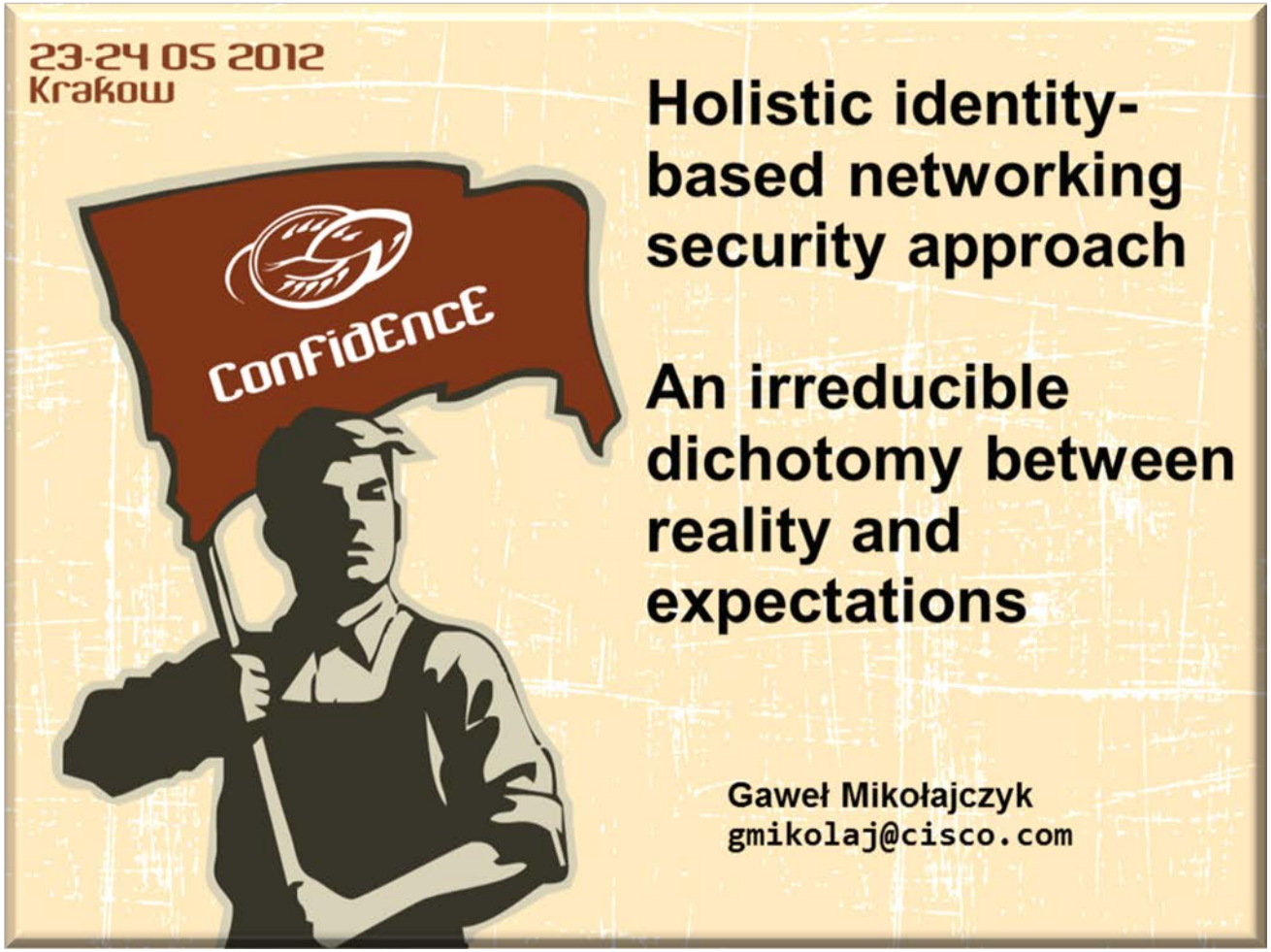
Network Security Treasures

Gaweł Mikołajczyk
gmikolaj@cisco.com

Progress Bar

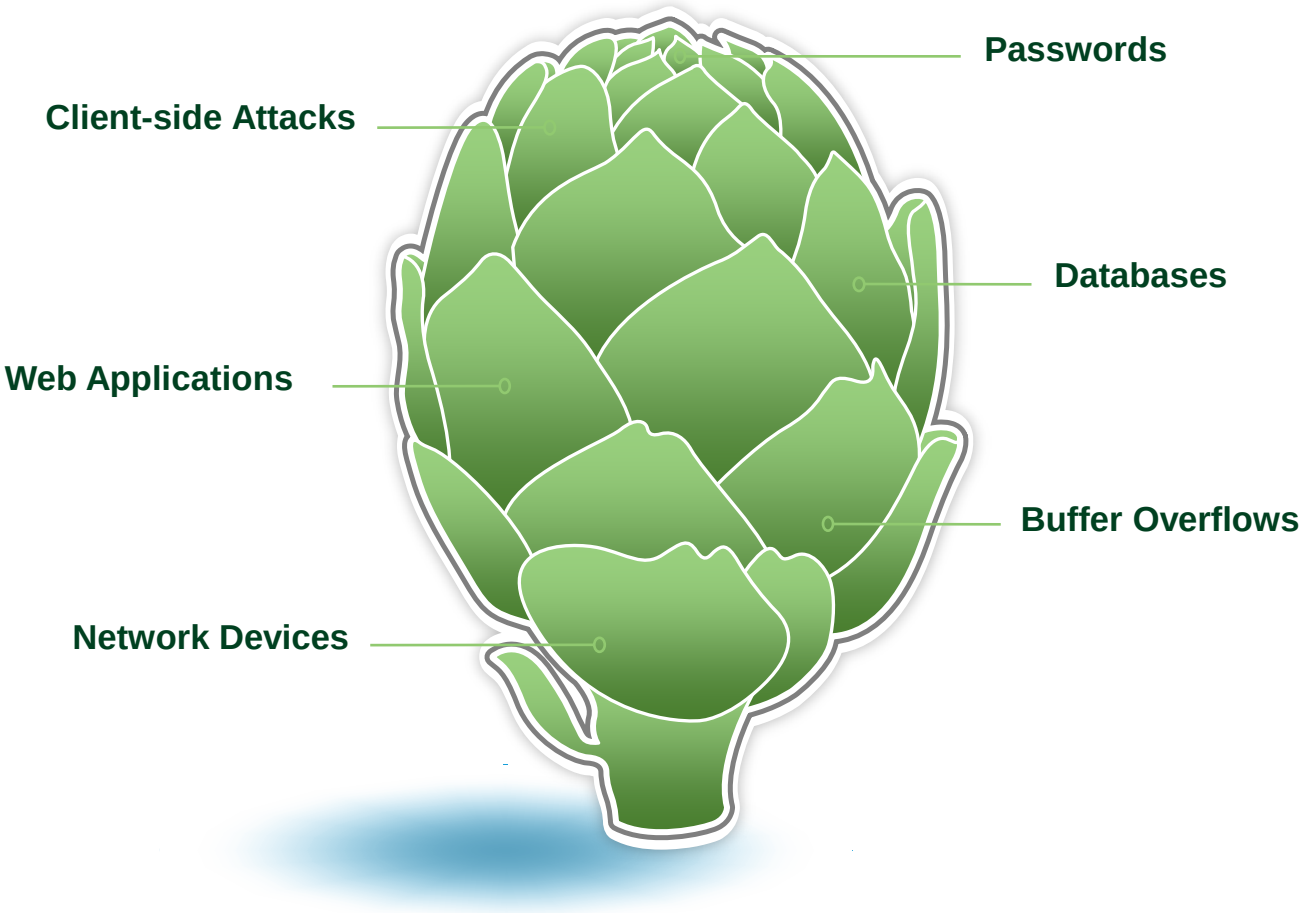
The saga continues!



http://www.youtube.com/watch?v=EBi1xlMg5XE

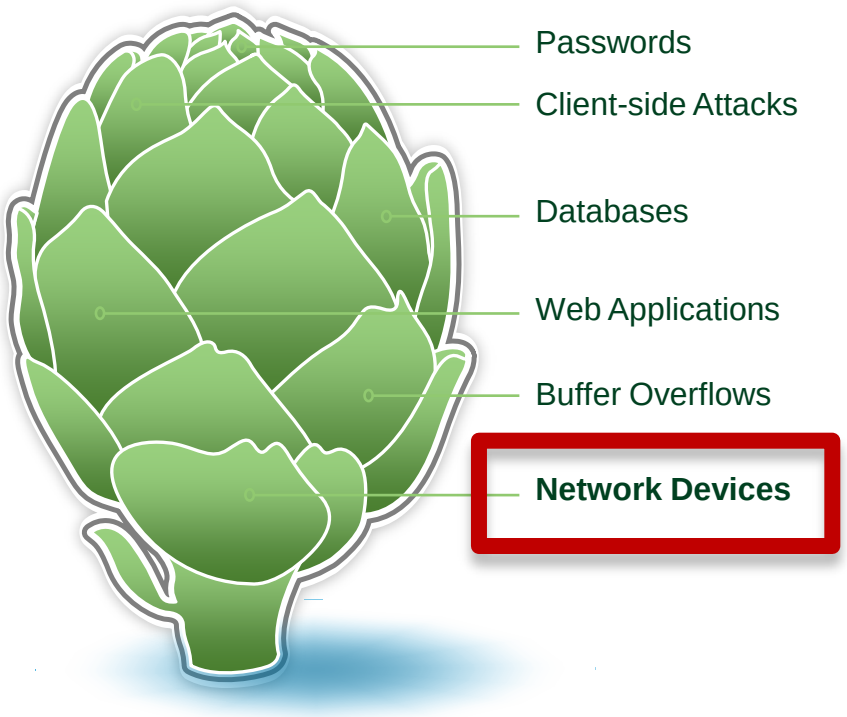
Progress Bar

The Artichoke of an Attack



Why Not an Onion?

- The typical “Onion Layer” of security has worked for a quite some time and should not be thrown out yet
- Attacks have always been targeted to where the data is
- Attackers just ride the leaves
- Blurred Perimeter, SaaS, Clouds … this is a different world



Security is made up of layers but these layers don’t always overlap!

The Artichoke resemblance…

- The heart is where the data sits
- Each leaf provides a layer of protection
- …but also a perfect avenue to attack
- **Not every leaf needs to be removed** in order to get at the heart of the artichoke
- All I need is a little taste

Artichokishly Delicious Example

- A server is hosting your company's blog
- It's behind firewalls, intrusion prevention modules, tiered infrastructure, secured servers etc.
- An SQL Injection vulnerability is found in Wordpress, the software running the blog
- SQL Injection leaf bypasses other leaves and executes commands directly on the database tier
- When the attacker is inside the database tier, **what else can they see**?

Stories from the Production

- Total Number of IP's in sample data: 6,216
- 9 Hosts vulnerable to MS06-040 (Netapi)
- 16 Hosts vulnerable to MS04-012 (DCOM)
- 8 Hosts vulnerable to SADMIN Overflow
- 57 Hosts vulnerable to MS05-047 (PNP)
- 49 Hosts vulnerable to MS05-039 (PNP)!

May not seem like large numbers, but **it only takes one hos**t to give up the keys to the kingdom!

Network-Based Attacks

- 5 IOS HTTP Auth bypasses
- 16 Default passwords
- 160 Weak or easily guessed passwords
- 230 Weak SNMP community strings

  Why is this bad?

Man in the Middle

- ARP Poisoning/Spoofing
  - The basis of most Network-focused MITM attacks
  - Focused on a Layer 2 broadcast domain
  - Not impossible to protect
- Packet Interception and Misdirection
  - Cleartext protocol sniffing
  - Encrypted protocol negotiation interception
  - Secure SHell, Secure Socket Layer, etc.

BRKSEC-2202 - Understanding and Preventing Layer 2 Attacks in IPv4 and IPv6 networks (2013 London)
https://www.ciscolive365.com/connect/sessionDetail.ww?SESSION_ID=3001&backBtn=true

- Applies for IPv4 and IPv6 yet different in details.

