

LUKI BEZPIECZEŃSTWA? NIE W MOIM KODZIE ŹRÓDŁOWYM!

Adam Czubak, PhD

PGP ✓ aczubak@4crypto.eu

 www.linkedin.com/in/adamczubak

Kierownik B+R projektu CyberEva CYBERSECIDENT/489912/IV/NCBR/2021 Uniwersytetu Opolskiego
Kierownik Zespołu Badawczego „Bezpieczeństwo IT” w Instytucie Informatyki Uniwersytetu Opolskiego

NSA CNSS (Committee on National Security Systems) 4011 Recognition

NSA CNSS (Committee on National Security Systems) 4013 Recognition

US Department of Defense (DoD) 8570.01-M Certification

CheckPoint CCSA

CISCO CCNP Security | Firewall Security Specialist | IPS Specialist | VPN Security Specialist | CCNA CyberOps



opole.dev

2023.10.24 Opole



Informacja o Prawach Autorskich

Wszelkie prawa zastrzeżone © 2023 Adam Czubak.

Niniejszy materiał chroniony jest prawami autorskimi i nie może być kopiowany, rozpowszechniany, adaptowany, ani wykorzystywany w inny sposób bez wyraźnej, pisemnej zgody autora.

Udostępnianie niniejszej prezentacji jest możliwe wyłącznie dla uczestników serii wydarzeń opole.dev [<https://opole.dev/>]. Uczestnik może przeglądać, wyświetlać oraz korzystać z zawartych tu treści wyłącznie dla swoich osobistych, niekomercyjnych celów edukacyjnych.

Tworzenie utworów pochodnych, w tym tłumaczeń, adaptacji, przekształceń, aranżacji oraz jakichkolwiek innych zmian w niniejszym materiale, jest dozwolone pod warunkiem wyraźnego wskazania autora wersji pierwotnej.

Kontakt z autorem:

Adam Czubak, PhD

Email: aczubak@4crypto.eu

Tel.: [+48 691 122 312](tel:+48691122312)

Agenda

1. Ot, klasyka...
2. Moduły i biblioteki na których polegamy
3. Apple i SSL
4. Uwierzytelnienie w CyberEva



#1 Ot, klasyka...

Czarna lista grzechów

1. Niepoprawna walidacja danych wejściowych
2. Niezaszyfrowane połączenia lub niezabezpieczone API, słabe mechanizmy uwierzytelniania i autoryzacji
3. Nieaktualne biblioteki (bądź takie z lukami)
4. Niewłaściwe zarządzanie błędami, w tym yświetlanie zbyt szczegółowych informacji o błędach może dostarczyć atakującym użytecznych danych
5. Brak mechanizmów ograniczających dostęp do krytycznych zasobów systemu

Buffer overflow

```
1 #include <cstdio>
2 #include <cstring>
3 #include <iostream>
4
5 const char *PASSWORD_FILE = "rictro";
6
7 int main()
8 {
9     char input[8];
10    char password[8];
11
12    std::scanf(PASSWORD_FILE, "%s", password);
13
14    std::cout << "Enter password: ";
15    std::cin >> input;
16
17    // Debug prints:
18    // std::cout << "Address of input: " << &input << "\n";
19    // std::cout << "Address of password: " << &password << "\n";
20    // std::cout << "Input: " << input << "\n";
21    // std::cout << "Password: " << password << "\n";
22
23    if (std::strncmp(password, input, 8) == 0)
24        std::cout << "Access granted\n";
25    else
26        std::cout << "Access denied\n";
27
28    return 0;
29 }
```

```
1 Enter password: rictro
2 Access granted
```

```
1 Enter password: hello
2 Access denied
```

```
1 Enter password: sunshinesunshine
2 Access granted
```

Buffer overflow

input								password							
h	e	l	l	o	\0			r	i	c	t	r	o	\0	

input								password							
s	u	n	s	h	i	n	e	s	u	n	s	h	i	n	e

Bezpieczeństwo jest gdzie?

Buffer overflow jest problemem w językach programowania, które nie zarządzają pamięcią automatycznie i pozwalają na bezpośredni dostęp do adresów pamięci, takich jak C i C++. W językach, które mają wbudowane mechanizmy zarządzania pamięcią i To ryzyko nie występuje.

1. W **Java** tablice są obiektami, które mają swój własny rozmiar. Próba przekroczenia granic tablicy wywoła wyjątek `ArrayIndexOutOfBoundsException`.
2. W **Pythonie** listy są dynamiczne i mogą zmieniać swój rozmiar. Nie ma również bezpośredniego dostępu do pamięci.
3. **C#** podobnie jak w Javie, C# ma wbudowane mechanizmy zarządzania pamięcią i kontrolę typów, co minimalizuje ryzyko.
4. **JavaScript** i inne skryptowe.
5. **Rust** jest podobny do C/C++, ale ma silne mechanizmy kontroli dostępu do pamięci, które praktycznie eliminują możliwość buffer overflow.

