Madison Gurkha
Your Security is Our Business

Attacking is easy,
defending is hard

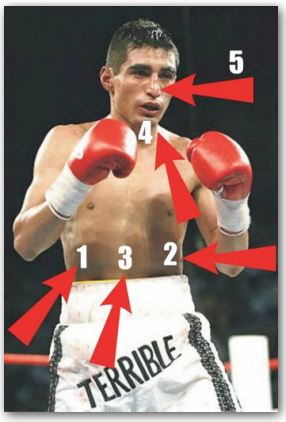
ir. Walter Belgers, CISSP, CISA

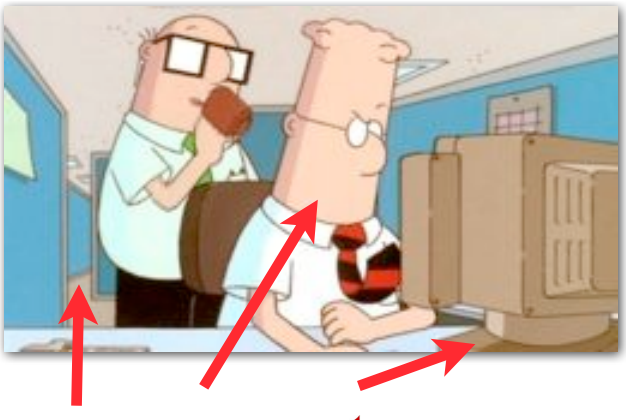
Walter Belgers

- Principal Security Consultant and Partner at Madison Gurkha B.V.
- Has been working in the IT security field for over 16 years

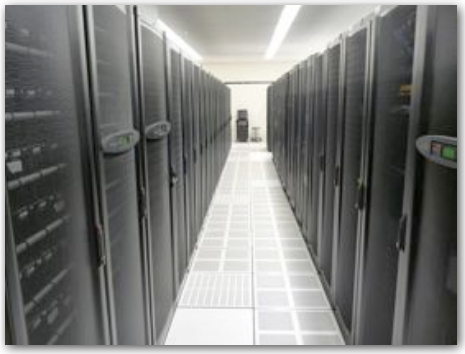
Madison Gurkha
Your Security is Our Business

- Madison Gurkha supports organisations with high quality services to efficiently identify, decrease and prevent IT security risks
  - With a focus on *technical* security aspects





Physical layer



Physical layer

Physical layer

Solutions

- Have a policy for physical security
- Don't buy locks from the local hardware store

Software

- Firmware
- Operating system
- COTS Add-on packages (backup software, database, web server)
- Homebrew applications (web application)

Firmware

- Override boot sequence using hardware
- Evil Maid attack
- (P)DoS attacks a/k/a "phlashing"

Firmware

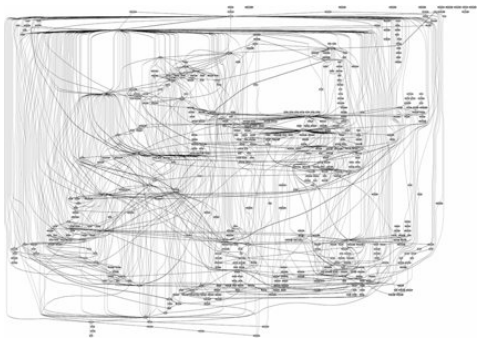
Solutions

- Trust your vendor :-)
- Do not leave your laptop unattended, even if you use (full) disk encryption

