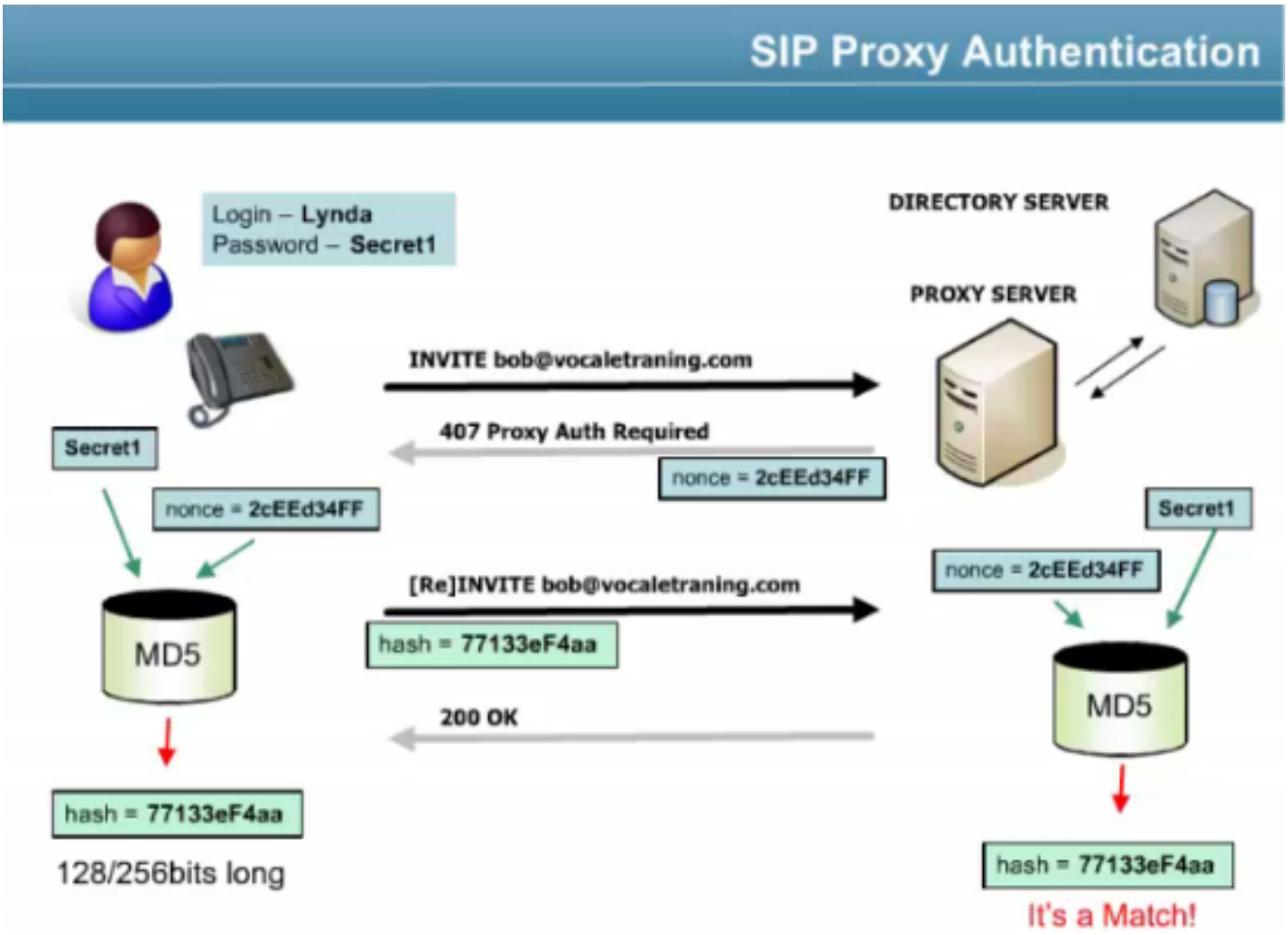
17 .- SIP Security

- Authentication
- Authorization
- Encryption
- Attacks and Responses
- Ethical Hacking

Authentication and Authorization

Proxy Authentication – when user needs to be authenticated proxy responses with a 407, sending a string nonce, user encrypt the password using nonce and MD5, and send back the invite including the hash with the password encrypted, it’s decrypted by the server.
401 unauthorized is a response to register messages
Once authentication has been made, authorization will determine what an authenticated person can do.
128 bit MD5 mechanism is proven to flawed.
SHA-1 at 160 bits is a little more secure but has issues, hence the development of SHA-2 that can produce hash sizes of up to 512 bits.
SHA-3 is currently in development and promises larger hash sizes and no flaws in the algorithm.d is defined in RFC 3262..

