Foundstone
A division of McAfee

802.1x and BEYOND!

Brad Antoniewicz

McAfee
Proven Security™

Hi, I’m @brad_anton

Agenda

About 802.1x Attacks Fuzzing/Tools

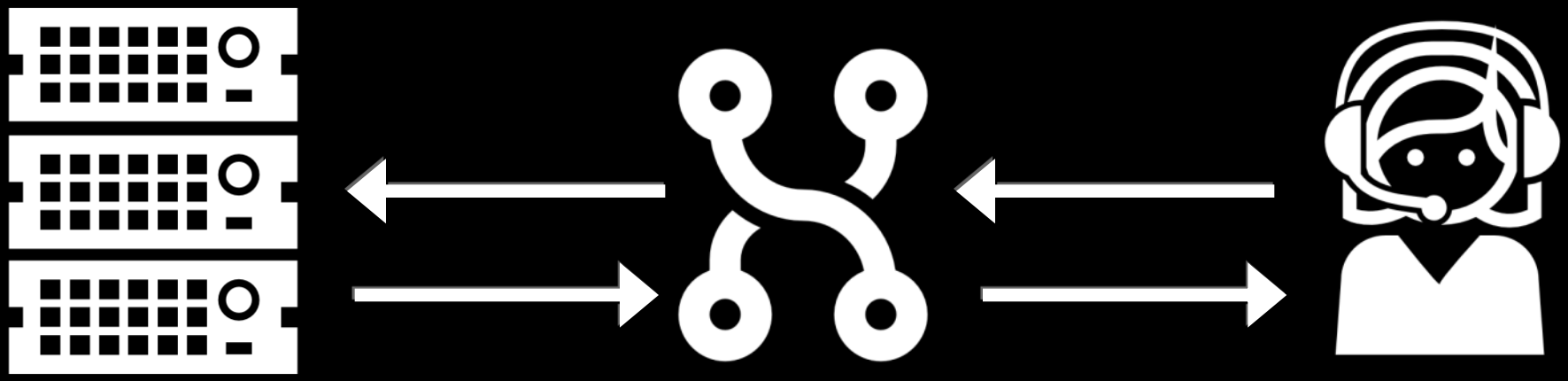
IEEE 802.1x

Port-Based network access control

Cause not everyone is welcome at church?

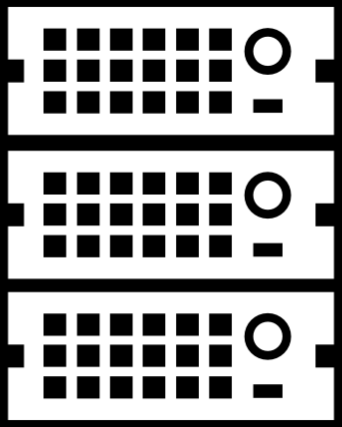
Flow

(IEEE 802.1x)

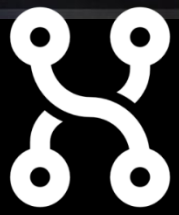


Authentication Server **Authenticator** **Supplicant**

802.11



RADIUS Server

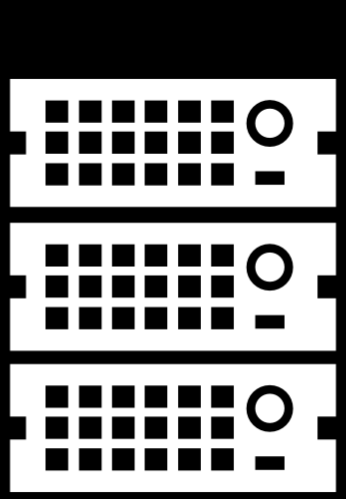


Access Point

Wireless Client

Brad.Antoniewicz@foundstone.com @brad_anton @foundstone

Ethernet



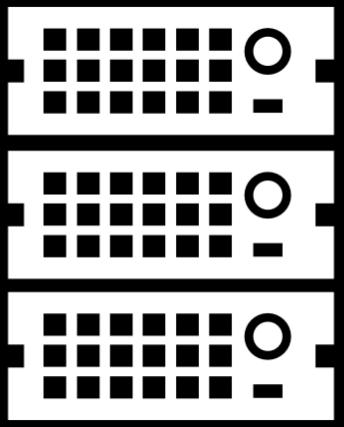
RADIUS Server

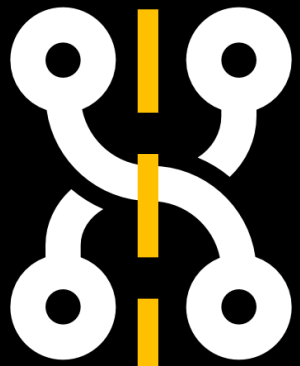
Network Switch

Wired Client

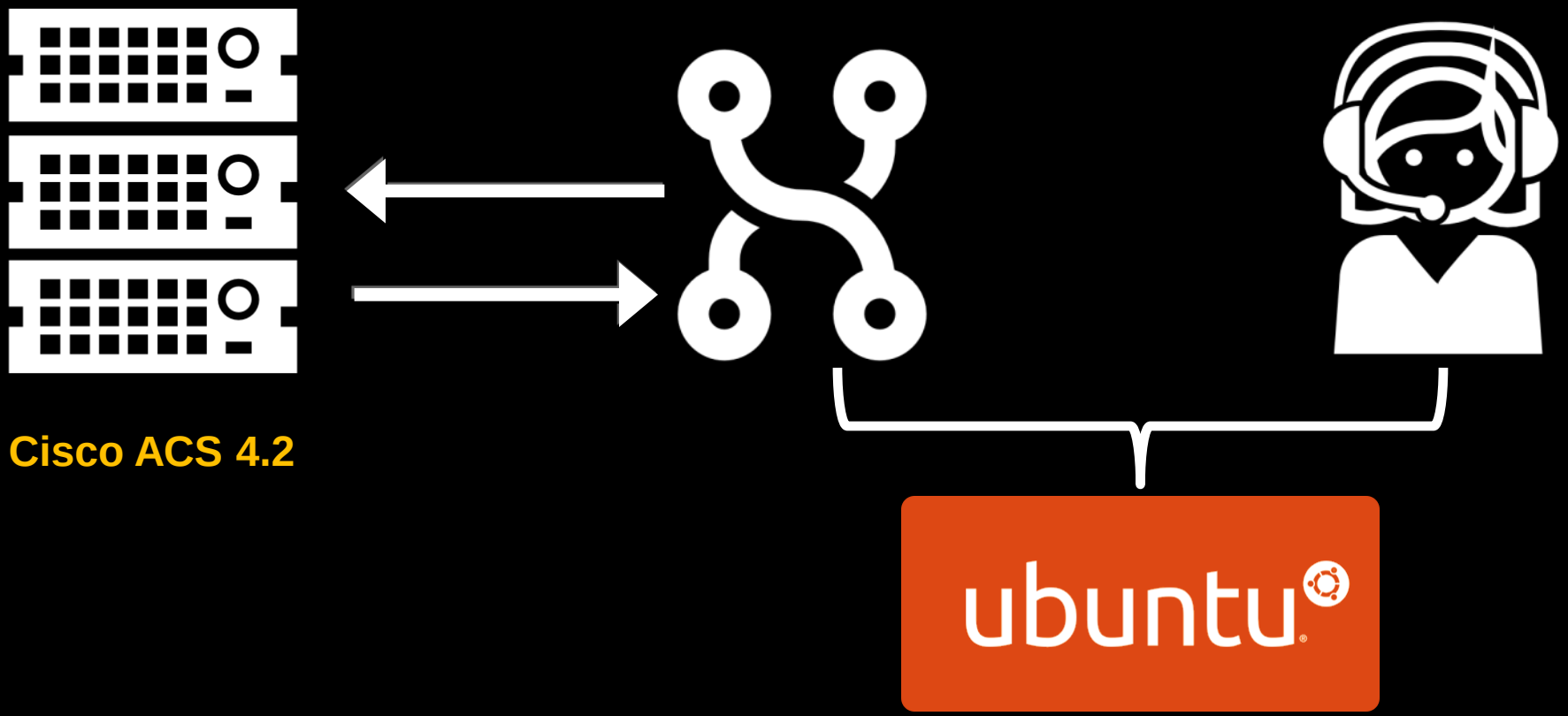
TRUSTED

UNTRUSTED





What if I….

