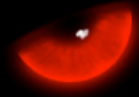
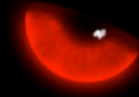


When the Lights go out

Hacking Cisco EnergyWise

Ayhan Koca & Matthias Luft
{akoca, mluft}@ernw.de



Agenda

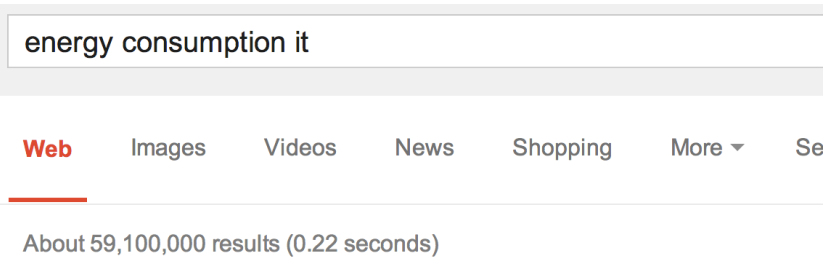
- Introduction
- Architecture & Protocol
- Attacks, Controls & Conclusions



Introduction

Energy Management

- IT equipment usually the biggest power consumer in (non-producing) corporate environments
- Energy savings is a relevant topic:
 - Big deal in data center design
 - DCIE-awareness, consolidation, AC technologies like Kyoto wheels...
 - Still relevant and a challenge in endpoints
 - Don't you wish your smartphone would live for a week? ;)



IT now 10 percent of world's electricity **consumption**,

See 100 percent of your energy use

Save 35 percent of your IT energy costs

Begin Saving Energy,
Costs and Carbon
Today



"green it"

Web

Images

Books

Videos

About 2,870,000 results (0.22 seconds)

"Green Data Center"

<http://www.cisco.com/c/en/us/products/switches/energywise-technology/index.html>

Same girl, different dress?



- Smart homes offer power control capabilities
- “Embedded” world offers energy management protocols
 - e.g. HDMI CEC contains power control commands, power consumption enumeration over USB
- Certain IPMI implementations/BMCs offer power management capabilities

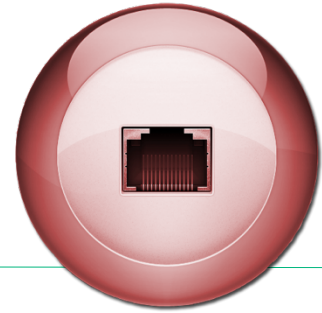
Cisco EnergyWise -vvv



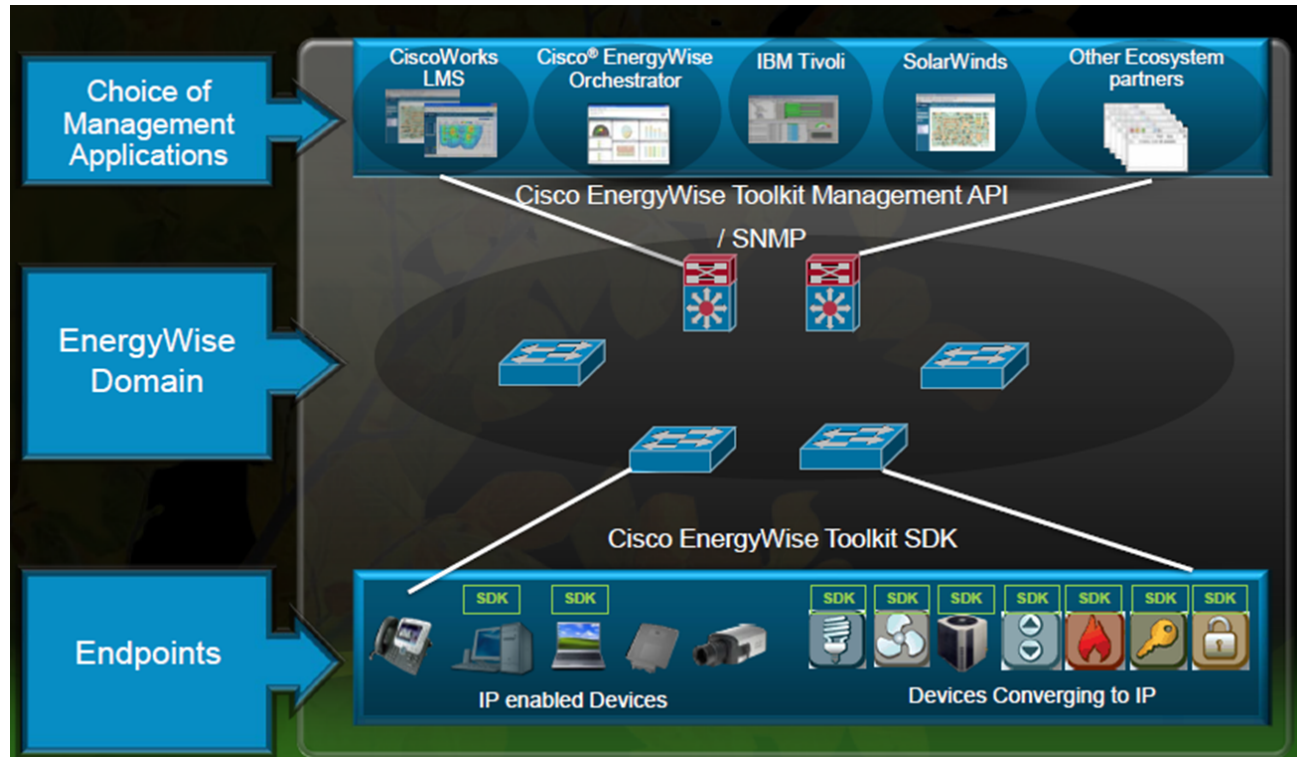
- Cisco-proprietary, IP-based EnergyManagement Protocol
- Provides support for PoE endpoints and arbitrary endpoints, that implement the EW API
- Allows energy management throughout the (Cisco) network.
 - Monitoring
 - Retriving & setting power levels
- Phase 1 vs. Phase 2

How does it work?