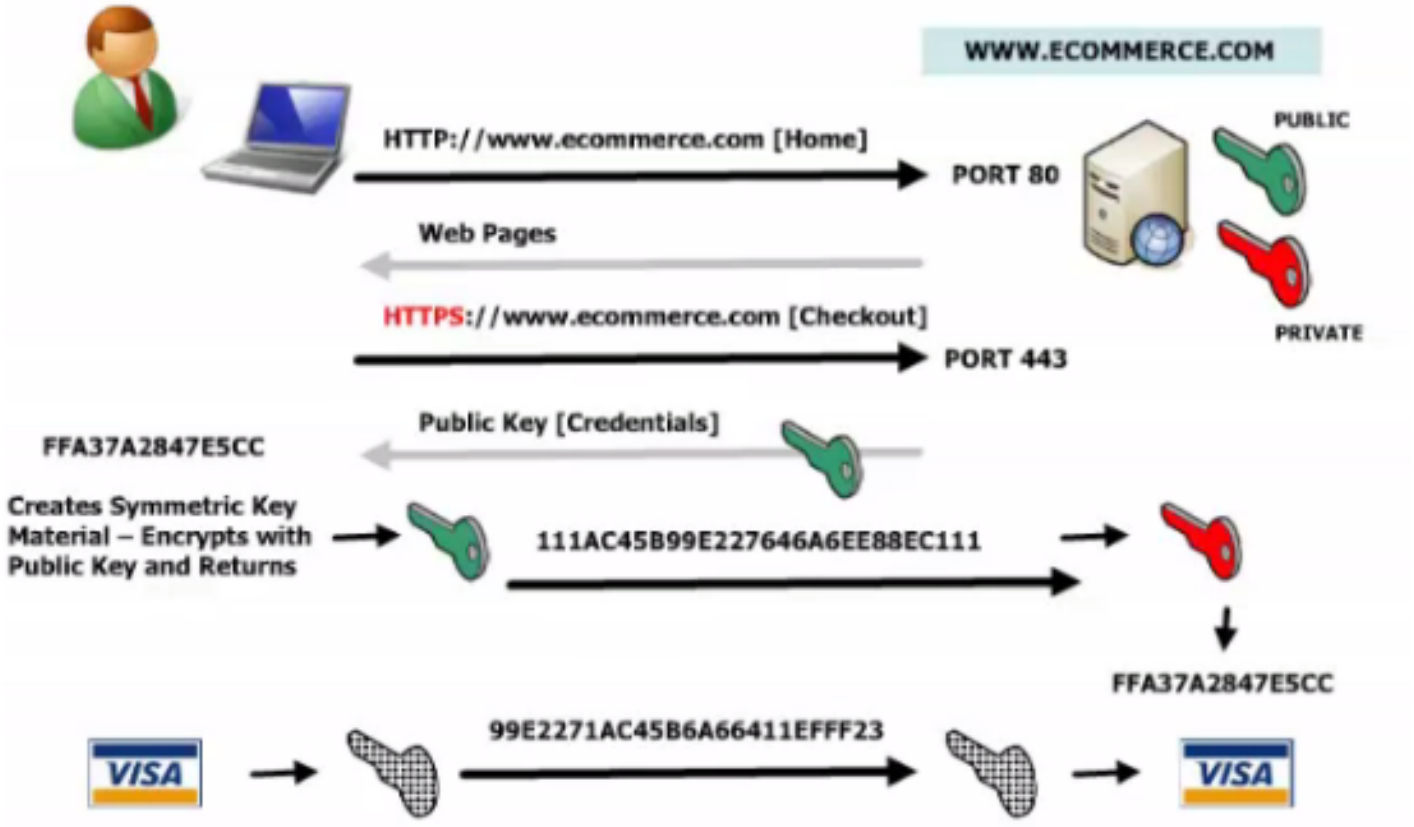


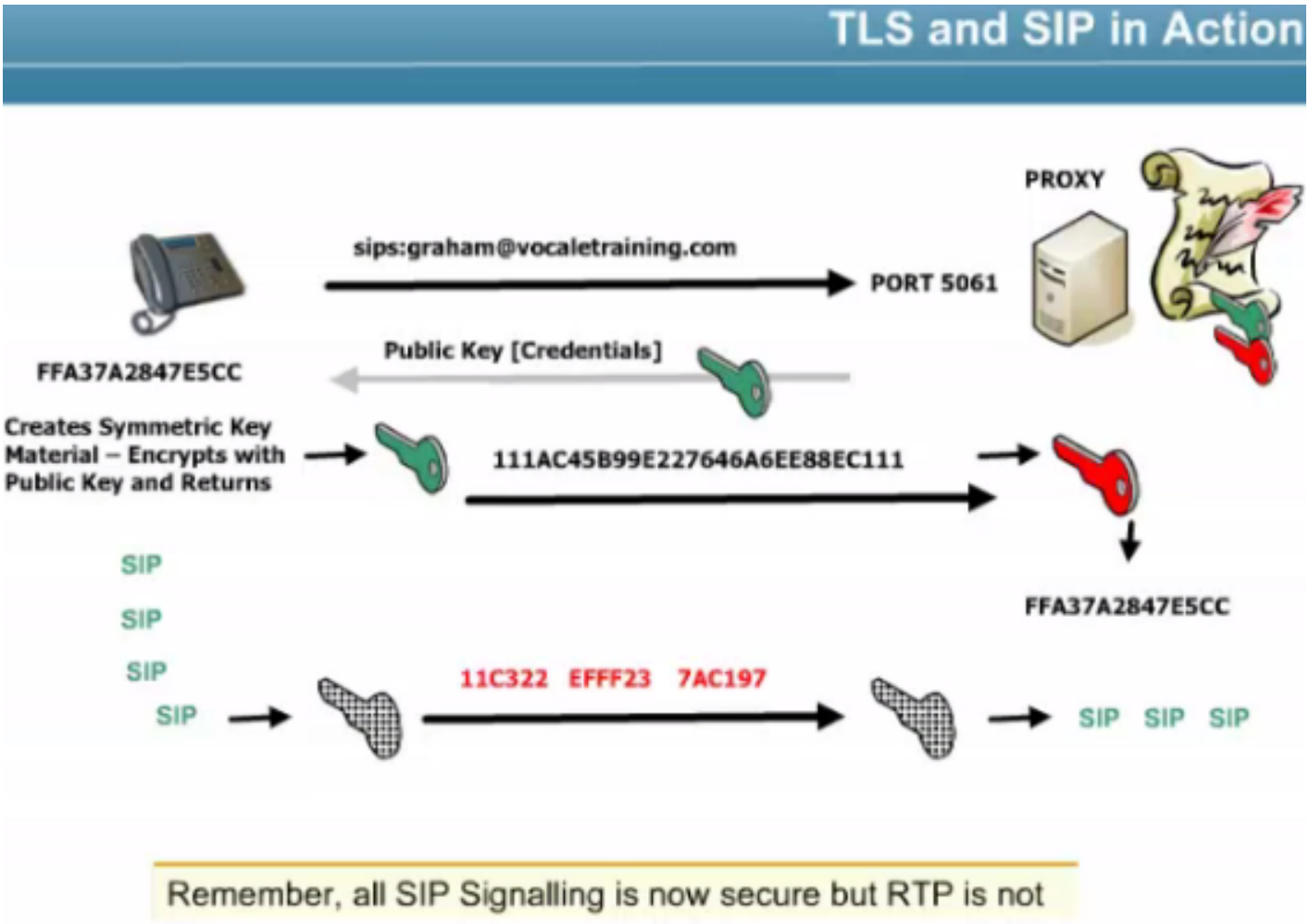
Encryption

There are many types of malicious attacks:

- VoIP interception, modification and replay
- Conversation eavesdropping
- Dictionary attacks
- Telephone number harvesting
- DOS and DDOS attacks
- SPIT and SPAM
- Flood attacks

Certificates and HTTPS





Certificate authorities manages the certificates for some companies.

