

---

# Check\_MK Security

Ralf Spenneberg

03. Mai 2017

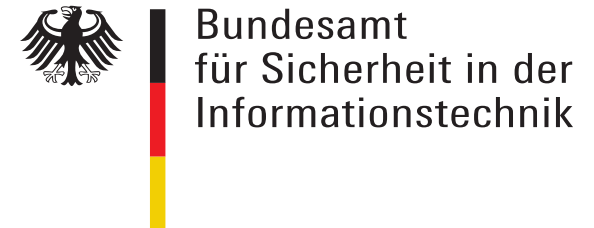
Check\_MK Conference

Kontakt:  
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 gängiger RFID-Schließkarten

## 32C3: Verschlüsselung gängiger RFID-Schließkarten

heise online 29.12.2015 11:31 Uhr - Stefan Krempel



(Bild: Winkhaus)

RFID-Transponderkarten, die für die elektronische Zutrittskontrolle eingesetzt werden, sind 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 "trivial" kloniert werden. Dies erklärte Ralf Spennberg, Chef der Firma OpenSource Trai am Chaos Communication Congress in Hamburg.



## SCHWACHSTELLE BEI EM4450 TRANSPONDERN

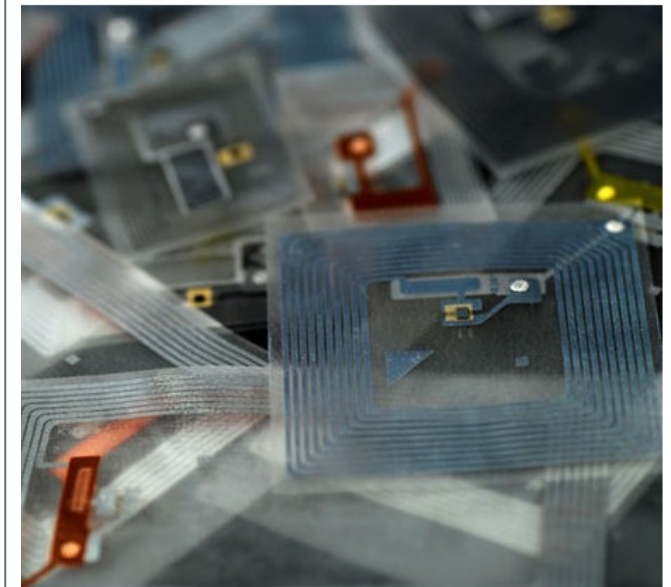
Die Transpondertechnologie MIFARE® DESFire® ist DIE Leittechnologie von Uhlmann & Zacher ...

SECURITY IS GENOMEN.

## Sleutel kan simpel gekopieerd 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.



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

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

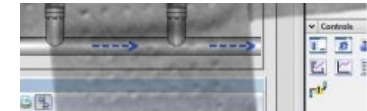
Gefällt mir

## 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

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



:45 pm

DATA CENTRE SOFTWARE NETWORK

### Security

## Daisy-chained red hell for power plants

World's first PLC worm

5 May 2016 at 14:05, Darren Pauli

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

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

The programmable logic controller (PLC) brain child of German hackers Ralf Spenneberg and OpenSource Security Ralf Spenneberg without the need of an infected laptop or desktop.

All other PLC malware such as Stuxnet relied on having an infected 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.

## German researchers of-concept worm that targets ICS/SCADA equipment

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

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

## PLC-Blaster PoC worm

In their proof-of-concept report 102, shared by Siemens OpenSource Security Ralf Spenneberg Protocol (ICCP), to find



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.

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 said does not rely on infected devices such as a laptop or desktop to spread the worm. The research team presented their discovery at BlackHat Asia.

and a German support and consulting group, dug up the responsibly coordinated disclosure with Siemens.