Niepoprawna walidacja danych wejściowych

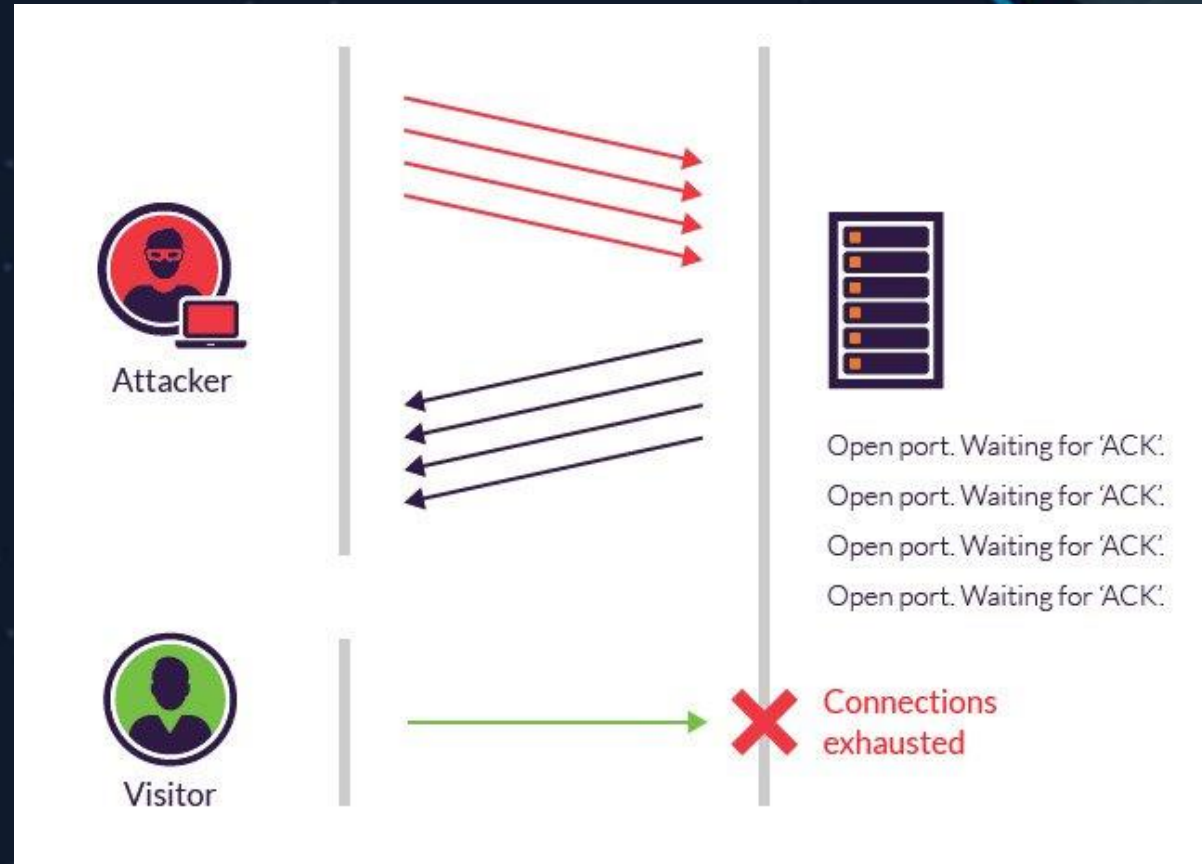
1. Formularze są już bezpieczne (SQL Injection czy Cross-Site Scripting (XSS))
2. Integracja z innymi systemami stanowi wyzwanie, czyli sanityzacja danych wejścia dotyczy również danych pobieranych automatycznie z innych systemów, a nie tylko od użytkownika.



