

Attribution 3.0 Unported

- You are free:
 - to Share — to copy, distribute and transmit the work
 - to Remix — to adapt the work
- Under the following conditions:
 - Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- With the understanding that:
 - Waiver — Any of the above conditions can be waived if you get permission from the copyright holder.
 - Other Rights — In no way are any of the following rights affected by the license:
 - Your fair dealing or [fair use](#) rights;
 - The author's [moral rights](#);
 - Rights other persons may have either in the work itself or in how the work is used, such as [publicity](#) or privacy rights.
- Notice — For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to [this web page](#).

Everything You Know About Client Security is Wrong

Or: What it Would Take to Build a Secure OS
That Even Our Parents Could Use

By: Michiel de Bruijn <mdb@x42.net>

Slides: <http://x42.net/DFN-CERT/ClientSecurity2010.ppt>
(also available in slightly-less-evil PDF format)

Security By The Book...

- Traditional client security solutions are designed to contain “outsider” threats
 - Everyone knows you need firewalls, least-privilege ACLs and, on Windows, antivirus software to “keep the bad guys out”
- Virtually every PC these days, especially in corporations, is protected by all of these measures
- Pretty much every home PC sold with Windows Vista or Windows 7 includes these measures out-of-the-box

...But The Books Are Wrong

- Just about every one of those corporations has multiple security crises every year (e-mail virus outbreaks, worm infestations)
- Consumers suffer even more: many home PCs are pretty much unusable because of malware

Yeah, Microsoft Sure Sucks

- “Everyone knows” this is all Microsoft’s fault
 - Insecure default configuration (especially prior to XP Service Pack 2)
 - Bad security model (root for everyone!)
 - Bugs, bugs and more bugs
 - Slow to respond to security issues (they knew about the “Google hack” IE bug *last year already!*)
 - Closed source, evil, blah...

...But So Do These Guys

• Cisco	US\$	36 100 M
• Check Point	US\$	924 M
• Computer Associates	US\$	4 271 M
• F-Secure	€	125 M
• McAfee	US\$	1 600 M
• Symantec	US\$	6 223 M
• Sophos	US\$	270 M

FY2009 (2008 for McAfee) revenue, as reported by company

Antivirus: a Multi-Billion-Dollar Failure

- Antivirus is prime example of addiction to an ineffective security solution
 - When daily antivirus updates don't work, demand *hourly* updates
 - Still, trivial worm variants paralyze entire corporate networks
 - Yet, everyone continues to buy *more* antivirus software
 - To the point of buying *multiple* antivirus engines
 - The fact that all arms races have a point of diminishing returns shouldn't come as a surprise: see history, evolution theory, etc.
 - Adding insult to injury, innovative new security solutions repeatedly fail in the market, due to not being antivirus-like enough

Security Through, Eh, Insecurity?

- Security software increases the complexity of systems, and thus the attack surface
 - Buffer overflows: All CA antivirus software
 - DoS: Cisco Security Agent
 - Much, much worse in not-so-well-known software
- Old trend: malware exploiting bugs in security software
 - Witty worm (ISS firewall)
- New trend: fake security software
 - Making victims pay actual cash for being exploited: priceless
 - Prediction: before the end of this year, at least one government organization somewhere **will** standardize on “XP Antivirus 2010”

Ineffectiveness All Around

- Apparently, more than US\$ 10 billion in combined annual revenue can't fix Microsoft's screw-ups. In fact, it often makes things worse
- The most measurable thing that “creating awareness” with consumers has achieved, is leading to an entirely new threat: fake security products
- OK, so we need to go open source: which free software package do I download to secure my Windows box?
- Is Windows so utterly broken that no third-party product can fix it?

Switch To Linux! Or OS X! Or *Anything*, Really!

- Even *OpenBSD* users can:
 - Download a file from the Internet
 - Execute it
 - Send outbound mail using SMTP. Or emit lots and lots of TCP/UDP packets. Or display a bunch of ads
 - Modify user-specific profile/startup files
- In short, OpenBSD could host most of the functionality of today's Windows-based malware
- Also: Both Windows 95 and NT 4.0, a year after their respective releases, weren't targeted by many viruses, and spyware had barely been invented at the time

So, What Happened?

