
OPPOSING FORCE
[RedPhishing] Wi-Fi, Phishing and Red Teaming
hackinthebox
Keeping Knowledge Free for Over a Decade

/me

- Matteo Beccaro | Twitter: @_bughardy_
  - Chief Technology Officer at @_opposingforce.
  - Conference speaker & trainer.
  - Messing around with networks and protocols.
  - Often flying around the globe.
- Founder & CTO at **Opposing Force**
  - The first Italian firm specialize in offensive physical security

OPPOSING FORCE

/agenda

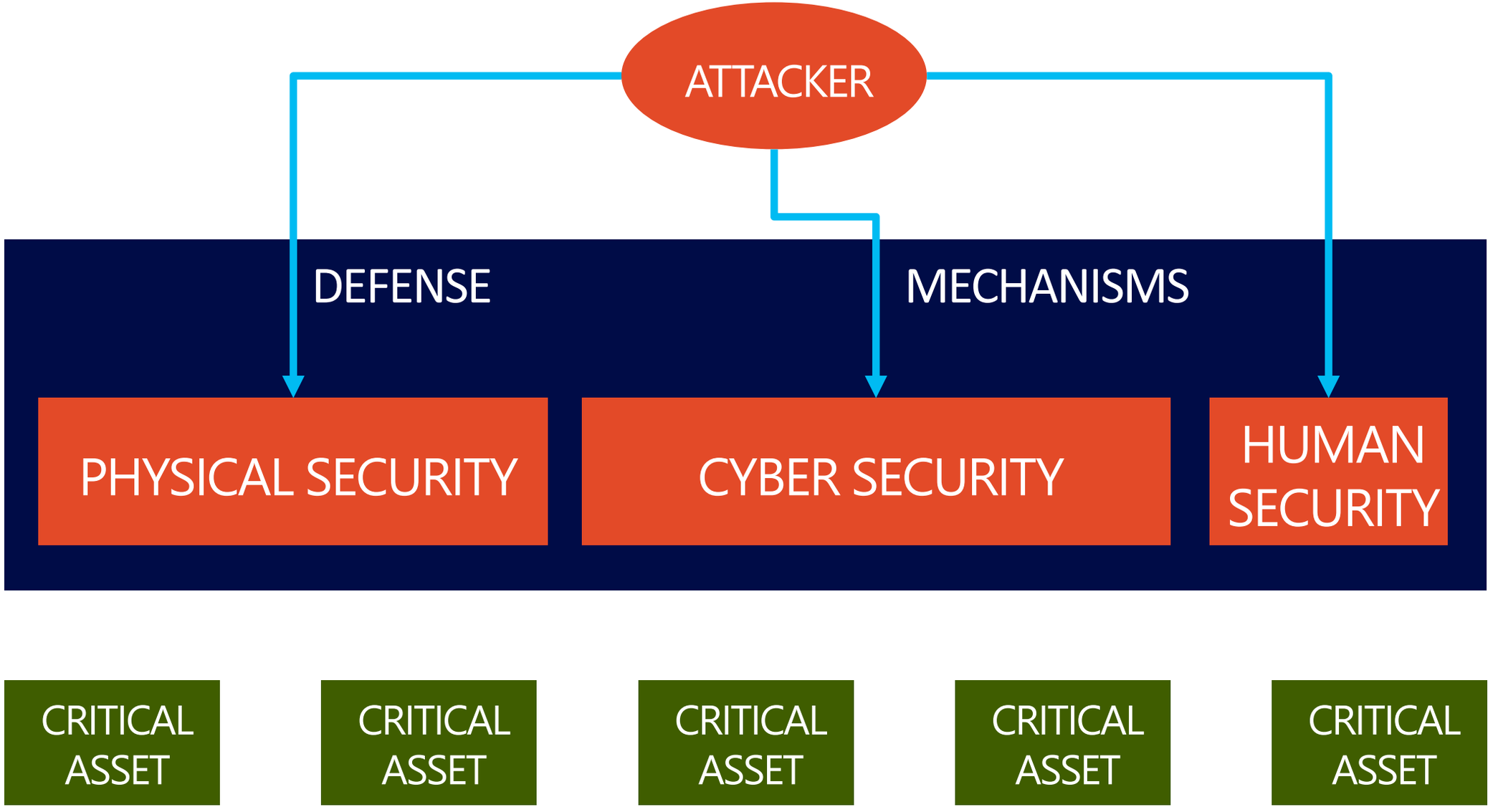
- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- Wi-Fi attacks and Phishing
- Q&A

