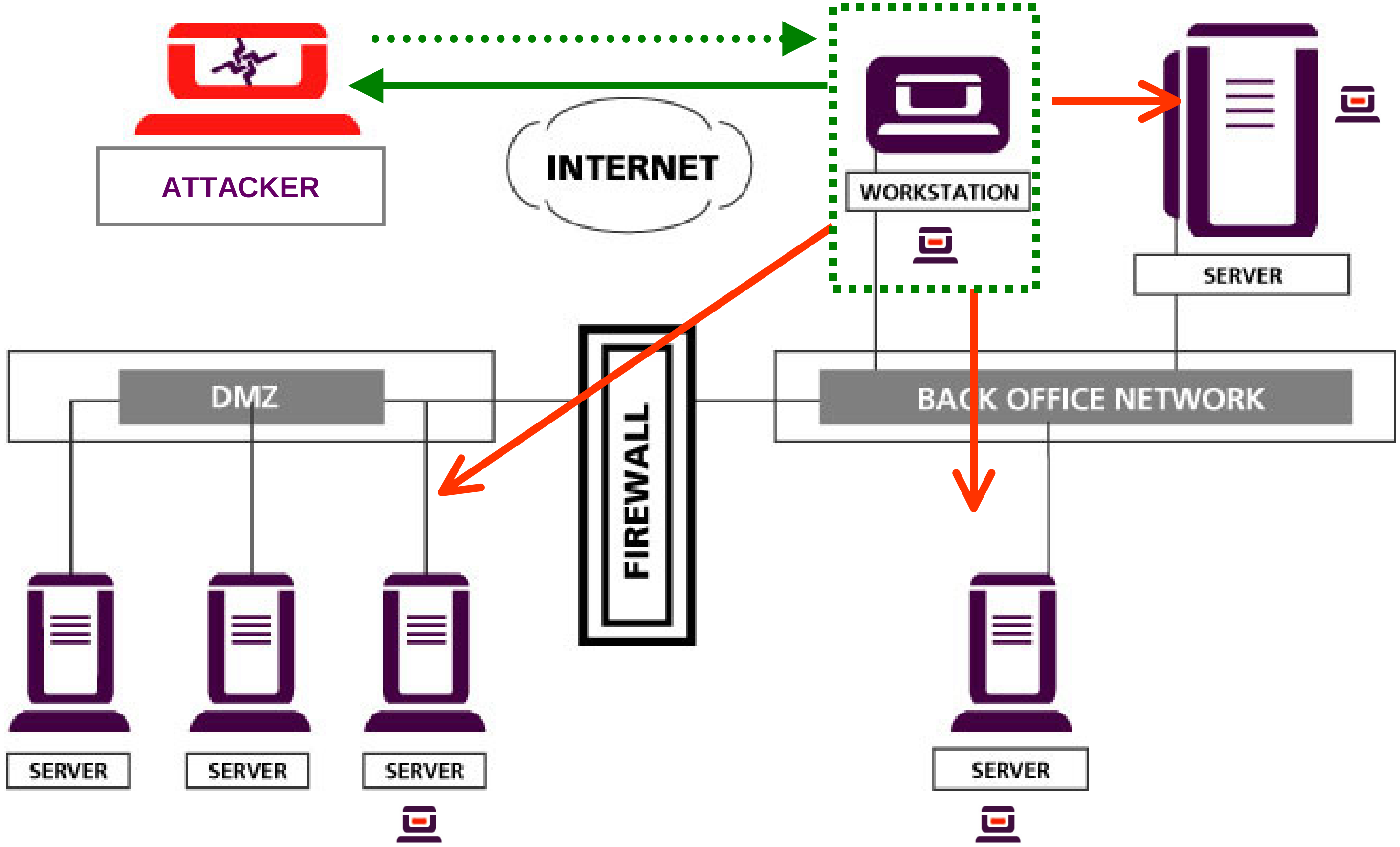
— A target server is attacked and compromised

— The acquired server is used as vantage point to penetrate the corporate net

— Further attacks are performed as an internal user

The *New* Thing (2001+)

CURRENT ATTACK TREND



Base Camp

A target workstations are attacked and compromised

Further attacks are performed as an internal user

Why go after the desktop?

Desktop and Workstation attacks

Law of minimium effort

Myriad of vulnerable applications

Web browsers, mail user agents, Media players, Instant Messaging

Business-oriented application clients, productivity tools, file viewers, re-usable components and vulnerable libraries, network asset management and security software agents (AV, backup, PF, IPS)

Difficult to implement inventory and change control

Difficult to deploy and manage countermeasures

Patches, security policies, access control mechanisms

Operated by careless, untrained, unaware users

Favourable attack scaling and probability of success

It is the front door to corporate and home networks

"The Weakest Link revisited" - IEEE S&P magazine vol.1 no.1

The desktop plays the role of host to various new attack vectors

NEW ATTACK VECTORS

Wireless

- 802.11
- Bluetooth

Interface with new peripherals using new kinds of I/O ports

- IEEE 1394 (Firewire)
- USB
- SCSI, PCMCIA, SATA, etc.

