

# 802.1x and BEYOND!

Brad Antoniewicz

# Hi, I'm @brad\_anton



# Agenda



About 802.1x

Attacks

Fuzzing/Tools

A photograph of two men standing in front of a large, ornate Gothic-style church door. Both men are wearing black t-shirts and have their arms crossed. The man on the left is looking upwards and to the right. The man on the right is wearing sunglasses and looking to the right. A red stanchion post is visible in the foreground on the left. A semi-transparent grey box is overlaid on the bottom left of the image, containing the text 'IEEE 802.1x' and 'Port-Based network access control'.

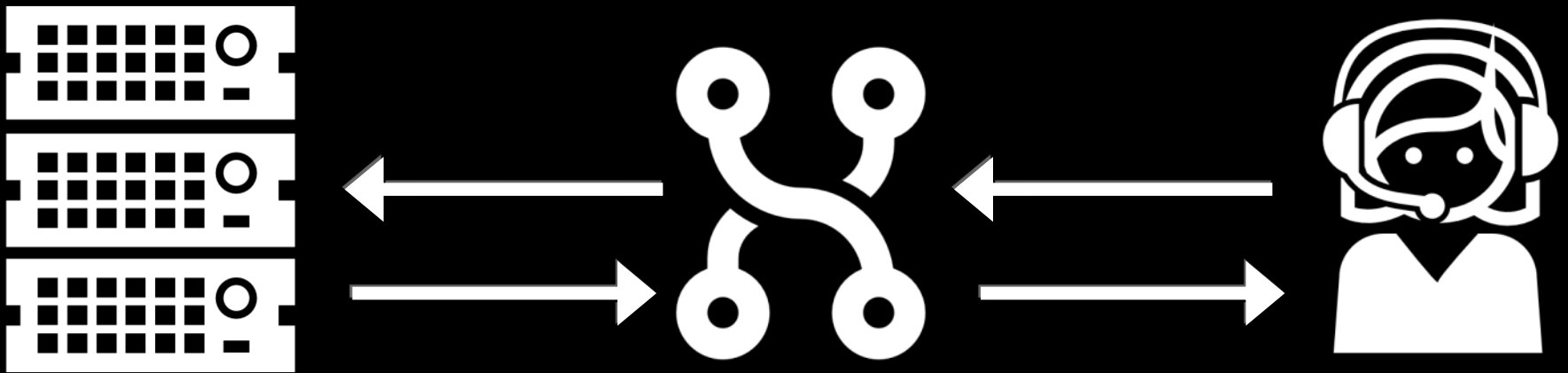
# IEEE 802.1x

Port-Based network access control

**Cause not everyone is welcome at church?**

# Flow

(IEEE 802.1x)