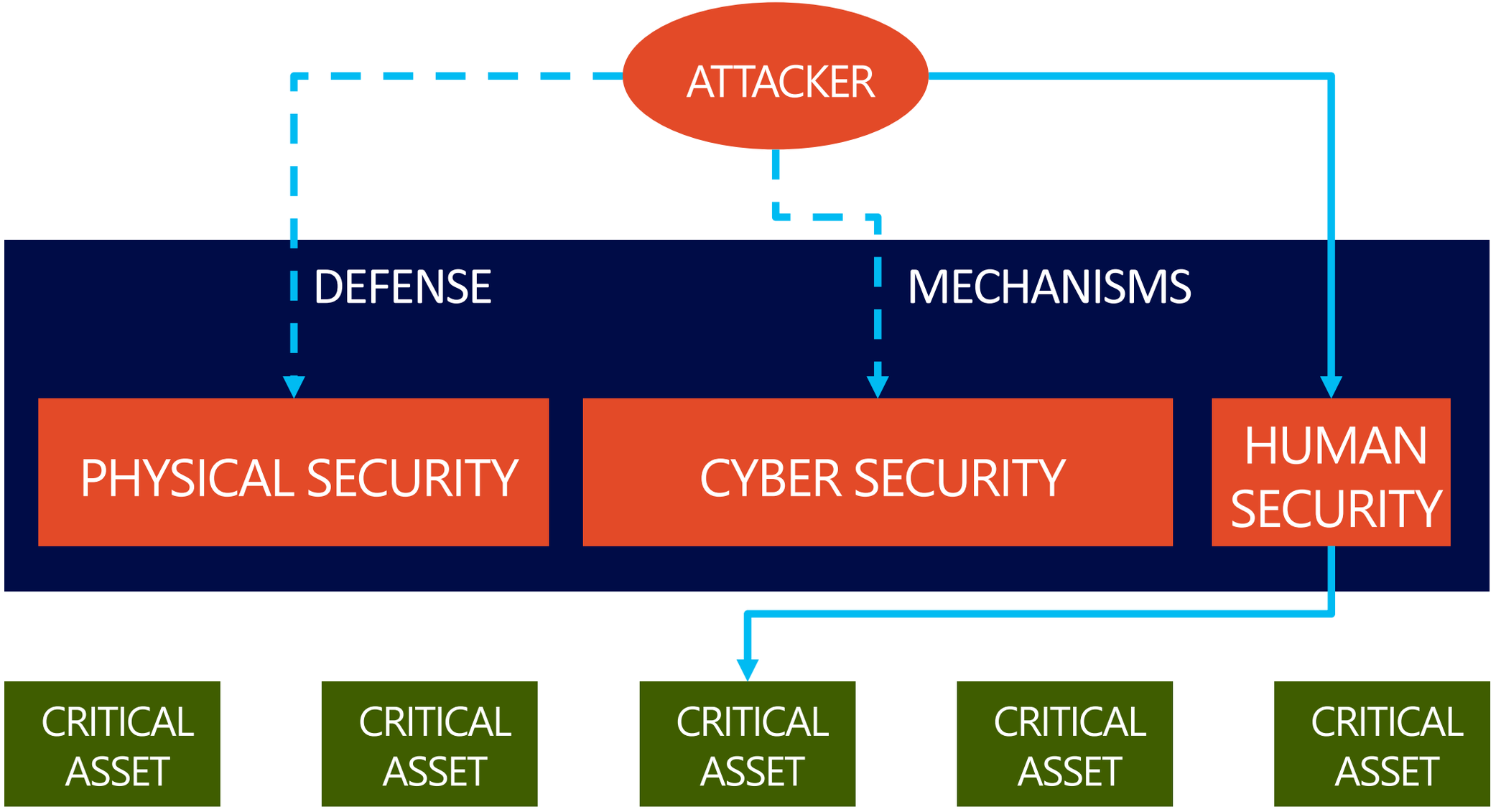
OPPOSING FORCE

/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- Wi-Fi attacks and Phishing
- Q&A

During a Red Teaming engagement the objective is **not** to stress the defence mechanisms in place but to obtain a **goal**.


