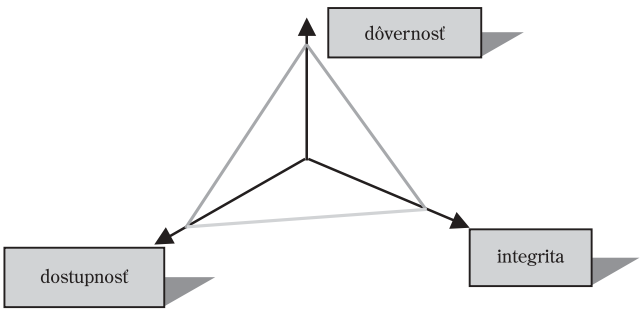
Mechanizmy zachovania integrity a dôvernosti správ

Mária Franeková

Úvod

Komunikačná bezpečnosť je nevyhnutná súčasť bezpečnosti informačného systému, ktorý môže slúžiť na archiváciu, spracovanie a prenos informácií v rôznych aplikáciách. V úvodnom príspevku (AT&P journal 11/2003) boli uvedené základné zložky bezpečnosti komunikácie, medzi ktoré patrí: dôvernosť, integrita a dostupnosť (obr. 1).



Obr.1 Základné zložky komunikačnej bezpečnosti

Bezpečnostná služba na zaistenie dôvernosti prenosu správ poskytuje ochranu proti neautorizovanému odhaleniu. Podľa ISO/OSI 7498/2 [1] sa dôvernosť užšie špecifikuje na: dôvernosť spojenia, prenosu správ, selektívnu dôvernosť a dôvernosť toku dát.

Bezpečnostná služba zaistenia integrity správ slúži na ochranu prenášaných dát pred neautorizovanou modifikáciou alebo zmenou pod vplyvom šumového prostredia a podľa [1] sa delí na: integritu prenosu správ, selektívnu integritu a integritu spojenia.

Obidve služby treba pokladať za základné bezpečnostné služby otvoreného prenosového systému, prostredníctvom ktorého komunikujú železničné zabezpečovacie systémy (úvodná problematika bola opísaná v AT&P journale 11/2003).

1. Mechanizmy zachovania integrity správ

Integritu správ, narušenú vplyvom šumového prostredia komunikačného kanála (označovanú podľa [1] aj ako slabú integritu), možno podľa normy pre otvorené prenosové systémy [2] ochrániť pomocou vhodne zvoleného bezpečnostného kódu (v teórii kódovania sa používa skôr označenie kanálový kód – channel code). Podľa [2] môžu byť na zabezpečenie prenosu použité iba detekčné bezpečnostné kódy, t. j. kódy pracujúce v režime ARQ (automatic request repetition).

Pri výbere bezpečnostného kódu vzhľadom na špecifiká prenosu treba kód hodnotiť podľa týchto kritérií:

- schopnosť detekcie systematických a náhodných chýb,
- aby pravdepodobnosť nedetegovanej chyby bola pod garantovanou hranicou,
- rýchlosť kódovacieho a dekódovacieho algoritmu (správa je platná len určitý čas, cyklický charakter prenosu),
- praktická realizácia algoritmu.

Najviac používaným detekčným kódom v tejto oblasti je blokový systematický cyklický kód, ktorý pracuje na princípe CRC-r (cyclic redundancy check). Dokáže detegovať jednoduché chyby a náhodné zhluky chýb dĺžky r, kde r je stupeň generujúceho polynómu $g(x)$ kódu.

V teórii kanálového kódovania však existuje množstvo efektívnych kódovacích a dekódovacích techník, ktoré síce patria do množiny samoopravných kódov (tzv. techniky FEC – forward error control), ale pri dekódovaní sa dá jednoznačne vyčleniť časť súvisiaca s detekciou, čo by umožnilo použiť techniky FEC v aplikáciách definovaných podľa [2]. Na druhej strane však treba skonštatovať, že niektoré techniky samoopravných kódov nemajú (bez zásahu do algoritmu) jasne oddeliteľnú časť detekcie a korekcie. Ide o techniky konvolučných kódovacích štruktúr, ktoré pracujú na princípe maximálne pravdepodobnostného dekódovania. Spomínaná vlastnosť sa dá jednoducho realizovať len pri množine blokových, systematických kódov využívajúcich syndrómové techniky dekódovania, akými sú napr. Hammingove, Bose Chaudhuriho Hocquenghove (BCH) a Reedove-Solomonove (RS) kódy. Na základe hodnoty syndrómu sa určí, či pri prenose v danom kódovom slove došlo, resp. nedošlo k narušeniu správy.

