Konsekvenser av Blast-RADIUS…

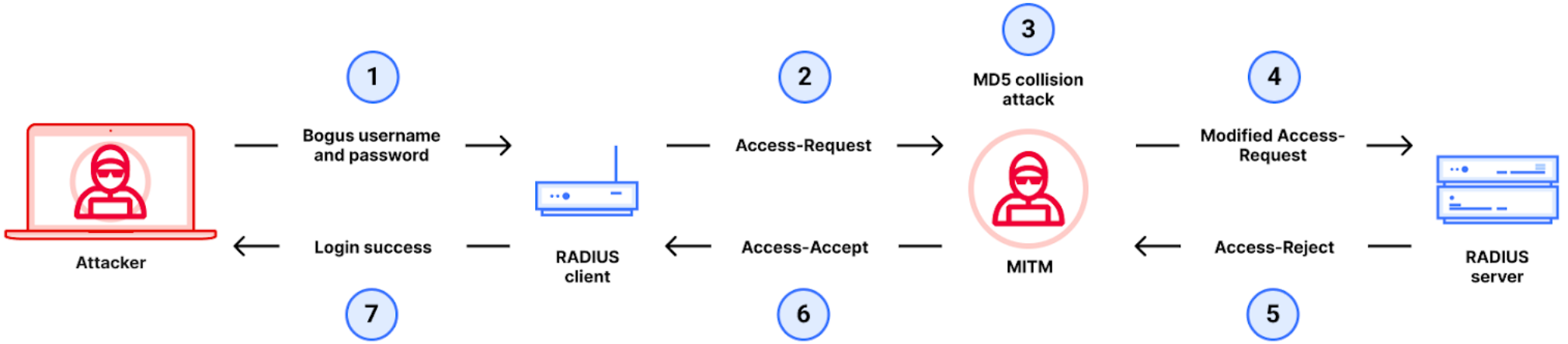
Blast-RADIUS

Herrnilsson@sunet.se

SUNET

Vad är problemet?

- MD5 kollisioner (RADIUS info går ju i klartext)

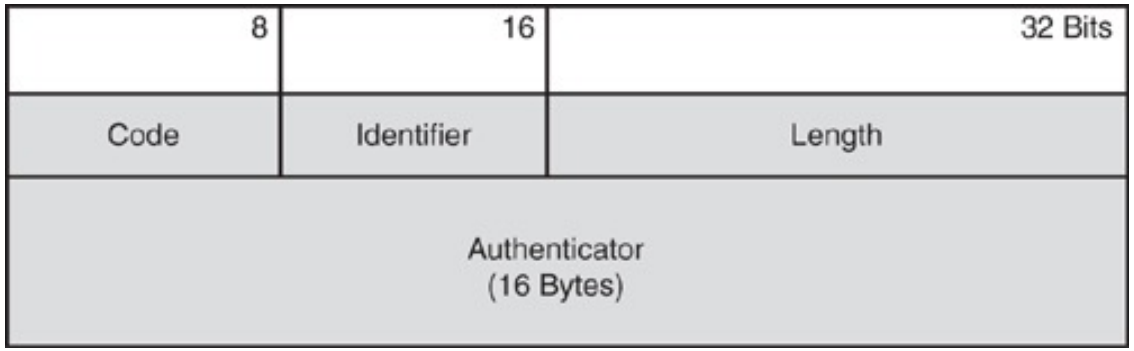


SUNET

“Säkerhet” i RADIUS paket?

Table 8-1. RADIUS Packet Header Structure Illustration

Fields	Description
Code	Code is the message type of the RADIUS packet. The code is a one-octet (8-bit) value that establishes the type of the RADIUS packet. The codes are 1 = Access-Request 2 = Access-Accept 3 = Access-Reject 4 = Accounting-Request 5 = Accounting-Response 11 = Access-Challenge
Identifier	The identifier matches request and reply packets. The identifier is a one-octet (8-bit) value. The identifier is a message sequence number that allows the RADIUS client to match a RADIUS response with the correct outstanding request; that is, the value in reply is equal to the value in request.
Length	The message length is a 2-octet (16-bit) message length including the header.
Authenticator	The authenticator is a 16-octet field (16-bytes) used to authenticate the reply from the RADIUS server. The value in the request packet is randomly generated, whereas the value in the reply packet is an MD5 hash of the reply message data appended with a shared secret using a vector value from the request packet.
Attributes	The attribute field contains an arbitrary number representing sets of AV pairs.