ATTACKER
DEFENSE MECHANISMS
PHYSICAL SECURITY
CYBER SECURITY
HUMAN SECURITY
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET


ATTACKER
DEFENSE
MECHANISMS
PHYSICAL SECURITY
CYBER SECURITY
HUMAN SECURITY
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET
CRITICAL ASSET

Enterprise Wi-Fi is a pretty interesting point of access in business environments:

- Password is usually chosen by the employee
- Re-use credentials for OWA access, etc
- Direct access to company Intranet (Windows-based networks)
- Usually also provides internet connectivity

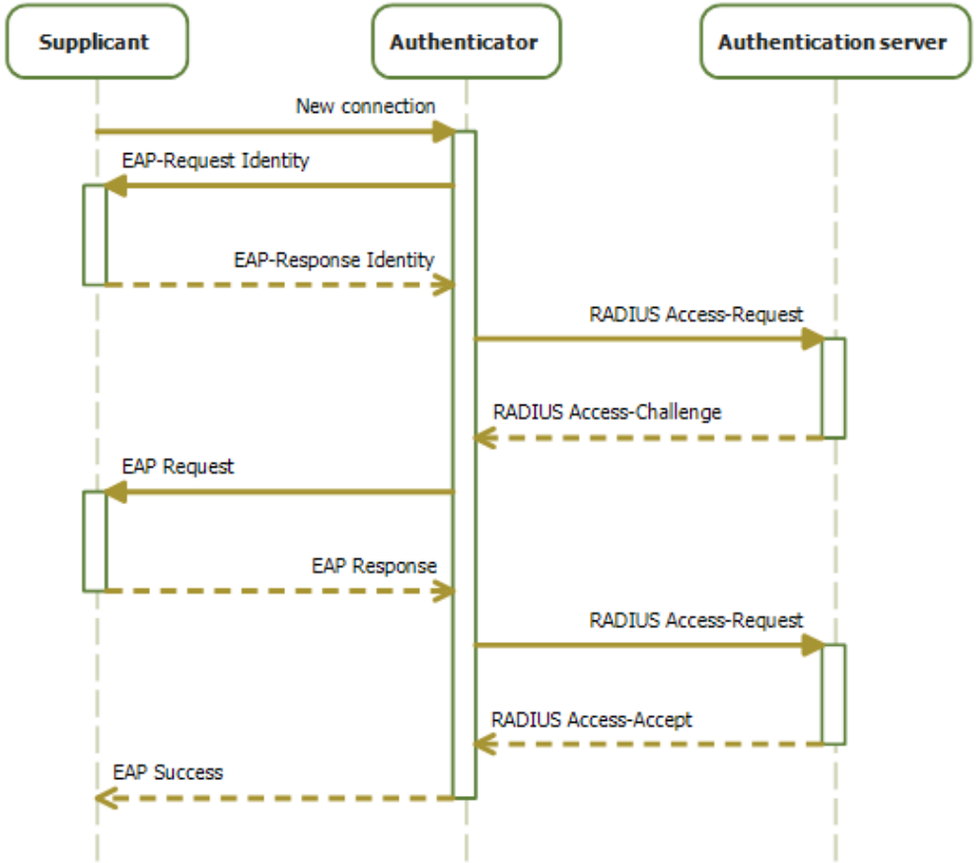
/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- Wi-Fi attacks and Phishing
- Q&A