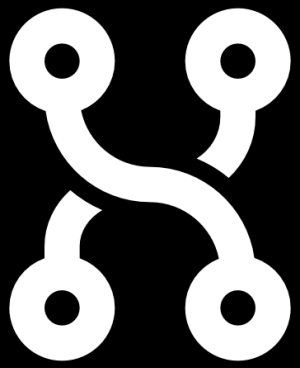


RFC3748

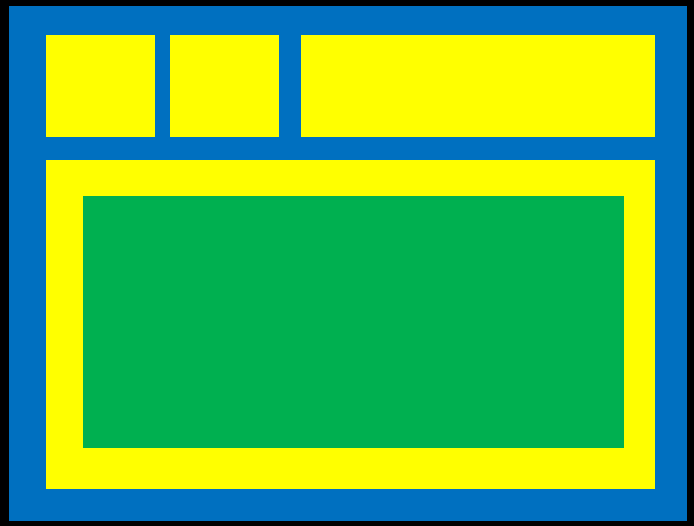
EAP

Extensible Authentication Protocol

(Layer 2)