- Really severe security problems are caused by those who profit from them
 - \$0.10 per infected PC
 - Much more for fake security products
- Market economics dictate that the most widely deployed platform will get targeted first
- And yes, Windows *is* trivial to exploit
 - However, that's a bonus, not a root cause
 - Many security-related issues (spam, Nigerian/lottery scams) would continue to flourish if Windows were to disappear from the face of the earth overnight

Exploits are Big Business

03-08-2009, 11:05

Exmanoize Offline
Junior Member

Hello!
I present new actual russian exploits pack "**Eleonore Exp v1.2**"

Exploits on pack:

- > MDAC
- > MS009-02
- > Telnet - Opera
- > Font tags - FireFox
- > PDF collab.getIcon
- > PDF Util.Printf
- > PDF collab.collectEmailInfo
- > **DirectX DirectShow**
- > **Spreadsheet**

installs on traffic:

- > on usa: **5-15%**
- > on mix: **10-25%**

[size=1]* Piercing indicates approximate, may vary and depends directly on the type and quality of traffic. size]

Price:

- > Eleonore Exp Pack 1.2 = 700\$
- > Cleans cryptor on AV = 50\$
- > Rebid on another domain = 50\$

* PACK is binding on domain.

- > Eleonore Exp Pack 1.2 with not binding domain(free on domain) = 1500\$

Who Needs Exploits Anyway?

“The trade in rogue anti-virus applications can make top-tier distributors an estimated \$1.2m a year, net security firm Symantec estimates.

A study by Symantec into the psychology of the scam found that 93 per cent of users deliberately downloaded and installed scareware packages, albeit without realizing what they were getting for their money.”

- The Register, October 20th 2009.

But My Linux Box is Secure!

- My Windows laptop is secure enough as well
 - Despite not running any antivirus or antispyware, and reluctantly running a firewall
- Fact is: you and I are not the problem
 - Getting *our* “Internet driving license” would be easy
- “Typical” consumers and “average” corporate users are not so lucky, though
 - Exploiting their mistakes is very profitable for large groups of relatively unskilled attackers
 - Before switching them all to Linux, we better make sure that this would actually solve the issue

Solving the Right Problem

- There is more to security than “use anything other than Microsoft products”
 - Sure, switching from IE to Firefox will make you safer for a while
 - So will forgetting English and switching to Esperanto. (Ever seen phishing mails in *that* language?)
 - Fact is, the mainstream platform will always be most attractive to subvert
 - Sendmail is probably the earliest example of that
 - “Bug free” is not achievable: any non-trivial platform will always have a popular exploitable service or application
 - “Fixing bugs faster” also doesn’t work: see “antivirus industry”...

Solving the Problem Right

- New security paradigm: “keep the insider safe”
 - Or, less respectfully: “solve the naive user problem”
- Requires new approaches in areas where current solutions have failed
 - Limiting execution and impact of malware
 - “Building a secure OS that even our parents could use”
(although implementation on top of an existing OS would be preferable)
 - Preventing information disclosure to unauthorized parties
 - Left as an exercise for the reader (since it involves fixing PKI, credit cards, the government and a few other things...)

Avoiding Past Mistakes

- The strict appliance model
 - Dozens of startups have offered simple boxes for “just browsing, Internet and IM”. There is a reason none of these startups are still around today...
- Central management and/or control
 - Variation 1, “take away all user rights – we’ll decide what’s good for you”, is a solved problem for corporate environments, but doesn’t scale past that
 - Variation 2, “system call policies for untrusted code” has significant issues even in a closed corporate environment

Avoiding Past Mistakes (2)

- Asking users to make security decisions
 - Early (and quite fundamental) failure: SSL
 - Did you click the lock icon? Verified the hostname, organization and issuer's statement? *Well, did you, punk?*
 - Continuing that trend: consumer firewalls
 - Taskhost.exe would like to connect to 198.81.129.125 on TCP port 2374. Allow or deny?
 - Hopefully the final word: UAC in Windows Vista
 - Likely the first security feature to feature in MBA case studies... (so, just maybe, 5 years from now, applications will finally stop asking users questions they can't answer)