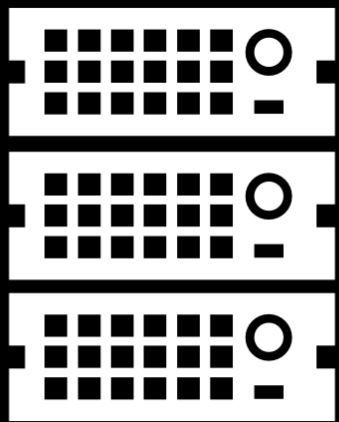


**Authentication Server**

**Authenticator**

**Supplicant**

# 802.11



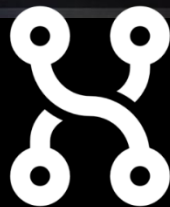
**RADIUS Server**



frankie muniz's forehead = great wifi

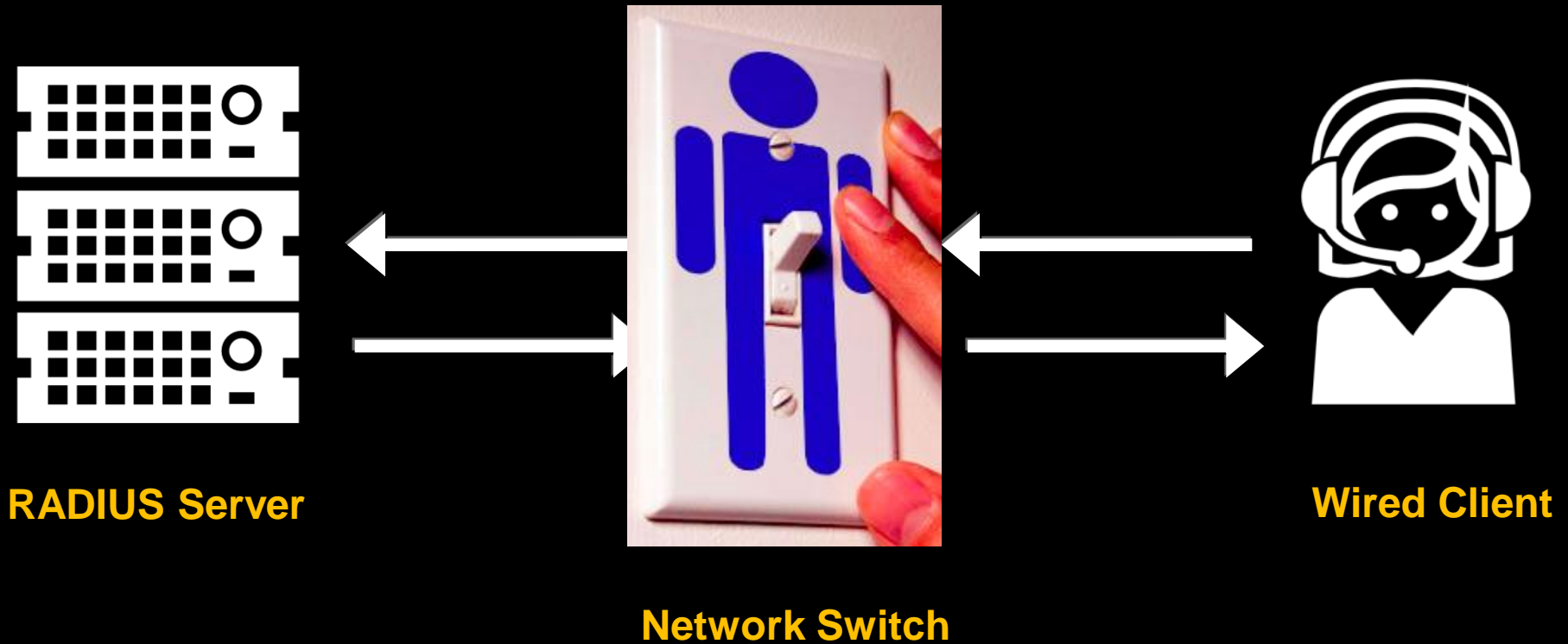


**Wireless Client**



**Access Point**

# Ethernet

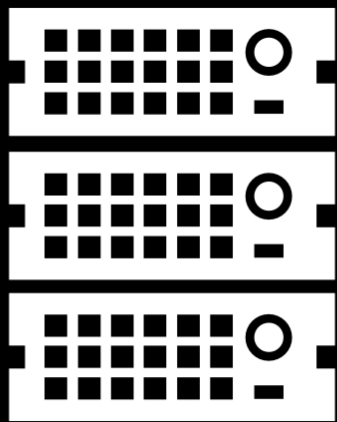


**RADIUS Server**

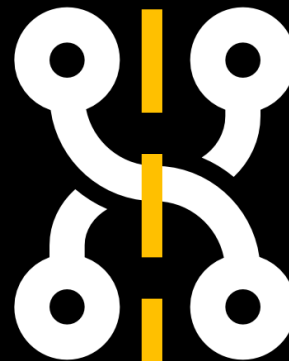
**Network Switch**

**Wired Client**

# TRUSTED

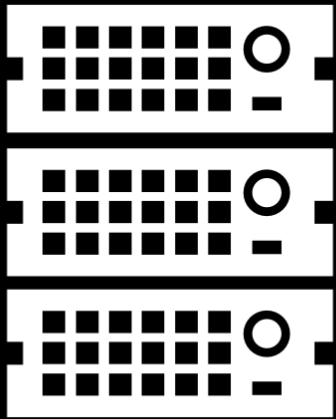


# UNTRUSTED

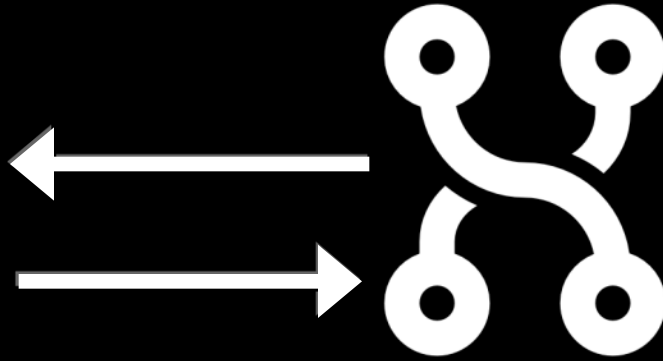




# What if I.....



Cisco ACS 4.2

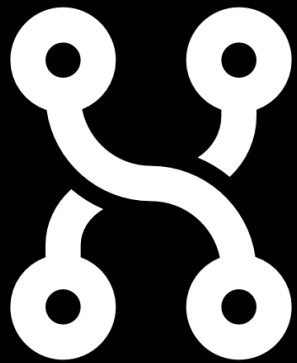




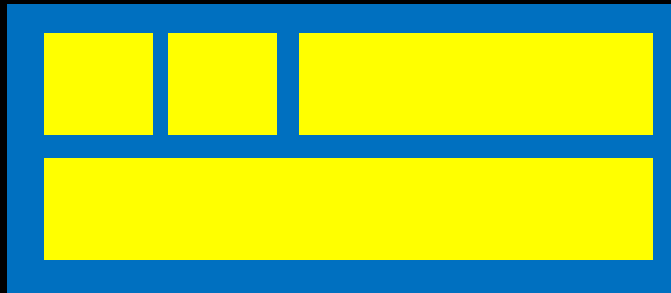
RFC3748

EAP

Extensible Authentication Protocol

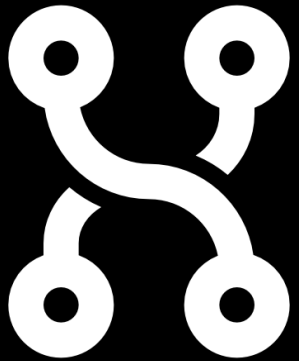


802.1x

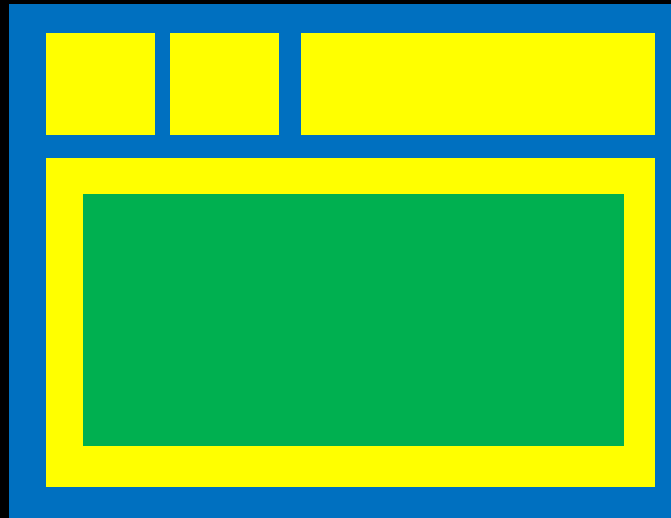


EAP

(Layer 2)

