

Securing Your System:

Security Hardening Techniques for SUSE® Linux Enterprise Server

Marcus Meissner

Software Engineer

SUSE

Roman Drahtmueller

Software Engineer

SUSE

Craig Gardner

Software Engineer

SUSE



Overview



What? and Why?



Architecture Dive: Inspection



Tools

What? and Why?

What Should “Security” Be?

What is Security?

Good software...

...does what you expect it to do, and does it well.

Secure software...

...is **good** software that does nothing else.



What to Do?

Software contains errors

- Malfunctions
- Crashes
- Downtime
- **Security Vulnerabilities**

Data loss and disclosure, identity theft,
system abuse, privilege transition

Apply Maintenance Updates



A Closer Look

Administration

Purpose, responsibilities, mandates, team play

Infrastructure

Network and network boundaries, services

Security Zones

Assets and protection, domains, domain transitions

Systems

Deployment, installation, configuration (hardening),
monitoring, maintenance, auditing

A Closer Look

Administration

Purpose, responsibilities, mandates, team play

Infrastructure

Network and network boundaries, services

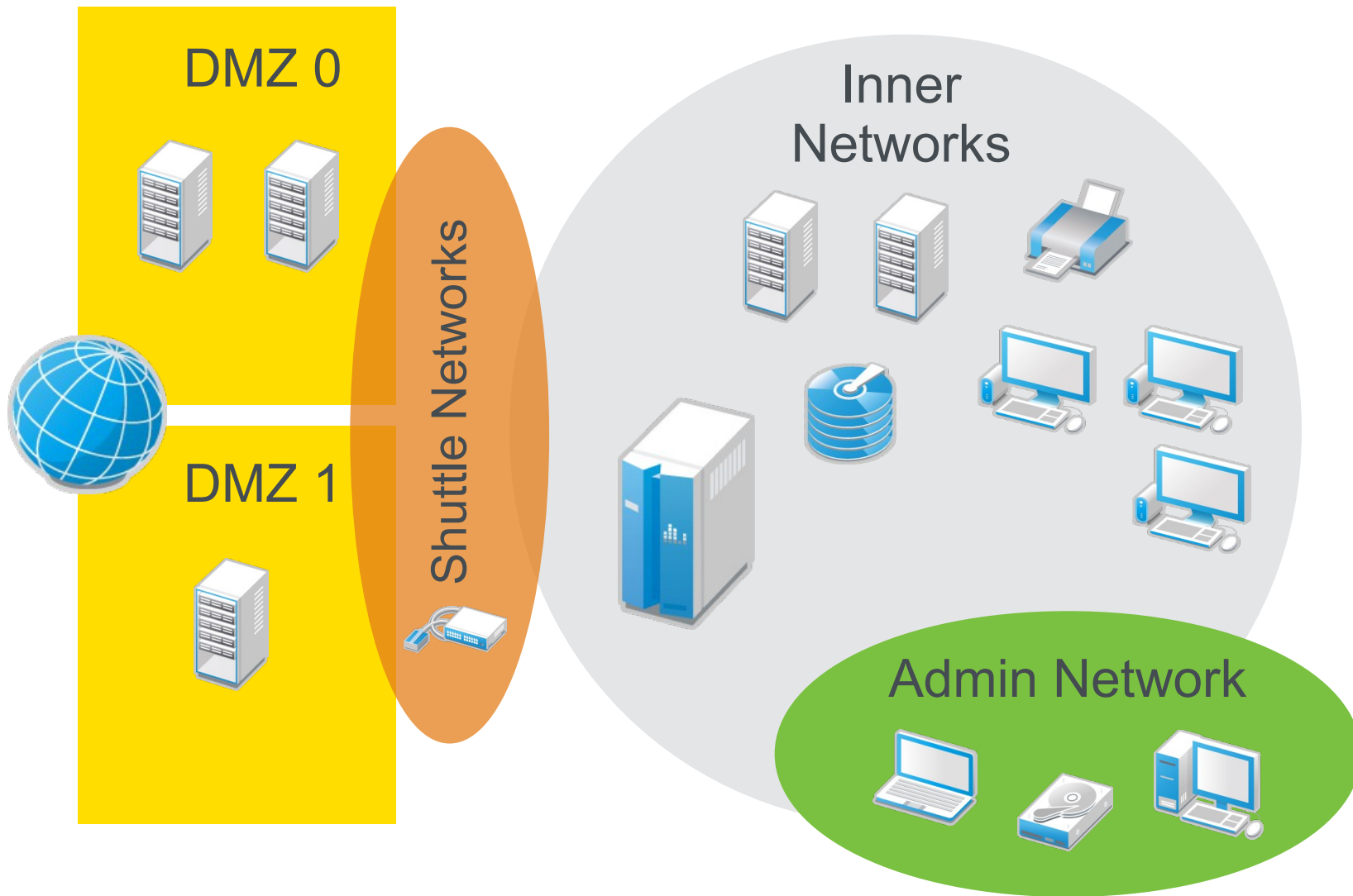
Security Zones

Assets and protection, domains, domain transitions

Systems

Deployment, installation, configuration (hardening),
monitoring, maintenance, auditing

Inspection, Configuration, Hardening



YaST Security Center