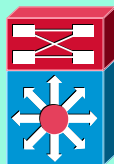
Overview



Cisco EnergyWise Architecture

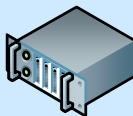


Relevant Entities



Switches, Routers
Domain Members

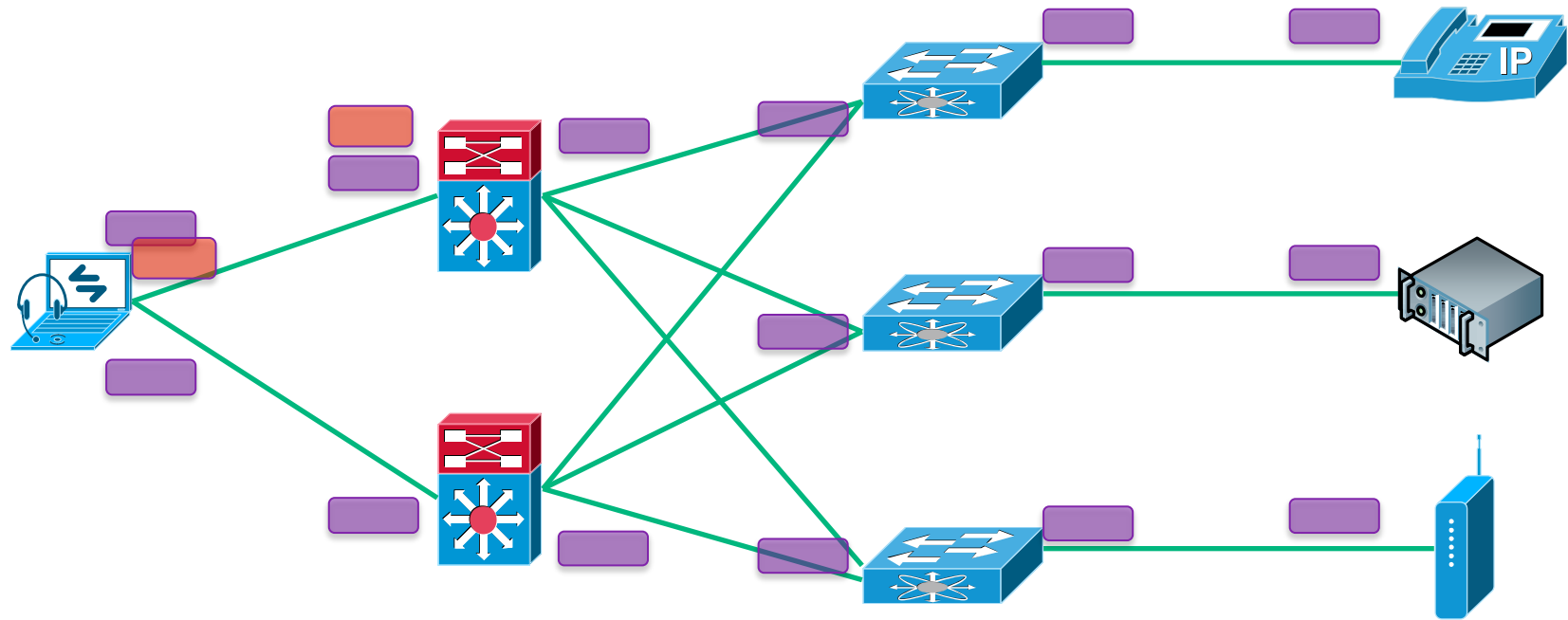
Endpoints/Children
Servers, Access Points, Phones



