
black hat
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS
APIC's Adventures in Wonderland
#BHUSA @BLACK HAT EVENTS

APIC's Adventures in Wonderland

Oliver Matula
omatula@ernw.de

Frank Block
fblock@ernw.de

APIC's Adventures in ACI Wonderland

Oliver Matula
omatula@ernw.de

Frank Block
fblock@ernw.de

Agenda

Who is this APIC you are talking about?

You said you have found vulns! Where are they?

Ok, fine! But what can I take away from this?

Introduction

The What and the Why

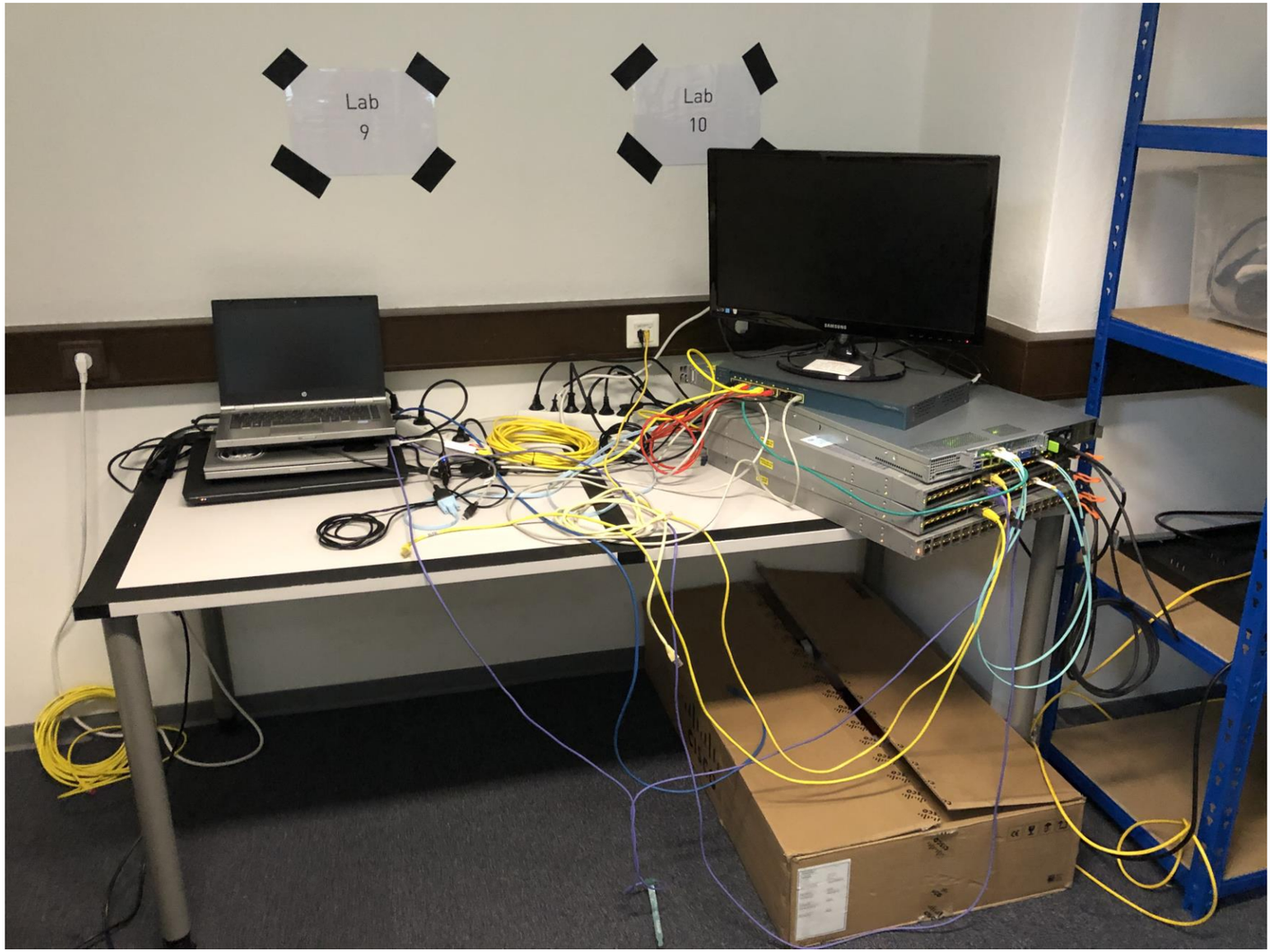
The What

Vulnerability Assessment of
Cisco Application Centric Infrastructure (ACI)

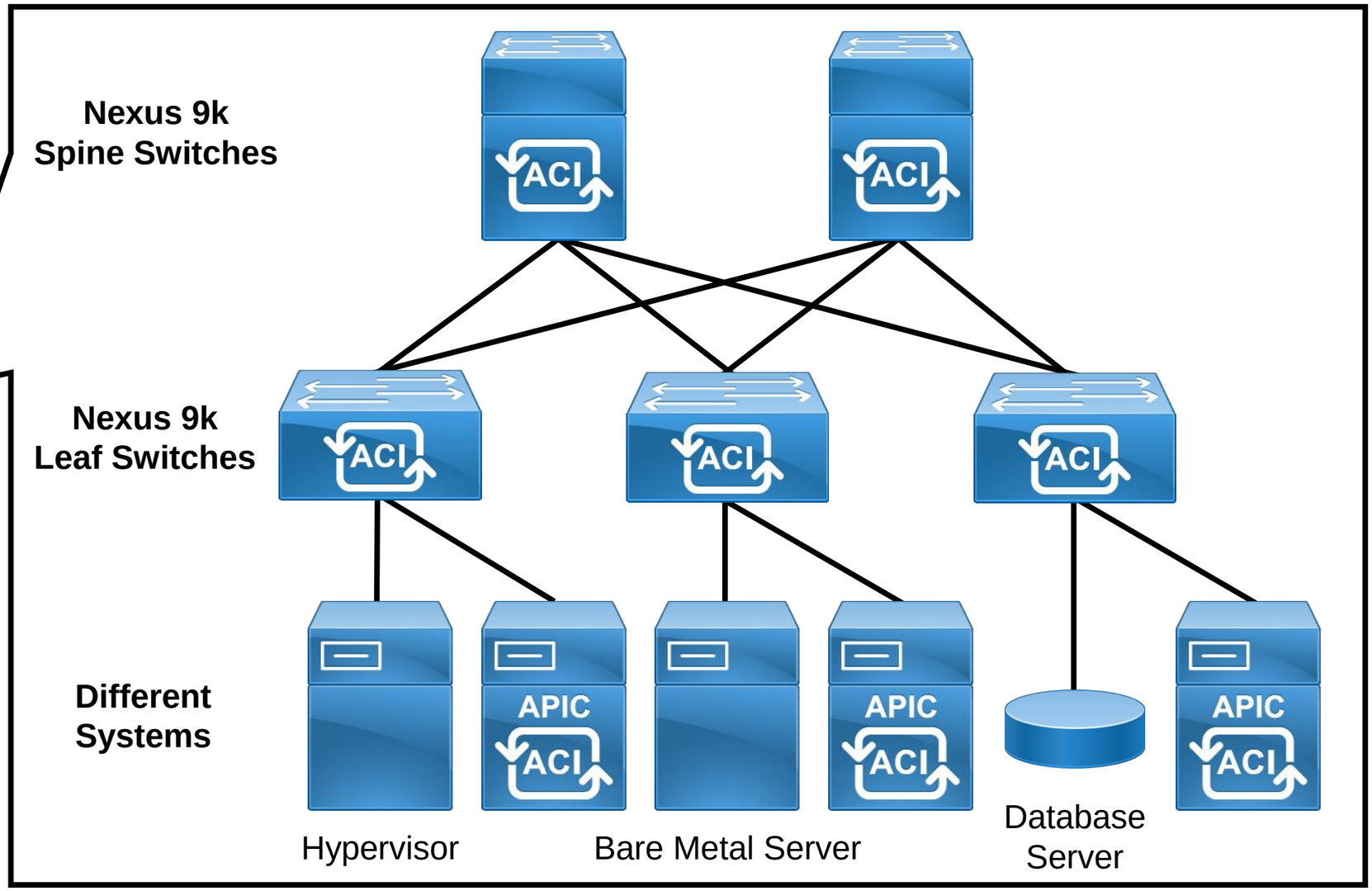
The Why

Not much research has been done,
since Cisco ACI is expensive

Lab Setup



Application Centric Infrastructure



System Details

Nexus 9k Leaf/Spine Switches

- Intel Xeon CPU (64 bit)
- Analyzed mainly Software Version 14.0(3d)
- Wind River Linux (kernel 3.14.62)
- ~300 processes, only two running as non-root user

Application Policy Infrastructure Controller (APIC)

- Intel Xeon CPU (64 bit)
- Analyzed mainly Software Version 14.1(1j)
- CentOS 7 Linux (kernel 4.14.104)
- ~500 processes, only ~20 running as non-root user

Vulnerability #1

The Register®
Biting the hand that feeds IT

Security

Sinister secret backdoor found in networking gear perfect for government espionage: The Chinese are – oh no, wait, it's Cisco again

Better ban this gear from non-US core networks, right?

By Iain Thomson in San Francisco 2 May 2019 at 07:02 151 SHARE ▼

https://www.theregister.co.uk/2019/05/02/cisco_vulnerabilities/

Attacker System

SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22

SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026

Mgmt Interface

Target (Nexus 9k Leaf Switch)

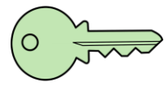
Attacker System

SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22

SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026

User 'local'

Public Key



Mgmt Interface

Target (Nexus 9k Leaf Switch)

Attacker System

SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22

SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026

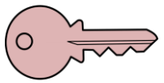
Mgmt Interface

User 'local'

Public Key | Private Key

Target (Nexus 9k Leaf Switch)

Attacker System



Attacker copies private key

Attacker Controlled Nexus 9k Leaf Switch

Firmware Image

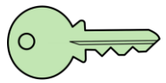
SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22

SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026

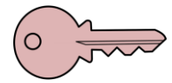
Mgmt Interface

User 'local'

Public Key



Private Key



Target (Nexus 9k Leaf Switch)

Attacker System

SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22

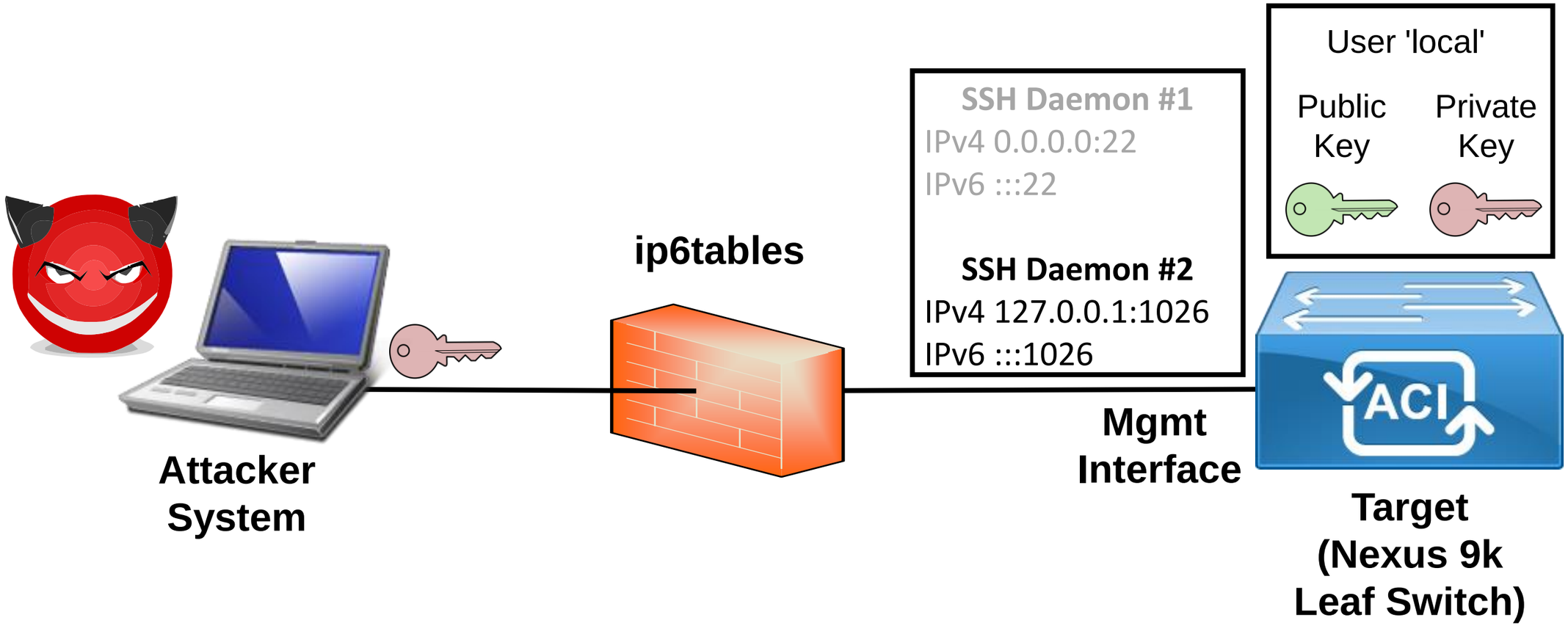
SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026