Recognizing Value in Current Solutions

- Successful (and profitable!) semi-appliances with central software management aspects: Apple iPhone/iPod and Microsoft Xbox 360
 - Not true general-purpose computing, in that all applications need to be approved by the manufacturer
 - Good security record: the iTunes App Store and Xbox LIVE have not offered malware even once
 - Lots of grumbling, though, from developers, content owners and consumers alike
 - As with PKI, it's unlikely that a central authority can be established which will satisfy all legitimate needs in a scalable manner

Positive Appliance Features

- Quick restart to solve “weirdness”
- Worst-case failure mode is that the OS reverts to factory defaults
- User-installed programs as well as data and preferences can be found and moved (backed up/restored) easily
 - To another PC or “the Cloud”
- Good user experience and enhanced security go hand in hand here
 - Especially when combined with a reliable versioning file system (automatic backup)

And a Few Deal Breakers

- Requirement for all software to be centrally approved
 - Stringent policy-based QA is key to the whole user experience and security of the system
 - “Single authority” or “benevolent dictatorship” model won’t scale, especially not past cultural boundaries
 - Multiple, localized, peer-to-peer authorities?
- (Mandatory) updates often degrade user experience
 - Partial solution: previous versions are kept, along with data and preferences at time of upgrade, to allow easy rollback

Rethinking the App Install Process

- Two fundamental truths of application installations:
 - Consumers will, no matter what happens, always want to be in control of what runs on their machine
 - “Jailbreaks” will occur under even the most liberal application approval policies: we can only strive to discourage these as much as possible
 - Developers will abuse any deployment mechanism we can come up with
 - Incompetence
 - Malice
 - Marketing departments (*yes, Adobe and HP, I am talking about you here*)

Rethinking the App Install process (2)

- Logical solution: applications should be *completely* isolated from each other within the user runtime environment
 - To the point of having *application-specific* ACLs on the file system
- Installing software should be a non-privileged operation
 - Shared components: bad. Disk space: cheap
 - Virtual machines (of course Java and .NET, but also VMware, Xen and such) make this technologically feasible
 - Applications are the new data

