Hardening Check_MK using SELinux

Ralf Spenneberg

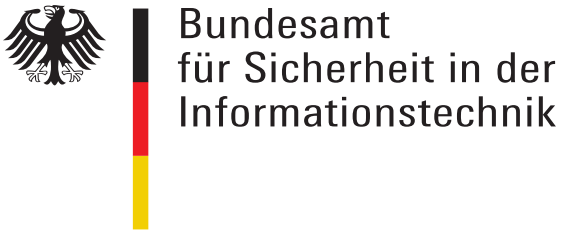
03. Mai 2018

Check_MK Conference #4

Contact:
info@os-s.net

Ralf Spenneberg

- OpenSource Training
- OpenSource Security
  - Seit 2013 Partner der Mathias Kettner GmbH



Security Research

heise online > News > 2015 > KW 53 > 32C3: Verschlüsselung gängi

32C3: Verschlüsselung gängiger RFID-Schließa

heise online 29.12.2015 11:31 Uhr – Stefan Krempl

(Bild: Winkhaus)

RFID-Transponderkarten, die für die elektronische Zutrittskon sich Sicherheitsexperten zufolge oft "trivial einfach" klonen.

Schlechte Nachrichten für alle, die ihren klassischen Haus- oder Chipkarte ersetzen wollen oder dies bereits getan haben: Die zu für einschlägige elektronische Schließsysteme könnten teils "tri Dies erklärte Ralf Spenneberg, Chef der Firma OpenSource Trai Chaos Communication Congress in Hamburg.

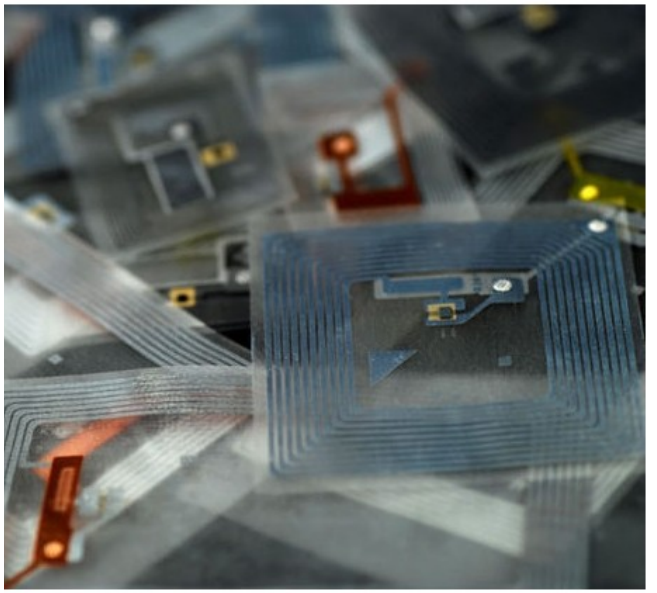
SCHWACHSTELLE BEI EM4450 TRANSPONDERN

Die Transpondertechnologie MIFARE® DESFire® ist DIE Leittechnologie von Uhlmann & Zacher ...

eutel kan simpel erd worden

30/12/15 om 14:37 - Bijgewerkt om 14:37
Bron: Datanews

sleutels inwisselen voor een draadloze oplossing moeten er op D-sleutel bedriegelijk makkelijk gekopieerd kan worden. Die en op het Chaos Computer Congress in Hamburg.



ieke sleutel voor een chipkaart lijkt makkelijk, maar het kan gevaarlijk zijn", van het bedrijf OpenSource Security. Hij doelt op het feit dat de kloond kan worden, zodat de ooit veilige sleutel nu in handen van derden r

OpenSource Security

Security Research

KERNEL-TREIBER

Fuzzing deckt USB-Sicherheitslücken auf

Black Hat Europe 2014

Sicherheitslücken in USB-Treibern können eine einfache Möglichkeit darstellen, um Systeme zu übernehmen. Mittels Fuzzing-Technologien fanden zwei Sicherheitsforscher zahlreiche potenzielle Lücken in Linux-Treibern.