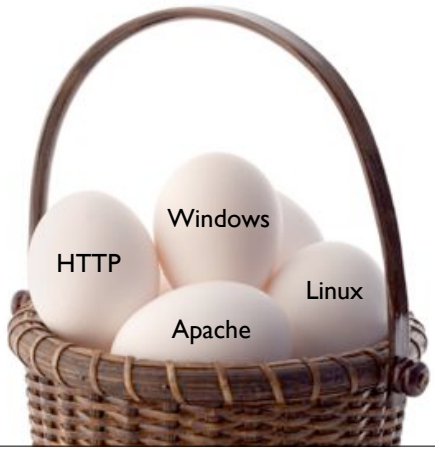
Software

Speed to Market

Complexity



Monoculture

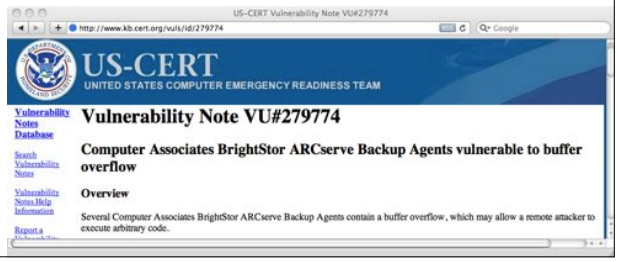


Software

Patching

✓ For OS and some packages: automated

- For many add-on packages: not automated



Patching

- For homebrew software: ???
- Security audits

Patching

- Lot of work: test, accept, production cycle
- Dependency on specific version
- High costs when updates cause downtime


Microsoft: Pirated Windows 7 Will Still Get Updates

http://www.tomshardware.com/news/windows-pirate

Google

Microsoft: Pirated Windows 7 Will Still Get Updates

2:21 PM - April 29, 2009 by Marcus Yam - source: Tom's Hardware US

Even Windows pirates get the security support from Microsoft.

Microsoft earlier this week clarified that all versions of Windows, both legitimate and illegitimate, receive security updates – and that policy will carry over to Windows 7.

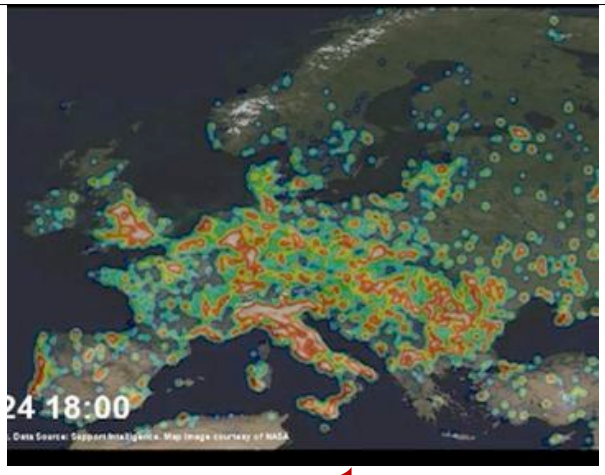
"There seems to be a myth that Microsoft limits security updates to genuine Windows users," wrote Microsoft's Paul Cooke, who works in Windows Client Enterprise Security. "Let me be clear: all security updates go to all users."

"Not only do all security updates go to all users' systems, but non-genuine Windows systems are able to install service packs, update rollups, and important reliability and application compatibility updates," Cooke continued in the blog entry. "In addition, the users of non-genuine Windows systems can also upgrade a lot of the other software on their computer. For example Internet Explorer 8 has numerous security- oriented features and improvements, and it is available to all users."

That's not to say that non-genuine copies of Windows are allowed to run completely free. Certain updates and software may be blocked at Microsoft's discretion, such as value-adding updates and non-security-related software.

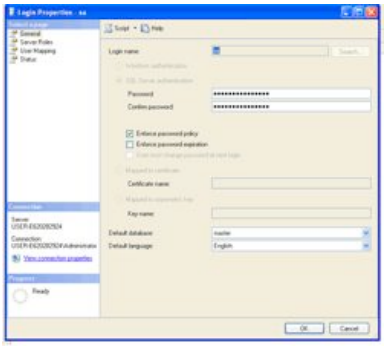
Zoom

Loading "http://www.tomshardware.com/news/windows-pirat...rity-patches,7666.html", completed 125 of 127 items (1 error)



