

Internet Security 2

General Windows Security 1/2

Markus Kammerstetter

Christian Platzer

inetsec@iseclab.org

Gilbert Wondracek

Edgar Weippl

News from the Lab

*Int. Secure Systems Lab
Technical University Vienna*

- Challenges
 - 32 solved Challenge 1 – good job!
 - One week to go
- Notable entities:
 - 15:02:23 LUKAS "Anonymous Dead" WEICHSELBAUM (<1h)
 - 15:49:05 GEORG "Lawless Myst" WILTSCHEK (<2h)
 - 15:51:24 BERNHARD "Mind Mole" URBAN (<2h)
- Upcoming Challenge:
 - Remote Exploit (starts next week)
 - Put last lecture to use

UCSB CTF 2010

*Int. Secure Systems Lab
Technical University Vienna*

- What is it
 - Applied Security
 - Team experience
 - Lots of fun
 - Free food
- When
 - Friday, December 2nd, 8am to 5pm Pacific Standard Time
 - That's 5 pm to 2 am for us *yawn*
- Who can participate
 - 20 - 25 Students from this Course
- How to participate?
 - Details will follow in the Lectures, once the Date is officially announced

<http://ictf.cs.ucsb.edu/>

News from the Field

*Int. Secure Systems Lab
Technical University Vienna*

- **Lion vulnerability** (yes, the latest Mac OS)
 - Allows to change password on unlocked Apple stations
 - Weakness in authentication module
- **Android**
 - Application permission escalation
 - Allows installation of arbitrary applications
 - Privilege escalation
 - Drops to root shell
 - Not seen in the wild yet
- **Bundestrojaner is a piece of ... software (Win DLL)**
 - Symmetrical AES block cipher (key hardcoded)
 - Kernel + Userland module
 - No Authentication (of C&C or Zombie)

General Windows Security

Overview

*Int. Secure Systems Lab
Technical University Vienna*

- This lecture will NOT be
 - An anti-windows campaign
 - A pro-windows campaign
 - A pro/contra unix campaign
 - about pushing ipride
- This lecture is supposed to be
 - A comparison of strength and weaknesses across
 - open Source
 - And commercial operating systems
 - Interesting

Overview

*Int. Secure Systems Lab
Technical University Vienna*

- Technical aspects
 - What happened to this OS ??
 - Exploiting Windows (BHO, shell code, etc.)
 - Securing Windows
- Non-technical aspects
 - Legacy
 - User Acceptance
 - Marketing
 - Security Rollouts

Windows

*Int. Secure Systems Lab
Technical University Vienna*

- 88% of all (desktop) computers run Windows.
 - Where does this number come from?
 - Why would I care?
 - When dealing with security issues, it is important to have knowledge of Windows.
 - Windows is the best example of a non-open source system and security issues.
 - Poll?
- Windows security is always in the news (major virus, worm and trojan outbreaks recently were on Windows). Why?
- Seeing the need, Microsoft finally started a major initiative for security a couple of years ago
 - It's not as bad as it used to be
 - < XP = lost cause

Code size (Windows vs. Linux vs. MAC OS)

*Int. Secure Systems Lab
Technical University Vienna*

Year	Microsoft	Linux	MAC OS
1981	DOS 1.0 (4k)	-	-
1984	Win 1.0x	-	1
1991	Win 3.0	-	7
1993	Win 3.11 (9M)	Debian	7.1
1996	Win NT 4.0 (16M)	Caldera	7.6
2000	2000 (30M)	Redhat (17M)	9.0
2001	XP (45M)	RedHat 7.1 (30M)	10.0
2004	Server 2003 (50M)	Ubuntu 4.1	10.3 (80M)
2008	Vista (~60M)	Ubuntu eee	10.6
2011	7 (? Said to be less)	Kernel 2.6.35(14M)	10.7 (~89 M)

So which OS is the best?

