Multi-factor Authentication using FIDO2 and Web Authentication with ASP.NET Identity

Brock Allen
brockallen@gmail.com
http://brockallen.com
@BrockLAllen


PASSWORDS ARE BAD
MMMKAY?
imgflip.com

Why are passwords so bad?

- Real issue is the human factor

- Memorable
  - Leads to low-entropy/weak passwords
  - Often are reused across accounts
- Symmetric
  - Makes phishing attacks possible

Careful who might be watching

Password managers

- Improve password hygiene
  - Generate unique, high entropy/strong password per account
  - Only enter password onto correct domain
- Inconvenient
  - Need installing on every device
  - Often backed by cloud storage/service
- Still symmetric
  - Password managers themselves are being attacked

Use something in addition to passwords

“your account is more than 99.9% less likely to be compromised if you use MFA” [1]

[1] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984

Multi-factor authentication

- Prove possession of something you have (access to)
  - In addition to password
- Traditional types
  - Email
  - Security token
  - SMS
  - Authenticator app

Comparisons

Email	Security token	SMS	Authenticator App
Cheap for all	Expensive	Cheap for user	Cheap for all
Dangerous if email is compromised	One device per account	Targetable	Usability issues
Not everyone has email		Requires cell phone service	

The human factor still exists!

Internet of Shit
@internetofshit

Читаю

Two factor sucks, so... why not just point a webcam at your token?
shodan.io/host/198.2.49.... via @djvc1993

Показать перевод

D-Link/Airlink IP webcam http config Version: 1.0

```
HTTP/1.0 200 OK
Server: Camera Web Server/1.0
Auther: Steven Wu
MIME-version: 1.0
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 1681
```

FIDO2: Fast identity online

- Un-phishable
  - Asymmetric keys used
  - Different key per website
- User-friendly
- Variety of device types
  - Hardware token
  - Mobile device/computer
- MFA or first factor
  - Passwordless

fido™ ALLIANCE | simpler stronger authentication

Terminology

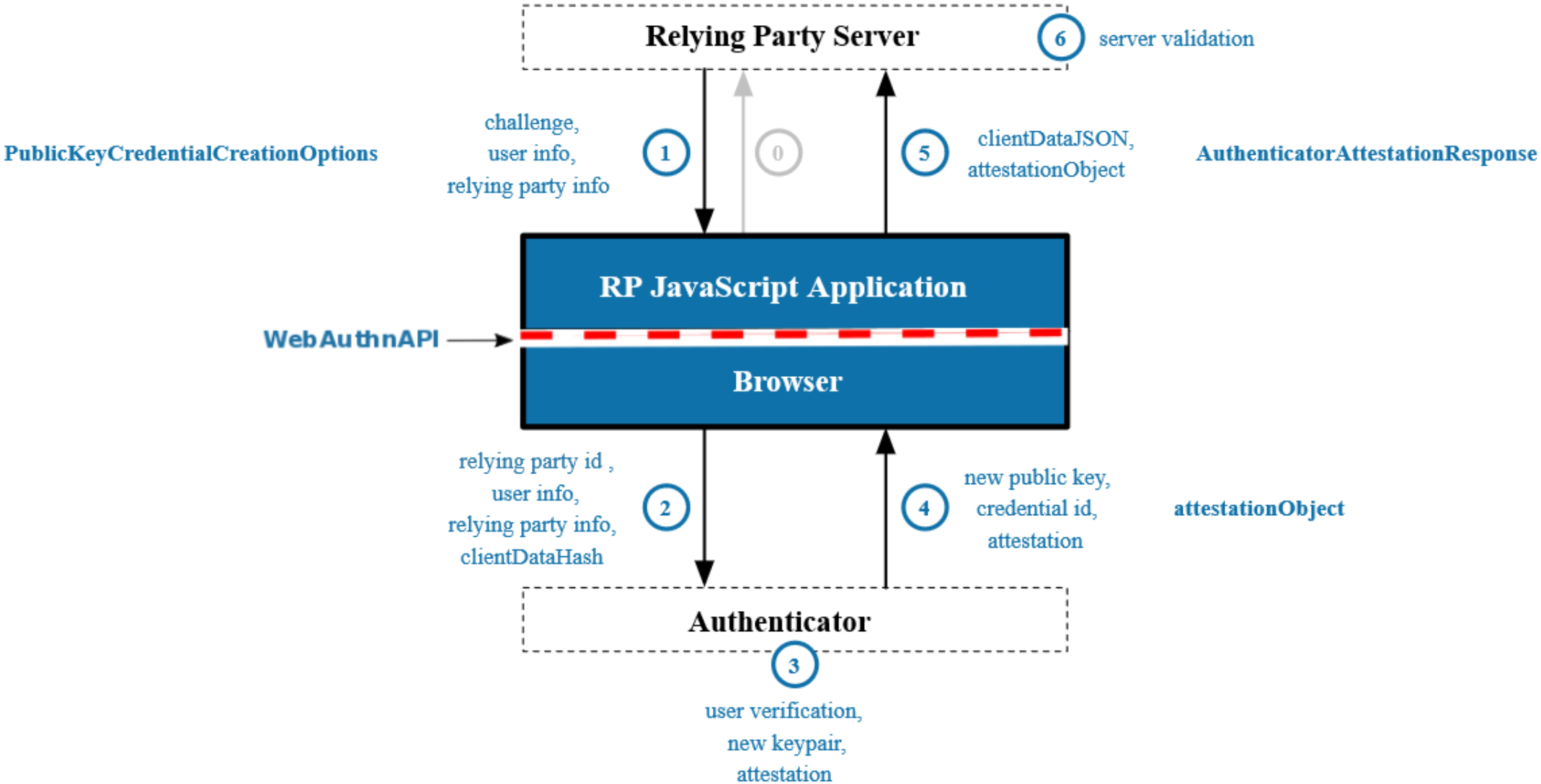
- RP/Relying party
  - Web application to which the user will be authenticating
  - Combination of server-side and client-side code
- Authenticator
  - FIDO device with which user authenticates
  - Roaming or platform
- Client Platform
  - Client (browser) and Client Device (hardware device client runs on)