Management
Applications



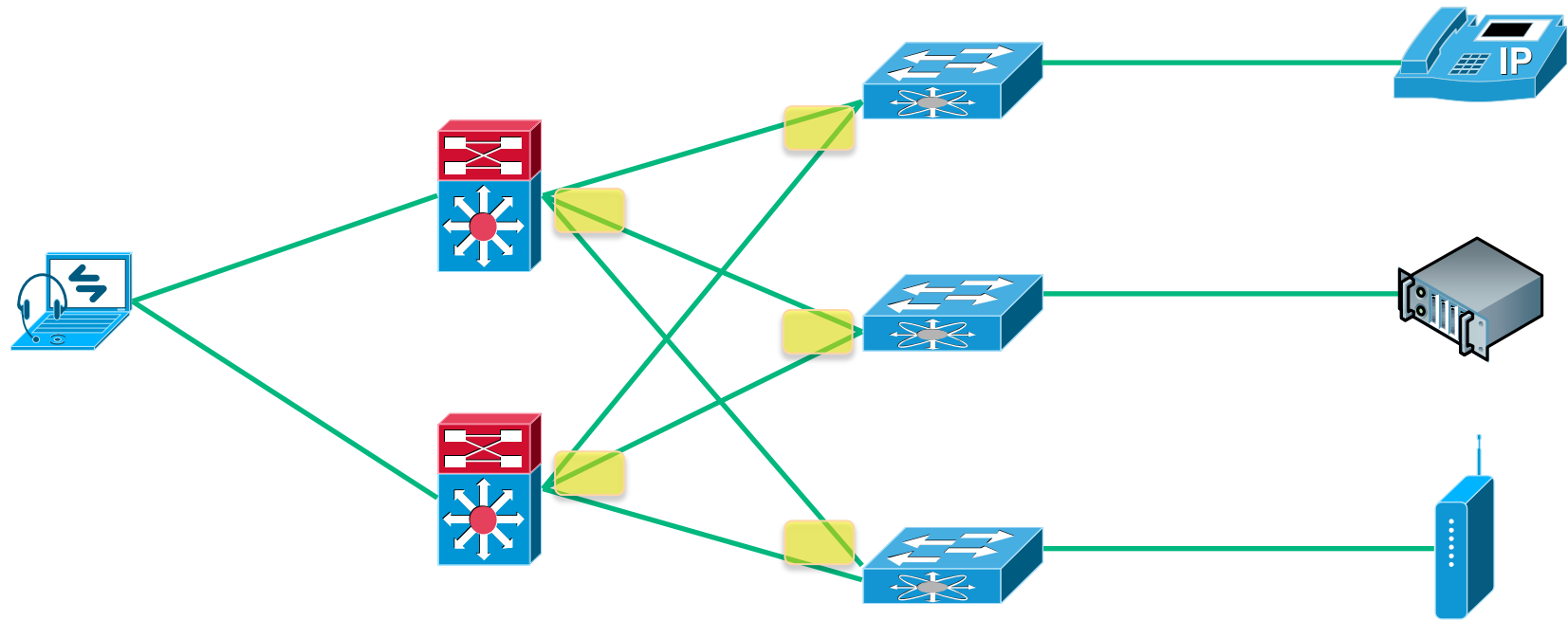
Neighbor Discovery – UDP



UDP Broadcast

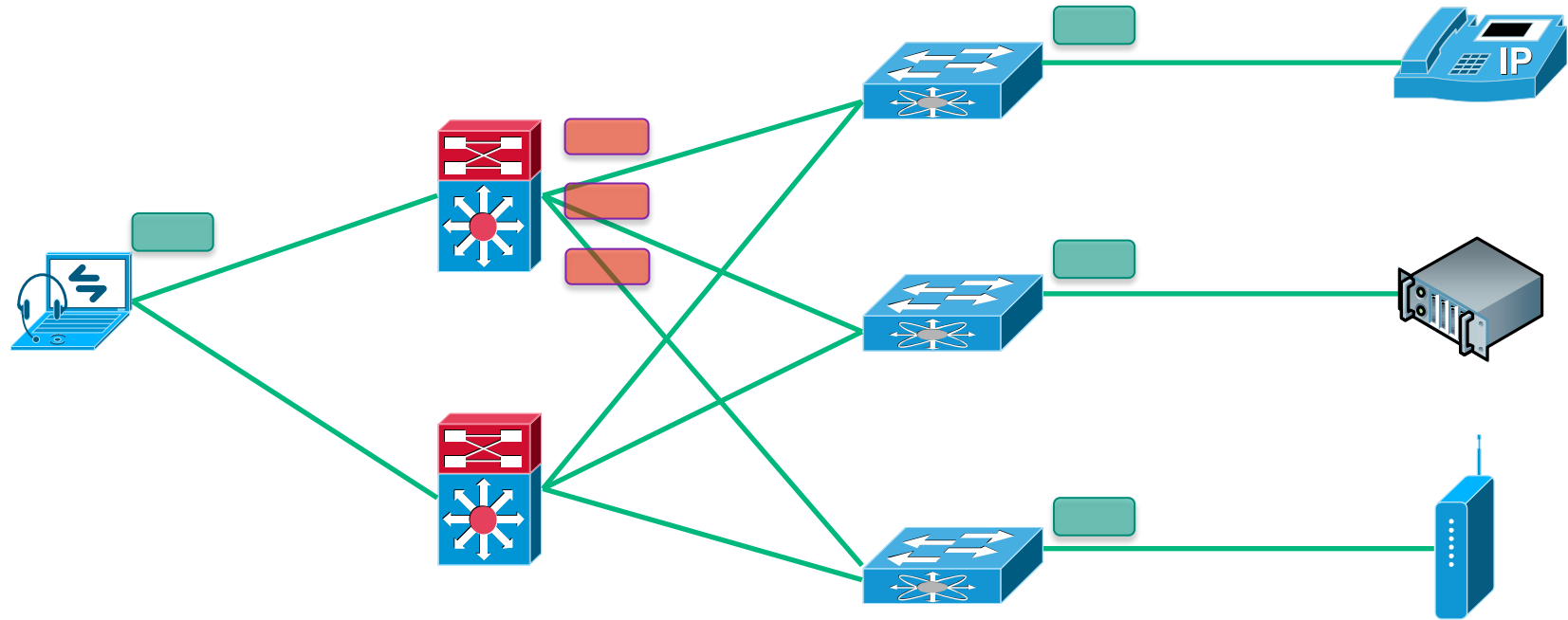
UDP Unicast

Neighbor Discovery – CDP



CDP

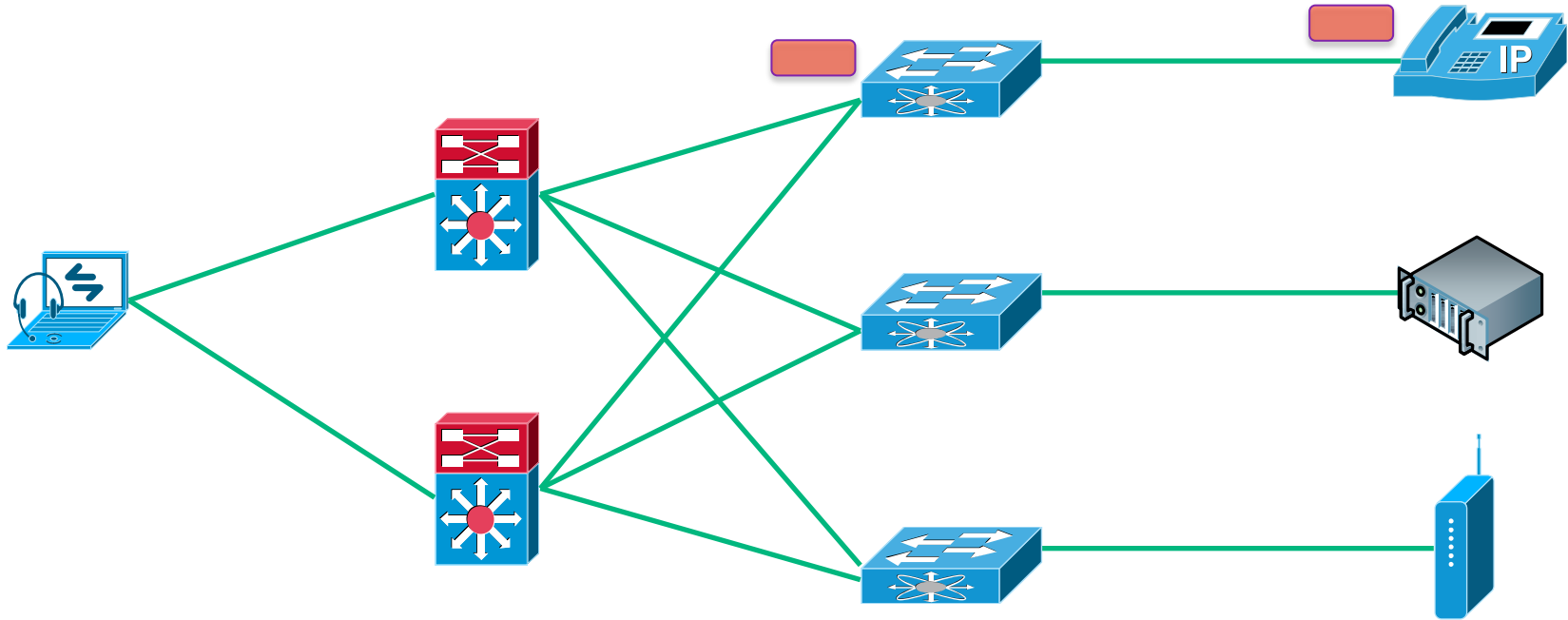
Queries



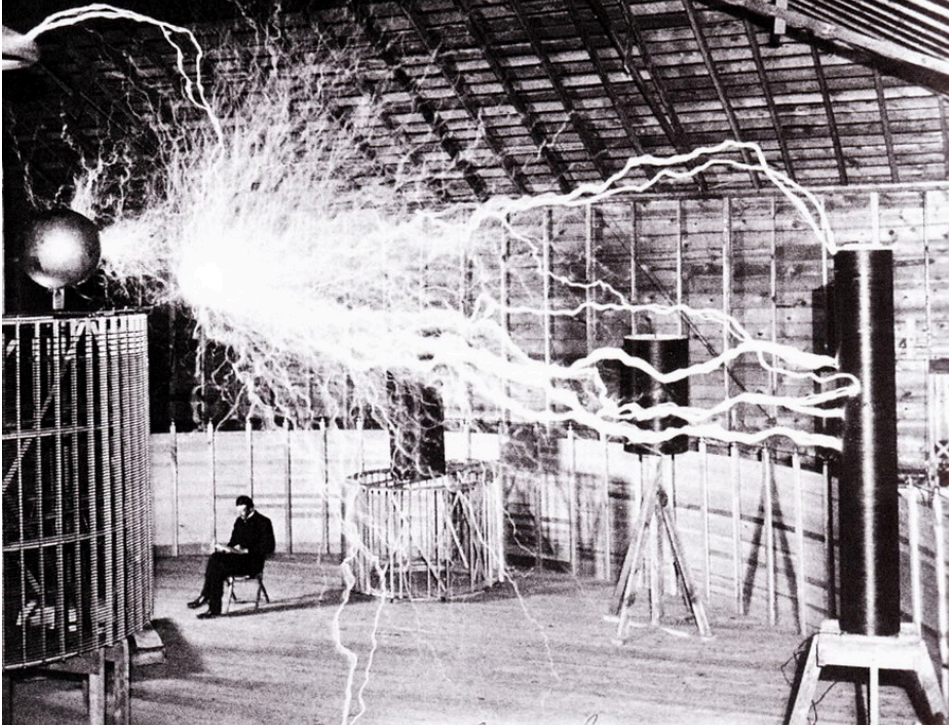
TCP Unicast

UDP Unicast

Queries – Answers



UDP Unicast



Demo

EW Attributes

- Importance
- Role
- Keyword
- Level
- Name

Levels

Category	Level	Description
Operational	10	Full
	9	High
	8	Reduced
Standby	7	Medium
	6	Frugal
	5	Ready
	4	Low
	3	Standby
Non-operational	2	Sleep
	1	Hibernate
	0	off

Well said...

... but does it matter?



Relevance?



- [SmartCities] will be at least interact with/require Energy Management Protocols
- Already a relevant number of [SmartBuildings] out there.
- Two of the five biggest companies in Germany are thinking about deploying EngeryWise at this very moment.

From a German Train

No.	Time	Source	Destination	Protocol	Length	Info
36	12.034912000	10.56.150.165	10.56.150.255	BROWSER	253	Domain/Workgroup Announcement MUC, NT Workstation,
37	12.631900000	Men-Mikr_02:40:94	Broadcast	ARP	56	Who has 10.56.150.232? Tell 10.56.150.129
38	12.827369000	10.56.150.168	10.56.150.255	NBNS	92	Name query NB ACHILLES<20>
39	13.059263000	10.56.150.152	255.255.255.255	UDP	510	Source port: 52897 Destination port: ew-disc-cmd