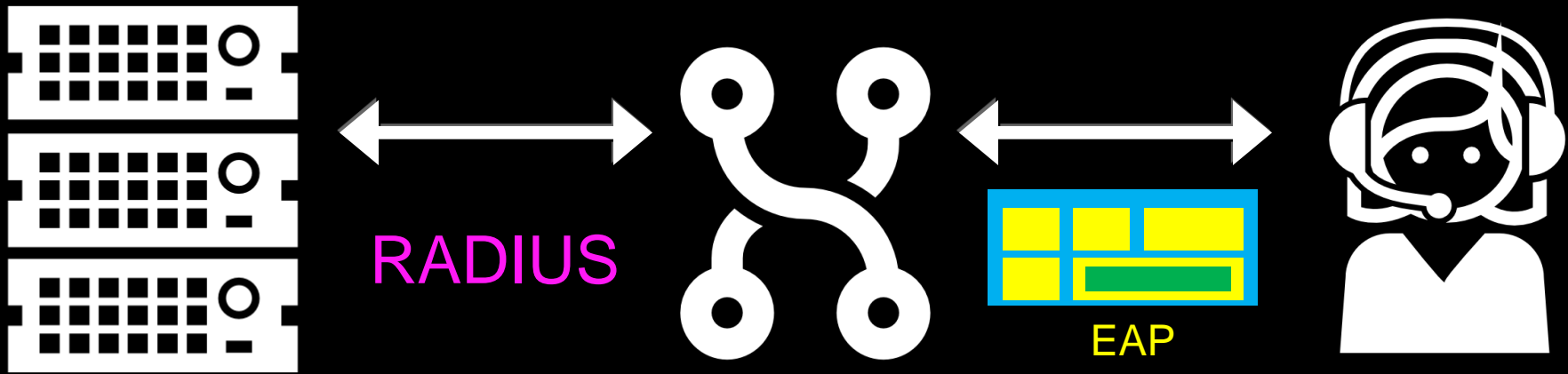


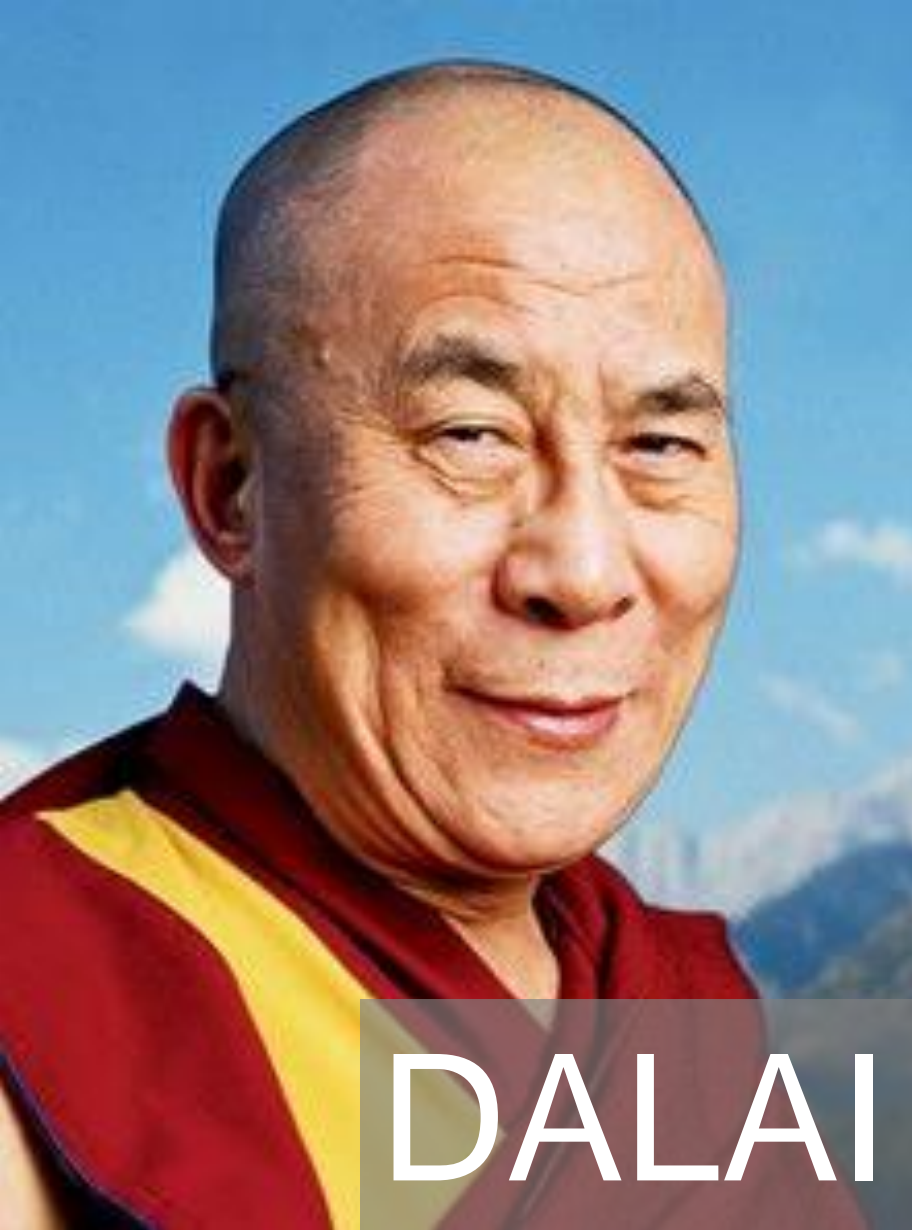
EAP



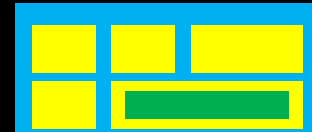
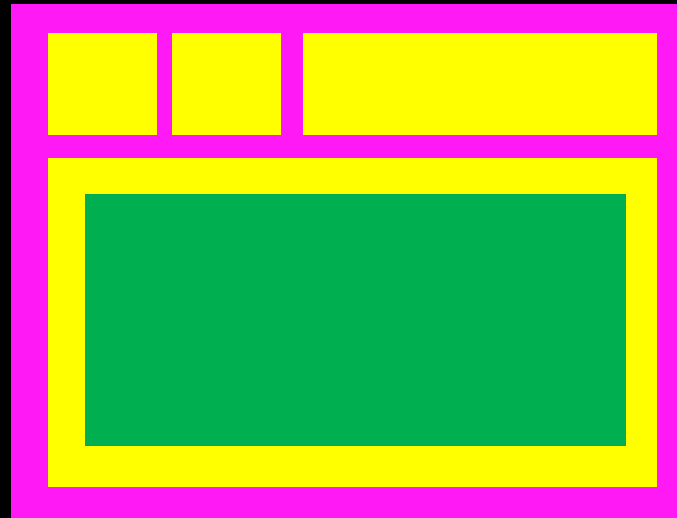
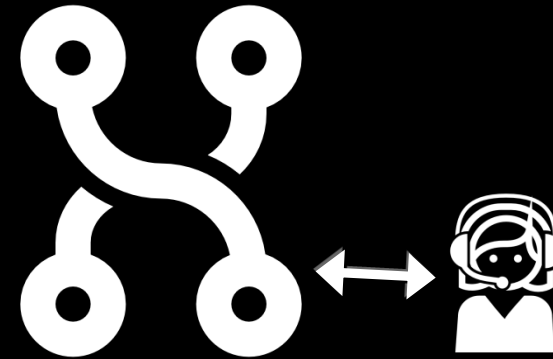
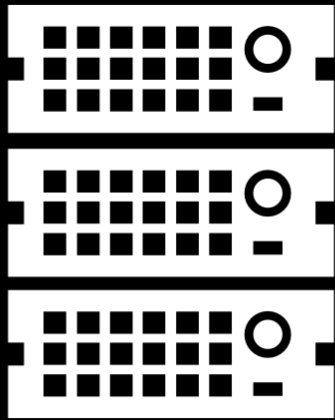
Type:  
PEAP, EAP-TTLS,  
EAP-FAST, etc..

(Layer 2)





# DALAI LAMA



RADIUS

(layer 3)

