ASYMMETRIK

FHIR + Security in NodeJS

HL7 FHIR DevDays 2018

June 20, 2018

Bryan Young, Andrew Marcus

ASYMMETRIK

Asymmetrik Secure FHIR server

Security Focused

NodeJS/Express Framework

Data Source Agnostic

Extensible

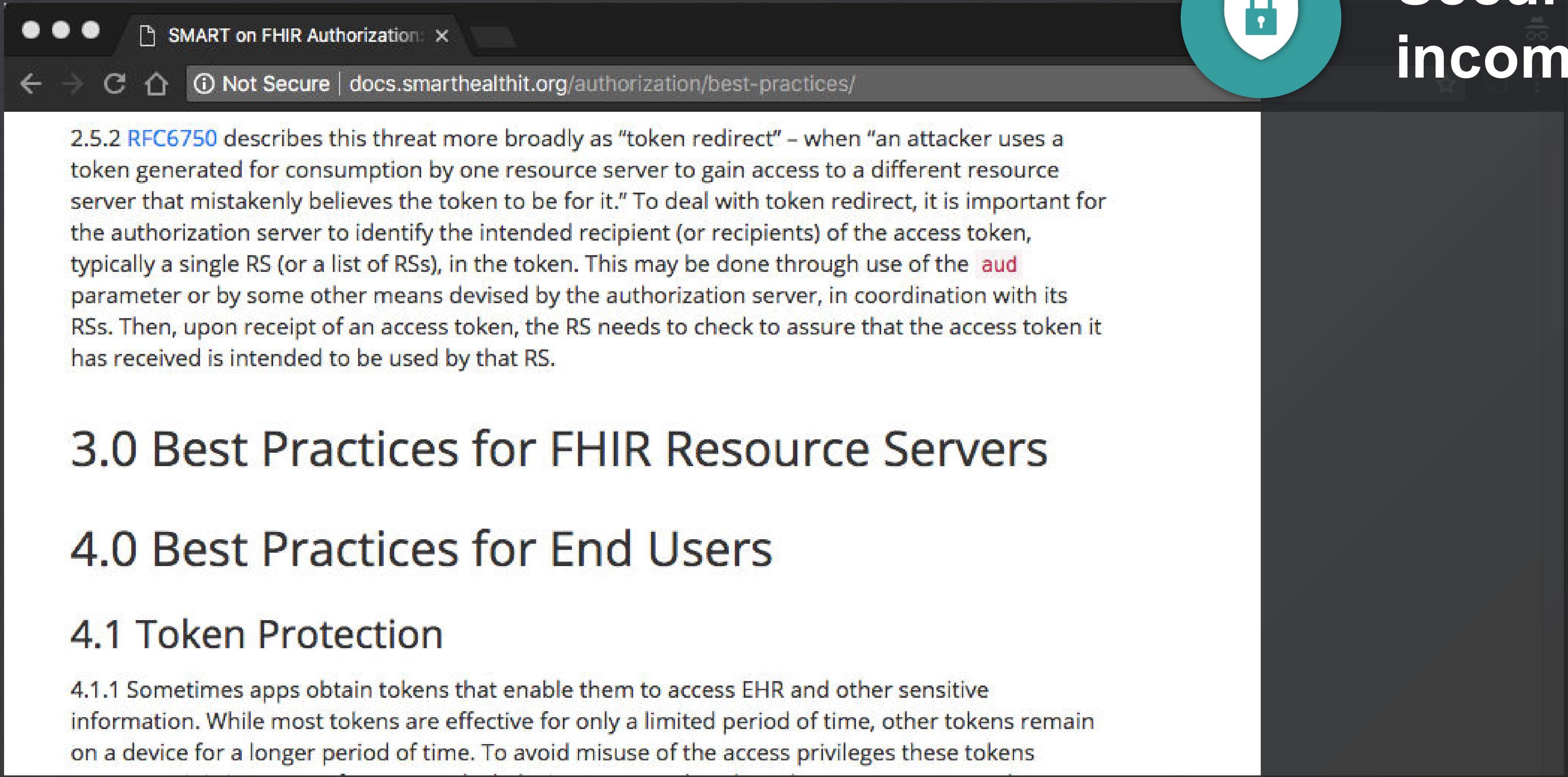
Winner of ONC Secure Server Challenge

Open Source: https://github.com/asymmetrik/node-fhir-server-core

ASYMMETRIK

FHIR is making interoperability better

Security is incomplete


SMART on FHIR Authorization
Not Secure
docs.smarthealthit.org/authorization/best-practices/