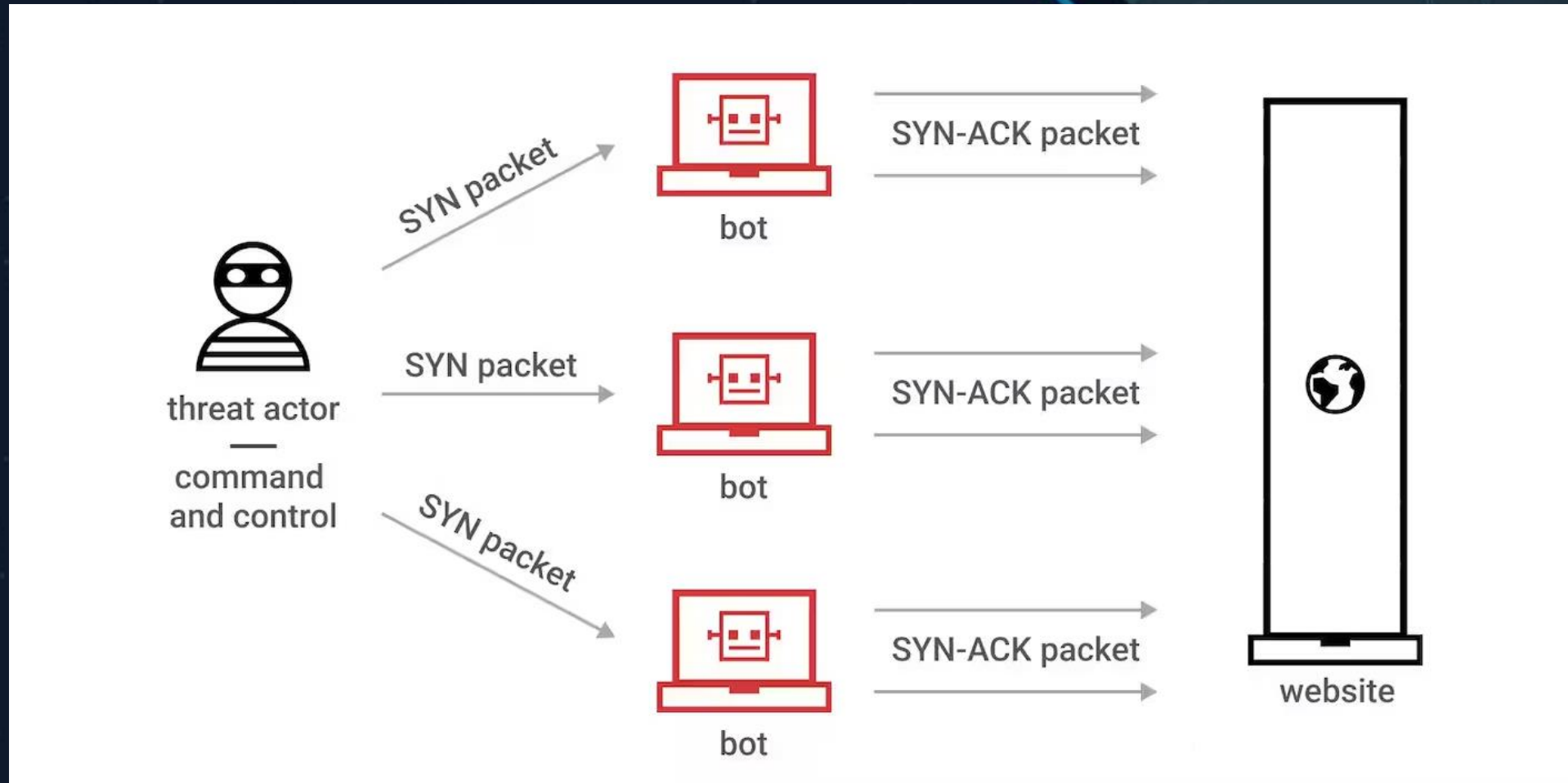


#2 Moduły i biblioteki na których polegamy

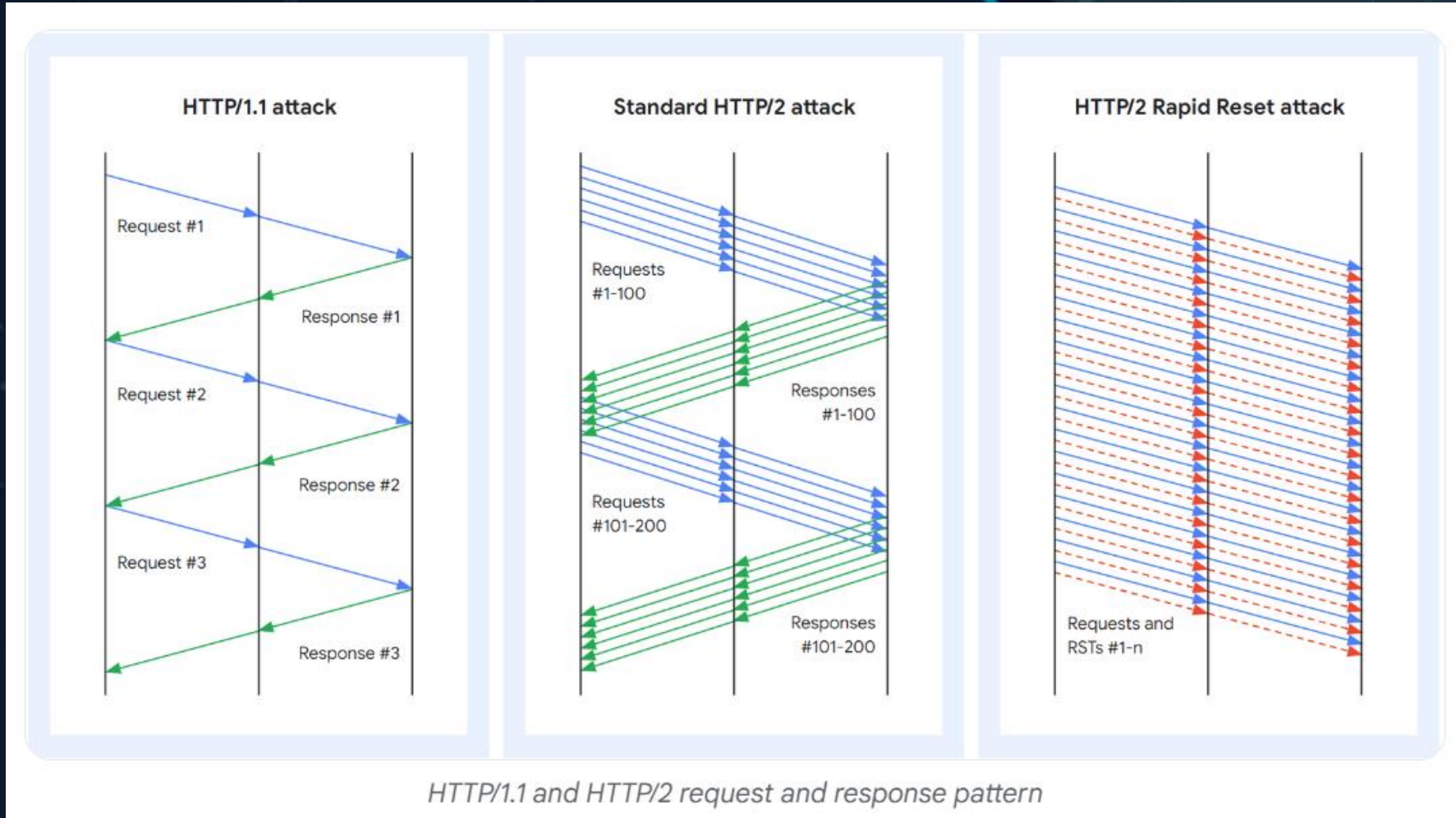
Klasyczny DoS 1.0 [SYN-Flood Attack]



DDoS 1.0 [Bot-Based SYN-Flood Attack]



HTTP/2 'Rapid Reset' DDoS 10.X.2023



Google, How it works: The novel HTTP/2 'Rapid Reset' DDoS attack

<https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack>



#3 Apple i SSL

Walidacja certyfikatu X.509

Ostrzeżenie: potencjalne zagrożenie bezpieczeństwa

Firefox wykrył problem i nie wczytał „**expired-rsa-dv.ssl.com**”. Witryna jest źle skonfigurowana lub zegar systemowy ma ustawioną nieprawidłową datę.

