Stav SSL/TLS na českém Internetu u HTTPS

Poslední aktualizace 3 ledna, 2025

Rok 2014 příliš nepřeje SSL/TLS knihovnám, v nichž bylo objeveno několik závažných chyb. Nejznámější z nich jsou asi Heartbleed, goto fail a CCS útok. Zmíněné zranitelnosti byly objeveny manuálním auditem kódu nebo automatickým „dokazovačem“. Tyto chyby nejsou chybami SSL/TLS protokolu, nýbrž chybami implementací.

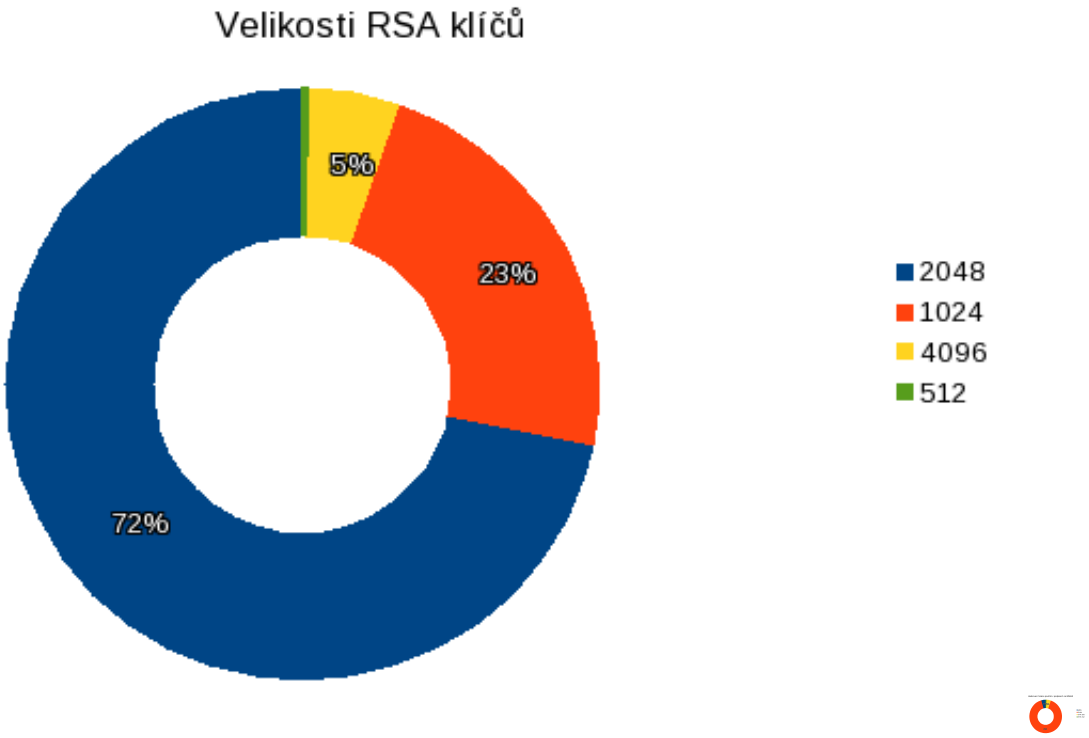
My jsme se již před časem zaměřili na scanování chyb konfigurací, které jsou lépe odhalitelné a odstranitelné.

Co se scanovalo

Vzhledem k tomu, že TLS je citlivé na jméno domény, které se posílá rozšířením SNI (server name indication), postupovali jsme podle doménových jmen namísto enumerace IPv4 adres. Na začátku jsme vycházeli z názvu domén druhého řádu v cz registru, s nejběžnější předponou www i bez.

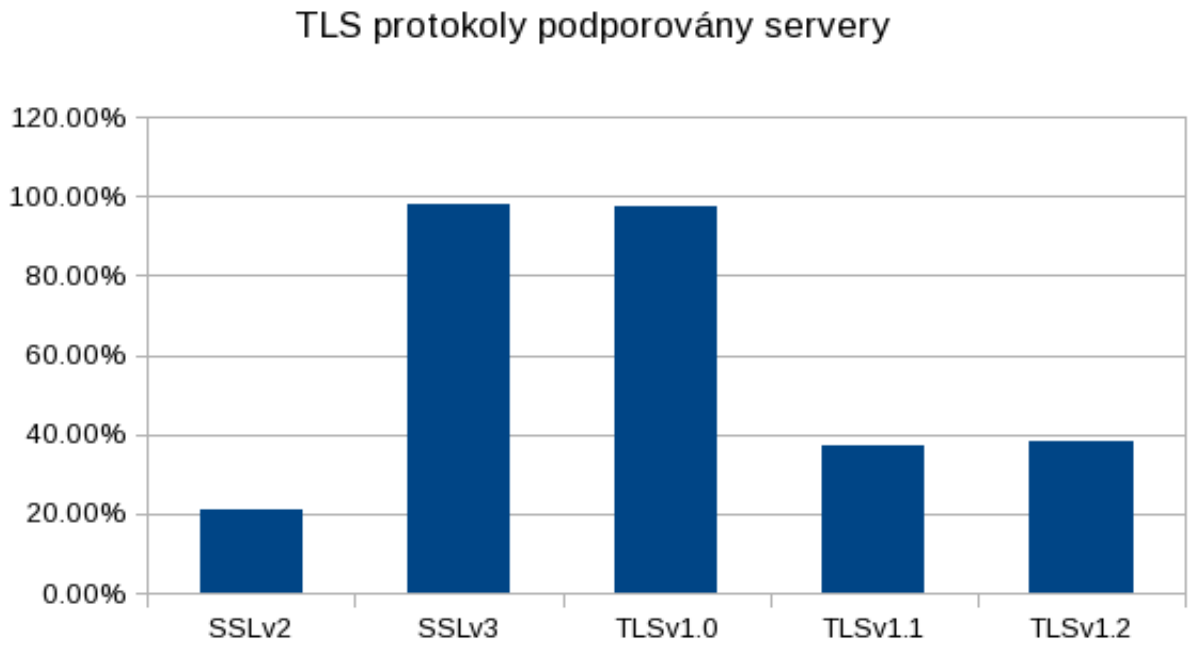
Celkově scanovaných domén bylo 1112865, odpovědí TLS serverů s řetězcem certifikátů na defaultním https portu se vrátilo 1088547. Unikátních serverových certifikátů zůstalo jen 24 276. Takto nízké číslo je způsobeno tím, že mnoho domén míří na hostingy a farmy, které vrací ten samý certifikát; nejvyšší počet jedné instance certifikátu byl až přes 90 tisíc. Největší délka řetězce byla 12 a vznikla spíš chybou konfigurace než záměrně.