40	13.421932000	3c:a9:f4:52:f5:54	Men-Mikr_02:40:94	ARP	42	Who has 10.56.150.129? Tell 10.56.150.235
41	13.425307000	Men-Mikr_02:40:94	3c:a9:f4:52:f5:54	ARP	56	10.56.150.129 is at 00:c0:3a:02:40:94

```

> Frame 39: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits)
> Ethernet II, Src: IntelCor_af:93:2c (00:24:d7:af:93:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.56.150.152 (10.56.150.152), Dst: 255.255.255.255 (255.255.255.255)
> User Datagram Protocol, Src Port: 52897 (52897), Dst Port: ew-disc-cmd (43440)

```

EnergyWise

```

Unknown: 0002
Pad: 000000000000
Unknown: 0011
Unknown: 0014

```

```
Hash: 8a474988ecc228b09ebd80d9fadc89398d28eaea
```

```
Sequence Number: 176819
```

EnergyWise ID

```

Message Type: 0100
Importance: 100
Unknown Field: 0a110e000a
Length of TLV table: 388
Number of TLVs in table: 16

```

EnergyWise Domain

Internet-wide Scan



- We also performed an Internet-wide scan for EnergyWise
 - Problem: No simple discovery possible (HMAC + further device details needed, handshake necessary)
 - Approach: Search for Port 43440 and perform host discovery (ie to check for Cisco devices)
 - Slow!

Some numbers

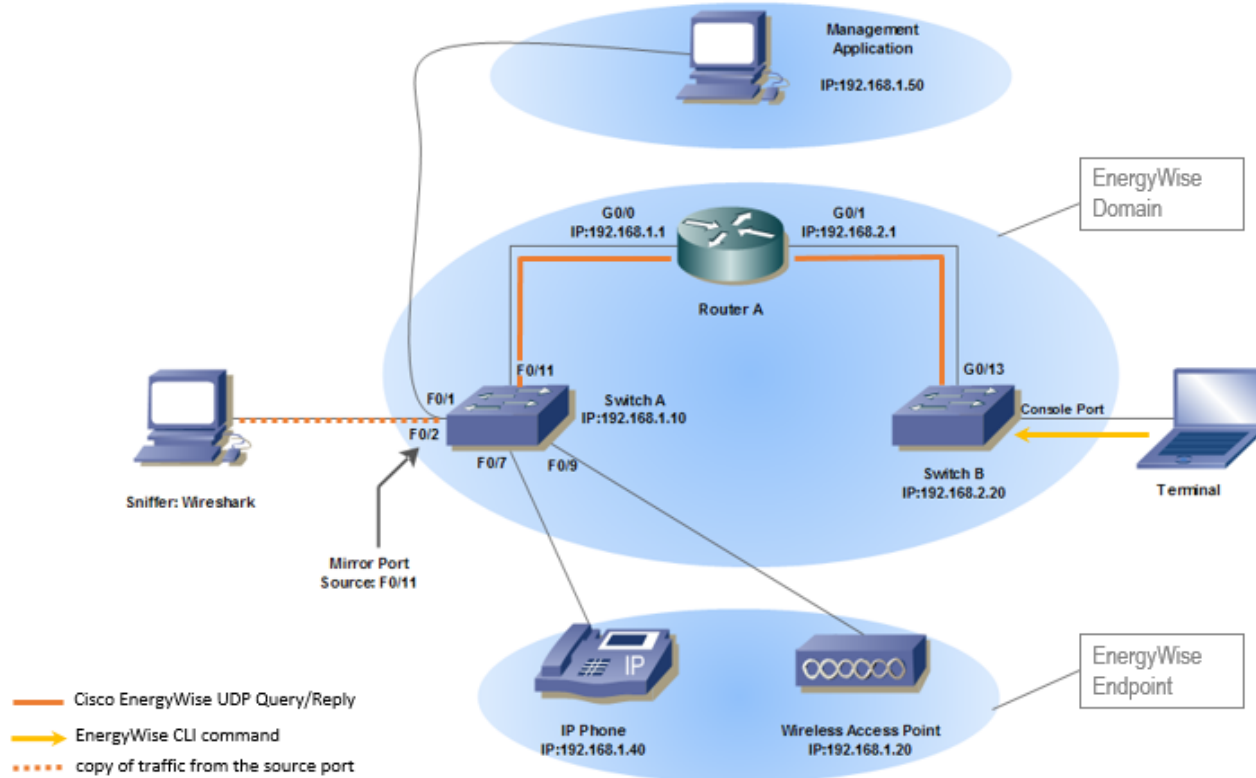


- 1.7mio hosts with TCP 43440 open
- Host discovery 5% done
- In those 5%, four identified Cisco devices
- => EnergyWise most likely already available on some Internet-exposed systems.

