

The Frugal CSO



IT Security Tools for Tough Times

A presentation to ISSA Ottawa Chapter
January 28 2010 by Derrick Webber

Topics

- Saving money: fashionable again
- Flood of talent and tools
- New economic models
- Frugal security tools
- Methodologies for evaluating inexpensive software
- Where to find frugal tools

About the speaker

Derrick Webber, CISSP, GCIH, GSNA

- IT security consultant with a systems and network background.
- First commercial Linux deployment in 1997 for an ISP – web servers, firewalls, monitoring, databases... the works.
- Implemented Linux and other free software solutions for many private and public sector clients, including e-commerce startups.
- Deployed frugal security solutions to meet client objectives (e.g. MITS, PCI DSS) despite budget restrictions.
- I'm not an Open Source zealot.... I'm just cheap ☺

Thrifty Giants



Amazon.com

- 2008: \$19.16 Billion in sales
- Famously frugal from the beginning...



Amazon.com

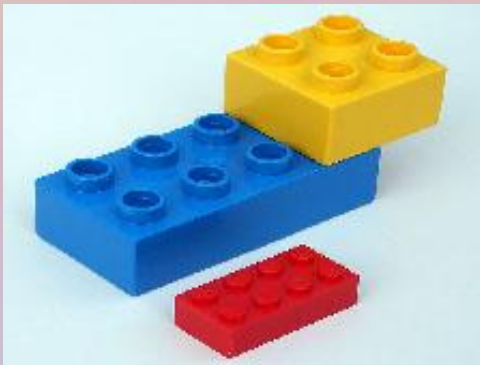
Famously frugal today:

- 2009: disabled the lights in cafeteria vending machines.
- Saves \$20,000 / year



Google

- First storage server chassis built from Duplo blocks (Lego)



Saving money: fashionable again

- Worldwide recession
- Canadian Government cutbacks
- Directors need to justify expensive security software
 - Focus on compliance: SOX, PCI, etc.
 - Little money left for anything else
- A maturing industry
 - Security is not black magic anymore

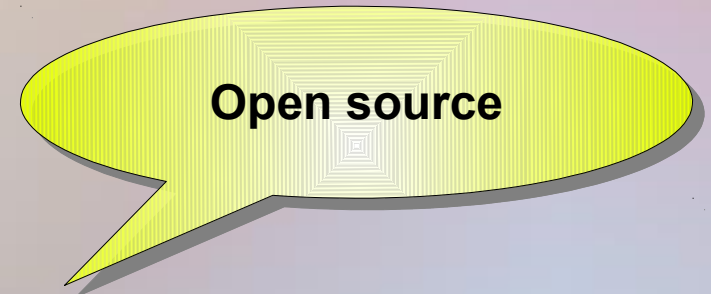
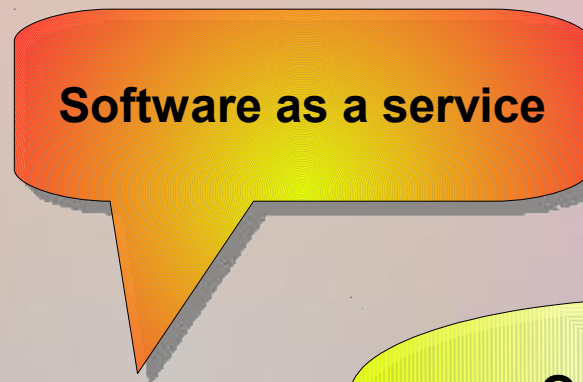
There is a returning appreciation of **thrift**

An embarrassment of riches

- The growth of the Internet seen a flood of developer talent, tools and communities.
- Lower barriers to entry:
 - Nearly anyone can afford a computer and Internet
 - Excellent development tools, educational material, helpful communities, all easily accessible
- Security products have matured
 - Basics of firewalls, IDS, anti-virus, network monitoring are well understood to the point they are now nearly commodities.

New revenue models

- Treating software as hardware is not the only sales methodology.
- Greed is not the only possible motivation for human action.