Téměř všechny klíče v nalezených certifikátech jsou RSA (ojediněle i větší než 4096). Dnes se 1024-bit RSA moduly již nepovažují za dostatečně velké (pokud se nepoužívají jen na pár dní). Nové certifikáty by měly mít RSA modulus velikosti alespoň 2048 bit. V hashovacích algoritmech pořád převažuje SHA-1, která se už dostala do stavu „deprecated“. V nově vydávaných certifikátech by se již vyskytovat neměla.



Podrobnější pohled na šifry a protokoly podporované servery

V tomto testu jsme nejprve vyčlenili pouze servery mající nějaký certifikát řetězící se k „důvěryhodné“ CA. Hlavním důvodem je, aby různé zastaralé embedded krabičky a další testovací instalace nezkreslovaly data více, než je nutné. Zbylo nám tedy 9954 strojů. Těch jsme se postupně vyptávali, jaké protokoly a jaké šifry podporují.



Stále překvapivá je podpora prastarého protokolu SSLv2 na úrovni 20 %. Nebezpečí podpory rozbitého SSLv2 spočívá v tom, že aktivní útočník může způsobit downgrade útok na nejslabší verzi, kterou server i klient přijme.

Podobně je to i u šifer podporovaných serverem (ciphersuites) – man-in-the-middle útočník může opět zkusit downgrade útok a vynutit nejslabší šifru podporovanou klientem i serverem. Podle grafu výše patří do kategorie slabých šifer exportní šifry, které byly omezeny na krátké klíče (40-bitová RC4 nebo DES). Jako prolomené jsou označeny „NULL“ šifry a anonymní Diffie-Hellman, resp. anynomní Diffie-Hellman nad eliptickými křivkami.

NULL šifry způsobí, že se vlastně nešifruje – původně byly zamýšleny na použití v případě, že je TLS již vevnitř jiného šifrovaného tunelu, což většina lidí nechce (povede se jim to zapnout omylem). „Nej-NULL ciphersuite“ je *TLS_NULL_WITH_NULL_NULL*, která značí, že se nic neautentizuje, nepoužívá se žádný symetrický klíč ani hash.

Podobně anonymní (neautentizovaný) Diffie-Hellman je určen pro speciální případy, na které asi jen tak nenarazíte a budete chtít, aby byl anonymní DH/ECDH vypnutý. Jedno z mála regulérních využití anonymního DH je pro oportunistické šifrování u SMTP.

Proti bouřce s Heartbleedem, goto failem a CCS nejsou tyto výsledky až tak špatné. Největší prohřešky představují možnost downgrade útoku mezi klientem a serverem na nejslabší možný protokol nebo nejslabší šifru podporovanou oběma stranami.

Jak nejrychleji nastavit a otestovat svůj server

Bylo by potřeba vypnout SSLv2 (ideálně SSLv3), exportní šifry, NULL šifry a anonymní key-exchange. Naopak pokud možno zapněte šifry podporující pefect forward secrecy, novější TLSv1.1, TLSv1.2 a podle možností i HSTS.

Velmi populární „testovač“ je Qualys SSL Server Test. Většinu nalezených problémů umí vysvětlit a odhalit chyby s nekompletním nebo transvalidním řetězcem certifikátů. Naštěstí už před nějakým časem přestal klást důraz na velmi teoretický BEAST útok.

Pro nastavení nejběžnějších serverů Apache, nginx a lighttpd existuje celkem pěkný „cheatsheet“ na cipherli.st. Nastavení lze odsud rovnou copy-pastovat, ale stejně je lepší si nejprve přečíst, co člověk tímto způsobem dělá – když se špatně nastaví HSTS, můžete klienty na dlouhý čas odříznout od poddomén domény, kde jste HSTS nastavili.

Podrobnější příručku k nastavení TLS najdete v SSL/TLS Deployment Best Practices od zmiňovaného Qualysu.

Autor: Ondrej Mikle, blog CZ. NIC