www.team-cymru.org

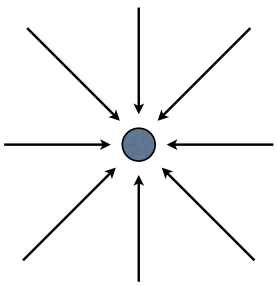
A6 Security Misconfiguration

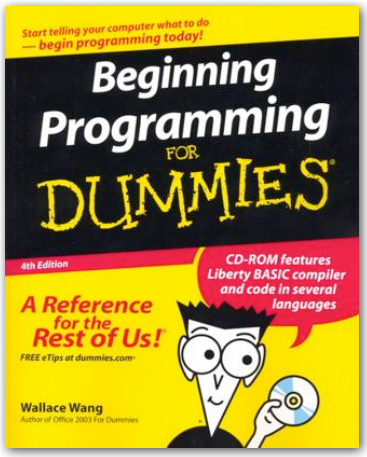


Hardening

- Installation ≠ Configuration
  - Almost always overlooked
- Default deny
  - Users, file permissions, installed software, configuration settings regarding functionality

Homebrew software





OWASP Top 10 – 2010 (New)
A1 – Injection
A2 – Cross-Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross-Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
A10 – Unvalidated Redirects and Forwards (NEW)

www.owasp.org

Solutions (technical)

- Deny all, except (safe installation/*hardening*)
- Separation of duties/modular approach
- Restrict permissions
- Simplicity/ergonomics

Solutions (other)

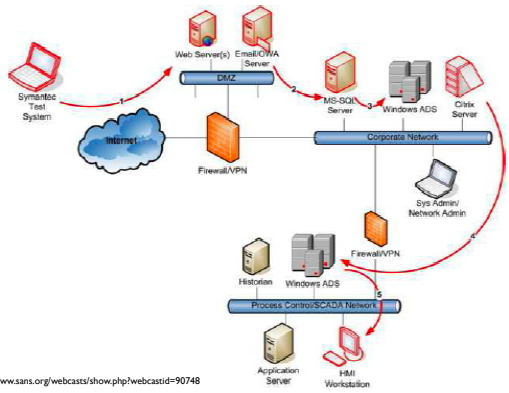
- Functional requirements ***and*** security requirements
  - Also for 3rd party software
- Use cases ***and*** abuse cases
- Educate programmers in secure programming
- Security testing

Other things to do

- *If All Else Fails... (and it will)*
- Multiple layers of defense (prevention)
- Logging and monitoring (detection)
- Have a plan ready (reaction)

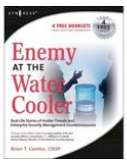
Insider attacks

- A malicious person becoming an insider
  - Physically
    - Burglary
  - Logically
    - Hacking



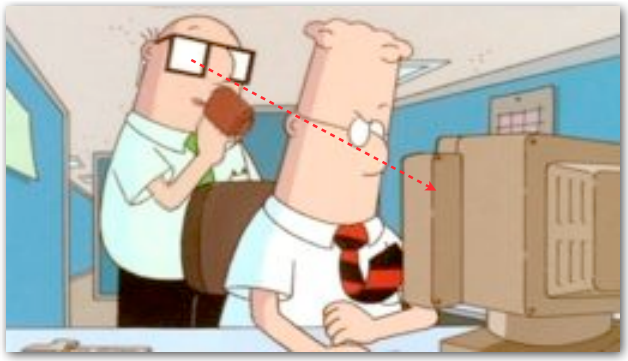
http://www.sans.org/webcasts/show.php?webcastid=90748

Insider attacks



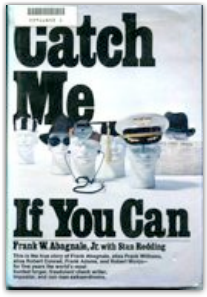
- Malicious insiders

- Insiders being (unknowingly) abused by outsiders



Insider attacks

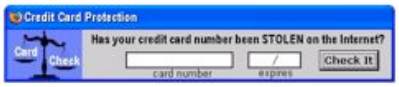
- Active
  - Social Engineering
  - Phishing
- Passive
  - Drive-by hacking