FIDO2 specifications

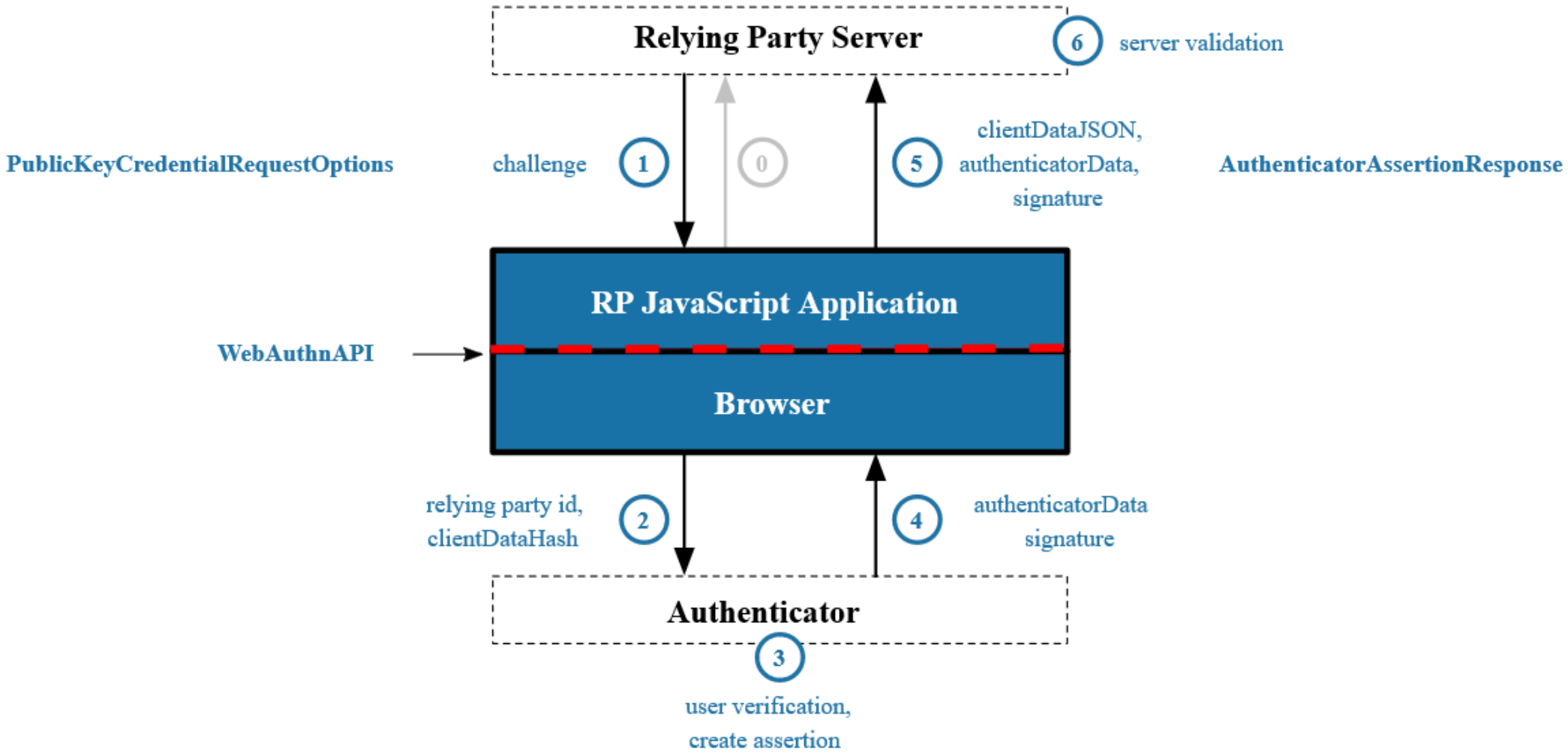
- Web Authentication: API for accessing public key credentials
  - JavaScript API to connect to client platform
- CTAP2: Client to authenticator protocol
  - API for client platform to connect to roaming authenticator

- Older specs for MFA only workflows:
  - U2F: universal second factor
  - CTAP1

The way it works: registration



The way it works: authentication



Authenticator type modalities

- Attachment modality
  - Platform authenticators
  - Roaming authenticators
- Credential Storage Modality
  - Client-side credential source (resident)
  - Server-side resident credentials source (non-resident)
- Authentication factor capability
  - User-verifying (e.g. PIN, biometric)
  - Non-user-verifying

Authenticator taxonomy

Authenticator Type	Authenticator Attachment Modality	Credential Storage Modality	Authentication Factor Capability
Second-factor platform authenticator	platform	Either	Single-factor capable
User-verifying platform authenticator	platform	Either	Multi-factor capable
Second-factor roaming authenticator	cross-platform	Server-side storage	Single-factor capable
First-factor roaming authenticator	cross-platform	Client-side storage	Multi-factor capable

ASP.NET Identity

- Extend Storage:
  - Maintain the authenticator key data
- Extend MFA registration:
  - FIDO specific MFA registration pages
- Intercept MFA login workflow:
  - Trigger and validate FIDO credentials
  - Issue login cookie

Summary

- MFA is important!
- FIDO2 authenticators are a great advance in MFA
- Fairly simple to integrate into ASP.NET applications


T. HANKS