

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT

**LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.**

www.theredhatsummit.com

Open Source Software Security in an Insecure World

Josh Bressers

Senior Security Engineer
Red Hat

2010-06-24

SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Closed source software is more secure than Open Source!

Open Source software is more secure than closed source!

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Is Any Software Secure?

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Is anything secure?



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



What does “secure” mean?

- Mitigating Risk
 - You can't eliminate risk, but you can control it
- Providing Trust
- Preparing for the inevitable

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts

-- Gene Spafford

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Security flaws

- **ALL** software has bugs.
- Some of these bugs have security implications.
- Not all software is written equally.



Examples

- Image file that crashes the image viewer?
 - Bug (just don't open it again).
- Image file that zips up your home directory and mails it to the bad guys?
 - Security flaw.
- Crash the computer with a network packet?
 - Security flaw.
- Crash the computer by smashing it with a hammer?
 - Not a security flaw (probably not a bug either).



Why does this matter?

SUMMIT

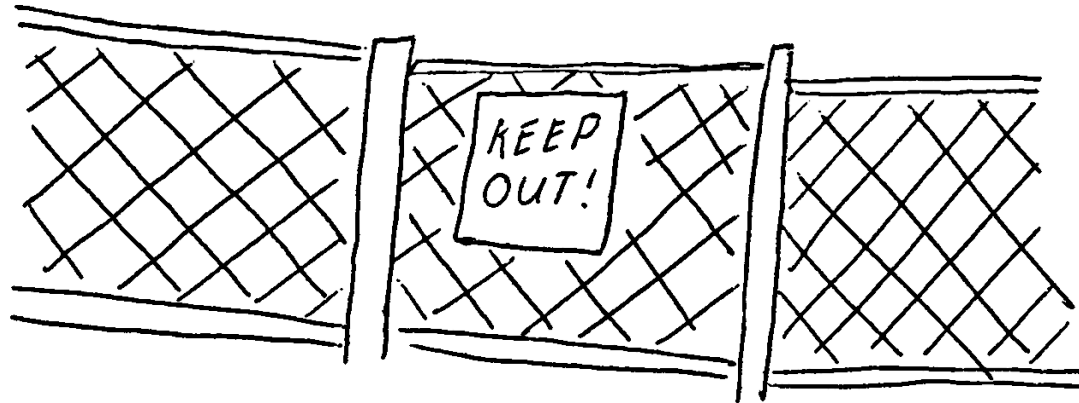
**JBoss
WORLD**

PRESENTED BY RED HAT



Can we trust proprietary software?

- Can you trust your vendor?



SUMMIT

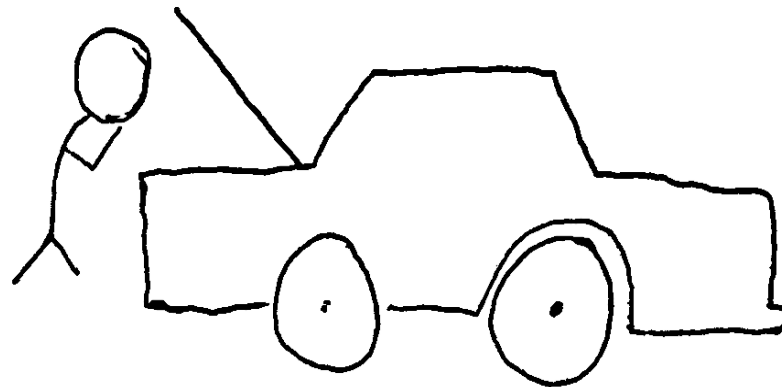
**JBoss
WORLD**

PRESENTED BY RED HAT



Can we trust Open Source?

- OF COURSE!
- You don't have to believe me
 - Let's understand how it works



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Is Open Source Software secure?

- This is the wrong question
- What is being done to minimize risk?

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



The challenge

- Everything has bugs
- How does Open Source handle security bugs?

