Podplukovník Ing. Karel B u r d a , CSc.

Možnosti moderní kryptografie ve vojenských aplikacích

V tomto příspěvku je vyložena problematika nových služeb moderní kryptografie. Uvedené služby jsou v článku vysvětleny a stručně jsou zde naznačeny jejich aplikace v soudobých vojenských komunikačních, informačních a řídících systémech.

* * *

Moderní komunikační, informační a řídící systémy se vyznačují rozsáhlostí, složitostí a vysokým stupněm automatizace. Tyto rysy způsobují, že na uvedené systémy se lze nepozorovaně napojit a využívat je pro cizí prospěch. Odolnost soudobých systémů vůči tomuto zneužití je všeobecně nízká, a proto se v současné době různými dodatečnými bezpečnostními mechanismy uvedená odolnost zvyšuje [1]. Mezi nejčastěji používané bezpečnostní mechanismy patří mechanismy založené na kryptografii. Protože s takovýmito mechanismy budou postupně přicházet do styku i příslušníci AČR, je tento článek zaměřen na seznámení širší vojenské veřejnosti s možnými vojenskými aplikacemi moderní kryptografie.

Kryptografický systém

Předpokládejme odesílatele, který chce předávat zprávy určitému příjemci. Oba chtějí tyto zprávy přenášet utajeně - to znamená tak, aby přenášeným zprávám nikdo kromě nich neporozuměl. Proto odesílatel podle určitých pravidel změní formu zprávy takovým způsobem, aby se stala nesrozumitelnou. Zpráva je takzvaně zašifrována do podoby kryptogramu. Tento kryptogram je pak předán příjemci, který podle stanovených pravidel změní jeho formu zpět do srozumitelné podoby.

Odesílatel pomocí šifrátoru nejprve zašifruje zprávu Z do podoby kryptogramu C. Parametrem, který určuje výslednou konkrétní podobu kryptogramu, je šifrovací klíč K_E. Vytvořený kryptogram je následně přenesen sdělovacím kanálem k příjemci. Dění v kanálu může sledovat a případně i ovlivňovat nepovolaná osoba - protivník. Cílem kryptografie je zajistit, aby protivník ze zachyceného kryptogramu C nebyl schopen odvodit přenášenou zprávu Z. Na straně příjemce se v dešifrátoru pomocí dešifrovacího klíče K_D provádí zpětná transformace kryptogramu na původní zprávu Z. Tento převod se nazývá dešifrování [2].

Podle vzájemného vztahu mezi šifrovacím a dešifrovacím klíčem rozeznáváme symetrický a asymetrický kryptosystém. Pokud platí, že dešifrovací klíč K_D lze relativně snadno odvodit z šifrovacího klíče K_E (zpravidla $K_D=K_E$), pak se jedná o takzvaný symetrický kryptosystém. V takovém případě je nutné utajovat jak dešifrovací, tak i šifrovací klíč. Pokud platí, že dešifrovací klíč K_D je odlišný a prakticky neodvoditelný

z šifrovacího klíče K_E, pak se jedná o takzvaný asymetrický kryptosystém. V tomto případě je nutné utajovat pouze dešifrovací klíč (tzv. tajný klíč) a šifrovací (tzv. veřejný) klíč je veřejně znám. Proto se velmi často asymetrické kryptosystémy označují jako veřejné kryptosystémy.

V moderní kryptografii je důležitou funkcí tzv. autentizační funkce. Tato funkce jednoznačně přiřazuje libovolné zprávě o jakékoliv délce krátkou postupnost cca 16 až 32 znaků. Tato postupnost se označuje jako autentizační kód zprávy (anglicky *„Message Authentification Code"* - *MAC*). Autentizační funkce je konstruována tak, že je prakticky nemožné pro autentizační kód nějaké zprávy nalézt jinou zprávu se stejným kódem. Součástí autentizační funkce je určitý parametr - tzv. klíč autentizační funkce. Pokud je tento klíč veřejně známý, tak se autentizační funkce nazývá hašovací funkce (*hash function*) a autentizační kód zprávy se nazývá haš zprávy.

Služby soudobé kryptografie

Moderní kryptografické systémy v současné době nezajišťují jen utajený přenos zpráv, ale poskytují i nové služby. K těmto službám patří autentizace osob a zpráv (anglicky *„authentication"*), kontrola integrity zpráv (anglicky *„information integrity"*), průkaznost (anglicky *„non-repudiation"*) a notářské služby (anglicky *„notarization"*) [3].

