

RFID: Výhodné je mať veci pod kontrolou

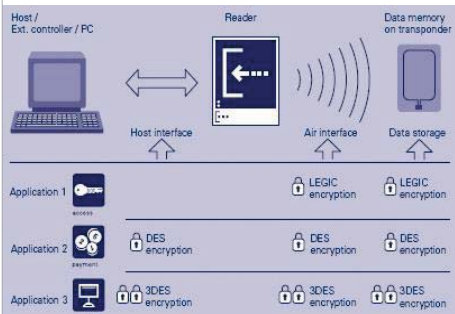
Bezkontaktné technológie na identifikáciu RFID (Radio Frequency Identification – identifikácia s využitím rádiových frekvencií) sa rýchlo udomácnujú vo viacerých oblastiach nášho života. Zamestnaní už bežne poznajú ID karty alebo prívesky z evidencie dochádzky alebo objednávania stravy v závodnej jedálni. Množstvo cestujúcich alebo lyžiarov zas ako cestovný lístok alebo permanentku.

Jadrom systémov sú rádiové frekvencie čipy, ktoré zaisťujú rýchlu a odolnú identifikáciu osôb, zvierat a predmetov. Čipy sú zapuzdrené napríklad v identifikačnej karte alebo prívesku (dochádzkové a prístupové systémy), diskovom transpondéri (dopravné prostriedky, kontajnery), sklenom transpondéri (zvieratá, cenné predmety) alebo samolepiacej etikete (identifikácia tovarov). V závislosti od typu aplikácie sa používajú čipy, ktoré majú svoje jedinečné číslo UID (Unique Identification Number), dané výrobcom, alebo čipy, ktoré okrem UID ponúkajú na uloženie informácií aj pamäťový priestor vo forme EEPROM.

Existuje viacero technológií a aj výrobcov čipov RFID. Ako sa v tejto „džungli“ orientovať? Technológie sa väčšinou podobajú využívanou frekvenciou a použitou normou ISO. Tie najstaršie využívajú frekvenciu 125 kHz (napr. RO čipy EM Marin) a pre svoju momentálnu cenovú dostupnosť sa u nás najviac využívajú, pokiaľ ide

o počet aplikácií. Novšie technológie používajú frekvenciu 13,56 MHz (napr. čipy RW Mifare Classic) a sú u nás najrozšírenejšie, čo sa týka počtu vydaných ID kariet (študentské ID karty, osobná doprava).

V krajinách, kde sa RFID využíva dlhšie, je dnes samozrejme využitie jedného čipu RW na viaceré aplikácie. Pri takýchto systémoch je



najdôležitejšia spoľahlivosť a hlavne vysoká bezpečnosť uložených informácií. Dnes je realitou vytvorenie duplikátu čipu využívajúceho 125 kHz. Niektoré technológie 13,56 MHz sú na tom lepšie, lebo na zabezpečenie uložených informácií využívajú prístupové kľúče a prenos medzi čipom a čítačkou jednotkou je zabezpečený napr. šifrovacou technológiou 3DES. Sú však známe prípady, keď boli pre nedostatočné fyzické zabezpečenie prístupových kľúčov narušené aj takéto systémy. Prednedávnom bola zverejnená informácia o možnosti vytvorenia klonu čipu Mifare Classic. V čom môže byť bezpečnostný problém? Napríklad v tom, ako a kde sú prístupové kľúče uložené, kto kľúče vytvára a ako sa kľúče zapisujú do čítacích obvodov a systémov.

Priekopníkom v tejto oblasti je švajčiarska spoločnosť Legic, ktorá ako prvá na svete v roku 1992 predstavila bezkontaktnú a bezpečnú

smart card technológiu pracujúcu s frekvenciou 13,56 MHz. Samozrejme pri tejto technológii je využitie 3DES šifrovania komunikácie medzi čipom a čítačím obvodom a priekopnícky a zatiaľ nikým nenapodobený systém generovania, archivácie a prenosu prístupových kľúčov (master tokenov) do čipov a čítacích obvodov prostredníctvom RF komunikácie z formátovacích ID kariet. To všetko až pre 127 nezávislých aplikácií s definovateľným priestorom na jednom čipe.

Takýto systém umožňuje, aby dodávateľ systému nemal v žiadnom prípade prístup k prístupovým kľúčom zákazníka. Takisto je zabezpečené, že radový zamestnanec organizácie, ktorý zapisuje do čítacích obvodov novo doda-



ných čítacích jednotiek prístupové kľúče, nepracuje s prístupovým kľúčom napísaným na papieri.

Na záver mi zostáva len dodať, že je určite lepšie mať systém pod kontrolou ako sa cítiť bezpečne.

■ Ing. MIROSLAV TREPÁČ, konateľ, WEGA LH, s. r. o.

Vyjadrenie zákazníka: Úspešné nasadenie KERBERa

1. Ako dlho spolupracujete s firmou SOMI Systems, a. s.?

S firmou SOMI Systems, a. s., spolupracujeme od roku 2003, keď sme pri nasadzovaní celopodnikového informačného systému využili ich bohaté skúsenosti v oblasti operačných systémov Linux. Neskôr sa vďaka kvalitným a spoľahlivo fungujúcim riešeniam spolupráca rozšírila aj na sieť LAN na báze metalických a optických prvkov.

2. Na aký účel ste nasadili náš produkt KERBER?

Pred nasadením riešenia KERBER sme na zabezpečenie pripojenia do internetu používali rôznorodé systémy a produkty, ktorých administrácia bola zložitá a neprehľadná. Nasadením produktu KERBER sme chceli zabezpečiť

komplexné riešenie obsahujúce hlavne firewall, antivírus a antispam, a to všetko s možnosťou jednoduchého správy. V neposlednom rade sme ho zvolili aj preto, že okrem už spomínaných funkcií umožňuje riadené pripojenie našich zamestnancov do internetu.

3. Aký bol prínos pre vašu firmu?

KERBER nám v prvom rade priniesol komplexný nástroj na správu pripojenia do internetu. Redukciou viacerých systémov do jedného sa znížili náklady na vlastníctvo. Znížil sa počet vírusov a rapídne sa zredukoval objem nevyžiadanej pošty, ktorá denne zatažovala e-mailové schránky našich zamestnancov. Aplikáciu rôznych pravidiel na prístup



na internet pre našich zamestnancov sa výrazne znížilo vyťaženie internetového pripojenia. A vďaka jednoduchému správe sa zjednodušila aj moja práca.

4. Aké sú vaše ďalšie plány s týmto produktom?

V budúcnosti plánujeme intenzívnejšie rozširovať funkcionality VPN a všetkým našim zamestnancom pracujúcim mimo firmy poskytnúť zabezpečené pripojenie do podnikovej siete prostredníctvom šifrovaného tunela VPN.



■ ŠTEFAN STIERANKA, systémový administrátor PPS Group, a. s.



SOMI Systems a. s.
ČSA 25, 974 01 Banská Bystrica,
e-mail: obchod@somisk, www.kerber.sk