Mechanizmy bezpečnej komunikácie používané v otvorených prenosových systémoch

Mária Franeková

Článok je venovaný problematike bezpečnosti dát v prenosových systémoch súvisiacich s bezpečnosťou definovaných v rámci železničného dopravného procesu. Úvodná časť je zameraná na sumár hrozieb a ochrán pre otvorené prenosové systémy. Podrobnejšie bude uvedená možnosť použitia kanálových kódovacích a kryptografických mechanizmov definovaných normou EN 50159-2 za účelom zachovania integrity a dôvernosti prenosu.

Úvod

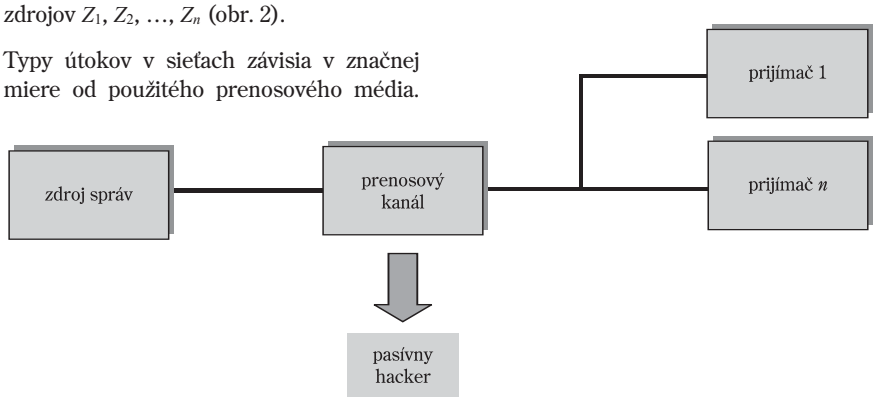
Prostredníctvom informačných a komunikačných technológií dochádza k manipulácii s informáciou v jej troch základných formách, ktorými sú: prenos, archivácia a spracovanie. Často ide o informácie veľkých hodnôt (tzv. citlivé informácie), pričom nesprávne zaobchádzanie s nimi môže viesť k majetkovým stratám alebo k ujme na cti (napr. pri zdravotných záznamoch, daňových priznaniach, bankových účtoch, obchodných záznamoch), či dokonca k stratám na životoch (napr. pri informáciách z oblasti riadenia dopravy). Takéto informácie musia byť chránené tak, aby k nim mali prístup len oprávnené osoby, aby sa dalo zistiť, kto informáciu vytvoril, zmenil, alebo odstránil, aby informácia nebola prezradená, ale aby bola dostupná, keď je to potrebné. Informačné a komunikačné technológie tvoria väčšinou informačný systém, ktorý je bezpečný natoľko, nakoľko je bezpečný jeho najmenej bezpečný článok [1]. Komunikačné cesty predstavujú jedno z najdôležitejších a zároveň najzraniteľnejších miest informačného systému. Komunikačná bezpečnosť rieši problematiku ochrany komunikácie medzi jeho jednotlivými komponentmi.

Bezpečnostné požiadavky elementov komunikačného systému závisia od toho, v akých aplikáciách je tento systém používaný. V prípade prenosu správ pre potreby železničného dopravného procesu je výber jeho častí špecifikovaný normami [2], [3]. Takýto prenos dostáva prívlastok „prenos súvisiaci s bezpečnosťou“ (z ang. safety-related transmission). Komunikačná bezpečnosť je vo všeobecnosti definovaná zachovaním:

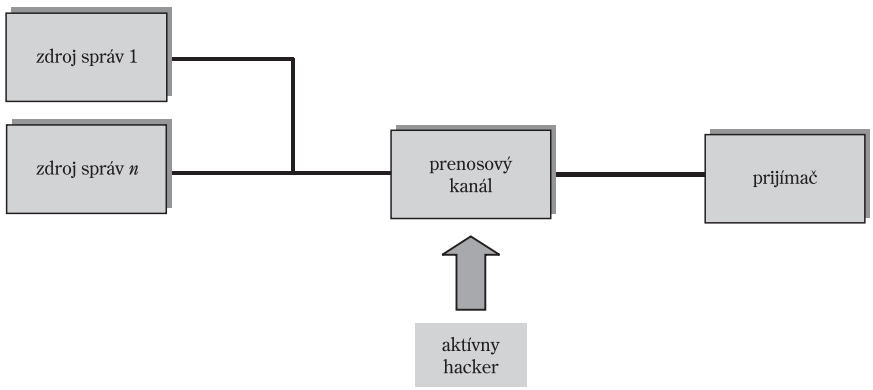
- dôvernosti – k údajom majú prístup len autorizované subjekty,
- integrity – dáta môžu byť modifikované len autorizovanými subjektmi a pôvod informácie je overiteľný,
- dostupnosti – dáta sú autorizovaným subjektom do určitej doby prístupné a nedochádza k odmietnutiu služby.