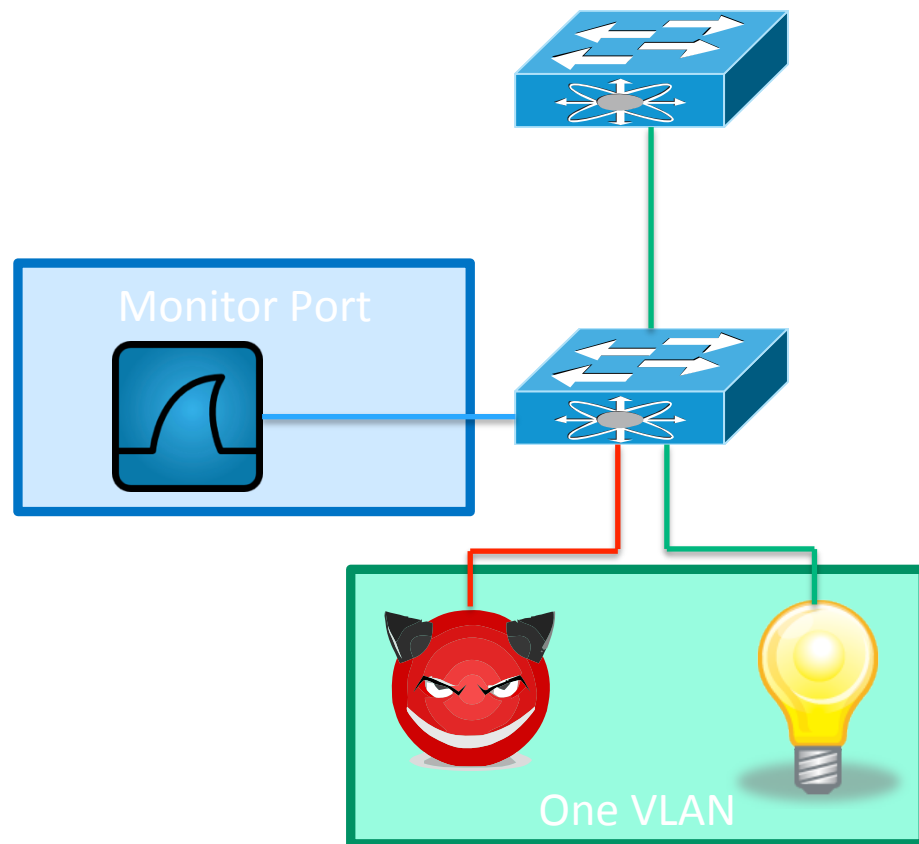
How does it actually work?

Protocol Reversing & Packet Structure





Our Lab



BlackHat Lab

Protocol RE

Main Idea

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF	
00	02	00	00	00	00	00	00	00	10	00	14	5E	87	74	CA	^#tE	
62	68	70	AC	C9	59	54	58	0B	42	E4	53	FA	4A	49	96	bhp-ÉYTX.BâSûJI-	
00	5C	CB	F0	57	53	2D	43	32	39	36	30	53	2D	32	34	.\\E8WS-C2960S-24	
54	53	2D	53	00	00	56	30	33	46	4F	43	31	36	34	37	TS-S..V03FOC1647	
5A	33	53	39	01	00	64	0A	11	0A	00	0A	00	89	00	08	Z3S9..d.....%. .	
00	00	00	08	00	00	00	18	00	00	00	00	53	77	69	74	Swit	
63	68	44	6F	6D	61	69	6E	00	00	00	17	00	00	00	1C	chDomain.....	
00	00	00	00	00	02	A9	B0	C0	A8	02	14	00	00	00	00	@°À.....	
00	00	00	00	00	00	00	31	00	00	00	0E	00	00	00	00	1.....	
00	10	00	00	00	21	00	00	00	10	00	00	00	00	D1	3D	!.....N=	
27	C5	00	00	00	09	00	00	00	0D	00	00	00	00	01	2A	00	'A.....*.
00	00	0E	00	00	00	0D	00	00	00	00	00	00	00	00	21	00	!
00	00	00	10	00	00	00	00	D1	3D	27	C5	00	00	00	29	00	N='A...)
00	00	00	0D	00	00	00	00	06								00	

- Identifying text strings
- Identifying environmental dependencies (IP, MAC, Date, Time)
- Identifying Cisco EnergyWise parameter (Importance, Name, Level)
- Identifying meta fields (fields describing other fields)

Protocol Reverse Engineering

Importance																Length																
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00	02	00	00	00	00	00	00	00	10	00	14	5E	87	74	CA		^	t	Ê													
62	68	70	AC	C9	59	54	58	0B	42	E4	53	FA	4A	49	96	bhp-	É	Y	T	X.	B	a	S	ú	J	I	-					
00	5C	CB	F0	57	53	2D	43	32	39	36	30	53	2D	32	34	.\	Ë	ö	W	S-	C	2	9	6	0	S	-	2	4			
54	53	2D	53	00	00	5	30	33	46	4F	43	3	36	34	37	TS-	S	..	V	0	3	F	O	C	1	6	4	7				
5A	33	53	39	01	00	64	0A	11	0A	00	0A	00	89	00	08	Z3	S	9	..	d		%	..									
00	00	00	08	00	00	00	18	00	00	00	00	53	77	69	74																	
63	68	44	6F	6D	61	69	6E	00	00	00	17	00	00	00	1C	ch	Domain															
00	00	00	00	00	02	A9	B0	C0	A8	02	14	00	00	00	00		©	°	À	..												
00	00	00	00	00	00	00	31	00	00	00	0E	00	00	00	00		1															
00	10	00	00	00	21	00	00	00	10	00	00	00	00	D1	3D		!															
27	C5	00	00	00	09	00	00	00	0D	00	00	00	01	2A	00	'	Å															
00	00	0E	00	00	00	0D	00	00	00	00	00	00	00	00	21																	
00	00	00	10	00	00	00	00	D1	3D	27	C5	00	00	00	29																	
00	00	00	0D	00	00	00	00	06	IP address																							

