Špecifiká použitia kryptografie v bezpečnostne relevantnom priemyselnom komunikačnom systéme

Mária Franeková

Článok je venovaný problematike použitia kryptografických mechanizmov v priemyselnom komunikačnom systéme, najme pre aplikácie riadenia bezpečnostne relevantných procesov s vyššou úrovňou integrity zabezpečenia SIL (*Safety Integrity Level*).
Kľúčové slová: priemyselný komunikačný systém, zabezpečenie informácií, bezpečnosť, kryptografické algoritmy, hašovacie funkcie, schémy digitálneho podpisu.

The article is concerned in topic of using of cryptographic technology in industrial communication systems, particularly in control applications of safety-related processes with higher SIL (*Safety Integrity Level*).
Keywords: industrial communication system, cybersecurity, safety, cryptographic algorithms, hash functions, digital signature technologies.

1. Úvod

Kryptografické metódy sú niekoľko desiatok rokov bežnými ochrannými prostriedkami v oblasti hardvérových zariadení COTS (*Commercial Off The Shelf*) používaných napr. vo finančnej sfére (bankový sektor, elektronický obchod) alebo v podnikových, kancelárskych informačných a komunikačných sieťach, avšak pre použitie v priemysle sú odporúčané len niekoľko posledných desiatok rokov. Svet priemyselnej komunikácie, ktorý donedávna používal proprietárne riešenia a väčšinou nepodporoval žiadne metódy založené na kryptografii, postupne prechádza na otvorené riešenia a snaží sa dohnať svet informačnej a komunikačnej techniky (ICT – *Information and Communication Technology*) aj v oblasti kryptografie a celkového vylepšenia bezpečnostného manažmentu aplikácií.

Dvere pre kryptografické mechanizmy v priemysle otvára hlavne nárast používania bezdrôtovej komunikácie a priemyselnej komunikácie so vzdialenými pracoviskami cez verejné siete. Dnes je už zrejmé, že bezdrôtové komunikačné systémy majú v automatizácii veľký potenciál, o čom svedčí (okrem už zaužívaných kancelárskych štandardov Wi-Fi, Bluetooth, ZigBee apod.) používanie relatívne nových štandardov zameraných na automatizáciu procesnej výroby, ako sú WirelessHART, WIA-PA a ISA 100.11a.

Posun integrácie bezdrôtových zariadení je zaznamenaný aj v špecifickej oblasti riadenia procesov, kde sú potrebné systémy (resp. zariadenia) s prívlastkom bezpečnostne relevantné (*safety-related*). Na vysvetlenie treba poznamenať, že systém je bezpečnostne relevantný, ak pri jeho prevádzke je vysoká pravdepodobnosť, že jeho nesprávne fungovanie vyvolá niektorý z nasledujúcich dôsledkov: stratu života, zranenie alebo ohrozenie osôb, vážne škody na životnom prostredí, významné straty alebo škody na majetku, nesplnenie dôležitého poslania či závažné hospodárske škody. Medzi bezpečnostne relevantné úlohy riadenia procesov patrí napr. riadenie všetkých druhov dopráv, procesov súvisiacich s distribúciou elektrickej energie alebo zemného plynu, procesov v jadrových elektrárňach, výrobných procesov v chemickom priemysle apod.

Zabezpečením na báze rôznych kryptografických schém a protokolov je potrebné sa zaoberať nielen na technologickej úrovni riadenia, ale aj vo vyšších vrstvách distribuovaného systému riadenia (DCS – *Distributed Control System*), napr. v spojení so systémami SCADA (*Supervisory Control and Data Acquisition*), kde je potrebné overovať informácie prichádzajúce z rôznych vzdialených snímačov (aby sa predišlo podvrhu) a je treba mať mechanizmy na podpísanie povelu, ktorý sa má vykonať, napr. na vzdialenom akčnom člene (schémy na overenie vierohodnosti zdroja).