Certyfikat witryny prawdopodobnie wygaś, co uniemożliwia programowi Firefox nawiązania bezpiecznego połączenia. Jeśli otworzysz tę stronę, atakujący będą mogli przechwycić informacje, takie jak hasła, adresy e-mail czy dane kart płatniczych.

Co zrobić w takim przypadku?

Problem leży prawdopodobnie po stronie witryny i nie masz możliwości jego rozwiązania. Możesz powiadomić administratora witryny o problemie.

[Więcej informacji...](#)

[Wróć do poprzedniej strony \(zalecane\)](#) [Zaawansowane...](#)

Błąd dotyczący prywatności

Niebezpieczona <https://expired-rsa-dv.ssl.com>

Połączenie nie jest prywatne

Osoby atakujące mogą próbować wykraść Twoje informacje ze strony **expired-rsa-dv.ssl.com** (na przykład hasła, wiadomości lub dane kart kredytowych). [Więcej informacji](#)

NET-ERR_CERT_DATE_INVALID

[Zaawansowane](#) [Wróć do bezpieczeństwa](#)

Certyfikaty SSL/TLS



DEMO

Connection security for opole.dev

You are securely connected to this site.
Verified by: Let's Encrypt
More information

{ OPOLE .DEV }

SPOTKANIA OPOLSKIEJ BRANŻY IT

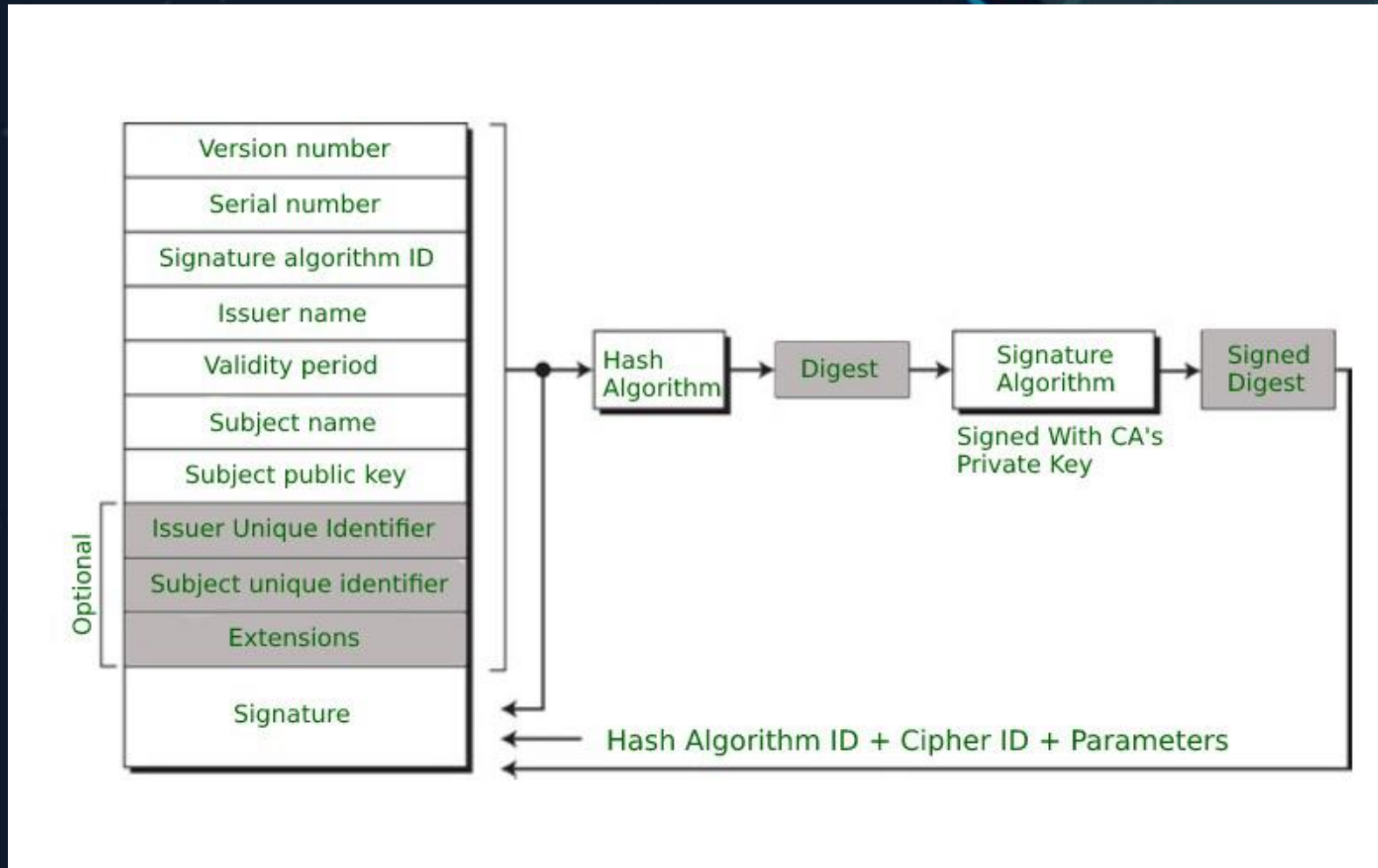
24 października, godzina 18:00 | Muzeum Diecezjalne