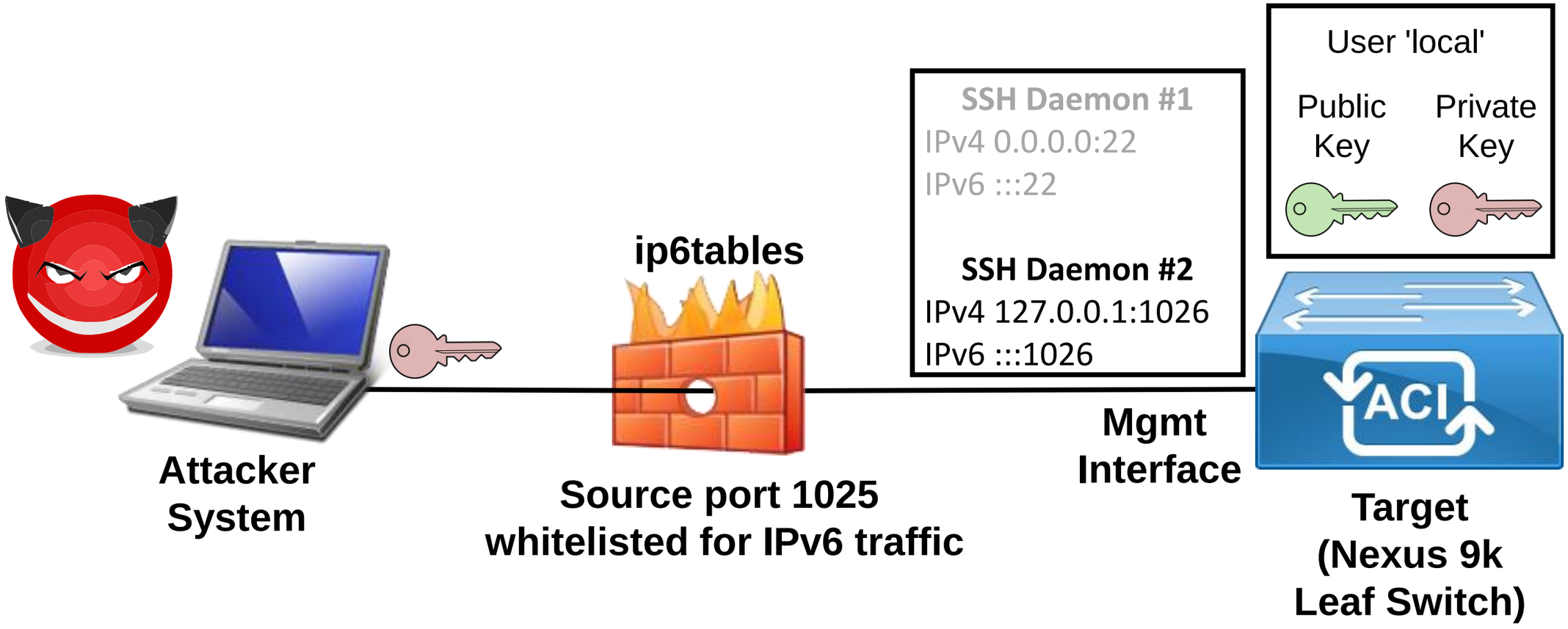
Mgmt Interface

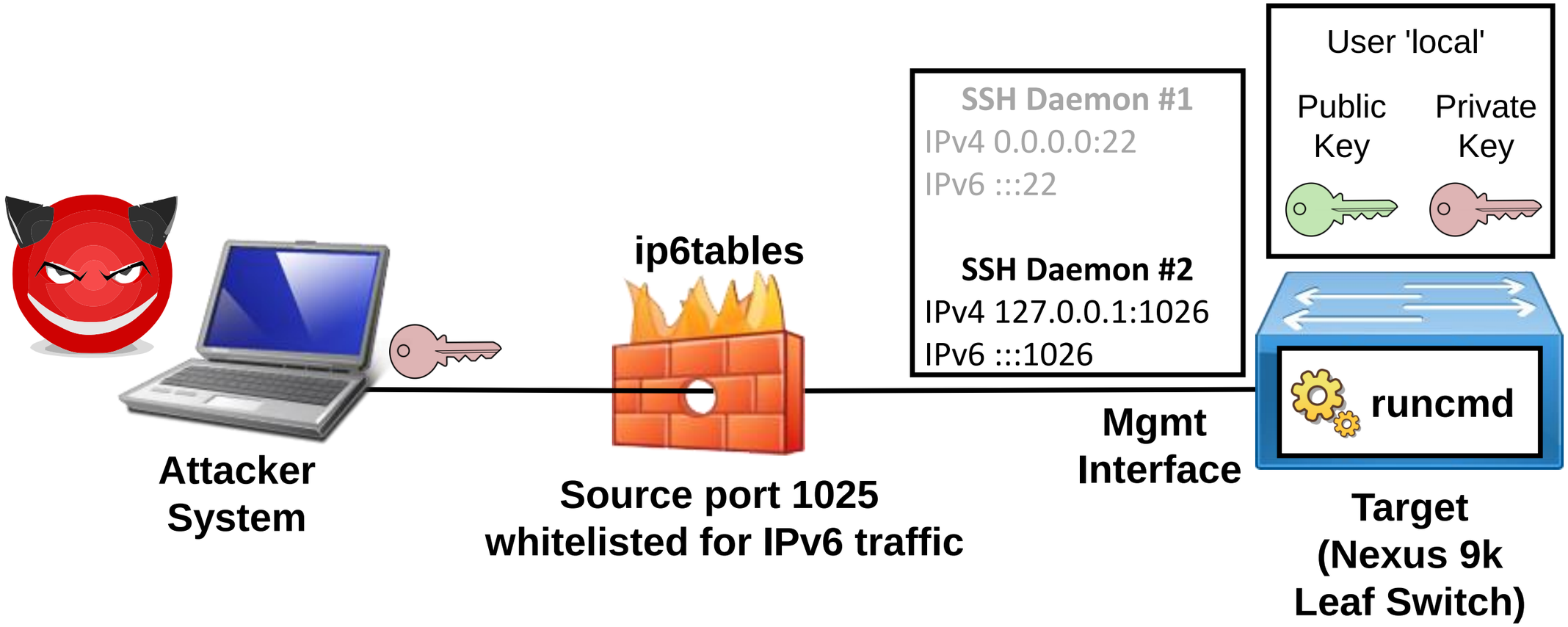
User 'local'

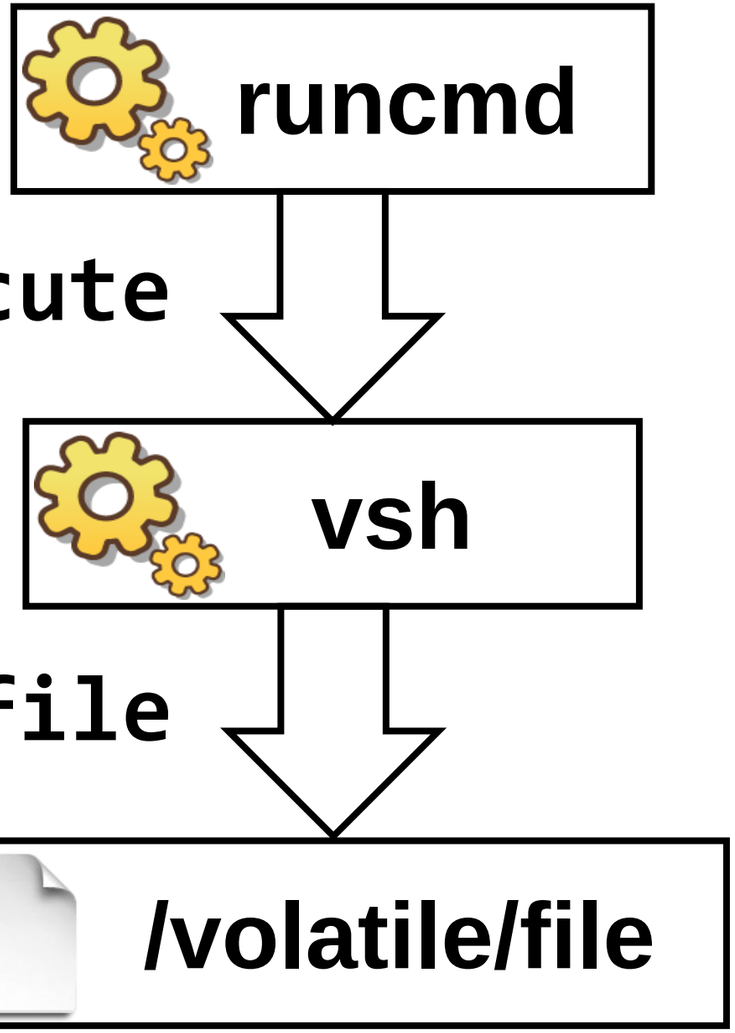
Public Key | Private Key

Target (Nexus 9k Leaf Switch)


User 'local'
Public Key
Private Key
SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22
SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026
ip6tables
ACI
Attacker System
Mgmt Interface
Target (Nexus 9k Leaf Switch)


User 'local'
Public Key
Private Key
SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22
SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026
ip6tables
ACI
Attacker System
Source port 1025 whitelisted for IPv6 traffic
Mgmt Interface
Target (Nexus 9k Leaf Switch)


User 'local'
Public Key
Private Key
SSH Daemon #1
IPv4 0.0.0.0:22
IPv6 :::22
SSH Daemon #2
IPv4 127.0.0.1:1026
IPv6 :::1026
ip6tables
runcmd
Attacker System
Source port 1025 whitelisted for IPv6 traffic
Mgmt Interface
Target (Nexus 9k Leaf Switch)




```
echo 'test' > file
```

Path Traversal Fails

```
echo 'test' > /tmp/file
echo 'test' > ../tmp/file
echo 'test' > bootflash:../tmp/file
echo 'test' > volatile:../tmp/file
```

Path Traversal Win

```
echo 'test’ >
bootflash:lxc/CentOS7/rootfs/tmp/../../tmp/file
```

`/bootflash/lxc/CentOS7/rootfs/tmp`
is symbolic link to `/var/volatile/tmp`

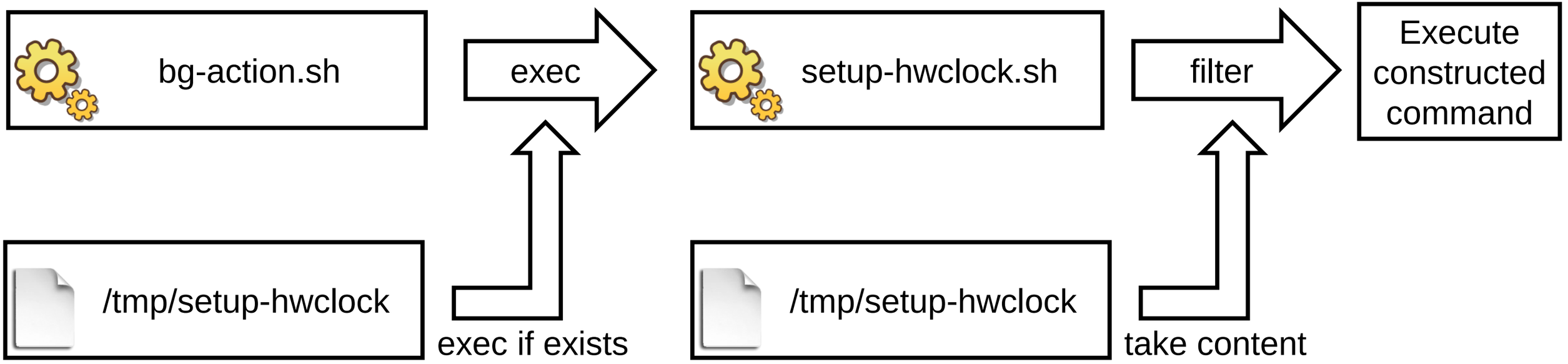
Path Traversal Win

```
echo 'test’ >
bootflash:lxc/CentOS7/rootfs/tmp/../../tmp/file
```

```
/bootflash/lxc/CentOS7/rootfs/tmp
```
is symbolic link to `/var/volatile/tmp`

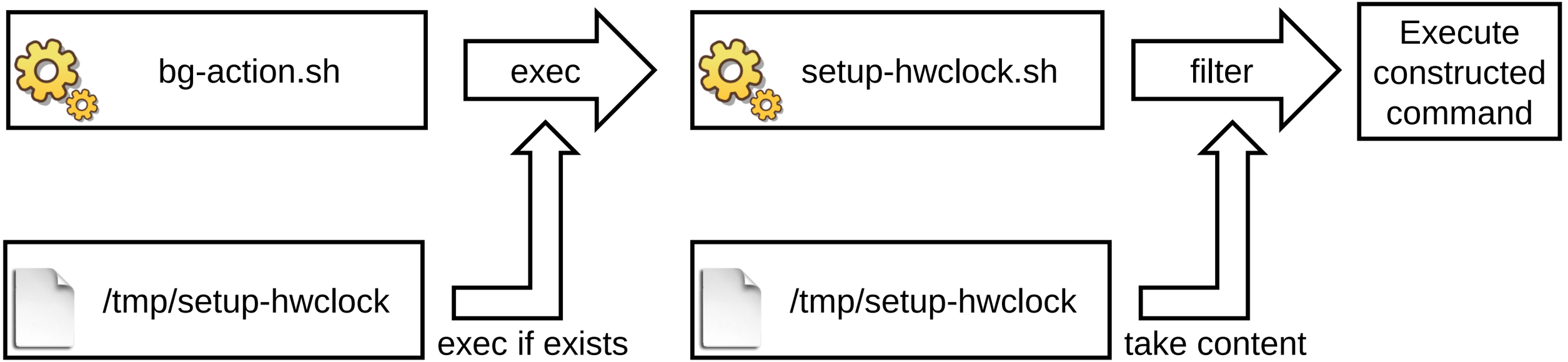
Can write arbitrary files with arbitrary content as user 'local‘ (CVE-2019-1836)

Cron job /bin/bg-action.sh run by root once per min.



