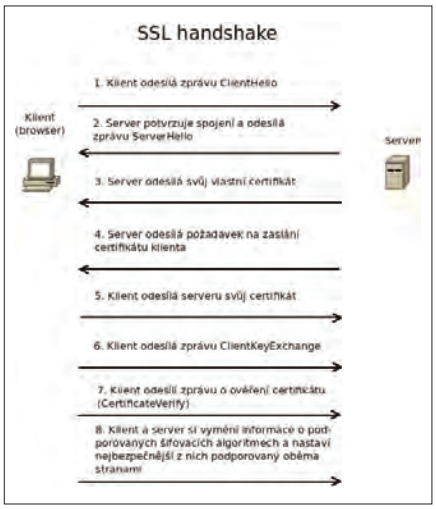
Jak bezpečné je vaše zabezpečené připojení přes SSL?



Pokud by měl poslední půlrok dostat nějaké přízvisko z pohledu počítačové bezpečnosti, pak by to nejspíš bylo „Půlrok bezpečnostních problémů se zabezpečenou komunikací SSL a TLS“.

JAROSLAV KODET

Běžný uživatel, který se alespoň trochu orientuje v oblasti bezpečnosti internetu, pravděpodobně uvede: „Používám HTTPS, tak jsem v bezpečí.“ Může to být i pravda, ale také nemusí.

O skutečné úrovni zabezpečení internetové komunikace totiž to „s“ na konci protokolu vypovídá poměrně málo. Vlastně jen to, že spojení je „nějakým způsobem“ šifrováno, a není tedy možné přečíst si například předání přihlašovacího jména a hesla přímo z odposlechnuté komunikace.

Úroveň zabezpečení síťové komunikace přitom závisí v podstatě na dvou faktorech, a to verzi zabezpečené vrstvy (SSL nebo TLS) a délce použitého klíče.

O tom, která verze šifrovacího algoritmu se používá, je rozhodnuto na základě vyjednání verze protokolu mezi serverem a klientem, přičemž nakonec se použije nejbezpečnější algoritmus podporovaný na obou stranách.

Toto chování je v naprostém pořádku, pokud opravdu komunikujete s tím, s kým chcete. Nicméně jestliže se stanete obětí útoku typu „man-in-the-middle“ (muž uprostřed), může se tento „muž“ pokusit ovlivnit dojednání použité kryptografie až na tak nízkou úroveň, kterou dokáže se svým výpočetním výkonem prolomit.

Výrazně mu to může zjednodušit slabá kryptografie na jedné či dokonce na obou stranách komunikace.

Na přiloženém obrázku by onen muž uprostřed vstoupil do komunikace ve fázi 2. Zde může přinutit obě strany ke snížení verze protokolu a z odposlechnuté komunikace poté rozšifrovat celou komunikaci.

Zastaralý šifrovací software

Aktuálně můžeme na internetu narazit na komunikaci zabezpečenou téměř všemi verzemi protokolů SSL a jeho nástupce TLS. Snad kromě SSLv1, který se nikdy příliš nerozšířil, především pro svou experimentální povahu.

SSLv2 pochází z roku 1995. Tato verze protokolu však byla postižena takovým množstvím chyb a bezpečnostních problémů, že ji už o rok později nahradila zcela přepracovaná verze SSLv3, se kterou se ještě stále můžeme setkat u mnoha internetových serverů, jež buď běží pod velmi starým operačním systémem, pro který se už neuvolňují bezpečnostní aktualizace, nebo mají příliš pohodlného administrátora.

Jak se naznačilo v předešlém odstavci, bezmála dvacet let stará verze SSLv3 už také přestala poskytovat náležitou ochranu. Jednoznačné doporučení tedy zní: co nejdříve upgradovat na nejnovější verzi TLS 1.2

Samotný upgrade nestačí

Při použití slabých „Diffie-Hellman“ parametrů je totiž zranitelná i nejnovější verze TLS 1.2. Právě použití slabé kryptografie stojí za zranitelností označovanou jako LOGJAM. Pro odstranění této chyby je třeba aplikovat doporučení zveřejněná na stránce *weakdh.org/sysadmin.html*.

Pro matematické a kryptografické nadšence je ještě vhodný i odkaz na podrobnosti zranitelnosti slabého šifrování.

Naše doporučení

Administrátoři internetových serverů by si měli ověřit úroveň jejich zabezpečení a následně případně aplikovat doporučení. SSLv3 ani TLS1.0 už za bezpečné považovat nelze, okamžitý upgrade je v podstatě povinnost, snad s výjimkou systémů, které jsou zranitelné úmyslně.

Všechny hlavní linuxové distribuce mají již opravené verze šifrovacích balíků v distribučních kanálech pro updaty. Po úspěšné aktualizaci by tedy měly být linuxové servery vůči zranitelnostem SSL/TLS odolné.

Pro jistotu je ale dobré se přesvědčit, že je velikost Diffie-Hellmann parametrů alespoň 2048 bitů. Záplatované jsou rovněž i produkty Microsoftu, a to pomocí služby Windows Update (samozřejmě s výjimkou produktů s ukončenou podporou).

Administrátoři klientských stanic, případně sami uživatelé, by zase měli dbát o pravidelné upgrady klientského softwaru (prohlížeč webu, e-mailový/groupwarový klient, klient sociálních sítí apod.) stejně jako operačního systému samotného.

O možnostech zakázání nedostatečně zabezpečené komunikace ze strany klientských aplikací pojednává příspěvek v sekci Rady a návody na stránkách CSIRT.CZ. ■

Autor pracuje jako bezpečnostní analytik sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ.

Jak jsme na tom v České republice?

Z veřejných statistik vyplývá, že k 1. červnu 2015 se v ČR nachází:
– 71 556 serverů postižených zranitelností POODLE
– 14 443 serverů postižených zranitelností FREAK