REVOCATION OF COMPROMISED SIM SECRETS VIA OCSP RESPONSES AND CRLs

INVENTOR:

MASSIMILIANO PALA

DESCRIPTION:

OVERVIEW:

In 3GPP networks, the authentication messages are routed to the Home network for validation - but until the home services have established if the credentials are active and the authentication is performed correctly, the network cannot know that these credentials are to be rejected.

This results in possible abuse of the system - both the guest network (receiving the request) and the home network (processing the request).

Today there is no public-key mechanism to revoke secrets from a SIM.

This invention extends the use of OCSP responses to include SIM's identifiers (IMSI) that can be leveraged as serial numbers of certificates - thus aligning the validation of X.509 credentials (typically used by Cable Networks) and SIM credentials (typically used in 3GPP Networks).

PREAMBLE:

This invention provides a mechanism to CONVERGE credentials/identity validity checking across 3GPP and Broadband Network independently of the type of credentials used (an X.509 certificate or a SIM Card).

In this setting, the Operator is identified by a CA Certificate or an End-Entity certificate. In addition to this, the Operator has an OCSP responder certificate to sign OCSP responses and/or a CRL signer certificate to sign the IMSI Revocation Lists (IRLs).

THE INVENTION:

In order to provide the possibility to validate the revocation status of a credential connected to a SIM without the need to perform an authentication or even contacting the home network, IRLs and/or OCSP responses can provide the authenticated source of information that can be used by 3rd parties (Roaming / Convergence).

[IRL Revocation Checking]

In order to check the validity of an IMSI, a client application (e.g., a network element like an MME or an eNodeB/gNodeB) retrieves (or it is given) the authoritative IRL signed by the operator's CRL signer's certificate. The client first validates the signature and the chain of associated certificates to be trusted. After that, the client evaluates the list of revoked IMSIs when it needs to evaluate the revocation status of a specific IMSI.

[OCSP Revocation Checking]

In order to check the validity of an IMSI, a client application (e.g., a network element like an MME or an eNodeB/gNodeB) queries the authoritative OCSP for the operator's credentials (this can be provided by signing the URL with the operator's A certificate). The OCSP responder checks the status of the specified IMSI, and returns a "Revoked" if the credentials have been reported not valid, "Good" if no indication of revocation information is available at the OCSP responder, and "Unknown" if the request is for an IMSI not known by / not assigned to the operator.

[COMMON FLOW]

After evaluating the IRL or the OCSP response and the chain of certificates (to a trusted anchor), the client can proceed allowing the communication (if not revoked) or rejecting the communication (without having to send the request to the HHS element).

THE WORKFLOW:

In this invention, an entity (e.g., a eNodeB, a gNodeB, an MME, etc.) receives a message (e.g., a request to attach to the network) from a device using a specified IMSI.

[IRL Revocation Checking]

When a IRL is available to the entity and/or it can be retrieved (e.g., via an HTTP request or other transport mechanisms), the entity proceeds to check if the IMSI to be check is present among the ones contained in a IRL. If a match is found, then the IMSI is to be considered revoked.

[OCSP Revocation Checking]

The IMSI value can be directly encoded in the field of the OCSP request that normally holds the serial number of the target certificate. The target CA identifier is calculated over the specific operator's OCSP responder certificate or over the specific operator's OCSP responder Issuer's Certificate.

The receiving OCSP responder checks that the request is for itself (by leveraging the CA identifier in the OCSP request) and looks up the status of the identified IMSI (either locally or by using additional remote resources like a remote database or a search service).

Alternatively, the OCSP responder can access the IMSI Revocation List (or IRL) that has the same structure of a X.509 CRL and where the serial numbers of the revoked IMSI are listed (one for each crlEntry in the IRL). The IRL is signed by the specific operator's CA or by the specific operator's EE certificate.

The OCSP responder builds the response and uses the "good" status if no revocation information is available to the responder. The OCSP responder provides the "unknown" status if the request

is not for an IMSI associated with the identified operator. The OCSP responder provides the "revoked" status if the request is for an IMSI that is marked as revoked.

OPTIONAL FEATURES:

[OCSP RELATED]

Optionally, for privacy purposes, instead of using the IMSI value in the serial number field, the IMSI value is first hashed by using a cryptographically secure hash function (e.g., typically SHA-256 or better).

Optionally, to address rainbow-tables attacks, instead of using the IMSI value in the serial number field, the IMSI value is first hashed together with the NONCE value that is carried inside the request.

Optionally, to provide a more efficient option to address rainbow-tables attacks, instead of using the IMSI value in the serial number field, the IMSI value is encrypted with the public key of the OCSP server's certificate. This option might not be available if the public-key algorithm of the OCSP's certificate does not allow for encryption.

Optionally, when encryption is not possible, instead of encrypting the IMSI with the OCSP server Certificate's key, the IMSI value is encrypted with an already shared key among the parties (e.g., a public key or a symmetric one).

[IRL RELATED]

All of the above examples also apply to the serial number fields in the IRLs.

Background

In order to support convergence for different types of access networks, a secure revocation system that can provide distributed revocation checking is paramount.
Specifically, a revocation system that can provide information related to different types of credentials across access networks can improve the efficiency of the network and allow for efficient credentials revocation checking in multi-tenant systems (i.e., convergence across operators and types of access networks).

Abstract

Convergence requires many building blocks. One of the needed building blocks is the possibility to validate the status of different types of identities across different types of access networks. This invention provides the possibility to leverage the revocation system used within the broadband industry to provide efficient revocation checking that allows both type of identities (i.e., the broadband one and the 3gpp one) to be securely validated.