*Int. Secure Systems Lab
Technical University Vienna*

Feature	Windows	MacOS	Linux
Stack ASLR	Vista	Snow Leopard	(2.4) 2.6
Libs/mmap ASLR	Vista	Lion	(2.4) 2.6
NX page flag	XP (SP2)	Leopard (X64)	< 2.6
EFS	XP (NTFS+SP3)	10.4	2.6
Moderately critical security patches	1 (7) 5 (XP)	1 (10.6)	0
Usable by „normal“ people	95? ME?	Mac OS 1.0	Ubuntu
Swallows Office Documents	Yes	Yes	No

The admin-legacy

Int. Secure Systems Lab
Technical University Vienna

- Working as non-administrator (“Great” idea ;-))
 - Default configuration on Windows system = admin!
 - Principle of *least privilege*
 - Administrator command shell using **runas.exe** (i.e., su -)
 - Store configuration and user information under
 \HKEY_CURRENT_USER
 - Run services under a restricted user (locking down)
 - Take care in giving debugging privileges when creating applications
- *I Love You* and *Nimda* would not have worked if computer did not run as **admin**.

Security @ Microsoft

*Int. Secure Systems Lab
Technical University Vienna*

- Trustworthy Computing
 - Windows security push
 - Lead for improved security
- What is it?
 - Training, code reviews
 - Threat models and security testing
- SD3 Security Framework
 - Mind setting
 - Principles to adhere strictly
 - Secure by Design
 - Secure by Default
 - Secure in Deployment

Update Policy

Int. Secure Systems Lab
Technical University Vienna

- Hotfix
 - Single issue / small number of issues
- Security rollup package (Patch day, 2nd Tuesday)
 - Single package
 - Multiple hotfixes
- Service pack
 - Major updates
 - Cumulative set of previous updates
 - (optional) Previously *unannounced* fixes
 - (optional) Feature changes
- Major problem: Often rebooting is **required!**
 - Most admins reboot
 - Linux Servers: Once a month (“necessary” only after kernel upgrade)
 - Windows Servers: Twice a month

Spyware

Spyware

*Int. Secure Systems Lab
Technical University Vienna*

- Any software that monitors and collects information about a user in a covert and unsolicited manner
- Goal of spyware
 - collect sensitive user information and surfing habits
- Task of spyware
 - component must monitor user behavior
 - component must leak information to environment (OS, network)
- Often implemented as browser extensions
 - Internet Explorer Browser Helper Object (BHO)
 - COM object that can hook into Microsoft's Internet Explorer
 - monitor/modify events
 - Plugins in Firefox

Spyware

*Int. Secure Systems Lab
Technical University Vienna*

- Interaction
 - between browser and spyware component
 - COM function invocations (exported by Internet Explorer)
 - between spyware component and operating system
 - Windows API calls
- In addition, it typically has a real company behind it that is making money from the information gathered
 - Adware is any software that injects unsolicited advertisements into a user's workspace
 - Scumware is a specific type of Adware that hides other advertisements with those from its own controlling source

Spyware

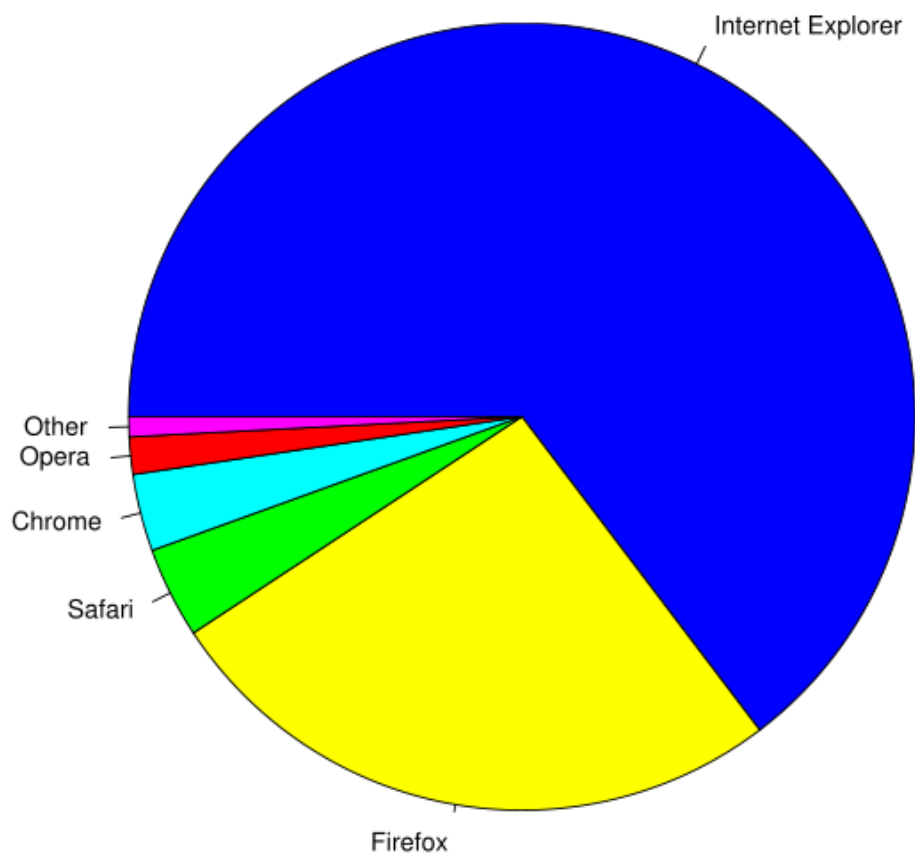
Typical routes of infection:

1. spyware is bundled with legitimate software package
 - end-user license agreement (EULA) even informs about this fact
 - EULA is very long (often hundreds of pages), user accepts without reading
 - Sidebars / Toolbars
 - classic examples are shareware programs
 - P2P file-sharing clients, torrent Downloaders (e.g., Kazaa)
2. “drive-by” downloads
 - exploit browser bug, in particular, vulnerabilities of Internet Explorer
 - WMF (Windows meta file) exploit, around Christmas 2005
 - Bank of India (2007)
 - insufficient ActiveX security settings
3. fake dialogs
 - display “Would you like to optimize your Internet” and perform installation when user agrees

Browser statistics (2009)

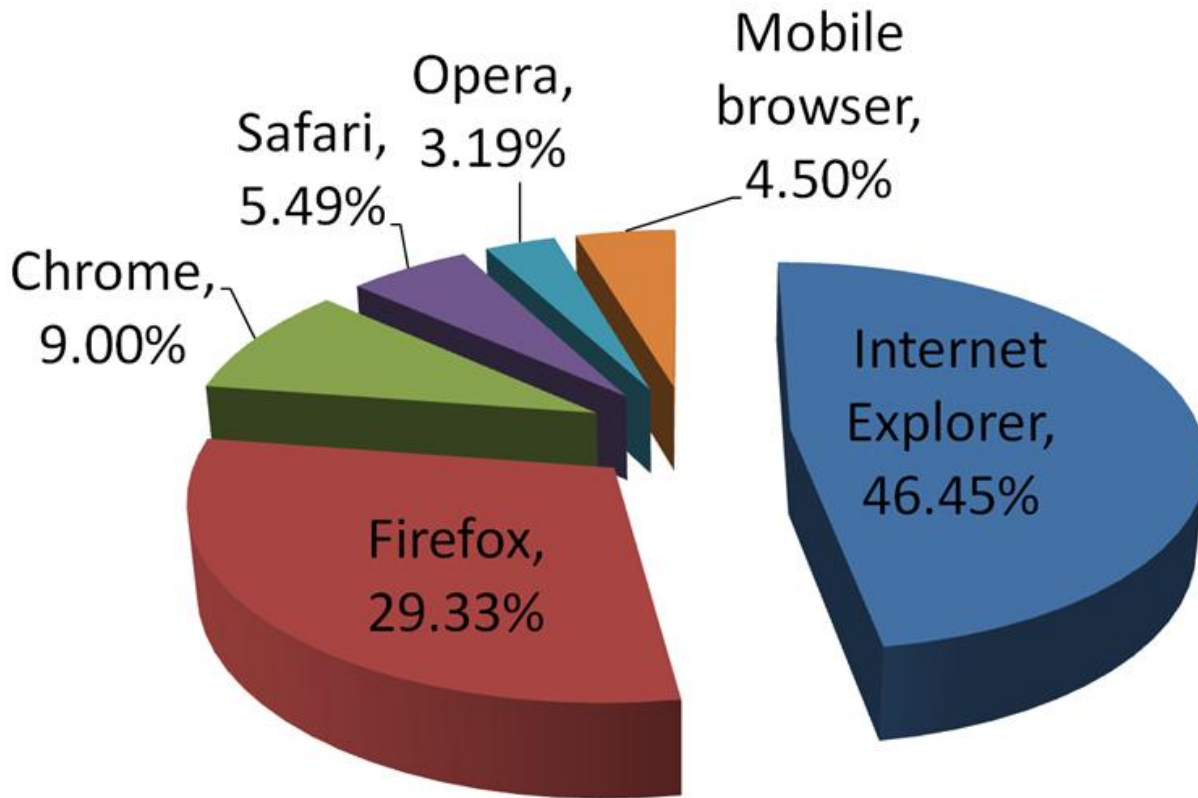
*Int. Secure Systems Lab
Technical University Vienna*

