

TRAIL *OF* **BITS**

JWTs, and why they suck

who?

1. Rory Mackie / @roddux

- AppSec at Trail of Bits

A. Development -> DevSecOps -> Sec Eng -> Pentesting/websec

❖ Purveyor of awful opinions (facts)

1) bad at lists



this guy

what?

JWTs are JSON Web Tokens *(more like Janky Worthless Tokens haha gottem)*



Actually a group noun referring to JWSs and JWEs – we're talking about JWSs.

The header is known as 'JOSE', which uses algorithms defined in the JWA standard, because ACRONYMS

Used (badly) for authentication and authorization

Popularised by SAAS companies that sell authentication products

apparently pronounced 'jot'³ which tells you everything really

why?

To convince you all *why* you should stop using JWTs for sessions, by:

- Teaching you the bad bits
- Making you question whether you *need* JWTs *(spoiler: you don't)*
- Giving you some more sensible options

how do i JWT

<base64-encoded JSON blob> . <base64-encoded JSON blob> . <signature>

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJibGFOIjoxMjN9.zSMlrWrNxUyhwpf3oSGyVdQA9CG25KlwHJVeaZNWuh8

(starts with eyJhb[. .] because that's what {“alg” looks like in base64)



<HEADER>.<CLAIMS>.<SIGNATURE>

Circle of shame



```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}. {  
  "blah": 123  
}. [Signature]
```

I GOT 99 PROBLEMS

and they're all JWTs

Problem 1: Irrevocable

Once issued there exists ***no means*** to revoke a JWT (builtin)


If you track state for each token you may as well have a database :^)

Having an expiry is ***not the same thing*** as being able to revoke a token

Problem 2: JSON

JSON is not a strong format


- Field ordering
- Duplicate fields
- Field data types



```
{  
  "alg": "HS256",  
  "typ": "JWT",  
  "alg": "none"  
}
```

Inconsistencies in the above between different libraries/langs¹

```
{  
  "user_id": "1234567890",  
  "user_name": "roddux",  
  "iat": 1516239022,  
  "iat": "1516239999"  
}
```



Problem 3: YOU DON'T NEED IT

YAGNI – *You Aren't Gonna Need It.*

You're not Facebook

You are also not Google

Just use a database, or memcached/Redis



\$£ sponsor me pls redis £\$

Problem 4: Too flexible

Too many options

Thirteen different alg types²s, and that's just for JWS

Seventeen types for JWEs

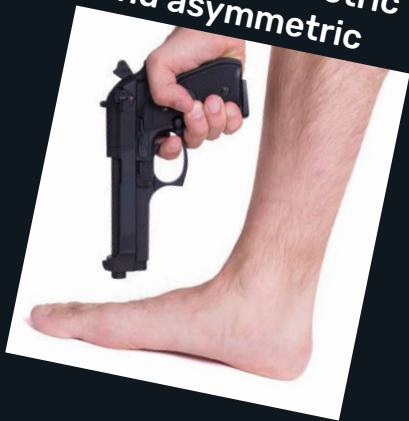
Too many ways to misconfigure those options, leading to ...

Problem 5: Footguns

token can specify which
key is used for validation



mixing symmetric
and asymmetric



parsing untrusted data



alg: none



Problems 6–99: You gotta parse 'em

You have to decode and parse RANDOM USER-SUPPLIED DATA in order to validate the token

Hope your Base64/JOSE/JSON/JWS parsing libraries are all
~~~**absolutely**~~~ bulletproof :^)

(spoilers: they are not) (~121 CVEs in JWT/JOSE/JWS libraries)

## Problem 7: Offline attacks against your keys

**Attackers can literally spend as long as they need to break your key signature algorithm. ECDSA is not bulletproof, and lots of crypto algos have had problems in the past that allow for privkey recovery.**

**Using JWTs allows attackers to try any attack they want (and any new, secret attack) to break your signatures**

# Bad implementations

List of high-profile JWT-related issues

<https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/>

<https://insomniasec.com/blog/auth0-jwt-validation-bypass>

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=JWT>

# Why you think you need JWTs

*"muh stateless"* – stop

*"b-but muh interoperability"* – use protobufs

*"everyone else is doing it!"* – doesn't mean it's a good idea

*"derp derp it protect me against CSRF"* – JWTs are not a security control, don't treat them as one. Also, other *superior* controls exist



# What to use instead

**Honest-to-goodness COOKIES with session IDs**

**HttpOnly, Secure, Sec-Fetch-Mode, SameSite...**

**why throw away hard-won security controls? for what?**

**congrats, XSS bugs are now a problem again**

but what if i JWT ***inside*** my cookies?

don't talk to me or my son ever again

TL;DW:



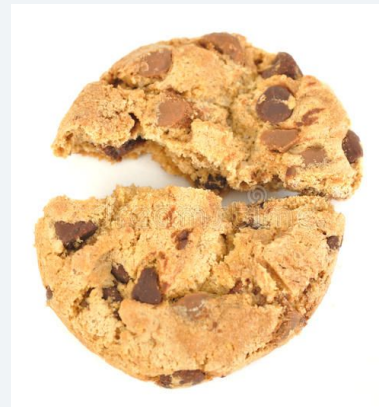
# REJECT MODERNITY



bad standard  
dumb logo  
khafkaesque nightmare  
doesn't care about you  
not flexible  
will leave you for next big thing  
did i mention alg:none?



# EMBRACE TRADITION



tasty snack  
everybody loves him  
cares about you  
not fussy  
been around forever  
gets on with your friends

# References

1. [An exploration of JSON interoperability vulnerabilities, Bishop Fox](#)
  - some other links here lol
  - sample text
2. [JWA RFC – JWT algorithm list](#)
3. [JWT RFC](#)
4. [Thomas Ptacek blogpost](#)
5. [Sec/Crypto/W.e podcast](#)

# Questions!

*( and maybe answers )*