 Security Overview

Security Overview

- Predefined Security Configurations
- Password Settings
- Boot Settings
- Login Settings
- User Addition
- Miscellaneous Settings

Security Setting

Status

Security Status

Security Setting	Status	Security Status	
Use magic SysRq keys	Disabled	✓	Help
Use secure file permissions	Configure	✗	Help
Remote access to the display manager	Disabled	✓	Help
Use current directory in root's path	Disabled	✓	Help
Use current directory in path of regular users	Disabled	✓	Help
Write back system time to the hardware clock	Enabled	✓	Help
Always generate syslog message for cron scripts	Disabled	✗	Help
Run the DHCP daemon in a chroot	Unknown	✗	Help
Run the DHCP daemon as dhcp user	Unknown	✗	Help
Disable remote root login in the display manager	Disabled	✓	Help
Disable remote access to the X server	Disabled	✓	Help
Remote access to the email delivery subsystem	Disabled	✓	Help
Disable service restart on update	Disabled	✓	Help
Disable service stop on removal	Disabled	✓	Help
Enable TCP syncookies	Enabled	✓	Help
Disable IPv4 forwarding	Disabled	✓	Help
Disable IPv6 forwarding	Disabled	✓	Help
Enable basic system services in runlevel 3 (multiuser with network)	Configure	✗	Help
Enable basic system services in runlevel 5 (multiuser with network and graphical login)	Configure	✗	Help
Enable extra services in runlevel 3	Configure	✗	Help
Enable extra services in runlevel 5	Configure	✗	Help

