Identifikace a autentizace II.

V minulém dílu jsme otevřeli otázky autentizace a identifikace. V této části si přiblížíme problematiku kryptografických protokolů, jejich cílů a východisek.

Přejděme nyní k pojmu kryptografického protokolu, který má zásadní význam pro metody autentizace opírající se o kryptografické techniky. Samo slovo protokol je obvykle chápáno jako určitý postup včetně souvisejících náležitostí (například diplomatický protokol).

Kryptografický protokol je sdílený algoritmus definovaný posloupností kroků, které precizují aktivity vyžadované na dvou či více entitách s cílem dosáhnout určitého bezpečnostního cíle. Tento algoritmus využívá kryptologické transformace. Cílem kryptografických protokolů bývá autentizace účastníků protokolu, utvoření dohody o kryptografickém klíči, výměna těchto klíčů apod. Někdy se v literatuře používá i pojem autentizační (identifikační) protokol či protokol typu výzva-odpověď.

Příklad:

Strany A a B si potřebují mezi sebou vyměnit tajné klíče pro symetrickou šifru. Použijí například poměrně jednoduchý Needham-Schroederův protokol s veřejným klíčem. To znamená, že strany A a B se předem dohodly na systému asymetrické šifry a mají vzájemně k dispozici veřejné klíče zmíněné asymetrické šifry.

Použijme následující značení:

P_A – veřejný klíč strany A
P_B – veřejný klíč strany B
k_A – tajný klíč pro symetrickou šifru vygenerovaný stranou A (předmět výměny)
k_B – tajný klíč pro symetrickou šifru vygenerovaný stranou B (předmět výměny)

Zprávy protokolu probíhají následovně:

A→B:	$P_B (k_A , A)$	(Z1)
B→A:	$P_A (k_A , k_B)$	(Z2)
A→B:	$P_B (k_B)$	(Z3)

Tedy slovně:

1. A nejprve zašle straně B zprávu (Z1).
2. B získá dešifrací klíč k_A a pošle A zprávu (Z2).
3. Strana A po dešifraci zprávy (Z2) ověří, zda získaný klíč k_A souhlasí s tím, který zaslala straně B ve zprávě (Z1) - tím strana A má provedenu jak autentizaci strany B, tak i ujištění, že strana B zná k_A .
4. A pošle B zprávu (Z3).
5. Strana B po dešifraci zprávy (Z3) ověří, zda získaný klíč k_B souhlasí s tím, který zaslala ve zprávě (Z2).[1]

Výsledkem průběhu tohoto autentizačního protokolu je vzájemná autentizace obou entit, jimi vygenerovaných klíčů a přenos utajovaného klíče. Obě strany jsou si tedy po provedení protokolu jisty identitou svého protějšku. Vědí, že klíč k_A (resp. k_B) mohla vygenerovat pouze strana A (resp. strana B). Vzhledem ke klíči, který spočtou jako $f (k_A , k_B)$ mají záruku, že ho znají pouze strany A a B.

Výhodou tohoto, a samozřejmě dalších autentizačních protokolů, je reciprocita autentizace (obě strany mají stejnou možnost ověření své identity) stejně jako nízký počet požadovaných výpočetních operací a vzájemně zasílaných zpráv. Shrňme nyní cíle autentizačních protokolů. Z hlediska ověřující strany výsledkem protokolu autentizujícího entitu je buď přijetí identity žadatele, nebo ukončení požadavku jeho zamítnutím. Navíc strana B není schopna zneužít identifikační výměnu s A tak, aby provedla záměnu totožnosti strany A s třetí stranou C (tj. strana B např. nemůže později tvrdit, že komunikovala se stranou C). Pravděpodobnost, že třetí strana C (odlišná od A) projde protokolem a podaří se jí hrát roli strany A, je zanedbatelně nízká. Strana B tudíž může přijmout totožnost strany A.

---

[1] Konkrétní klíč pro utajené spojení mezi A a B symetrickou šifrou lze spočítat jako $f (k_A , k_B)$. Zde f je nějaká vhodná předem dohodnutá funkce.

Nyní se podívejme jaké jsou běžné techniky narušitelů, jak jim čelit a v čem spočívají nejčastější příčiny selhání autentizačních protokolů:

Technika	Protiopatření
znovupřehrání minulé zprávy	využití techniky výzva-odpověď, užití hodnot používaných pouze jedenkráte (tím může být náhodné číslo, pořadové číslo či časový údaj)
kombinací částí stávajícího a částí minulých průběhů autentizačního protokolu vytvořit úspěšnou (pro narušitele) modifikaci protokolu	seřazení všech zpráv v průběhu protokolu (např. pomocí pořadových čísel)
odraz, tím míníme zaslání informací z protokolu zpět původci zprávy	je užití ve výzvě identifikátoru přijímající strany; konstrukce takových protokolů, kde každá zpráva má jinou formální podobu, apod.
volitelné otevřené texty (tzv. chosen text attack - narušitel v protokolu výzva odpověď volí postupně cílevědomě své výzvy tak, aby získal nějakou informaci o dlouhodobém klíči ověřující strany)	techniky s nulovým rozšířením informací (zero knowledge) nebo je v odpovědích na výzvu využito náhodné čísla volené odpovídající stranou
záměrné zpožďování zpráv	kombinované užívání náhodných čísel a krátkých intervalů na odpověď; užití časového údaje a dalších vhodných technik

Protokol bude neúspěšný, jestliže nejsou dosaženy cíle, ke kterým byl protokol zamýšlen. Tedy jestliže protivník „cosi“ získá manipulací se samotným protokolem (nikoliv např. rozbitím použité šifry).

Nejčastějšími příčinami nezdarů autentizačních protokolů jsou:
- slabost určitého kryptografického primitivu (základního stavebního prvku kryptografických algoritmů, obdoba pojmu procedura, např. způsob generování klíčů, algoritmus pro testování prvočísel atd.),
- deklarované garance, které má protokol zajistit, neplatí či nebyly správně pochopeny,
- přehlédnutí nějakého principu aplikovatelného na širokou třídu kryptografických primitivů (jako např. šifrování).

Příkladem autentizačních protokolů na bázi symetrických šifer jsou např. Needham-Schroederův protokol, protokol systému Kerberos, dále ISO/IEC 9798-2 a ISO/IEC 9798-4 atd. Z protokolů na bázi systémů s veřejným klíčem uvedeme např. modifikovaný Needham-Schroederův protokol a protokol X-509. K některým z těchto protokolů se ještě v budoucnu vrátíme.

Úloha třetích důvěryhodných stran

Pro některé typy autentizačních protokolů, zejména těch, které ustavují klíče (key establishment protocols), je důležitým pojmem důvěryhodná třetí strana (trusted third party). V síti, kde více entit spolu komunikuje a má potřebu spolu navazovat různé typy autentizovaných spojení, je často užitečné vydělit jednu entitu a svěřit jí určité bezpečnostní funkce. Tato entita, které budeme říkat důvěryhodná třetí strana (DTS), hraje potom v autentizačních protokolech roli určitého prostředníka, zprostředkovatele. Např. může sloužit jako bezpečná schránka pro tajné kryptografické klíče, vede databázi uživatelů atd. My se zde zmíníme o roli certifikační autority.

Problematika certifikace z hlediska kryptologických protokolů se začala rozvíjet teprve v posledních letech. Jestliže se vrátíme k výše uvedenému Needham-Schroderovu protokolu s veřejným klíčem, pak si nyní všimněme poznámky, ve které se hovoří o předpokladu, že obě strany mají k dispozici autentický veřejný klíč opačné strany. Toto umožňují certifikáty veřejných klíčů. Certifikát je digitálně podepsaná struktura dat, spojující identitu vlastníka certifikátu (subjektu) s veřejným klíčem.

Certifikační autorita (CA) je potom entita, které bylo svěřeno vydávat certifikáty koncovým entitám. Je zodpovědná za ustavení a ověření autentičnosti veřejných klíčů. Spojuje pevně veřejný klíč s vyznačeným jménem pomocí podpisu certifikátů, uděluje certifikátům pořadová čísla a odvolává certifikáty. CA generuje, odvolává , publikuje a archivuje certifikáty. Ty jsou uloženy v úschovně, aby byly dostupné všem uživatelům certifikací. CA autentizuje identitu subjektu certifikace odlišně v závislosti na typu požadavku. Problematice certifikačních autorit jsou věnovány články Ing. Petra Budiše v Data Security Management 1/97 a 1/98.

Digitální certifikáty potvrzují vlastnictví veřejného klíče určitým jednotlivcem či jinou entitou. Dovolují verifikovat tvrzení, že daný veřejný klíč patří skutečně určitému zadanému jednotlivci. Certifikáty nám pomáhají

chránit se před někým, kdo se vydává za někoho jiného např. prostřednictvím telefonu a sdělí nám takto určitý veřejný klíč. Tento veřejný klíč pak mylně pokládáme za klíč někoho jiného.

Nejvíce rozšířený akceptovaný formát pro certifikáty je definován mezinárodní normou X.509. Certifikáty pak mohou být čteny či zapisovány libovolnou aplikací odpovídající normě X.509.

Cílem tohoto dvoudílném článku bylo uvést čtenáře do problematiky autentizace, rozebrat obsah tohoto pojmu a vysvětlit význam kryptografických protokolů pro autentizační postupy.

Literatura: Menezes, A.J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, Inc. 1997

Ing. Jaroslav Pinkava, CSc.
Jaroslav.Pinkava@aec.cz