DH GROUP BASED 2nd FACTOR AUTHENTICATION FOR ACCESS NETWORKS

INVENTOR:

MASSIMILIANO PALA

Description

Identities and Cryptography are always evolving. To manage uncertainty, one of the possible option for Access Network is to deploy 2nd Factor Authentication. When combined with identities (e.g., in the form of certificates or otherwise verifiable format), the use of a 2FA together with a trusted source of time can lower the risk of device cloning and possible weakness in the public-key algorithms used.

Background

Access Networks use, today, a single set of credentials. This can lead, if not properly managed, to theft of service, credentials sharing, and/or device cloning.

This invention changes the status quo and introduces a mechanism to leverage existing (or new) 2nd Factor Authentication such as TOTP or HOTP that are not affected by potential algorithmic issues with public key cryptography.

For a second-factor authentication to be usable in this form, entities must have access to a trusted (or shared) source of time.

Abstract

After being successfully authenticated and registered to the Access Network for the first time, the device establishes a series of secrets with the Access Network by using secure Key Exchange mechanisms (e.g., traditional and elliptic-curve key exchange algorithms or newer post-quantum Key Encapsulation Mechanisms)

By combining these secrets with secure time information (from the network and/or internal clock), the device can start using the Time-based One-time Password Algorithm (TOTP) as specified in RFC 6238 and HMAC-based One-time Password algorithm (HOTP) as specified in RFC 4226 for authenticating entities.

Access Networks can now leverage the use of a 2nd Factor Authentication when admitting new entities to the network to mitigate possible issues with public-key cryptography security.

For the Time considerations, we notice that in many environments time is provided as part of the network services/protocols. This is true for DOCSIS and 5G but not for WiFi. When that information is not readily available, the use of protocols such as Precision Time Protocol or DOCSIS Time Protocol can help addressing the availability and/or synchronization of time information across the entities.

NOVEL APPROACH: In this invention, time is not a concept related to the current time, but it is an abstract concept. Indeed, for the 2nd Factor Authentication to properly work, the entities have to agree on the source of time, but the absolute value of the time itself is irrelevant. This consideration allow us to minimize the requirement for the precision of the time information.

NOVEL APPROACH: In this invention we leverage the 2nd Factor Authentication that uses, to calculate the output, time information together with exchanged symmetric secrets. The output of the 2nd Factor Authentication can then be used in lieu of NONCES in modern protocols. This change allow us to keep the randomness required for NONCEs and, at the same time, allow us to include an authentication that is not based on public key cryptography.

NOVEL APPROACH: When the 2nd Factor Auth is enabled, it is possible to leverage it to generate ephemeral encryption keys based on the output of the TOPT or HOTP. Because of this capability, it is possible to dynamically encrypt data before it is transferred to the device, even when the communication channel is not encrypted. For example, when a Firmware upgrade is sent to the device, the device can provide

Idea Development Comments (Please provide further details if you selected Other, and provide the project if you selected Current Project Work or Co-Innovation in the previous question

While looking at possible alternatives for how to provide secure authentications in the event of public-key failures, I thought about a possible source of secrets that might not be affected by quantum. I already investigated alternatives ways to combine symmetric-based identity with public-key identities (see the linked applications). In this work, we expand our coverage of options for how to leverage/use symmetric secrets to augment Access Network security.
The use of Hash-Based or One-Time tokens is novel in that it requires a good source of time. The synergies with the linked applications about secure time delivery (and the PKI Node Innovation Project that we plan to present in November) makes this a very interesting option for operators to enable 2nd Factor Auth.

