draft-popov-tokbind-negotiation-00

Andrei Popov, Microsoft Corp.

TLS Extension for Token Binding Protocol Negotiation

- In order to use the Token Binding protocol, the client and server need to agree on the Token Binding protocol version and the parameters (signature and hash algorithm, length) of the Token Binding key.
- draft-ietf-tokbind-protocol-00 used ALPN IDs to negotiate Token Binding parameters.
- In Dallas, Tokbind WG reached consensus that a new TLS extension should be defined for Token Binding parameters negotiation, instead of using ALPN.
- draft-popov-tokbind-negotiation-00 specifies the “token_binding” TLS extension to negotiate Token Binding parameters without introducing additional network round-trips.

Token Binding Negotiation Client Hello Extension

```
struct {
    uint8 major;
    uint8 minor;
} ProtocolVersion;
enum {
    rsa2048_pkcs1.5_sha256(0), rsa2048_pss_sha256(1), ecdsap256_sha256(2), (255)
} TokenBindingKeyParameters;
struct {
    ProtocolVersion token_binding_version;
    TokenBindingKeyParameters key_parameters_list<2..2^16-1>
} TokenBindingParameters;
```

- "token_binding_version" indicates the supported version of the Token Binding protocol. Prototype implementations of Token Binding drafts can indicate support of a specific draft version, e.g. {0, 0} or {0, 1}.
- "key_parameters_list" contains the list of identifiers of the Token Binding key parameters supported by the client, in descending order of preference.

Token Binding Negotiation Server Hello Extension

- The server uses the "token_binding" TLS extension to indicate support for the Token Binding protocol version offered by the client and to select key parameters.
- The server that supports Token Binding and receives a client hello message containing the "token_binding" extension, will include the "token_binding" extension in the server hello if all of the following conditions are satisfied:

1. The server supports the Token Binding protocol version offered by the client.
2. The server finds acceptable Token Binding key parameters on the client's list.
3. The server is also negotiating Extended Master Secret TLS extension.

- Same structure as the client-side token_binding extension.
- "token_binding_version" echos the Token Binding protocol version advertised by the client.
- "key_parameters_list" contains exactly one Token Binding key parameters identifier selected by the server from the client's list.

Negotiating Token Binding Protocol Version and Key Parameters

- The server MUST only select a Token Binding key parameters identifier that the client offered.
- The server SHOULD select the server’s most highly preferred key parameters identifier which is also advertised by the client.
- In the event that the server supports none of the key parameters that the client advertises, then the server MUST NOT include "token_binding" extension in the server hello.
- The client receiving the "token_binding" extension MUST terminate the handshake with a fatal "unsupported_extension" alert if any of the following conditions are true:

1. The client did not include the "token_binding" extension in the client hello.
2. "token_binding_version" does not match the Token Binding protocol version advertised by the client.
3. "key_parameters_list" includes more than one Token Binding key parameters identifier.
4. "key_parameters_list" includes an identifier that was not advertised by the client.
5. Extended Master Secret is not negotiated.

Open Issue

- A client can negotiate e.g. ecdsap256_sha256 with the IDP and rsa2048_pkcs1.5_sha256 with the RP.
- In this case, the IDP will receive “referred” binding with rsa2048_pkcs1.5_sha256.
- If the IDP can’t handle rsa2048_pkcs1.5_sha256, it will issue an unbound token.
- Question: should we allow the server’s token_binding extension to contain multiple key parameter IDs, so that the client would not send “referred” bindings with key parameters that the IDP does not support?

Links And Contact Information

- TLS Extension for Token Binding Negotiation: https://tools.ietf.org/html/draft-popov-tokbind-negotiation-00
- The Token Binding Protocol Version 1.0: https://tools.ietf.org/html/draft-ietf-tokbind-protocol-01
- Token Binding over HTTP: https://tools.ietf.org/html/draft-ietf-tokbind-https-01
- GitHub: https://github.com/TokenBinding/Internet-Drafts

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