

# Authenticated Access to Network

## Are Identity-based Security Schemes Going to Save Our LANs?

Cédric BLANCHER

cedric.blancher@eads.net  
EADS Innovation Works  
EADS/CTO/IW/SE/CS

sid@rstack.org  
Rstack Team  
<http://sid.rstack.org/>

Bellua Cyber Security - Jakarta - 2007 October 30-31  
<http://bellua.com/bcs/>

# whoami

```
~$ finger sid@rstack.org  
[rstack.org]  
finger: connect: Connection refused
```

oOps!

- Head of Computer Security Research Lab at EADS Innovation Works in France
- Focus : network security, wireless
- Rstack.org core member

Website : <http://sid.rstack.org/>

Blog : <http://sid.rstack.org/blog/>



# whoami

```
~$ finger sid@rstack.org  
[rstack.org]  
finger: connect: Connection refused
```

## oOps!

- Head of Computer Security Research Lab at EADS Innovation Works in France
- Focus : network security, wireless
- Rstack.org core member

Website : <http://sid.rstack.org/>

Blog : <http://sid.rstack.org/blog/>



# Motivations

What powers local networks security today ?

- Networks segregation, VLANs
- Firewalls
- IDS/IPS maybe
- Physical access restrictions

Honestly...

Very little have really changed since 1999 !

# Motivations

What powers local networks security today ?

- Networks segregation, VLANs
- Firewalls
- IDS/IPS maybe
- Physical access restrictions

Honestly...

Very little have really changed since 1999 !

# Agenda

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse?
- 4 Conclusion and final thoughts

# Agenda

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

# Something wrong with LAN security ?

How do we authenticate people physically connecting to the network ?

- Employees ?
- Visitors ?
- Trespassers ?

More importantly...

How do we give them proper access and privileges ?  
Or not...

# Something wrong with LAN security ?

How do we authenticate people physically connecting to the network ?

- Employees ?
- Visitors ?
- Trepassers ?

More importantly...

How do we give them proper access and privileges ?  
Or not...

# What can we do ?

Hopefully, network vendors come to our rescue !

- Provide network access authentication
- And identity based security features

Whao !

Sup4 k3wl !

## But wait...

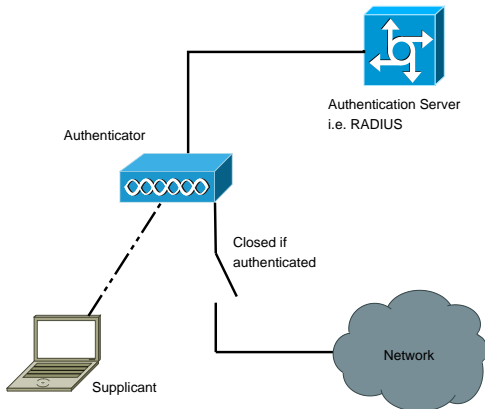
Ever heard of IEEE 802.1x ?

- "Port-Based Network Access Control"
- First published in 2001
- Revised in 2004 to integrate 802.11 (Wi-Fi) extensions

802.1x provides network base authentication  
Exactly what we need :)

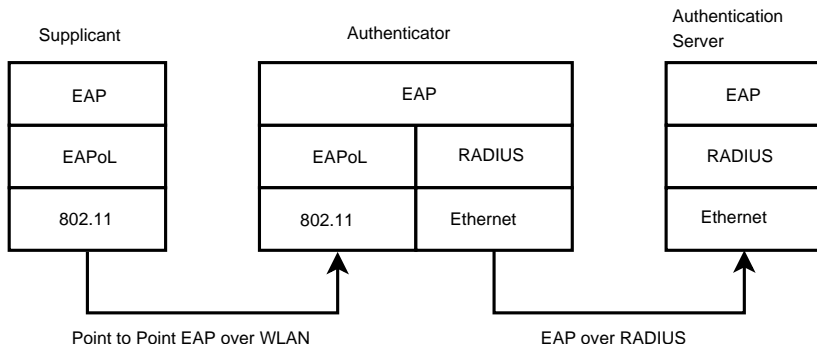
## How does it work ? (1/3)

802.1x allows a layer 2 equipment to authenticate a given network node against a RADIUS server