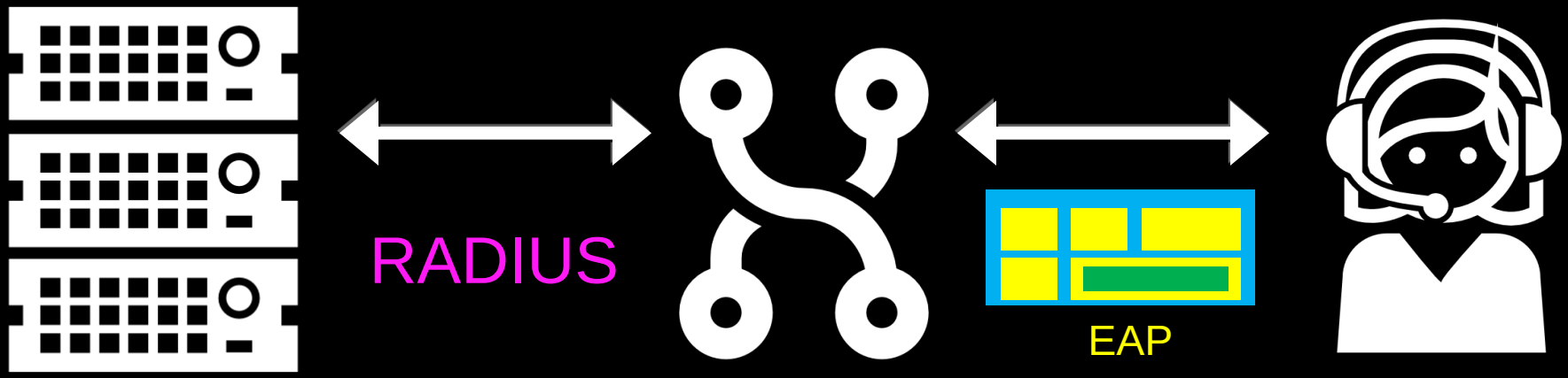


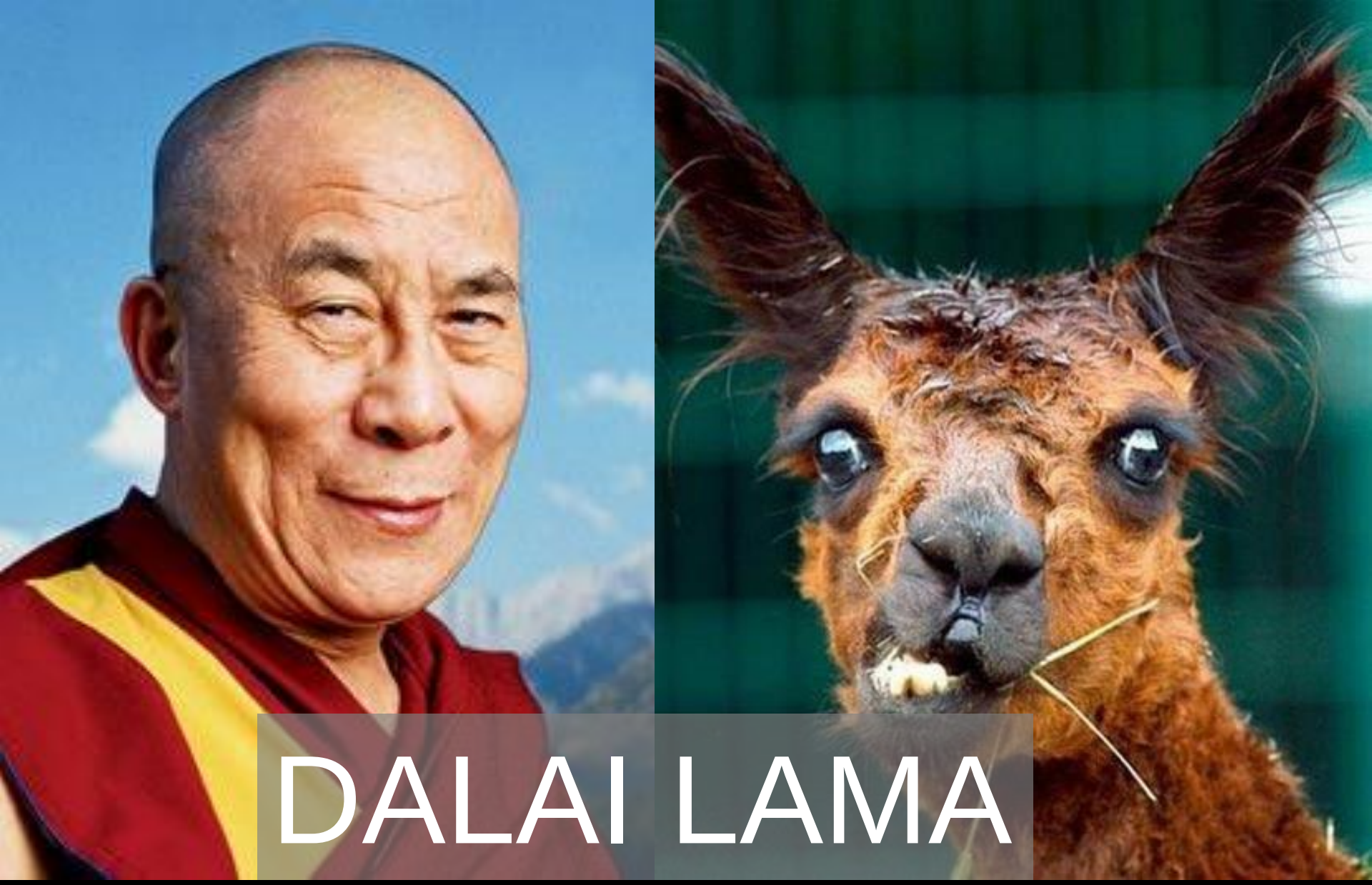
EAP

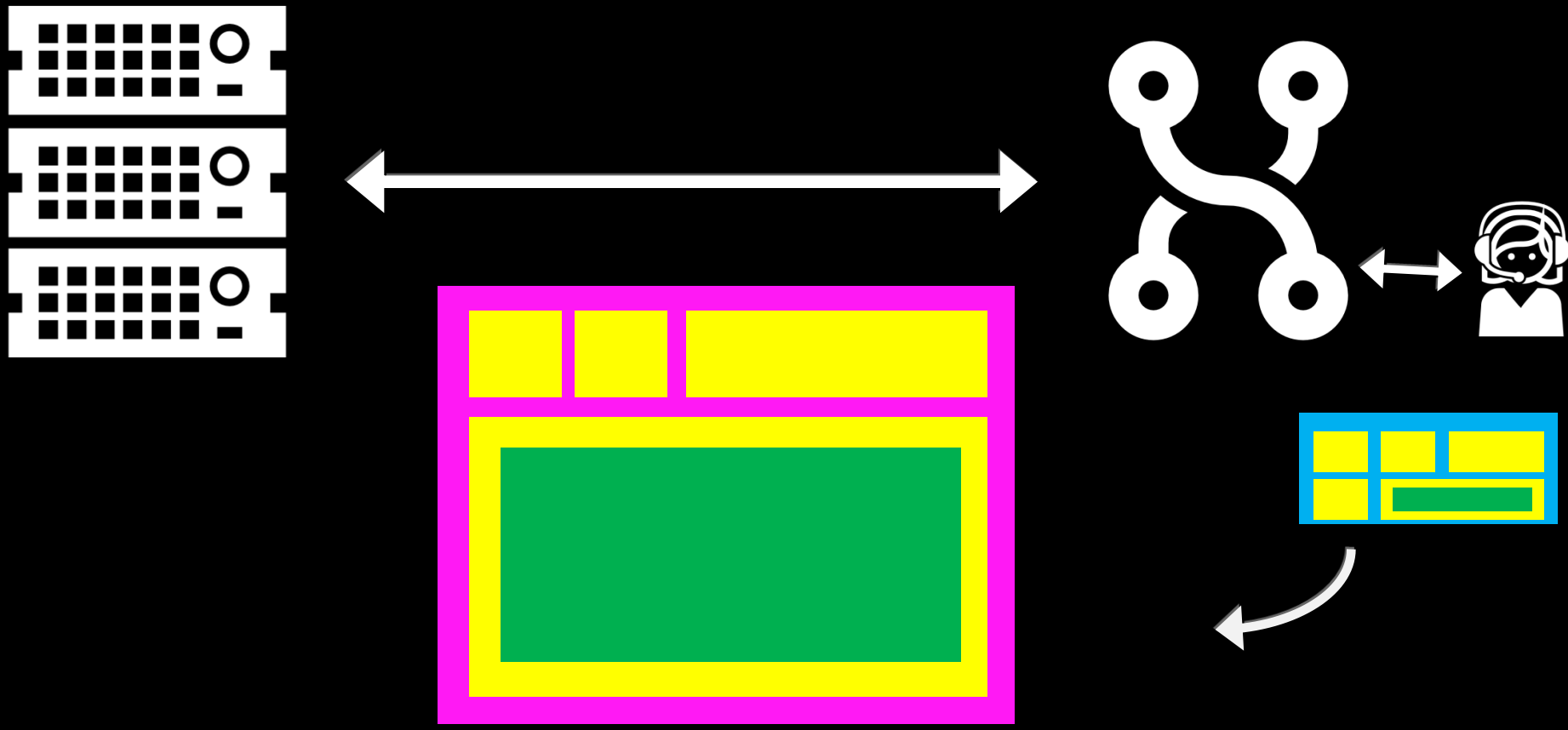


Type:
PEAP, EAP-TTLS,
EAP-FAST, etc..

(Layer 2)







(layer 3)