New revenue models

- Software as a service
 - Salesforce.com, WebEx, Postini
- “Freemium”
 - Free limited version, make revenue from payware versions with more functionality (e.g. Splunk)
- No charge software
 - Revenue from support alone (e.g. Untangle, Ubuntu)
- Free (libre) Open Source Software
 - Revenue is not always the primary motivation

Free (libre) Open Source Software



“Software for which the human readable source code is available for use, study, reuse, modification, enhancement and redistribution.”

Free (libre) Open Source Software

- Free as in freedom, not necessarily free of cost
- Not the same as “public domain”
- Usually licensed.
 - Do what you want in-house
 - Often restrictions on incorporating into other products
- Some have dual licenses
 - Commercial license to allow use in closed source projects (e.g. MySQL)

Famous Open Source Projects

- The original Unix
- Linux and BSD
- Java and Solaris
- The Apache Projects
- MySQL and Postgres
- SugarCRM
- Asterisk PBX
- OpenOffice



Open Source, open for business

- Google
 - Approximately 450,000 Linux servers (2006)
- Movie studios
 - Disney, Pixar, Dreamworks, Sony, ILM
 - Use Linux almost exclusively for special effects, servers and desktops. (Avatar too)
- IBM
 - Major Linux focus starting in 1999
 - \$2 billion in Linux services revenue by 2003

Open Source in Government

- Germany
 - Foreign Office: Linux on servers and desktop in 230 embassies. 65% savings
 - Munich: 11,000 Linux desktops by 2011
- France
 - Gendarmerie: Linux on desktops and servers
 - Cut IT budget 70%, saving EU50 million
- US Department of National Defense
 - DoD CIO directive Oct 2009 that Open Source be considered in all procurement (even for classified use)

Fear of Free Software

- If it's free it can't be good (poor quality)!
- Accountability: no one to sue!
- No support!
- Backdoored by China / mafia / my competitors!
- Software patents!
- Giving stuff away is unnatural!

These fears can be overcome by doing a little research.

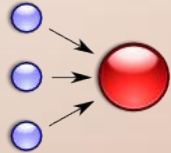
Frugal Security Tools



Frugal Tools

- A sample of the better lower-cost security products
- Selection criteria:
 1. Inexpensive or free
 2. Established track record
 3. Widely deployed
 4. Higher level tools

Tool Categories



Perimeter



Network monitoring

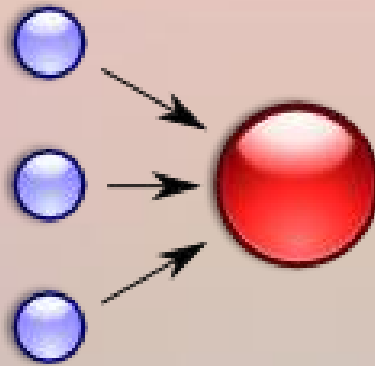


Endpoint protection



Developer security tools

Network perimeter





- “Unified Threat Management” product
 - Firewall
 - Router / QoS
 - Intrusion Prevention
 - VPN
 - Web filter / Email filter / Perimeter antivirus
- Free and payware add-ons (e.g. better filtering and AV)
- Large support industry has developed around it

www.untangle.com



- Another Unified Threat Management product
 - Firewall
 - Intrusion prevention
 - DoS limitation
 - VPN (IPSec, SSL, L2tp, pptp)
 - Software, hardware appliance, virtual appliance versions
- Also have dedicated mail and web gateways
- Low cost but not free



- Intrusion detection / prevention appliance
- Built on open source Snort IDS
- Much better than Snort alone:
 - Automatic rule updates
 - Graphical interface
 - Customizable responses for IPS
- Commercial and free versions
- Hardware and virtual appliance versions

<http://www.stillsecure.com/strataguard>



- Web application firewall
- Rules based. Detection only or IPS mode.
- Installs as a module into the Apache web server
- Apache's proxy mode turns it into a transparent WAF to filter traffic to other web servers
- Engine only: GUIs and rule generator add-ons available to make it into a complete solution.
- Vendor sells non-free hardware appliances that are complete solutions.

www.modsecurity.org

Network Monitoring





- Centralized host intrusion detection
 - Log analysis
 - File integrity
 - Alerting and active response
 - Agent and agentless monitoring
 - Web GUI
- Monitors Linux, Unix, Windows, Mac, VMware
- From Third Brigade, now owned by Trend Micro
- Open Source and free