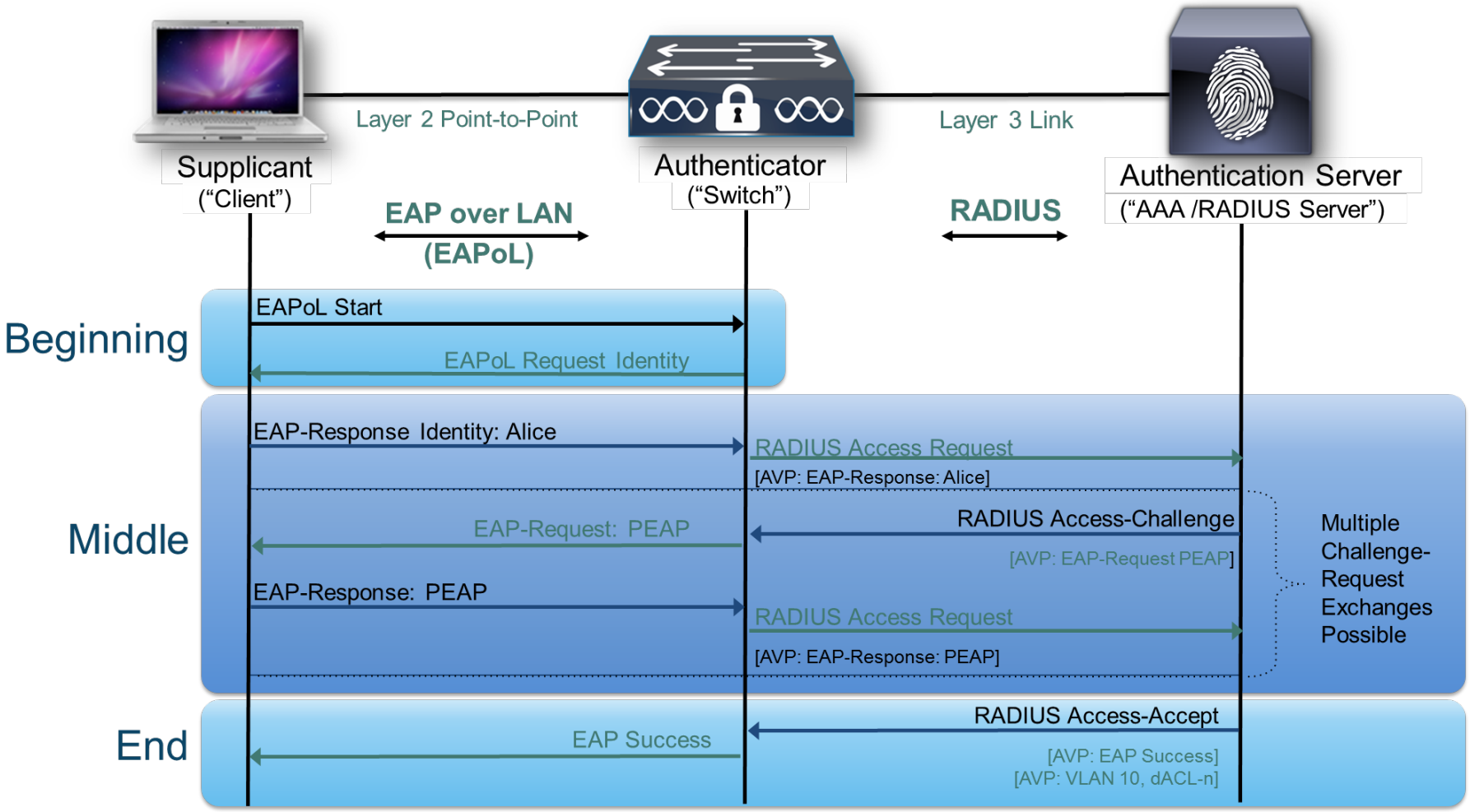
CONFidence 2013 - IPv6 insecurities at First Hop
http://www.data.proidea.org.pl/confidence/10edycja/materialy/prezentacje/GawelMikolajczyk_IPv6.pdf

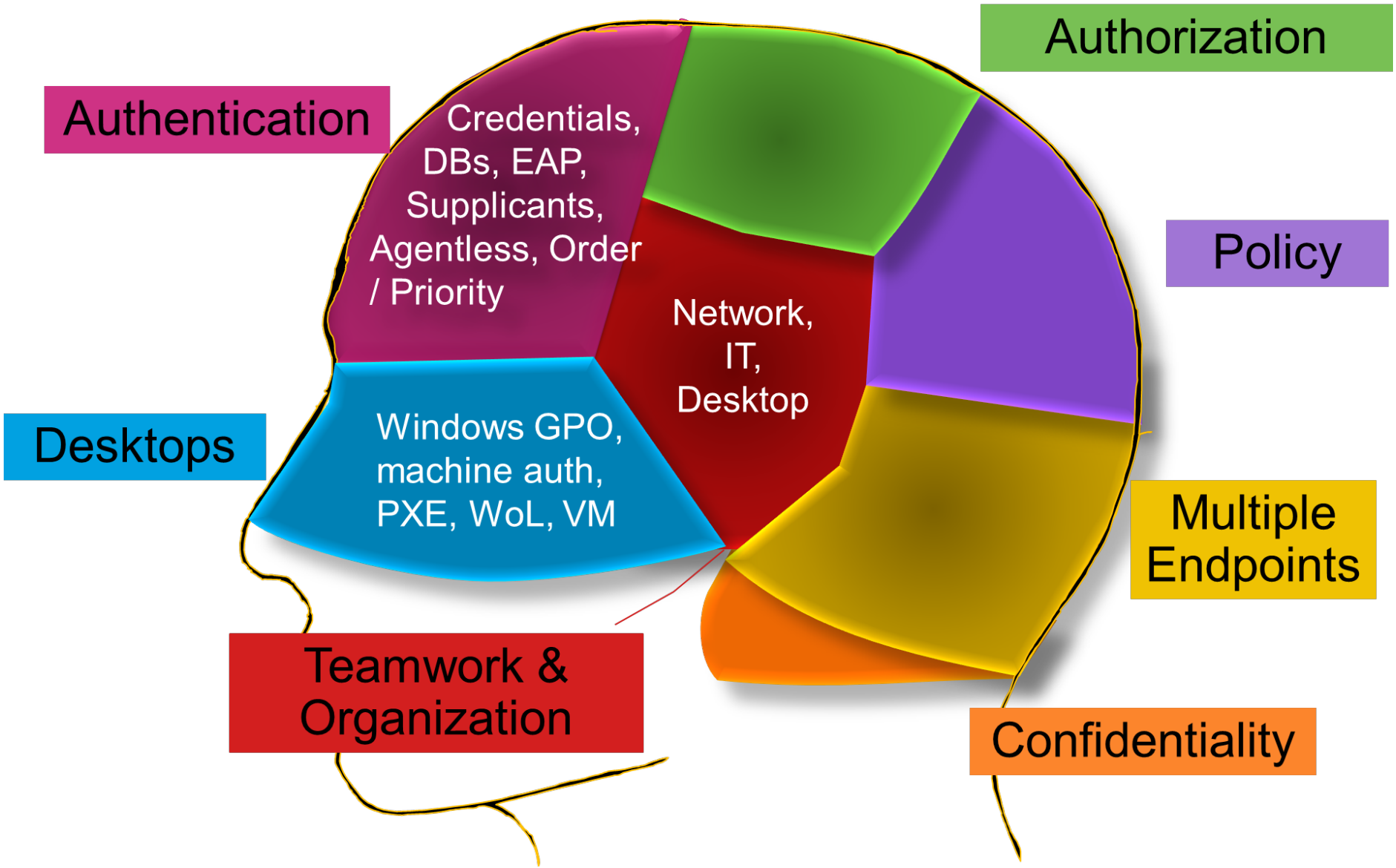
Progress Bar

CONFIDENCE
2013

EAP IN CHAINS

IEEE 802.1X Provides Port-Based Access Control Using Authentication





Identifying the Machine AND the User

The next chapter of authentication: EAP-Chaining

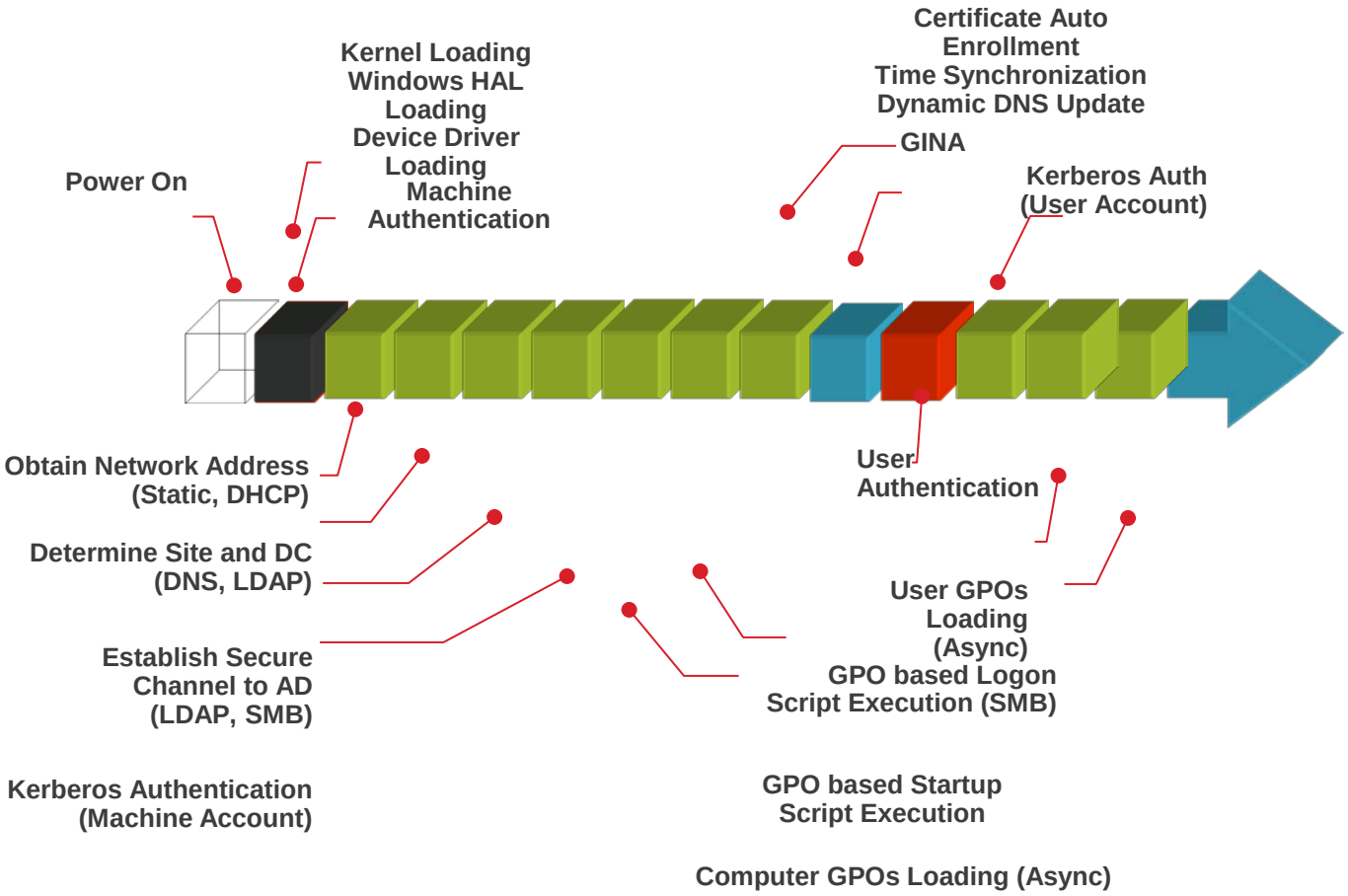
- IETF EAP Method Update (EMU) working group is in process of standardizing on **Tunneled EAP (TEAP).**

  Next-Generation EAP method that provides all benefits of current EAP Types.

  Also provides EAP-Chaining.

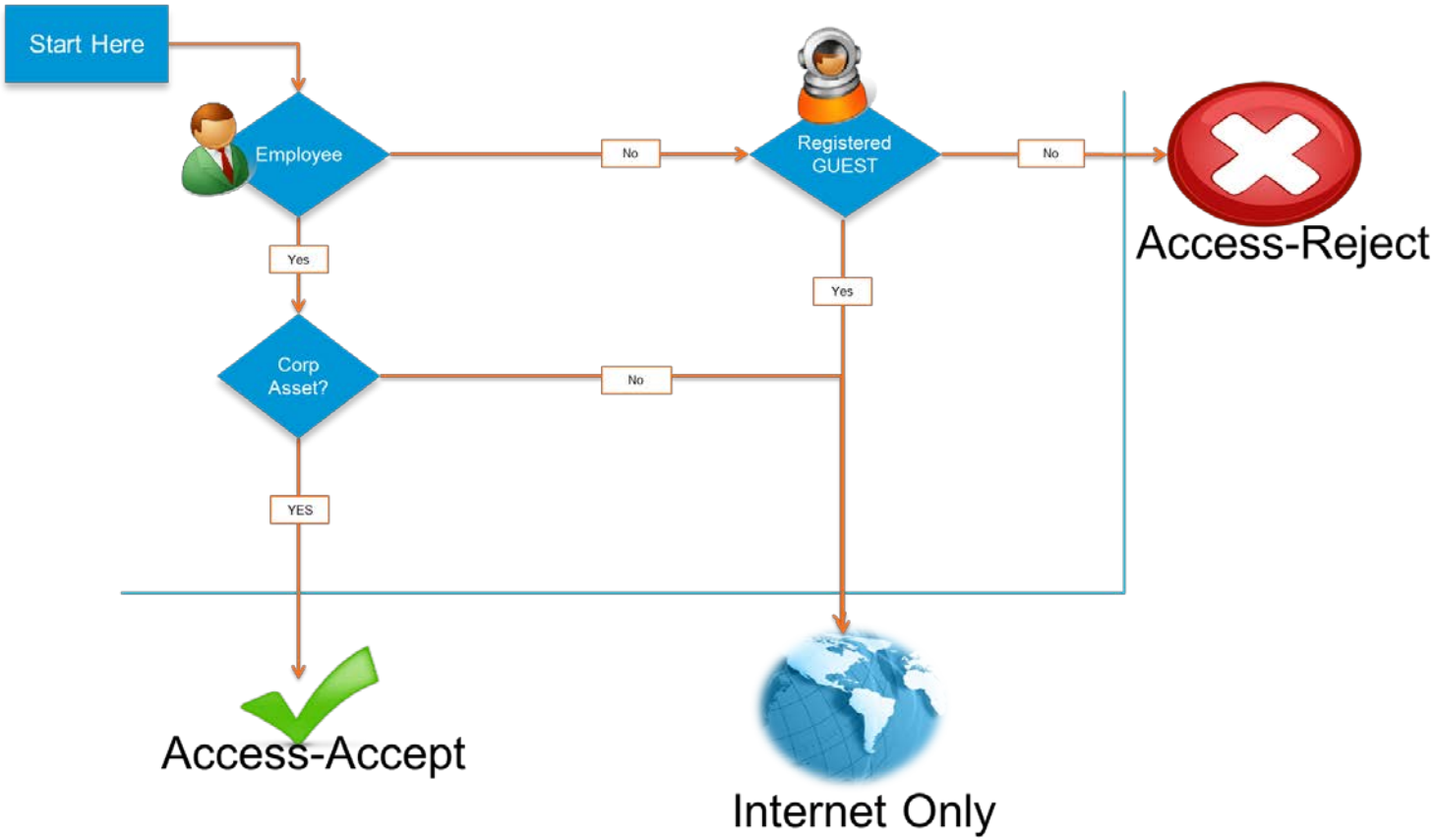
  http://tools.ietf.org/html/draft-ietf-emu-eap-tunnel-method-06

Machine and User Authentication complexity



Why Identify BOTH Machine and User?