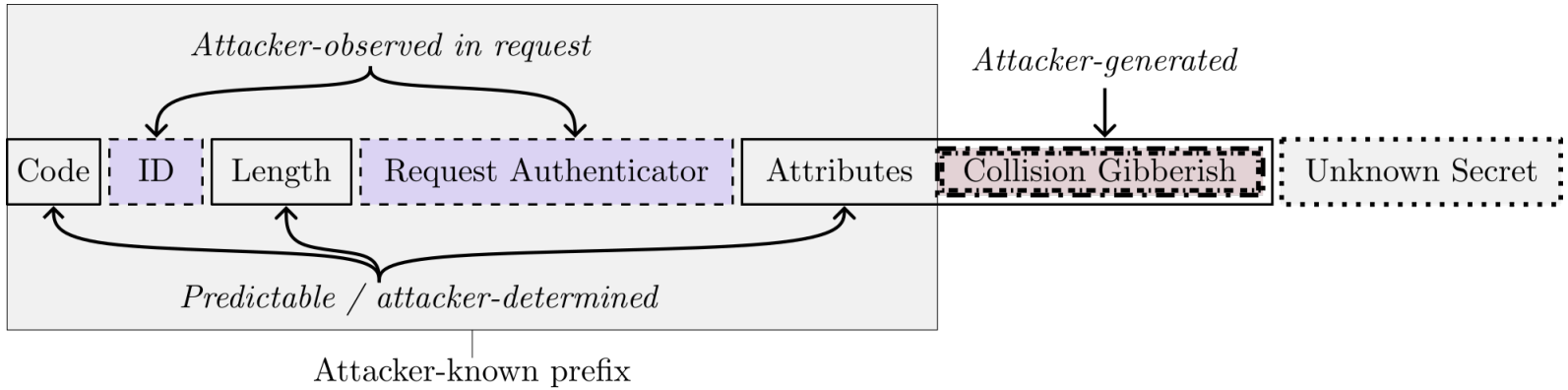


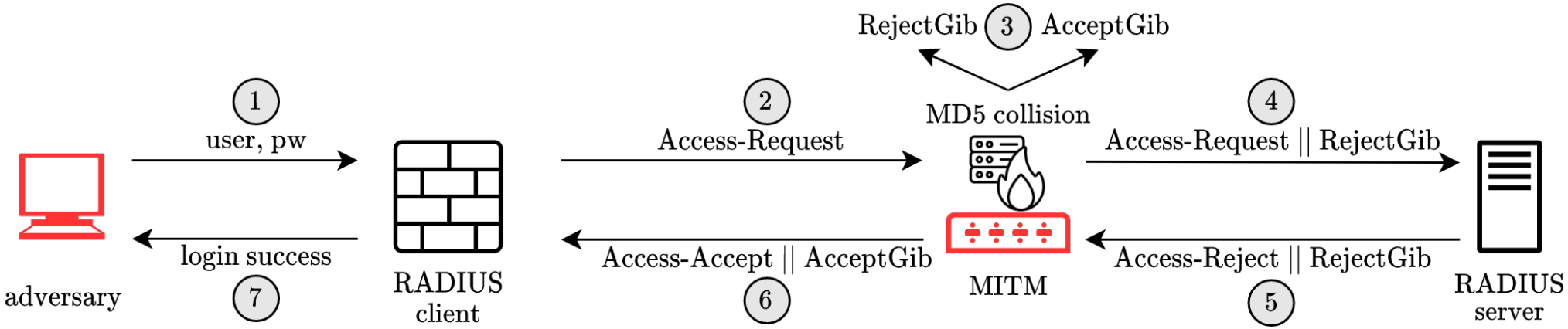
Request packets include a value called a Request Authenticator that is essentially a random nonce.

The Response Authenticator is computed as:
MD5(Code||ID||Length||Request Authenticator||Packet Attributes||Shared Secret),

SUNET

Exempel på hack?





SUNET

Hur illa är det?

- Detta har varit känt redan april 2024 hölls hemligt tills juli 2024 (i väntan på Microsoft…)
- Som tur är klarar vi oss som kör eduroam därför att EAP trafik är tunnlad i TLS
  https://eduroam.org/eduroam-response-to-the-blastradius-vulnerability/
  https://eduroam.org/wp-content/uploads/2024/07/eduroam-blast-vulnerability.pdf
  men….
- OBS!!!! Detta problem gäller ALL RADIUS trafik och inte bara på serversidan. Dags för er att göra hemläxa över var ni använder RADIUS.