# RADIUS

RFC2865/2869

Remote Access Dial-In User Service



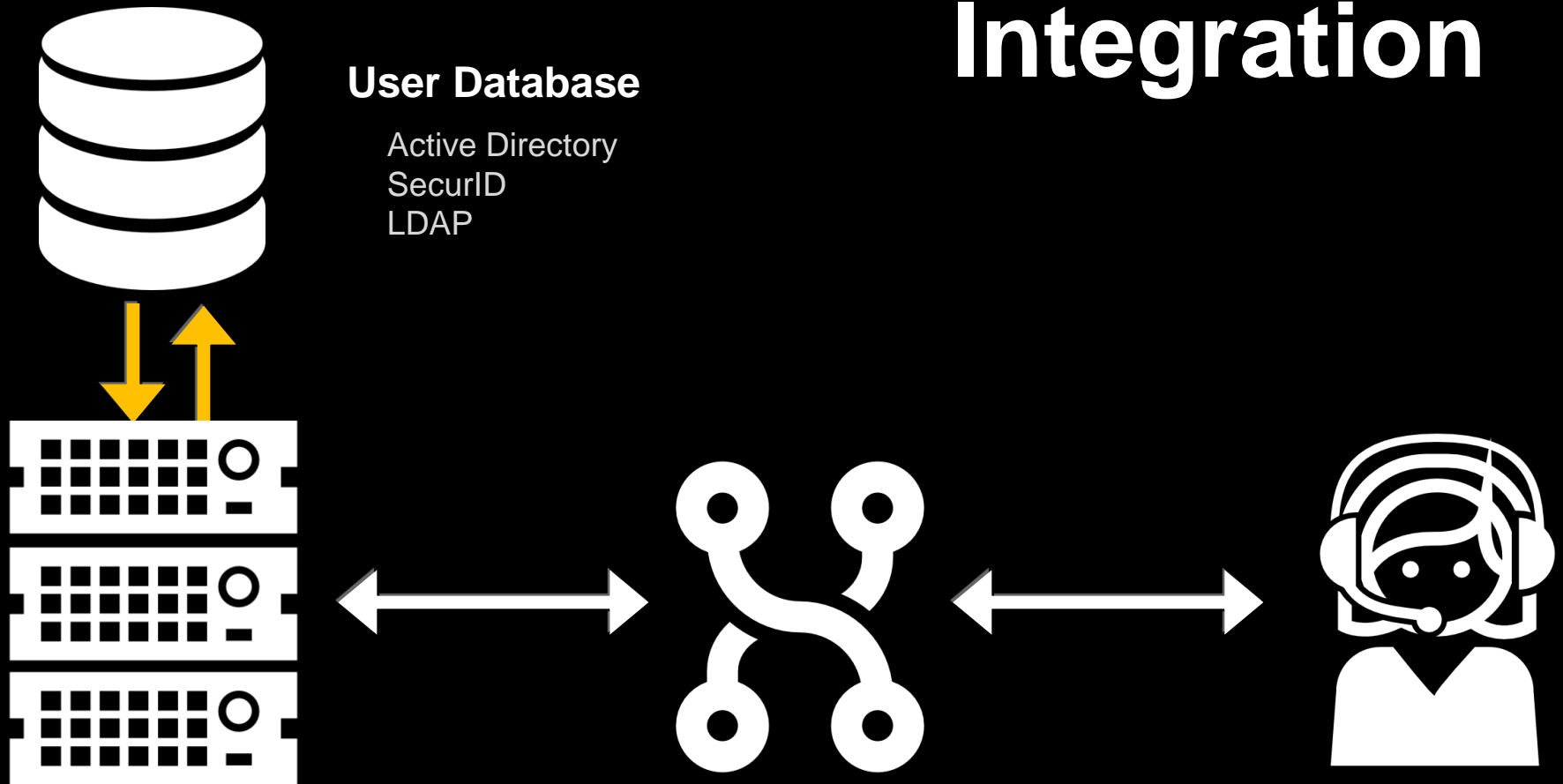
DSL/Dialup



VPN



# Integration

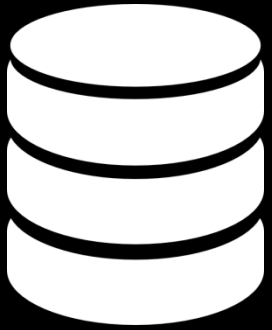


## User Database

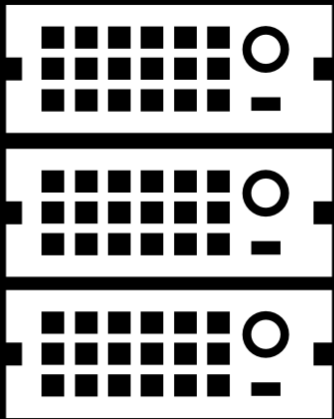
Active Directory  
SecurID  
LDAP



# Surface



## External Auth Handler



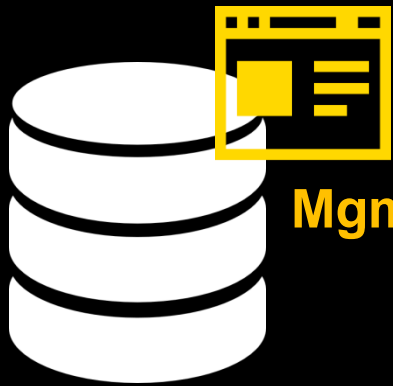
RADIUS/EAP/Types



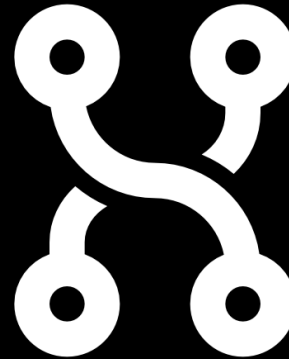
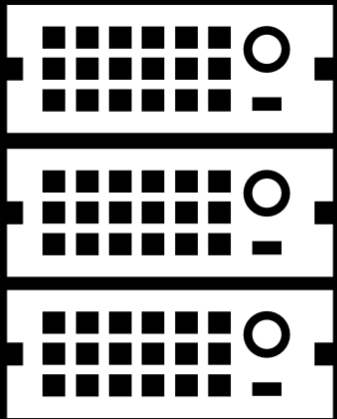
802.1x/EAP/Types



(Protocol/Configuration/Handling issues)