The need: provide differentiated access for IT-managed systems



User and Machine Policies

I Know Who You Are, But are You Logging In from a Managed Device?

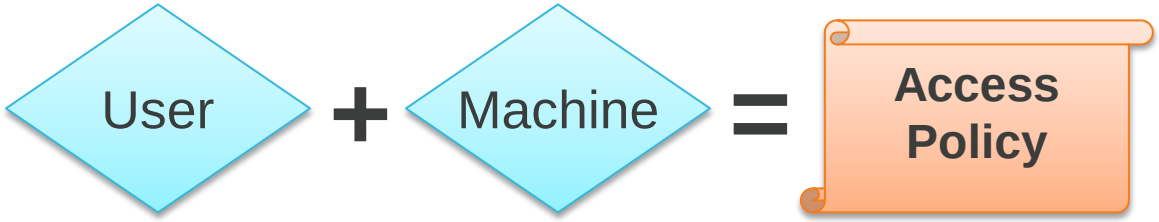
- User identity …
  - Username/password credentials (802.1X or WebAuth)
  - User certificate (802.1X)

- Machine "identity" …
  - MAC Address?
  - Machine certificate?

How credible is the information used?

Fidelity Meter

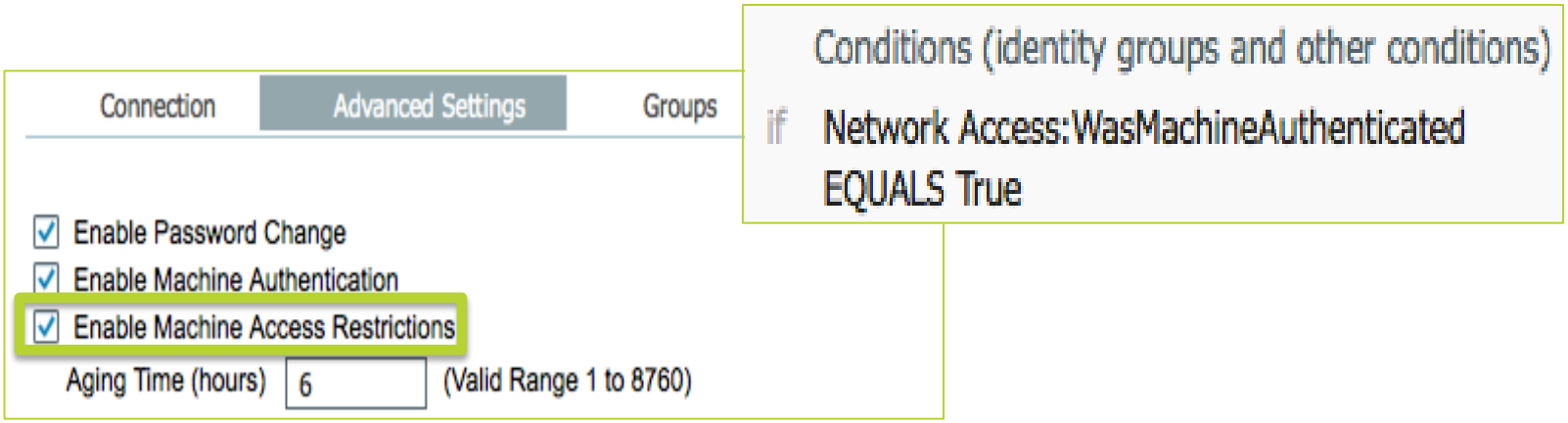
- How do I tie the two together in a single policy?



How to Enforce Machine and User Authentication

Option 1: Machine Access Restrictions (MAR)

- The RADIUS attribute [31] Calling-Station-Id is a must from the NAD.
- The machine authenticates successfully and RADIUS Server caches its MAC address in the so called MAR cache.
- For user authentication to pass, on top of valid user credentials/certificate, the RADIUS attribute [31] Calling-Station-Id in the RADIUS access-request must contain a valid MAC address from the MAR cache.

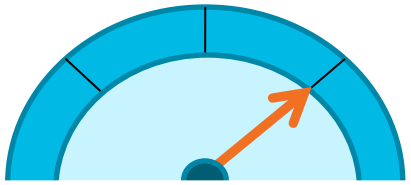


Identifying the Machine AND the USER

Machine Access Restrictions (MAR)

- MAR provides a mechanism for the RADIUS server to search the previous authentications and look for a machine-authentication with the same Calling-Station-ID.
- This means the machine must do authenticate before the user.

  i.e. Must log out, not use hibernate, etc….
- More possible limitations.



Fidelity Meter

Machine Access Restrictions (MAR)

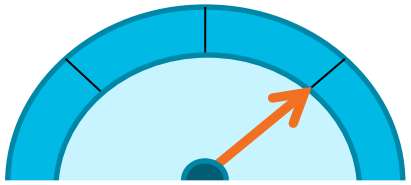
Limitations

- Potential Issues with MAR:

  Wired/WiFi transitions: Calling-Station-ID (MAC address) is used to link machine and user authentication; MAC address will change when laptop moves from wired to wireless breaking the MAR linkage.

  Machine state caching: The state cache of previous machine authentications is not persistent across RADIUS Server reboots.

  Hibernation/Standby: 802.1X fails when the endpoint enters sleep/hibernate mode and then moves to a different location, or comes back into the office the following day, where machine auth cache is not present in new RADIUS server or has timed out.

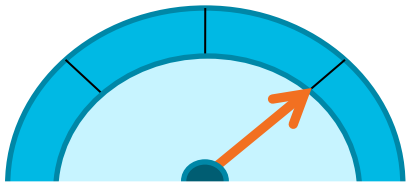


Fidelity Meter

Machine Access Restrictions (MAR)

Potential Issues with MAR

- **Spoofing**: Linkage between user authentication and machine authentication is tied to MAC address only. It is possible for endpoint to pass user authentication only using MAC address of previously machine-authenticated endpoint.



Fidelity Meter

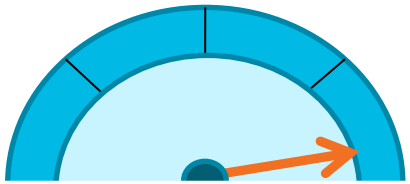
Enter EAP-Chaining

- EAP Chaining includes both ‘machine’ and ‘user’ identities in a **single EAP transaction**

Mar 24,12 07:25:42.316 PM	✓		jeppich >> host/labstation	F0:DE:F1:94:65:9C	3750x	both_user_&_machine_credentials_p...

- Authentication methods such as EAP-FAST, PEAP provide **separate EAP transactions**

May 14,12 05:46:16.233 PM	✓		jeppich	F0:DE:F1:94:65:9C	switch	PermitAccess
May 14,12 05:45:29.560 PM	✓		host/labstation	F0:DE:F1:94:65:9C	switch	PermitAccess



Fidelity Meter

EAP-FAST Method

- EAP-FAST is an EAP method that enables secure communication between a peer and a server by using the Transport Layer Security (TLS) to establish a mutually authenticated tunnel.
- EAP-FAST has three phases:

  - **Phase 0** - PAC Provisioning- Provisions tunnel PAC to client for subsequent tunnel establishment using TLS Session resumption

  - **Phase 1** - Negotiates the EAP-method type, EAP-FAST version, TLS ciphers, and authenticate the server to establish a protected tunnel

  - **Phase 2** - Once the tunnel is established, authenticates the client based on the identity and credentials transferred inside the tunnel using other EAP methods.

Let's compare using EAP-FAST

Separate EAP Transactions for "Machine" and "user"

Phase 0 – PAC Provisioning

Phase 1- tunnel establishment

Phase 2- user credentials sent through tunnel using inner method of authentication

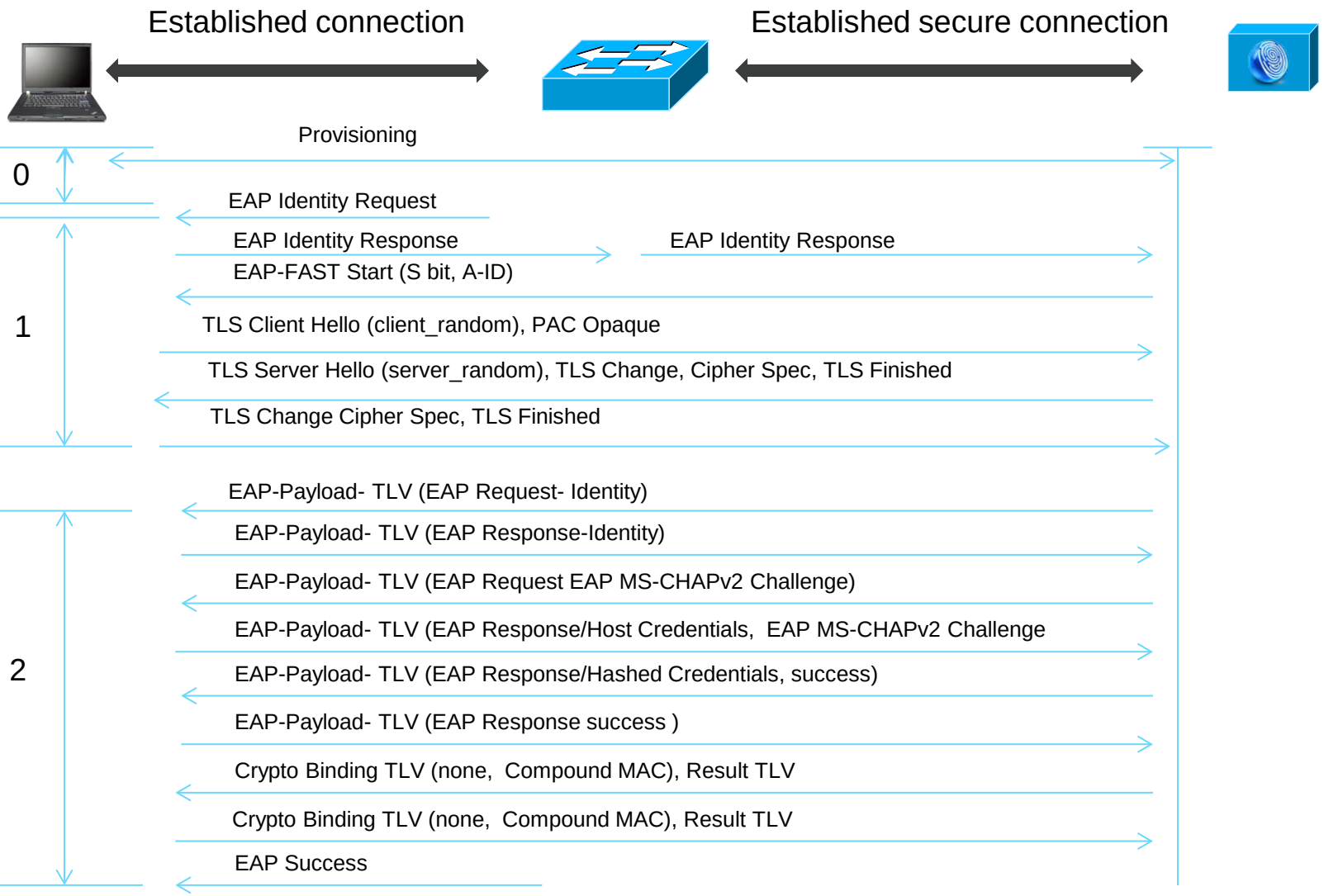
May 14,12 05:46:16.233 PM	✓	jeppich	F0:DE:F1:94:65:9C	switch	PermitAccess
May 14,12 05:45:29.560 PM	✓	host/labstation	F0:DE:F1:94:65:9C	switch	PermitAccess