IP address

UDP Packet

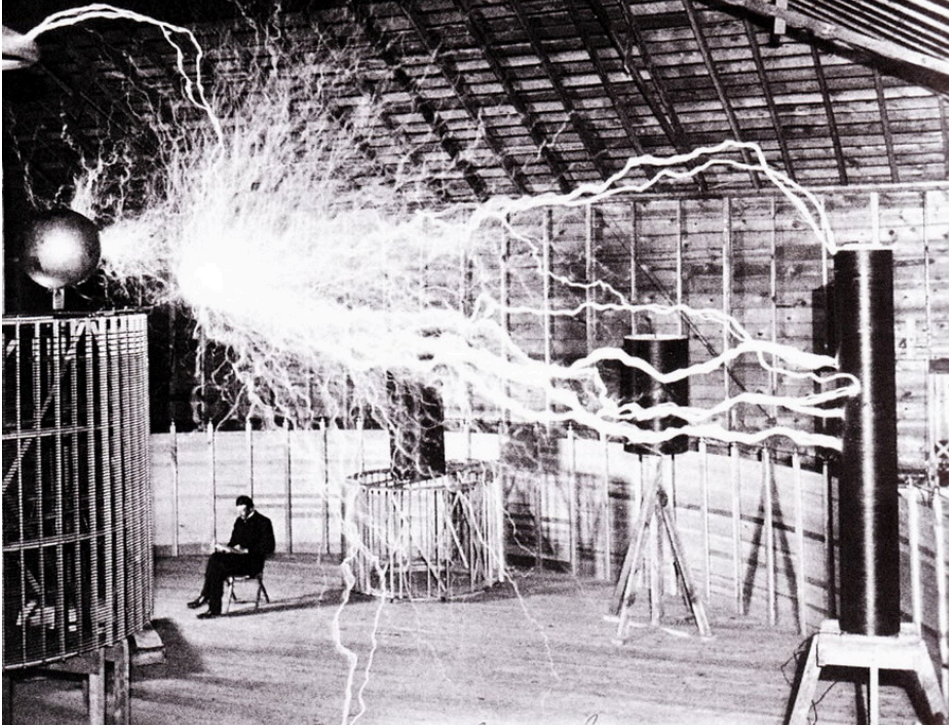
0x02	PAD	0x10	0x14	HMAC	Sequence Number
------	-----	------	------	------	-----------------

	EnergyWise ID	Message Type	Importance	Unknown	Length of TLV table	Number of TLVs in table	TLVs
	Model Number	Version ID	System Serial Number				

TCP Packet

0x02	PAD	0x12	0x14	HMAC	Sequence Number
------	-----	------	------	------	-----------------

	UUID	Message Type	Importance	Unknown	Length of TLV table	Number of TLVs in table	TLVs
--	------	--------------	------------	---------	---------------------	-------------------------	------



Demo

Relevant Protocol Details



- Authentication: HMAC
 - Management Secret vs. Domain Secret vs. Endpoint Secret
- Sequence number
- UUID vs. EW-ID

Hacking EnergyWise



```
+ Ethernet II, Src: Dell_e3:df:4e (00:24:e8:e3:df:4e), Dst: Ci
+ Internet Protocol Version 4, Src: 192.168.2.65 (192.168.2.65
+ User Datagram Protocol, Src Port: 54252 (54252), Dst Port: e
- Energywise
    Unknown: 0002
    Pad: 000000000000
    Unknown: 0010
    Unknown: 0014
    Encrypted Data: 0000000000000000000000000000000000000000
    Sequence Number: 6081520
+ Energywise ID
    Message Type: 0100
    Importance: 100
    Unknown Field: 0a110a000a
    Length of TLV table: 137
    Number of TLVs in table: 8
+ Energywise Domain
+ Energywise Reply To
+ Energywise ???
+ Energywise ???
+ Energywise Name (query)
+ Energywise Level (query)
+ Energywise ???
- - -
```

TLV Protocol?

How would you not fuzz this?

Dizzy Script (dizzy: c0decafe.de)

```
field("Unknown", 16, "\\x00\\x02", full),  
field("PAD", 48, "\\x00\\x00\\x00\\x00\\x00\\x00", none),  
field("Unknown", 16, "\\x00\\x10", full),  
field("Unknown", 16, "\\x00\\x14", full),  
field("Encrypted_Data", 160, "\\x5E\\x87\\x74\\xCA\\x62\\x68\\x70\\xAC\\  
field("Sequence_Number", 32, "\\x00\\x5c\\xcb\\xf0", none),  
field("EnergyWise_ID", 256, "\\x57\\x53\\x2D\\x43\\x32\\x39\\x36\\x30\\x  
field("Message_Type", 16, "\\x01\\x00", none),  
field("EnergyWise_Importance", 8, "\\x64", none),  
field("Unknown_Field", 40, "\\x0A\\x11\\x0A\\x00\\x0A", none),  
field("Length_of_TLV_table", 16, "\\x00\\x89", none),  
field("Number_of_TLVs_in_table", 16, "\\x00\\x08", none),
```

Fuzzing Results

```
Switch8#  
01:33:23 UTC Wed Mar 30 2011: Unexpected exception to CPUvector  
-Traceback= 0x108C0CCz 0x539408z 0x538028z 0x538128z 0xE8642Cz 0x  
Writing crashinfo to flash:/crashinfo_ext/crashinfo_ext_2
```

- A system crash can be caused by a malformed packet.
- The devices crashes when the following query is sent:
 - the tenth byte in the header has the value 0x15.
 - The valid value is 0x10.
- <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140806-energywise>

Fuzzing Results

- A system crash can be caused by a malformed packet.

```
SwitchB#
```

```
01:33:23 UTC Wed Mar 30 2011: Unexpected exception to CPUvector  
-Traceback= 0x10BC0CCz 0x539408z 0x538028z 0x538128z 0xE8642Cz 0x
```

```
Writing crashinfo to flash:/crashinfo_ext/crashinfo_ext_2
```

sa-20140806-energywise

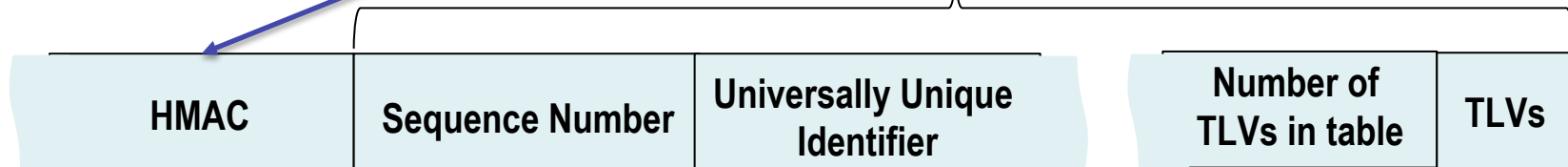
Authentication?

- Shared-secret based
- First naïve approach: Replay
 - Which worked!