## How does it work ? (2/3)

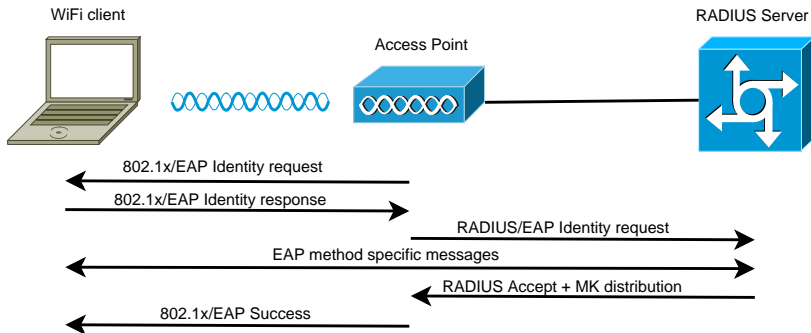
802.1x relies on an authentication protocol known as EAP<sup>1</sup>



<sup>1</sup>Extensible Authentication Protocol, RFC 3748

# How does it work ? (3/3)

## 802.1x wireless authentication example



# Agenda

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

## Beyond authentication

If we are able to authenticate nodes and/or users

- We can gather users profiles
- We can push information to network devices
- We can adapt network context to user

### Dynamic VLAN assignment

We can push a VLAN using RADIUS attributes

- 64 - Tunnel-Type (13, VLAN)
- 65 - Tunnel-Medium-Type (6, 802)
- 81 - Tunnel-Private-Group-ID (VLAN name or number)

## Want more ?

VLAN assignment is one thing. We can do better...

- We can also provide an IP address
- We can push this IP to DHCP servers pools
- We publish this information to layer 3+ devices
  - Routeurs
  - Firewalls
  - IDS/IPS
  - Etc.

### Security impact

We've moved security from physical location to user identity



## Want more ?

VLAN assignment is one thing. We can do better...

- We can also provide an IP address
- We can push this IP to DHCP servers pools
- We publish this information to layer 3+ devices
  - Routeurs
  - Firewalls
  - IDS/IPS
  - Etc.

### Security impact

We've moved security from physical location to user identity



# Applications

Some applications of identity based network security

- Users roaming : whatever plug, same network
- Guests access : unauthenticated users on dedicated VLAN
- Security zones : different medium, different authorizations
- Etc.

And...

A big move towards Network Access Control

# Applications

Some applications of identity based network security

- Users roaming : whatever plug, same network
- Guests access : unauthenticated users on dedicated VLAN
- Security zones : different medium, different authorizations
- Etc.

And...

A big move towards Network Access Control

# Network Access Control

Network Access Control is a scheme mostly pushed by Cisco (CNAC<sup>2</sup>) and Microsoft (NAP<sup>3</sup>). Other vendors are closely following, such as Juniper (UAC<sup>4</sup>)

- Based on 802.1x for nodes and/or users authentication
- Additional security services
  - Policy check and enforcement
  - Quarantine zones for sanitizing and upgrading
  - Devices type differentiation
  - Etc.

Heart of the system ?

A software agent running between node and network device

<sup>2</sup>Cisco Network Admission Control

<sup>3</sup>Network Access Protection

<sup>4</sup>Unified Access Control

# Agenda

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats**
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats**
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

## 802.1x limitations (1/3)

All your devices must support 802.1x

- How do you do with printers, APs, switches, routers, etc.
- You have to create exceptions for them
- Exceptions are controlled by MAC addresses

Ever heard of MAC spoofing ?!

Food for thoughts : what happens if I bridge a 802.1q trunk ?

## 802.1x limitations (1/3)

All your devices must support 802.1x

- How do you do with printers, APs, switches, routers, etc.
- You have to create exceptions for them
- Exceptions are controlled by MAC addresses

Ever heard of MAC spoofing ?!

Food for thoughts : what happens if I bridge a 802.1q trunk ?

## 802.1x limitations (2/3)

You have to be very careful when choosing your authentication method

- Cleartext authentication (EAP-GTC)
- Proxified challenge/response (EAP-MD5)

What if I plug a hub between node and network, and sniff traffic?  
Guess what!

## 802.1x limitations (2/3)

You have to be very careful when choosing your authentication method

- Cleartext authentication (EAP-GTC)
- Proxified challenge/response (EAP-MD5)

What if I plug a hub between node and network, and sniff traffic?  
Guess what !

## 802.1x limitations (3/3)

What about hijacking an authenticated access ?

- Some switches just open port, then all connected devices can go through when first one is authenticated
- 802.1x access is a port/MAC based authorization

- Unplug legitimate node
- Plug it on a hub with your rogue box
- Get MAC address
- Plug hub in network
- Legitimate node authenticate
- Spoof it if needed

## 802.1x limitations (3/3)

What about hijacking an authenticated access ?