2.5.2 RFC6750 describes this threat more broadly as "token redirect" – when "an attacker uses a token generated for consumption by one resource server to gain access to a different resource server that mistakenly believes the token to be for it." To deal with token redirect, it is important for the authorization server to identify the intended recipient (or recipients) of the access token, typically a single RS (or a list of RSs), in the token. This may be done through use of the `aud` parameter or by some other means devised by the authorization server, in coordination with its RSs. Then, upon receipt of an access token, the RS needs to check to assure that the access token it has received is intended to be used by that RS.

3.0 Best Practices for FHIR Resource Servers

4.0 Best Practices for End Users

4.1 Token Protection

4.1.1 Sometimes apps obtain tokens that enable them to access EHR and other sensitive information. While most tokens are effective for only a limited period of time, other tokens remain on a device for a longer period of time. To avoid misuse of the access privileges these tokens

ASYMMETRIK

And now, some technical stuff

ASYMMETRIK

Configure the server

Set up audit logging

Define profiles, & supported FHIR versions

Go!

```
const { VERSIONS } = require('@asymmetrik/node-fhir-server-core/src/constants');
const fhirServerCore = require('@asymmetrik/node-fhir-server-core');
const eventService = require('./audit/event.service.js');


const config = {
	server: {
		port: 443,
		ssl: { key: 'path/to/key.pem',  cert: 'path/to.cert.pem'  }
	},
	events: {
		auditEvent: eventService.writeAuditEventRecords,
		provenance: eventService.writeProvenanceRecords,
	},
	profiles: {
		patient: {
			service:   path.resolve('./profiles/patient/patient.service.js'),
			versions: [ VERSIONS.STU3 ]
		}
	}
};
// Now start the server
const server = await fhirServerCore(config).catch(console.error);
```