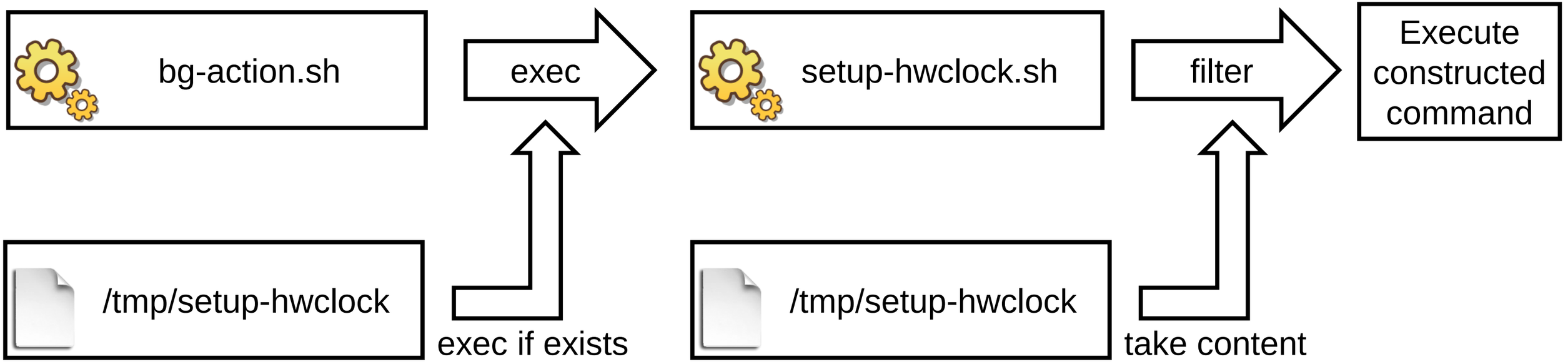
Cron job /bin/bg-action.sh run by root once per min.

Filters ";", "||", "&&", but not "$()"



Cron job /bin/bg-action.sh run by root once per min.

Filters ";", "||", "&&", but not "$()"



Can run arbitrary commands as root user via /tmp/setup-hwclock file (CVE-2019-1803)

Exploit Chain

Finally, chain vulnerabilities to

1. **Upload reverse shell**
2. **Execute reverse shell as root**
3. **Get CVE with Critical CVSS Score 9.8 (CVE-2019-1804)**

Exploit Chain

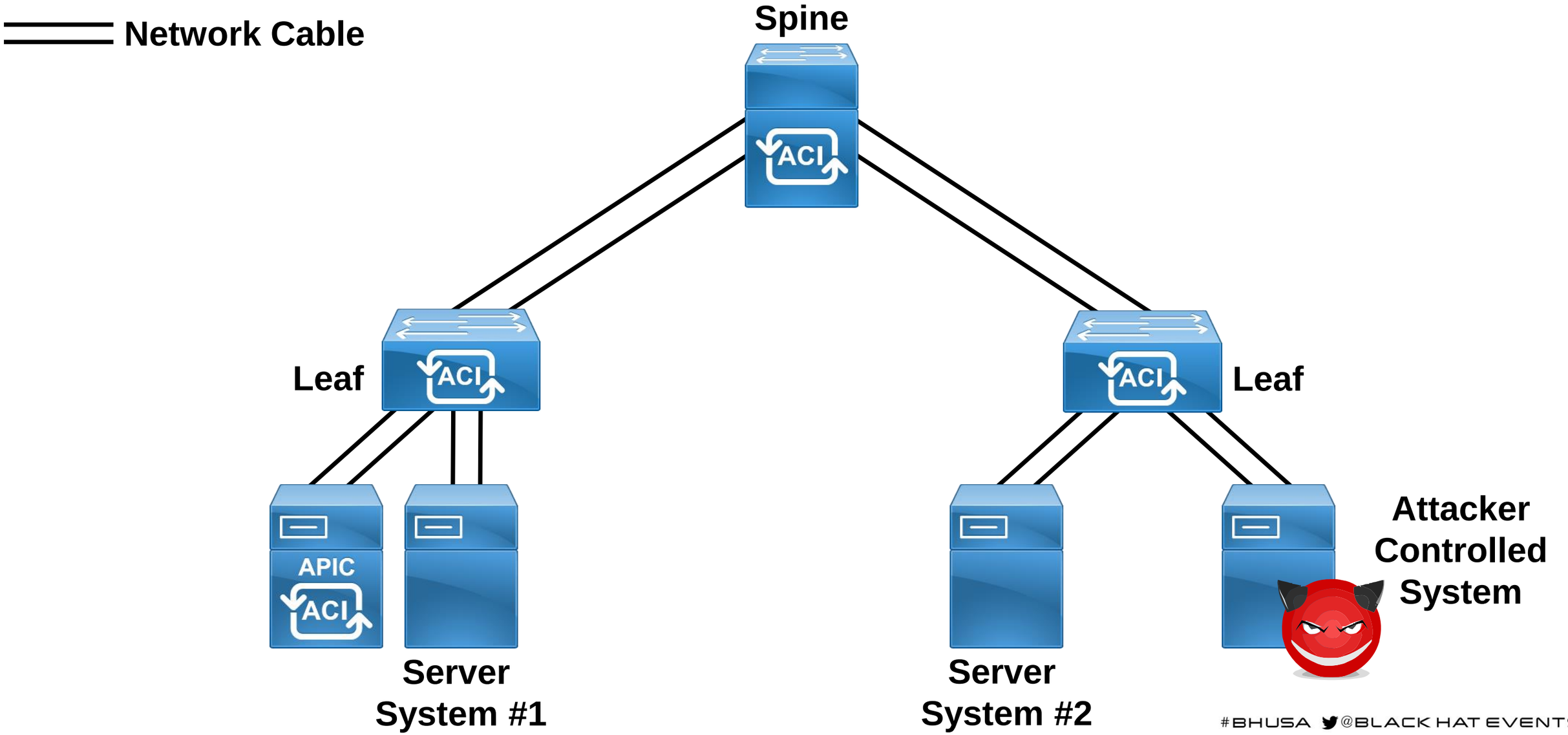
Finally, chain vulnerabilities to

1. **Upload reverse shell**
2. **Execute reverse shell as root**
3. **Get CVE with Critical CVSS Score 9.8 (CVE-2019-1804)**

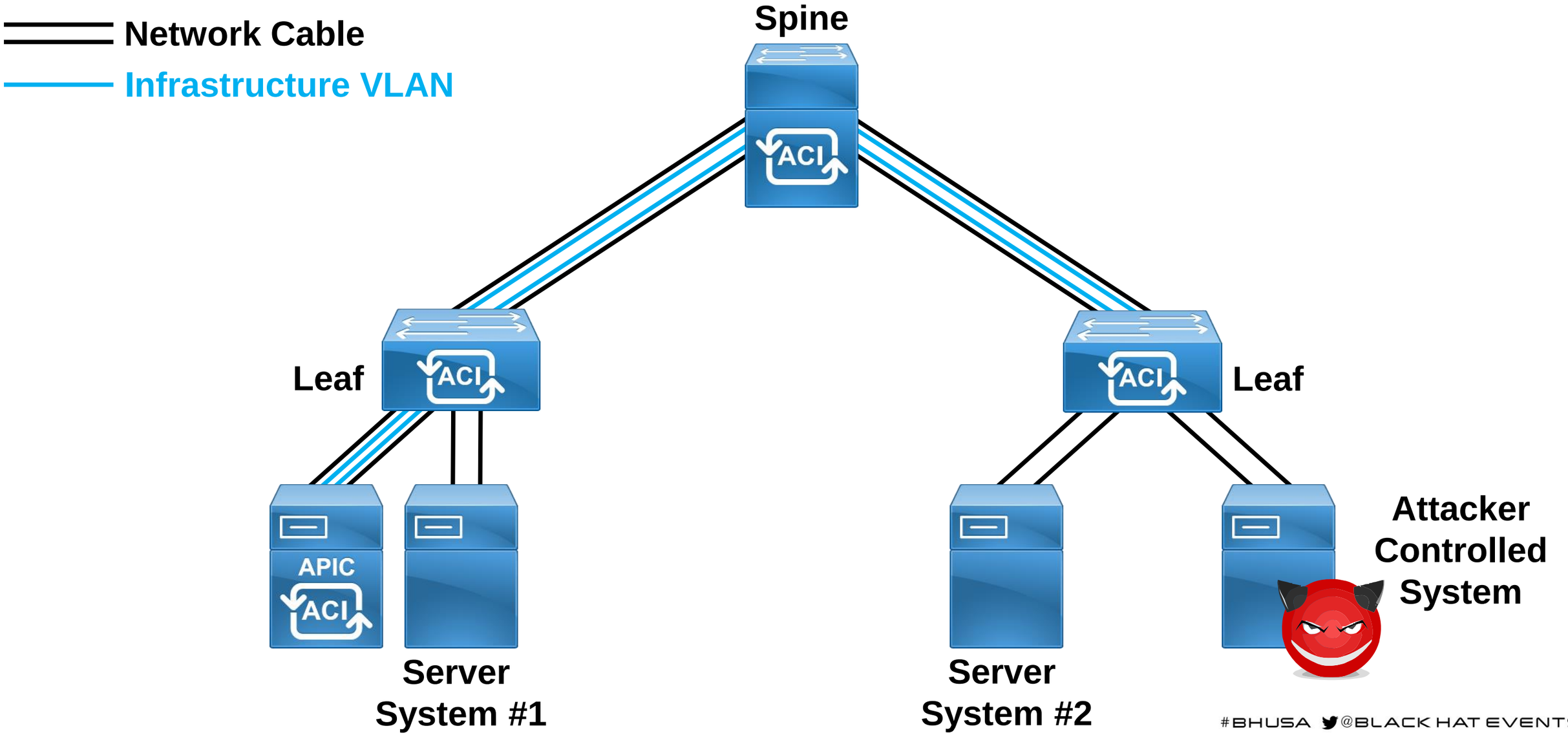
Demo time!