Usage share of web browsers: September 2009



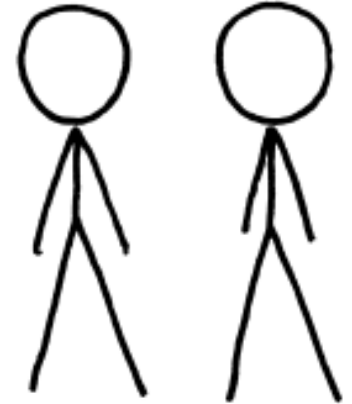
Browser statistics (2010)

Int. Secure Systems Lab
Technical University Vienna



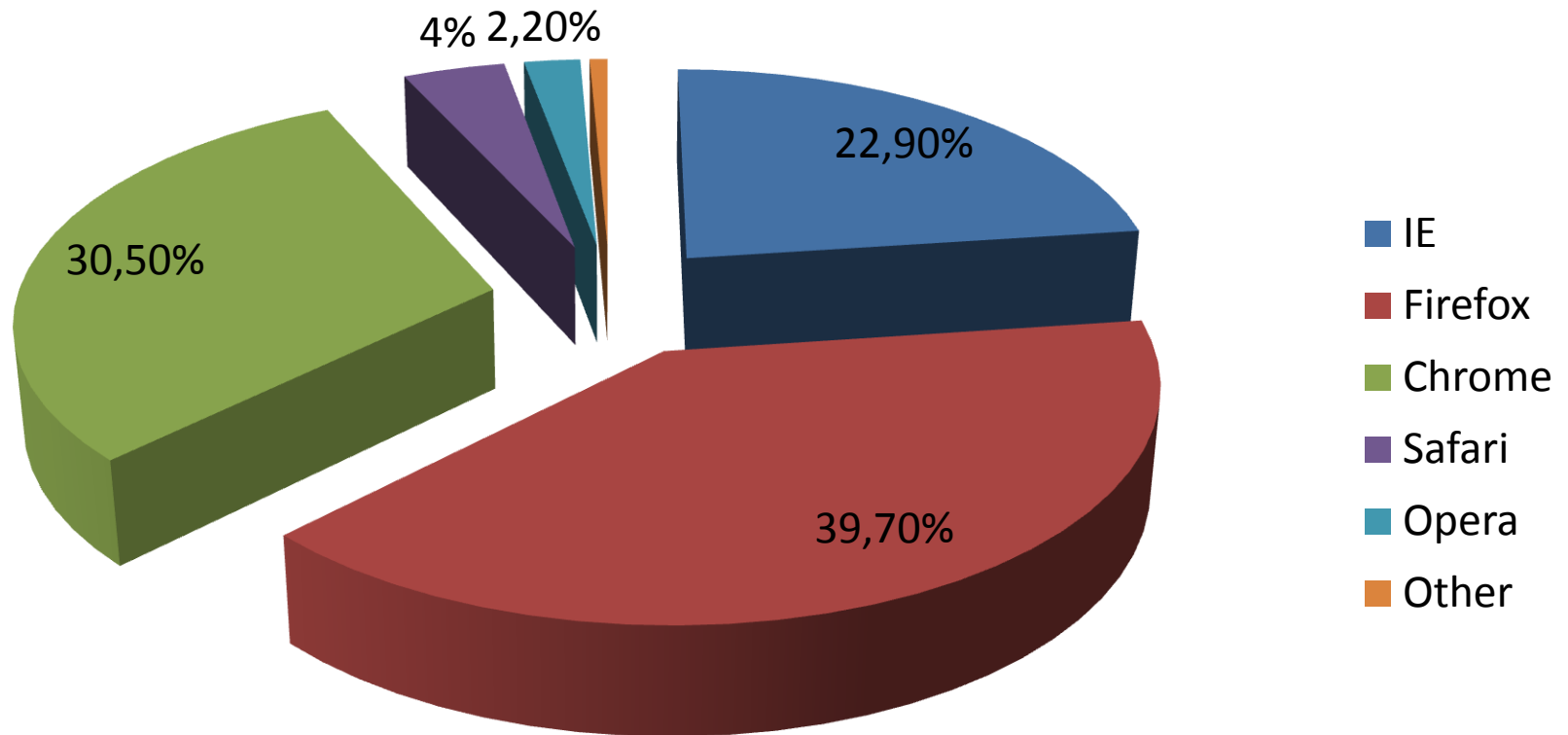
I'M A MAC
|
AND SINCE YOU DO
EVERYTHING THROUGH
A BROWSER NOW, WE'RE
PRETTY INDISTINGUISHABLE.