PATIENT IDEA

Oct 15, 2021

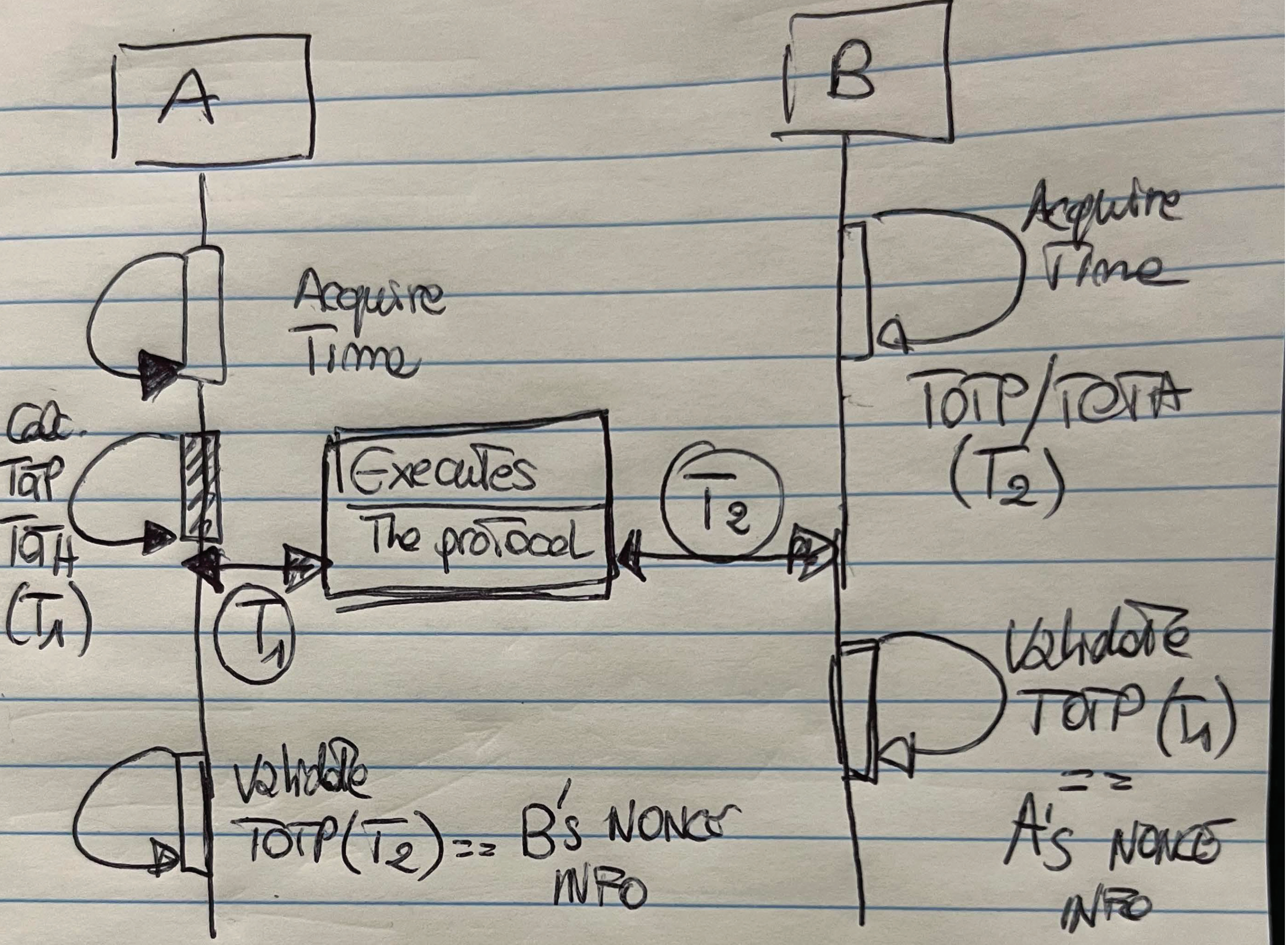
Max Pala

- GROUP BASED 2ND FACTOR AUTHENTICATION / TIME BASED AUTH
  - Use ECDH / DA to establish the "MASTER" secret
  - Uses the "MASTER" secret together with TOKEN based authenticators (STANDARD)

Devices can use Diffie-Hellman like algorithms to establish the MASTER secret(s) for the Token-Based Auth.

→ This removes the centralized generation of secrets

→ Can provide Quantum Resistance based on the fact that this is hash-based and


A
B
Acquire Time
Acquire Time
Calc. TOTP TOTA (T1)
Executes The protocol
T1
T2
TOTP/TOTA (T2)
Validate TOTP(T1) == A's NONCE INFO
Validate TOTP(T2) == B's NONCE INFO