Tab. 1. Porovnanie dĺžok kľúčov kryptografických algoritmov pre dosiahnutie rovnakej úrovne zabezpečenia

Ekvivalentné zabezpečenie kryptografických algoritmov (bit)		
dĺžka kľúča symetrických algoritmov	dĺžka kľúča asymetrických algoritmov	
80 (2DES)	RSA 1 024	ECC 160
112 (3DES)	RSA 2 048	ECC 224
128 (AES-128)	RSA 3 072	ECC 256
192 (AES-192)	RSA 7 680	ECC 384
256 (AES-256)	RSA 15 360	ECC 521

Možno skonštatovať, že v dnešnej dobe dochádza v priemysle k integrácii prvkov zabezpečenia ICT (*cybersecurity*) s prvkami bezpečnosti (*safety*) [1]. Priemyselné domény podniku sú prepojené s kancelárskymi doménami ako aj vzdialenými pracoviskami výrobného podniku. V rámci priemyselnej domény (často ide o doménu reálneho času) sa môžu vyskytovať štandardné ako aj bezpečnostne relevantné zariadenia, ktoré komunikujú napr. prostredníctvom priemyselného Ethernetu alebo bezdrôtovo. Funkčná bezpečnosť je riešená pomocou prídavných bezpečnostných profilov, ktoré sú implementované do softvéru bezpečnostne relevantných zariadení (v priemysle väčšinou s úrovňou funkčnej bezpečnosti SIL 3). V kancelárskej doméne sa bezpečnostná politika informačných systémov podniku a sietí realizuje osvedčenými princípmi zabezpečenia používanými v ICT (zabezpečenie dôvernosti, integrity, autentizácie a dostupnosti), podobne ako to je pri komunikácii prostredníctvom verejnej siete so vzdialeným priemyselným pracoviskom.

Zhrnuté základné dôvody nástupu kryptografie v priemysle možno vyjadriť nasledovne:

- používanie cenovo dostupnejších otvorených prenosových médií so zameraním na bezdrôtové komunikácie,
- nárast úloh so vzdialeným monitorovaním a riadením procesov s podporou prenosových prostriedkov a hardvéru COTS, napr. sietí VPN (*Virtual Private Network*) a zabezpečených komunikačných protokolov IPsec (*Internet Protocol Security*), SSL (*Secure Socket Layer*) a TLS (*Transport Layer Secure*),
- prepojenie priemyselných a kancelárskych domén v oblasti riadenia výrobného podniku,
- vývoj jednotných štandardov riadenia rôznych procesov, napr. železničnej dopravy, s plánovaním prenosov prostredníctvom mobilnej komunikácie.

Ak ide len o prostriedky kryptografie pre potreby bezpečnostne relevantnej komunikácie, pri navrhovaní vhodných kryptografických mechanizmov je trendom nevyvíjať špecifické kryptografické ochrany, ale používať verejne známe dostupné kryptografické štandardy z oblasti COTS, ktoré sú implemento-

vané do prídavných bezpečnostných profilov, u ktorých ale musí byť vykonaná podrobná bezpečnostná analýza na báze kvalitatívnych a kvantitatívnych metód [2].

Je známe, že aplikované kryptografické princípy chránia pred väčšinou kybernetických hrozieb, ale ich použitie v priemyselnom bezpečnostne relevantnom komunikačnom systéme treba zvažovať od prípadu k prípadu, na základe dôkladnej analýzy hrozieb pre daný systém. Základnou koncepciou otvoreného priemyselného bezpečnostne relevantného komunikačného systému (z pohľadu použitia kryptografických mechanizmov) je navrhnúť ho tak, aby mal schopnosť odolávať s určitou pravdepodobnosťou útokom, nezákonným alebo škodlivým udalostiam, ktoré zhoršujú dostupnosť, autenticitu, integritu a dôvernosť uložených či prenesených údajov a súvisiacich služieb, ktoré tento systém ponúka.

2. Presadzované prístupy pri použití kryptografie v bezpečnostne relevantnom priemyselnom komunikačnom systéme

Základné dôvody použitia kryptografie v oblasti otvorených sietí v priemysle sú založené na skutočnosti, že siete zahŕňajú základné užitočné hodnoty priemyselného systému v podobe hardvéru, softvéru, dát a prenosového média, kde je ťažko kontrolovateľný prístup neoprávnených subjektov či objektov, čím predstavujú veľké riziko ohrozenia zabezpečenia informácií.