- Some switches just open port, then all connected devices can go through when first one is authenticated
- 802.1x access is a port/MAC based authorization

- Unplug legitimate node
- Plug it on a hub with your rogue box
- Get MAC address
- Plug hub in network
- Legitimate node authenticate
- Spoof it if needed

# Solutions ?

Some ideas to harden network security

- Don't let fixed nodes get unplugged (cyanolit rulez!)
- Use strong authentication protocols (PEAP, EAP-TLS)
- Put non-802.1x devices on specific networks
- Use PVLAN when possible for them

Hardening configuration gives DoS opportunities...

Anyway, having 802.1x makes things better than without it, if you're aware of limitations !

# And what about laptop theft ?

Attacker can steal your laptop, with your credentials !

- Login/passwords
- Certificates

He can find everything he needs to access the network

## Solution ?

- Full hard-drive encryption (mandatory for laptops)
- Use of TPM device to store certificates
- Smartcards and other authentication tokens
- Theft response procedure !

# And what about laptop theft ?

Attacker can steal your laptop, with your credentials !

- Login/passwords
- Certificates

He can find everything he needs to access the network

## Solution ?

- Full hard-drive encryption (mandatory for laptops)
- Use of TPM device to store certificates
- Smartcards and other authentication tokens
- Theft response procedure !

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 **Limitations and caveats**
  - 802.1x
  - **Network Access Control**
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

## NAC-like limitations (1/2)

We want to only allow access to sanitized boxes

- Need to spot compromised hosts
- Need to enforce cleaning
- Need to verify security state
- Then grant acces

Do you seriously think it will work ? !

## NAC-like limitations (1/2)

We want to only allow access to sanitized boxes

- Need to spot compromised hosts
- Need to enforce cleaning
- Need to verify security state
- Then grant acces

Do you seriously think it will work ? !

## NAC-like limitations (2/2)

It only relies on software client-side components

- Can you trust client-side agent?
- What makes you sure you can detect malwares?
- What makes you think you can actually clean them?
- Therefore, can you rely on this to grant access?

### Face the truth

Nowadays malwares are so rootkit savvy that

- They're difficult to detect in the first place
- They're close to impossible to remove automatically

Non-compliance to security policy would have to be a No-Go.

OK, how do you feed all your laptops with updates on time then?



## NAC-like limitations (2/2)

It only relies on software client-side components

- Can you trust client-side agent?
- What makes you sure you can detect malwares?
- What makes you think you can actually clean them?
- Therefore, can you rely on this to grant access?

### Face the truth

Nowadays malwares are so rootkit savvy that

- They're difficult to detect in the first place
- They're close to impossible to remove automatically

Non-compliance to security policy would have to be a No-Go.

OK, how do you feed all your laptops with updates on time then?



## NAC-like limitations (2/2)

It only relies on software client-side components

- Can you trust client-side agent?
- What makes you sure you can detect malwares?
- What makes you think you can actually clean them?
- Therefore, can you rely on this to grant access?

### Face the truth

Nowadays malwares are so rootkit savvy that

- They're difficult to detect in the first place
- They're close to impossible to remove automatically

Non-compliance to security policy would have to be a No-Go.

OK, how do you feed all your laptops with updates on time then?



# Does NAC makes thing better ?

Actually, NAC is good to enforce updates policy

There's no reason it would be more efficient to detect compromised hosts than local AV alone...

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats**
  - 802.1x
  - Network Access Control
  - VLAN deployment**
  - Can things get worse?
- 4 Conclusion and final thoughts

# You said VLAN ?

Ever heard of VLAN hopping ?

- Double 802.1q encapsulation
- Dynamic configuration protocols exploitation
  - DTP negotiation
  - Taking advantage of VTP
  - Etc.

Better have a look at security best practices for switches configuration

# You said VLAN ?

Ever heard of VLAN hopping ?

- Double 802.1q encapsulation
- Dynamic configuration protocols exploitation
  - DTP negotiation
  - Taking advantage of VTP
  - Etc.

Better have a look at security best practices for switches configuration

## And what about VoIP ?

What has VoIP to do with VLANs?

- IP phones have access to sanctified Voice VLAN
- IP phones have access to data VLANs when bridging desktops

- Some phones leak Voice VLAN on data link
- IP phone can be exploited
- What is I can spoof a VoIP phone ?

Last word on VoIP : what happens when someone breaks into Voice VLAN ?...

## And what about VoIP ?

What has VoIP to do with VLANs?