Vulnerability #2

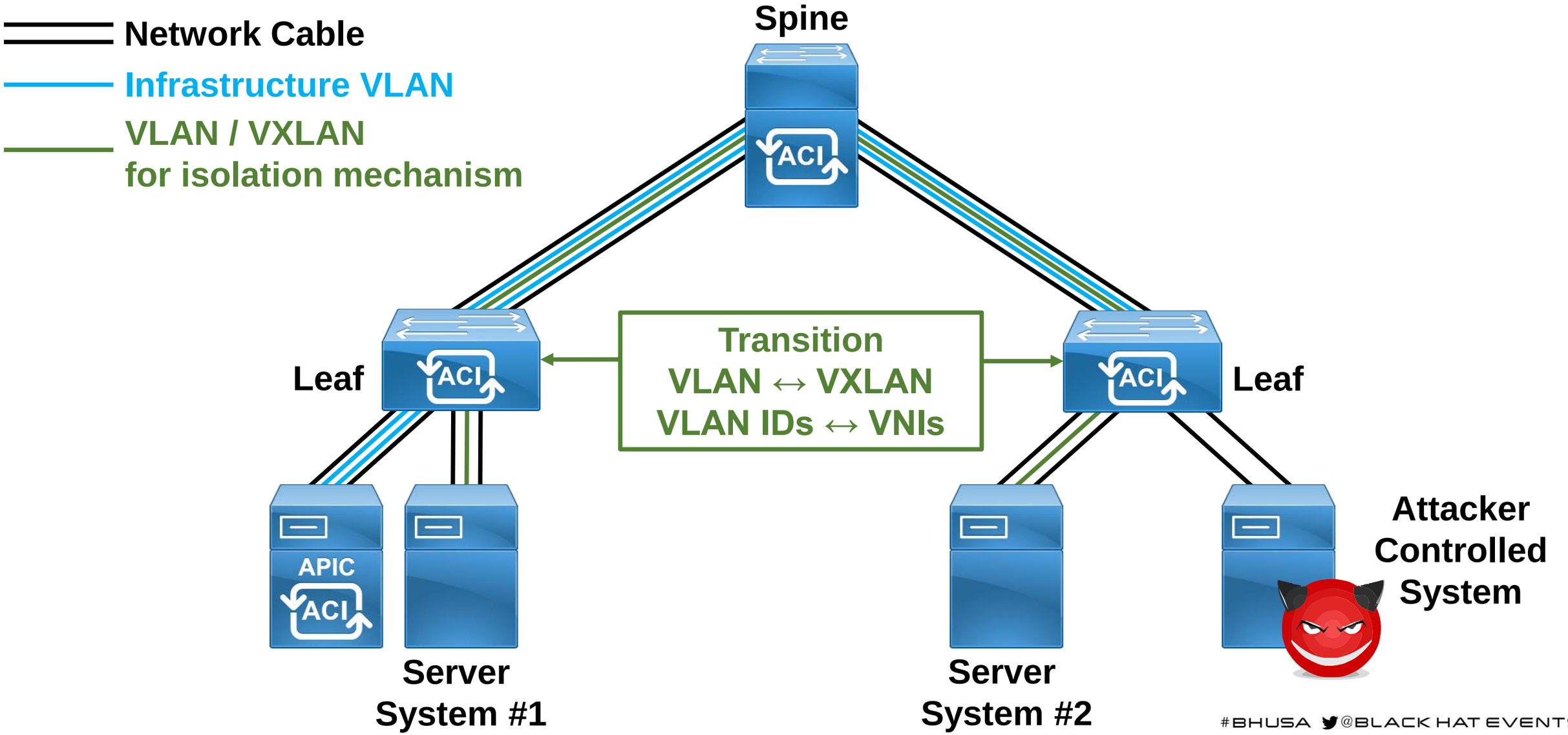
Attack Scenario



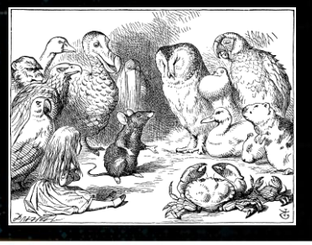
Attack Scenario

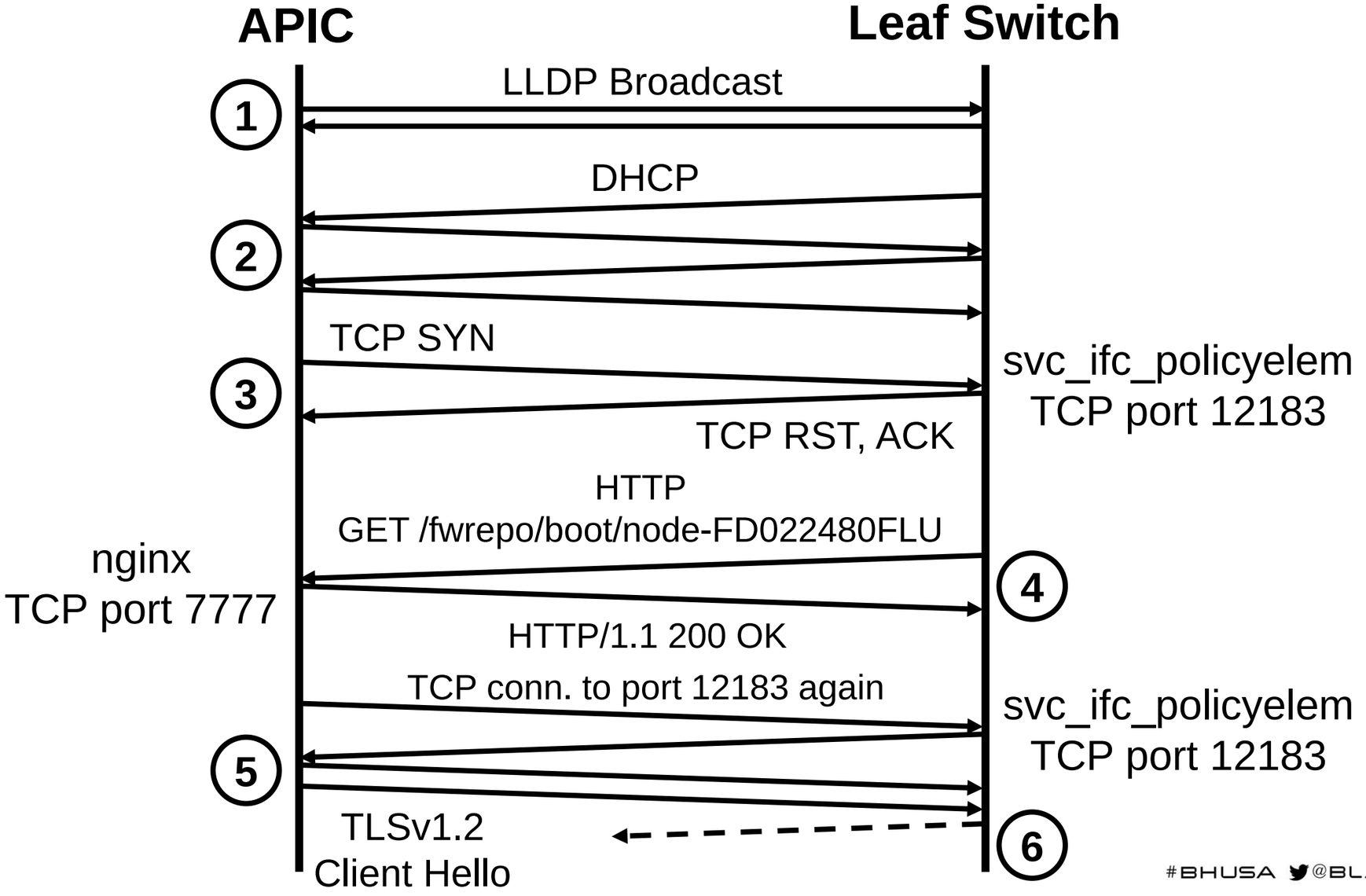


Attack Scenario

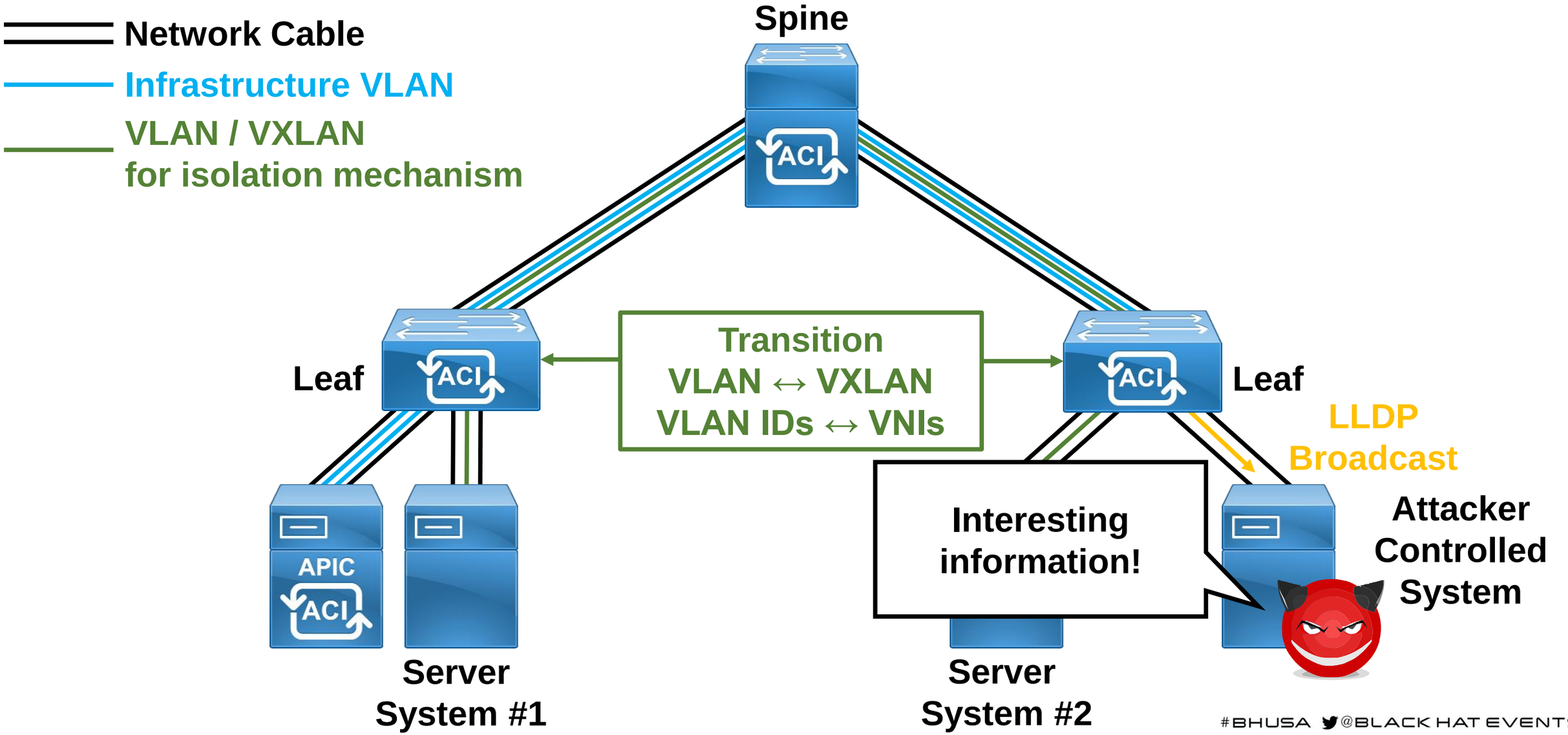


Network Communication

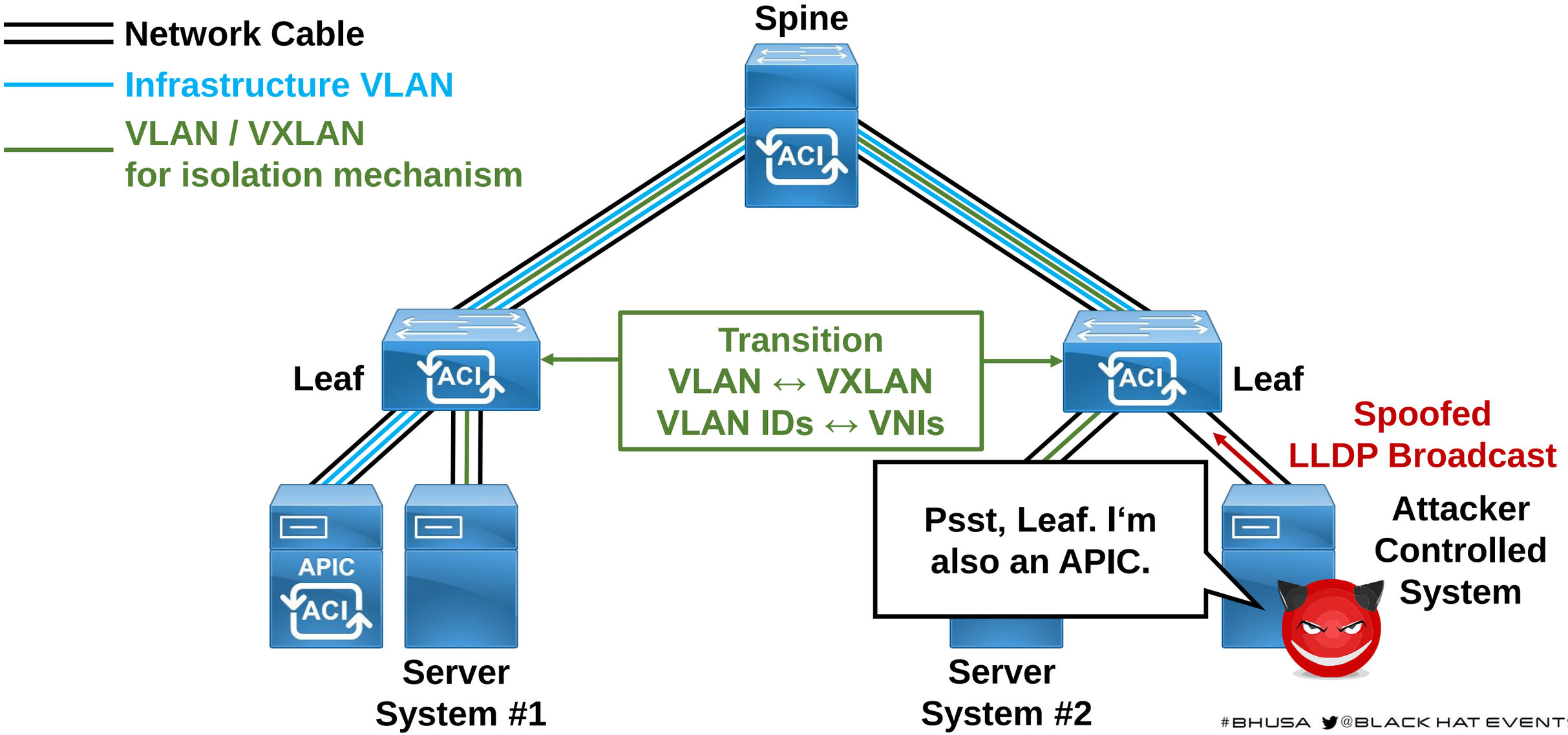




Attack Scenario



Attack Scenario



CVE-2019-1890

Attacker controlled system can join infra VLAN and access internal services!

