SUSE® Security Certifications

Andreas Stieger
Project Manager Security
astieger@suse.com

Alexander Bergmann
Security Engineer
abergmann@suse.com

SLES 12 is CC certified!

Common Criteria

- ISO/IEC 15408 (ITSEC, CTCPEC, TCSEC)
- Accepted by 26 countries
- Tested and verified by independent 3rd party (the evaluator), at different Evaluation Assurance Levels
- Certificate created by government agency
- Includes development processes, IT infrastructure, physical security, and HR procedures

Common Criteria

- Protection Profile: OSPP: 2.0 (including advanced management, advanced audit, and virtualization)
- With augmentation for Flaw Remediation (FLR)
- EAL4, with mutual recognition!

Common Criteria

- x86-64 (Intel and AMD), s390x
- Visualization with KVM
- First time SELinux was used to separate virtual machines
- With btrfs and full system rollback…
- … or with full disk encryption
- Audit, IPSec, SSH, …
- Installation via a special ISO (also contains FIPS modules)

SLES 12 is CC certified!

SLES 12 is FIPS 140-2 validated!

FIPS 140-2

Federal Information Processing Standard (FIPS)

- FISMA, NIST SP 800, FedGov, financial industry
- Certificate is issued by NIST (US) and CSE (Canada)

FIPS 140-2 ensures that

- Crypto algorithms/modes follow the newest standard
- No obvious crypto weakness exists
- No outdated algorithms or too short keys are used
- Self tests and integrity checks with each invocation of CM

FIPS 140-2 – current status

SLES 12 is FIPS 140-2 validated on x86-64!

- Kernel
- OpenSSL
- OpenSSH Client + Server
- Mozilla NSS
- StrongSWAN (IPSec)
- libgcrypt (Disk encryption)

Run SLES 12 SP1 with FIPS 140-2 validated CSMs from the certification module.

FIPS 140-2 – how to enable

Enable functionality:

- zypper in -t pattern fips
- Boot with “fips=1”

Check status:

- cat /proc/sys/crypto/fips_enabled

Enforce use of FIPS 140-2 validated binaries:

- Enable “Certifications module”
- zypper in -t pattern certification-fips
- Packages are downgraded to frozen versions

FIPS 140-2 going forward

- **We are re-validating SLES 12 SP2 to FIPS 140-2**
- **We are adding the IBM System z platform**
- **ETA: mid 2017**

SLES 12 is FIPS 140-2 validated!

SLES 12 and DISA STIG

DISA STIG

- Security Technical Implementation Guides
- Developed by the Defense Information Systems Agency
- Secure configuration guides for military field users
- Mandatory for US DoD customers through DISA, when published

DISA STIG - Status

- SUSE is currently developing STIGs based on:
  - General Purpose Operating System SRG
  - Web Server SRG

- Content complete, in verification state at DISA

- We want:
  - matching SCAP / OVAL content for automation
  - cooperation with technology partners and community
  - further roles / SRGs based on demand

Is it available...?

STIG drafts available for download now

http://example.com/123

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS)

- A standard for organizations that handle credit card data.
- The standard is administered by the PCI Security Standards Council that consist of the five major payment brands.
- Version 1.0 was published in 2004.
- Version 3.2 was released in April 2016.

PCI Security Standards Council ®

PCI DSS: High Level Overview

- 6 objective areas
- 12 requirements

- Covering a wide spectrum
  - Define formal processes
  - General system design guidance
  - Documentation
  - General system hardening

Build and Maintain a Secure Network and Systems
Protect Cardholder Data
Maintain a Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor and Test Networks
Maintain an Information Security Policy

PCI DSS: Essentials

Protect Cardholder Data

	Data Element	Storage Permitted
Cardholder Data	Primary Account Number (PAN)	Yes (unreadable)
	Cardholder Name	Yes
	Service Code	Yes
	Expiration Date	Yes
Sensitive Authentication Data	Full Track Data	No
	CAV2/CVC2/CVV2/CID	No
	PIN/PIN Block	No

PCI DSS: Some Examples

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

- **Identify insecure services, protocols and ports allowed**
  - ✔ listening services (`netstat` / `ss`)
  - ✔ process list (`ps`)
  - ✔ check installed programms (`zypper` / `rpm`)
- **Limit in- and outbound traffic to that which is necessary**
  - ✔ YaST firewall module (`iptables`)
  - ✔ TCP wrapper (`hosts.allow`/`hosts.deny`)

PCI DSS: Some Examples

Requirement 3: Protect stored cardholder data

- **Full disk encryption**
  - ✔ using LUKS/dm-crypt

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Use strong cryptography and security protocols**
  - ✔ using IPSec (strongSwan / OpenVPN)
  - ✔ using TLS v1.2 (Apache HTTP Server)

PCI DSS: Some Examples

Requirement 6: Develop and maintain secure systems and applications

- **Install vendor-supplied security patches**
  - ✔ Using the SUSE Update Stack (`zypper`)
    - Identify patches based on the severity level (low/moderate/important).
    - Check system status for certain CVEs.
  - ✔ This task can be automated via SUSE Manager
  - ✔ Checking system patch level via OVAL profile

PCI DSS: Some Examples

Requirement 7: Restrict access to cardholder data by business need to know

- **Restrict access to privileged user IDs**
  - ✔ “traditional Unix permissions” (rwx)
  - ✔ Access Control Lists (ACLs)
  - ✔ Capabilities
  - ✔ Login access (PAM)
  - ✔ SELinux and AppArmor

PCI DSS: Some Examples

Requirement 10: Track and monitor all access to network resources and cardholder data

- **Verify creation and deletion of system level objects**
  - ✔ Advanced Intrusion Detection Environment (AIDE)
  - ✔ Check system configuration status via Machinery
  - ✔ Using the Linux Audit Framework

SUSE Linux Enterprice Server PCI DSS Guide

>>> URL to-be-announced <<<

Questions

Thanks