GNAP

IETF 113 Hackathon

Aaron Parecki and Justin Richer
What is GNAP?

- Delegation protocol (like OAuth)
- Built on lessons learned from many years of OAuth deployments
- Minimizes security exposures through front-channel
- Flexible data access request for APIs and subject information
What was our focus?

- Protect requests with HTTP Signatures
- Make requests for tokens
- User interaction at AS
- Get usable access tokens
What did we build?

- **New code:**
  - PHP CLI & Web Client
  - SPA Client (JavaScript)
- **Significant Updates to:**
  - Java Web Client
  - Java Authorization Server
- **Leveraged existing libraries and standards**
  - Especially for HTTP structured fields and crypto primitives
What did we learn?

- HTTP Message Signatures is complex to do from scratch
  - Requires crypto, structured fields, HTTP message manipulation, etc.
  - Surprising fiddly bits (e.g., order of parameter fields)
  - Transparent if available within an HTTP library, but we aren’t there yet
- It’s actually possible to implement GNAP clients from scratch in relatively short order, if you already have a signing mechanism
- I still hate JavaScript
Improving the Specs

- **GNAP**
  - Need a way to communicate proof parameters (signature alg, digest alg, etc)
  - Polling uses an empty POST, why not GET?
  - Need to clarify grant lifecycle operations (already a set of open issues)
  - Need to reference hash methods from existing registry (open issue)
  - Need to clarify what the front-channel hash protects (probably with diagrams)
  - Some potential protocol cleanup/bikeshedding (“finish” vs “nonce”, “user_code.code”, etc)

- **HTTP Structured Values**
  - Would benefit from an implementer’s quickstart guide

- **HTTP Message Signatures**
  - Parameter order needs to be stable
  - Some library support, but more is needed (ours was all by hand)
Web-Based Java Client
Web-based Java Client - Configuration
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant Endpoint</td>
<td><a href="https://gnap-as.herokuapp.com/api/as/transaction">https://gnap-as.herokuapp.com/api/as/transaction</a></td>
</tr>
<tr>
<td>Continuation Token</td>
<td>bD1KntPzcL1iE32zBR9mJ5ziAgS/JHXTTThmLgyK8BazMJSjvWiykdmWcrQoJNSx</td>
</tr>
<tr>
<td>Interaction URL</td>
<td><a href="https://gnap-as.herokuapp.com/api/as/interact/3oUG3WzAX">https://gnap-as.herokuapp.com/api/as/interact/3oUG3WzAX</a></td>
</tr>
</tbody>
</table>

Web-based Java Client - Grant Started
"Client"

Access:
- foo
- bar
- baz
- photo-api

[Approve]  [Deny]
Web-based Java Client - Grant Completed

Grant Endpoint: https://gnap-as.herokuapp.com/api/as/transaction
Token: EV4dq5e25tBwul4g6U6Khinx2t1AG6CLaCTZQAVsdcmDoEs3zdZLORcvr5s06kf
Continuation Token: HelyHgToto6Jr9SBJfJvRRJdJOBlWrXw575EJrKXqXoGfnOwSY15P5JavkKak4
Web-based Java Client - In the Background
JavaScript SPA Client - Configuration
### Client

**Access:**
- foo
- bar
- baz
- photo-api

**Subject Identifiers:**
- email
- opaque

---

JavaScript SPA Client - Java AS Approval Page
<table>
<thead>
<tr>
<th><strong>Grant Endpoint</strong></th>
<th><a href="https://gnap-as.herokuapp.com/api/as/transaction">https://gnap-as.herokuapp.com/api/as/transaction</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Awaiting Callback</strong></td>
<td>dIlhZeitbTl9R2UxgCRbfvfBdvjp44fXqz1V3h6WIFfh5tq2sgH1fbKtAxlyYl</td>
</tr>
<tr>
<td><strong>Continue Token</strong></td>
<td>F0ETJacXsFJ4FtNQGGe23nOGCyoX004R2Vr4prpmpLHjtfSmC0aHyYGzSxzEH7M</td>
</tr>
<tr>
<td><strong>Access Token</strong></td>
<td><a href="mailto:user@example.com">user@example.com</a></td>
</tr>
<tr>
<td><strong>Opaque Identifier</strong></td>
<td>650D53FB0C7236D1C569F17D8F4A980D</td>
</tr>
</tbody>
</table>
Web-Based PHP Client
PHP Web Client - Start

Log In
Response from AS:

Array
(
    [instance_id] => 6237014a4e9880220ba6d078
    [interact] => Array
        (
            [redirect] => https://gnap-as.herokuapp.com/api/as/interact/oChg5I2jGr
            [finish] => 6HoKva5lcICKX7X9R27c
        )
    [continue] => Array
        (
            [uri] => https://gnap-as.herokuapp.com/api/as/transaction/continue
            [access_token] => Array
                (
                    [value] => Or2r38cJHUeo8RvAgh6Qlnc05BO63fG0mYzWv9emtx19gaRXIlr2oS4eOd81juiA
                )
        )
)

Continue to AS
A Sample App

Access:
  • api

Subject Identifiers:
  • iss_sub
  • opaque

Approve  Deny
PHP Web Client - Response from AS:

Array
(
    [access_token] => Array
        (
            [value] => OSYIlZ98t3lpPa53wqfRChb4LiVrjc0najWBrjScML6dcmxw910U32tP7qGq86
            [access] => Array
                (0) => Array
                    (
                        [type] => api
                    )
        )
    [subject] => Array
        (
            [sub_ids] => Array
                (0) => Array
                    (
                        [sub] => 04A0E49D47B6A63C1659A6320C2F1B5
                        [format] => ias_sub
                        [ias] => https://gnap-as.herokuapp.com
                    )
                (1) => Array
                    (
                        [format] => opaque
                        [id] => 04A0E49D47B6A63C1659A6320C2F1B5
                    )
            [updated_at] => 2022-03-20T12:20:51.826Z
        )
    [continue] => Array
        (
            [uri] => https://gnap-as.herokuapp.com/api/as/transaction/continue
            [access_token] => Array
                (value] => SKqg2tDCXfdJ1/pRicuhLD1wUUXznUPervpaxKpwehjUDbV2jQq2qMQQQ3L6891l4
        )
)
Logged In

Subject ID: 04A0EA9D7EBCA63C1659A68320C2F1B5

Access Token:

Array
{
    [value] => OSYZL19sH3zlpqPa5JwqfRcb4LisiVRjc5nsjNB1rScML6cismxw9iOU32Ft7qGqB6
    [access] => Array
        {
            [0] => Array
                {
                    [type] => api
                }
        }
    }

Log Out

PHP Web Client - Logged In
Command Line PHP Client
aaronpk@M1XK330M7C gnap-client-php % php gnap-cli.php start
Visit this URL in your browser:
https://gnap-as.herokuapp.com/api/as/interact/xzStGFmL3

OR

Visit this URL: https://gnap-as.herokuapp.com/device
and enter this code: LA2BZYMZ
PHP CLI Client - Scanning QR Code
A Sample App

Access:
- api

Subject Identifiers:
- iss_sub
- opaque

[Approve] [Deny]

Please return to your device.
PHP CLI Client - Polling
ACCESS TOKEN:

Array
(
    [value] => Sw5aRQTI2EN7WhujK86qlsvLx5zqW0GNiw8ZfvtCGjYbCnh80d2JNcGo35V9Zbvt
    [access] => Array
        (
            [0] => Array
                (
                    [type] => api
                )
        )
)

SUBJECT:
EA48D7A4C79196FD7A595DEDAD16EE5E
aaronpk@H1XK330M7C gnap-client-php %