Cain and Abel

Minsoo Jin & Alex Kornilenko

Overview

LSA Secret - Local Security Authority

-stores important data like windows local login passwords

-stored in registry at HKEY_LOCAL_MACHINE/Security/Policy/Secrets

-need system privilege

-windows local login passwords use LM/NTLM hash (and stored)

LM/NTLM Hash

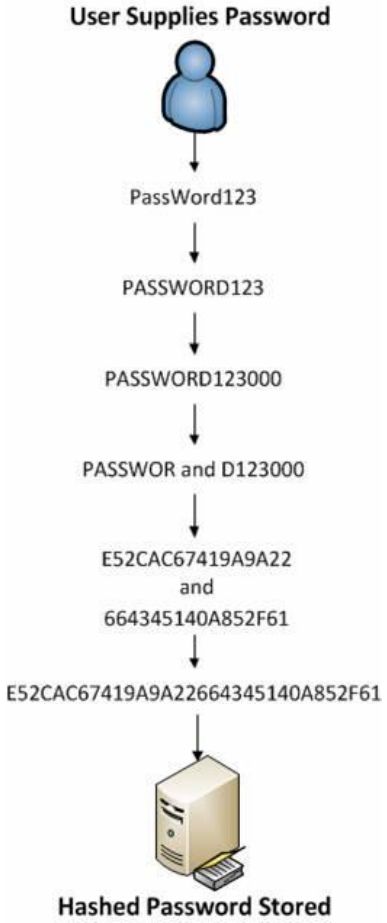
-Microsoft security protocol (Microsoft's hash functions basically)

-stored in c:₩windows₩system32₩config₩SAM

-file is encrypted and locked when Windows is running, but Cain can bypass the lock and decrypt the SAM file to get LM/NTLM hashes

LM Hash (Win98, 2000, XP)

-based on DES
-only supports up to 14 characters
-passwords longer than 7 characters are divided and hashed separately
-password is converted into all uppercase letters in the first process of hash



NTLM Hash (Win7, Vista, 8+)