RADIUS

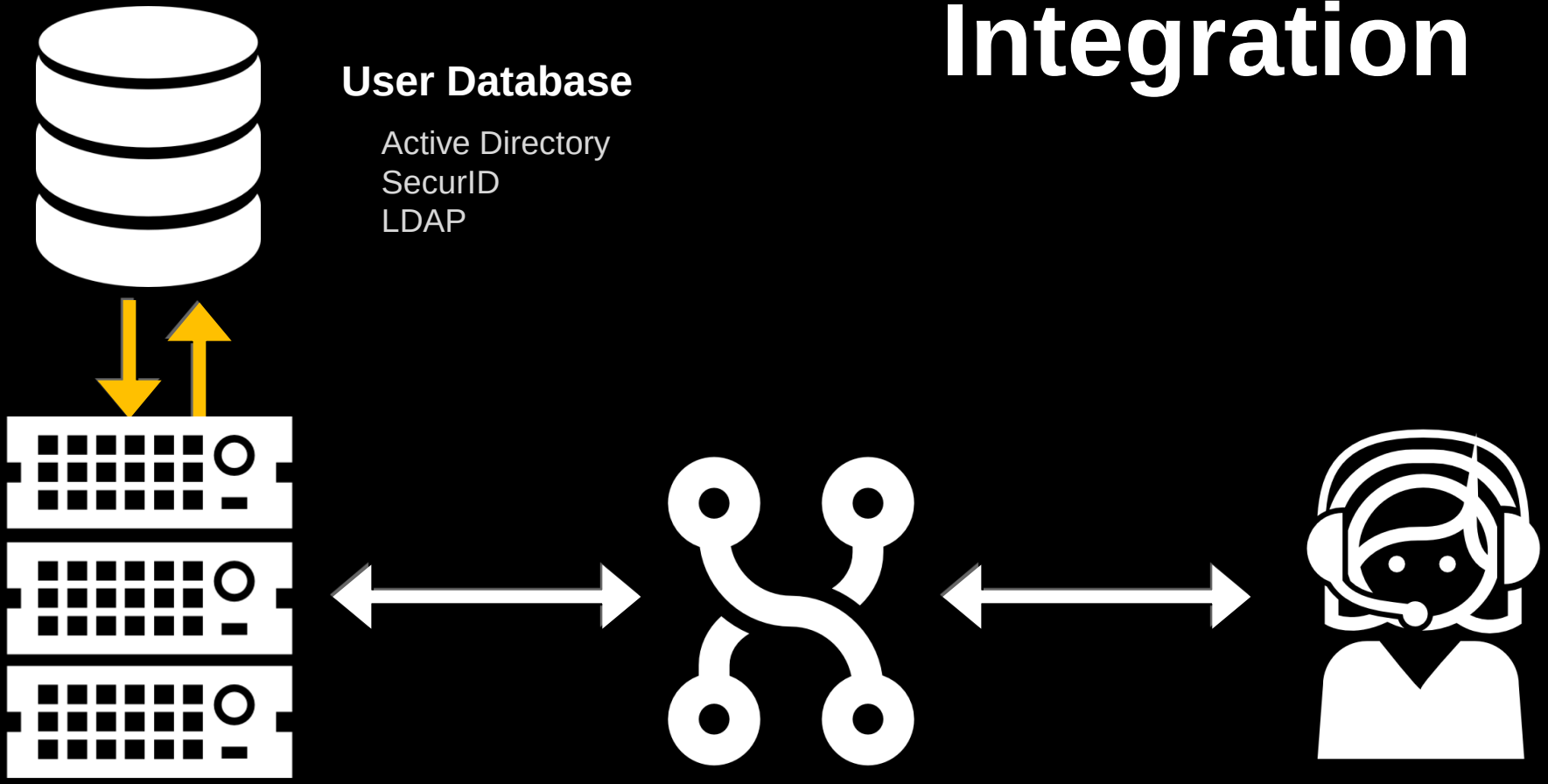
RFC2865/2869

Remote Access Dial-In User Service

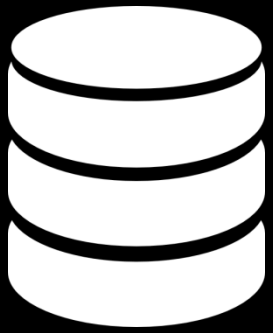
DSL/Dialup

VPN

Integration

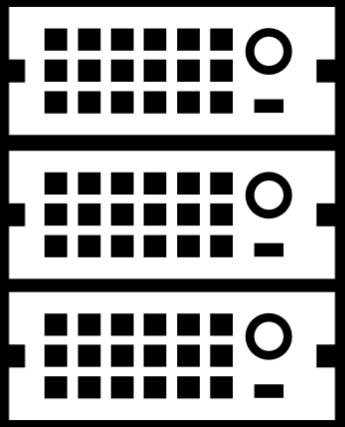


Surface

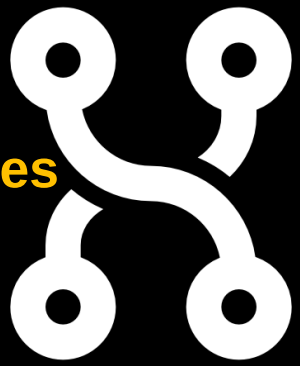


Surface

External Auth Handler

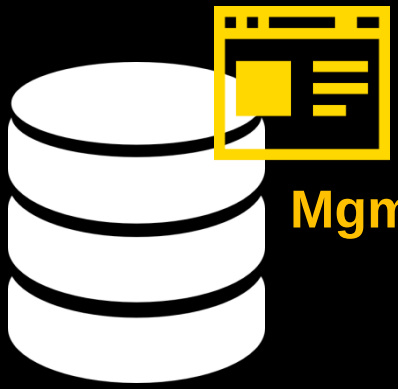


RADIUS/EAP/Types

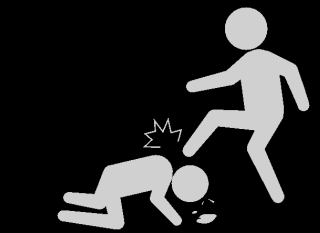


802.1x/EAP/Types

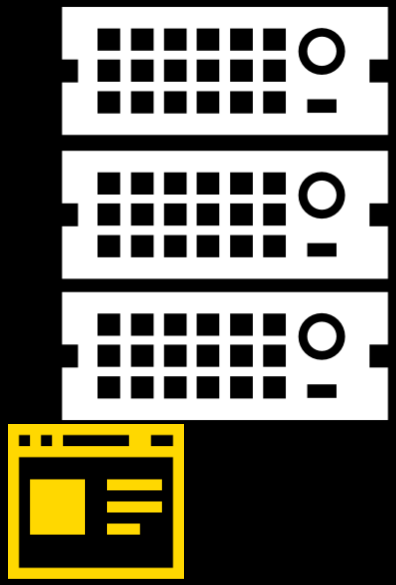
(Protocol/Configuration/Handling issues)



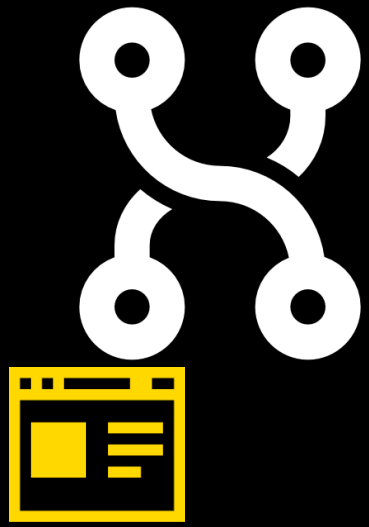
Mgmt Web UI



Surface



Mgmt Web UI



Mgmt Web UI

Attacks

(Protocol Issue)

Sniffing

no need to be fancy, just use Wireshark

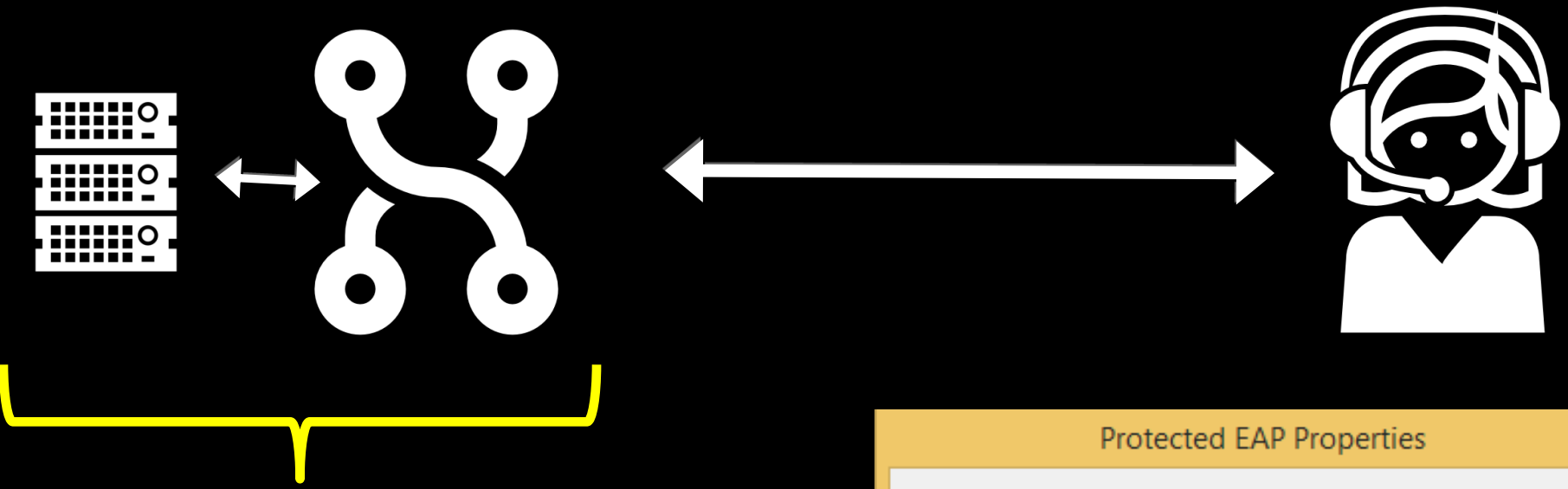
Offline Brute-Force

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

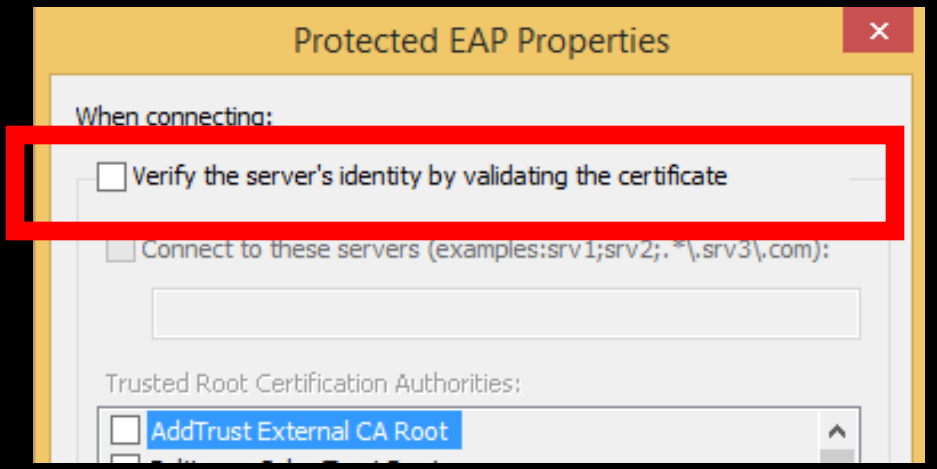
Clear-text Data

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

(Configuration Issue)