Zmíněné služby nabývají v moderních komunikačních, informačních a řídících systémech velkého významu. Jde o to, že v rozlehlých a složitých systémech se protivník může na uvedené systémy nekontrolovaně napojit, a tak tento systém buď zneužívat, nebo ochromit. Proto je důležité, aby oprávnění uživatelé tohoto systému mohli na dálku a elektronickou cestou prokázat své oprávnění služby systému využívat. V tomto případě se jedná o tzv. autentizaci osob. Dále je důležité, aby příjemce zprávy získal zároveň s přijetím zprávy i důkaz, že odesílatelem této zprávy je osoba, která se jako odesílatel udává - tzv. autentizace zpráv. Taktéž se v rozsáhlých systémech požaduje, aby příjemce zprávy získal s přijetím zprávy i důkaz, že daná zpráva nebyla během přenosu účelově nějakou jinou osobou pozměněna - tzv. kontrola integrity zpráv. Často se vyžaduje i to, aby uživatelé systému nemohli později popírat skutečnost, že využili určitých služeb daného systému - tzv. průkaznost. Poslední z uvedených kryptografických služeb zajišťuje nezpochybnitelný záznam a případné zveřejnění určitých informací - tzv. notarizace zpráv.

Pro AČR je v současné době aktuální otázkou problém autentizace. V tomto případě se rozlišuje autentizace osob a autentizace zpráv. Autentizace osob se provádí při vstupu osob do chráněných prostorů nebo před použitím řídících, informačních nebo komunikačních systémů těmito osobami.

Cílem **autentizace osob** je ověřit zda příslušná osoba je tou osobou, za kterou se vydává, a má-li tudíž příslušná práva. Autentizace osob se v současné době provádí buď znalostí, nebo předmětem anebo kombinací znalosti a předmětu. Autentizace znalostí je založena na tom, že ověřovaná osoba musí prokázat znalost jisté utajované informace - v praxi se nejčastěji používá heslo. Další možností, kde se právě uplatňuje kryptografie, je využití tajného klíče asymetrického kryptografického systému. V tomto případě zařízení chránící přístup do systému předá ověřované osobě nějaké náhodné číslo. Ověřovaná osoba toto číslo zašifruje svým tajným klíčem a tento kryptogram předá

kontrolnímu zařízení. Uvedený kryptogram je v zařízení dešifrován veřejným klíčem ověřované osoby. Pokud je výsledek shodný s původním náhodným číslem, pak je prověřované osobě umožněn vstup do systému.

Uvedená autentizace se technologicky realizuje pomocí čipových karet - v tomto případě se pak jedná o autentizaci předmětem. Proti případnému zneužití karty při její ztrátě nebo krádeži jsou tyto karty chráněny ještě heslem - tj. znalostí. Takovýto způsob autentizace se používá například před zahájením každého telefonního hovoru u telefonů GSM nebo před každou transakcí u bankomatu. Popsaný způsob autentizace je považován za velmi bezpečný a dá se předpokládat jeho široké použití i v AČR. V této souvislosti by byla vhodná standardizace těchto karet pro AČR. Cílem této standardizace by mělo být to, aby uživatel měl jednu jedinou kartu, která by mu umožňovala autentizaci ve všech možných situacích - jak při vstupu do různých chráněných prostorů, tak při přihlašování do různých informačních nebo řídících systémů.

Dalším problémem je **autentizace zpráv**. V tomto případě jde o ověření zda danou zprávu skutečně odeslal ten, kdo se jako odesílatel udává. Jde tedy o zjištění, zda je zpráva věrohodná nebo podvržená. U symetrických kryptosystémů je autentizace jednoduchá - zpráva je autentická, protože zprávu mohl do daného kryptogramu správně zašifrovat pouze odesílatel, který zná tajný klíč. Složitější situace je u asymetrického kryptografického systému. Tam může pomocí veřejného klíče zprávu zašifrovat kdokoliv a v této zprávě se může vydávat za kohokoliv. V uvedeném případě se autentizace zpravidla zajišťuje digitálním podpisem. Haš zprávy se zašifruje tajným klíčem odesílatele a takto vzniklý kryptogram se připojí ke zprávě. Dvojice zpráva a zašifrovaný haš se odešle k příjemci zprávy. Na přijímací straně adresát přijatý zašifrovaný haš nejprve dešifruje veřejným klíčem odesílatele. Získá tak původní haš zprávy, který porovná s hašem přijaté zprávy. Pokud jsou obě porovnávané hodnoty stejné, pak zpráva pochází skutečně od udávaného odesílatele. Navíc uvedený postup zaručuje i to, že zpráva nebyla během přenosu pozměněna.