- APIC ~60, Leaf & Spine ~15 services on infra VLAN
- VXLAN tunnel endpoints exposed
- Services on management interface also exposed

CVE-2019-1890

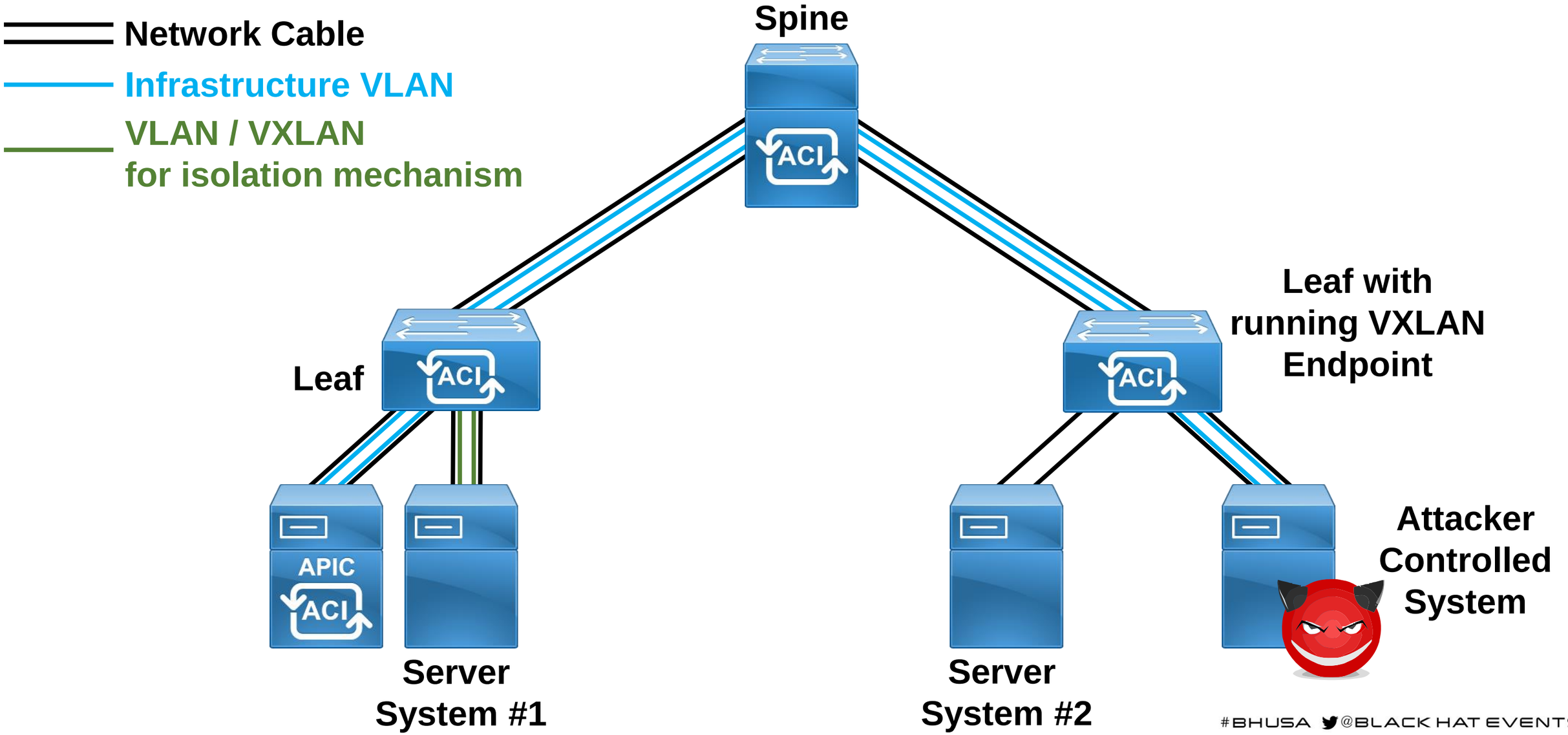
Attacker controlled system can join infra VLAN and access internal services!

- APIC ~60, Leaf & Spine ~15 services on infra VLAN
- VXLAN tunnel endpoints exposed
- Services on management interface also exposed

Demo time!

Going down the rabbit hole

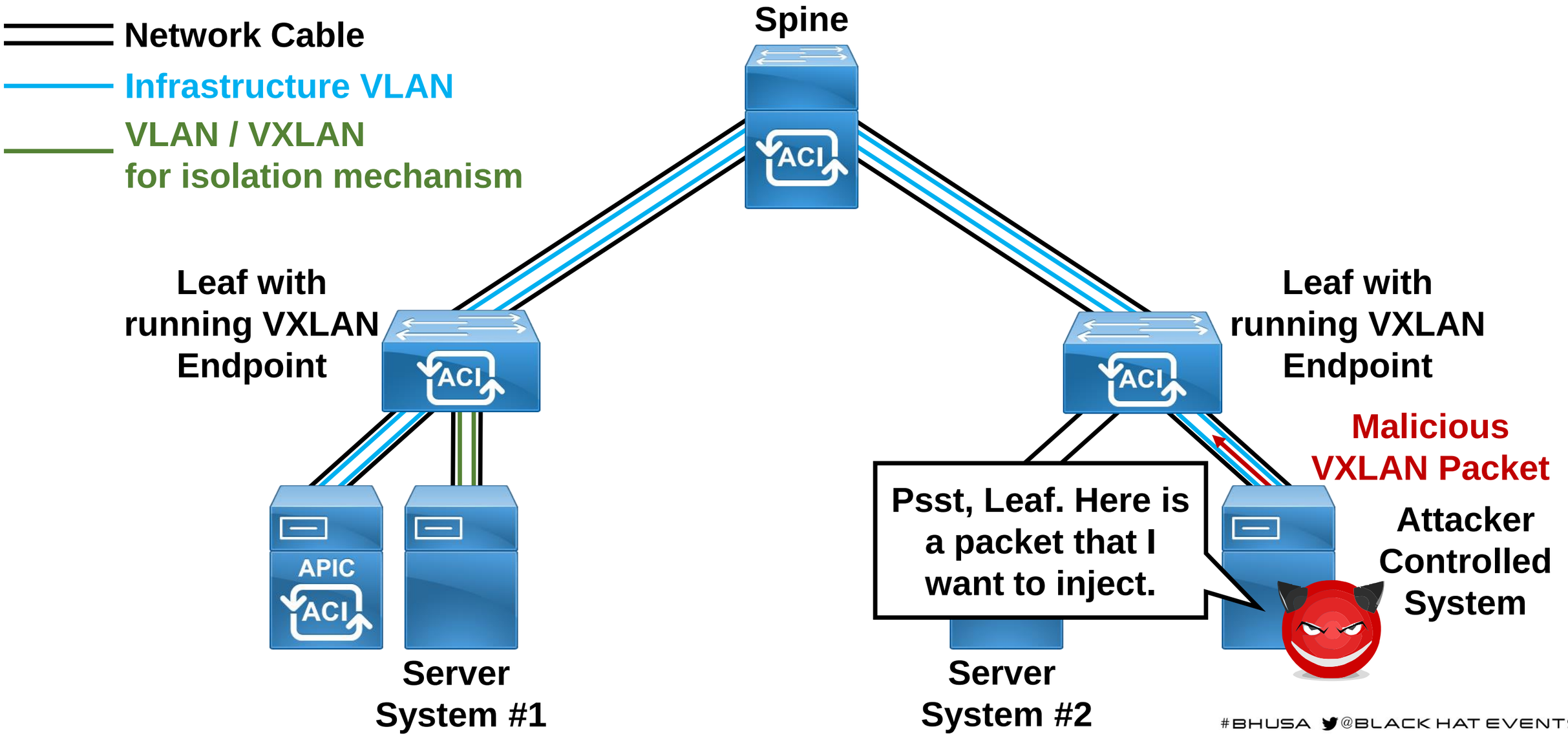
VXLAN Endpoint



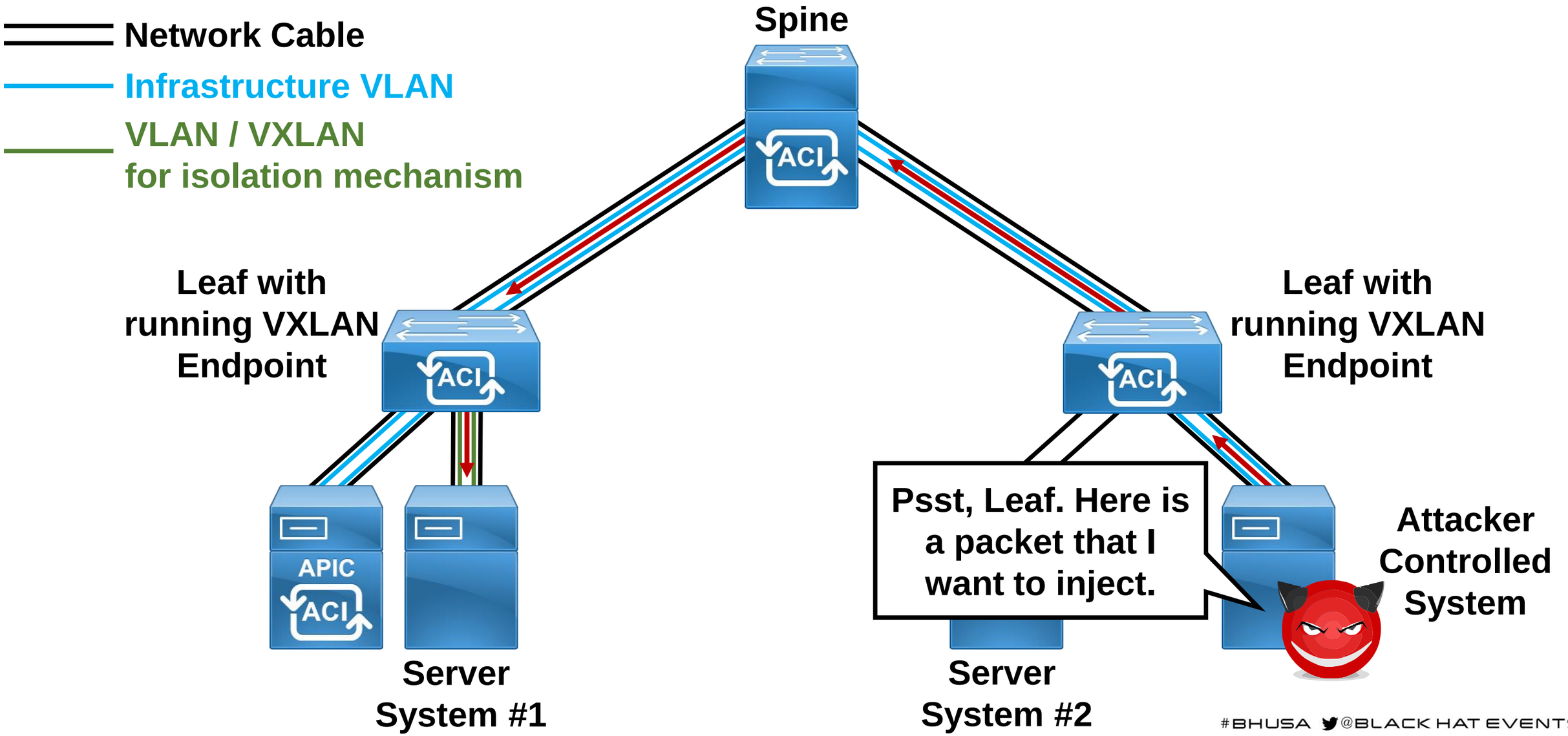
Crafting a VXLAN Packet

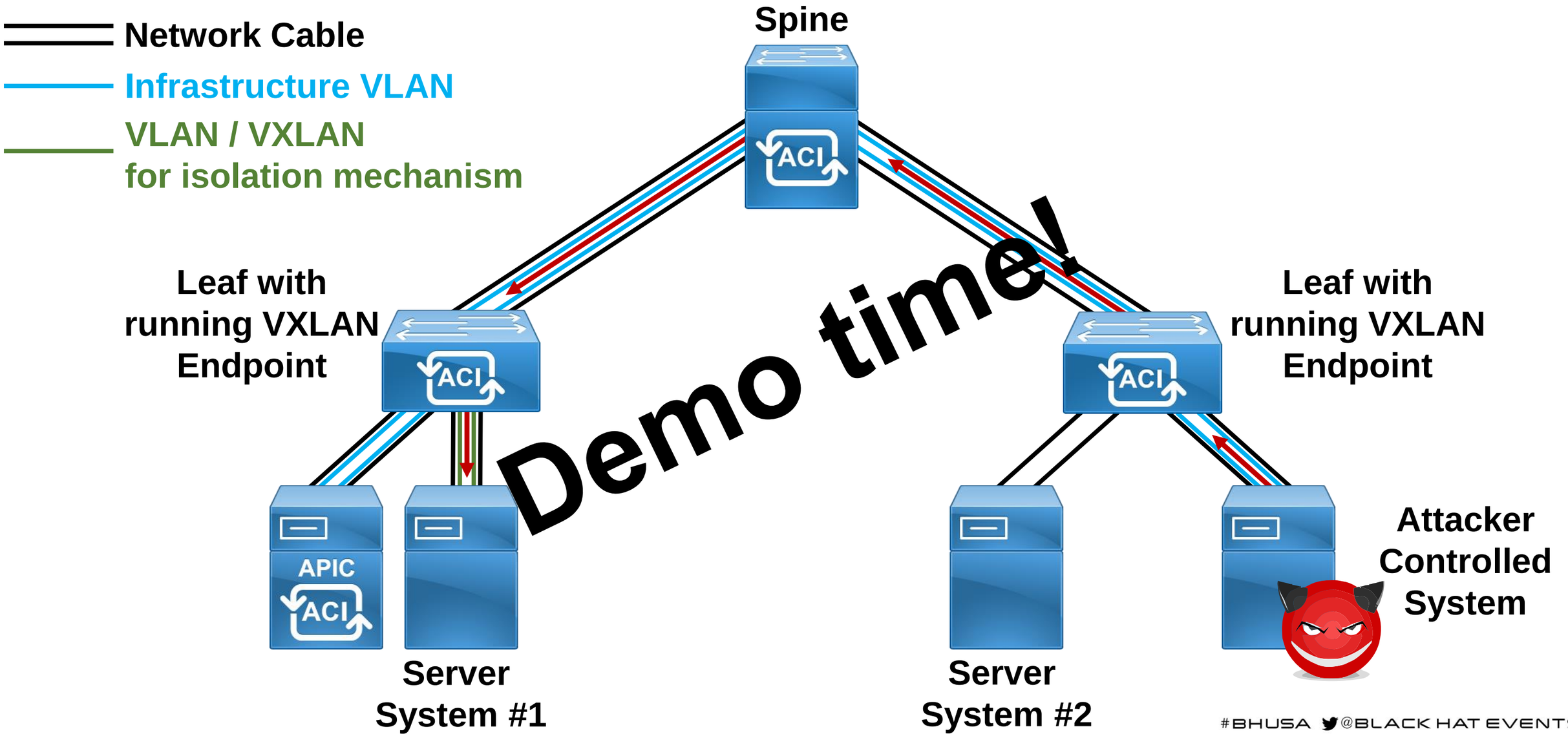
Layer	Protocol	Value
7….	…	…
7.3	IP	src = 192.168.200.11, dst = 192.168.200.20
7.2	Ethernet	src = 01:23:45:67:89:ab, dst = cd:ef:11:22:33:44
7	VXLAN	vni = target VNI
4	UDP	dst = VXLAN Endpoint
3	IP	dst = Address of Leaf