Pri použití týchto typov blokových kódov pre potreby ochrany prenosu v železničných aplikáciách je nutné vypočítať pravdepodobnosti nedetegovanej chyby v kódovom slove a zvážiť, či výsledná hodnota, ktorá vyjadruje pravdepodobnosť zlyhania dekodéra, je vyhovujúca.

Pre blokové systematické (n, k, t) kódy, so známou váhovou funkciou kódových zložiek A_i možno pravdepodobnosť nedetegovanej chyby kódového slova p_{ned} pre binárny symetrický kanál BSC vypočítať podľa:

$$p_{ned} \geq \sum_{i=\left\| \frac{d_{\min}+1}{2} \right\|}^{n} A_i p_b^i (1-p_b)^{n-i} \qquad (1)$$

kde $d_{\min}$ je minimálna Hammingova vzdialenosť kódu,
A_i – celkový počet kódových slov s váhou i v kódovom slove dĺžky n,
p_b – bitová chybovosť kanála,
$||x||$ – predstavuje celočíselnú hodnotu.

Váhová funkcia kódu sa dá matematicky vyjadriť len pre niektoré typy blokových kódov, napr. pre Hammingove a Reedove-Solomonove kódy.

Pre cyklické kódy CRC-r sa pravdepodobnosť nedetegovanej chyby, alebo zvyškovej chybovosti p_{zvys} aproximuje vzťahom (2):

$$p_{zvys} = 2^{(d_s-2-r)} / 2^{(d_s-2)} = 2^{-r} \qquad (2)$$

kde d_s predstavuje dĺžku zhluku chýb pri prenose,
r je redundancia kódu alebo stupeň generujúceho polynómu.

Pre znakové Reedove-Solomonove kódy v Galoisovom poli GF (2^m) možno určiť odhad pravdepodobnosti chyby symbolu p_s pri prenose cez kanál BSC podľa:

$$p_s = \frac{1}{2^{m-1}} \sum_{j=t+1}^{2^{m-1}} j \binom{2^m}{j} p_b^j (1-p_p)^{2^m-1-j} \qquad (3)$$

kde m predstavuje počet bitov na symbol,
t je počet korigovaných znakov,
p_b je bitová chybovosť kanála.

Silná integrita sa definuje v prípade hrozby útoku aktívnym útočníkom. Je zaručená prostriedkami na zaručenie slabej integrity

a doplnená o aplikácie prostriedkov kryptografie, najmä s použitím bezpečných hašovacích funkcií v kombinácii s asymetrickou kryptografiou. Kryptografické hašovacie funkcie patria medzi základné stavebné bloky kryptografických algoritmov [3]. Niektoré hašovacie funkcie sú porovnateľné s funkciami zabezpečujúcimi integritu údajov, čo realizujú pomocou mapovania veľkej množiny dát na podstatne menšiu množinu (hašovaciu hodnotu – odtlačok). Hašovacie funkcie musia spĺňať požiadavky jednocestnosti – one way function (praktická nemožnosť z hašovacej hodnoty určiť pôvodnú správu), odolnosti proti kolíziám (praktická nemožnosť nájsť dve rovnaké správy, ktoré poskytujú rovnakú hašovaciu hodnotu) a jednoduchosti výpočtu.

V súčasnej dobe existuje niekoľko modelov nekľúčovaných a kľúčovaných hašovacích funkcií:

Nekľúčované:
- všeobecný model iteračnej hašovacej funkcie,
- hašovacie funkcie založené na báze blokových šifier – typu MDC (modification detection code) MD2, MD4, MD5,
- hašovacie funkcie založené na modulárnej aritmetike – typu MASH (modular arithmetic secure hash) MASH-1, 2,
- jednoúčelové hašovacie funkcie:
- typu MD (message digest) MD2, MD4, MD5,
- typu SHA (secure hash algorithm) SHA 1/256/384/512,
- typu RIPEMD-128/256/160/320.