Device drivers and connected peripherals

- PDA, cellphone, audio/video player, camera, gaming console
- External storage, microphones, headphones, etc.

Desktops expose a wider attack surface

"The Rise of the Gadgets" - IEEE S&P magazine vol.1 no.5

“Bad Peripherals" - IEEE S&P magazine vol.3 no.1

Most importantly... Who is the target of the attack ?

How is it done?

REQUIREMENTS FOR A DESKTOP/CLIENT-SIDE ATTACK

Traditional information gathering does not apply

Server-side infrastructure

- Delivery of probing code
- Servers: DHCP, DNS, HTTP, FTP, Samba
- Second-stage code delivery
- Command and control

Blind exploitation

- Must contemplate possible endpoint security solutions
- Must contemplate avoid user attention.

Command and control

- Must contemplate target network topology (viewed from the inside)
- Must contemplate the life-cycle of the exploited process
- Must contemplate end user behavior

Profile: Network hacker+virus writer+reverse engineer

A TALE ABOUT SSH

Re-inventing the wheel part I...

BAD CRYPTO?

SSH v1.x protocol

- Blowfish, IDEA, DES, 3DES, RC4
- CRC-32 for packet integrity
- CBC and CFB modes

1998- “CRC insertion attack”

- Known plaintext
- CRC-32 compensation with extra garbage

Paper: http://www.coresecurity.com/files/files/11/CRC32.pdf

Advisory: http://www.coresecurity.com/common/showdoc.php?idx=131&idxseccion=10

Research, report, develop patch, distribute to vendors

- Great!
- Are we better yet?

2001- “SSH1 compensation <u>attack detector</u> vulnerability”

- Michel Zaleswki @ Bindview: The patch is wrong!
- http://www.coresecurity.com/common/showdoc.php?idx=81&idxseccion=10

GO HACK YOURSELF!

Yet another controversial topic...

GO HACK YOURSELF!

Improving the security of your site by breaking into it (1993)

Dan Farmer, Wietse Venema

http://www.porcupine.org/satan/demo/docs/admin_guide_to_cracking.html

Emergence of network vulnerability scanners (1994-1996)

- Strobe
- nfsshell
- SATAN
- iss121.shar (OSS, shell script)

...turns into a hundreth million dollar industry... (1996-1998)

- ISS Internet Scanner, Secure Networks Inc. Ballista, Wheelgroup NetSonar
- Network Associates CyberCop Scanner, Bindview, Nessus, eEye, GFI, nCircle, Qualys, Foundstone, Rapid7.....

But are we better yet?

- False positives, false negatives, scale & priorization, remediation & patch management
- The quest for completness

An attempt to improve

AUTOMATED PENETRATION TESTING

Automated penetration testing and exploitation tools (2001+)

- Core IMPACT ($)
- Metasploit
- Canvas ($)
- SAINT Exploit ($)
- Various OSS projects

Let’s get back to the basics from Mr. Farmer and Mr. Venema

- Use real exploits
- Combine with network penetration testing practices
- Integrate into a business process
- Skript kiddies do it!

Filter out false positives and identify false negatives

- Challenge: Turn exploits into software engineered artifacts
- Quest for completness... Again?!
- Reliability, coverage

Prioritize better

- Penetrate & Patch?

Blasfemy!!

An attempt to understand attacks rather than vulnerabilities

PARADIGMS AND BUSINESS MODELS

Call security now!

“Il Gatopardo”

Il Gatopardo (1963)

- Film director Lucchino Visconti’s story about a nobleman in the Sicily of the 1800s
  http://www.imdb.com/title/tt0057091/

Mainframe security paradigm

- The ivory tower

Antivirus security paradigm

- The evil is in the air

Firewall security paradigm

- Us & Them. People wear hats

Vulnerability scanner paradigm

- Offensive is good... but not **too** offensive and not **that** good

IDS security paradigm

- If you can’t stop them...

Endpoint security paradigm

- AV+FW vs. the user

Network IPS security paradigm

- AV+FW vs. people that wear hats. Really, now it works!

SSON, PKI, ESM, ID mgmt, NAP/NAC security paradigm

- One ring to rule them all

Changing (new?) technologies but the underlying model remains the same...

HOW DO I ADD VALUE TO MY INFOSEC SYSTEM?

Centralized management & deployment

- Policies, ACLS, RBAC, identities, authorization tokens, etc.