Results

– Authentication EnergyWise over TCP

```
KEY    = HMAC_SHA1 (UUID, SECRET)
HMAC   = HMAC_SHA1 (KEY, DATA)
```



Results

– Authentication EnergyWise over UDP

$\text{HMAC} = \text{HMAC_SHA1}(\text{SECRET}, \text{DATA})$

HMAC

Sequence Number

**Universally Unique
Identifier**

**Number of
TLVs in table**

TLVs

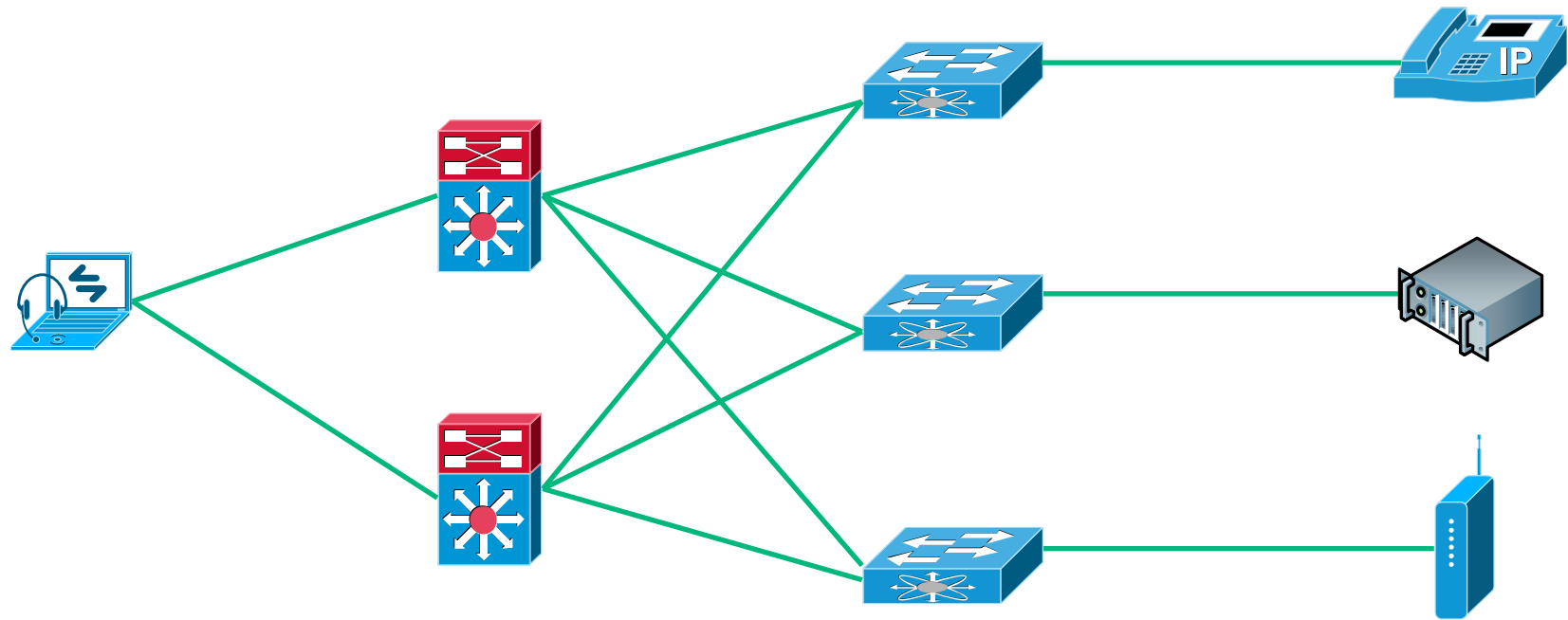
Resulting Problems

- Reverse engineered HMAC algorithm allows cracking.
- Resulting attack path:
 - ① Sniff an HMAC
 - ② Crack the Secret
 - ③ Hijack the Domain

Sniff the Secret

- Flooding-based protocol
 - Sniffing is almost too easy
- However:
 - Management Secret vs. Domain Secret
vs. Endpoint Secret

Different Types of Secrets



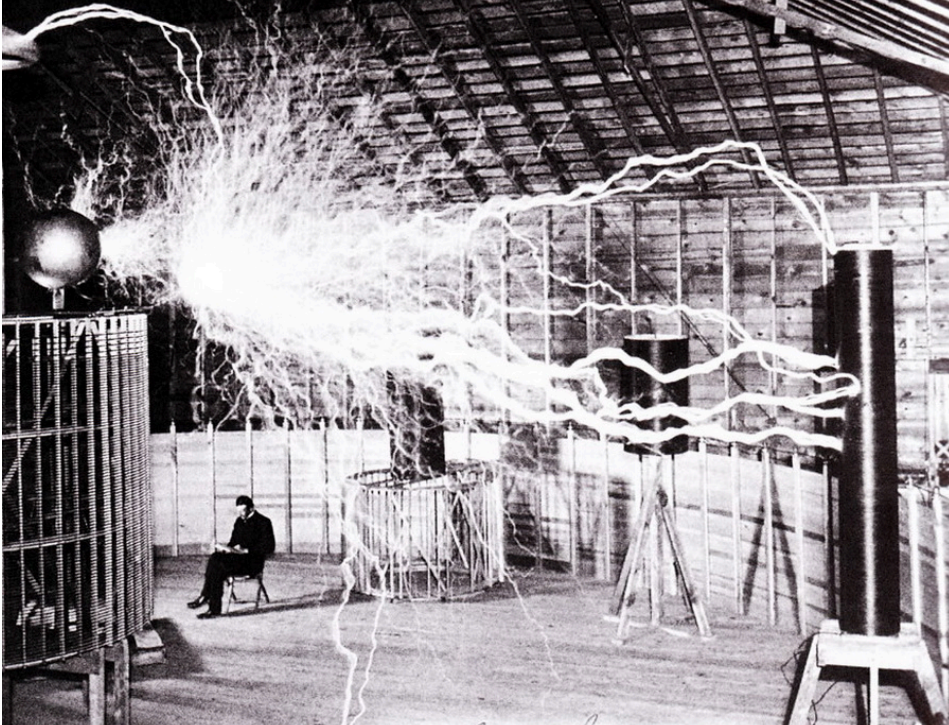
Crack the Secret

- EW is supposed to cover the whole data center – how likely is a key change on a regular base?
 - Device can only be members of one domain – at least according to design guide, does not apply to our tools ;)
- **Still, strong secrets will help.**
 - However, not giving any numbers on SHA1 cracking speeds – guess the guys over at Passwords¹⁴ will improve that again anyways ;)

Hijack the Domain

- This is where our tools come into play... ;-)





Demo

Problems

- Compromised server/domain member
 - Best case: No hijacking possible, 43440 filtered in local packet filters
 - Most likely case (at least): Shut down all servers in your segment
 - Worst case: Shut down the whole data center

Organizational Problems

– Devices sold on eBay?

