Protokol TLS

Jan Jiroušek, SPCSS

- **Protokol TLS pro zabezpečenou komunikaci**

Protokol TLS

Protokol TLS

- Dříve SSL, kryptografický protokol, „S“ v HTTPS
- Verze SSL 1,2,3, TLS 1.0 – známé bezpečnostní problémy
- TLS 1.1 – konec podpory v běžném SW na začátku roku 2020
- TLS 1.3 – nová verze z r. 2018

Protokol TLS

Protokol TLS v EET

- Specifikace rozhraní vyžaduje TLS 1.1 a vyšší
- Doporučená verze je TLS 1.2
- Aktuálně podporované verze TLS 1.1 a TLS 1.2, od počátku provozu EET

Protokol TLS

Ukončení podpory TLS 1.1

- Využívá řadu šifrovacích algoritmů aktuálně považovaných za „nedostatečně silné “
- Nejsou (zatím) známé konkrétní útoky a hackerské nástroje
- Obecný konsensus bezpečnostní komunity požaduje ukončení podpory TLS 1.1 v první polovině roku 2020, např:
  - Plánované ukončení podpory v hlavních prohlížečích
  - Oznámená úprava hodnocení Qualys SSL Labs

Protokol TLS

Ukončení podpory TLS 1.1 v EET

- V souladu se ZoKB a VoKB musí EET používat „aktuálně odolné kryptografické algoritmy a kryptografické klíče“
- Specifika EET
  - (Potenciálně) obtížná aktualizace pokladních zařízení
  - Specifický způsob použití – pro jednoúčelové API, obsah zpráv podepisován
  - Souběh s obnovou certifikátů
  - Start 3. vlny k 1.5.2020

Protokol TLS

Návrh plánu změn TLS v EET

- ASAP – podpora TLS 1.3 na Playgroundu
- 6.1.2020 – ukončení podpory TLS 1.1 na Playgroundu
- 6.1.2020 – podpora TLS 1.3 na Produkčním prostředí
- 1.4.2020 – ukončení podpory TS 1.1 na Produkčním prostředí
- 1.5.2020 – start 3. vlny EET

Prezentace předběžného plánu,
uvítáme komentáře a připomínky dodavatelů pokladen (obratem)

Bude publikován a jednotlivé termíny postupně potvrzovány na etrzby.cz

etržby
MÁ DÁTI. DAL.

SPCSS

Ministerstvo financí
České republiky

Protokol TLS – Cipher suites

Cipher Suites

# TLS 1.2 (suites in server-preferred order)				
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)			WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)			WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)			WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)			WEAK	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			WEAK	112

# TLS 1.1 (suites in server-preferred order)				
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			WEAK	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	WEAK	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			WEAK	112

Protokol TLS – Cipher suites

Návrh úpravy TLS Cipher suites v EET při ukončení podpory TLS 1.1

TLSv1.3 (nové šifry):

- TLS13-AES128-GCM-SHA256
- TLS13-AES256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

TLSv1.2 (nové šiftry, redukce slabých šifer, doplnění ECDSA šifer):

- ECDHE-ECDSA-AES128-GCM-SHA256 (vyžaduje ECDSA TLS certifikát)
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384 (vyžaduje ECDSA TLS certifikát)
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305-SHA256 (vyžaduje ECDSA TLS certifikát)
- ECDHE-RSA-CHACHA20-POLY1305-SHA256