AND I'M
A PC.
|
AND SINCE YOU DO
EVERYTHING THROUGH
A BROWSER NOW, WE'RE
PRETTY INDISTINGUISHABLE.



Browser statistics (2011)

Int. Secure Systems Lab
Technical University Vienna



Spyware

Int. Secure Systems Lab
Technical University Vienna

- Spyware is becoming a major security issue
 - Analysis performed by Webroot and Earthlink showed that a large portion of Internet-connected computers are infected with spyware (... Windows problem?)
 - Spyware tends to monitor the behavior of users and steal private information (profit, targeted advertisement, etc.)
 - Antispyware programs: Booming business... but how effective?
 - Just like virus/worm detectors, they use signatures
 - Malware needs to be *known*

Spyware

- Spyware authors have many options when it comes to looking for good vantage points
 - Layered Service Providers (LSPs) sit between Winsock and the Base Service Provider
 - E.g., filter network traffic, intercept user data / actions, etc.
 - Legitimate use: Parental control, Web content filtering
 - Browser Helper Objects (BHOs) i.e., plug-ins and Toolbars for IE seem to be the most popular spyware implementation techniques
 - A study showed that of 120 samples, 90 had BHO architecture
 - The Netbanking example

Component Object Model

Int. Secure Systems Lab
Technical University Vienna

- COM is a binary standard realized by Microsoft to enable a component-based market
 - Every COM object is derived from a set of interfaces
 - All COM interfaces have as their root interface *IUnknown*
 - *IUnknown* contains a function called *QueryInterface()*
 - Using this function, one can query for implemented interfaces and get a pointer to them
 - *QueryInterface()* enables the discovery of capabilities

Browser Helper Objects (BHOs)

Int. Secure Systems Lab
Technical University Vienna

- A BHO is in essence...
 - ... a simple Component Object Model (*DLL*) object that implements the *IObjectWithSite* interface.
 - IE will load all registered BHOs (that are COM servers) when it starts. It does this by looking at the Class Identifiers (CLSIDs) under
 - *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects*
 - The *IObjectWithSite* interface has a function called *SetSite()*
 - When IE is started, it instantiates the BHO and calls *SetSite* with a pointer to itself.
 - BHO has access to functions and pointers in IE (e.g., open a new window, etc.)

Browser Helper Objects (BHOs)

Int. Secure Systems Lab
Technical University Vienna

- A BHO can “listen” to events fired by IE such as *Before Navigate*, *Navigate Complete*, *New Window*, etc.
 - The events of interest are defined in the interface *IWebBrowser2* (check the MS documentation)
 - That’s why BHO’s / Plugins are dangerous
 - Useful for Honeypots
 - Imitate IE and gather data

Useful Spyware Tools

*Int. Secure Systems Lab
Technical University Vienna*

- HijackThis (www.hijackthis.de)
 - Low-level tool, very useful in doing research as well as removal
- Spybot, Adware: Freeware tools
 - Signature based so they do not catch all spyware
 - We currently have a project where we crawl the web and test how effective signature-based solutions are
 - Codename: FIRE

Conclusion

*Int. Secure Systems Lab
Technical University Vienna*

- Browsers are an attackers main target!
 - Strong Anti-IE tendency
 - Underlying OS does not necessarily matter
 - Example: Bank transactions
 - Once infiltrated, shellcode can be written for any platform
- OS dependency starts to disappear
- Protection?
 - Use the least popular Browser
 - User the least popular OS 😊