Belastingdienst doet 'dom' met USB-stick

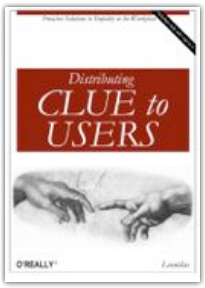
24 jun 09 - Door Karel Ornstein en Guido van Ophoven

Medewerkers van ING, de Belastingdienst, het AMC, de PvdA, SP, de Marokkaanse ambassade en tal van andere organisaties hebben zonder nadenken een gevonden USB-stick in de bedrijfscomputer gestopt.



Educating users

- A process, not just an awareness session

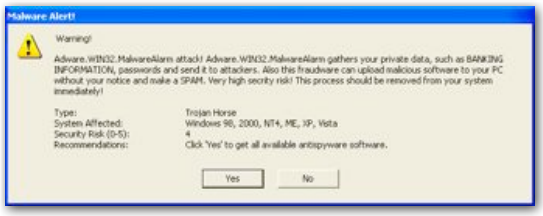


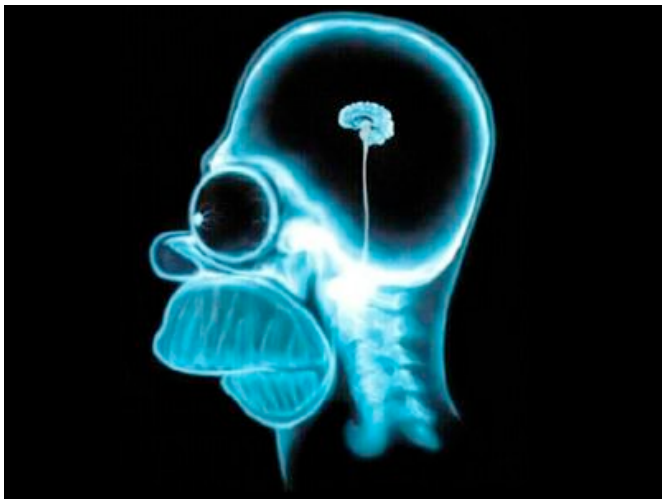
Attack vectors

- Browser plugins
- Screensaver, picture in an email
- Codec to play a clip
- P2P-software
- Anti-malware


Security Warning
Do you want to install and run "[after accepting our agreements] PrecisionTime/DateManager, free 10 second GAIN ad-supported downloads that display 3) exact time/date, and [2] GAIN branded ads selected based on websites you view? Click here to read our agreements. Click Yes to accept" signed on 10/20/2003 12:18 PM and distributed by:
The Gator Corporation
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001.4 CA
Caution: The Gator Corporation asserts that this content is safe. You should only install/view this content if you trust The Gator Corporation to make that assertion.
Always trust content from The Gator Corporation
Yes
No
More Info


FoistAntiSpyware
Spyware has been detected on your computer. Run our free scan now!
Stop Spyware Now
9 out of 10 computers are infected with spyware!
There is a good chance you are one of them!
Scan Now
Is this happening to you?


Malware Alert!
Warning!
Adware.WIN32.MalwareAlarm attack! Adware.WIN32.MalwareAlarm gathers your private data, such as BANKING INFORMATION, passwords and send it to attackers. Also this fraudware can upload malicious software to your PC without your notice and make a SPAM. Very high security risk! This process should be removed from your system immediately!
Type: Trojan Horse
System Affected: Windows 98, 2000, NT4, ME, XP, Vista
Security Risk (0-5): 4
Recommendations: Click 'Yes' to get all available antispyware software.
Yes
No




Pas op. Aardig

Solutions

- Find all known risks and act on them
- Fix bugs on all systems for all software
- Keep doing this
- Do secure installations (configurations)
- Embed security in the devpt process
- Educate and screen users and keep on doing this
- Monitor and be ready

walter@madison-gurkha.com