00 : 07 : 05 : 01

DNI GODZIN MINUT SEKUND

[Dowiedz się więcej](#) [Poprzednie spotkania](#)

Certyfikaty SSL/TLS



Walidacja certyfikatu X.509

1. Nawiązanie połączenia: Strona połączenia nawiązuje połączenie z serwerem webowym i żąda certyfikatu SSL.
2. Pobranie certyfikatu: Serwer przesyła certyfikat SSL do strony połączenia.
3. Sprawdzenie ważności: Strona połączenia weryfikuje, czy certyfikat jest aktualny i nie wygasł.
4. Sprawdzenie wydawcy: Strona połączenia sprawdza, czy certyfikat został wydany przez zaufaną instytucję certyfikującą (CA).
5. Sprawdzenie domeny: Strona połączenia sprawdza, czy certyfikat jest wydany dla domeny, z którą użytkownik próbuje się połączyć.
6. Sprawdzenie CRL i OCSP: Opcjonalnie, strona połączenia może sprawdzić listę odwołanych certyfikatów (CRL) lub użyć protokołu OCSP, aby upewnić się, że certyfikat nie został odwołany.
7. Sprawdzenie algorytmów: Strona połączenia sprawdza, czy algorytmy szyfrujące i podpisu są silne i aktualne.
8. Sprawdzenie łańcucha certyfikatów: W przypadku certyfikatów wielopoziomowych, strona połączenia weryfikuje cały łańcuch certyfikatów aż do głównego certyfikatu korzeniowego.
9. Potwierdzenie weryfikacji: Jeżeli wszystkie kroki weryfikacji zakończą się sukcesem, strona połączenia ustanawia zaszyfrowane połączenie z serwerem.
10. Błąd weryfikacji: W przypadku niepowodzenia któregoś z kroków, strona połączenia wyświetli ostrzeżenie o niebezpiecznym połączeniu.

Certyfikaty SSL/TLS



DEMO

opole.dev - spotkania opolskie

Certificate for www.opole.dev

https://opole.dev

Connection security for opole.dev

You are securely connected to this site.

Verified by: Let's Encrypt

More information

{ OPOLE .DEV }

SPOTKANIA OPOLSKIEJ BRANŻY IT

24 października, godzina 18:00 | Muzeum Diecezjalne

00:07:05:01

DNI GODZIN MINUT SEKUND

[Dowiedz się więcej](#) [Poprzednie spotkania](#)

HTTPS – CA w MMC



ĆWICZENIE

Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

Console Root

- Certificates - Current User
 - Personal
 - Trusted Root Certification Authorities
 - Certificates**
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Active Directory User Object
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification Authorities
 - Trusted People
 - Client Authentication Issuers
 - Other People
 - Local NonRemovable Certificates
 - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	C
AAA Certificate Services	AAA Certificate Services	2029-01-01	Client Authenticati...	Sectigo (AAA)		
AddTrust External CA Root	AddTrust External CA Root	2020-05-30	Client Authenticati...	Sectigo (AddTrust)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025-05-13	Client Authenticati...	DigiCert Baltimore ...		
Certum CA	Certum CA	2027-06-11	Client Authenticati...	Certum		
Certum Trusted Network CA	Certum Trusted Network CA	2029-12-31	Client Authenticati...	Certum Trusted Net...		
Certum Trusted Network CA 2	Certum Trusted Network CA 2	2046-10-06	Client Authenticati...	Certum Trusted Net...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2028-08-02	Client Authenticati...	VeriSign Class 3 Pu...		
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	2038-01-19	Client Authenticati...	Sectigo (formerly C...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	1999-12-31	Time Stamping	Microsoft Timesta...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031-11-10	Client Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	2031-11-10	Client Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	2038-01-15	Client Authenticati...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	2038-01-15	Client Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	2031-11-10	Client Authenticati...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	2038-01-15	Client Authenticati...	DigiCert Trusted Ro...		
DST Root CA X3	DST Root CA X3	2021-09-30	Client Authenticati...	DST Root CA X3		
Entrust Root Certification Auth...	Entrust Root Certification Authority	2026-11-27	Client Authenticati...	Entrust		
Entrust Root Certification Auth...	Entrust Root Certification Authori...	2030-12-07	Client Authenticati...	Entrust.net		
GlobalSign	GlobalSign	2029-03-18	Client Authenticati...	GlobalSign Root CA...		
GlobalSign Root CA	GlobalSign Root CA	2028-01-28	Client Authenticati...	GlobalSign Root CA...		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	2034-06-29	Client Authenticati...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	2038-01-01	Client Authenticati...	Go Daddy Root Cer...		
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	2034-01-16	Client Authenticati...	IdenTrust Commer...		
ISRG Root X1	ISRG Root X1	2035-06-04	Client Authenticati...	ISRG Root X1		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	2000-01-01	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2043-02-27	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2043-02-27	<All>	Microsoft ECC TS R...		
Microsoft Root Authority	Microsoft Root Authority	2020-12-31	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	2021-05-10	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	2035-06-24	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	2036-03-23	<All>	Microsoft Root Cert...		

Actions

- Certificates
- More Actions

Contains more actions that can be performed.