**Mgmt Web UI**



**Mgmt Web UI**



**Mgmt Web UI**

# Attacks



# Sniffing

no need to be fancy, just  
use Wireshark

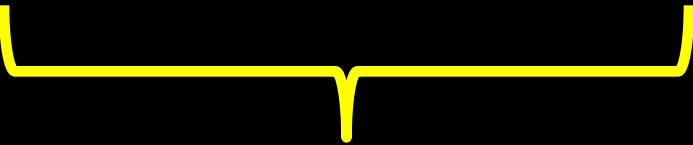
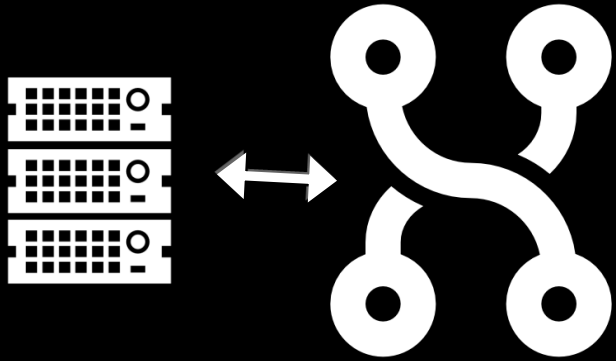
## Offline Brute-Force

**Shared Secret/User-Password:** john  
**CHAP:** hashcat  
**EAP Data..:** asleep, and eapmd5pass

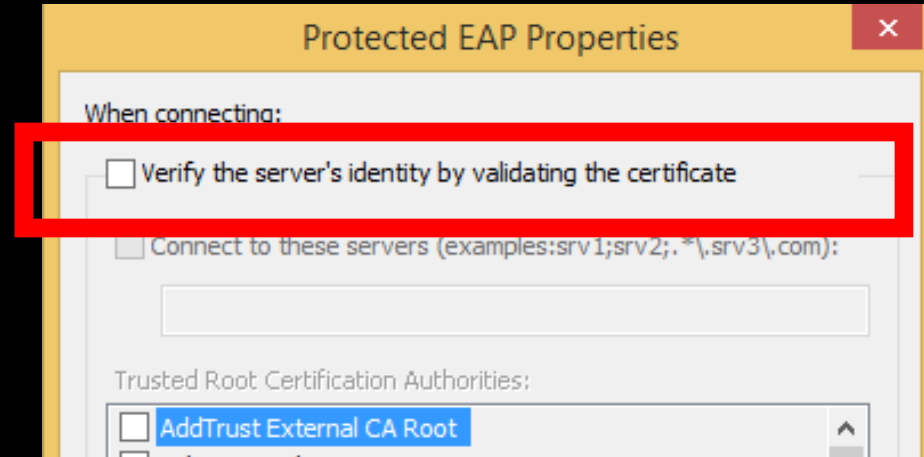
## Clear-text Data

User-name AVP/Eap Ident  
NAS-Id  
Calling-Station  
State

(Configuration Issue)

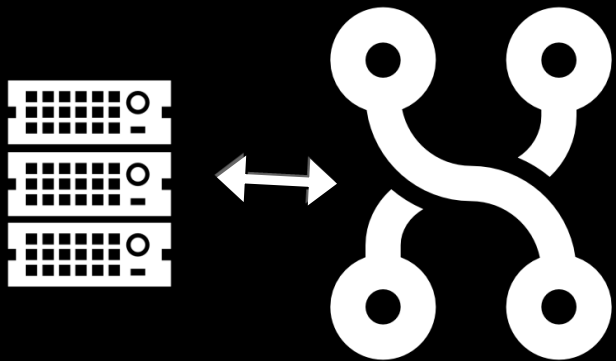


**Attacker Controlled**



# Impersonation

(Configuration Issue)