Injecting VXLAN Packet



Injecting VXLAN Packet




Network Cable
Infrastructure VLAN
VLAN / VXLAN
for isolation mechanism
Spine
ACI
Leaf with
running VXLAN
Endpoint
ACI
Demo time!
Leaf with
running VXLAN
Endpoint
ACI
APIC
ACI
Server
System #1
Server
System #2
Attacker
Controlled
System

Vulnerability #3

Link Layer Discovery Protocol

LLDP is a OSI-layer 2 protocol using Type-Length-Value Structures

Type	Length	Value
7 bits	9 bits	0-511 octets

TLV type values

TLV Type	TLV Names	Usage
0	End of LLDP Data Unit	Mandatory
1	Chassis ID	Mandatory
2	Port ID	Mandatory
3	Time To Live	Mandatory
4	Port Description	Optional
…	…	…
127	Custom TLVs	Optional

Link Layer Discovery Protocol

```
▾ Cisco Systems, Inc - ACI Unknown-D8: 00:00
    1111 111. .... .... = TLV Type: Organization Specific (127)
    .... ...0 0000 0110 = TLV Length: 6
    Organization Unique Code: 00:01:42 (Cisco Systems, Inc)
    Cisco Subtype: ACI Unknown-D8 (0xd8)
    Unknown 0xD8: 0000
```

```
00f0  05 00 00 00 00 fe 05 00  01 42 01 01 fe 06 00 01   ........ .B......
0100  42 d8 00 00 fe 05 00 01  42 c9 01 fe 0f 00 01 42   B....... B.......B
```

LLDP Buffer Overflow

- LLDP running as root on all leafs and spines.
- NX and PIE activated.

- What happens when the length value for subtype 0xd8 is modified?

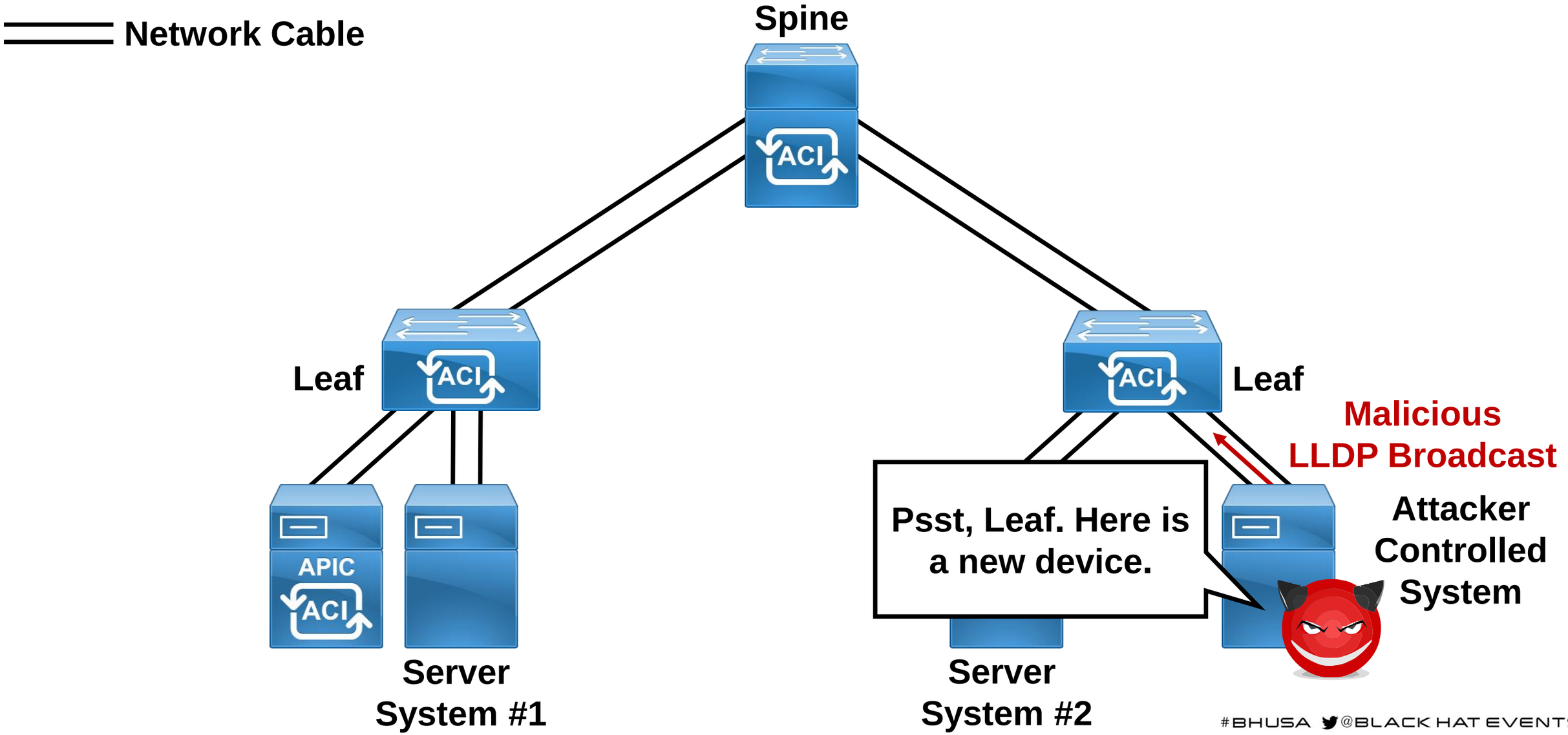
LLDP Buffer Overflow

- LLDP running as root on all leafs and spines.
- NX and PIE activated.

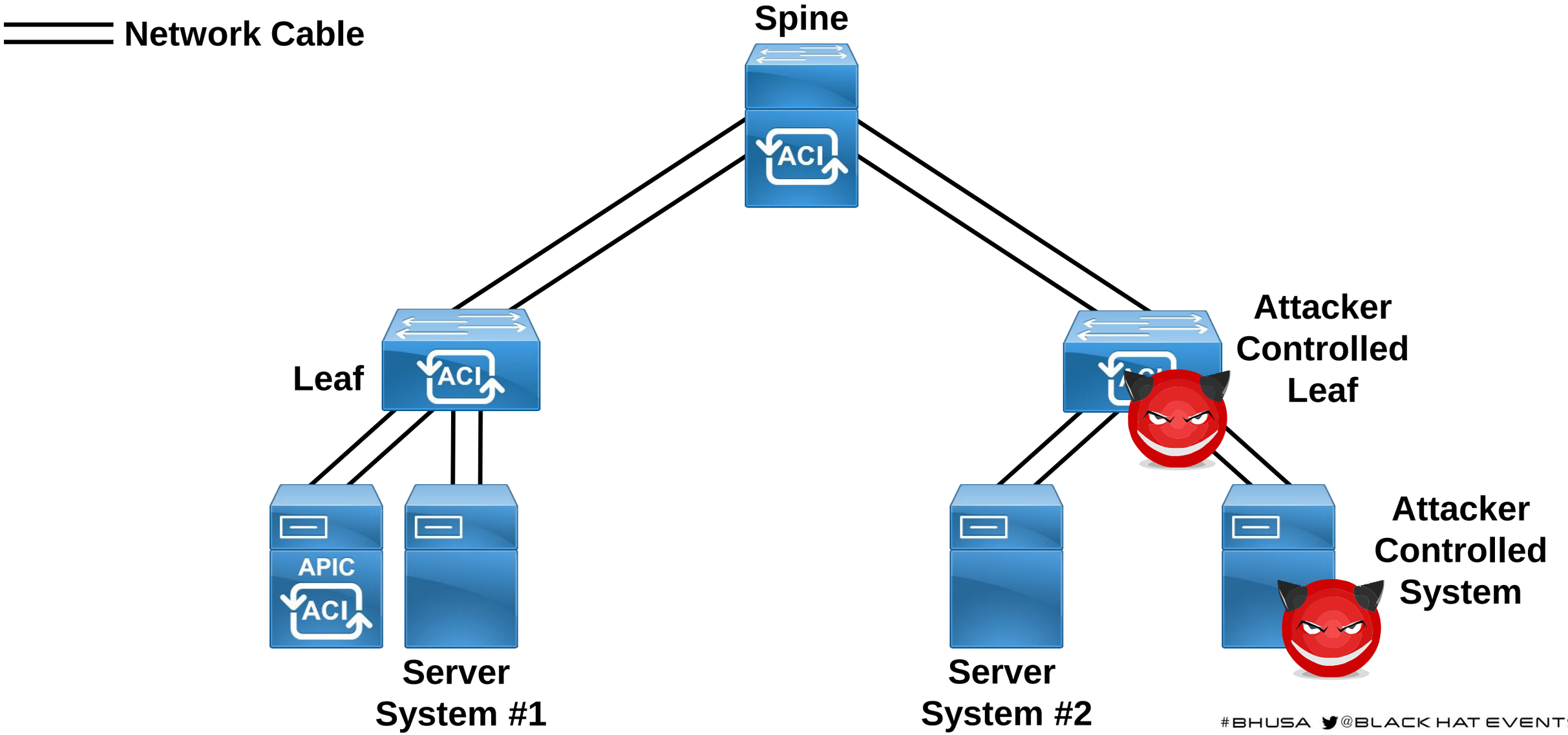
- What happens when the length value for subtype 0xd8 is modified?

CVE-2019-1901

Attack Scenario



Attack Scenario



Remaining Problems

```
Leaf1# fgrep libc- /proc/14432/maps
eea77000-eec1c000 r-xp 00000000 00:0e 39765                              /lib/libc-2.15.so
eec1c000-eec1d000 ---p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eec1d000-eec1f000 r--p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eec1f000-eec20000 rw-p 001a7000 00:0e 39765                              /lib/libc-2.15.so
```

```
Leaf1# fgrep libc- /proc/14443/maps
eea41000-eebe6000 r-xp 00000000 00:0e 39765                              /lib/libc-2.15.so
eebe6000-eebe7000 ---p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eebe7000-eebe9000 r--p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eebe9000-eebea000 rw-p 001a7000 00:0e 39765                              /lib/libc-2.15.so
```

Remaining Problems

```
Leaf1# fgrep libc- /proc/14432/maps
eea77000-eec1c000 r-xp 00000000 00:0e 39765                              /lib/libc-2.15.so
eec1c000-eec1d000 ---p 001a5000 00:0e 39765                              /lib/libc-2.15.so
```

```
[root@apic1 ~]# acidiag fnvread
      ID   Pod ID                 Name    Serial Number         IP Address    Role        State   LastUpdMsgId
-------------------------------------------------------------------------------------------------------------
     101       1                 Leaf1      FDO22480FLU          [redacted]/32    leaf       inactive   0x2000000cde97c
     102       1                 Spine      FDO22472FAZ          [redacted]/32   spine         active   0
     103       1                 Leaf2      FDO22480FHY          [redacted]/32    leaf         active   0

Total 3 nodes
```

```
eeb93000-eeb94000 ---p 001a5000 00:0e 42419                              /lib/libc-2.15.so
eeb94000-eeb96000 r--p 001a5000 00:0e 42419                              /lib/libc-2.15.so
eeb96000-eeb97000 rw-p 001a7000 00:0e 42419                              /lib/libc-2.15.so
```

Remaining Problems

```
Leaf1# fgrep libc- /proc/14432/maps
eea77000-eec1c000 r-xp 00000000 00:0e 39765                              /lib/libc-2.15.so
eec1c000-eec1d000 ---p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eec1d000-eec1f000 r--p 001a5000 00:0e 39765                              /lib/libc-2.15.so
eec1f000-eec20000 rw-p 001a7000 00:0e 39765                              /lib/libc-2.15.so
```