Phase 0 – PAC Provisioning

Phase 1- tunnel establishment

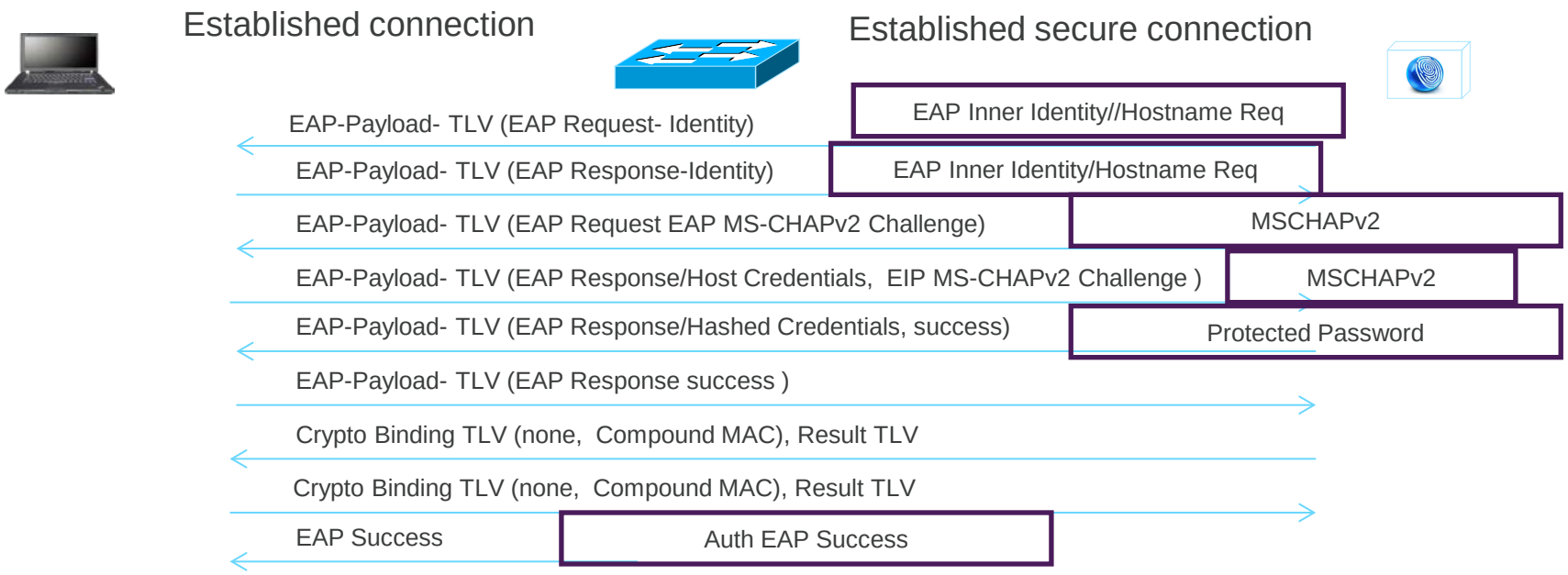
Phase 2- machine credentials sent through tunnel using inner method of authentication

EAP-FAST with EAP MS-CHAPv2



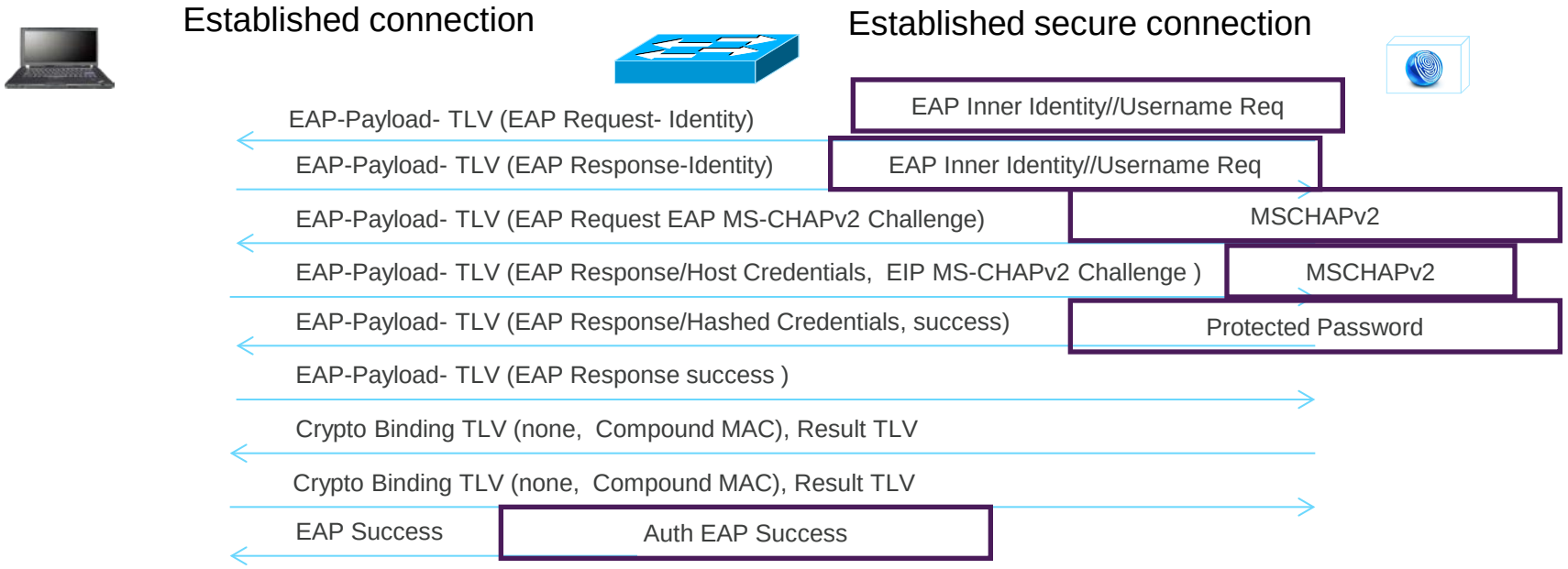
EAP-FAST – Machine

- PAC files will be used instead of certificates for mutual authentication between client and server.
- Phase 0: PAC provisioning Machine PAC to client.
- Phase 1: Negotiates the EAP-method, EAP version and employs TLS handshake to negotiate TLS ciphers and authenticate the server to establish the tunnel.
- Phase 2: Server authenticates the client based on the identity and credentials based inside the tunnel



EAP-FAST – User

- PAC files will be used instead of certificates for mutual authentication between client and server.
- Phase 0: PAC provisioning provision Tunnel /Machine PAC to client.
- Phase 1: Negotiates the EAP-method, EAP version and employs TLS handshake to negotiate TLS ciphers and authenticate the server to establish the tunnel.
- Phase 2: Server authenticates the client based on the identity and credentials based inside the tunnel



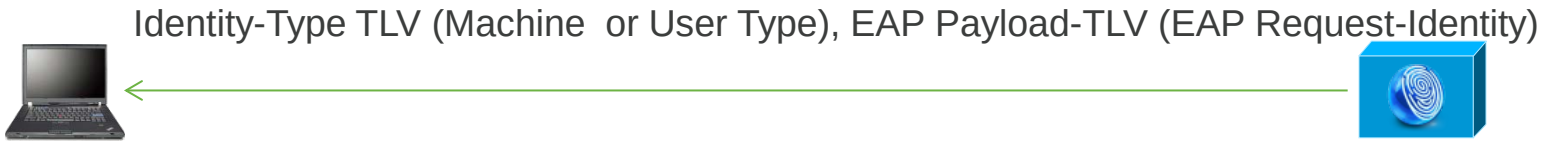
EAP-FAST Summary

- Secure EAP method using PAC files for mutual authentication between client and server.
- PAC files are used for secure TLS establishment and for user/machine authorization.
- Separate EAP transactions for machine and user identities
- Cannot prove ‘ownership’ the user is logging into the same system.

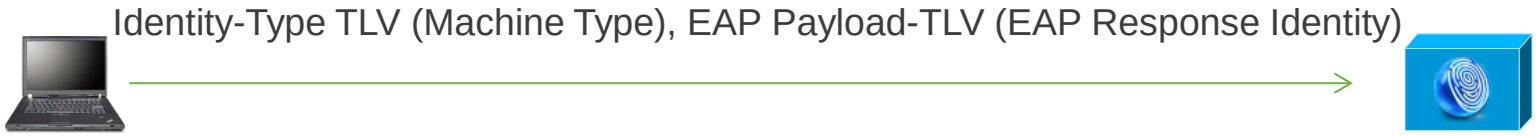
EAP-Chaining Details

Optional **Identity-Type TLV** is employed at the at the start of the second phase of EAP-FAST authentication, **indicate EAP Chaining**:

The Server sends the Identity-Type TLV, request identity to the client.



The client responds back with either the same identity request or proposes another identity-type.

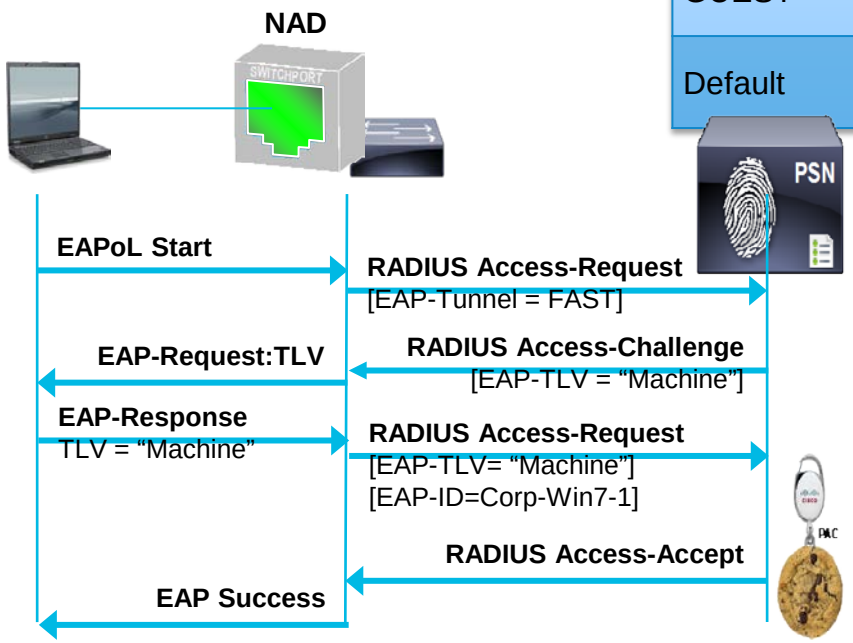


Client can also respond back with no Identity-Type TLV to indicate non-support of EAP Chaining (*Will fall back to EAP-FAST EAP method)*

EAP-Chaining Flow (1)

1. Machine Authenticates
2. Server Issues Machine AuthZ PAC

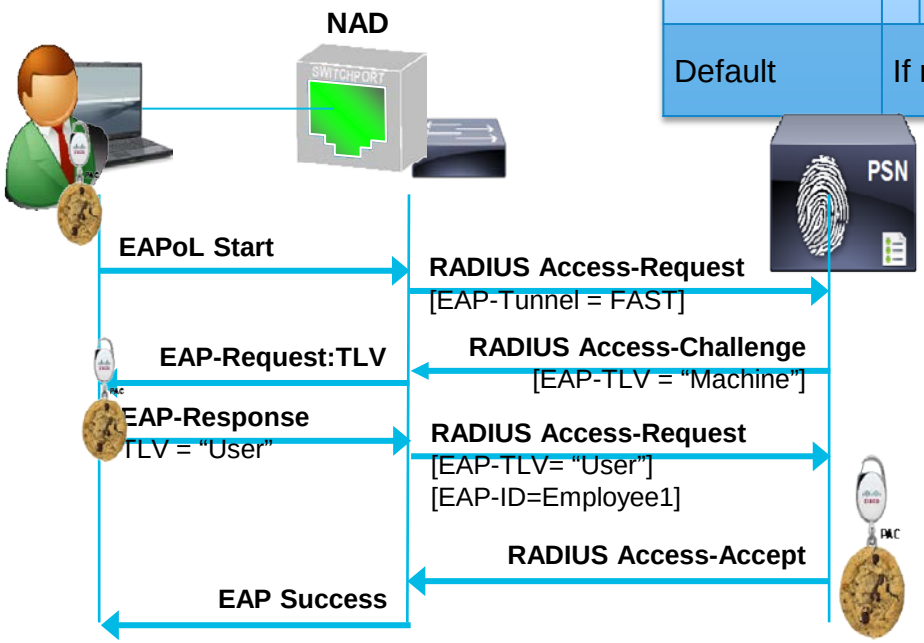
Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChaining Result = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	

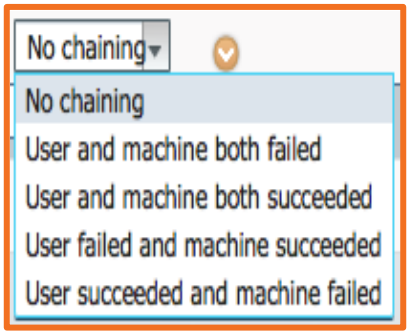


EAP-Chaining Flow (2)

3. User Authenticates
4. Server receives Machine PAC
5. Server issues User AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChainingResult = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	





EAP-Chaining Summary

- Secure EAP method using PAC files for mutual authentication between client and server.
- PAC files are used for secure TLS establishment and for user/machine authorization.
- Single EAP transaction for machine and user identities
- **Prove 'ownership'** the user is logging into the same system.
- Based upon intermediate results for user & machine, can have different authorization policies:

'user failed and machine succeeded'

'user succeeded and machine succeeded'

'machine failed and user succeeded'

'both user and machine failed'

If EAP Chaining is not supported on the device, the fall back is for EAP-FAST.

EAP-Chaining | TEAP Call To Action

- Evaluate the technology based on EAP-FAST today.
- It is deployable on selected platforms since almost a year.
- The TEAP will follow. **You will be ready**.

