

SIP Authentication and Integrity

draft-undryer-sip-digest-00.txt

James Undery - james@ubiquity.net

Why more integrity?

HTTP Digest only protect the Request URI and body

REGISTER relies on To, From and Contact headers

Future extensions rely on header X

Why a new scheme

The choices

- Extend Digest scheme using qop parameter
 - Backwardly compatible
 - step-down attack

- New scheme
 - Clean slate to incorporate changes from RFC 2069 to RFC 2617
 - Can't remove Basic and Digest :-)

Authentication-Info

Why use it?

- ❑ To authenticate server to client!
- ❑ Prevent unnecessary 401s

What's wrong?

- ❑ HTTP form doesn't quite work

What could be better?

- ❑ Proxy-Authentication-Info
- ❑ Cover qop parameter