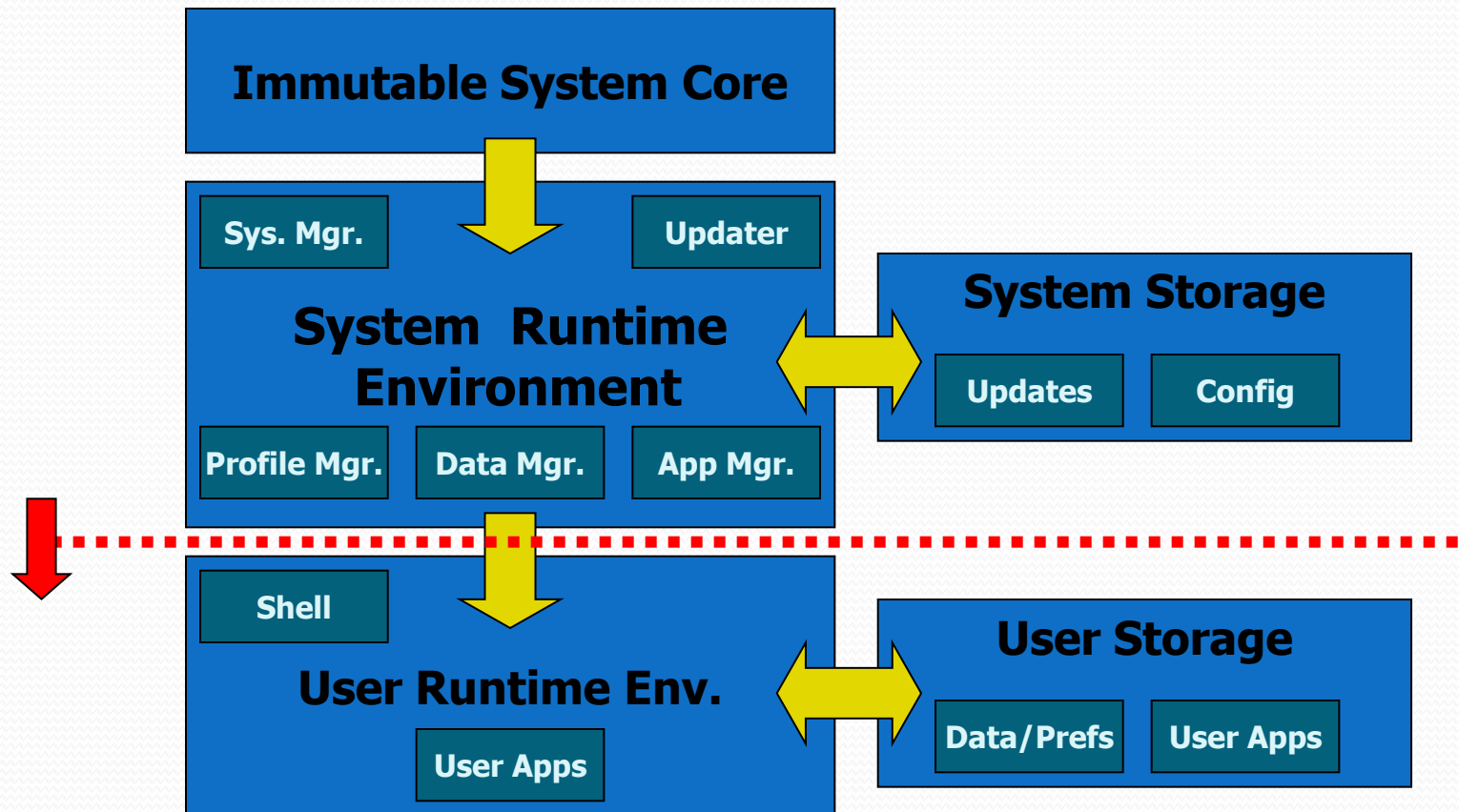
Security Implications of App Isolation

- Impact of misbehaving applications on the system is minimal
 - Newly installed apps have no access to existing data
- Difficult to exploit other applications
 - Apps that *want* another app to extend them, have to explicitly include code for that
- System integration features should be difficult to abuse
 - Well-defined API is key (as well as very, very hard to get right)

Living With Full App Isolation

- Applications display standard security requirements at install time, together with license agreement and privacy statement.
 - Connect anonymously to server X in domain Y for purpose Z
 - Handle files of type X or system wide-event Y
 - Start up automatically
 - Access user data
- All other permissions have to be explicitly granted using a standard OS-supplied interface
 - Includes all authenticated connections
 - Only way to change default file/event handlers
 - Easily enable/disable auto-start items

The Technology Picture So Far



So, Where Do I Buy This OS?

- Not in any Microsoft store, that's for sure...
 - But, alas, nowhere in Linux land either
 - Apple comes close, but only due to non-scalable and ultimately unacceptable policies
- At best, it's an interesting research project
 - Could be built upon many existing OS kernels and userland components
 - Opportunities for fundamental security research
- Truth is, even with increasing awareness, fundamental changes are very hard to make in the marketplace
 - Also see: IPv6

Interesting Open Issues

- Permission description language for applications
 - Which network, file system and shared resource access is required?
 - For which purpose and with which constraints?
 - API follows more or less directly from this
 - UI is a more important aspect: how to manage exceptions?
- Application-specific file system ACLs
- System-wide user data manager with versioning
 - Keeping applications up-to-date is just a special case here

Interesting Open Issues (2)

- Making some very common use cases safe
 - Installing a driver for a all-in-one printer/scanner device
 - Peer-to-peer file sharing
 - Corporate VPN access with admission control
- Extending security permissions beyond the local machine
 - Moving users back from their walled gardens to a more e-mail like mechanism?
 - Possibly even making e-banking truly safe?

Questions?

Michiel de Bruijn <mdb@x42.net>

Slides: <http://x42.net/DFN-CERT/ClientSecurity2010.pdf>