Apple i SSL

[Print subscriptions](#) [Sign in](#) [Search jobs](#) [Search](#) [Europe edition](#) ▼

Support the Guardian

Fund independent journalism with €5 per month

Support us →

The Guardian

News

Opinion

Sport

Culture

Lifestyle

More ▼

World UK Climate crisis Environment Science Global development Football **Tech** Business Obituaries

Apple

Analysis

Apple's SSL iPhone vulnerability: how did it happen, and what next?

Charles Arthur

SSL vulnerability in iPhone, iPad and on Mac OS X appeared in September 2012 - but cause remains mysterious as former staffer calls lack of testing 'shameful'

Advertisement



Charles Arthur, Apple's SSL iPhone vulnerability: how did it happen, and what next? (2014)

<https://www.theguardian.com/technology/2014/feb/25/apples-ssl-iphone-vulnerability-how-did-it-happen-and-what-next>

Walidacja certyfikatu SSL/TLS

```

static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}

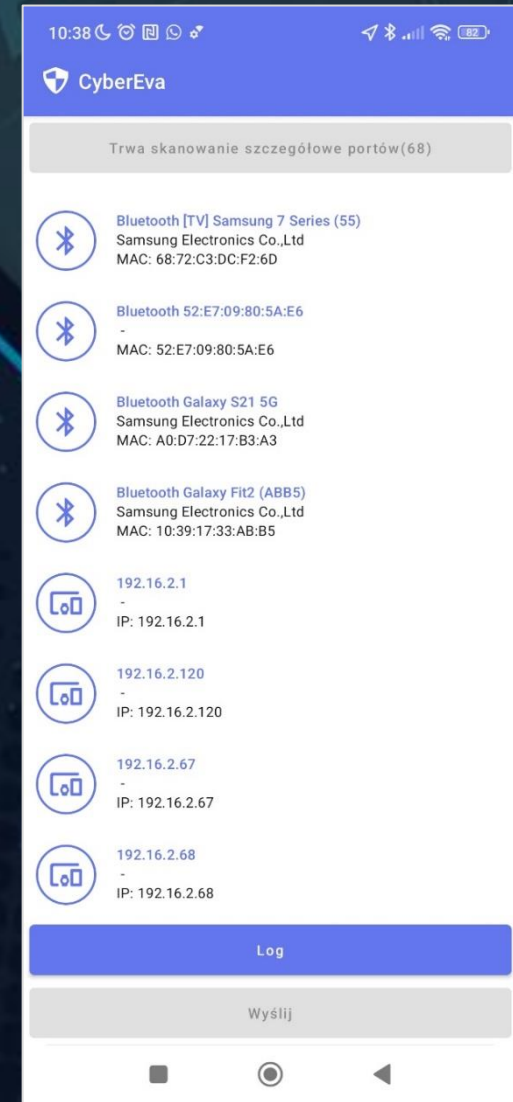
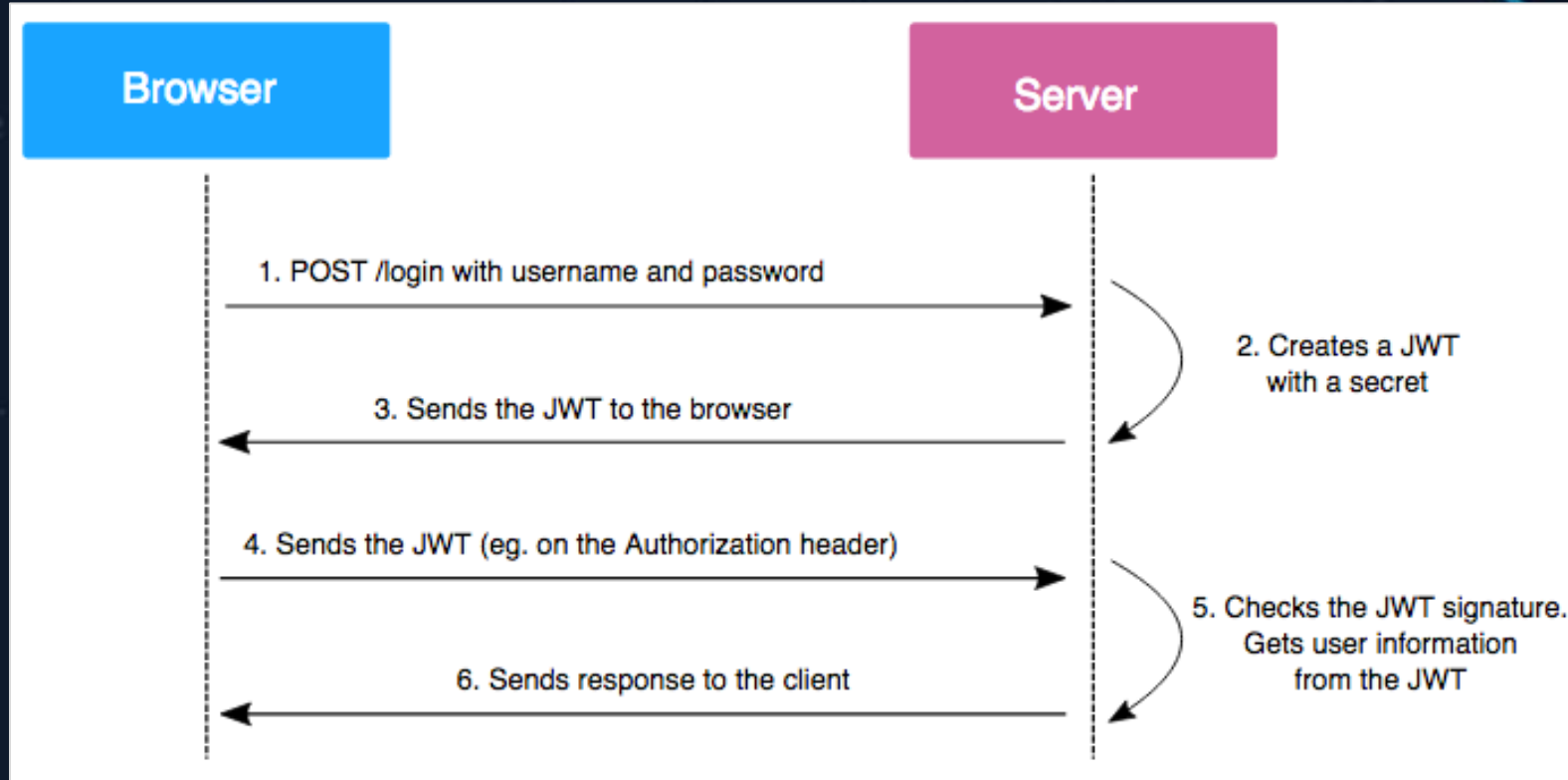
```