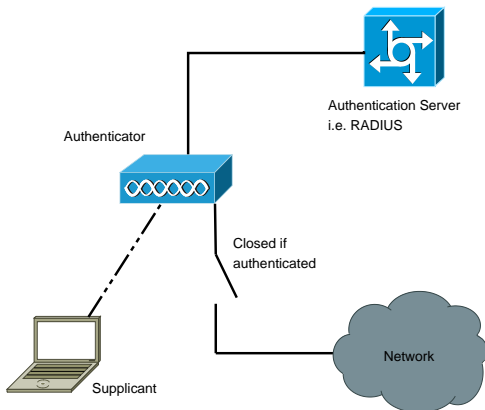
- IP phones have access to sanctified Voice VLAN
  - IP phones have access to data VLANs when bridging desktops
- Some phones leak Voice VLAN on data link
  - IP phone can be exploited
  - What is I can spoof a VoIP phone ?

Last word on VoIP : what happens when someone breaks into Voice VLAN ?...

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats**
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - **Can things get worse?**
- 4 Conclusion and final thoughts

## Architectural thoughts

Let's get back to 802.1x architecture

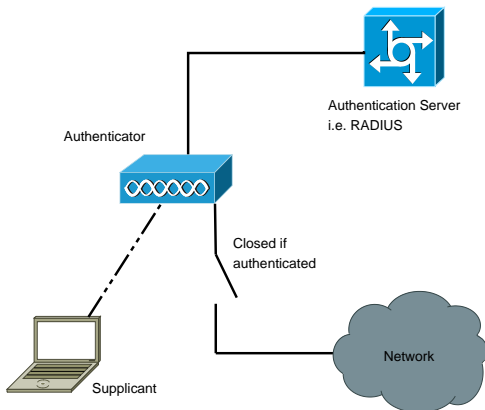


Is there anything we should be worried about ?



# Architectural thoughts

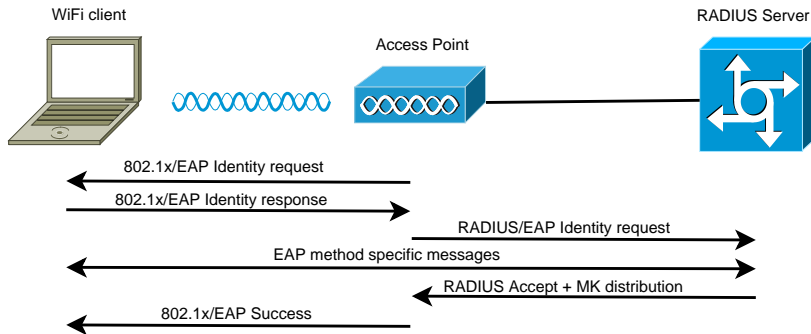
Let's get back to 802.1x architecture



Is there anything we should be worried about ?

# OK, here's the answer

Client is in direct communication with RADIUS server



See what I mean ?

# What it means

There's a threat that RADIUS can be compromised

- Access to authentication database
- Possible access for malicious nodes!

## Difficult to believe ?

- Roberto was bidding a remote FreeRADIUS flaw and exploit
- Cisco layer 2 devices can be DoSed (or more) with an EAP packet<sup>a</sup>
- What about OpenSSL flaws ?

---

<sup>a</sup>Greets to our FT R&D friends ;)

Don't let protocols fool you : you can send directly data from client to RADIUS over EAP



# Agenda

- 1 Authenticated network access
- 2 From authentication to identity based security
- 3 Limitations and caveats
  - 802.1x
  - Network Access Control
  - VLAN deployment
  - Can things get worse ?
- 4 Conclusion and final thoughts

# Conclusion

In the end

- 802.1x makes things better when properly deployed
- 802.1x support is getting better as new products come
- NAC does not seem a valuable investment to me

**Beware!**

You RADIUS is exposed, take care of it

# Network security doomed ?

Is today network security model able to deliver what we need ?

- Network security does not scale
- Segregation breaks applications
- In the end, we never get what we need

What do we see in the end

- Protocol stacking over HTTP
- Peer to peer applications and networking development

In the end, all this stuff is only bypassing your security...

# Network security doomed ?

Is today network security model able to deliver what we need ?

- Network security does not scale
- Segregation breaks applications
- In the end, we never get what we need

What do we see in the end

- Protocol stacking over HTTP
- Peer to peer applications and networking development

In the end, all this stuff is only bypassing your security...

## Is there a better solution ?

Rethink the network...

- Re-establish global connectivity
- Move to IPv6<sup>5</sup>
- Have a less fragmented network
- Let the network do its job !

Network is there to route packets  
Move security to IPSEC

OK, lots of work, but no one said security was easy :)

---

<sup>5</sup>A thankful and respectful thought to Itojun who passed away yesterday :(  
 