Token Binding Protocol I-D Changes Since IETF 94

Andrei Popov, Microsoft Corp.

TokenBindingID.tokenbinding_type

TB types are contextual: the same binding can be Provided from the RP's perspective and Referred from the IDP's perspective.

1. IDP binds a token to the Referred TB ID;
2. RP attempts to binary-match the Referred TB ID in the token and the Provided TB ID established with the client;
3. The first byte (tokenbinding_type) differs, so the RP rejects the token.

To avoid this issue, the latest I-D moves tokenbinding_type from TokenBindingID struct to the TokenBinding struct:

struct {

TokenBindingType tokenbinding_type;

TokenBindingID tokenbindingid;

opaque signature<0..2^16-1>;// Signature over the exported keying material value

Extension extensions<0..2^16-1>;

} TokenBinding;

Specified TokenBinding.signature Format

- When an rsa2048_pkcs1.5 or rsa2048_pss key is used, TokenBinding.signature contains the signature generated using, respectively, the RSASSA-PKCS1-v1_5 or RSASSA-PSS signature scheme defined in [RFC3447]. RSAPublicKey.modulus and RSAPublicKey.publicexponent contain the length-prefixed modulus and exponent of the RSA public key represented in big-endian format.
- When an ecdsap256 key is used, TokenBinding.signature contains a pair of integers, R followed by S, as defined in [ANSI.X9-62.2005]. R and S are encoded in big-endian format. ECPoint.point contains the X coordinate followed by the Y coordinate. The X and Y coordinates are unsigned integers encoded in big-endian format. Future specifications may define Token Binding keys using other elliptic curves with their corresponding signature and point formats.

New Security Considerations

- A server can use tokens and Token Binding IDs to track clients. Client applications that automatically limit the lifetime of tokens to maintain user privacy SHOULD apply the same validity time limits to Token Binding keys.
- In addition to EMS, renegotiation indication extension is now listed as a prerequisite for Token Binding (only for TLS 1.2 and older TLS versions).
- The manner in which a token is bound to the TLS layer is application-defined and beyond the scope of TBPROTO. However, the resulting bound token needs to be integrity-protected, so that an attacker cannot remove the binding or substitute a Token Binding ID of their choice without detection.

New IANA Registration

- The latest I-D adds a registration for the "EXPORTER-Token-Binding“ value in the TLS Exporter Label Registry.

Links And Contact Information

- TLS Extension for Token Binding Negotiation: https://datatracker.ietf.org/doc/draft-ietf-tokbind-negotiation/
- The Token Binding Protocol Version 1.0: https://datatracker.ietf.org/doc/draft-ietf-tokbind-protocol/
- Token Binding over HTTP: https://datatracker.ietf.org/doc/draft-ietf-tokbind-https/
- GitHub: https://github.com/TokenBinding/Internet-Drafts

- Dirk Balfanz balfanz@google.com
- Andrei Popov andreipo@microsoft.com

The Token Binding Protocol Message Format

```
struct {
    ExtensionType extension_type;
    opaque extension_data<0..2^16-1>;
} Extension;
struct {
    TokenBindingType tokenbinding_type;
    TokenBindingID tokenbindingid;
    opaque signature<0..2^16-1>;// Signature over the exported keying material value
    Extension extensions<0..2^16-1>;
} TokenBinding;
struct {
    TokenBinding tokenbindings<0..2^16-1>;
} TokenBindingMessage;
```

Token Binding ID Format

```
struct {
    TokenBindingKeyParameters key_parameters;
    select (key_parameters) {
        case rsa2048_pkcs1.5:
        case rsa2048_pss:
            RSAPublicKey rsapubkey;
        case ecdsap256:
            ECPoint point;
    }
} TokenBindingID;
```

- Provided_token_binding is used to establish a Token Binding when connecting to a server.
- Referred_token_binding is used when requesting tokens to be presented to a different server.