OSSIM

- Integration of 15 leading open source products:
 - OSSEC (Integrity and event monitor)
 - Snort (Intrusion detection)
 - Nagios (Network availability monitor)
 - NTOP network performance monitor
 - OSC-NG (endpoint inventory)
- Correlation engine for alerting and response
- Incident and response ticketing system
- Reports and analysis



- Centralized log collector and log search engine
- Takes syslog and other log feeds
- Ad hoc event investigations
- Accepts any log format without you first having to write parsers.
- GUI with dashboards, drill-down for investigation
- Free for up to 500MB/day and one server
- Payware version adds unlimited capacity and more features

www.splunk.com

NetWitness Investigator



- Real-time network capture and traffic analysis
- Session level traffic analysis
- Wireshark on steroids
- Freeware version only runs on Windows 2003
- Payware version runs on Linux as well

www.netwitness.com/products/investigator.aspx

System Monitoring

- Many excellent system availability & performance monitoring solutions available:

- **Zenoss**



- **Zabbix**



- **Groundwork**



- Endpoint discovery, availability monitoring and alerting, SLA reporting, dashboards
- Commercial Open Source

Endpoint protection





- Network Access Control (NAC)
- Free and Open Source, commercially supported
- Endpoint vulnerability scanning
- Device isolation and remediation
- Captive portal to restrict network guests
- Protocol blocking (e.g. peer to peer traffic)
- Integrates with Snort IDS
- Wireless access point control

www.packetfence.com



TRUECRYPT

- Real-time encrypted physical or virtual disks
- Full disk encryption
- Cross platform: Windows, Linux, Macintosh
- Plausible deniability
 - “Hidden” encrypted volumes
- Passwords and key files (two factor authentication)
- AES and other algorithms
- Not FIPS accredited.

www.truecrypt.org

Developer tools



Developer libraries

- OWASP Enterprise Security API (ESAPI)
 - Helps guard against security-related design and implementation flaws. Even in existing applications.
 - Java (.Net and PHP versions in beta)
- OWASP AntiSAMy
 - API for sanitizing user HTML/CSS
 - Java, .NET and Python
- PHPIDS
- OWASP Development Guide
 - Practical guide to designing, developing and deploying secure web applications and web services. With code examples.

Evaluating Frugal Software



Wheeler's IRCA

- Developed by David A. Wheeler

http://www.dwheeler.com/oss_fs_eval.html

1. **I**dentify candidates
2. **R**ead existing reviews
3. **C**ompare attributes to requirements
4. **A**nalyze in depth

Identify Candidates

- Research suitable products
 - Search engines (but maybe avoid Bing)
 - Enterprise Open Source Directory
 - www.eosdirectory.com
 - OpenLogic Exchange
 - olex.openlogic.com
 - Icewalkers (Linux products only)
 - icewalkers.com
 - VMware Virtual Appliance Marketplace
 - www.vmware.com/appliances

Read reviews

- Search engines will also find reviews
- EOS Directory and OpenLogic also rate products
- Many “reviews” will be individuals posting to community forums:
 - Good to gauge health, popularity and reputation of frugal products.
 - Official support forums and FAQs can indicate product quality and responsiveness of the developers to bugs.

Compare with requirements

- Briefly compare the leading product's attributes with your functional needs.
- Also compare on
 - Cost (including cost to implement)
 - Market share
 - Support and reliability
 - Scalability and Performance
 - License
 - Interoperability and fit with your infrastructure
- Get down to one or two most promising products

Analyze in depth

- Try the leading candidates first hand.
- Virtualization is your friend
 - Check the VMWare site for an appliance, or a pre-configured version of the OS required.
- Performance test
- Interoperability and security
 - Lock in: how easy to move to something else if the product is abandoned? (same as for proprietary)
- Usability and support
 - Documentation is often inferior

Frugal tricks

- Proprietary vendors will often discount their price to avoid losing a sale (especially to newcomers and OSS).
- Let them know you're evaluating competing products, including frugal products.
- Don't let a big discount lead you into adopting a product that doesn't meet your requirements (all of them).



Conclusion

- Being frugal is now a necessity, and it's trendy.
- Wealth of excellent low cost and free security products available.
- New revenue models = better for you
- Don't fear Open Source.
- Evaluate frugal products much like any other.

Questions?