USB-Geräte als mögliche Einfallstore für Angriffe sind eigentlich keine Neuheit. Die beiden Sicherheitsforscher Sergej Schumilo und Ralf Spenneberg wiesen in ihrem Vortrag auf der Black Hat Europe darauf hin, dass bereits 2005 in einem Vortrag, ebenfalls auf einer Black Hat-Konferenz, vor entsprechenden Lücken gewarnt worden war. Trotzdem ist das Problem offenbar gravierend: Mit Hilfe von Fuzzing-Technologien fanden Schumilo und Spenneberg zahlreiche Bugs in Linux-Kernel-Treibern für USB-Geräte.

Zufälligen Eingabedaten

Security Research

Gefällt mir

DATA CENTRE SOFTWARE NETWOR

Security

Daisy-chained res
hell for power pla

World's first PLC worm

5 May 2016 at 14:05, Darren Pauli

BlackHat Asia A world-first proof-of-
critical infrastructure, including power
and stop.

It is a stand-alone attack but *The Re*
can be produced by combining two ir

The programmable logic controller (P
brain child of German hackers Ralf S
OpenSource Security Ralf Spennebe
without the need of an infected laptop or desktop.

All other PLC malware such as Stuxnet relied on having an infecte
controllers, meaning an infection could be stopped from proliferating by removing those machines.

Spenneberg and Brüggeman claim the attack spreads like cancer between default Siemens S7 1200
PLCs, and could be reworked to target other systems.

Researchers Create Self-Propagating Worm That Targets SCADA Equipment

Malware is slowly making its way into the ICS/SCADA field

May 9, 2016 15:44 GMT · By

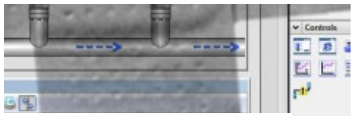
German researchers
of-concept worm tha
ICS/SCADA equipmer

Their research builds or
last year's Black Hat USA
PLCs.

The OSS team led by Ra
virus, that can live in the
spread to other similar c

PLC-Blaster PoC wo

In their proof-of-concep
SIMATIC S7-1200 PLCs.
port 102, shared by Sien
Protocol (ICCP), to find



SC Magazine > News > Researchers discover ICS attack method that spreads through networks

Jeremy Seth Davis, Senior Reporter

May 06, 2016

Researchers discover ICS attack method that spreads through networks

Share this content:

A team of researchers published a report detailing their discovery of a new method of launching attacks that would threaten global critical infrastructure and utility providers through a worm that could spread directly through utility networks.

Iranian hackers targeting critical infrastructure

The attack, discovered by Ralf Spenneberg, Maik Brüggeman, and Hendrik Schwartke at OpenSource Security, a German security consulting firm, relies on a programmable logic controller (PLC) worm that the researchers saiddoes not rely on infected devices such as a laptop or desktop to spread the worm. The research team presented their discovery at BlackHat Asia.

sponsibly coordinated disclosure with Siemens.

lity

ect

k.

ıe

n Autor

OpenSource Security

Retrospective

- Default Password removed
- Livestatus now restricted by Xinetd
- Best Practice Checks included

Mandatory Access Control

- On DAC users may assign any privileges to a file
- MAC systems prohibit users assigning to broad privileges
- On UNIX MAC may even confine the root user

Linux MAC

- SELinux
- AppArmor
- SMACK
- Grsecurity
- ...

SELinux History

- Initiated by the NSA in the 1990s
- First released 2000 as GPL code
- Included first in Fedora Core 2
- Today available in
  - Fedora
  - RHEL/CentOS/OL
  - Debian (not default)

SELinux

- Default Deny
- Everything is about Labels
  - Processes
  - Files
  - Any Resource
- Rules allow processes to access resources based on labels

Simple Example

- Process Apache
  - system_u:system_r:httpd_t:s0
- Webpage /var/www/html/index.html
  - unconfined_u:object_r:httpd_sys_content_t:s0
- Rule
  - allow httpd_t httpd_sys_content_t:file { getattr ioctl lock map open read };

Where do the Labels come from?