Progress Bar

CONFIDENCE
2013

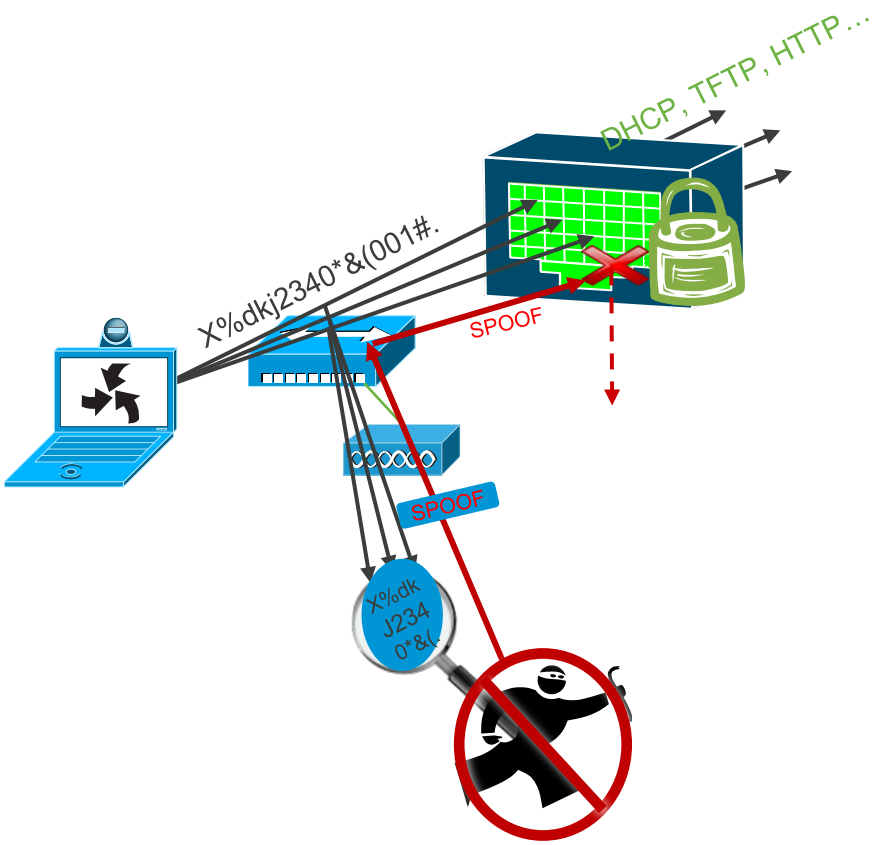
MACSEC OF THE STORM

Saving the L2 Confidentiality

- MACSec is a Layer 2 encryption mechanism (Ratified in 2006)
  - 802.1AE defines the use of AES-GCM-128 as the encryption cipher.
  - Works to extend to AES-GCM-256. Need hardware support.
- Builds on 802.1X for Key Management, Authentication, and Access Control
- 802.1X-2013 defines the use of MACSec, MACSec Key Agreement (MKA) (Previously 802.1AF), and 802.1AR (Ratified in 2013)
- Authenticated Encryption with Associated Data (AEAD)
- HW implementations run are very efficient
  - 1G and 10G line rate crypto currently deployed
- Intel AES-NI support in CPU (FIPS 140-2 Validated)

Encrypting everything Hop-by-Hop

- Physical MiTM into the access link is a feasible attack using very small factor PC and others
- The attacks have been demonstrated (DEFCON19 – *A Bridge Too Far*).
- 802.1X EAP authentication phase is used to derive the 802.1AE session key for encryption.
- Encryption can be done in software and in hardware on the endpoint.
- **Switch crypto support in hardware is necessary**

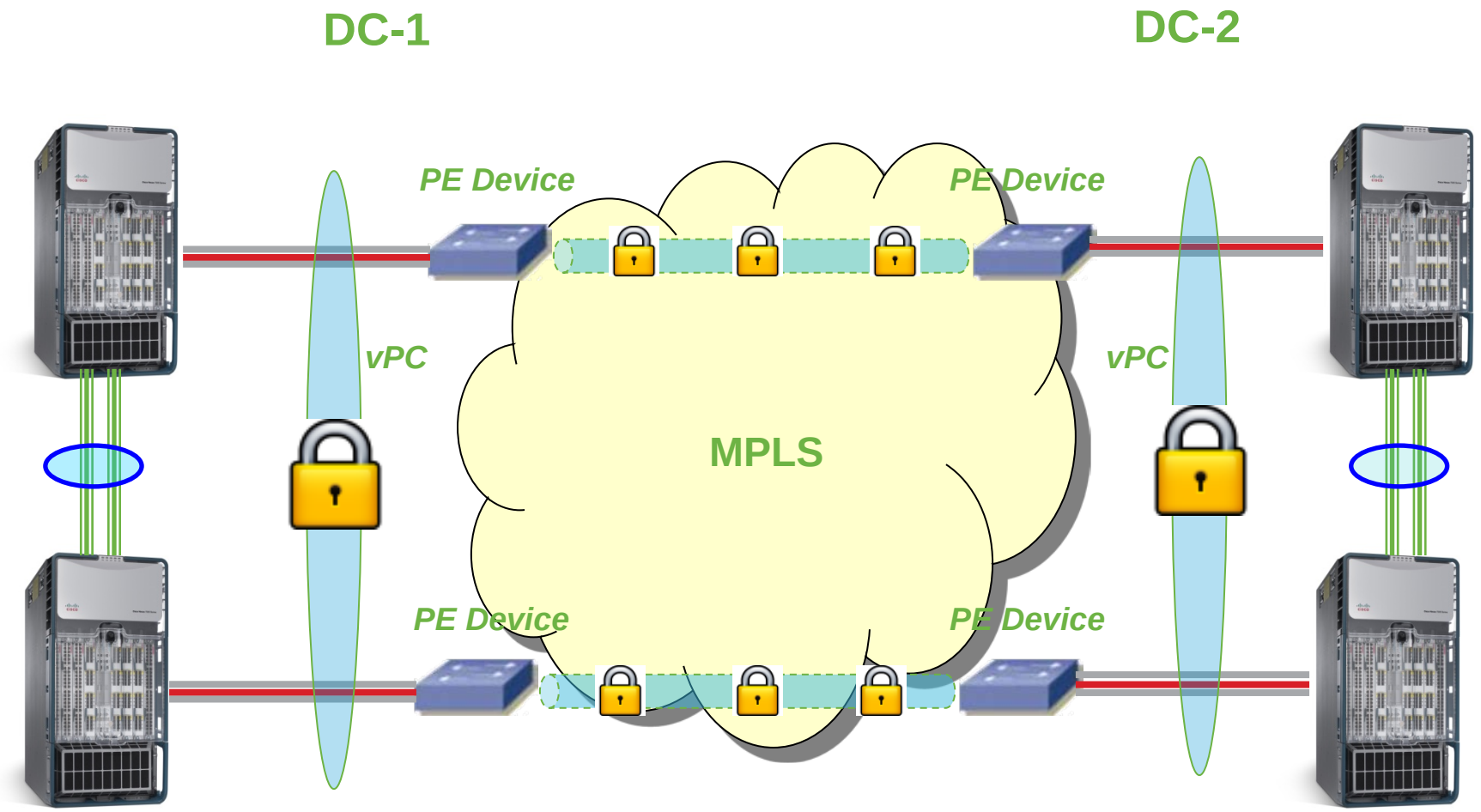


AES Galois/Counter Mode (GCM)

- Block cipher mode of operation for Authenticated Encryption with Associated Data (AEAD)
- High speed, low latency, low cost
  - Most efficient mode for packet networks
- Widely adopted in the industry
  - Layer 3+: IPSec, TLS, DLTS, SSH, *SRTP*
  - Layer 2: 802.1AE MACSec, Gigabeam, *802.11*
  - Storage encryption: 1619.1, LTO-4
  - Inside commercial crypto silicon
  - NIST SP 800-38D

Massively Scalable Encrypted DC InterConnect

Dual Access with EoMPLS Connectivity



Progress Bar

CONFIDENCE
2013

THE ART OF PROFILING

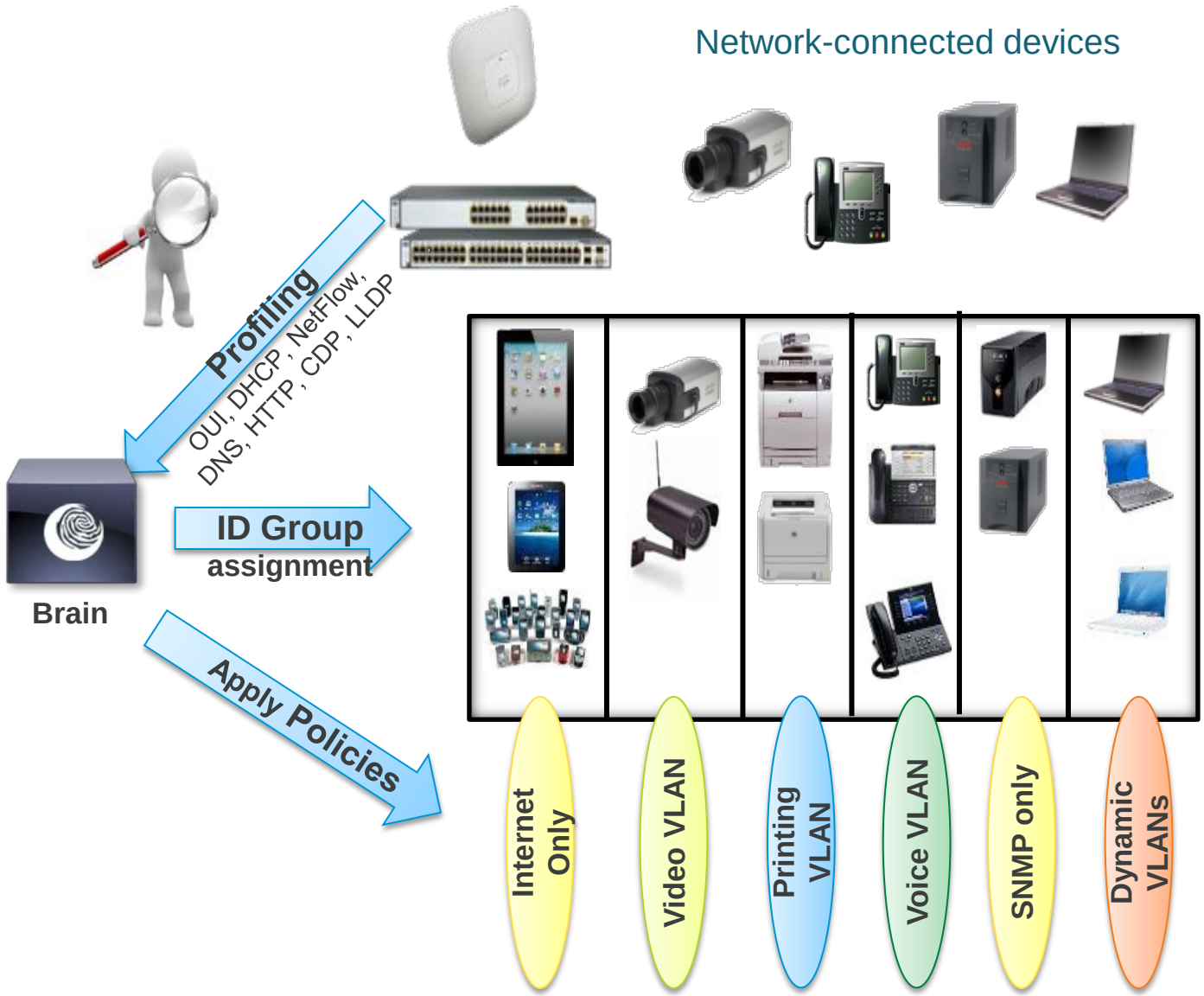
Profiling in Networking Security

- What Profiling is:
  - Dynamic classification of every device that connects to network using the infrastructure.
  - Provides the context of “What” is connected independent of user identity for use in access policy decisions

PCs	Non-PCs			
	UPS	Phone	Printer	AP

- What Profiling is NOT:
  - An authentication mechanism.
  - An exact science for device classification.

Central Profiler: 3 Steps

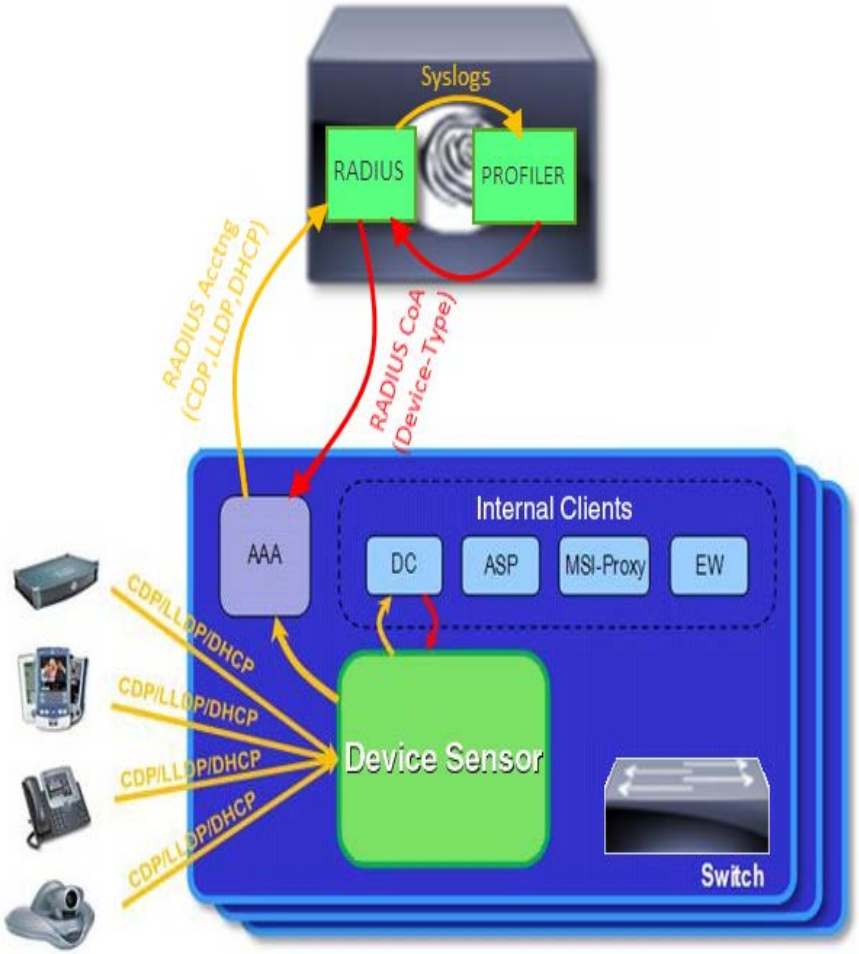


Profiling Probes – the sources

- Profiler could use various sources to identify devices.
- RADIUS
- HTTP | Captive Portal
- DHCP | DHCP SPAN
- SNMP Query | Trap
- Network Scan (nmap)
- DNS
- NetFlow
- CDP | LLDP