Iranian hackers targeting critical infrastructure

lity

ect  
k.

re

1 Autor

OpenSource security



# Security

---

- Monitoring Security Parameters
- What Systems are monitored?
- The security of these systems may not be compromised!
- Sensitive Data must be protected!
- The Monitoring must be protected



# Security Parameter

---

- Successful Backups
- Validity of Certificates of SSL/TLS Services
- Blacklists

# Agent

---

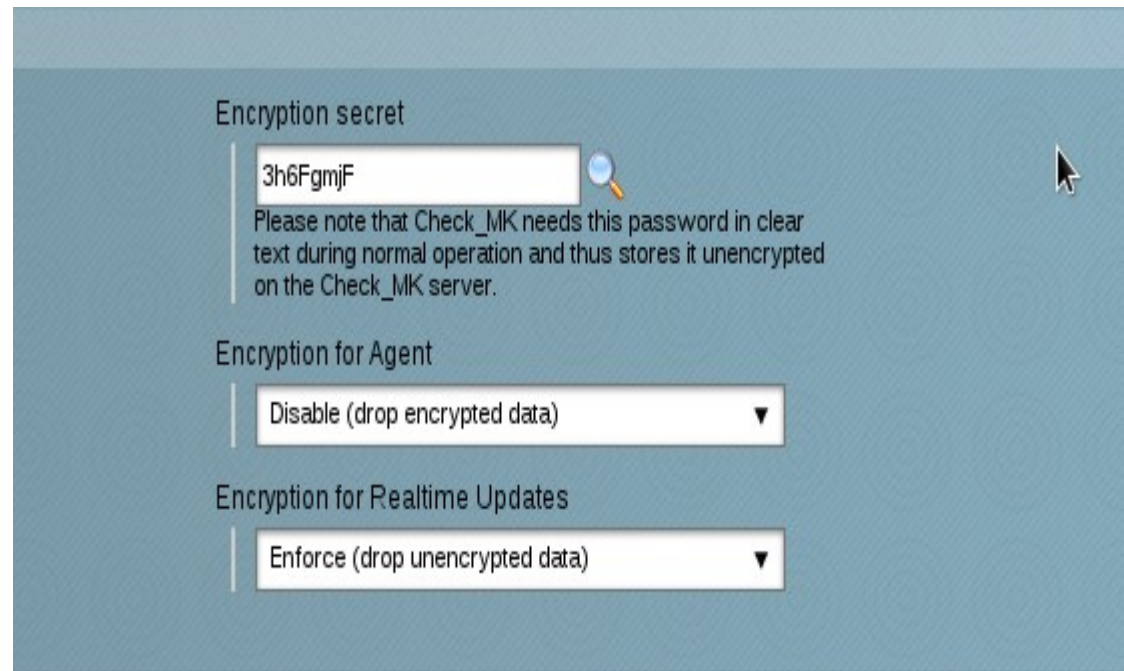
- Does not accept any data over the network
- Manual Installation on the target system
- The admin manages the Agent
  - ➔ Send Data
  - ➔ Selection of additional Plugins
  - ➔ Required Logins of Plugins





# Agent - Added Security

- SNMP
  - Views
  - ACLs
  - SNMPv3
- Agent
  - only\_from
  - Embedded Encryption (1.4.0)
  - Invocation via SSH



The screenshot displays the configuration interface for the Check\_MK Agent, specifically the 'Encryption' section. It features three main settings:

- Encryption secret:** A text input field containing the value '3h6FgmjF'. Below the field, a note states: 'Please note that Check\_MK needs this password in clear text during normal operation and thus stores it unencrypted on the Check\_MK server.'
- Encryption for Agent:** A dropdown menu currently set to 'Disable (drop encrypted data)'.
- Encryption for Realtime Updates:** A dropdown menu currently set to 'Enforce (drop unencrypted data)'.

# SNMP

---

```
access-list 99 permit 192.168.222.74
```

```
snmp-server view mkview system included
```

```
# snmp v1/v2
```

```
snmp-server community checkmk view mkview R0 99
```

```
# snmp v3
```

```
snmp-server group mkgroup v3 priv read mkview access 99
```

```
snmp-server user mkuser mkgroup v3 auth md5 mk-pass priv aes 128 mk-encrypt
```

# OMD

---

- Administration done as site user
- Password/Public Key login possible
- All processes use the site user
  - Apache
  - CMC/Nagios
  - etc
- Root access only required for
  - Creation, removal and renaming of the sites
  - Update of the OMD/Check\_MK Edition

# Multisite / WATO

---

- Default user omdadmin/omd
- HTTPS
  - Apache of the OS
- User management
  - Separate admin accounts
  - LDAP connections
    - **LDAP is clear text!**
    - **SSL/TLS required**