These checks got skipped



#4 Uwierzytelnienie w CyberEva

Case - JWT



Case – JWT Java Web Tokens

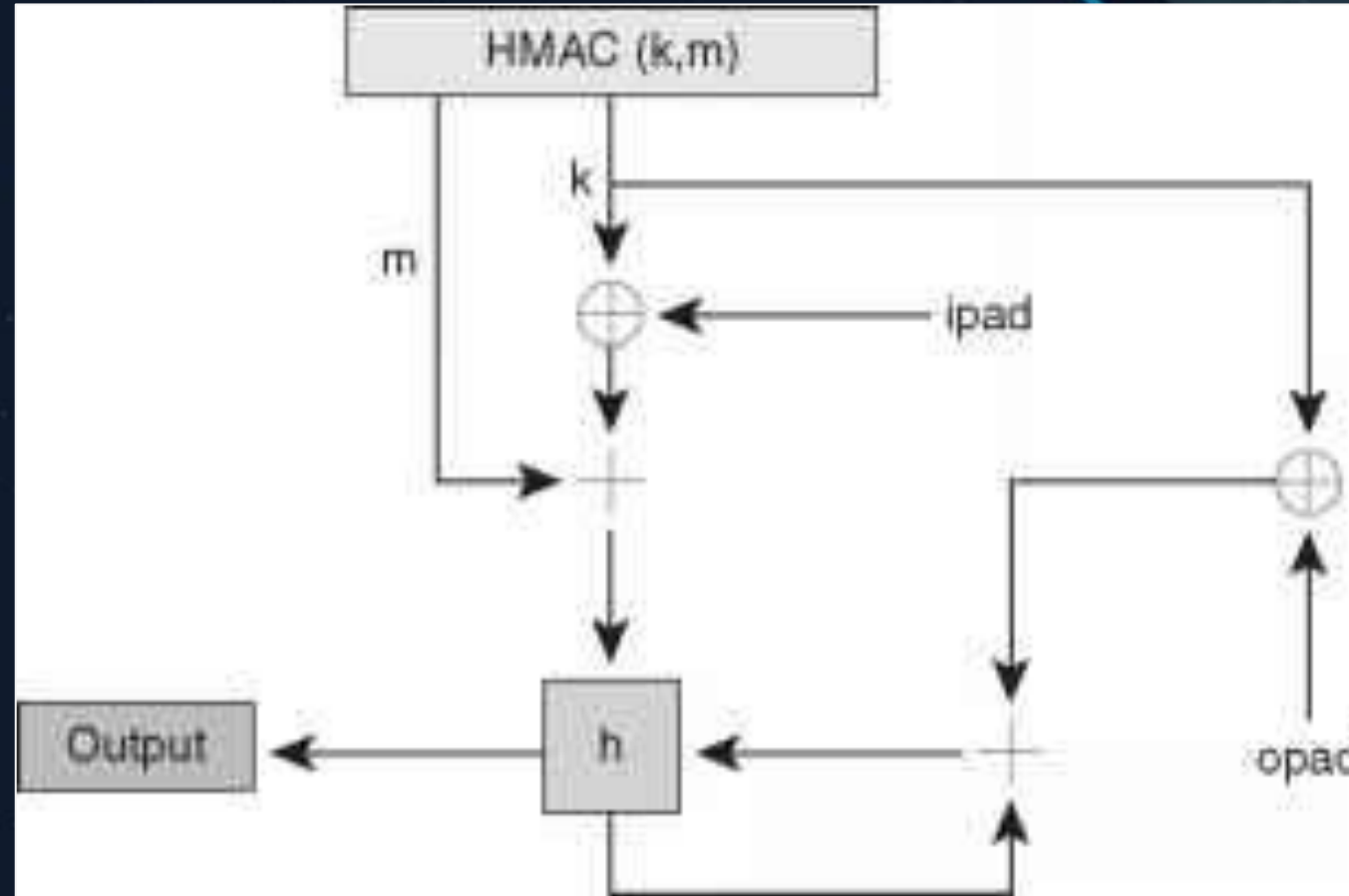
The JWT's Header

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

The JWT's Data

```
{  
  "iat": 1416929109,  
  "jti": "aa7f8d0a95c",  
  "scopes": [  
    "repo",  
    "public_repo"  
  ]  
}
```