Medzi základné služby zabezpečované kryptografickými systémami patria:

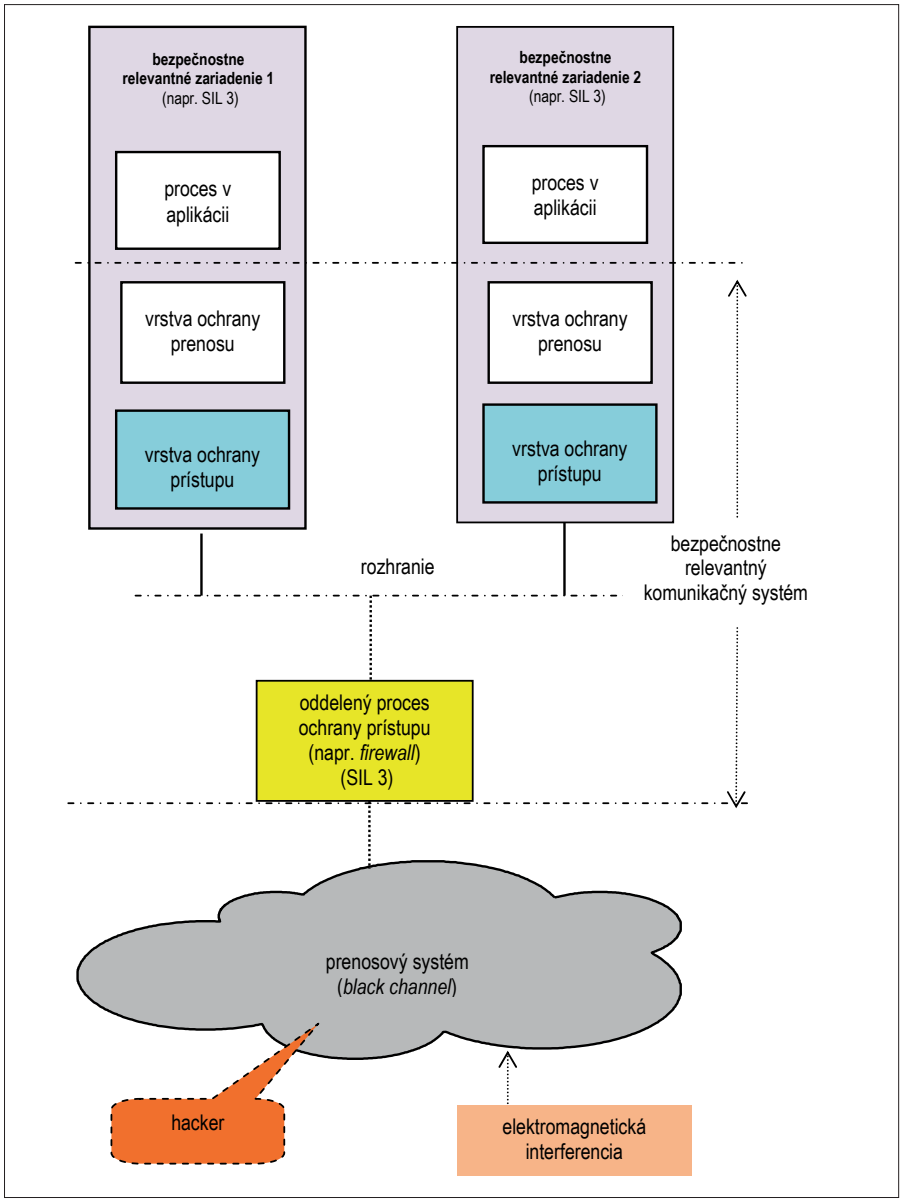
– Dôvernosť (*confidentiality*). Je zaručená službou, ktorá chráni dáta pred všetkými okrem tých, ktorí majú pre ňu autorizáciu. K zaisteniu dôvernosti sa volia rôzne spôsoby od fyzických ochrán až k matematickým algoritmom, ktoré pretvárajú zrozumiteľný informačný obsah na obsah nepovolanému užívateľovi nezrozumiteľný.
– Integrita dát (*data integrity*). Je zaručená službou, ktorá znemožňuje neautorizovanú modifikáciu dát. Na zaistenie integrity dát musí existovať možnosť detegovať manipuláciu s dátami (napr. vkladanie dát, odstraňovanie a zamieňanie dát), ktorá je realizovaná neautorizovanými subjektmi.
– Autentizácia (*authentication*). Je zaručená službou, ktorá ma vzťah k identifikácii. Autentizácii podliehajú nielen účastníci komunikácie (subjekty komunikácie), ale aj samotná informácia (objekt komunikácie), ktorá by mala byť autorizovaná vzhľadom k svojmu pôvodu, dobe vzniku, dátovému obsahu, okamžiku odoslania atď. Z tohto dôvodu sa autentizácia v kryptografii delí na: autentizáciu entity (subjektu) a autentizáciu pôvodu dát (objektu). Autentizácia dát v sebe zahŕňa kontrolu integrity dát a vierohodnosť zdroja.
– Neodmietnuteľnosť (*non-repudation*). Je zaručená službou, ktorá bráni entite poprieť predchádzajúce záväzky alebo aktivity. Ak dôjde ku sporu, že entita poprie nejakú svoju aktivitu, situácia sa rieši na základe kryptografických procedúr, ktoré v sebe zahŕňajú nezávislú tretiu stranu.