Kľúčované:
- MAC a jeho modifikácie (message authentication code).

Z uvedených typov sa za výpočtovo bezpečné dnes považujú funkcie s najvyššou hodnotou hašovacieho reťazca [4].

2. Mechanizmy zachovania dôvernosti správ

V súčasnej dobe existuje množstvo kryptografických techník na báze symetrického, asymetrického alebo kombinovaného spôsobu šifrovania [3], [4], ktoré môžu byť použité na zachovanie dôvernosti správ.

Pri výbere kryptografickej techniky podľa [2] treba vziať do úvahy špecifikácie prenosu v rámci otvoreného systému, čo vyžaduje splnenie požiadaviek na:
- rýchlosť algoritmu,
- bezpečnosť algoritmu,
- praktickú realizovateľnosť algoritmu.

Treba si uvedomiť, že na rozdiel od techník kanálového kódovania, kryptografické mechanizmy zahŕňajú použitie nielen algoritmov, ale aj metód na generovanie, prenos a archiváciu kľúčov. Vývoj kryptografie je omnoho dynamickejší ako vývoj techník kanálového kódovania. Ak sa šifra stane štandardom, tento je prijímaný na dobu maximálne 5 – 10 rokov a sila jeho algoritmu musí byť pravidelne prehodnocovaná. Pre prenosové systémy súvisiace s bezpečnosťou treba vziať do úvahy pri výbere kryptografických mechanizmov aj túto skutočnosť a vychádzať z najmodernejších, odbornou verejnosťou posúdených algoritmov.

Pre železničné aplikácie požiadavku dôvernosti správy z dôvodu vyššej rýchlosti lepšie spĺňajú šifrovacie algoritmy pracujúce na báze systému s tajným kľúčom v porovnaní so systémom s verejným kľúčom. V norme [2] sa na tieto účely odporúča etalón symetrickej kryptografie – algoritmus DES, ktorý je celosvetovou normou viac ako 20 rokov. Výhody jeho použitia v železničných aplikáciách:
- rýchlosť šifrovania/dešifrovania,
- cyklický charakter algoritmu (vhodnejšie pre HV realizáciu),
- jeden algoritmus pre šifrovanie aj dešifrovanie.

Algoritmus DES v súčasnej dobe však už nepatrí medzi výpočtovo bezpečné šifry [5]. Medzi jeho najväčšie bezpečnostné slabiny patrí: malá dĺžka kľúča, existencia slabých, poloslabých a potenciálne

symetrické šifrovacie algoritmy			
DES	**RC**	**AES**	**iné**
Data Encryption Standard	Rivest Cipher	Advanced Encryption Standard	
2-DES	RC4	Mars	IDEA
3-DES	RC5	Serpent	Blowfish
FEAL	RC6	Twofish	Skipjack
		RC6	Safer
		Rijndael	GOST

Tab.1 Najpoužívanejšie symetrické šifrovacie algoritmy

slabých kľúčov, malý počet permutácií v algoritme, utajené časti algoritmu S boxov a ich malá nelinearita.

Perspektívne treba počítať s voľbou niektorého z nástupcov DES. V tab. 1 je znázornený prehľad symetrických šifrovacích algoritmov, ktoré boli vyvinuté s cieľom nahradiť DES.