RADIUS är gammalt och behöver uppdateras

RADIUS kom ut 1991 och med säkerhet baserat primärt på MD5 är det bara en tidsfråga innan andra ”hack” dyker upp men hjälp är på väg
Inom IETF är nya standarder/rekommendationer på väg att bli RFC:er 2025
https://datatracker.ietf.org/wg/radext/documents/

Document		Date	Status	IPR	AD/Shepherd
Active Internet-Drafts (5 hits)					
draft-ietf-radext-radiusdtls-bis-03 **(Datagram) Transport Layer Security ((D)TLS Encryption for RADIUS**	40 pages	2024-10-21	I-D Exists WG Document Review: secdir Early Jan 2024		
draft-ietf-radext-radiusv11-11 **RADIUS/1.1, Leveraging ALPN to remove MD5**	41 pages	2024-10-18	RFC Ed Queue : EDIT Submitted to IESG for Publication : Experimental Reviews: secdir opsdir LC genart LC secdir LC artart LC Aug 2023		Paul Wouters Jan-Frederik Rieckers
draft-ietf-radext-tls-psk-11 **Operational Considerations for RADIUS and TLS-PSK**	24 pages	2024-10-17	Approved-announcement to be sent::AD Followup 49 Submitted to IESG for Publication : Best Current Practice Reviews: secdir secdir LC Sep 2023 Action Holder: Paul Wouters 21		Paul Wouters Valery Smyslov
draft-ietf-radext-deprecating-radius-03 **Deprecating Insecure Practices in RADIUS**	77 pages	2024-08-07	I-D Exists WG Document Jan 2024		