Vymenované bezpečnostné funkcie je možno prostriedkami kryptografie splniť pomocou nasledujúcich bezpečnostných mechanizmov: šifrovacie mechanizmy, integritné techniky (hašovacie funkcie, autentizačný kód správy), identifikačné techniky a schémy digitálneho podpisu.

V bezpečnostne relevantnom priemyselnom komunikačnom systéme možno prenášané a uchovávané dáta chrániť pomocou kryptografických mechanizmov v prípade, ak nie je možné v používanej aplikácii pri komunikácii vylúčiť úmyselný útok.

Vo vzťahu k požadovanej úrovni integrity bezpečnosti aplikácie a povahe bezpečnostne relevantného procesu je potrebné podľa štandardov platných pre bezpečnostne relevantnú komunikáciu ([3], [4]) vykonať podrobnú bezpečnostnú analýzu zvolenej kryptografickej ochrany a preukázať primeranosť:

– technickej voľby kryptografických techník – týka sa voľby šifrovacieho algoritmu (napr. symetrický alebo asymetrický), kľúčových charakteristík (napr. fixné alebo vytvárané počas spojenia – relačné kľúče), zvolenej dĺžky kľúča, frekvencie obnovy kľúča a fyzického uloženia kľúčov,
– technickej voľby kryptografických architektúr – týka sa kontroly správneho fungovania zvolených kryptografických mechanizmov vo fáze vývoja, testovania a prevádzky a kryptografických procesov, keď



Obr. 1. Presadzované prístupy pri implementovaní kryptografie v priemyselnom bezpečnostne relevantnom komunikačnom systéme

sú implementované mimo bezpečnostne relevantné zariadenia,
– činnosti správy kryptografických kľúčov – táto časť bezpečnostnej analýzy sa týka vytvorenia, uloženia, distribúcie a zrušenia dôverných kľúčov, správy zariadení a procesu revízie primeranosti kryptografických techník vo vzťahu k rizikám od zlomyseľných útokov.

Prístupy pri aplikovaní kryptografie pri komunikácii medzi bezpečnostne relevantnými zariadeniami v priemyselnom komunikačnom systéme možno rozdeliť na dve riešenia (*obr. 1*):
– kryptografická technika je súčasťou bezpečnostných ochrán konkrétneho bezpečnostne relevantného zariadenia (vrstva ochrana prístupu – na *obr. 1* znázornená modrou farbou),
– kryptografická technika je súčasťou bezpečnostných ochrán niekoľkých bezpečnostne relevantných zariadení, ktoré komunikujú v rámci internej priemyselnej siete, a je implementovaná do oddelenej vrstvy ochrany prístupu (na *obr. 1* znázornenej žltou farbou).

Druhý prístup je viac presadzovaný. Odporúča sa použiť napr. firewall, ktorý však musí byť zahrnutý do bezpečnostnej politiky bezpečnostne relevantnej aplikácie.

Firewall na realizáciu bezpečnostnej politiky využíva aj kryptografické mechanizmy. Okrem ochrany prístupu môže zabezpečovať aj iné bezpečnostné služby (napr. dôvernosť). Jeho základnou úlohou je blokovať neautorizovanú sieťovú prevádzku medzi internou (chránenou) a externou sieťou napr. tak, že nedovolí vytvoriť priame spojenie medzi uzlom v sieti Internet a uzlom v priemyselnej sieti. Firewall môže byť nakonfigurovaný tak, aby povolil komunikáciu len pomocou určitých protokolov, napr. protokol siete Profinet.

Okrem vrstvy ochrany prístupu je vždy súčasťou bezpečnostne relevantného zariadení aj vrstva ochrany prenosu, v ktorej sú umiestnené bezpečnostné ochrany, ktoré eliminujú účinky elektromagnetického rušenia v prenosovom systéme, ktorý je vzhľadom na neznáme, resp. veľmi pravdepodobnostné správanie označovaný aj ako *black channel*.