Distributed Device Sensors

- Device Classifier and Analyzers – achieving scale



Distributed Device Sensor

EndPointMACAddress	00-21-55-D6-01-33
EndPointMatchedProfile	Cisco-IP-Phone-7945
EndPointPolicy	Cisco-IP-Phone-7945
EndPointProfilerServer	ISE-02
EndPointSource	RADIUS Probe
Framed-IP-Address	10.100.15.100
IdentityGroup	Cisco-IP-Phone

Switch Device Sensor Cache

```
# show device-sensor cache all
Device: 0021.55d6.0133 on port GigabitEthernet1/0/1
-------------------------------------------------
Proto Type:Name                          Len Value
cdp      2:address-type                   17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 64 0F
                                             64
cdp     16:power-type                      6 00 10 00 06 2E E0
cdp     11:duplex-type                     5 00 0B 00 05 01
cdp     25:power-request-type             12 00 19 00 0C 01 33 00 03 00 00 2E E0
cdp      6:platform-type                  23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
                                             6E 65 20 37 39 34 35
cdp      5:version-type                   17 00 05 00 11 53 43 43 50 34 35 2E 39 2D 30 2D 33
                                             53
cdp      4:capabilities-type               8 00 04 00 08 00 00 04 90
cdp      3:port-id-type                   10 00 03 00 0A 50 6F 72 74 20 31
cdp      1:device-name                    19 00 01 00 13 53 45 50 30 30 32 31 35 35 [illegible] 36 30
                                             31 33 33
dhcp    50:requested-address               6 32 04 0A 64 0F 64
dhcp    54:server-identifier               6 36 04 0A 64 07 64
dhcp    55:parameter-request-list          9 37 07 01 42 06 03 0F 96 23
dhcp    60:class-identifier               40 3C 26 43 69 73 63 6F 20 53 79 73 [illegible] 65 6D 73 2C
                                             20 49 6E 63 2E 20 49 50 20 50 68 [illegible] 6E 65 20 43
                                             50 2D 37 39 34 35 47 00
dhcp    12:host-name                      17 0C 0F 53 45 50 30 30 32 31 35 [illegible] 44 36 30 31 33
                                             33
dhcp    61:client-identifier               9 3D 07 01 00 21 55 D6 01 33
```

IP Phone

SEP002155D60133

10.100.15.100

Cisco Systems, Inc. IP Phone CP-7945G

SEP002155D60133

ISE Profiling result

cdpCacheDeviceId	SEP002155D60133
cdpCacheDevicePort	Port 1
cdpCacheDuplex	01:
cdpCachePlatform	Cisco IP Phone 7945
cdpCachePowerConsumption	2e:e0
cdpCacheVersion	SCCP45.9-0-3S

dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7945G
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.100.15.100
dhcp-server-identifier	10.100.7.100
dot1xAuthAuthControlledPortCont[illegible]ol	2
dot1xAuthAuthControlledPortStatu	2
dot1xAuthSessionUserName	00-21-55-D6-01-33
host-name	SEP002155D60133

Progress Bar

CONFIDENCE
2013

RAINING FLOWS

Threat Defense – the network-centric approach

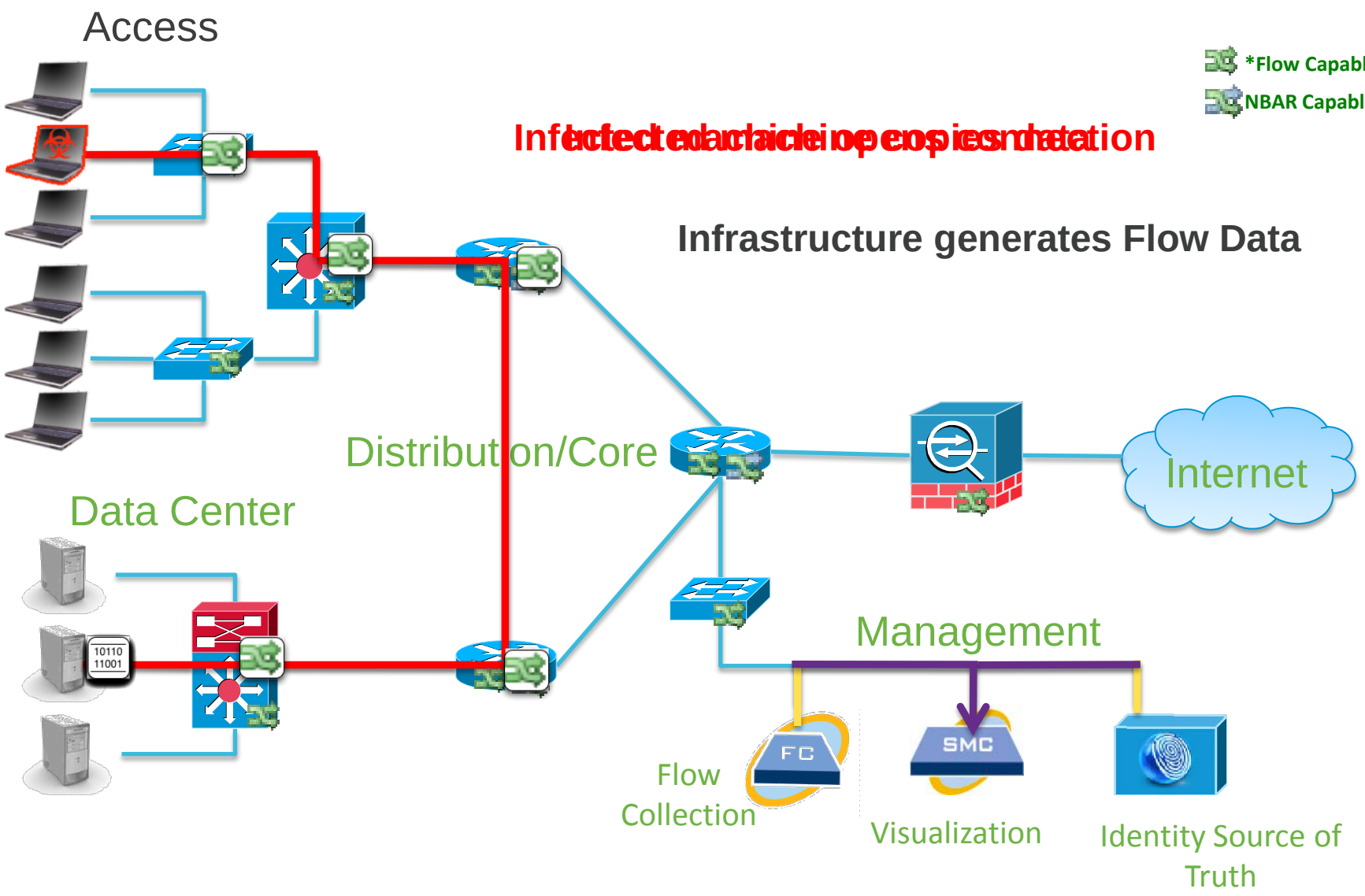
- Get the identity from the 802.1X | Webauth | MAB - authenticated machines
- Collect all the possible flows from the infrastructure
  - can generate the flows in hardware | software
  - can use Flow generation tools from raw network traffic (SPAN et al.)

LITERALLY EVERYTHING.

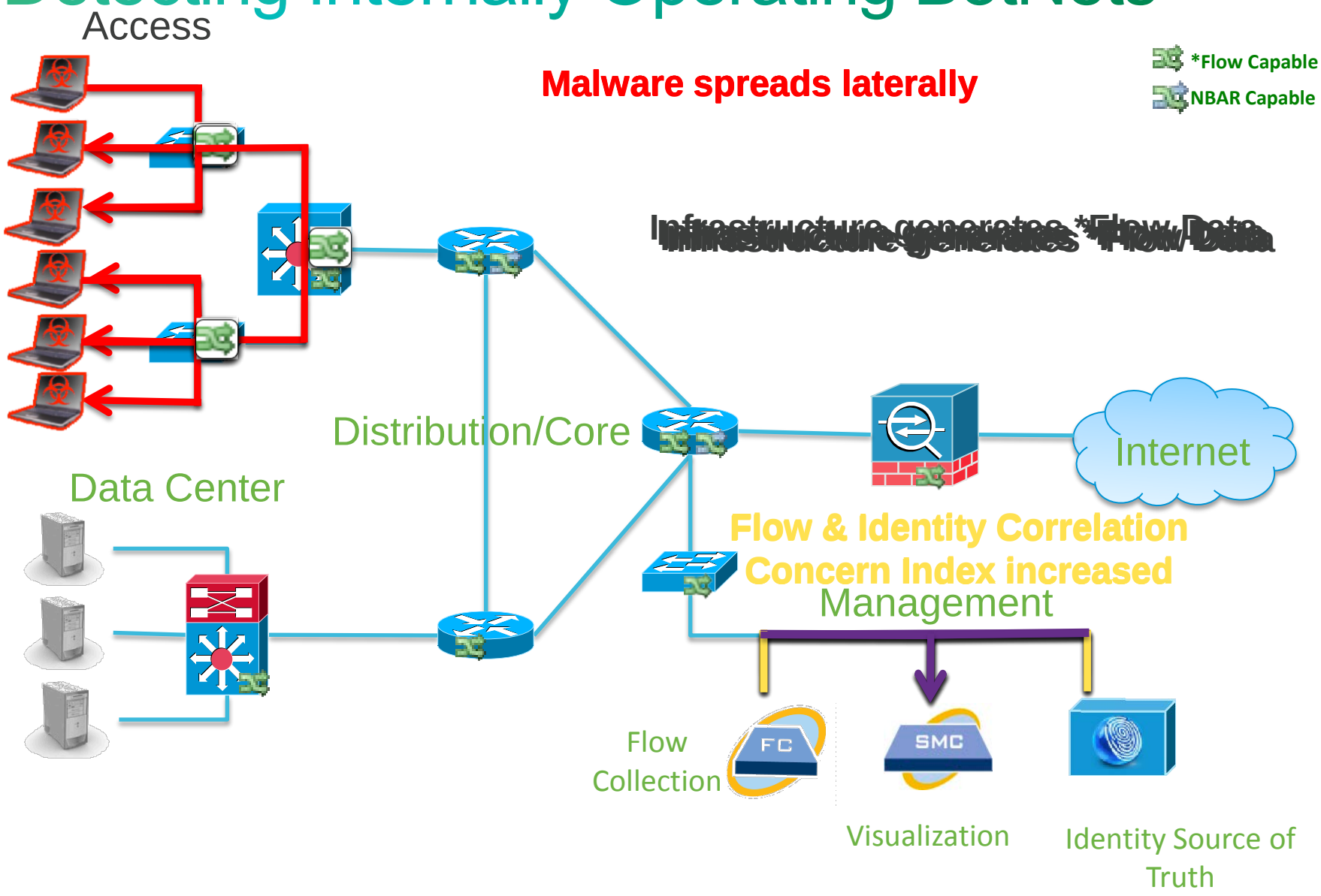
- Correlate those two for:

1. Detecting data loss
2. Detecting network reconnaissance
3. Detecting internally operating contagion
4. Detecting command and control channels

Detecting Data Loss



Detecting Internally Operating BotNets



Network-Centric Paradigm shift

- **Artificial intelligence** advances
- Detection algorithms

  Minnesota Intrusion Detection System (MINDS) algorithm [Ertoz et al, 2004] processes data from a number of flows.

  Xu et al. algorithm [Xu, Zhang et al, 2005] classifies traffic sources.

  The **volume prediction algorithm** [Lakhina et al, 2004] uses the Principal Components Analysis (PCA) methodology

  The **entropy prediction algorithm** [Lakhina et al, 2005] predicts the entropy of source and destination ports and destination IPs.

  The **TAPS algorithm** [Sridharan et al, 2006] targets a specific class of attacks by classifying a subset of suspicious traffic sources

- The focus is shifting **from mainly applying signature-based techniques** to defend against known threats to leveraging new techniques in artificial intelligence based **real-time analytics to detect the unknown threats** that are already proliferating inside our networks.

Progress Bar

CONFIDENCE
2013

TRAPPED UNDER IKE

What is Advanced Cryptography today?