Centralized generation of security value

- AV/IDS signatures, patches, certificates, vulnerability checks etc.

Centralized/hierachical distribution of security value

- AV/IDS signature updates
- Remote/local vulnerability checks
- Patches
- Certificates

Meanwhile, outside of our information security world...

THIS IS NOT HAPPENING!

Open Source Software

An overflow of (irrelevant?) information became available

Peer-to-Peer systems

Mobile code

Proliferation of gadgets with embedded systems

Technology-backed social networks

Reputation/Collaboration systems

Can current infosec technologies and business models ignore them? Should?

.epilog

Where do we go from here?

15 years in the information security world

A new generation entered the information security discipline in the early 90s

- Hands-on practitioners with their foundations on home computing
- Computers, and security, perceived as a “game”
- Internet networking, open standards, low cost HW/SW and the “Web” was not taken for granted

And what have they done ?

- Contributed to create an information security market and an industry to service it
- Pointlessly re-invented the wheel (several times)
- Embraced and promoted open and unmediated discussion about security issues
- Advanced and industrialized offensive security technology
- Got rich, famous and/or to jail
- Delved for 15 years at the intersection of Art, Science & Business

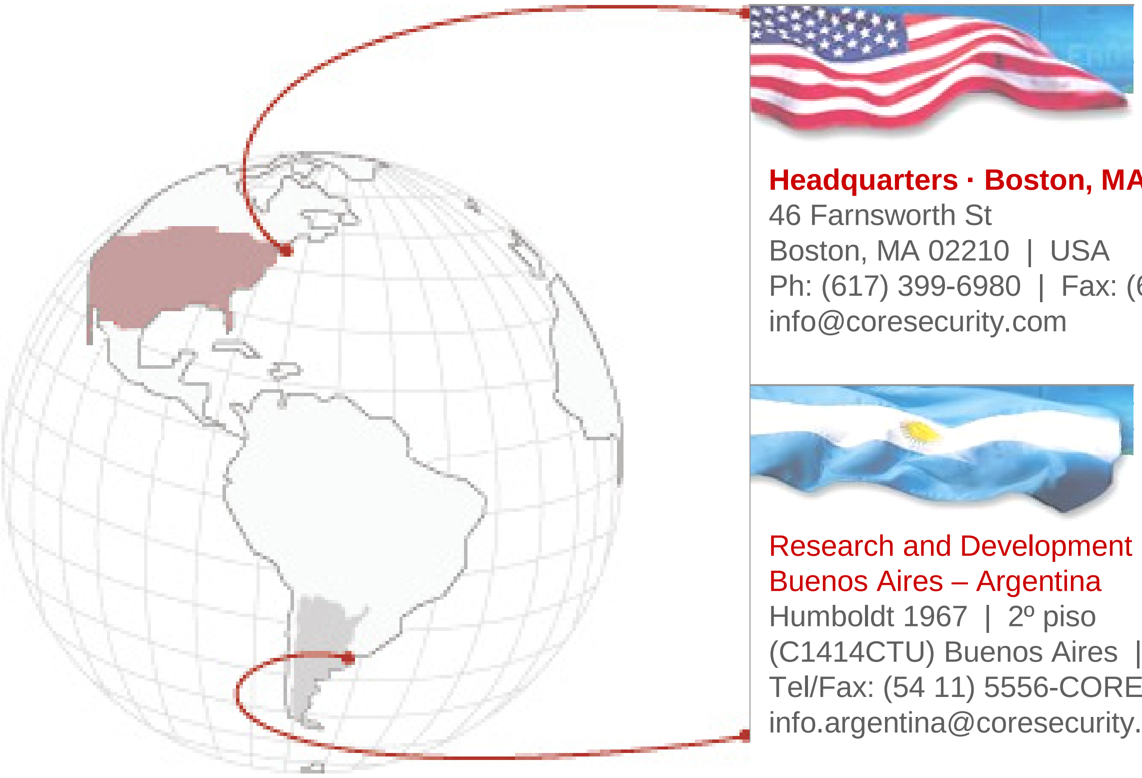
Did it make any difference?

What should we do to help the next generation?

GRACIAS!

Iván Arce ivan.arce {#} coresecurity.com

CONTACT INFORMATION



Headquarters · Boston, MA
46 Farnsworth St
Boston, MA 02210 | USA
Ph: (617) 399-6980 | Fax: (617) 399-6987
info@coresecurity.com

Research and Development Center
Buenos Aires – Argentina
Humboldt 1967 | 2º piso
(C1414CTU) Buenos Aires | Argentina
Tel/Fax: (54 11) 5556-CORE (2673)
info.argentina@coresecurity.com

www.coresecurity.com