Case – JWT Java Web Tokens



Case – JWT Java Web Tokens – RFC7518

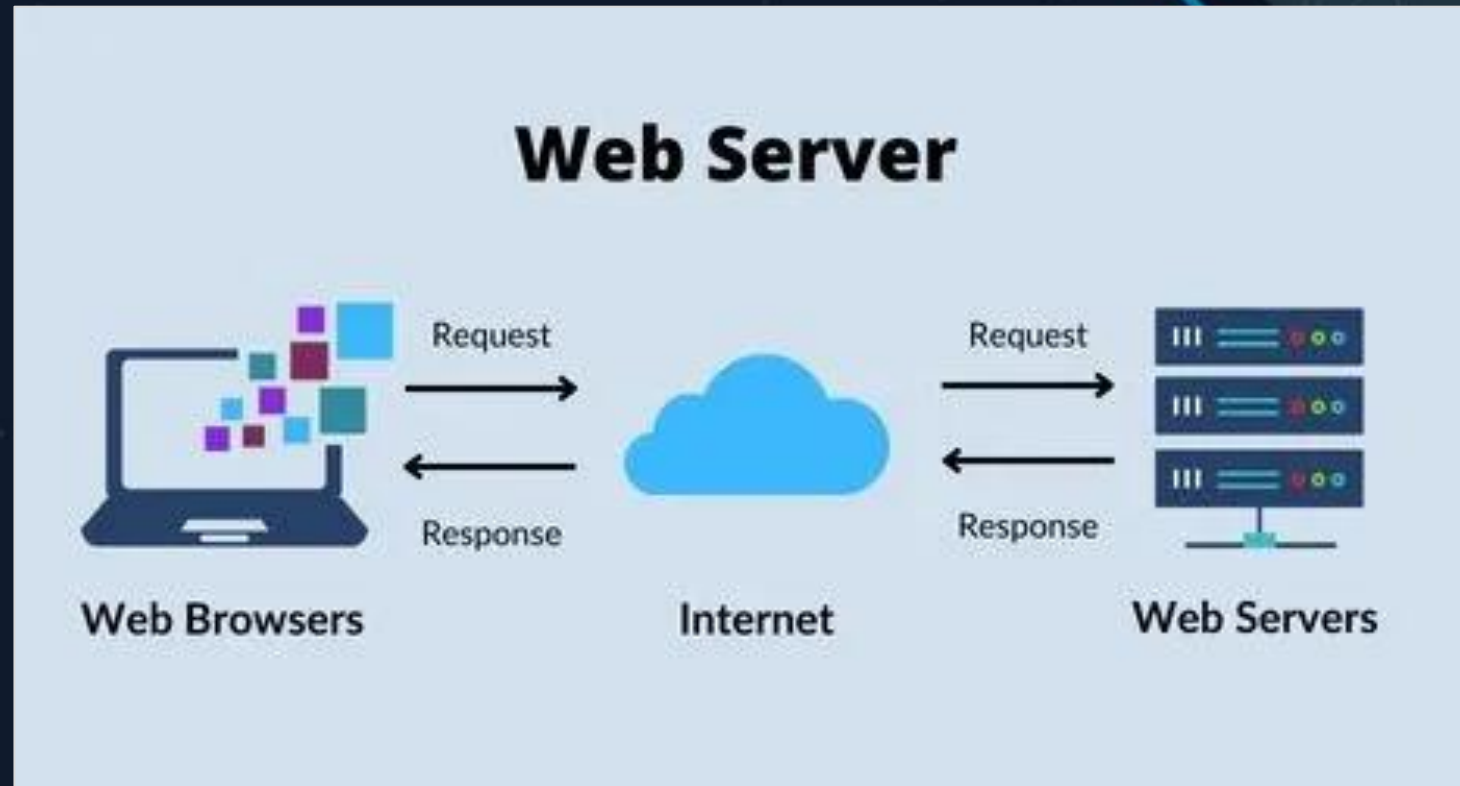
3.1. "alg" (Algorithm) Header Parameter Values for JWS

The table below is the set of "alg" (algorithm) Header Parameter values defined by this specification for use with JWS, each of which is explained in more detail in the following sections:

"alg" Param Value	Digital Signature or MAC Algorithm	Implementation Requirements
HS256	HMAC using SHA-256	Required
HS384	HMAC using SHA-384	Optional
HS512	HMAC using SHA-512	Optional
RS256	RSASSA-PKCS1-v1_5 using SHA-256	Recommended
RS384	RSASSA-PKCS1-v1_5 using SHA-384	Optional
RS512	RSASSA-PKCS1-v1_5 using SHA-512	Optional
ES256	ECDSA using P-256 and SHA-256	Recommended+
ES384	ECDSA using P-384 and SHA-384	Optional
ES512	ECDSA using P-521 and SHA-512	Optional
PS256	RSASSA-PSS using SHA-256 and MGF1 with SHA-256	Optional
PS384	RSASSA-PSS using SHA-384 and MGF1 with SHA-384	Optional
PS512	RSASSA-PSS using SHA-512 and MGF1 with SHA-512	Optional
none	No digital signature or MAC performed	Optional

The use of "+" in the Implementation Requirements column indicates that the requirement strength is likely to be increased in a future version of the specification.

Case – JWT – Credential Reuse





Źródła:

1. ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa
2. CISA – Cybersecurity & Infrastructure Security Agency (U.S. Department of Homeland Security)
3. Washington Post & BBC
4. CERT Polska , NASK
5. Sophos
6. Bleeping Computer
7. Obserwacje własne





Zapraszamy na przyszłoroczną

III edycję Konferencji CACS - Conference on Applied Cybersecurity

21-22.X.2024

Park Naukowo-Technologiczny w Opolu

<https://cacs.uni.opole.pl>