Útoky na správy pri prenose sa môžu vykonávať neúmyselne, napr. vplyvom šumového prostredia prenosového kanála alebo úmyselne, prostredníctvom nekompetentnej osoby. Z hľadiska hrozieb v otvorených prenosových systémoch nás zaujímajú najviac hrozby úmyselné, spôsobené vonkajšími a vnútornými útočníkmi (hackeri, zlyhanie ľudského faktora a pod.). Útok v rámci prenosu možno najčastejšie vykonávať prostredníctvom prerušenia komunikácie, odpočúvaním komunikácie a modifikáciou správ. V prípade vykonávania pasívneho útoku odpočúvaním správ komunikácia na úrovni end-to-end predstavuje problém existencie niekoľkých prijímačov P_1, P_2, …, P_n (obr. 1) a v prípade vykonávania aktívneho útoku modifikáciou správ je tu problém existencie viacerých zdrojov Z_1, Z_2, …, Z_n (obr. 2).

Typy útokov v sieťach závisia v značnej miere od použitého prenosového média. Na ich elimináciu sú definované bezpečnostné funkcie, ktoré sa v komunikačnej infraštruktúre implementujú prostredníctvom bezpečnostných mechanizmov. V súčasnosti existuje viacero noriem a kritérií, v ktorých sú definované bezpečnostné funkcie a mechanizmy v rámci komunikácie, pričom každá norma používa iné kritériá s rozličných členením do tried. Snáď najglobálnejší pohľad ponúka štandard ISO/OSI 7498-2 [4], ktorý definuje bezpečnosť komunikácie v rámci sedemvrstvového modelu OSI [5]. Štandard definuje základné bezpečnostné služby pre komunikačné siete, ktoré komunikujú v rámci 7-vrstvového modelu OSI (Open system inter-connection). Štandard bol vydaný aj ako odporúčanie ITU-T X.800. Bezpečnostné služby podľa ISO 7498-2 môžu byť



Obr.1 Úmyselné útoky pasívne (odpočúvanie správ)



Obr.2 Úmyselné útoky aktívne (modifikácia správ)

v praxi implementované v rôznych vrstvách komunikačného protokolu.

1. Ohrozenia a bezpečnostné mechanizmy otvoreného systému

Komunikácia medzi časťami zabezpečovacieho systému sa uskutočňuje buď cez otvorený, alebo uzavretý prenosový systém. Uzavreté prenosové systémy [6] sú charakterizované určitou kontrolou nad systémom, známymi charakteristikami a počtom komunikujúcich účastníkov. Druhá trieda – otvorené prenosové systémy [7] zahŕňa všetky systémy, ktorých charakteristiky sú neznáme, resp. čiastočne známe, ktoré sa v rámci životného cyklu menia a ktorým hrozí narušenie správ aj z vonkajšieho prostredia (napr. cez sieť internet).

Podľa [7] sa prístup k zariadeniam súvisiacim s bezpečnosťou $ZSB_1, \ldots, ZSB_n$ (safety-related equipment), ktoré sú pripojené na otvorený prenosový systém, musí realizovať prostredníctvom špeciálneho bezpečnostného rozhrania prístupovej ochrany RPO (obr. 3). Implementácia bezpečnostných funkcií do RPO závisí od typu ohrozenia, predpokladaného v rámci otvoreného systému. Podľa [7] je definovaných sedem tried otvorených prenosových systémov. Najvyšší stupeň ohrozenia predstavuje sieť internet a širokopásmové siete typu WAN vrátane mobilných a rádiových sietí.

Podľa normy platnej pre otvorené systémy sú definované pri komunikácii tieto typy ohrozenia: opakovanie, vymazanie, vloženie, preradenie, poškodenie, oneskorenie a maskovanie správ. Na elimináciu týchto ohrození je potrebné použiť silné bezpečnostné mechanizmy.

ohrozenia	ochrany							
	poradové číslo	časová pečiatka	uplynutie času	identifikátory zdroja a miesta určenia	spätnoväzobná správa	identifikačná procedúra	bezpečnostný kód	kryptografické techniky
opakovanie	X	X						
vymazanie	X							
vloženie	X			X	X	X		
zmena poradia	X	X						
poškodenie							X	X
oneskorenie		X	X					
maskovanie					X	X		X