- Upgrade to all crypto algorithms and key sizes
  - Authenticated Encryption
  - Elliptic Curve Cryptography
- Scales well to
  - High security levels
  - High throughput
  - High numbers of connections
- Anticipates industry trends for IPSec VPNs
  - Compatible with security and scalability requirements of next decade
  - Current products must meet these requirements and also interoperate with future products
- Compatible with Industry | Government Standards
  - Algorithms only get weaker over time due to advances in cryptanalysis
  - Industry is at the cusp of an algorithm transition, which is needed to keep computational costs down

Cryptographic Suite

Encryption

Data Authentication

Key Establishment

Signatures

Hashing

Crypto Recommendations

	Now	Soon
	AES-128-GCM, AES-128-CCM	AES-128-GCM, AES-128-CCM
	HMAC-SHA-256	HMAC-SHA-256
	DH-2048, RSA-2048	ECDH-P256
	RSA-2048	ECDSA-P256
	SHA-256	SHA-256

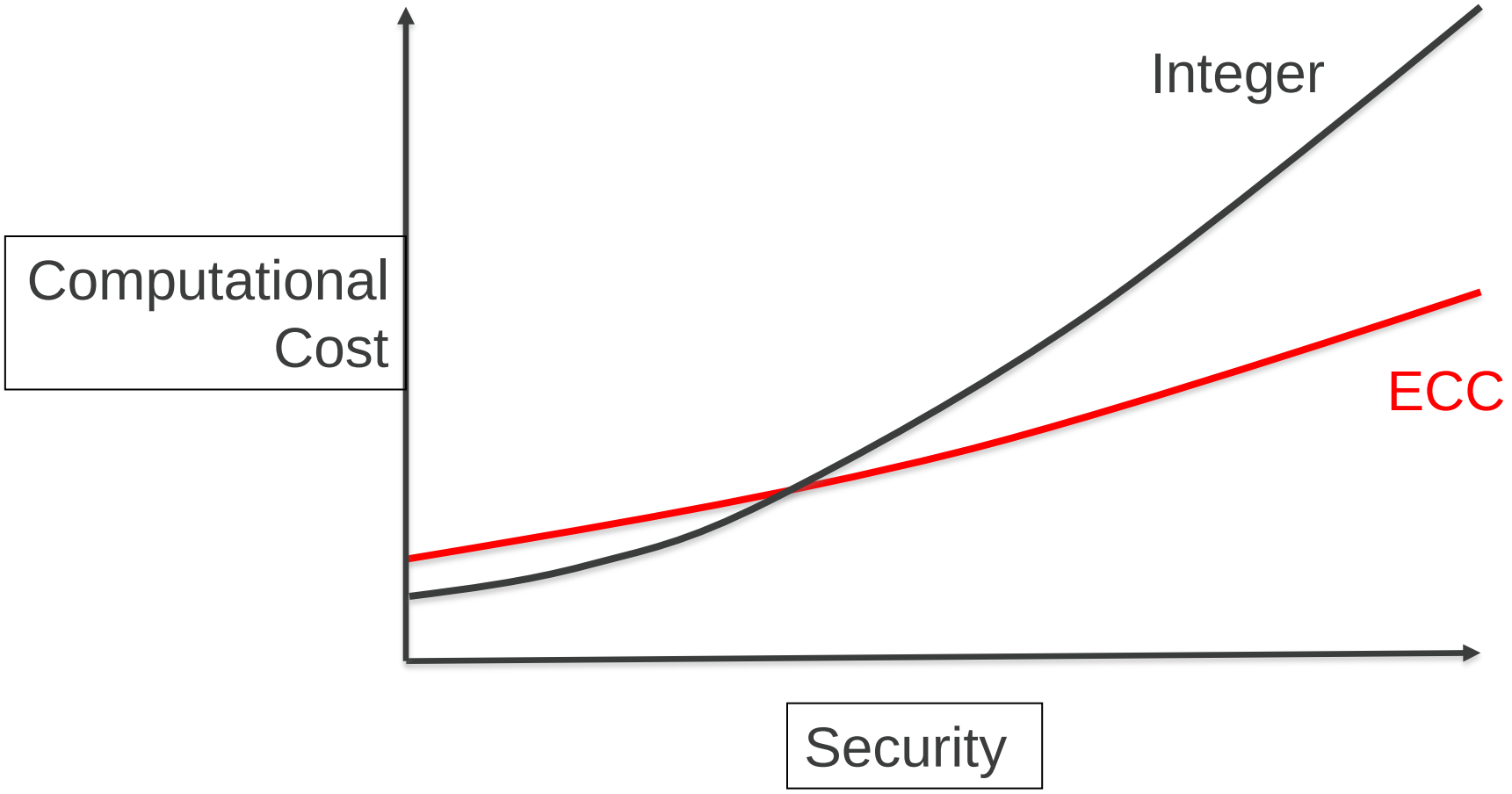
Elliptic Curve Cryptography

- Alternative crypto mathematics
  - Invented in 1985
  - Promoted by NSA
  - Adopted in some niches (e.g. Smart Grid)
- More efficient than RSA at higher security levels
  - Current commercial security (96 or 112 bits) - ECC slower
  - 128 bits strength – ECC operations faster
  - 256 bits strength – ECC much faster

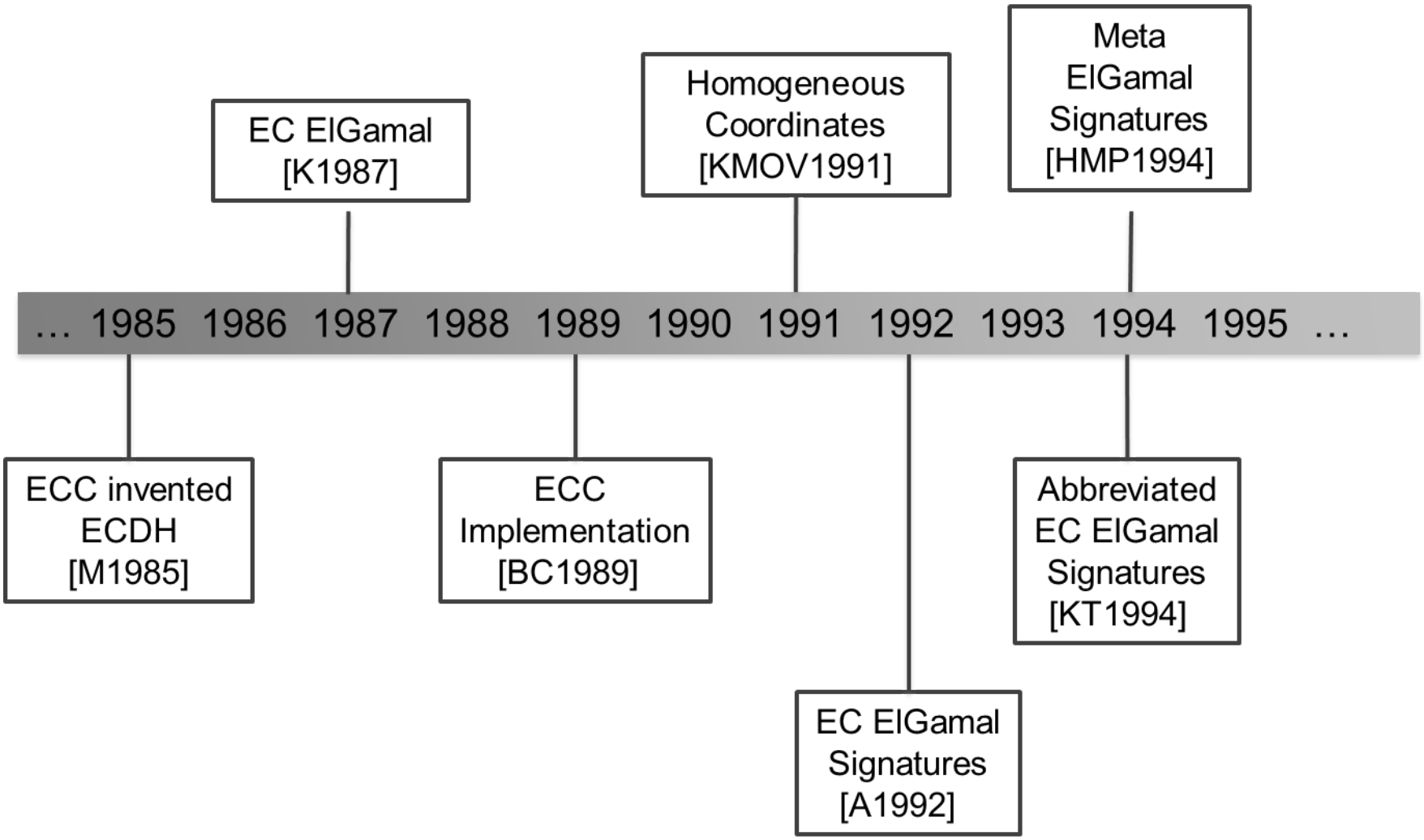
ECC History

- Many ECC patents
  - Slow adoption
- RFC 6090 *Fundamental Algorithms of ECC*
  - Subset of basic ECC that predates patents
    - Simplifies IPR analysis
- Closely based on pre-1994 references
  - Security: survived > 17 years of review

ECC Efficient at High Security

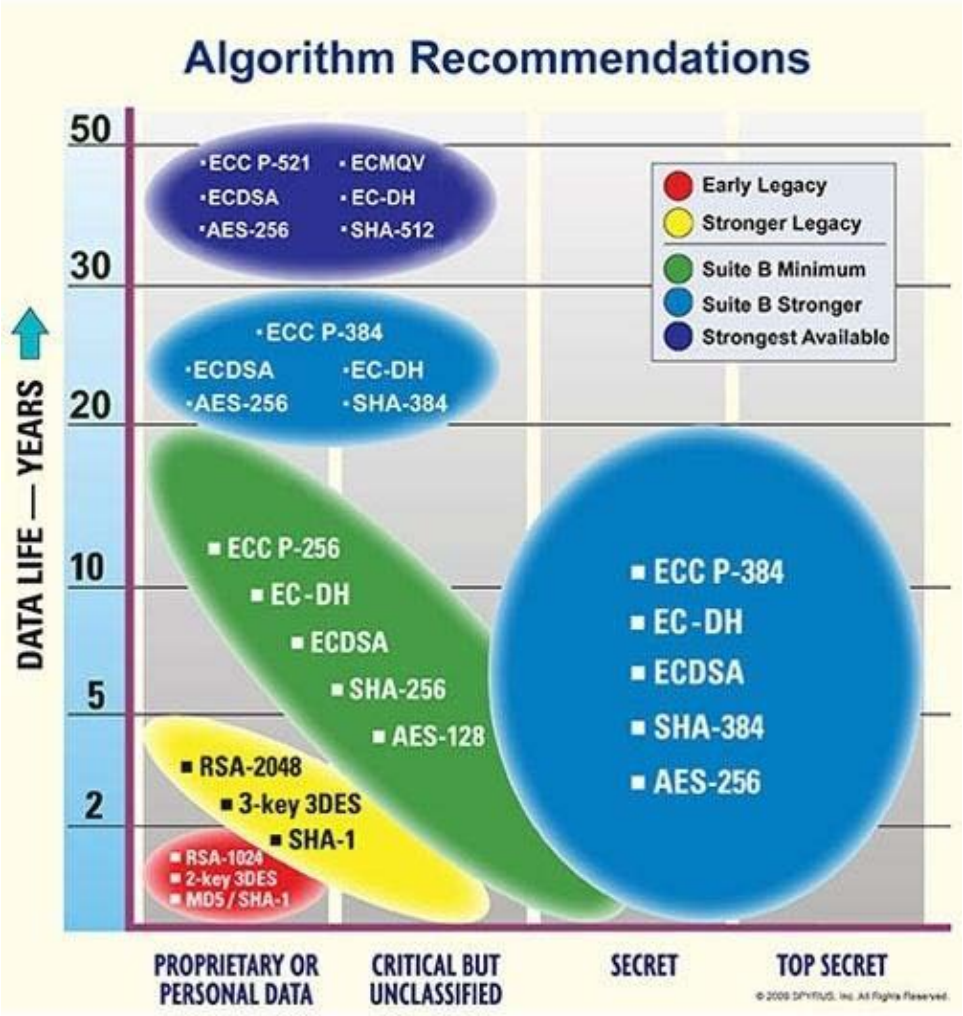


Timeline



DoD Suite B Standards

- NSA (National Security Agency) oversees and sets standards for DoD and other federal organizations
- NSA defines Suite B –a set of cryptographic algorithms
- Suite B for IPsec VPN is defined in RFC 4869
- Chart shows NSA's recommendation of algorithms to be used to protect data at different levels