Help

Cancel

OK

What “Local Security” Does in the Background

Run another YaSTmodule

Change settings in files in /etc/sysconfig

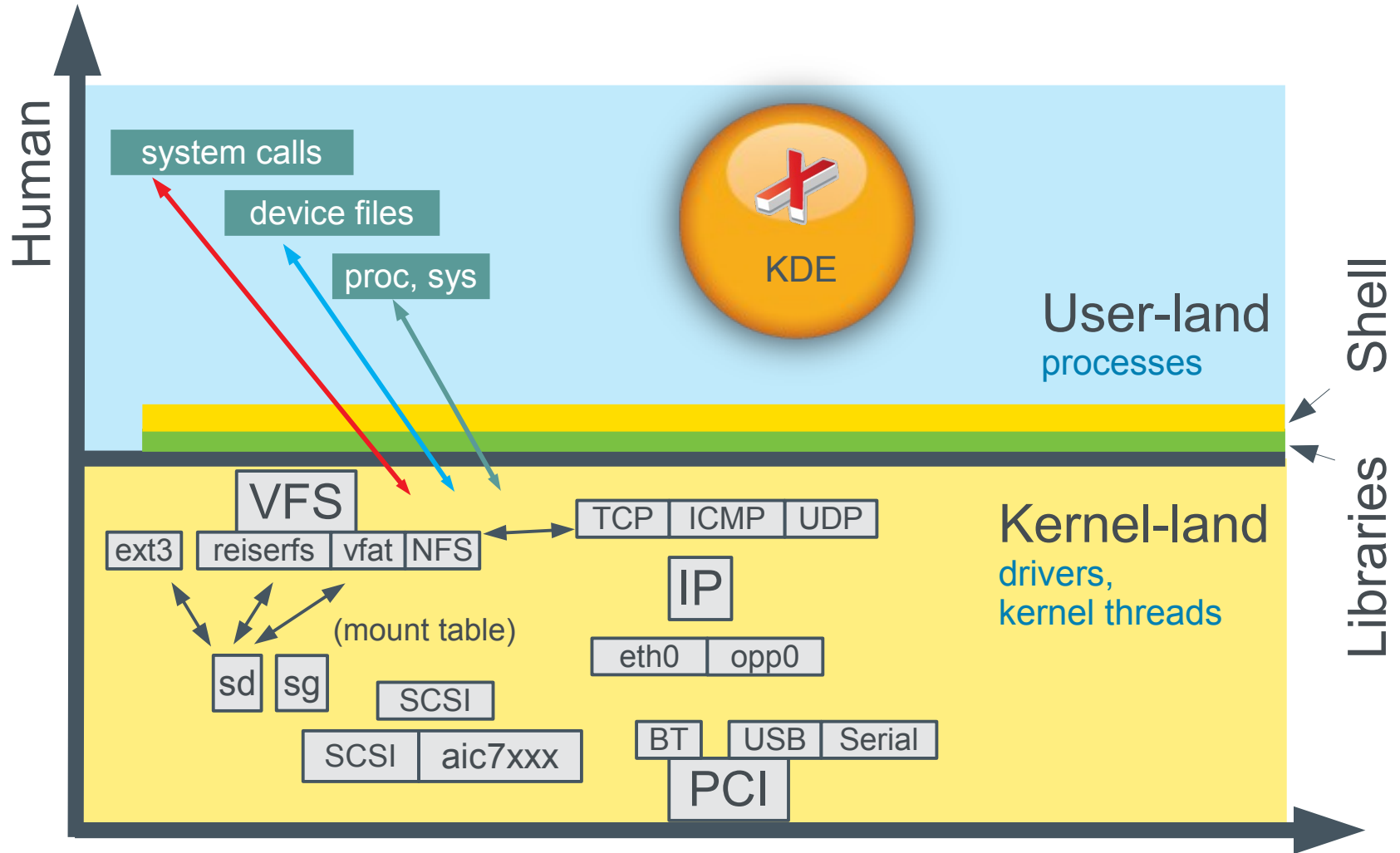
Modify configuration files directly



Architecture and Design

Schematical Overview:

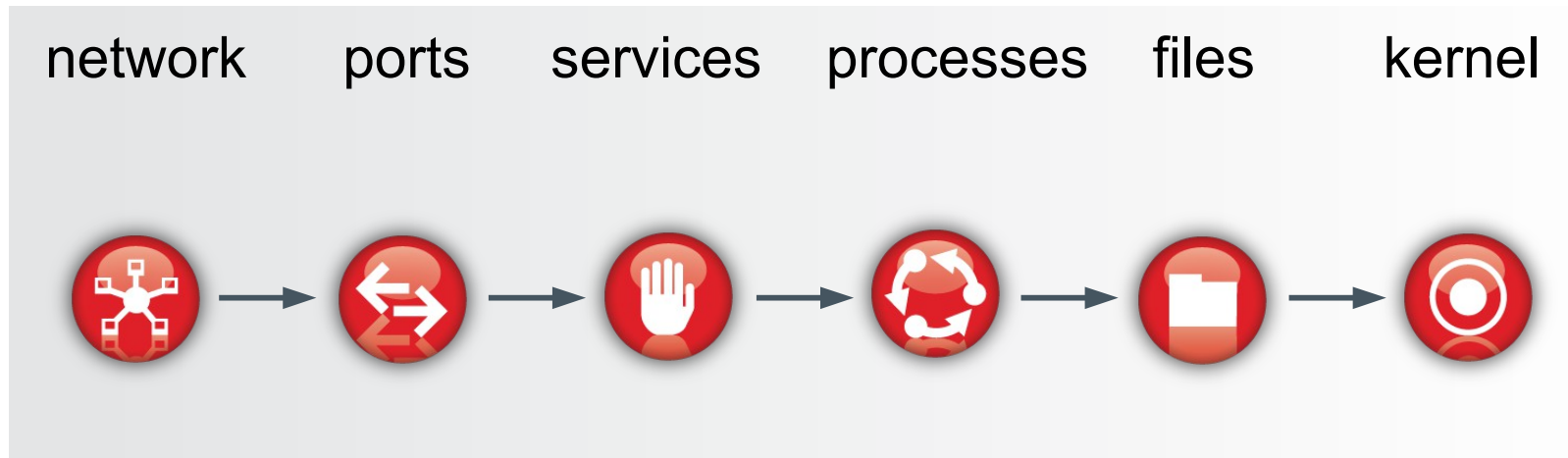
O/S Kernel + Userland



Physics/Electronics

Inspection

Approach your system as if you were an attacker:



Network

Interface addresses: all interfaces enabled and conn.?

Routing setup: IP-forwarding on/off?

Netfilter rules: active, any?

maintain ARP table records

Other tweakables:

txqueuelen, mtu

ICMP replies, ICMP redirects

ECN

slow-start



Ports

port scan: Open TCP and UDP sockets

```
nmap -sS -v -O ip.address.on.network
```

Compare to output of

```
netstat -anpl
```

Discrepancies...?

(Not all services are userland process bound! (knfsd))

Watch out for UDP sockets!



Services

Disable all services that are not needed, permanently

Remove the runlevel symlinks (`insserv -r <servicename>`)

Kill the servers (`rcapache2 stop`)

Verify if they the services are really dead!

Remove the packages from the system?



Processes

Get to know all processes on your system in person...

```
ps faux
```

```
rpm -qfi /usr/sbin/nscd
```

...and deactivate whatever is not needed running.



Files

Permissions: /etc/permissions* from
/etc/sysconfig/security

Use `chkstat -set <permissions file>` or `SuSEconfig`

```
find / /usr ... -mount -type f \( -perm +2000 -o -perm  
+4000 \) -ls
```

Integrity measures: AIDE, RPM

maintain offsite RPM database backup for `rpm -Va`

maintain offsite AIDE database backup

Mount options: /etc/fstab, /proc/mounts



Kernel: Use AppArmor!

Example profile: dhcp daemon



```
#include <tunables/global>

/usr/sbin/dhcpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability dac_override,
  capability net_bind_service,
  capability net_raw,
  capability setgid,
  capability setuid,
  capability sys_chroot,

  /db/dhcpd.leases*   lrw,
  /etc/dhcpd.conf     r,
  /etc/hosts.allow    r,
  /etc/hosts.deny     r,
  /usr/sbin/dhcpd     rmix,
  /var/lib/dhcp/dhcpd.leases* rwl,
  /var/lib/dhcp/etc/dhcpd.conf r,
  /var/run/dhcpd.pid  wl,
}
```



Tools

Tools

The YaST Security Center

The YaST AppArmor profile generator

Integrity: AIDE and RPM

Port Scanner: nmap

Vulnerability scanner: openSCAP + OVAL



More Tools, More Considerations

System Monitoring: Nagios, Ganglia

Syslog Monitoring: logwatch, Sentinel

Vulnerability scanner: openvas





Corporate Headquarters
Maxfeldstrasse 5
90409 Nuremberg
Germany

+49 911 740 53 0 (Worldwide)
www.suse.com

Join us on:
www.opensuse.org

Unpublished Work of SUSE. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