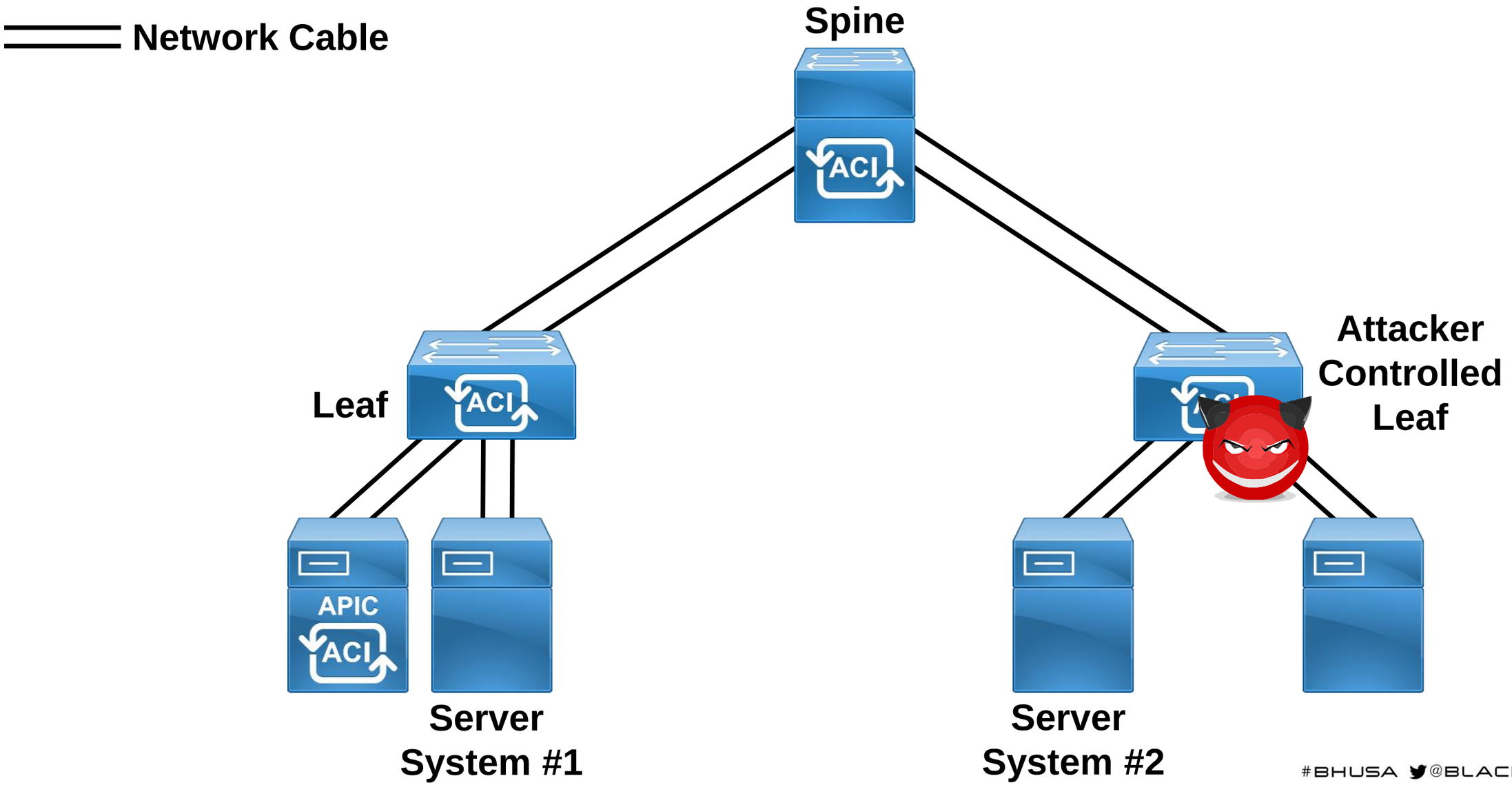
```
[root@apic1 ~]# acidiag fnvread
 ID       Pod ID          Name       Serial Number         IP Address       Role       State      LastUpdMsgId
--------------------------------------------------------------------------------------------------------------
 101      1               Leaf1      FDO22480FLU                /32    leaf       inactive   0x2000000cde97c
 102      1               Spine      FDO22472FA7                /32   spine         active   0
 103      1               Leaf2      FDO22480HH                 /32    leaf         active   0

Total 3 nodes
```

```
Leaf1# fgrep libc- /proc/13562/maps
eeb90000-eeb93000 r-xp 00000000 00:0e 42419                              /lib/libc-2.15.so
eeb93000-eeb94000 ---p 001a5000 00:0e 42419                              /lib/libc-2.15.so
eeb94000-eeb96000 r--p 001a5000 00:0e 42419                              /lib/libc-2.15.so
eeb96000-eeb97000 rw-p 001a7000 00:0e 42419                              /lib/libc-2.15.so
```

Demo time!

Going further down the rabbit hole

Attack Scenario



Going further down the rabbit hole

```
Leaf2# ifconfig -a 2>&1 | egrep '^[^ \t]'
eth0      Link encap:Ethernet  HWaddr
inband_hi Link encap:Ethernet  HWaddr
inband_lo Link encap:Ethernet  HWaddr
kpm_inb   Link encap:Ethernet  HWaddr
kpm_mgmt  Link encap:Ethernet  HWaddr
lo        Link encap:Local Loopback
mgmt0     Link encap:Ethernet  HWaddr
psdev0    Link encap:Ethernet  HWaddr
psdev1    Link encap:Ethernet  HWaddr
psdev2    Link encap:Ethernet  HWaddr
```

Going further down the rabbit hole

```
Leaf2# ifconfig -a 2>&1 | egrep '^[^ \t]'
eth0      Link encap:Ethernet  HWaddr
inband_hi Link encap:Ethernet  HWaddr
inband
kpm_ir
kpm_mg
lo
mgmt0
psdev0
psdev1
psdev2
```

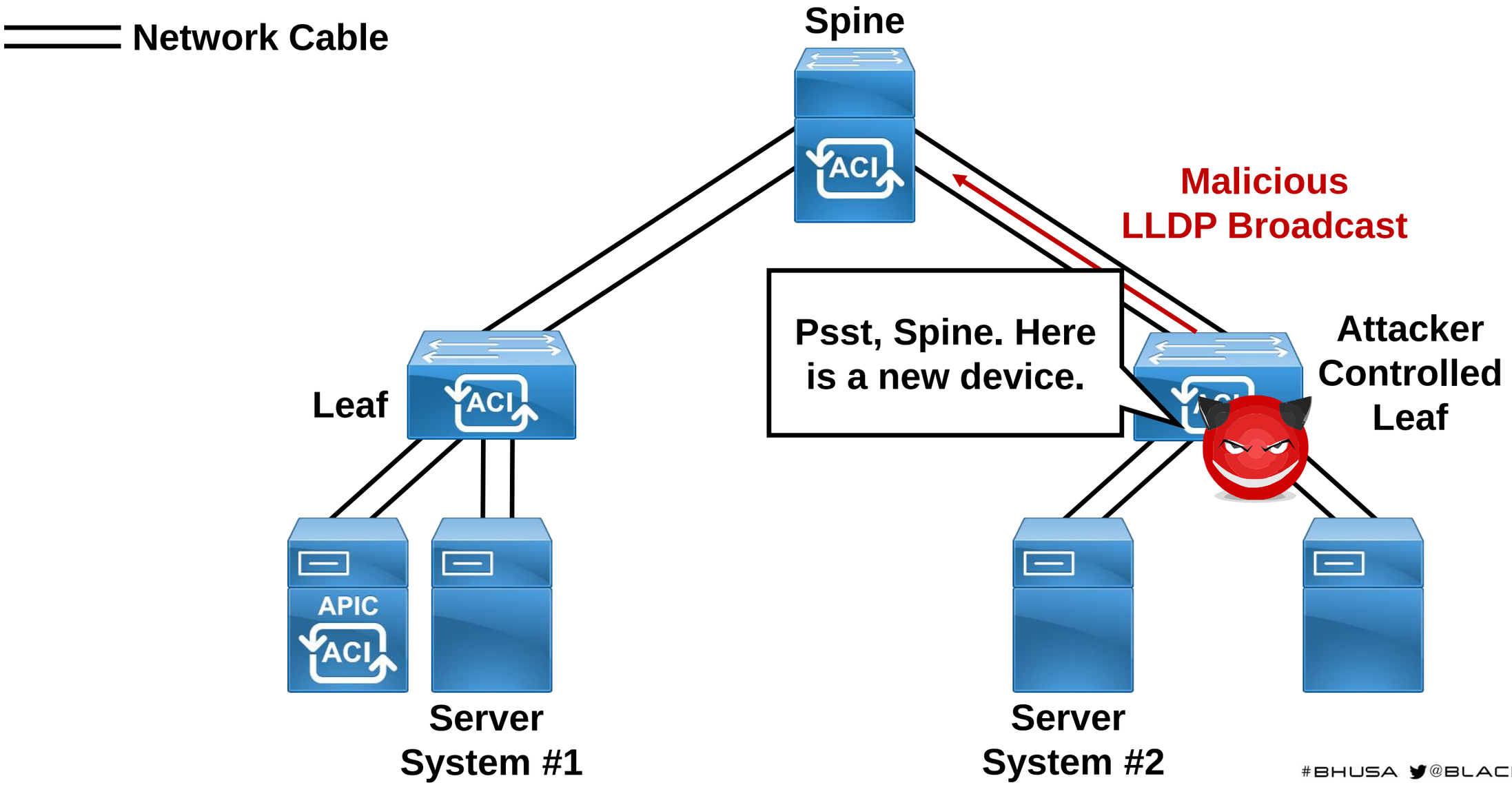
```
Leaf2# readelf -s /isan/plugin/0/isan/lib/libistack_pm.so | grep net_l2
    34: 00002518   223 FUNC    GLOBAL DEFAULT   11 net_l2_send
    35: 000022d9   575 FUNC    GLOBAL DEFAULT   11 net_l2_msend
    38: 0000119a  2960 FUNC    GLOBAL DEFAULT   11 net_l2_pkt_recv_w_flags
    40: 00004bac     4 OBJECT  GLOBAL DEFAULT   23 net_l2_recv_callback_arg
    41: 000010d7   195 FUNC    GLOBAL DEFAULT   11 net_l2_process_data_msg
    43: 00000f0a   191 FUNC    GLOBAL DEFAULT   11 net_l2_del_membership_if_
    44: 000025f7  1259 FUNC    GLOBAL DEFAULT   11 net_l2_register
    45: 00004ba8     4 OBJECT  GLOBAL DEFAULT   23 net_l2_recv_callback_fn
    46: 00002ae2   400 FUNC    GLOBAL DEFAULT   11 net_l2_mgmt_register
    47: 00001d2a  1455 FUNC    GLOBAL DEFAULT   11 net_l2_send_prepare
    48: 00000fc9   270 FUNC    GLOBAL DEFAULT   11 net_l2_pkt_drop
    49: 00000de2    52 FUNC    GLOBAL DEFAULT   11 net_l2_unregister
    50: 00000e16   244 FUNC    GLOBAL DEFAULT   11 net_l2_add_membership_if
```

net_l2_register*(socket_fd, 1, &a3, &ethertype.type, 1, 0)*

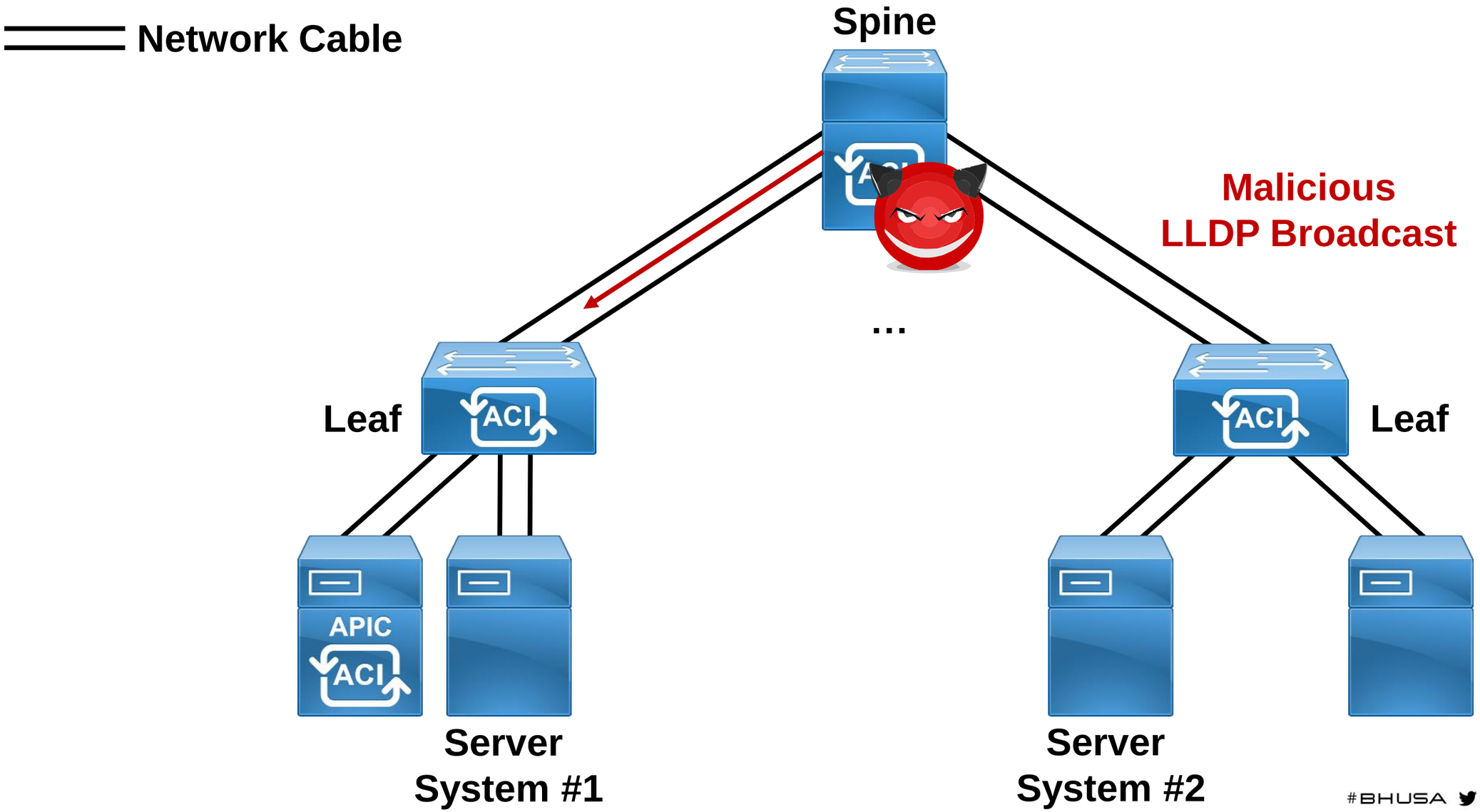
net_l2_send*(socket_fd, &a2, &intf.if_id, pstruct.padding, l2_message_length, l2_frame.dst_address)*

```
struct l2_frame {
    char dst_address[6];
    char src_address[6];
    char ethertype[2];
    char msg[payload_length];
};
```