This is available on our Github Wiki

ASYMMETRIK

How to ensure conformance

Automate conformance statements

Validate payloads

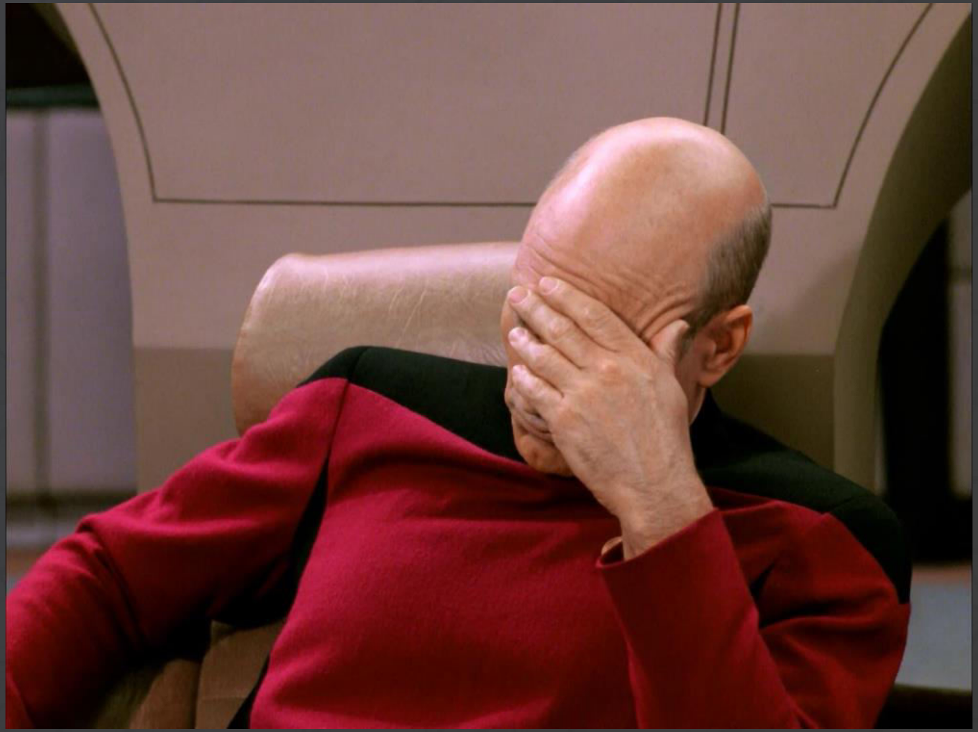
Run conformance tests

Goal

Data is trusted by

- Database
- Client app

Learn from our mistakes



ASYMMETRIK

CHALLENGE

FHIR is

a beast

+100 Resources

+100 Extensions

+50 Profiles

&

evolving

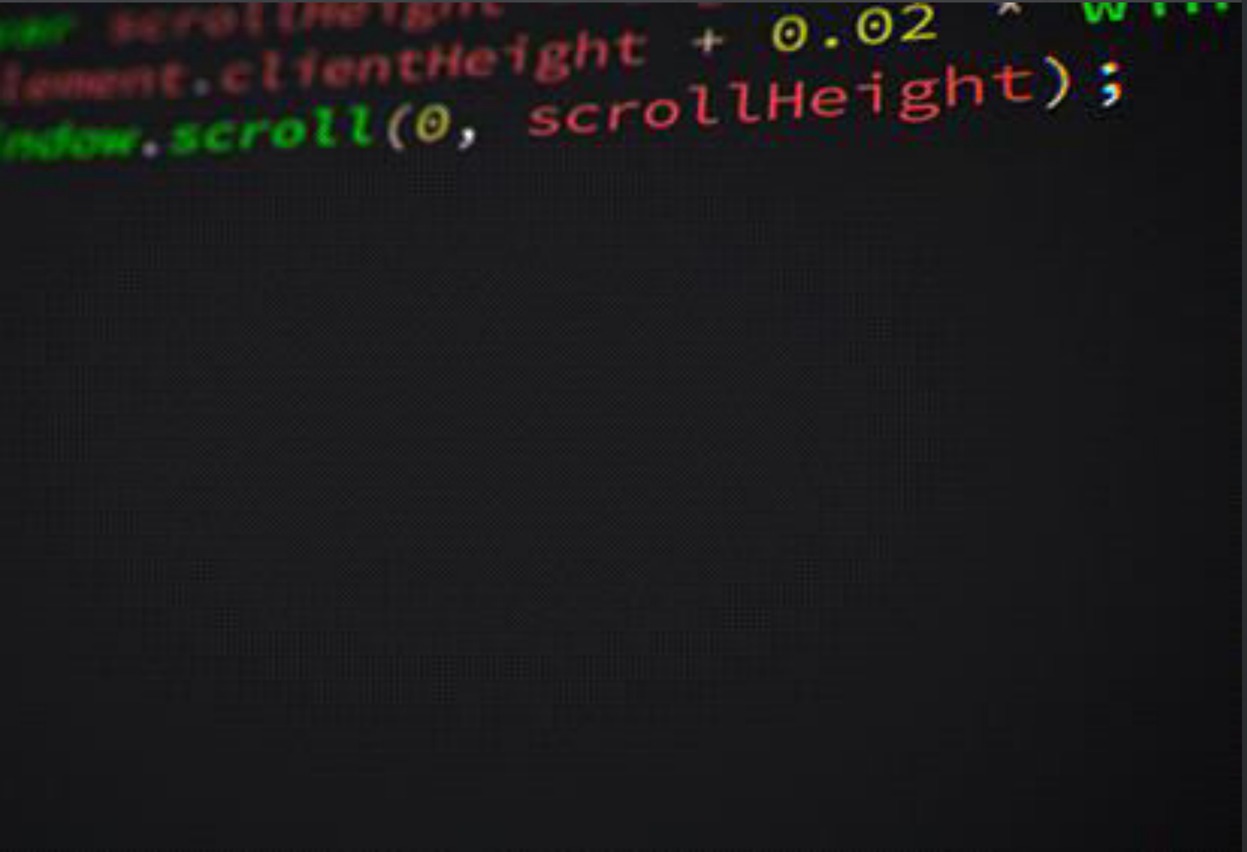
Frequent new versions

Breaking changes

ASYMMETRIK

WHAT WE DID

Self-Writing Code



```
lement.clientHeight + 0.02
ndow.scroll(0, scrollHeight);
```

Each version of FHIR has JSON Schemas

Automated scripts write validation code

- Added to repo
- Unit tests included

LESSONS LEARNED

But robots can't do everything

We must add definitions by hand after script runs

ASYMMETRIK

LESSONS LEARNED

JSON Schemas are not complete

Code fields:

- Not enforceable

Search params:

- Not parseable

✓ **Let's fix this!**

```
"language":{
  "description":
        "The ISO-639-1 alpha 2 code in lower case for the
        language, optionally followed by a hyphen and the
        ISO-3166-1 alpha 2 code for the region in upper
        case; e.g. \"en\" for English, or \"en-US\" for
        American English versus \"en-EN\" for England
        English.",
  "$ref": "CodeableConcept.schema.json#/definitions/
        CodeableConcept"
}
```

ASYMMETRIK

CHALLENGE

Which versions should you support?

- DSTU2: still used by most EHRs
- STU3: mature, but not widely adopted