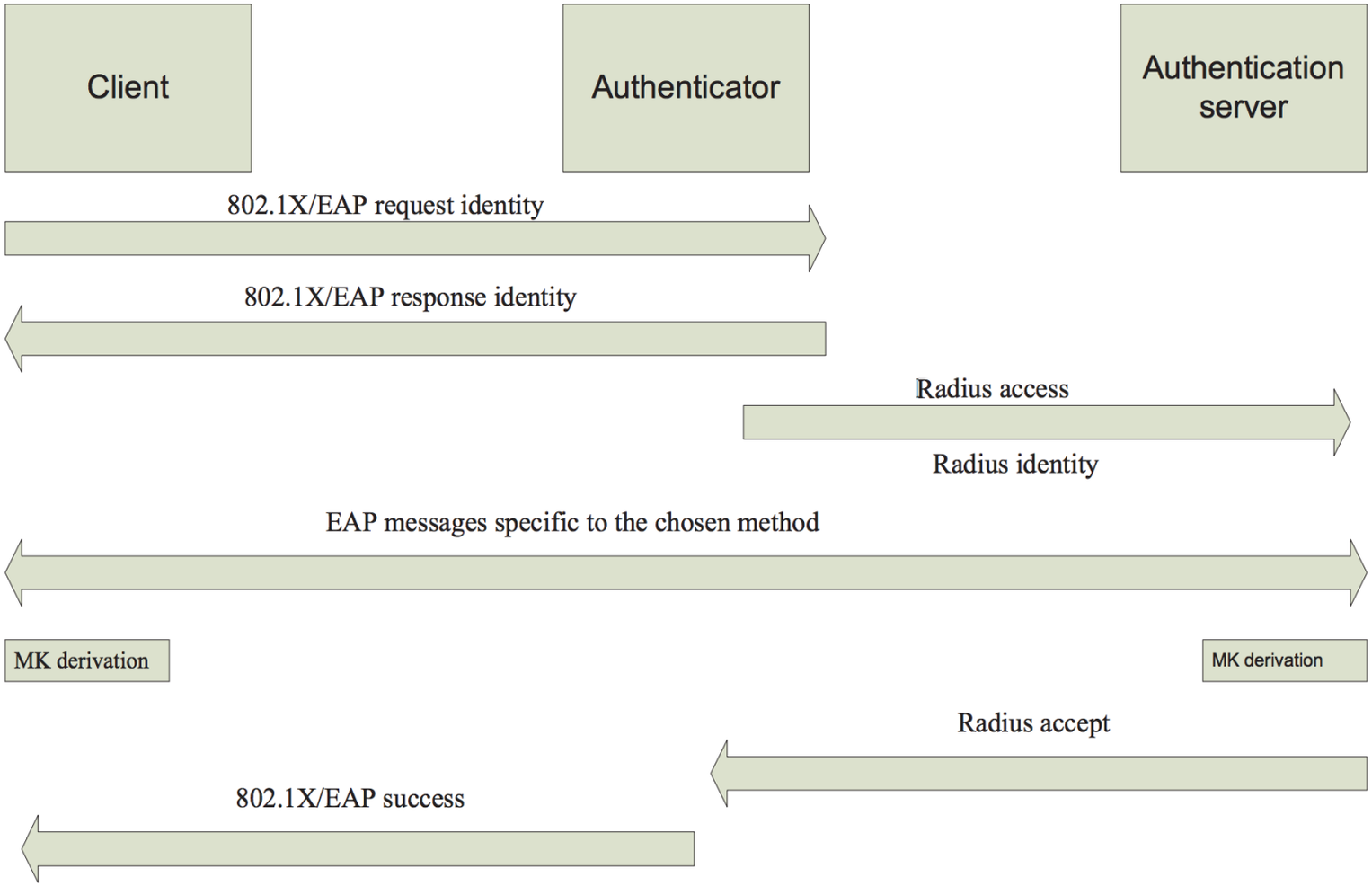
Security in WPA(2) Enterprise

/802.11x

- Version of WPA for enterprise networks
- Supports dynamic delivery of master keys
- Authentication in Enterprise mode relies on the IEEE 802.1X authentication standard
- Uses a 802.1x RADIUS authentication server to authenticate users
- Must implement a full 802.1X infrastructure to support
- FreeRadius/Hostapd: de-facto OSS servers
- 802.11x defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 known as EAP over LAN or EAPOL



OPPOSING FORCE


Client
Authenticator
Authentication server
802.1X/EAP request identity
802.1X/EAP response identity
Radius access
Radius identity
EAP messages specific to the chosen method
MK derivation
MK derivation
Radius accept
802.1X/EAP success

Extensible Authentication Protocol (EAP)

EAP Type	Mutual Auth.	Certificate Required	Key Delivery	Security	Usage
EAP-TLS	Yes	Server and Client	Yes	Highest	Medium
PEAP	Yes	Server Only	Yes	High	Highest
EAP-TTLS	Yes	Server Only	Yes	High	High
LEAP	Yes	No	Yes	Low	Low
EAP-MD5	No	No	No	Lowest	Lowest
…	…	…	…	…	…

PEAP stands for Protected Extensible Authentication Protocol

PEAP uses password-based authentication for device authentication and certificate-based authentication to verify server identities

PEAP is the most popular enterprise Wi-Fi security mechanism used

- Typical usage (in order of popularity)
  - **PEAPv0** with EAP-MSCHAPv2
    - Native support on Windows
  - **PEAPv1** with EAP-GTC
  - **PEAPv0/1** with EAP-SIM (Cisco)
  - **PEAP-EAP-TLS**

/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- WPA(2) Enterprise Edition
- Wi-Fi attacks and Phishing
- Q&A

OPPOSING FORCE

/802.11x-hacking

A brief introduction to hacking Wi-Fi Enterprise PEAP networks

OPPOSING FORCE

Hostapd-WPE is a patch written for Hostapd that transform it into an attack server.