- Everything is stored in the policy
- Files are labeled on the filesystem
  - xattr
  - setcon/restorecon
- Processes may change their label during creation

SELinux and Check_MK

- Check_MK Monitoring Host
  - Running Check_MK Raw/Enterprise Edition
- Check_MK Monitored Host
  - Running Check_MK Agent
    - Xinetd
    - SSH

Check_MK Monitored Host: Agent

- Default invocation: xinetd
  - Type: inetd_child_t
  - Extensive access required
  - This access is granted other xinetd services as well
- Via ssh as root
  - Running unconfined
  - No restrictions

Agent SELinux Policy Module

```
policy_module(check_mk_agent, 1.1.0)

########################################
#
# Declarations
#
type check_mk_agent_t;
type check_mk_agent_exec_t;
unconfined_run_to(check_mk_agent_t, check_mk_agent_exec_t)
inetd_tcp_service_domain(check_mk_agent_t, check_mk_agent_exec_t)

unconfined_domain(check_mk_agent_t)

type check_mk_agent_var_lib_t;
files_type(check_mk_agent_var_lib_t)

files_var_lib_filetrans(check_mk_agent_t, check_mk_agent_var_lib_t, { dir file lnk_file })
```

Caveats

- Who uses all plugins?
- Who uses all local scripts?
- Who may know what people come up with?

Check_MK Monitoring Server

- All services running as unconfined_service_t
- Even apache
- Only required changes:

  bin/omd must be initrc_exec_t

  http_can_network_connect → true

Check_MK Monitoring Server

- Policy Module (2015)
  - ~/share/doc/check_mk/treasures/selinux/
- Assigning appropiate types to OMD files
- Confining Apache

Treasures SELinux Policy Module

- Written for RHEL 6 (needs tweaks for RHEL 7)
  - commplex_port_t → commplex_main_port_t
- Only works for the first site (port 5000)
- No domains for
  - Check_MK Microcore
  - Liveproxyd
  - ...

Optimal: SELinux Policy Module

- Separate Domains:
  - cmc
  - liveproxyd
  - icmpsender
  - icmpreceiver
  - mkeventd
  - rrdcached

Community Effort

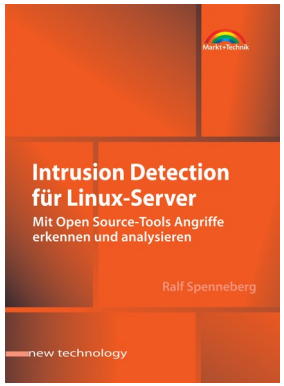
- Check_MK may do so many things
- Everything needs to be allowed
- Not all can be tested by myself

https://code.opensource-security.de/os-s/checkmk-selinux

Discussion

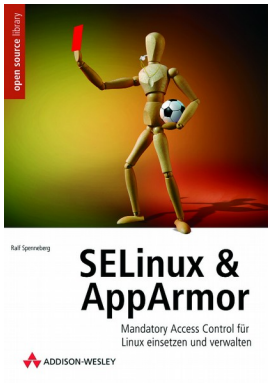
?

Bücher


Markt+Technik
Intrusion Detection
für Linux-Server
Mit Open Source-Tools Angriffe
erkennen und analysieren
Ralf Spenneberg
new technology


open source library
Ralf Spenneberg
Linux-Firewalls
mit iptables & Co.
Sicherheit für Linux-Server
und -Netzwerke
ADDISON-WESLEY


Open Source Library
Linux-Firewalls
Ralf Spenneberg
Linux-Firewalls
Sicherheit für Linux-Server
und -Netzwerke mit IPv4 und IPv6
ADDISON-WESLEY


open source library
Ralf Spenneberg
SELinux &
AppArmor
Mandatory Access Control für
Linux einsetzen und verwalten
ADDISON-WESLEY


open source library
Ralf Spenneberg
Intrusion Detection
und Prevention
mit Snort 2 & Co.
Einbrüche auf Linux-Servern erkennen und verhindern
ADDISON-WESLEY


Michael Kofler, Ralf Spenneberg
KVM für die
Server-Virtualisierung
Von Konfiguration und Administration
bis Clustering und Cloud
ADDISON-WESLEY
ALWAYS LEARNING
PEARSON


open source library
Ralf Spenneberg
VPN mit Linux
Grundlagen und Anwendung Virtueller
Privater Netzwerke mit Open Source-Tools
ADDISON-WESLEY


Open Source Library
Ralf Spenneberg
2. Auflage
VPN mit Linux
Grundlagen und Anwendung virtueller
privater Netzwerke mit Open-Source-Tools
ADDISON-WESLEY