SUMMIT

**JBoss
WORLD**

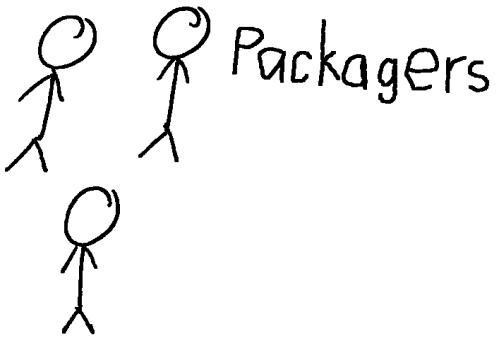
PRESENTED BY RED HAT



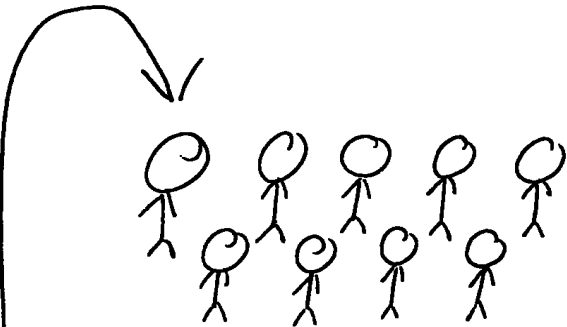
ONE USER



Report
bug to
Fedora



Packagers

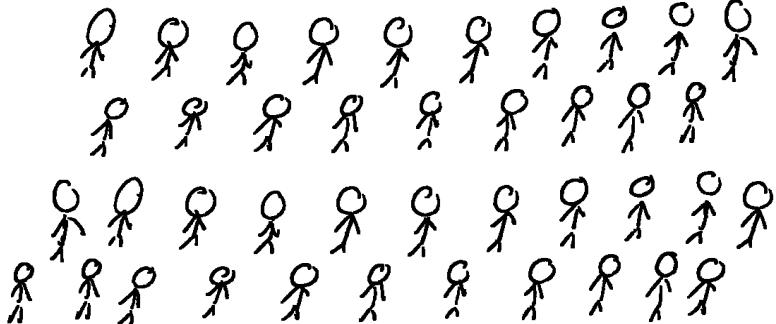


Upstream

OH HEY
THIS COULD BE
A SECURITY
ISSUE!



CERT/vendor-sec
OSS-security



SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



Can we prove something is secure?

- Do you trust your vendor?
- Does your vendor trust their vendors?
- You can't prove a negative
“This software has no security flaws”



What can we do?

- Look at the source
 - Probably expensive
 - You don't have to do this alone
 - Many others are already doing this

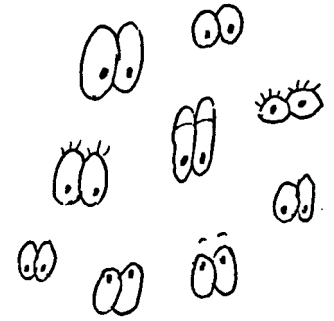
SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Power in numbers



- Linus' Law
 - Given enough eyeballs, all bugs are shallow
- Even critics can produce positive outcomes

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Community

- Vendor-sec
- Oss-security
- Red Hat / Canonical / Suse / Debian
 - We compete from a business side
 - Our security teams work together

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Trust

- With Open Source your vendor has no secrets
- **YOU** can be the vendor
 - Do you trust yourself?

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Looking forward

- Browsers
- Cloud
- New threats

SUMMIT

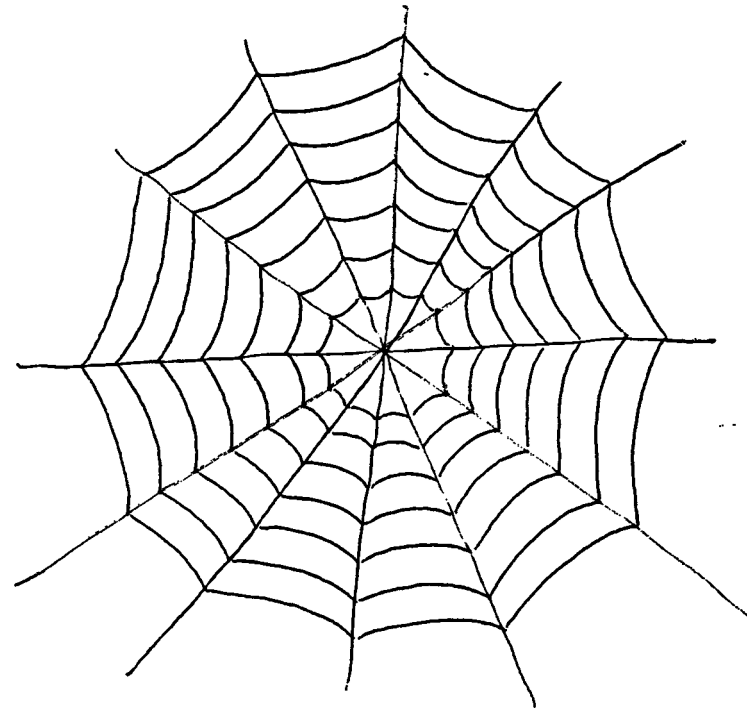
**JBoss
WORLD**

PRESENTED BY RED HAT



Browsers

- The web is becoming the computer
- Physical access is no longer needed
 - Just a username and password



SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Modern computing



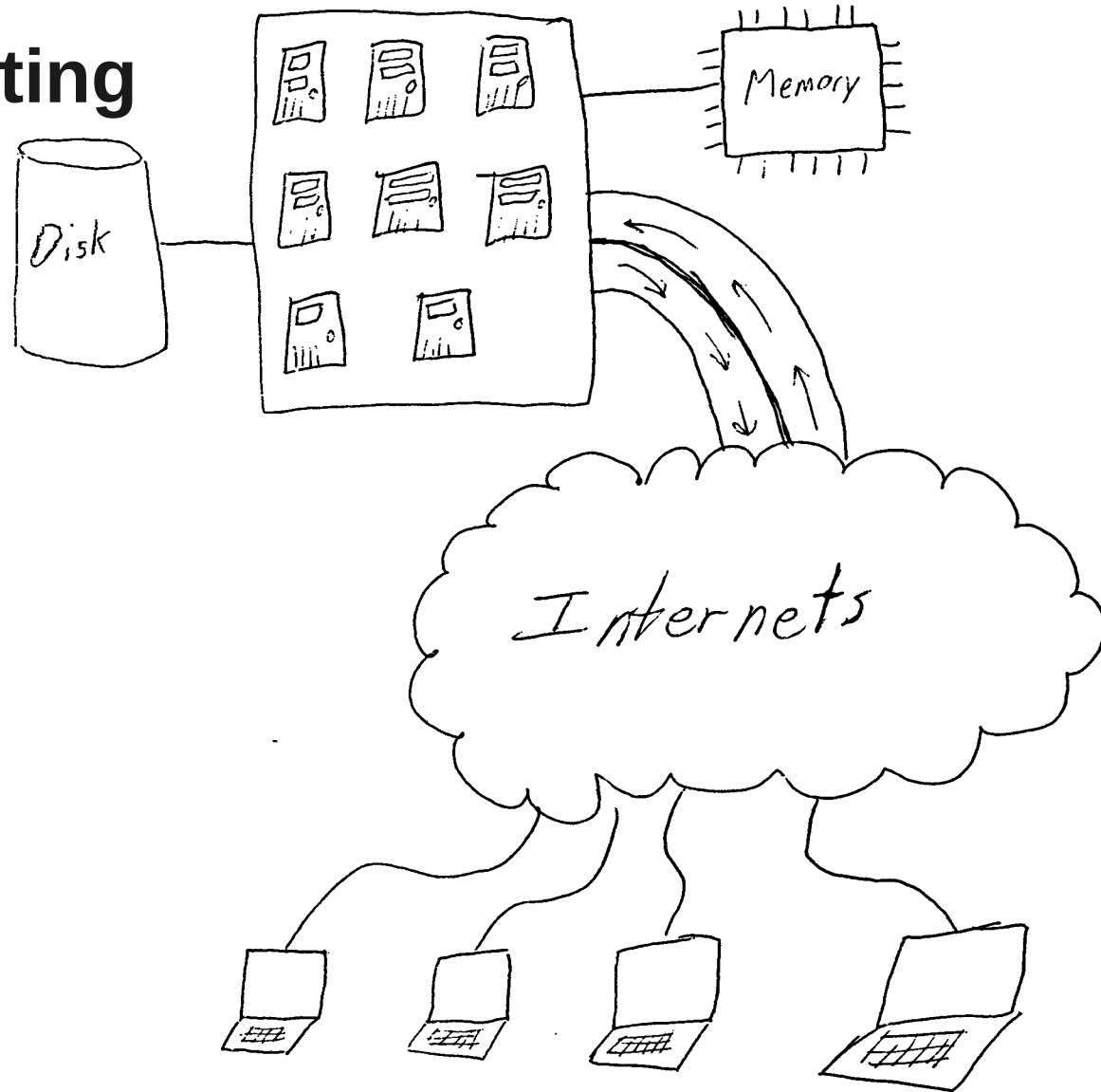
SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Cloud computing



SUMMIT

JBoss
WORLD

PRESENTED BY RED HAT



New threats

- What we know
- What we know we don't know
- What we don't know we don't know

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



Questions?

In God We Trust;
From Everyone Else,
We Need Source Code.

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT



FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

[#summitjbw](https://twitter.com/summitjbw)

READ THE BLOG

<http://summitblog.redhat.com/>

SUMMIT

**JBoss
WORLD**

PRESENTED BY RED HAT