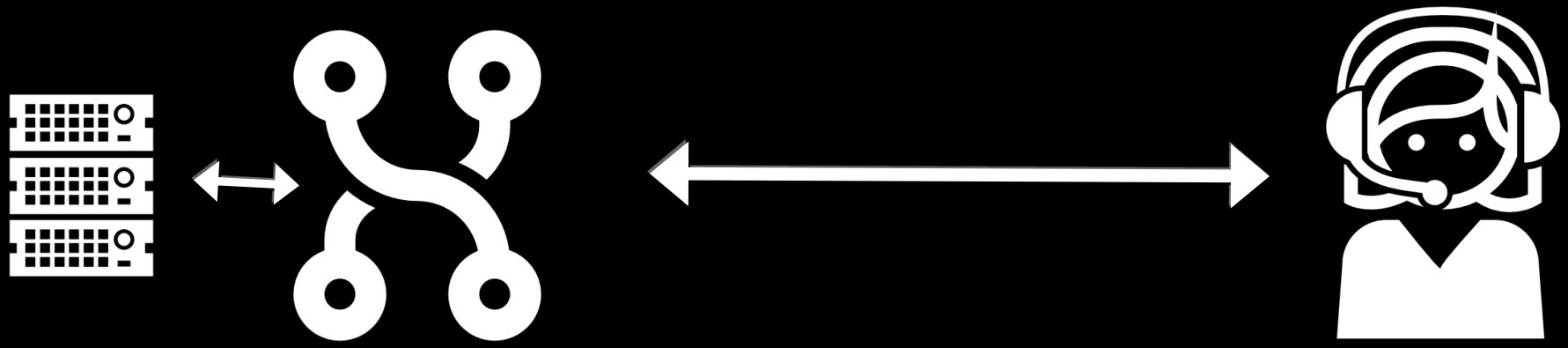


Attacker Controlled

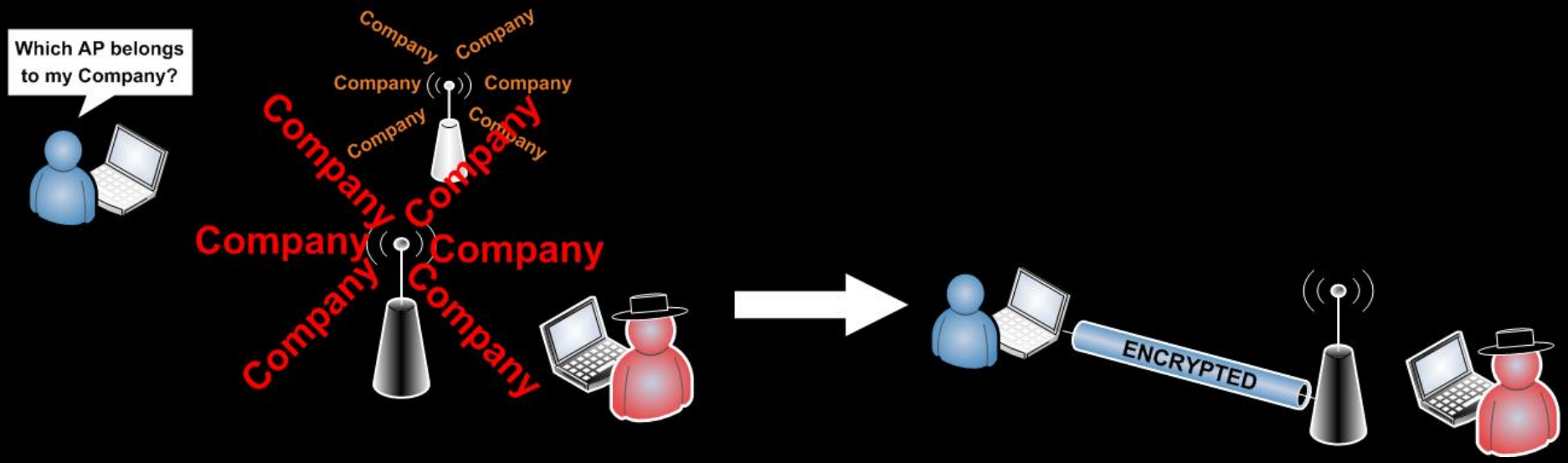


Impersonation

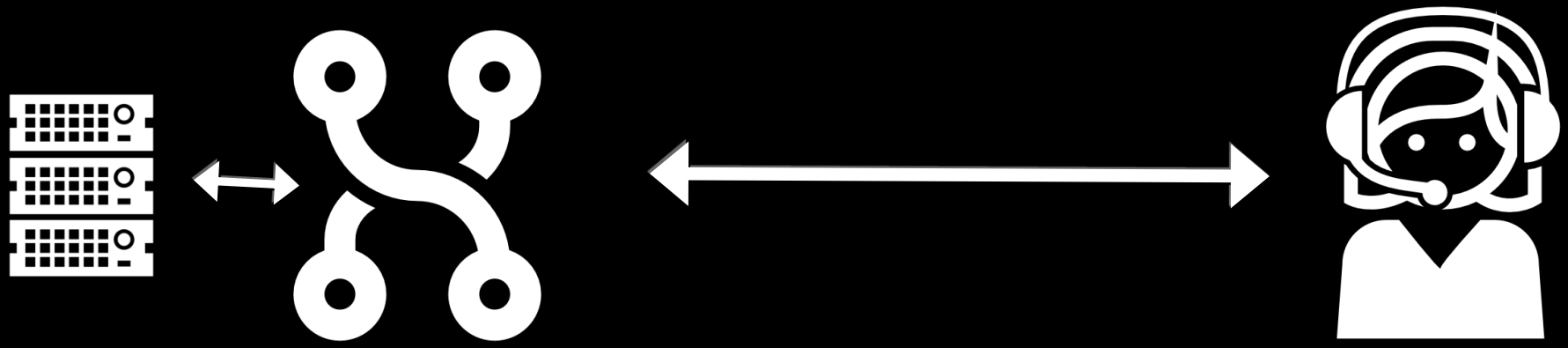
(Configuration Issue)



FreeRADIUS-WPE



(Configuration Issue)