WPE stands for **Wireless Pwnage Edition**.

Many different benefit compared to Hostapd:

- Automates some manual configurations
- Adds credential logging for multiple EAP types
- Etc

/802.11x-hacking

- PEAP and EAP-TLS use server-side certificates
- High-level security but fake certificates can be created
  - Often users will be prompted to accept the certificate

Attacker setup a new AP with Hostapd-WPE server

- Client connects and accepts fake certificate
- Malicious Radius server logs authentication details over MSCHAPv2 in the tunnel
- Attacker perform bruteforce/dictionary cracking attack to recover password

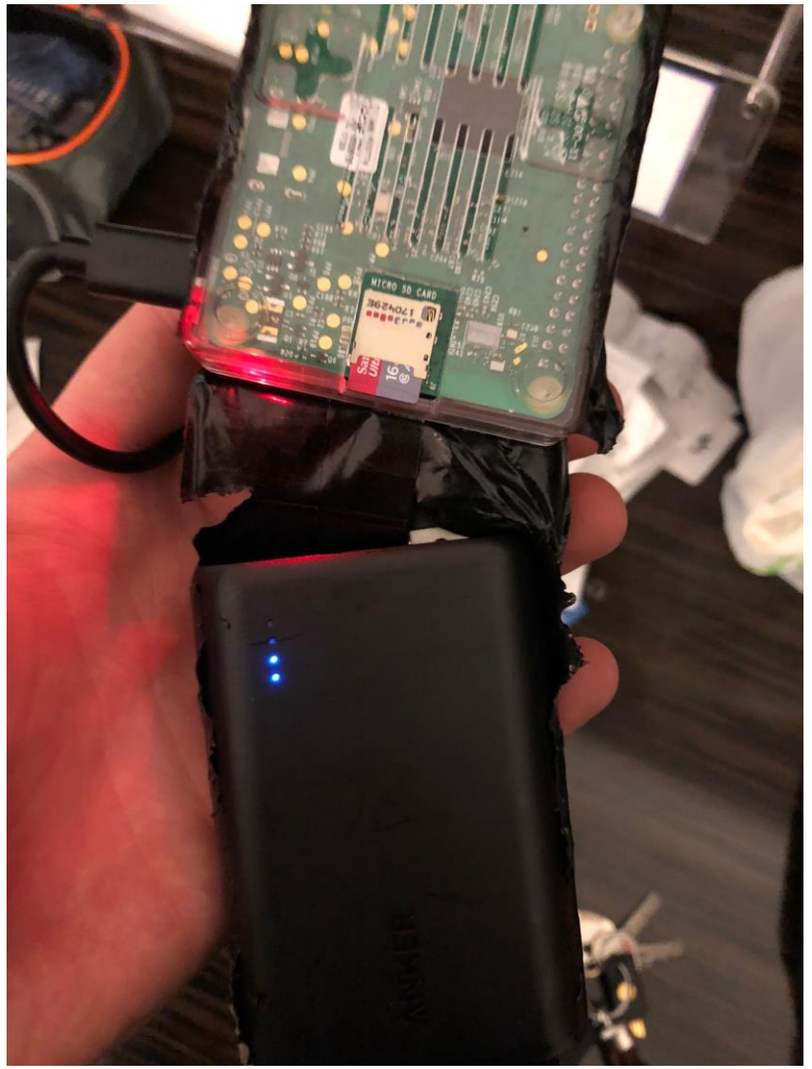
/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- Wi-Fi attacks and Phishing
- Q&A

/more-tools

Basic arsenal for this attacks is pretty straightforward:

- Dropbox machine (RPi)
- External battery
- External Wi-Fi antenna for longer range
- (optional) Cellular dongle to retrieve data remotely
- (optional) 3D printer to create a proper stealth box



OPPOSING FORCE

/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- WPA(2) Enterprise Edition
- Wi-Fi attacks and Phishing
- Q&A

OPPOSING FORCE

Wi-Fi and Phishing

During a Red Teaming engagement we faced a new issue: the victim **did not** get prompt for accepting our fake certificate.