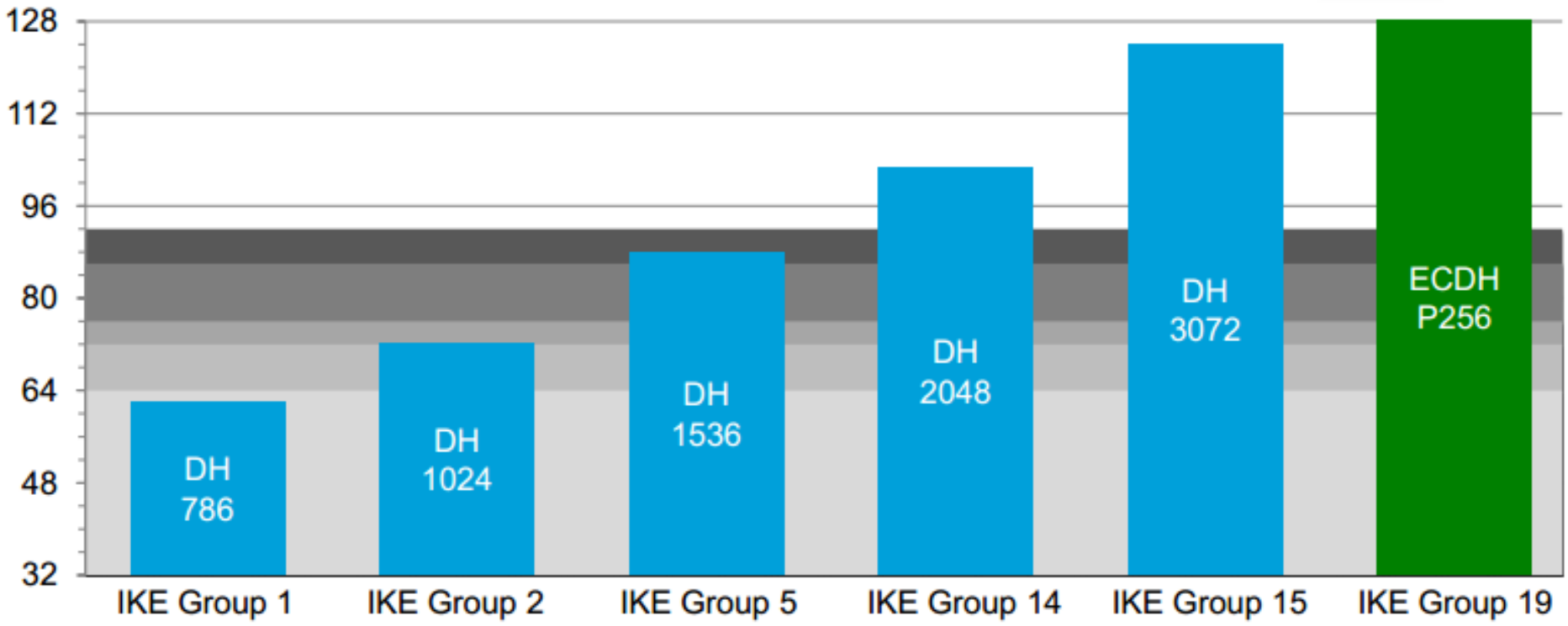


Suite B Components

Encryption	Advanced Encryption Standard (AES) – FIPS PUB 197 (with keys sizes of 128 and 256 bits) http://csrc.nist.gov/publications/PubsFIPS.html
Key Exchange	Elliptic Curve Diffie-Hellman (ECDH) – NIST Special Publication 800-56A (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) – FIPS PUB 186-3 (using the curves with 256 and 384-bit prime moduli) http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
Hashing	Secure Hash Algorithm (SHA) – FIPS PUB 180-3 (using SHA-256 and SHA-384) http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

- NIST SUITE B - http://www.nsa.gov/ia/programs/suiteb_cryptography/

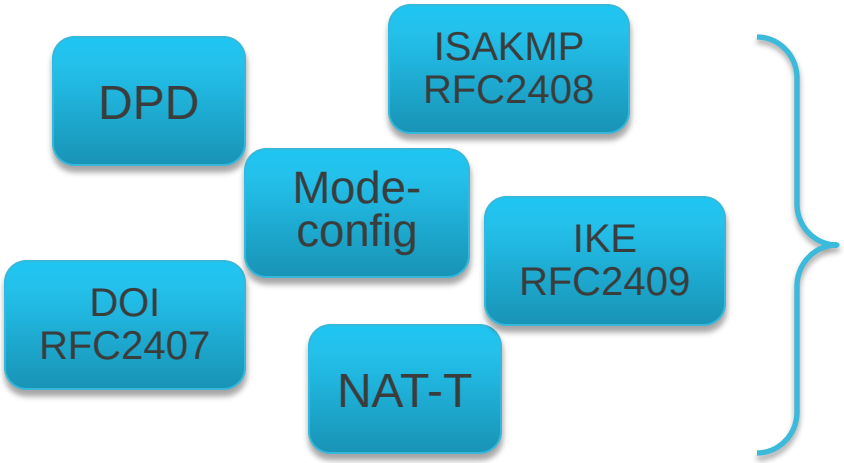
Cryptographic Strength



Enter IKEv2 – in a few words

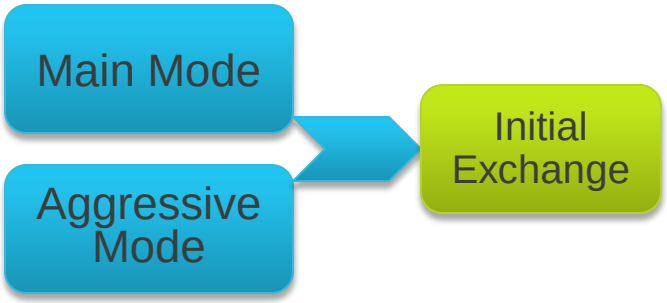
- Defined in RFC 4306 - updated by RFC 5996
  - No interoperability with IKEv1
  - Not widespread … yet
- Both are using the same basic structure aiming at
  - Privacy
  - Integrity
  - Authentication
- Both run over UDP 500/4500

Key Comparisons



IKEv2 RFC5996

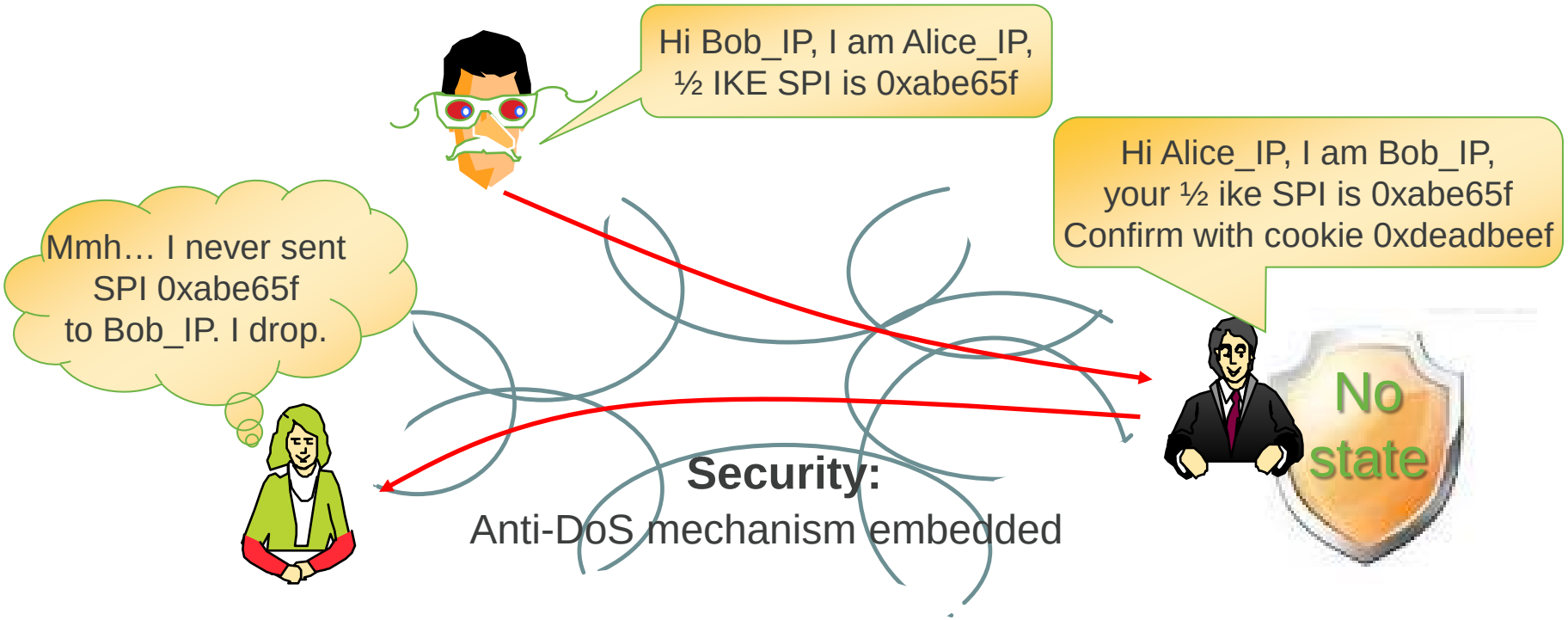
Coalesces important specifications under a single RFC



Key differentiators

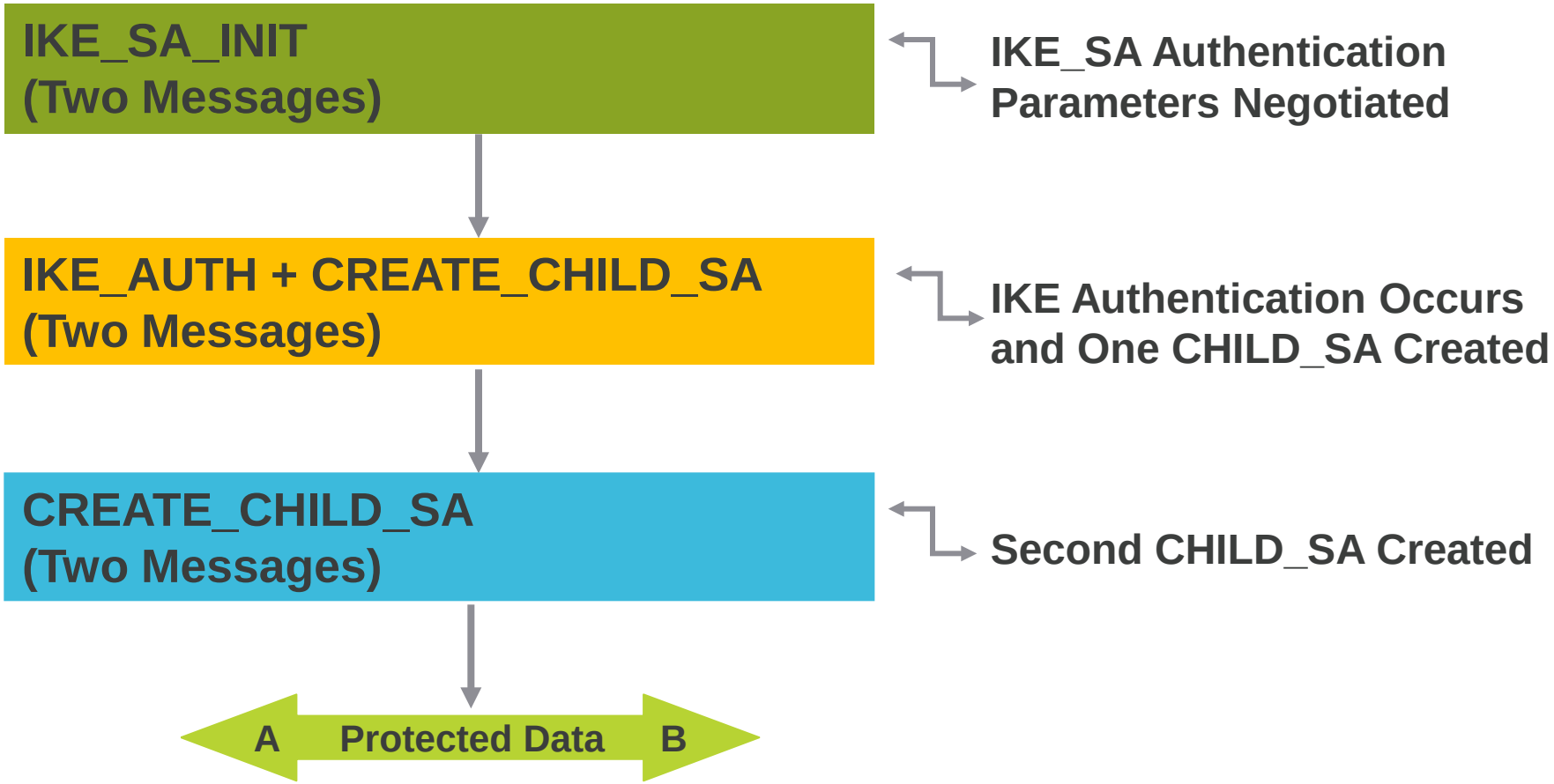
	IKEv1	IKEv2
Auth messages	6 max	Open ended
First IPsec SA	9 msgs min	~ 4-6 msgs min
Authentication	pubkey-sig, pubkey-encr, PSK	Pubkey-sig, PSK, **EAP**
Anti-DOS	Never worked	Works!
IKE rekey	Requires re-auth (expensive)	No re-auth
Notifies	Fire & Forget	Acknowledged

The anti-clogging cookie



- The first two packets only exchange cookies and proposals
- The cookies are used to prevent DoS attack (anti-clogging)
- Cookies are used when-needed and may increase the number of initial messages

IKEv2 exchanges overview



Informational Exchanges

- Mostly used for housekeeping
  - Delete notifies
  - Liveness checks
  - Initial Contact
  - Error reporting (various notifications)
- Must be acknowledged
  - Will be retransmitted otherwise (until give up)
- Cryptographically protected
  - Only after Initial Exchange
- Used for Configuration Exchange
  - Similar to Mode-Config

Extensible Authentication Protocol (EAP)

- No X-AUTH in IKEv2; EAP instead
- EAP – authentication framework that provides common functions for various methods:
  - Tunneling - EAP-TLS, EAP/PSK, EAP-PEAP…
  - Non-tunneling – EAP-MSCHAPv2, EAP-GTC, EAP-MD5,…
- Implemented as additional IKE_AUTH exchanges
- Only used to authenticate the initiator to responder
- Responder MUST use Certificate
- Can severely increase number of messages (12-16)
- EAP comes with caveats – RTFM approach applies.

Next-Gen Crypto – Call To Action

- NGE with IKEv2 is deployable today for:
  - Remote Access VPN
  - Static Site-to-Site VPN
  - Dynamic Site-to-Site VPN

  Consider **migrating** your overlay IPSec VPNs in the near future.

  Use in all your new, green-field non-SSL VPN deployments today.

SUCCESS

Thank you!

Gaweł Mikołajczyk
gmikolaj@cisco.com