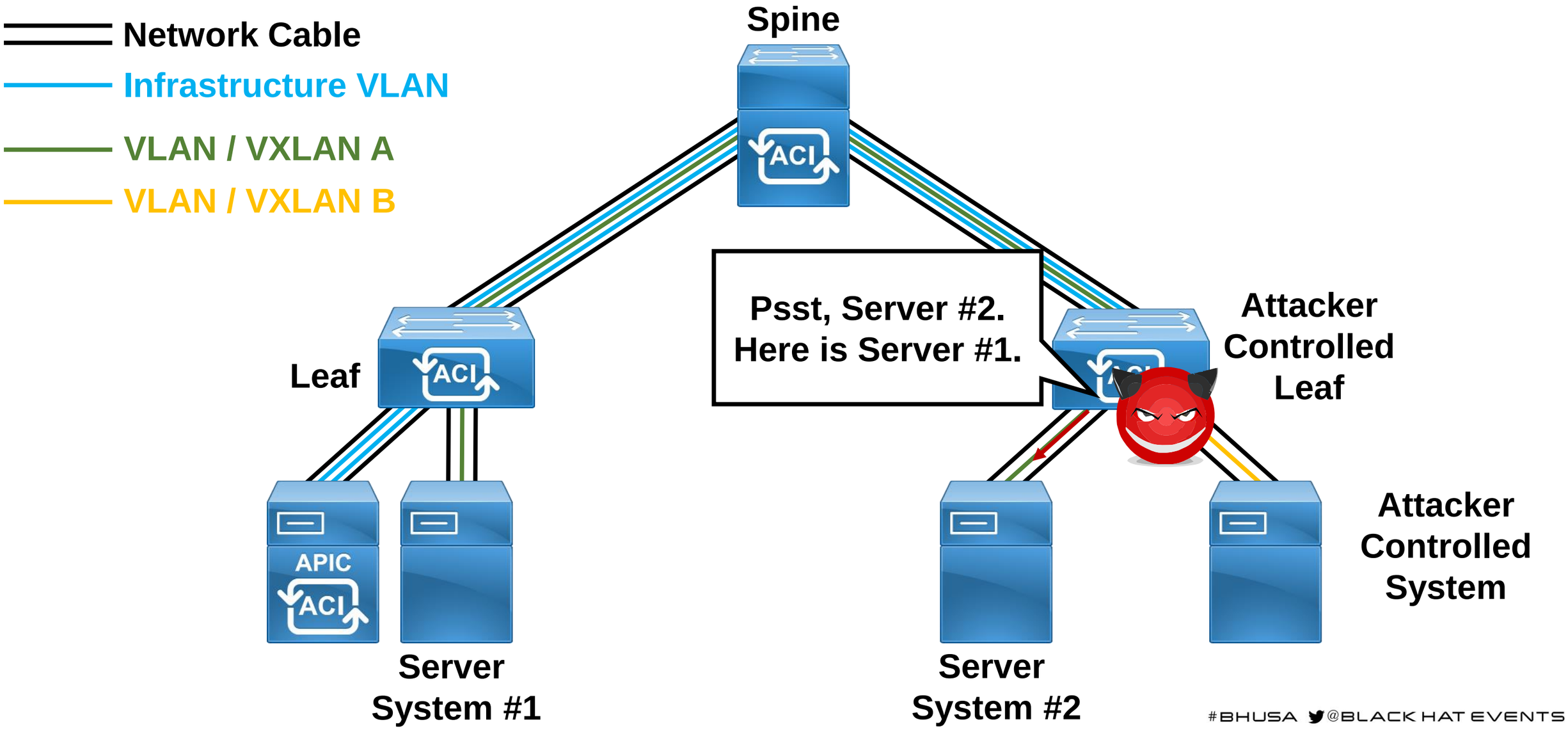
Attack Scenario



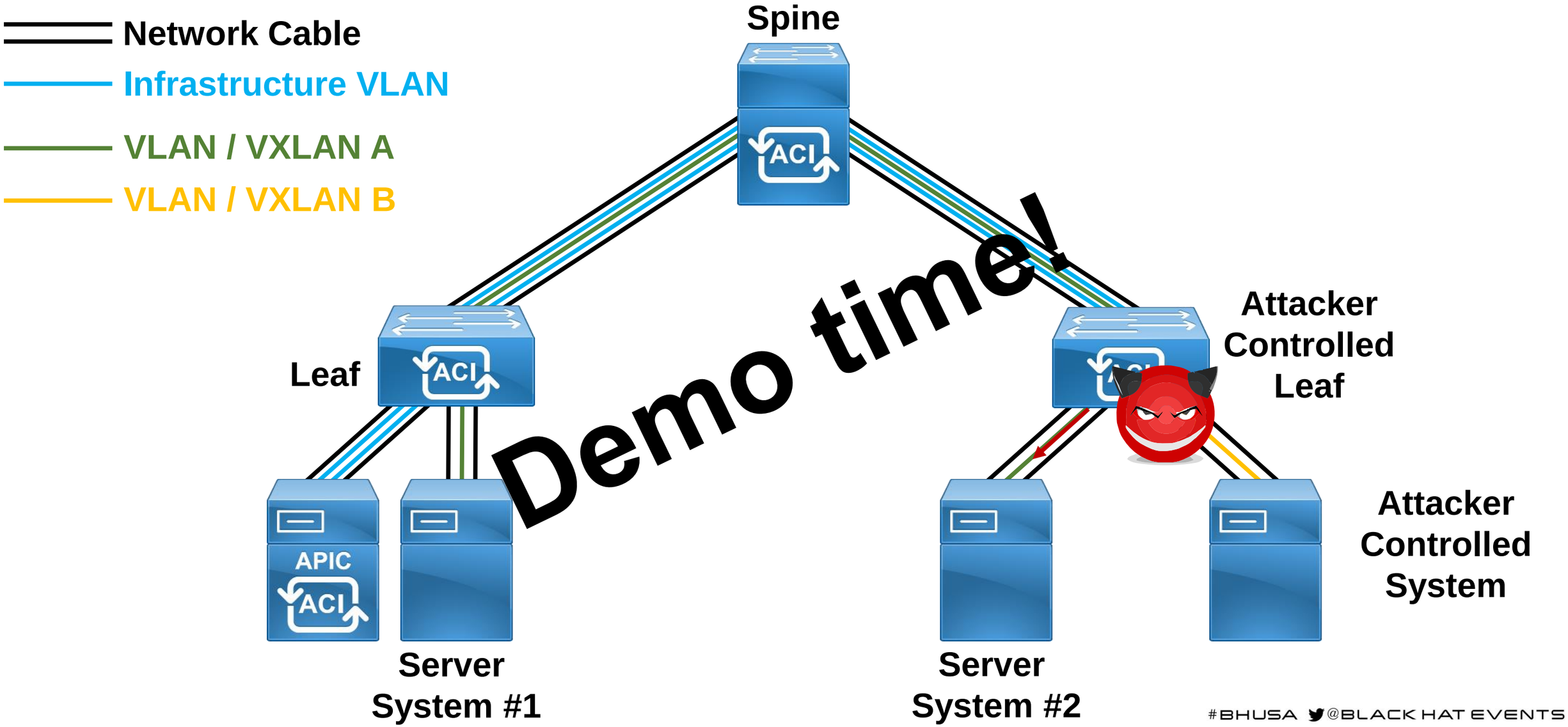
Attack Scenario



Attack Scenario

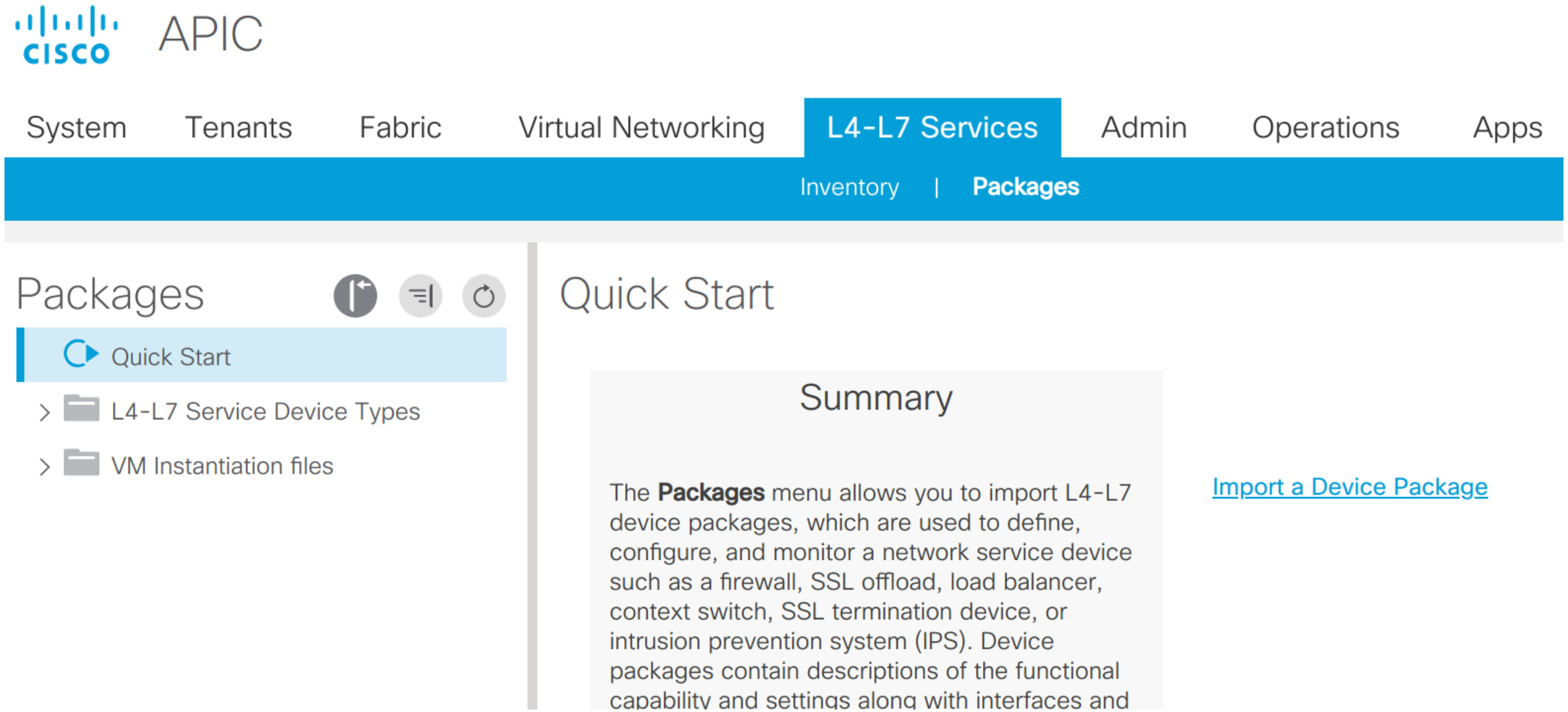


Attack Scenario



Vulnerability #4

Going down the APIC hole



Going down the APIC hole

```
surf@machine /tmp % unzip -l asa-device-pkg-1.0.1.zip | tail
        0  2019-05-08 18:46   utils/
      420  2014-07-28 15:05   utils/env.py
       97  2014-07-28 15:05   utils/__init__.py
      844  2014-07-28 15:05   utils/errors.py
     4979  2014-07-28 15:05   utils/service.py
    22462  2014-07-28 15:05   utils/util.py
      939  2014-07-28 15:05   utils/protocol.py
      581  2019-05-08 18:45   ../../../../../../../etc/cron.d/ernw_cronjob
---------                     -------
   581500                     68 files
```

Going down the APIC hole

```
surf@machine /tmp % unzip -l asa-device-pkg-1.0.1.zip | tail
        0  2019-05-08 18:46   utils/
      420  2014-07-28 15:05   utils/env.py
       97  2014-07-28 15:05   utils/__init__.py
      844  2014-07-28 15:05   utils/errors.py
     4979  2014-07-28 15:05   utils/service.py
    22462  2014-07-28 15:05   utils/util.py
      939  2014-07-28 15:05   utils/protocol.py
      581  2019-05-08 18:45   ../../../../../../../etc/cron.d/ernw cronjob
---------                     -------
   581500                     68 files
```

CVE-2019-1889

Recommendations

- Update immediately!
- Watch out for new Updates.

- Think about how to use your ACI fabric.

- Restrict Access to the management interfaces.
- Deactivate LLDP wherever it is not necessary.

- Do not import Device Packages from Spam/4chan/Stackoverflow !

Thanks for your Attention!

Questions?

See Whitepaper and exploit files for more details!

Security Advisories

- Vulnerability #1
  - Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Symbolic Link Path Traversal Vulnerability
    - CVE-2019-1836 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-fabric-traversal
  - Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Root Privilege Escalation Vulnerability
    - CVE-2019-1803 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-rpe
  - Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Default SSH Key Vulnerability
    - CVE-2019-1804 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-sshkey

Security Advisories

- Vulnerability #2
  - Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure VLAN Unauthorized Access Vulnerability (High)
    - CVE-2019-1890
      https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass

- Vulnerability #3
  - Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure Mode Link Layer Discovery Protocol Buffer Overflow Vulnerability
    - CVE-2019-1901
      https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190731-nxos-bo

Security Advisories

- Vulnerability #4
  - Cisco Application Policy Infrastructure Controller REST API Privilege Escalation Vulnerability
    - CVE-2019-1889
      https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ccapic-restapi