- R4: ready any day now

ASYMMETRIK

WHAT WE DID

Why not all of them?

Our server lets you implement several at a time

Separate endpoints for each:

- /dstu2/patient
- /stu3/patient
- /r4/patient

Goal

Translate between versions

ASYMMETRIK

LESSONS LEARNED

FHIR doesn’t make versioning easy

- Breaking changes between versions
- No version info presented with records
- No client/server version negotiation

✓ **Let’s fix this!**

ASYMMETRIK

LESSONS LEARNED

Building a secure OAuth2 in production is hard

- Many dev tools for FHIR consumers
- Few dev tools for FHIR producers

✓ **Let's fix this!**

- Need to add patient info
- Several ways to return scopes from tokens
- Limited support from test tools

ASYMMETRIK

BEST PRACTICE

Encrypt your communications

DON'T	DO
✗ Use self-signed certs in production It's worth the hassle and cost to get a real certificate Use **TLS 1.0**	✓ Always, *always*, *always* use SSL/TLS At least **TLS 1.2** with **256-bit** AES keys We recommend **TLS 1.3** support We recommend **512-bit** AES keys

ASYMMETRIK

BEST PRACTICE

Filter out bad requests

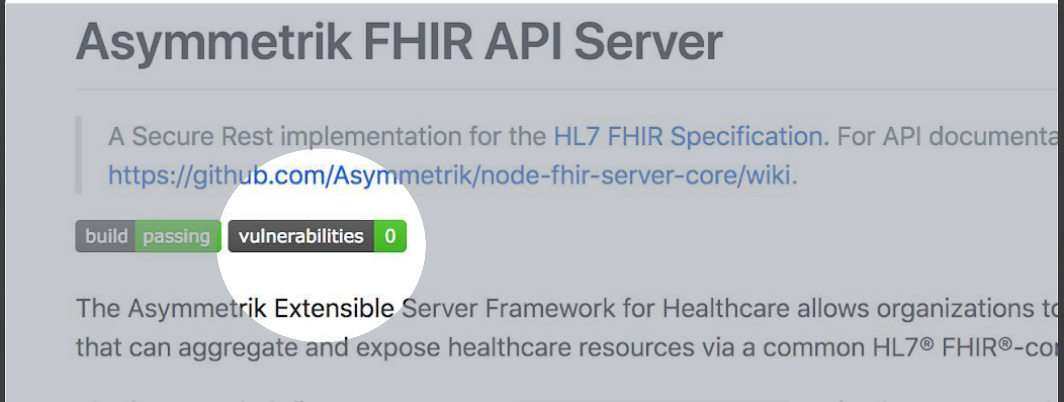
DON'T	DO
✗ Write URL params directly to the database or the screen	✓ Block SQL/No-SQL Injections Filter out database commands
✗ Let hackers outside your memory sandbox	✓ Block Cross-Site Scripting (XSS) Filter out JS and other unsafe HTML
	✓ Block buffer overflow attacks Truncate values longer than your variables can support

