

IBM Linux Security Direction & Activities

Doc Shankar

IBM Linux Technology Center

dshankar@us.ibm.com

Agenda

- What's Different About Linux[®] Security?
- Linux Security Today
- Linux Security Activities at IBM
 - ▶ LTC
 - ▶ IBM Research
 - ▶ eServer
 - ▶ Tivoli
- Linux Security Strategy at IBM

What's Different About Linux Security?

- Source code availability
 - ▶ Most programmers take extra precautions
 - ▶ Community inspection/review
 - ▶ Community audit
- Patch speed
 - ▶ One example – Network Time Demon(ntpd)
 - ▶ Open source distributors released workaround/fixes within hours
 - ▶ Other vendors took days
- Community participation
 - ▶ Lot of interest from research community
 - ▶ Hard for one vendor to do this
 - ▶ Large/talented community has spanned interesting projects
- Maturing a lot faster than Unix® security
- Cryptography comparison
 - ▶ Crypto is hard to do right – the only way is to keep open
 - ▶ The only way to tell good crypto from bad crypto is to have it examined by experts
 - ▶ Open source crypto algorithms are strong – e.g, DES, AES
 - ▶ Open crypto is not only better – it's cheaper (AES is free)
- Comparison to secure protocols
 - ▶ (Same points as above)
 - ▶ Open committee design is better (SSL, IPSEC, TLS, S.MIME, SET,...)

Is Open Source More Secure?

- Simply publishing code does not mean people will examine it for security flaws
- Security researchers are fickle and busy people
- So, while Open Source is a good thing, it is NOT a guarantee for security
- There are so many open source libraries that no one has ever heard of, and no one has ever evaluated
- On the other hand, Linux has been looked at by a lot of very good security engineers

Linux Security Today

- Linux can achieve C2 functionality
 - ▶ Authentication via PAMs (Pluggable Authentication Modules)
 - ▶ Authorization via ACLs (Access Control Lists)
 - ▶ Auditing weak - being worked
 - ▶ Object reuse - some support
- Achieving C2 assurance can be difficult
 - ▶ Lack of formal process
 - ▶ Lack of formal documentation
 - ▶ Need to understand better security implications of open source
 - ▶ Need commitment from brands (distributors)
 - ▶ Fairly expensive
 - ▶ Business case

Linux Security Activities at IBM - LTC

- LSM
- Kerberos
- Secure configuration
- EIM
- PKI
- Security white papers
- Hardware crypto enablement
- PKCS # 11 support
- IPSEC
- Open SSL
- NSA collaboration
- Certification

Linux Security Activities at IBM - Research

- NSA collaboration
- Linux Security Enterprise white paper
- SELinux Performance
- Verification tools for LSM hooks
- Authentication (LSM)
 - ▶ Program
 - ▶ User
 - ▶ Data
- Authorization (LSM)
- Linux on 4758

Linux Security Activities at IBM - zSeries

- Runs native, in an LPAR or under z/VM™
- Takes advantage of S/390® hardware and the robust security of S/390 OS
- The most secure platform for Linux
 - ▶ Logical Partitioning (LPAR)
 - Provides separation of operating environments
 - Currently ITSEC E4
 - Supports Linux today
 - ▶ Crypto(PCICC & PCICA)
 - Currently FIPS 140-1 Level 4
 - Integrated symmetric and public key support
 - Linux drivers for SSL accelerator
 - WebSphere® integration with SSL acceleration
 - ▶ Hipersockets
 - Increased physical security vs. channels

Linux Security Activities at IBM - Tivoli

- Access Manager for eBusiness
- Access Manager for Operating Systems
- Access Manager for Business Integration
- Risk Manager
- Identity Manager
- Privacy Manager

Linux Security Strategy at IBM

- Ensure Linux is a secure platform
- Ensure Linux platform security is synergistic with IBM® and other vendor middleware security
- Contribute security enhancements to the Linux Open Source communities where it makes sense
- Work aggressively with the distributors to release the appropriate security enhancements
- Ensure adequate processes are being followed to obtain higher levels of security certification
- Work closely with the government & marketplace to formulate Linux security requirements
- Ensure synergy with IGS security offerings
- Ensure synergy between LTC & platform-specific activities
- Ensure IBM & Linux security strategies are complementary

Legal Statement

- This work represents the views of the author and does not necessarily reflect the views of IBM.
- IBM, s/390, WebSphere, zSeries, and z/VM are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries.
- Linux is a registered trademark of Linus Torvalds.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, and service names may be trademarks or service marks of others.