- Experienced 7-10 times over the last 10 years buying a device on eBay including its configuration.
 - => one time even from one of our customers!

Controls



The obvious ones...

- Use strong shared-secrets.
- Use ntp-shared-secrets
- Use different secrets
 - Management vs. Domain vs. Endpoint



More specific...

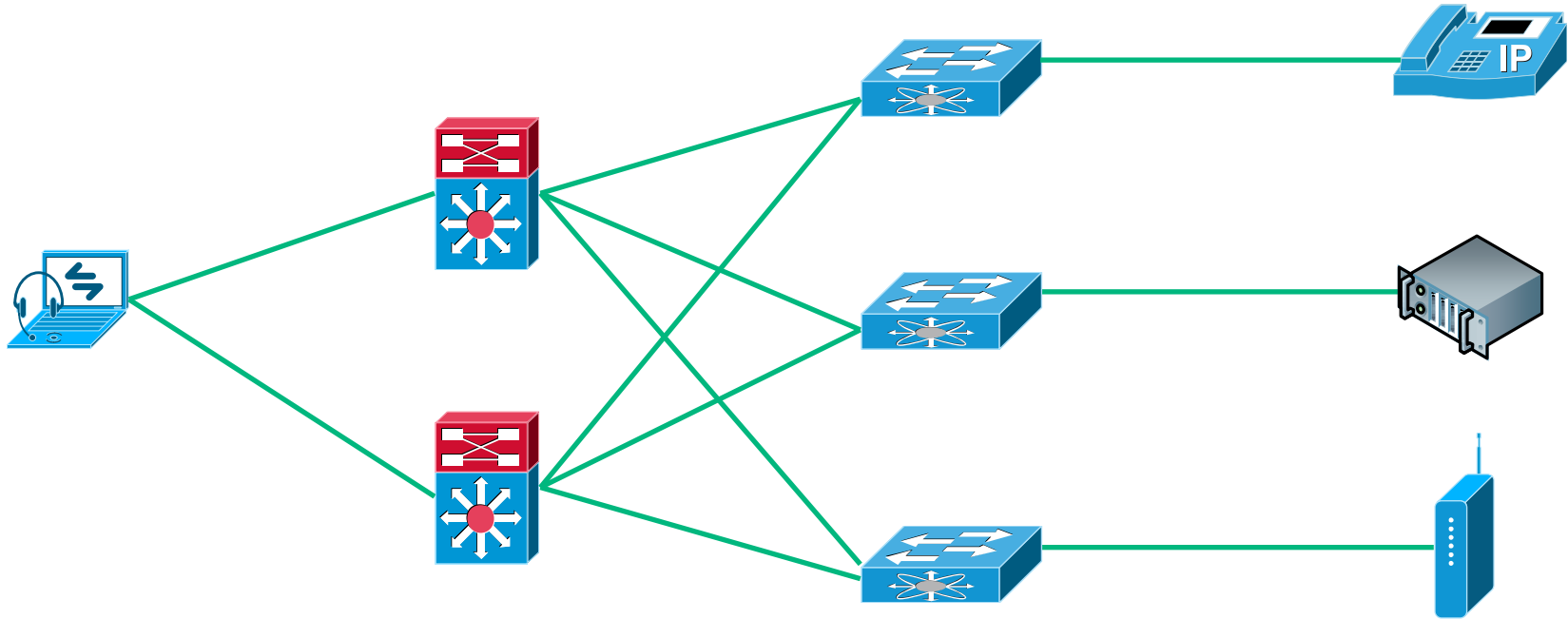
- Purge configurations during decommissioning
- If EnergyWise is only used for monitoring power usage, disable the ability to set power levels
 - no energywise allow query set
- Or of course, actual crypto...

Segmentation

- Segmentation: Use different EnergyWise domains, where possible
 - “Take your IP Phone with you”
- Segmentation & Filtering: restrict EnergyWise ports to the local subnet.
- Currently talking about including this in the EW design guide with cisco



Segmentation



Future Work & Conclusions

Future Work



- Port tools to Loki modules
- Analyze few missing protocol details
- More efficient cracker
- Hardening guide

Conclusions



- EnergyWise contains Security Mechanisms
 - However, pure PSK-based security is not appropriate anymore for 2014 infrastructure protocols
- Good old basic principles still apply: Segmentation!
- You got the toolset to assess EnergyWise domains if you encounter them ;-)
 - ... and probably some arguments when someone wants to introduce EW in your environment.

There's never enough time...

THANK YOU...



@uchi_mata



akoca@ernw.de
mluft@ernw.de



...for yours!

Code & Slides:

<https://www.insinuator.net>
(..soon)

Shout Outs



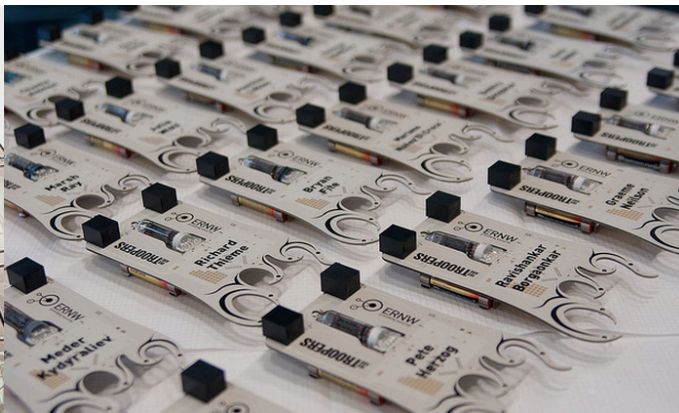
- Angus Blitter, @BryanFite
 - ... for bringing our attention to EnergyWise.
- Florian Horsch, @flouSH
 - ... for printing the awesome demo device.
- Florian Barth, @der_cthulhu
 - ... for soldering the awesome demo device.
- Felix Wilhelm, @_fel1x
 - ... for support in some RE work.
- Enno Rey, @Enno_Insinuator
 - ... for great overall support and feedback.
- Daniel Mende, c0decafe.de
 - ... for performing the Internet-wide scans.
- Niki Vonderwell, @NikiVonderwell
 - ... for some inspiration on the slide work.



Join us for TROOPERS15



Workshops, Conference, Roundtables, PacketWars Hacking Contest, 10k Morning Run, ...



March
16th-20th 2015

Heidelberg,
Germany

www.troopers.de

Sources & References

- [SmartCities]
 - <http://fedscoop.com/will-smart-cities-power-future-cybercrime-mass-surveillance/>
- [SmartBuildings]
 - <http://haxpo.nl/wp-content/uploads/2014/02/D2T1-Alices-Adventures-in-Smart-Building-Land.pdf>
- [EWDesignGuide]
 - Cisco EnergyWise Design Guide



Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners!