3. Špecifiká pri výbere kryptografických mechanizmov

Treba si uvedomiť, že priemyselný komunikačný systém pozostáva v mnohých prípadoch z množstva uzlov, u ktorých je nutné zabezpečiť komunikáciu v reálnom čase. Aj menšie narušenie takéhoto systému môže byť z pohľadu reálneho času kritické. Bezpečnostne relevantné aplikácie však vyžadujú voľbu parametrov kryptografických mechanizmov v čo najvyššej bezpečnostnej úrovni, čo má značný vplyv na časovú náročnosť vykonávania operácií.

V porovnaní s technikou COTS pri použití kryptografie v priemyselnom bezpečnostne relevantnom komunikačnom systéme treba vziať do úvahy tieto špecifiká:
– obmedzený výpočtový výkon zariadení – u niektorých (napr. u zariadení s osembitovou architektúrou) môže sťažovať použitie princípov modernej, hlavne asymetrickej kryptografie, ktorá je založená na zložitých matematických operáciách z teórie čísel a modulárnej aritmetiky,
– požiadavka odozvy pri prenose dát cez sieť v reálnom čase – kryptografická operácia musí byť vykonaná v reálnom čase, aby bol dodržaný požadovaný čas odozvy,
– efektívna správa kryptografických kľúčov.

Kľúč je najväčšou slabinou kryptografických protokolov. Okrem implementácie kryptografických algoritmov je potrebné v reálnom čase riešiť aj správu kryptografických kľúčov. Kryptografické aplikácie sú bez správy kľúčov neúplné. Kľúč uložený v zariadení je veľmi zraniteľný. Treba ho často obmieňať, najlepšie je vytvárať pre každú novú komunikáciu vždy nový.

Najviac odporúčané kryptografické techniky v bezpečnostne relevantnom priemyselnom komunikačnom systéme sú šifrovacie techniky a techniky digitálneho podpisu. Vzhľadom na obmedzený priestor si uveďme aspoň stručný prehľad algoritmov a režimov činnosti odporúčaných pre sledovanú oblasť bezpečnostne relevantných priemyselných softvérových aplikácií.

3.1 Mechanizmy šifrovania

Mechanizmy šifrovania sa vo výrobných podnikoch používajú napr. na utajenie výrobné receptov, procedúr a celkového *know-how* podniku. Pri použití šifrovania na prevádzkovej úrovni riadenia v bezpečnostne relevantných riadiacich aplikáciách sa z dôvodu urýchlenia výpočtov využívajú špeciálne moduly – bezpečnostné integrované obvody s rýchlym procesorom [5], v ktorom sa vykonáva šifrovanie a správa kľúčov oddelene, čo odľahčuje procesor zariadenia. V prípade neoprávnenej manipulácie s kľúčmi či pri detegovaní neoprávneného vniknutia do modulu sú kľúče automaticky zničené.

Pre bezpečnostne relevantnú komunikáciu sú odporúčané overené štandardy blokových šifier; použitie prúdových šifier je vzhľadom na ich omnoho slabšie zabezpečenie neodporúčané. Z množiny blokových šifier sa možno viazať na kryptografické prostriedky využívajúce jeden kľúč. Ide o symetrické šifrovacie systémy, ktoré majú pre priemyselné aplikácie niekoľko výhod: umožňujú šifrovať dáta vysokou rýchlosťou, používajú relatívne malé dĺžky kľúčov, sú založené na jednoduchších matematických princípoch (substitúcie, permutácie) a ponúkajú okrem bezpečnostnej služby dôvernosť aj autorizáciu zdroja dát (komunikujúce entity zdieľajú tajný kľúč, na ktorom sa dohodli alebo ho zabezpečeným spôsobom získali). Okrem toho možno ich zabezpečenie zvýšiť, ak sú kombinované s vhodným režimom činnosti. Pre bezpečnostne relevantné aplikácie sa neodporúča použiť režim elektronickej kódovacej knihy ECB (*Electronic Code Book*), ale z dôvodu zvýšenia zabezpečenia je presadzovaný režim zreťazenia blokov šifrovaného textu CBC (*Cipher Block Chaining*), ktorý používa pred šifrovaním a po dešifrovaní spätnoväzobný mechanizmus, čím eliminuje niektoré typy útokov, napr. opakovanie bloku (*block replay*). Dnes sa ešte za výpočtovo bezpečný algoritmus symetrických šifier považujú niektoré modifikácie algoritmu DES (*Data Encryption Standard*), hlavne 3-DES s tromi kľúčmi, u ktorého je, aj vzhľadom na existujúce krypto-analytické útoky, efektívna dĺžka kľúča 112 bitov. Viac je však presadzovaný kryptografický štandard AES (*Advanced Encryption Standard*) [6] vo verziách AES-128, AES-192 a AES-256, ktorý sa v súčasnej dobe aplikuje vo všetkých sférach komunikácie a ukladania údajov na rôznych programovacích jazykoch a platformách a považuje sa za výpočtovo bezpečnú šifru.