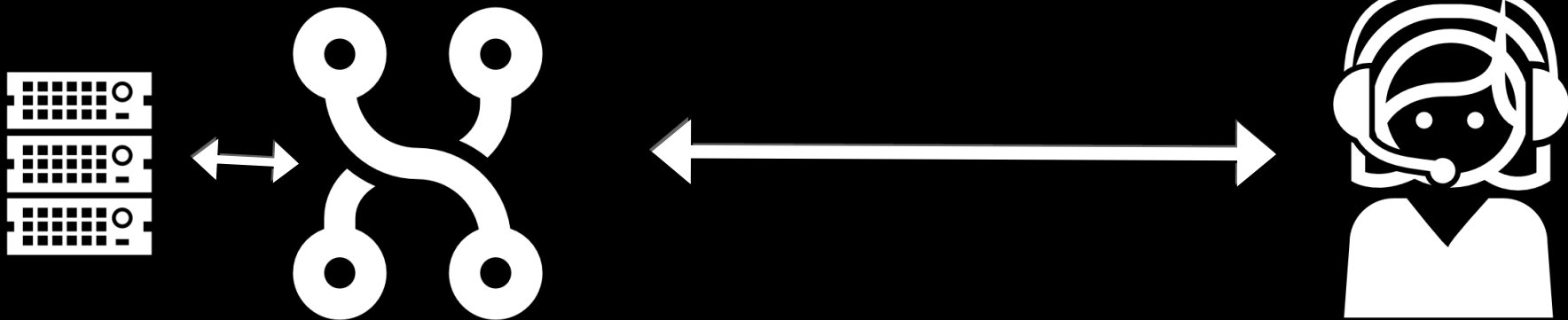


# FreeRADIUS-WPE

Which AP belongs to my Company?







# hostapd-wpe

<https://github.com/OpenSecurityResearch/hostapd-wpe>

- Supports Tons of EAP-Types (including EAP-FAST Phase 0)
- Always Returns EAP-Success
- Requests PAP first
- Responds to all 802.11 probe requests
- Heartbleed (Cupid)
- Saves to file/outputs NETNTLM format

Thanks to JoMo-Kun, @lgrangeia, and @haxorthematrix for Patches/Functionality and improvement suggestions

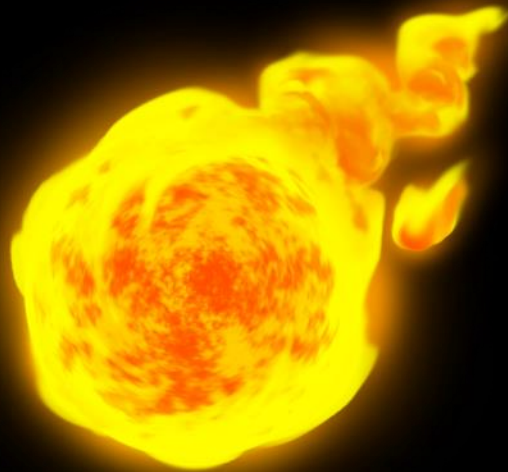


**WHERE ARE THE**

**HANDLER BUGS?!**

made on imgur

# Fuzz



## RADIUS/EAP/802.1x

# Peach Overview

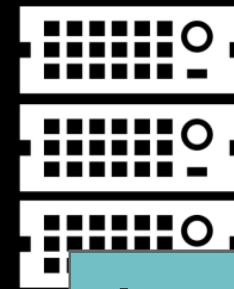
DataModel

Transformers,  
mutators, etc..

