HTTPS Token Binding with TLS Terminating Reverse Proxies

draft-ietf-tokbind-ttrp-05

IETF 102

~~San Francisco~~

Montreal

July 2018

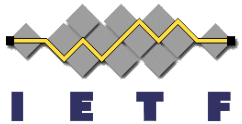
Brian Campbell

~~Problem~~ Opportunity Statement

- HTTPS application deployments often have TLS ‘terminated’ by a reverse proxy in front of the actual application
  - products, open source, as-a-services
- For general applications in such deployments to take advantage of token binding, some information needs to be communicated from the TLS layer to the application
- In the absence of a standard, different implementations will do it differently (or not do it at all)
- Alarming shortage of acronyms
  - TLS Terminating Reverse Proxy -> TTRP

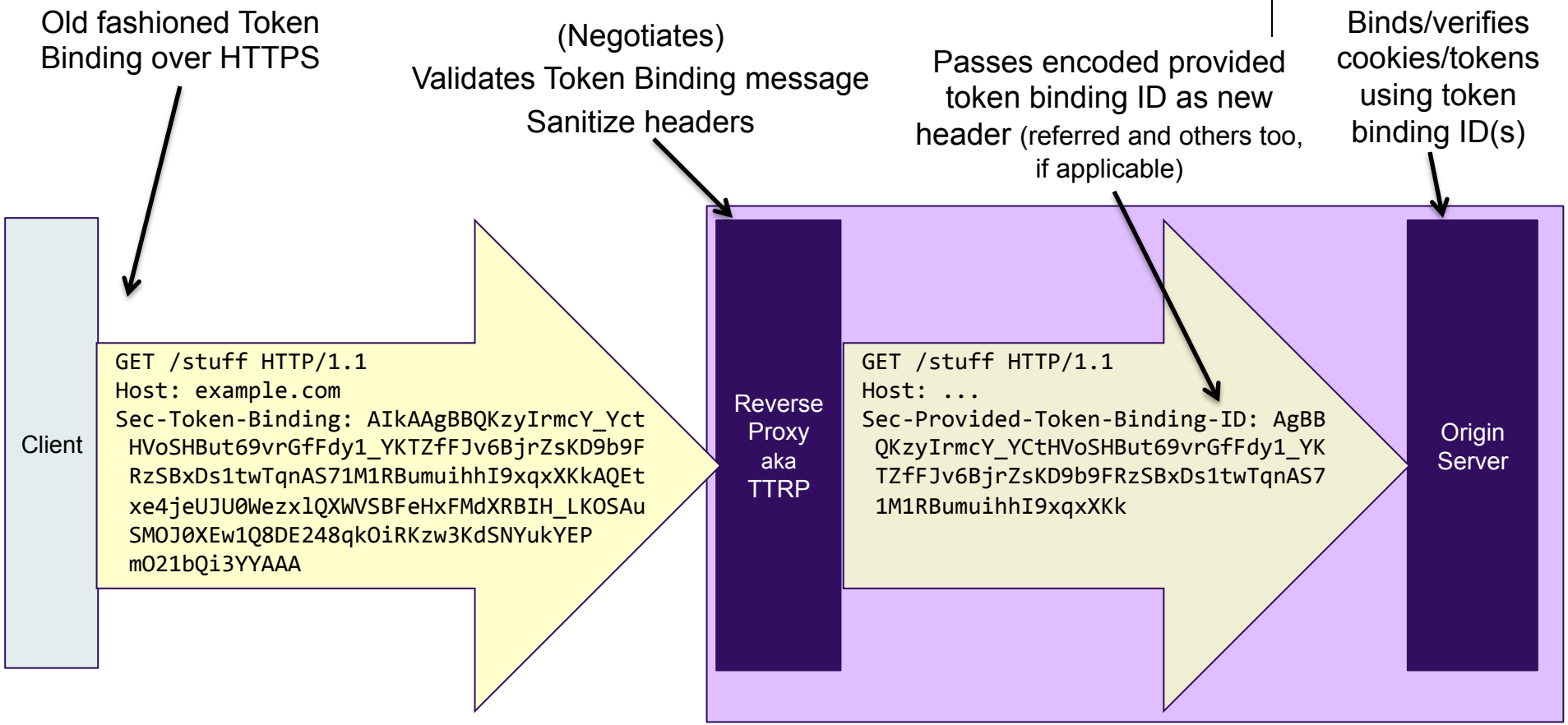
Solution Overview

draft-ietf-tokbind-ttrp-05



- Define HTTP headers that enable a TTRP and backend server to function together as a single logical server side deployment of HTTPS Token Binding
- TTRP validates the TokenBindingMessage from the `Sec-Token-Binding` header and removes it from dispatched request
- `Sec-Provided-Token-Binding-ID` header with base64url encoded provided TokenBindingID added to dispatched request
- `Sec-Referred-Token-Binding-ID` header with encoded referred TokenBindingID added to dispatched request (if applicable)
- `Sec-Other-Token-Binding-ID` header with comma-separated list of additional Token Bindings as hex(type) | “.” | base64url(ID) added to dispatched request (if applicable)
- Trust between the TTRP and backend server
- TTRP required to sanitize headers

Different view of the Overview



Happenings since London

- Reviews
- Drafts -04 & -05 published
- Add a TLS Versions and Best Practices section with BCP195 and also mention of ietf-tokbind-tls13 and ietf-tls-tls13
- Use the HEXDIG core ABNF rule for EncodedTokenBindingType and mention case-insensitivity in the text (rather than spelling it out in ABNF)
- Example with Sec-Other-Token-Binding-ID added
- Editorial updates
- Add to the Acknowledgements and remove the 'and others' bit

IETF 101, London

Some Design Motivation & Rational

- Make the common and simple usage simple (especially for the web application developer) while making the other possible (as requested)
  - The overwhelming vast majority of the time the provided_token_binding(0) is going to be the only Token Binding in an HTTP request
    - “Token Binding protocol implementations SHOULD make Token Binding IDs available to the application as opaque byte sequences” - TBPROTO
    - `Sec-Provided-Token-Binding-ID: … the ID …`
  - referred_token_binding(1) is a distant second and for a somewhat specialized audience
    - `Sec-Referred-Token-Binding-ID: … the ID …`
  - 254 other currently undefined token binding types
    - “An implementation MUST ignore any unknown Token Binding types.” - TBPROTO
    - “the TokenBindingMessage MAY contain other TokenBinding structures. This is use case-specific, and such use cases are outside the scope of this specification.”- HTTPSTB

Next Steps Post Montreal...

As TBNEGO, TBPROTO & HTTPTB go to RFC, progress this to WGLC, s'il vous plaît?