SUNET

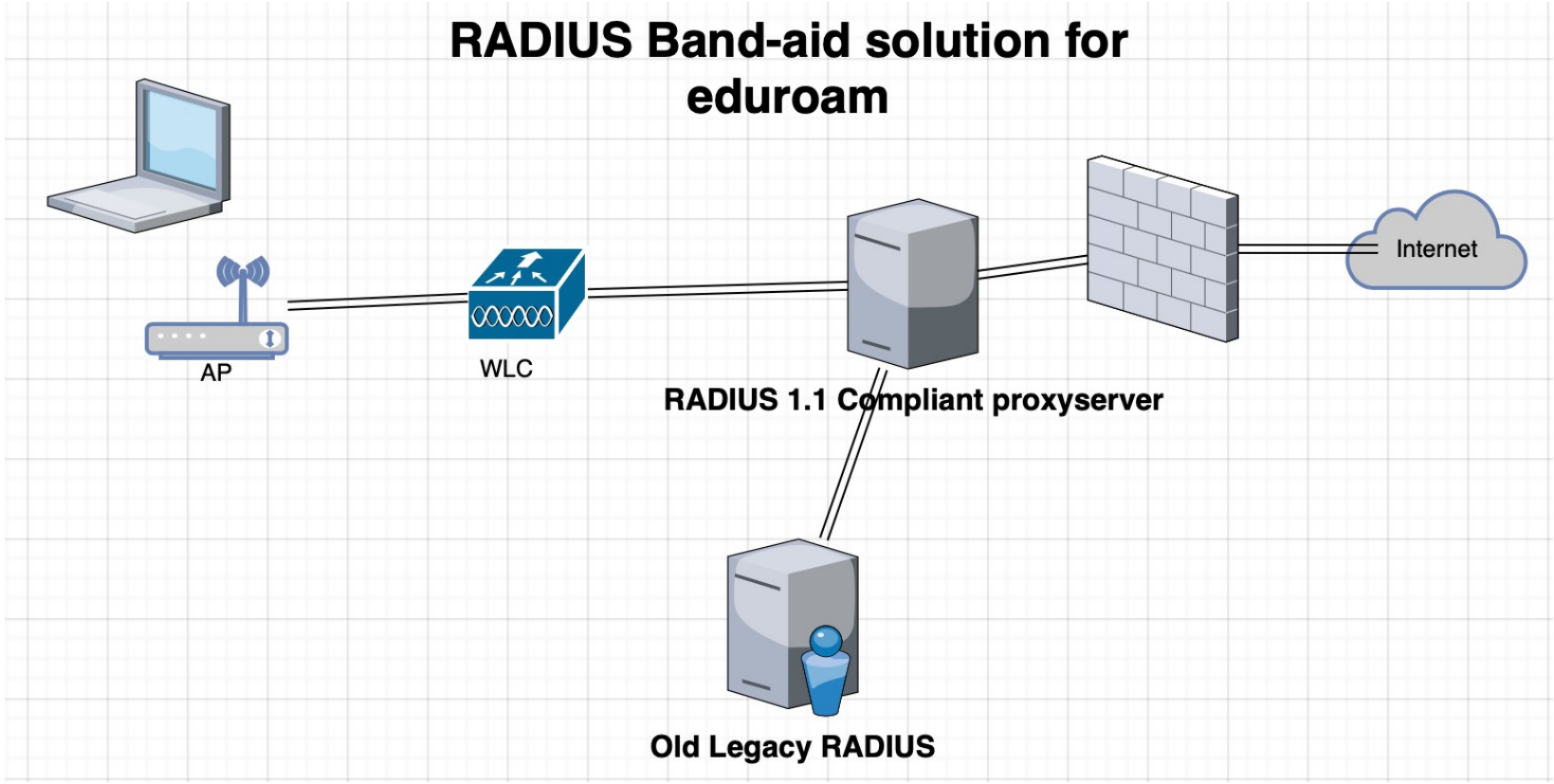
RADSEC tills RADIUS 11 dyker upp

- Det kommer nog att ta ett tag innan vi ser alla tillverkare implementera det nya 1.1 protkollet så det får nog bli RADSEC tills vidare.
- Men RADSEC är ju komplicerat då det fram tills nu krävt att börjar hålla på med PKI och certifikat.
- Nu finns dock ett alternativ när man inte har behov av ”Dynamic Peer Discovery” utan bara kör point-to-point vilket i praktiken alla i Sverige gör: TLS/PSK där den tidigare nyttjade Shared Secret används för att kicka igång TLS sessionen.
- Just nu finns TLS/PSK implementerat i senaste FreeRADIUS samt RadsecProxy samt är på gång till RADIATOR.

Framtida rekommendationer runt nuvarande RADIUS

- Där du själv kontroll (egna nät/AS) kan man kanske köra på ett tag till men rekommendationen om trafik lämnar nät under egen kontroll kommer att vara att köra krypterad trafik antingen via RADSEC i någon form eller det kommande RADIUS 1.1 eller vad det nu kommer att slutligen kallas.
- Finns det patchar till era RADIUS så installera NU, speciellt ni med NPS.

Men hur ska vi göra med alla legacy RADIUS servrar?



SUNET

Breaking News!!!! Radsecproxy på Windows

https://www.dropbox.com/scl/fo/2bew85046oi5xmqbyyoji/AJTD9DoQapvKANo6cLkpCU8?rlkey=hekljb7487om56c3nvr9em2h9&dl=0

https://wiki.geant.org/display/H2eduroam/Running+radsecproxy+on+Windows

SUNET

Ny eduroam policy????

- I samband med ”bodelningen” mellan SWAMID och eduroam är en helt ny policy för eduroam på G.
- IdP:er måste vara anknutna eller kopplade till SUNET och bör vara med i SWAMID.
- Naturligtvis ska europeiska policys och servicedefinitioner följas

- Alla IdP:er kör minst RADSEC. TLS/PSK innan slutet av 2026
- Bara dåliga eller obefintliga infosidor om att sätta upp eduroam duger inte:
  Alla använder onboarding-verktyg (CAT, geteduroam, kommersiell lösning) för den vanliga plattformarna.
- Alla IdP.er ansvarar för att en gång per år meddela kontaktinfo så att det går att få tag i folk.
- Ett nytt verktyg som ersätter meta.eduroam.se måste tas fram och kommer ansvaret att SP:ar underhåller detta att öka.
- Sunets RADIUS servrar behöver migreras till nya och (förhoppningsvis) manageras av NOC:en (diskussioner förs)
- Till detta behövs ett RADIUS Lab samt lite mera folk som jobbar med eduroamsaker. ☺

SUNET

Nytt på eduroam fronten?

- Diskussionerna kring WPA3 och kravet på WPA2 i eduroam går varma
- Trenden att gå över till EAP-TLS (klient cert) ökar med hjälp av geteduroam
- PEAP går kanske inte i graven men med Entra Id blir det inte lika enkelt.
- OpenRoaming via Passpoint börjar känns mera moget.

Länkar till mer info:

- https://www.blastradius.fail
- https://www.inkbridgenetworks.com/blastradius/faq
- https://www.linkedin.com/pulse/escaping-blast-radius-ryan-williams-sr--i3p3e/
- https://datatracker.ietf.org/wg/radext/documents/
- https://radsecproxy.github.io
- https://www.blastradius.fail/pdf/radius.pdf

Frågor funderingar?

SUNET

Sunet dagarna