V této souvislosti je zapotřebí poznamenat, že problematika digitálního podpisu je pro AČR aktuální, protože v současné době v ČR probíhá legislativní proces, jehož cílem je digitální podpis právně zakotvit. Po právním zakotvení digitálního podpisu pak budou moci funkcionáři AČR podepisovat veškeré elektronické dokumenty.

Další kryptografickou službou je **kontrola integrity zpráv**. Cílem této služby je poskytnout příjemci zprávy důkaz, že daná zpráva nebyla během přenosu systémem účelově pozměněna nějakou neoprávněnou osobou. Tato služba se často zajišťuje šifrováním dané zprávy, a to i přesto, že obsah zprávy není důvěrný. Protivník pak může pozměnit pouze kryptogram, což příjemce ihned pozná, neboť dešifrovaný text nedává smysl. Další možností je použití digitálního podpisu. Odesílatel jednoduše zprávu digitálně podepíše a příjemce provede standardní kontrolu digitálního podpisu. Získá tak důkaz o tom, že zpráva byla, respektive nebyla pozměněna. Aplikace této služby se dá v AČR předpokládat především u softwarového vybavení prvků komunikačních, informačních a řídících systémů. Uvedeným způsobem se bude kontrovat například řídící software telefonních ústředen, řídících počítačů zbraňových systémů apod.

V rozsáhlých systémech - především řídících - se často vyžaduje, aby uživatelé systému nemohli později popírat to, že využili určitých služeb tohoto systému nebo

vydali systému určité příkazy - tzv. průkaznost. Uvedená služba je zpravidla založena na tom, že každý požadavek nebo příkaz uživatele systému je systémem akceptován jen s digitálním podpisem uživatele. Takto podepsané požadavky nebo příkazy se archivují na bezpečném místě, a tak je možno zpětně zjistit původce určitého požadavku nebo příkazu.

Poslední z uvedených kryptografických služeb je **notarizace zpráv**. Tato služba zajišťuje v technických systémech úlohu analogickou notáři. Zabezpečuje nezpochybnitelnou archivaci a případné zveřejnění určitých informací. K realizaci uvedené služby se používá digitální podepisování dokumentů notářem. Tyto dokumenty se spolu s příslušnými časovými údaji spravují důvěryhodným způsobem na bezpečném místě.

* * *

S rostoucí rozlehlostí a složitostí různých systémů (komunikačních, informačních, řídících, výrobních atd.) a s rostoucí mírou jejich automatizace se stává problémem zajištění jejich bezpečnosti. Jde o to, aby dané systémy plnily úlohy, ke kterým byly zřízeny a aby je nebylo možné zneužít. Na zajištění této bezpečnosti se významnou měrou podílí kryptografie. Současná kryptografie se dnes nevyužívá jen k utajenému přenosu zpráv, ale i k šifrovanému ukládání dat a programů. Dále se kryptografie používá k autentizaci osob a zpráv, ke kontrole neporušenosti dat, k digitálnímu podepisování, k platbám elektronickou cestou a podobně.

Použitá literatura:

[1] **Klíma,V.**: Bezpečnost a ochrana dat. Softwarové noviny, 1996, č. 2, s.35-44.
[2] **Grošek,O.-Porubský, Š.**: Šifrovanie. Praha, Grada 1991.
[3] **Schneier, B.**: Applied Cryptography. New York, John Wiley & Sons 1996.

Sám jste řekl, že řadu posádek vydržujete neefektivně.

To je pravda. Pracujeme na tom, abychom snížili infrastrukturu. V naší koncepci je stanoveno, že infrastruktura má být až o třetinu nižší. Na druhou stranu jsou zde určité problémy při opouštění některých posádek - Vimperk, Rokycany, Zbiroh. Opouštění má dvojí efekt. My tyto posádky sice nepotřebujeme, na druhou stranu to má pro tamní region nezanedbatelný negativní ekonomický dopad.

Generálporučík Ing. Jiří Šedivý, náčelník GŠ AČR,
„O profesionální armádě"
Televize ČT 2 - „21", 1. 9. 2000