SIP with TLS only secures signaling, but no audio or other media, SRTP needs to be used to encrypts audio.
SSL (Secure Sockets Layer) first introduced via the Netscape browser, v3 introduced certificate support and SHA-1 support (http, ftp, smtp use it).
TLS has replaced SSL, RFC 5246 TLS 1.2
TLS is based on a shared secret known only to the server and the client, ensure that all SIP signaling messages are encrypted, work on an end to end basis where all systems between the UAs must support TLS or the call will fail. Can work on a hop by hop basis but this requires a new TLS session established between each point on the network.

If security/encryption along the whole path is needed to the end destination the use the sip address type of sips:
Crypto - RFC 4568
RFC 4474 – Caller ID Identity
RFC 6347 and 5763 – DTLS/SRTP
S/MIME (Secure Multipurpose Internet Mail Extensions) – was developed so emails can be encrypted and also digitally signed for proof of sender (only the sender needs a certificate and associated

encryption keys) (for email encryption both sender and recipient require certificates), SIP has adopted S/MIME standard to enable it to encrypt SDP body parts to ensure information privacy, SIP headers are encrypted using TLS.
sRTP can generate encryption keys between two UA without the need of a certificate authority.
IPSec is a heavyweight solution as it requires a PKI to be in place:

- Adds a lot of overhead in the encapsulation process
- Is tended to be implemented in a lot of VPN

Attacks and Responses

Attacks

- DOS: Systems send vast numbers of SIP INVITE to a UA or Server, the system hangs or shuts down, denying service to the users.
- DDOS: Destributed Denial of Service occurs when there are multiple focused external attacks on a SIP gateway.
- Call Pattern Tracking: Find out who is making calls to whom, when and for how long, helps to build up a call profile for a user or even a company.
- ARP Poisoning: Fools using MAC address so host in a conversation thinks they are talking to the correct MAC.
- Intereection/Modification: Occurs when a n unknown 3rd party intercepts SIP signaling, makes changes or even adds to the SIP messages and forwards messages on
- Directory Harvest for SPIT: using whois, dns and google to 'Directory Harvest' telephony numbers that can be used to send unsolicited VoIP messages to SPIT is the IP tellephony variant of SPAM.
- Hacking: Describe attacks on a network server or end device, Hacking starts by 'footprinting' the network to check for vulnerabilities then use tools to exploit them.
- Spoofing: Modify packets so that the recipient thinks you are someone else, can modify MAC, IP, extensions, etc.
- Eaversdropping: Voice capture for playback, building directory numbers for a SPIT attack and also Call PAttern Tracking.
- Capture + Replay: capture for playback.

Response

- Firewalls: Prevent attacks, closing unneeded ports and providing a barrier to TCP/UDP ports scans, apply security policies to control incoming/outgoing traffic.
- SPIS: By using SIPs your sip UA is requesting a Secure Session, preventing capturee spoofing intersection and modification.
- Authentication: If a SIP device is not authenticated with a Proxy or other SIP server then it cannot communicate.
- Authorization: Determines what an autheenticated SIP UA can do, this also prevents rogue SIP devices from accessing services that you want to keep locked down.
- Anti-Harvesting: Ensure that your DNS has secure Zone transfers to known devices.
- VLAN Port Security: ARP poisoning and MAC spoofing is possible as any device can register its MAC address with a LAN switch, use switch port security.

- PKI: Is the foundation of securing all SIP signaling and other network traffic, try to use certificate authority such as VeriSign.
- TLS, SRTP and IPSec: TLS secure sip messages, Seecure RTP media streams, SBC can break end to end security, IPSEC Encrypts all traffic regardless of the tyepe of traffic, it needs PKI.

RFC 4475 - SIP Torture test messagees

Ethical Hacking

- Capture conversation
- SIP vicious
- Cain
- HoverIP - Port scanning
- SIPScan
- SIPtap

NIST National INstitutes of Standards and Technology

- Separate your networks public and private voice and data
- Use an ALG firewall or SBC
- STUN: doesnt work with symmetric NAT
- TURN: works but is limited to a single UA behind NAT
- ICE: is good but can take time to call setup and not all deevices are compatible with ICE yet
- UpnP : not good with multiple NAT but fine for home use

Use Strong autheentication such as SHA-1 or MD5

Use TLS end to end encryption or even an IPSec connection.

Dont use softphone in a security sensitive network as the PC runs on usually vulnerable OS attack.

Revision #2
Created 7 May 2023 02:22:50 by Cesar Gzz
Updated 7 May 2023 05:19:27 by Cesar Gzz