# Distributed Monitoring

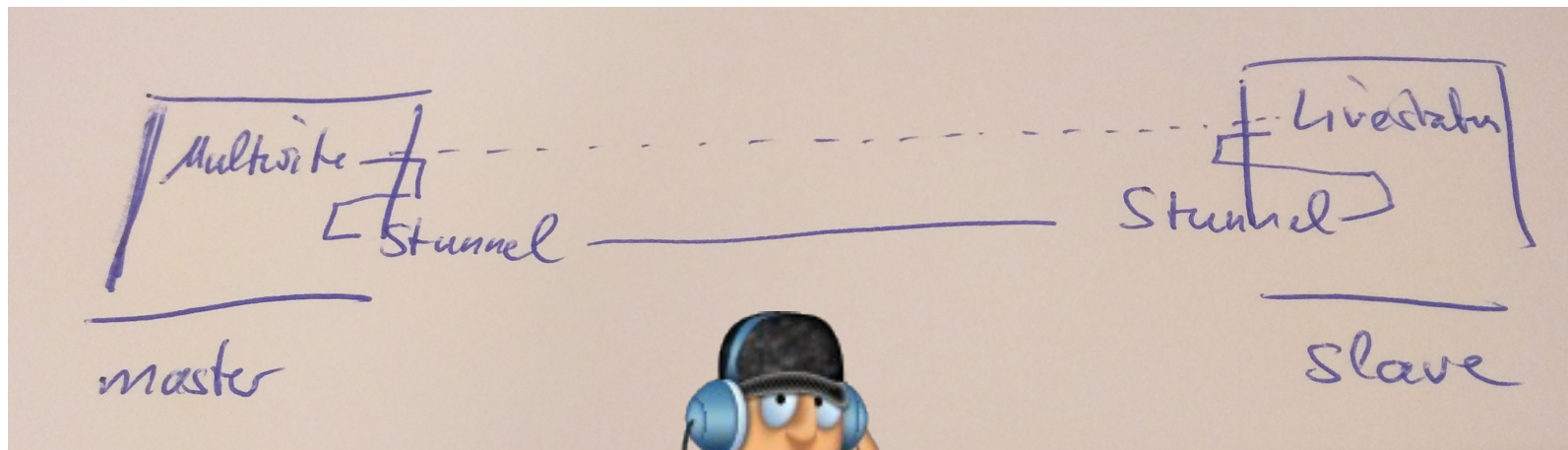
---

- Livestatus via TCP
- No restrictions by default
- Livestatus does not support any authentication nor authorization
- Livestatus supports commands!

# Distributed Monitoring Added Security

---

- At least restrict the IP addresses
  - `~site/etc/xinetd.d/mk-livestatus: only_from`
- Better use SSL/TLS
  - Stunnel may be used as proxy





# SSL/TLS Connections

---

- Use valid certificates!
- Place certificate authorities in OS SSL store
- Do not disable certificate checks!
- Otherwise Man-in-the-Middle attacks are possible

# Agent Bakery

---

- Pro
  - Centrally stored configuration
  - Documentation
  - Local adaption possible
  - Separate agents per host
- Con
  - Potential sensitive data stored centrally
  - Local files may be overwritten

# Automatic Agent Updates

- Signature using RSA Keys
- Download via HTTPS
- Registration required
  - Administrative account
- Master Switch
- Host restriction
- Signature passphrase protected

Prerequisites			
State	Edit	Test	
✓		Signature keys	You have created 2 signature keys for signing agents
✓		Configuration of update plugin	You have 1 rules for deploying the update plugin
✓		Baked agents	You have 20 baked agents containing the update plugin
✓		Signed agents	You have signed some or all agent packages
✓		Registered agents	Number of agents that have registered for updates: 1
✓		Master switch	Agent updates are enabled

Host Selection

▼ Activate update only on the selected hosts

Conditions .....

- ☐ Match folder
- ☐ Match Host Tags
- ☐ Match Host Groups
- ☐ Match only the following hosts
- ☐ Exclude the following hosts

Test with this host name .....

Change Selection

# Automatic Agent Updates

---

- Pro
  - Always current agents
- Con
  - (Almost) all configuration must be stored centrally
  - Admin of the target host loses control of the agent
  - Local files may be overwritten automatically

# Automatic Agent Updates

---

Authenticity of agent and plugins  
required

# Diskussion

---

?



# Bücher