-based on MD4

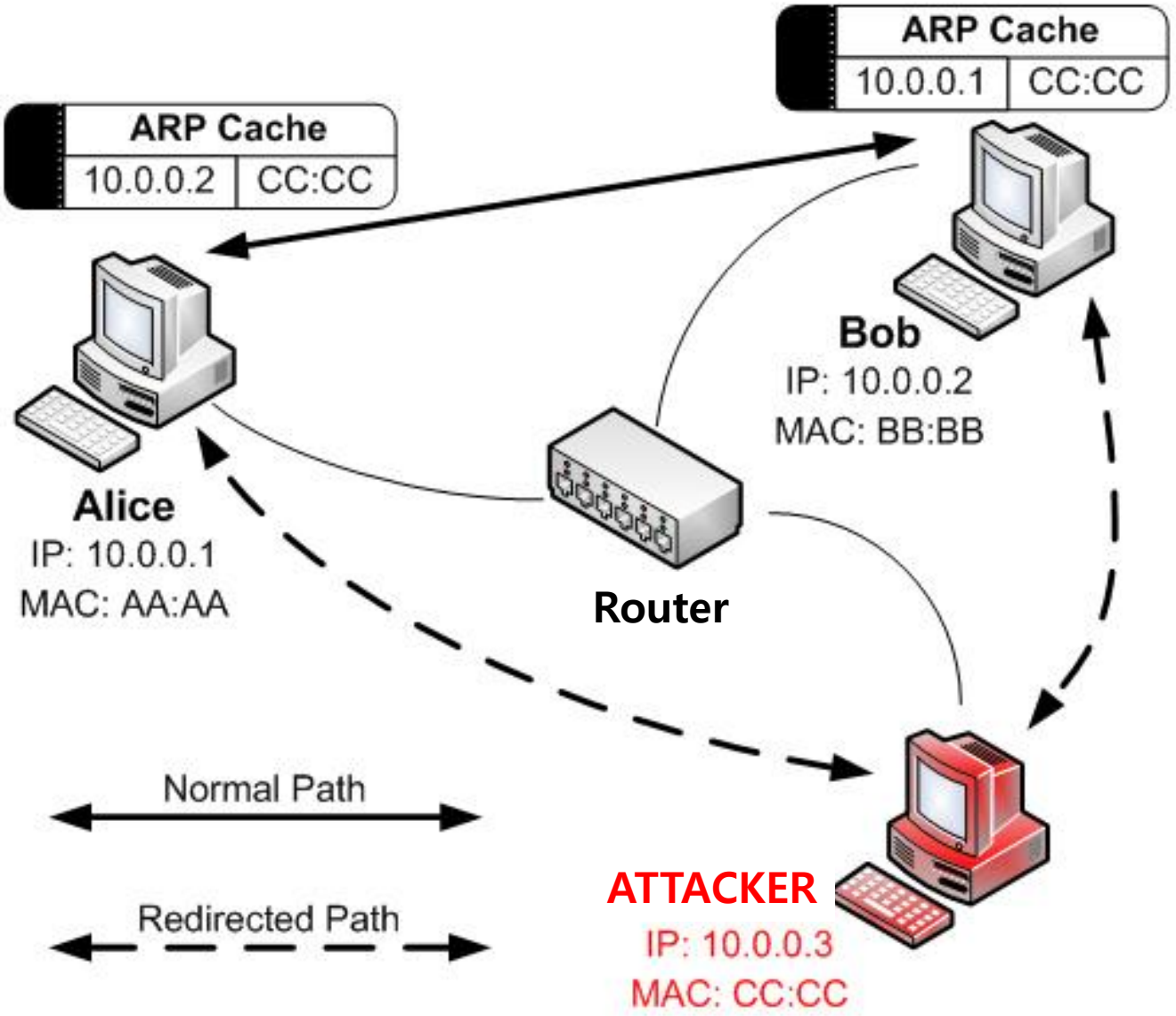
-no maximum length limit

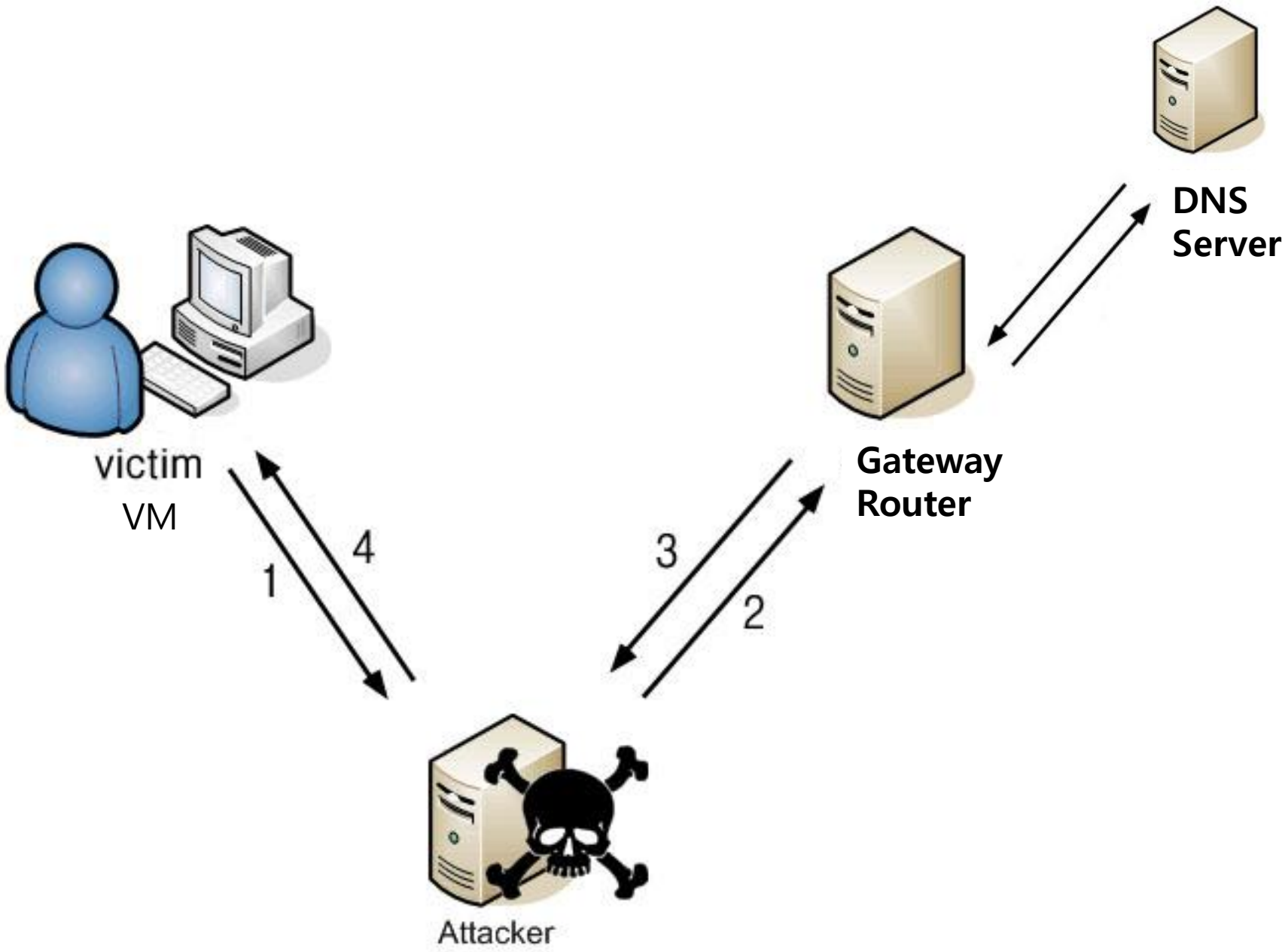
-more secure than LM hash

-but Windows does not use salting

-vulnerable to rainbow table attacks

ARP Cache Poisoning/DNS Spoofing




DNS
Server
victim
VM
Gateway
Router
1
2
3
4
Attacker

Bypassing HTTPS