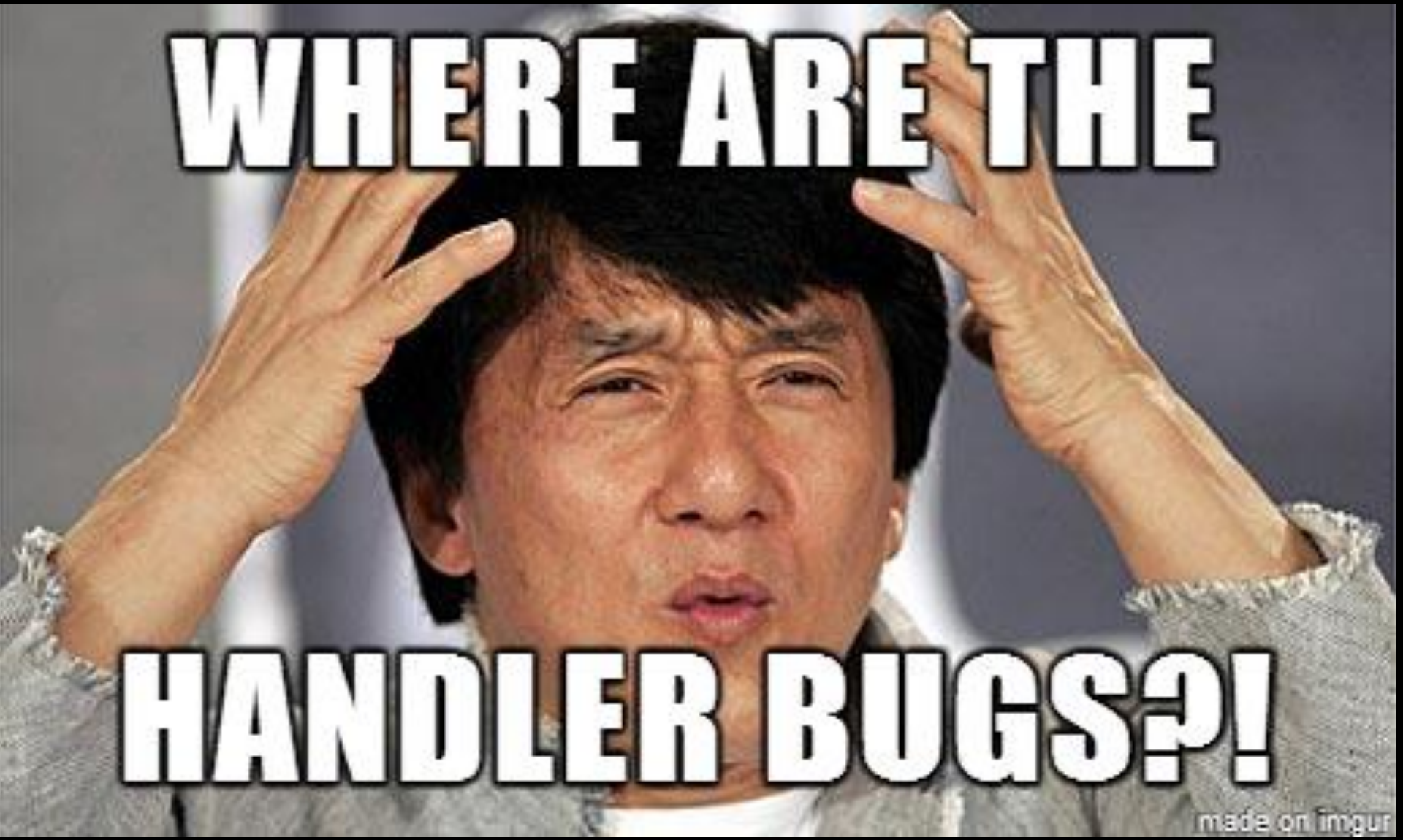


hostapd-wpe

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

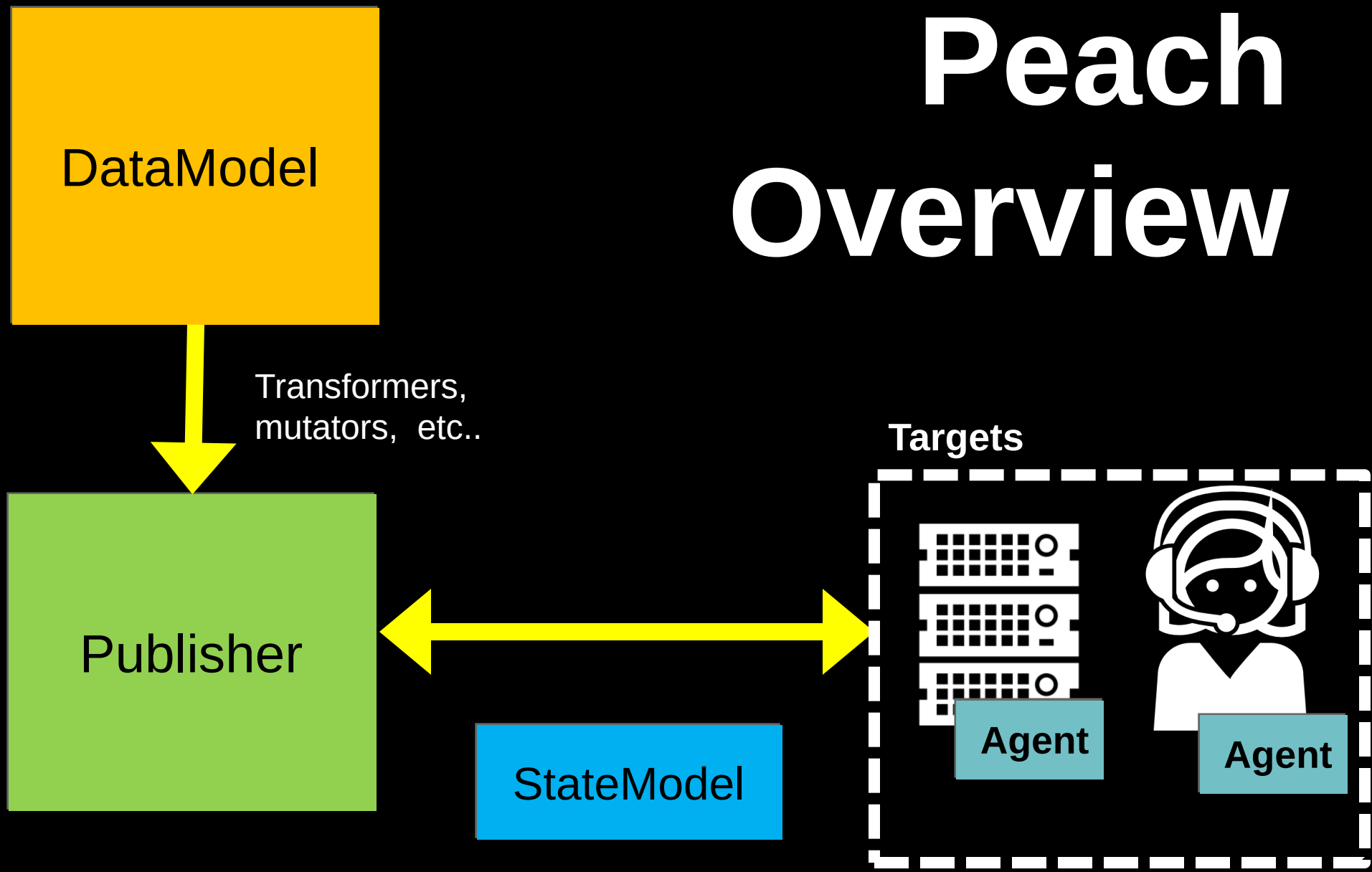
Thanks to JoMo-Kun, @lgrangeia, and @haxorthematrix for Patches/Functionality and improvement suggestions