Tab.1 Matica ohrození/ochrán podľa EN 50159-2

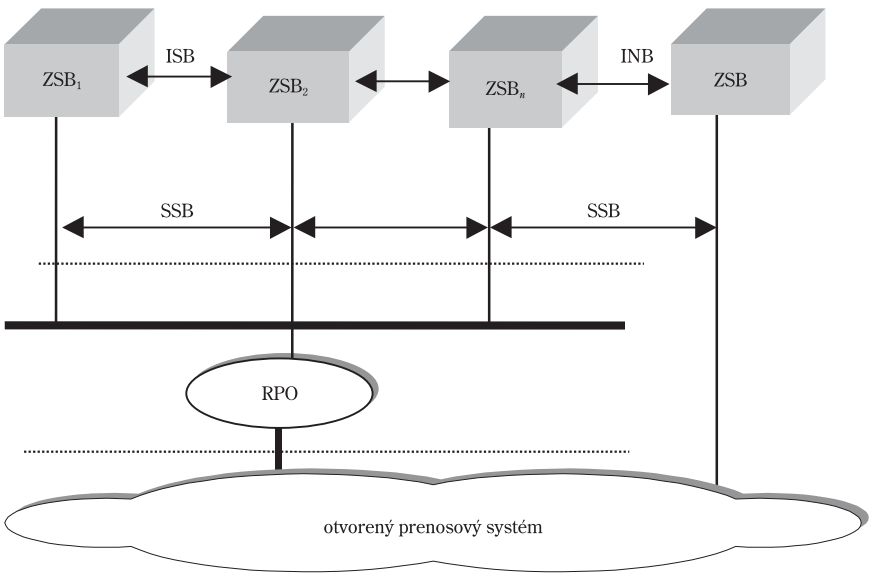
Prehľad ochrán definovaných v [7] je uvedený v tab. 1.

Záver

S rozvojom informačných a komunikačných technológií rastie význam riešenia bezpečnosti dát počas komunikácie. Komunikáciu medzi zabezpečovacími zariadeniami možno realizovať v rámci uzatvoreného, alebo otvoreného prenosového systému. Trendom v železničnej sieti je použitie otvoreného prenosového prostredia, s možnosťou prepojenia komunikácie na verejnú telefónnu a dátovú sieť, alebo Internet.

Cieľom tohto príspevku bol opis útokov a bezpečnostných mechanizmov vhodných na ochranu správ prenášaných v rámci otvorených prenosových systémoch medzi železničnými zabezpečovacími zariadeniami súvisiacimi s bezpečnosťou. Pri výbere vhodných bezpečnostných opatrení treba vychádzať zo súčastného stavu komunikačnej infraštruktúry a z typov ohrození, ktoré v tomto prostredí vznikajú.

Útoky na správu typu poškodenie (corruption) a maskovanie (masquerade) možno eliminovať s použitím rýchlych kanálových kódovacích a dekódovacích techník a prostriedkov, pracujúcich na báze modernej kryptografie. To však bude témou ďalšieho voľne naväzujúceho príspevku.



ZSB – zar. súvisiace s bezpečnosťou (Safety-related equipment)
ZNB – zar. nesúvisiace s bezpečnosťou (Non safety-related equipment)
ISB – informácia súvisiaca s bezpečnosťou (Safety-related information)
INB – informácia nesúvisiaca s bezpečnosťou (Non safety-related information)
SSB – správa súvisiaca s bezpečnosťou (Safety related message)
SNB – správa nesúvisiaca s bezpečnosťou (Non safety-related message)
RPO – rozhranie prístupovej ochrany (Access protection process)

Obr.3 Komunikácia prostredníctvom otvoreného prenosového systému

Literatúra

[1] DOBDA, L.: Ochrana dat v informačních systémech, Grada, Praha, 1998

[2] RÁSTOČNÝ. K., ZAHRADNÍK, A.: Železničné zabezpečovacie systémy, AT&P Journal, 9/2002, s. 34-36

[3] KUNHART, M.: Design of Interlocking RAMS Parameters, 11. Medz. konferencia ŽU v Žiline, Veda, vzdelávanie a spoločnosť, 17.-19.9.2003, s.141-144

[4] HANÁČEK, P., STAUDEK, J.: Bezpečnost informačních systému, metodická príručka, Úřad pro státní informační systém, 2000

[5] KÁLLAY, F., PENIAK, P.: Počítačové síte a jejich aplikace, Grada, Praha, 1999

[6] ČSN EN 50159-1 Drážní zařízení – Sdělovací zabezpečovací systémy a systém zpracovaní dat, Část 1: Komunikace v uzavřených přenosových zabezpečovacích systémech., ČTN, april 2002

[7] ČSN EN 50159-2 Drážní zařízení – Sdělovací a zabezpečovací systémy a systém zpracovaní dat, Část 2: Komunikace v otvořených přenosových zabezpečovacích systémech, ČTN, máj 2002

Ing. Mária Franeková, PhD. 8

**Katedra riadiacich a informačných systémov
Elektrotechnická fakulta
Žilinská univerzita**