Further analysis revealed that:

Server certificate requirements

You can configure clients to validate server certificates by using the **Validate server certificate** option on the **Authentication** tab in the Network Connection properties. When a client uses PEAP-EAP-MS-Challenge Handshake Authentication Protocol (CHAP) version 2 authentication, PEAP with EAP-TLS authentication, or EAP-TLS authentication, the client accepts the server's certificate when the certificate meets the following requirements:

- The computer certificate on the server chains to one of the following:
  - A trusted Microsoft root CA.
  - A Microsoft stand-alone root or third-party root CA in an Active Directory domain that has an NTAuthCertificates store that contains the published root certificate.For more information about how to import third-party CA certificates, click the following article number to view the article in the Microsoft Knowledge Base:

    295663 How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store

- The IAS or the VPN server computer certificate is configured with the Server Authentication purpose. The object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1.
- The computer certificate does not fail any one of the checks that are performed by the CryptoAPI certificate store, and it does not fail any one of the requirements in the remote access policy.
- The name in the Subject line of the server certificate matches the name that is configured on the client for the connection.
- For wireless clients, the Subject Alternative Name (SubjectAltName) extension contains the server's fully qualified domain name (FQDN).
- If the client is configured to trust a server certificate with a specific name, the user is prompted to make a decision about trusting a certificate with a different name. If the user rejects the certificate, authentication fails. If the user accepts the certificate, the certificate is added to the local computer trusted root certificate store.

Note With PEAP or with EAP-TLS authentication, servers display a list of all the installed certificates in the Certificates snap-in. However, the certificates that contain the Server Authentication purpose in EKU extensions are not displayed.

https://support.microsoft.com/en-gb/help/814394/certificate-requirements-when-you-use-eap-tls-or-peap-with-eap-tls

Getting a valid Microsoft Root CA certificate

Further analysis revealed that:

/redphishing

218	Government of Venezuela, Superintendencia de Se	Autoridad de Certificacion Raiz de la Republica Bol	DD83C519D43481FAD4C22C03D702FE9F3B22F51	0E88EB6EA256E19EF8D3ABD61A24D38DBAD632816DD957294427E4724D81A38	NotBefore	28/11/2017
219	Halcom D.D.	Halcom CA FO	0409565B77DA582E6495AC0060A72354E64B0192	5A1B5D6BC65523B40A6DEFFA45B48E4288AE8DD86DD70A5B858D4A5AFFC94F	NotBefore	26/09/2017
220	Halcom D.D.	Halcom CA PO 2	7FBB6ACD7E0AB438DAAF6FD50210D007C6C082	FE7114D07A147759891FF37B4F53EB43568296BC3BF89BC12CAFB186985EF28D	NotBefore	26/09/2017
221	Halcom D.D.	Halcom Root CA	535B001672ABBF7B6CC25405AE4D24FE033FD1C	8B3FDB151AF759C566143E07C950EDE4F9E8C7CF808453D33BCB78E52A400AF9	Active	
222	Halcom D.D.	Halcom Root Certificate Authority	23D731FEDC5C8BB97DE6DC8E13B411BD4F24004	D7BA3F4FF8AD05633451470DDA3378A3491B90005E5C687D2B68D53647CFDDE	Active	
223	HARICA	Hellenic Academic and Research Institutions ECC R	9FF1718D92D59AF37D7497B4BC6F84680BBAB66	44B545AA8A25E65A73CA15DC27FC36D24C1CB9953A066539B11582DC487B483	Active	
224	HARICA	Hellenic Academic and Research Institutions RootC	FE45659B79035B98A161B5512EACDA580948224D	BC104F15A48BE709DCA542A7E1D4B9DF6F054527E802EAA92D595444258AFE7	Active	
225	HARICA	Hellenic Academic and Research Institutions RootC	010C0695A6981914FFBF5FC6B0B695EA29E912A6	A040929A02CE53B4ACF4F2FFC6981CE4496F755E6D45FE0B2A692BCD52523F36	Active	
226	I.CA První Certifika?ní Autorita, A.S.	I.CA – Qualified Certification Authority	D2441AA8C203AECAA96E501F124D52B68FE4C37	C0C05A8D8DA55EAF27AA9B910B0A6EF0D8BBDED346928DB872E182C2073E98	NotBefore	26/09/2017
227	I.CA První Certifika?ní Autorita, A.S.	I.CA – Standard Certification Authority	90DECE77F8C825340E62EBD635E1BE20CF7327DD	6468BF8CF3CF688EBB2A6841BD70E97B5229B49DF8690D7B74193E9CE3886141	NotBefore	26/09/2017
228	I.CA První Certifika?ní Autorita, A.S.	I.CA První certifikační autorita a.s.	64902AD7277AF3E32CD8CC1DC79DE1FD7F8069E	1AA980C8C0D316F25029978982F033CBB3A3F4188D669F2DE6A8D84EE00A157	Disable	24/04/2018
229	I.CA První Certifika?ní Autorita, A.S.	I.CA První certifikační autorita a.s.	AB16DD144ECDC0FC4BAAB62ECF0408896FDE52E	77A03F69E4F3955589ACACA06F6773A0D98D16DEA05C6D94EE3EF6FB2BEB760	Disable	24/04/2018
230	I.CA První Certifika?ní Autorita, A.S.	I.CA Root CA/RSA	9B0959898154081BF6A90E9B9E58A4690C9BA104	D3D607A9FF24A19523B6DA9D2C649446F8788CB96D9FD130972E120C1367773C	Active	
231	IdenTrust	DST Root CA X3	DAC9024F54D8F6DF94935FB1732638CA6AD77C1	0687260331A72403D909F105E69BCF0D32E1BD2493FFC6D9206D11BCD6770739	Active	
232	IdenTrust	IdenTrust Commercial Root CA 1	DF717EAA4AD94EC9558499602D48DE5FBCF03A2	5D56499BE4D2E08BCFCAD08A3E38723D50503BDE706948E42F55603019E528AE	Active	
233	IdenTrust	IdenTrust Public Sector Root CA 1	BA29416077983FF4F3EFF231053B2EEA6D4D45FD	30D0895A9A448A262091635522D1F52010B5867ACAE12C78EF958FD4F4389F2F	Active	
234	Image-X Enterprises Inc	ESIGNIT.ORG	9F8DE799CF8764ED2466990564041B194919EDE8	C665175BD60ED70A5EEA3344CBE5D1A6936F79BC27A8384E4C734200417C279F	Active	
235	Inera AB (SITHS)	Inera AB	585F7875BEE7433EB079EAAB7D05BB0F7AF2BCC	FC50B26BDC4A8FDF1344CC80157AE13AC671E2706FACFC0605FE34E249EB72D	Active	
236	Inera AB (SITHS)	SITHS CA	16D86635AF1341CD34799445EB603E273702965D	B2F3C4216AF7AFF72462466DC13CD2810DB8EED853EABB9A063A608EFC18FBE	Disable	26/09/2016
237	Internet Security Research Group	ISRG Root X1	CABD2A79A1076A31F21D253635CB039D4329A5E	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C	Active	31/07/2018
238	IZENPE S.A.	IZENPE S.A.	4A3F8D6BDC0E1ECFCD72E377DEF2D7FF92C19BC	B0877AEE2D39274DF831F66FDEEB7717557C258FC9EB55231A9F8A647A75433F	Disable	24/04/2018
239	IZENPE S.A.	Izenpe.com	30779E9315022E94856A3FF8BCF815B082F9AEFD	23804203CA45D8CDE716B8C13BF3B448457FA06CC10250997FA01458317C41E5	Active	
240	Japan Local Authority Information Systems (J-LIS)	Application CA G3 Root	6F3884568E99C8C6AC0E5DDE2DB202DD002E366	54B4FC43D44AA4CA9FC03CA7E9949FBAE267A064D02DA21852412A381B5D15	NotBefore	29/03/2018
241	Japan Local Authority Information Systems (J-LIS)	Application CA G4 Root	21DACE4C2C34E66468EE06314DB055A0A89D4C1	D1A0319098034E3AEC729A0B5C3111229D9D26E3E623E8C5E6843FA06EE8E2E4	Active	27/06/2017
242	Japan Local Authority Information Systems (J-LIS)	Japan Local Government PKI Application CA	968338F113E36A7BABDD08F7776391A68736582E	06DB3AF2DB7BAEE00C03B9578288BBDE541D906EB0069327413295FFB486008E	Disable	24/04/2018
243	Korea Information Security Agency (KISA)	KISA RootCA 1	027268293E5F5D17AAA4B3C3E6361E1F92575EAA	6FDB3F76C8B801A75338D8A50A7C02879F6198B57E594D318D3832900FEDCD7	Active	
244	Krajowa Izba Rozliczeniowa S.A. (KIR)	SZAFIR ROOT CA	D3EEFBCBBCF49867838626E23BB59CA01E305DB	FABCF5197CDD7F458AC33832D3284021DB2425FD6BEA7A2E69B7486E8F51F9C	Active	09/30/2017
245	Krajowa Izba Rozliczeniowa S.A. (KIR)	SZAFIR ROOT CA2	E252FA953FEDDB2460BD6E28F39CCCCF5EB33FD	A1339D33281A0B56E557D3D32B1CE7F9367EB094BD5FA72A7E5004C8DED7CAF	Active	
246	LAWtrust	LAWtrust Root Certification Authority 2048	335A7FF00927CF2DF278E2C9192F7A4D5534F80C	9B14E8F5F6EA167666E76DCD6BECC190861D5E8970B99A9470F0231236049704	Active	
247	LuxTrust	LuxTrust Global Root 2	1E0E56190AD18B2598B20444FF668A0417995F3F	54455F7129C20B1447C418F997168F24C58FC5023BF5DA5BE2EB6E1DD8902ED5	Active	
248	LuxTrust	LuxTrust Global Root CA	C93C34EA90D9130C0F03004B98BD8B3570915611	A1B2DBEB64E706C6169E3C4118B23BAA09018A8427666D8BF0E28891EC051950	Active	
249	Macao Post	Macao Post eSign Trust	06143151E02B45DDBADD5D8E56530DAAE328CF	6EA1DB6719D6041A06FC0898E5B3CF349A8FA8ECEE85EDB005965628F617F7C8	Active	
250	Microsec e-Szignó CA	MicroSec e-Szigno Root CA	2388C9D371CC9E963DFF7D3CA7CEFCD625EC190	327A3D761ABADEA034EB998406275CB1A4776EFDAE2FDF6D0168EA1C4F5567	Disable	24/04/2018
251	Microsec e-Szignó CA	MicroSec e-Szigno Root CA 2009	89DF74FE5CF40F4A80F9E3377D54DA91E101318E	3C5F81FEA5FAB82C64BFA2EAECAFCDE8E077FC8620A7CAE537163DF36EDBF37	Active	
252	Microsoft Corporation	Microsoft ECC Product Root Certificate Authority 2	06F1AA330B927B753A40E68CDF22E34BCBEF3352	CACA93B9D23D2B6FA76E8B8471931E0DF3EC6F63AF3CDBB936C41954A187232	Active	26/06/2018
253	Microsoft Corporation	Microsoft Root Authority	A43489159A520F0D93D032CCAF37E7FE20A8B419	F38406E540D7A9D90CB4A9479299640FFB6DF9E224ECC7A01C0D9558D8DAD77	Disable	30/01/2018