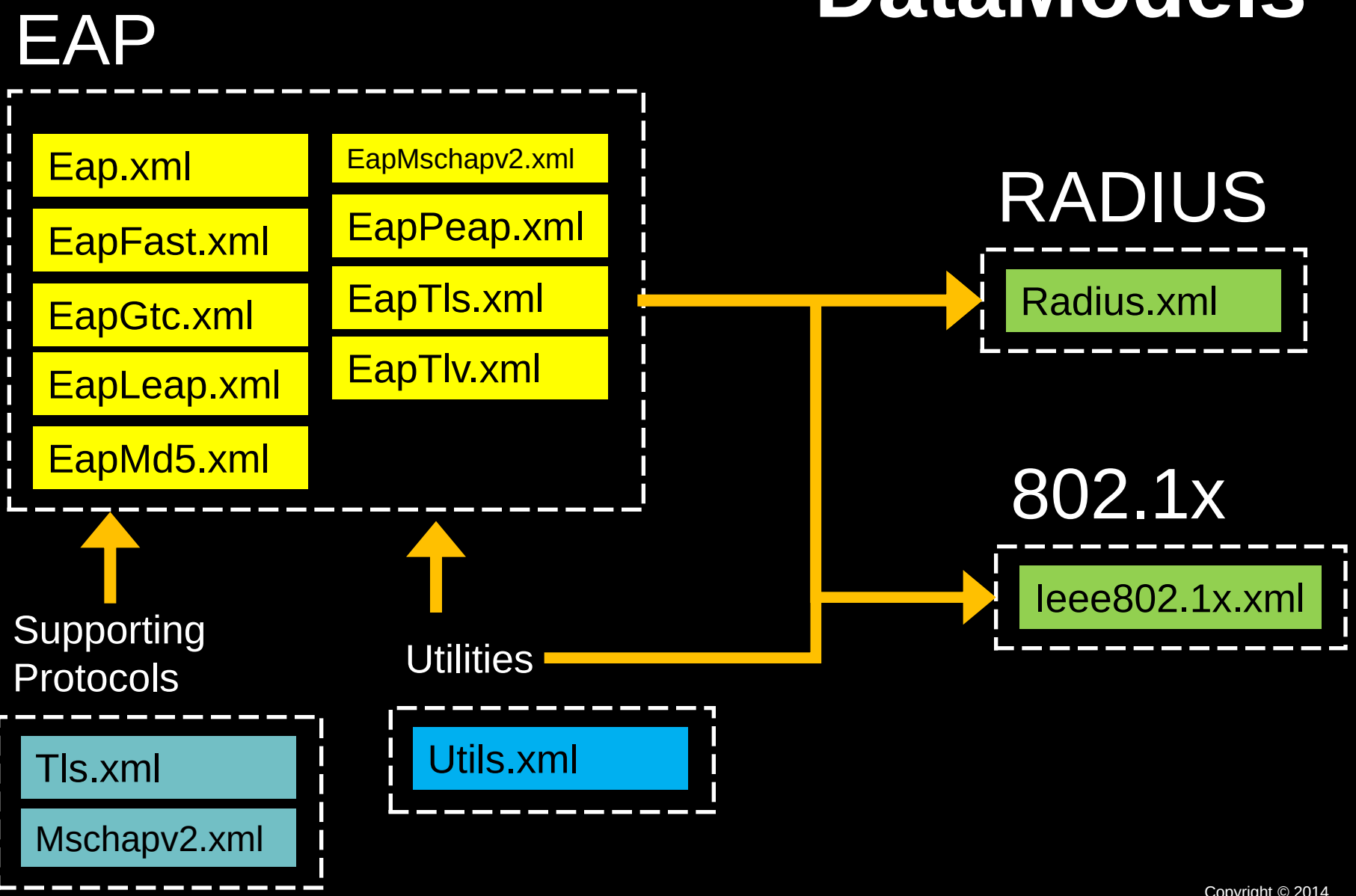
Fuzz

RADIUS/EAP/802.1x

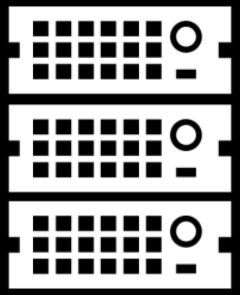
Peach Overview

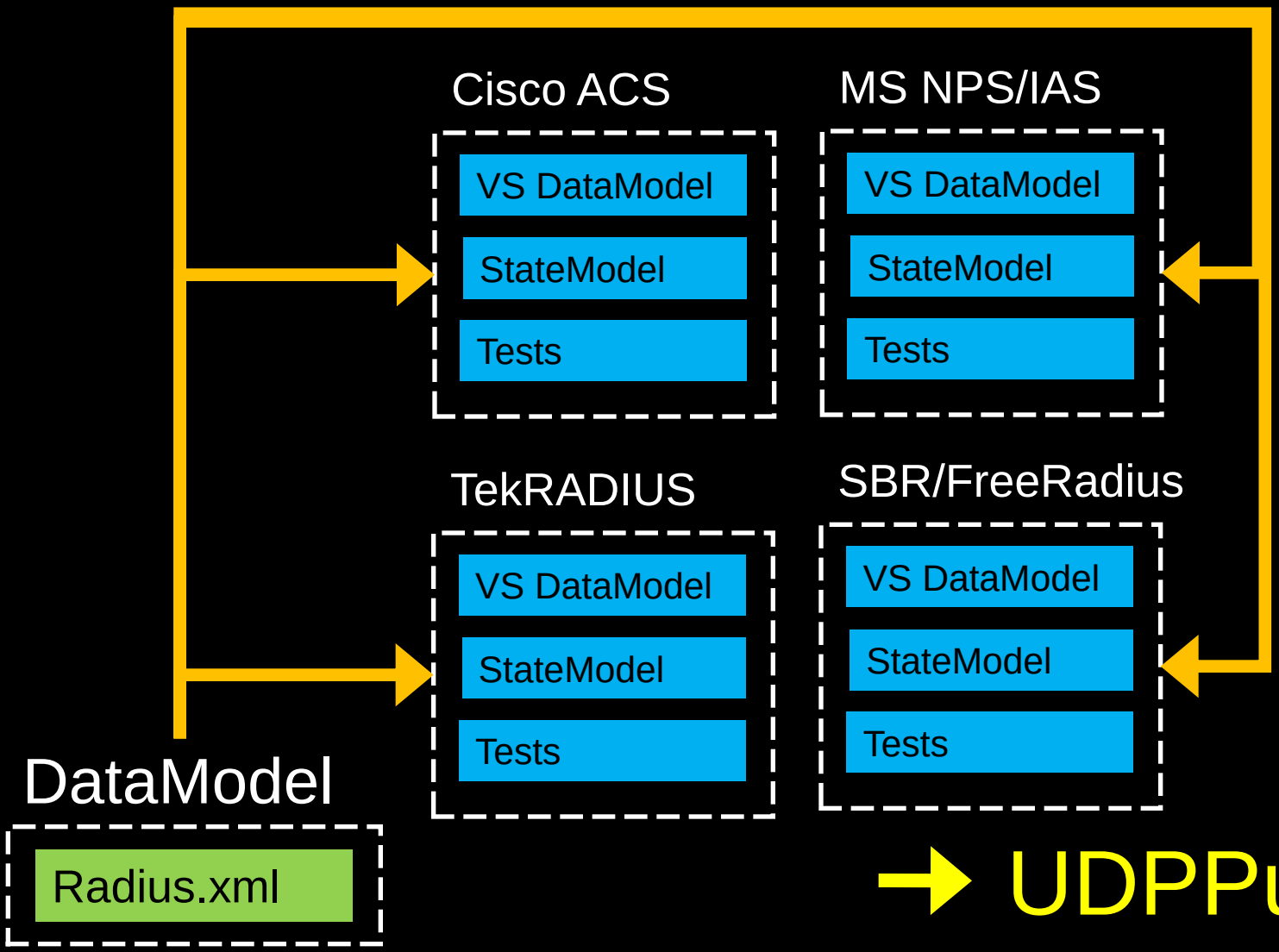


DataModels

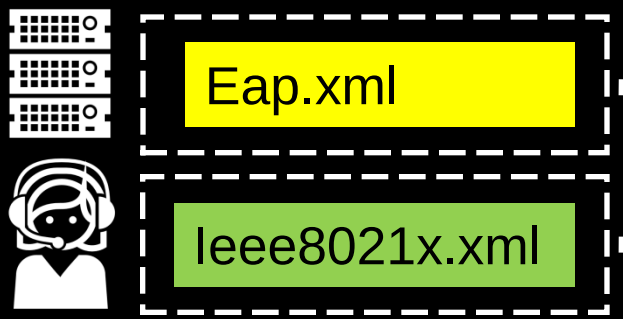


Fuzzers





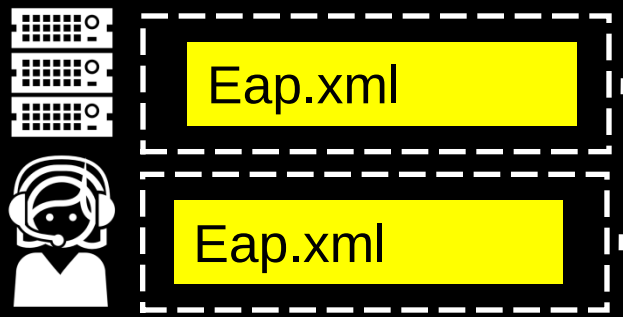
Publishers



RadiusPublisher

RawEthernetPublisher

TLS



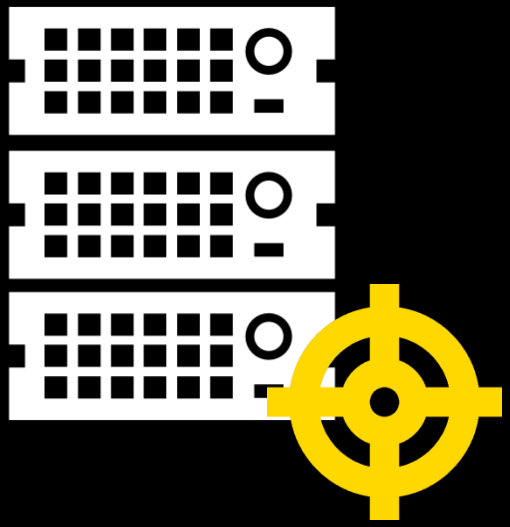
RadiusPeapPublisher

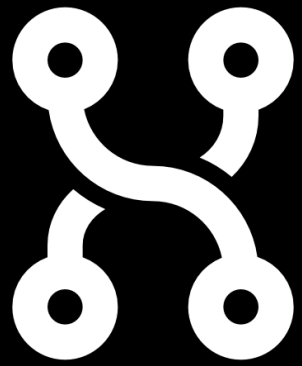
EthernetPeapPublisher

all via wired, supports all tunneled EAP Types

StringMutator.Data.cs:

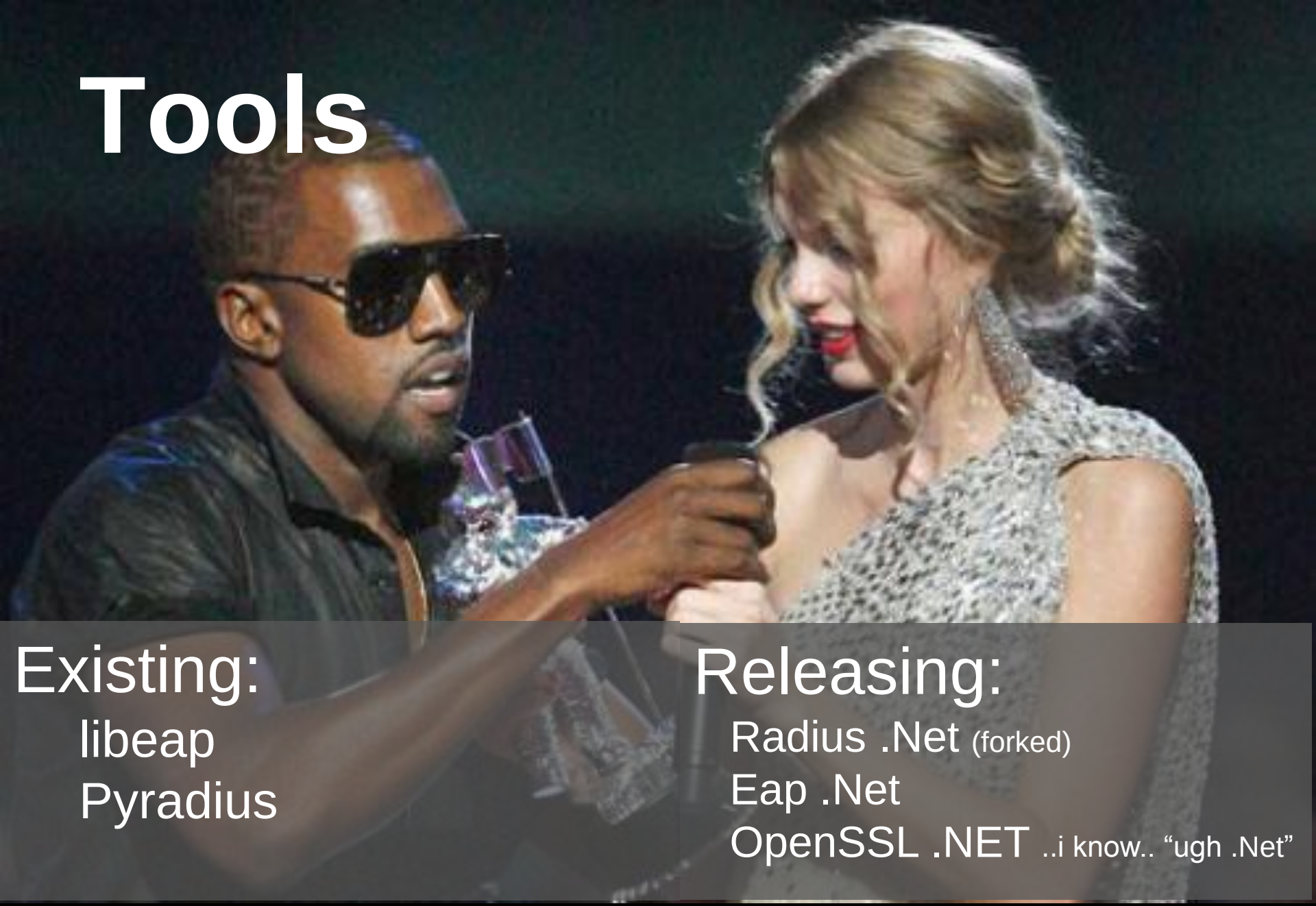
```
namespace Peach.Core.Mutators
{
    public partial class StringMutator
    {
        static readonly string[] values = new string[] {
            LDAP Injection
            XSS
            SQL Injection
            CMD Injection
            etc…

        }
}
```





RADIUS/802.1x/EAP

Tools



Existing:

- libeap
- Pyradius

Releasing:

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

Libz

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

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

Msg-Auth. (RADIUS)

Cisco: Ignores
Others: Access-Reject

Brute-Force

Or Enumeration …whatever

`eapEnum.exe`

Password

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

Usernames

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