Publisher

StateModel

Targets



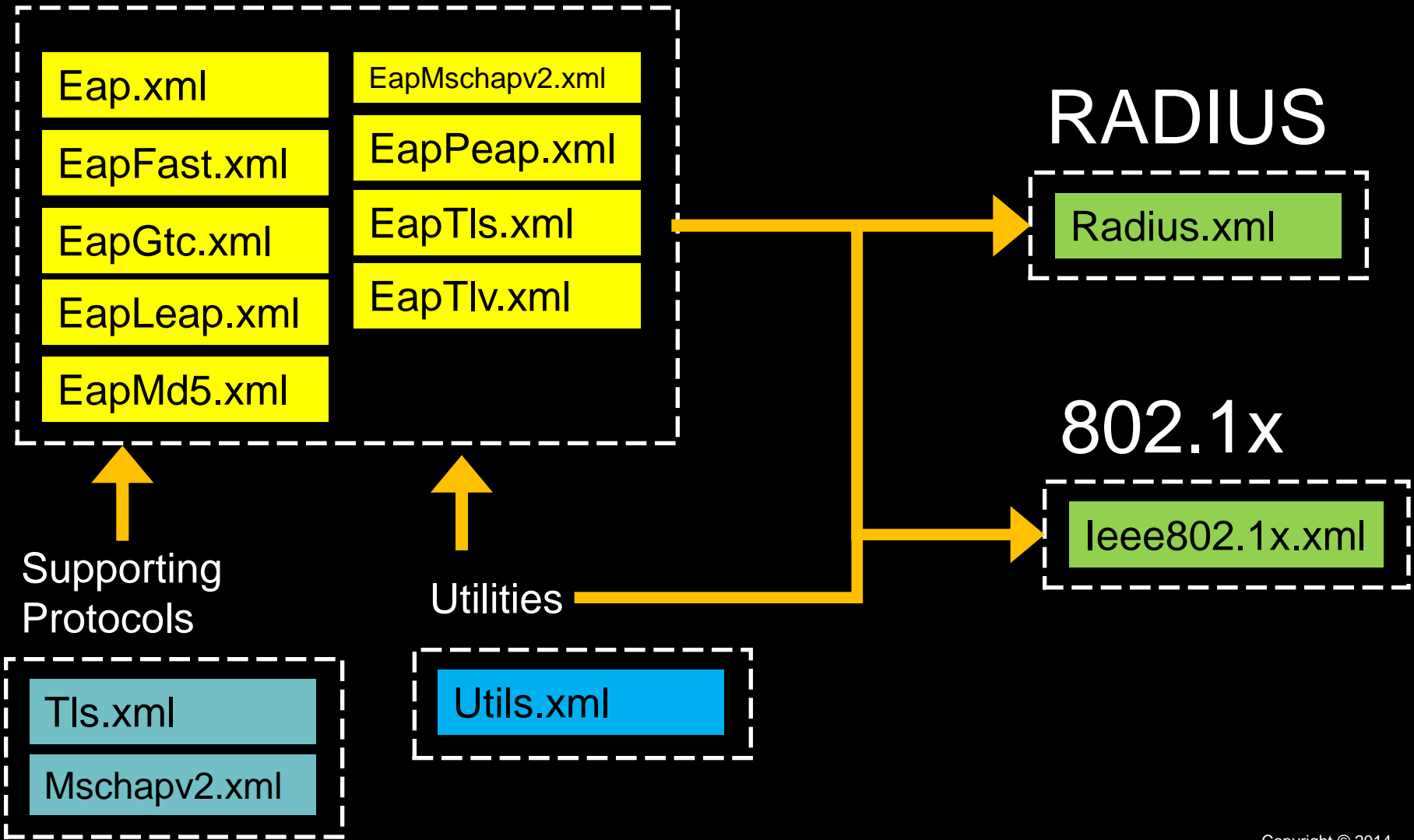
Agent



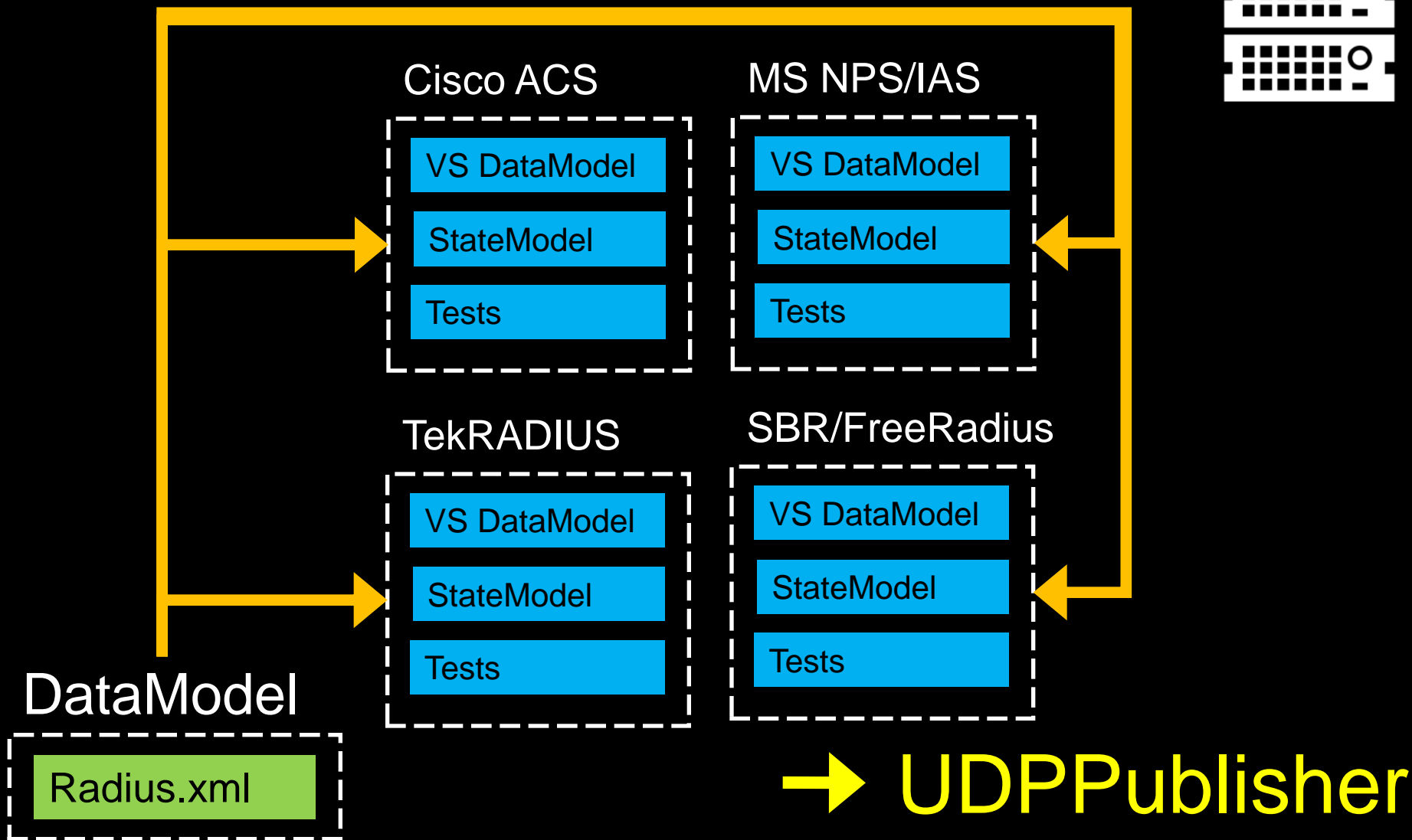
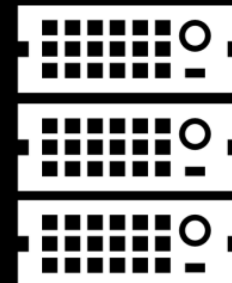
Agent