https://gallery.technet.microsoft.com/Trusted-Root-Program-32d53c74

OPPOSING FORCE

Wrapping it up

- Buy and prepare a phishing domain

e.g. wifi-auth.opfor.it

- Obtain a valid certificate using letsencrypt.org

```
root@pwnmachine:~# certbot --apache -d wifi-auth.opfor.it --register-unsafely-without-email
Saving debug log to /var/log/letsencrypt/letsencrypt.log

[...]
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Congratulations! You have successfully enabled https://wifi-auth.opfor.it
```

- Retrive the privkey.pem and fullchain.pem files

```
root@dropbox:~#scp pwnmachine:/etc/letsencrypt/live/wifi-auth.opfor.it/*.pem .
```

Wrapping it up

- Configure hostapd-wpe to use this certificate

```
server_cert=../../hostapd-wpe/certs/fullchain.pem
private_key=../../hostapd-wpe/certs/privkey.pem
```

- Place your dropbox and enjoy

```
mschapv2: Wed Aug 29 20:46:14 2018
        username:    matteo.beccaro
        challenge:   1b:43:da:2a:16:51:e1:e7
        response:    fb:86:6b:18:c1:90:fc:a0:c3:5c:4b:a5:1d:ae:c9:43:a6:7d:37:23:ce:c1:4a:af
        jtr NETNTLM: matteo.beccaro:$NETNTLM$1b43da2a1651e1e7$fb866b18c190fca0c35c4ba51daec943a67d3723cec14aaf
```

What’s Next?

We’re developing a tool to automatically get a new domain, obtain a valid certificate through letsencrypt *certbot* and set up a fake AP with such valid certificate.

Execute on your dropbox and deploy!

/agenda

- Introduction
- WPA(2) Enterprise Edition
- 101 introduction to Wi-Fi hacking
- Wi-Fi and Red Teaming
  - Tools of the trade
- WPA(2) Enterprise Edition
- Wi-Fi attacks and Phishing
- Q&A

OPPOSING FORCE

Any question?

Don’t be shy..

Opposing Force

Thank you

engage@opposingforce.it | www.opposingoforce.it | @_opposingforce