Štandard, ktorý bol odbornou verejnosťou v súťaži s pracovným názvom AES (Advanced Encryption Standard) určený za štandard tohto tisícročia je algoritmus Rijndael [6]. Je to iteračná bloková šifra, ktorá bola skonštruovaná na „dobrých" základoch algoritmu DES. Rijndael používa opakujúce sa kolá s variabilnou dĺžkou bloku a variabilnou dĺžkou kľúča. Dĺžka vstupného a výstupného bloku je definovaná 128 bitmi, ale šifra môže podporovať aj bloky väčších dĺžok. Dĺžka kľúča je voliteľná spomedzi 128, 192 alebo 256 bitov. Rijndael bol implementovaný SV aj HV na rozličných procesoroch s veľmi malými nárokmi na pamäť aj veľkosť kódu, v čipových kartách a špecializovanom hardvéri. Je vhodný aj pre paralelné spracovanie. Z hľadiska bezpečnosti je Rijndael pokladaný za výpočtovo bezpečnú šifru a na jeho kryptoanalýzu zatiaľ neexistuje žiaden efektívny algoritmus. Pri jeho návrhu boli vzaté do úvahy známe útoky a samotný algoritmus bol navrhnutý tak, aby týmto útokom čo najefektívnejšie odolával. Rijndael bol testovaný na existenciu slabých kľúčov DESovského typu, slabých kľúčov typu IDEA, na odolnosť voči diferenciálnej a lineárnej kryptoanalýze, ďalej tzv. truncated differentials attack, square attack, interpolačnému útoku a útoku pomocou príbuzných kľúčov.

Algoritmus Rijndael sa môže použiť ako symetrická bloková šifra, ale je možné jeho použitie aj pri iných aplikáciách:
- ako bloková šifra v algoritme CBC-MAC (cipher block chaining),
- ako iteračná hašovacia funkcia, pričom samotný algoritmus slúži ako kolová funkcia,
- pomocou modu OFB (output feedback) možno Rijndael použiť ako synchrónnu prúdovú šifru, resp. v mode CFB (cipher feedback) ako samosynchronizujúcu prúdovú šifru,
- pomocou algoritmu Rijndael možno vytvoriť generátor pseudonáhodných čísel.

Záver

Cieľom tohto príspevku bol opis bezpečnostných mechanizmov, ktoré sú vhodné na ochranu dôvernosti a integrity správ prenášaných v rámci otvorených prenosových systémov medzi železničnými zabezpečovacími zariadeniami súvisiacimi s bezpečnosťou železničnej prevádzky.

Na zachovanie integrity správ boli naznačené nekonvenčné spôsoby použitia kanálových kódovacích techník z množiny samoopravných kódov FEC, z ktorých sa vzhľadom na špecifikum prenosu ako perspektívne javia nebinárne Reedove-Solomonove kódy. Bol predstavený matematický aparát na výpočet pravdepodobnosti chyby dekódovacích, syndrómových techník pri blokových, lineárnych a systematických kódoch.

V otázke zachovania dôvernosti správ boli naznačené možnosti výberu kryprografického a hašovacieho kódu so zameraním na výpočtovo bezpečné algoritmy. Pre otvorené prenosové systémy súvisiace s bezpečnosťou sú vhodné rýchle algoritmy symetrických blokových šifier v kombinácii s blokovými hašovacími funkciami.

Perspektívnou náhradou za algoritmus DES sa javí algoritmus Rijndael, ktorý z hľadiska bezpečnosti je v súčasnosti pokladaný za výpočtovo bezpečnú šifru. Pri výbere symetrického šifrovacieho algoritmu je nutné venovať pozornosť problematike kľúčového hospodárstva, bezpečnému generovaniu, archivácii a prenosu kľúčov.

Literatúra

[1] HANÁČEK, P., STAUDEK, J.: Bezpečnost informačních systémů. Metodická príručka. Úřad pro státní informační systém 2000.

[2] ČSN EN 50159-2 Drážní zařízení. Sdělovací a zabezpečovací systémy a systém zpracování dat. Část 2: Komunikace v otevřených přenosových zabezpečovacích systémech. ČTN 2002.

[3] MENEZES, A., VAN OORSCHOT, VASTONE, S.: Handbook for Applied Cryptography. CRC Pres 1996.

[4] STALLINGS, W.: Cryptography and Network Security. Principles and Practise. Prentice Hall 2003.

[5] PŘIBYL, J., KODL, J.: Ochrana dat v informatice. ČVUT, Praha 1996.

[6] DAEMEN, J., RIJMEN, V.: AES Proposal: Rijndael. Leuven 2002.

Ing. Mária Franeková, PhD.

Katedra riadiacich a informačných systémov
Elektrotechnická fakulta
Žilinská univerzita