ASYMMETRIK

BEST PRACTICE

Guard against vulnerable packages

DON'T	DO
✗ Trust that other people's code is secure	✓ Use a static code analysis tool ✓ Analyze your dependencies for vulnerabilities We use snyk.io as part of our CI build pipeline


Asymmetrik FHIR API Server

A Secure Rest implementation for the HL7 FHIR Specification. For API documenta
https://github.com/Asymmetrik/node-fhir-server-core/wiki.

The Asymmetrik Extensible Server Framework for Healthcare allows organizations t
that can aggregate and expose healthcare resources via a common HL7® FHIR®-co

ASYMMETRIK

BEST PRACTICE

Store logs separate from data

DON'T	DO
✗ Store logs in the same place as your data If your server is ever compromised, a hacker could change your logs	✓ Store audit, provenance and system logs in a separate database If possible, a separate environment
✗ Store secrets or PHI in your logs Unless they are stored in a secure place	✓ Scrub PHI and secrets out of your system logs

ASYMMETRIK

BEST PRACTICE

Return token to server to get scopes

DON'T	DO
✗ Blindly trust OAuth2 tokens A hacker could spoof and re-sign token if they have the client secret	✓ Send tokens back to the OAuth2 server to verify them Ask server to give you scopes and patient ID There are several ways to do this, depending on your OAuth server

ASYMMETRIK

BEST PRACTICE

Define scopes for every endpoint

DON'T	DO
✗ Allow access to any data without checking user's scopes	✓ Define and check scopes for every endpoint user/Observation.* patient/Observation.read
✗ Allow patients to access the records of other patients	✓ Return a 403 Unauthorized code if user doesn't have sufficient scopes
	✓ Consider allowing finer-grained control based on user object

ASYMMETRIK

BEST PRACTICE

Hide the existence of records

DON'T

✗ Allow a hacker to figure out whether a user or patient is in your database

- Never say why access is denied

- Never imply there are other records the user can't access

DO

What if a patient visits **/patient/_search?**

✓ Only return 1 or 0 results

- The patient's own record, or no records

✓ Or, completely prevent patients from accessing the patient search endpoint

ASYMMETRIK

BEST PRACTICE

Test the unhappy paths

DON'T	DO
✗ Assume that incoming requests are valid	✓ Write tests for:
✗ Assume that the user has permission to access resources	Bad parameters
	Bad data
	Unauthorized access
	Compromised tokens

ASYMMETRIK

PROBLEM

Let’s fix this!

✓ **Make FHIR easier to develop**

- Spec entirely parseable
- Versions forward and backward compatible
- More development tooling

✓ **Make FHIR more secure**

- Best practices
- Use FHIR checklist
- Security tests
- OAuth2 reference servers

ASYMMETRIK

Please Contribute!

Code: FHIR Open-Source Secure Server

- https://fhir.health
- https://github.com/Asymmetrik/node-fhir-server-core

About Us

- https://asymmetrik.com/healthcare

Asymmetrik Healthcare Podcast

- https://soundcloud.com/asymmetrik-healthcare

Song: We Didn't Start the FHIR

- https://soundcloud.com/asymmetrik-healthcare/we-didnt-start-the-fhir

ASYMMETRIK

Thanks!

Andrew Marcus

amarcus@asymmetrik.com

Bryan Young

byoung@asymmetrik.com