# DataModels

## EAP



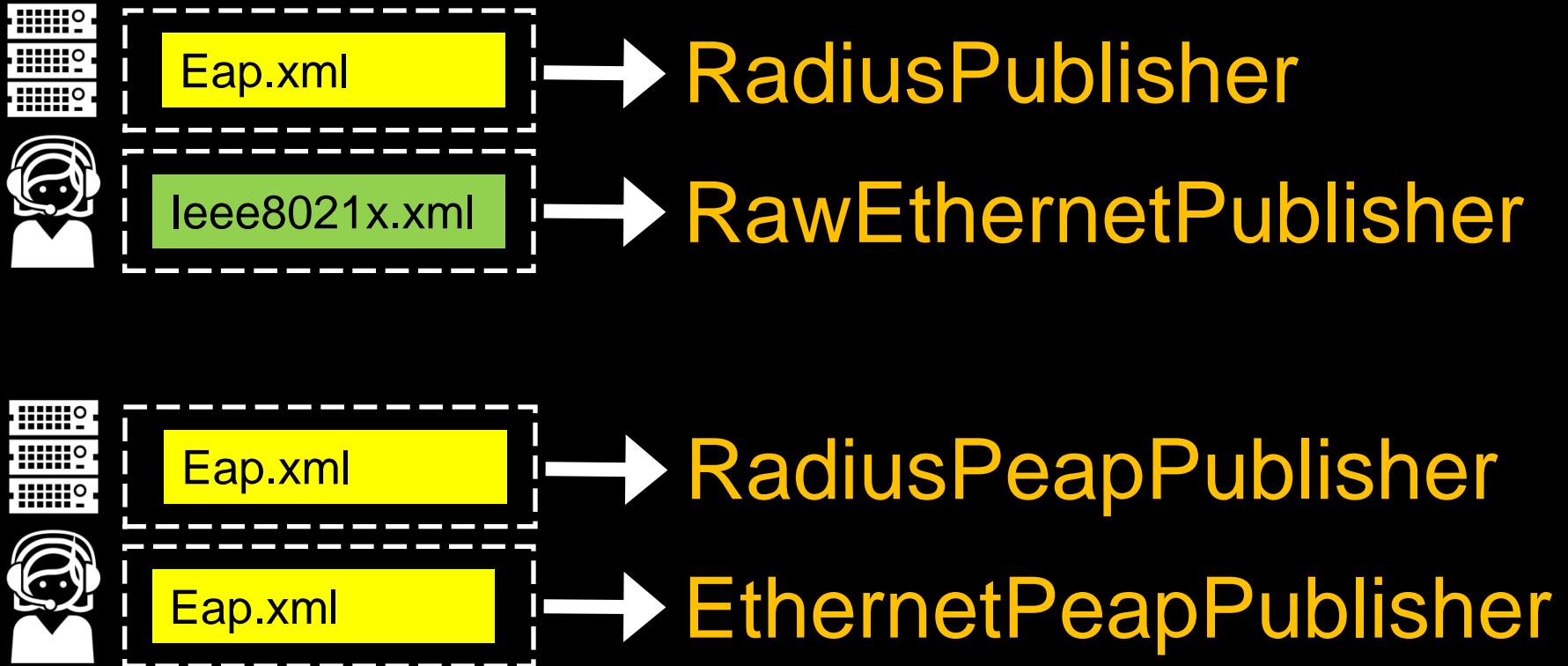
# Fuzzers





**MICHAEL CERATOPS**

# Publishers



all via wired, supports all tunneled EAP Types

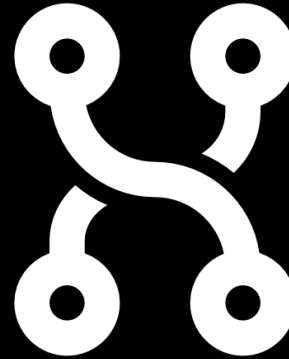
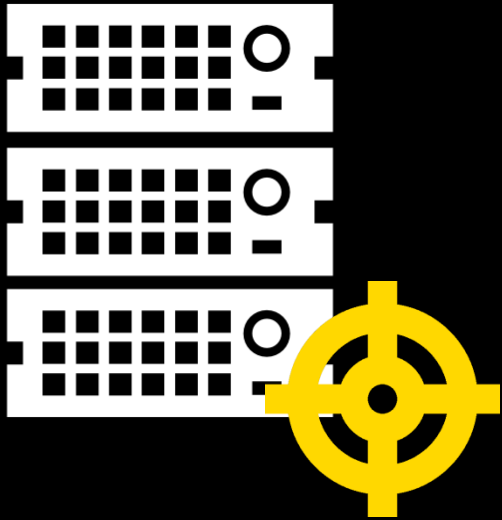


# StringMutator.Data.cs:

```
namespace Peach.Core.Mutators
{
    public partial class StringMutator
    {
        static readonly string[] values = new string[] {
```

- LDAP Injection**
- XSS**
- SQL Injection**
- CMD Injection**
- etc...**





# RADIUS/802.1x/EAP

# Tools

A photograph of a man and a woman dancing at a party. The man is on the left, wearing dark sunglasses and a dark shirt, holding a drink. The woman is on the right, wearing a silver sequined dress and has her hair styled up. They are both smiling and looking at each other. The background is dark with some light spots, suggesting a club or party setting.

Existing:  
libeap  
Pyradius

Releasing:  
Radius .Net (forked)  
Eap .Net  
OpenSSL .NET ..i know.. “ugh .Net”

## Eap.NET (New)

```
RadiusEapSession eClient = new RadiusEapSession(host, secret)
EthernetEapSession eSvr = new EthernetEapSession(dev, pub, priv)
EapPacket ePkt = new EapPacket(bytes) // Recv
```

```
EapPacket ePkt = new EapPacket(Code, Type, ID);
ePkt.SetEapData(bytes);
```

## OpenSSL.NET (Fork)

```
SslUdp SslClient = new SslUdp(false)
SslUdp SslSvr= new SslUdp(pub, priv, true)
SslSvr.Send(ePkt.RawData)
```

# Profiling



**RadiusEapProfiler.exe**

## AVP-State (RADIUS)

Maintains State of the Connection  
Active/Passive  
Cisco: "acs/Number/Number"  
MS NPS: 38 Bytes

## EAP-Res/Ident Msg-Auth. (RADIUS)

Username  
MS NPS: Will reject if ! valid  
Others: Doesn't matter

Cisco: Ignores  
Others: Access-Reject

# Brute-Force

Or Enumeration ...whatever



**eapEnum.exe**

**Password**

a.k.a Active Brute Force (..meh)

**Username**

NPS: Eap-Resp/Identity

**EAP-Type**

Client Downgrade

# TODO

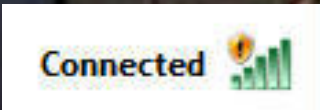
wpa\_supplicant-wpe  
enumeration/profiles/exploits

# Notes for the researchers

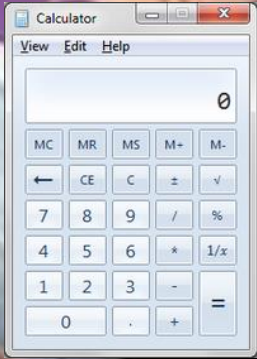
- Don't try to fuzz EAP over WiFi or using wpa\_supplicant or through an authenticator
- eapol\_test is great ("make eapol\_test" in wpa\_supplicant)
- netsh lan reconnect will start a 802.1x connection on Windows 7 and 8.1
- +hpa +ust to find the real goodies



# Exploitation



&





@brad\_anton

Brad.Antoniewicz@foundstone.com

\*many of the pics in this presentation were found on the internet – credit goes to [images.google.com](http://images.google.com)