802.1x and BEYOND!

Brad Antoniewicz
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

frankie muniz's forehead = great wifi
What if I....

Cisco ACS 4.2

ubuntu
RFC3748

EAP
Extensible Authentication Protocol
EAP

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

(Layer 2)
DALAI LAMA
RADIUS RFC2865/2869
Remote Access Dial-In User Service

DSL/Dialup

VPN
Integration

User Database
Active Directory
SecurID
LDAP
External Auth Handler

RADIUS/EAP/Types

802.1x/EAP/Types

(Protocol/Configuration/Handling issues)
Attacks
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
Impersonation

(Configuration Issue)

Attacker Controlled

Protected EAP Properties

When connecting:

- [ ] Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; \srv3.com):

Trusted Root Certification Authorities:

- [ ] AddTrust External CA Root

Brad.Antoniewicz@foundstone.com  @brad_anton  @foundstone
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
WHERE ARE THE Handler Bugs?!
Fuzz

RADIUS/EAP/802.1x
Peach Overview

DataModel

Publisher

Targets

Agent

Agent

Transformers, mutators, etc..

StateModel
DataModels

EAP
- Eap.xml
- EapFast.xml
- EapGtc.xml
- EapLeap.xml
- EapMd5.xml
- EapMschapv2.xml
- EapPeap.xml
- EapTls.xml
- EapTlv.xml

RADIUS
- Radius.xml

802.1x
- Ieee802.1x.xml

Supporting Protocols
- Tls.xml
- Mschapv2.xml

Utilities
- Utils.xml
Publishers

all via wired, supports all tunneled EAP Types
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”
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

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 not valid
- Others: Doesn’t matter

Msg-Auth. (RADIUS)
- Cisco: Ignores
- Others: Access-Reject

RadiusEapProfiler.exe
Brute-Force

Or Enumeration …whatever

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

Usernames
NPS: Eap-Resp/Identity

EAP-Type
Client Downgrade

eapEnum.exe
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
*many of the pics in this presentation were found on the internet – credit goes to images.google.com