Pokiaľ to výpočtový výkon zariadenia dovoľuje, pre šifrovanie menších objemov dát je možné v bezpečnostne relevantných aplikáciách v priemysle použiť aj kryptografické prostriedky využívajúce pár kľúčov. Ide o asymetrické šifrovacie systémy, u ktorých v porovnaní so symetrickými šifrovacími systémami odpadá problém s tvorbou zabezpečeného kanála pri prenose kľúča a podľa spôsobu prevádzky môže byť kľúčový pár používaný bez zmeny dlhšiu dobu. Za výpočtovo bezpečný a najviac používaný sa dnes považuje algoritmus RSA (*Rivest Shamir Adleman*). Podľa predbežných odhadov sa bezpečná dĺžka parametrov RSA (modul N ako súčin dvoch prvočísel) dostáva nad hranicu modulu $N = 2\,000$ (čomu odpovedá 300- až 600- ciferné číslo). Z toho vyplýva odporúčanie nepoužívať už RSA s dĺžkou menšou ako 2 048 bitov a pre dlhodobé zabezpečenie je pripravovaná implementácia o dĺžke 8 192 bitov. Názory odborníkov na zväčšovanie veľkosti kryptografického modulu N sa rôznia, niektorí kryptológovia v oblasti asymetrickej kryptografie odporúčajú prejsť v čo najkratšom čase na kryptografiu na báze eliptických kriviek ECC (*Elliptic Curve Cryptography*), ktorá je novým perspektívnym smerom v modernej asymetrickej kryptografii.

3.2 Mechanizmy digitálneho podpisu

Mechanizmy digitálneho podpisu majú svoje opodstatnenie v bezpečnostne relevantných aplikáciách všade tam, kde je potrebné overiť vierohodnosť informácie prichádzajúcej zo vzdialených uzlov alebo odchádzajúcej do nich. Ďalšie oblasti použitia sú napr. overenie pravosti aktualizácie softvéru ešte pred jej vykonaním, kontrola zmien v konfigurácii hardvéru (napr. zmena kalibračných údajov snímačov) a iné.

V súčasnosti sú najznámejšie tieto schémy digitálnych podpisov s použitím asymetrickej kryptografie:
- RSA, u ktorej je bezpečnosť založená na obtiažnosti faktorizácie veľkých čísel (veľkosť modulu *N*),
- DSA (*Digital Signature Algorithm*; s modifikovaným algoritmom El Gamal), u ktorej je bezpečnosť založená na zložitosti výpočtu diskrétnych logaritmov,
- ECDSA (*Elliptic Curve Digital Signature Algorithm*; modifikácia DSA s algoritmom eliptických kriviek), u ktorej je bezpečnosť tiež založená na zložitosti výpočtu diskrétneho logaritmu označovaného ako ECDLP (*Elliptic Curve Discrete Logarithm Problem*) [7].

Všetky schémy digitálneho podpisu sú naviac založené na bezpečnosti použitej hašovacej funkcie.

Úroveň zabezpečenia kryptografických algoritmov možno vyjadriť pomocou ekvivalentnej bezpečnosti, ktorá vyjadruje, ako sa zmenšuje veľkosť kľúča (v bitoch) pri zohľadnení vplyvu v súčasnosti známych kryptoanalytických útokov na algoritmus.

V *tab. 1* sú porovnané veľkosti kľúčov pre dosiahnutie rovnakej úrovne zabezpečenia pre symetrické systémy (2-DES, 3-DES, AES) a asymetrické systémy (RSA a ECC). Parametre v dole tmavomodrom poli sú odborníkmi na kryptografiu pokladané na najbližšie desaťročie za výpočtovo bezpečné.

4. Záver

Ak by sme si na záver položili otázku, či spomenuté kryptografické metódy vhodne zvolených parametrov dokážu uchrániť bezpečnostne relevantný priemyselný komunikačný systém od všetkých kybernetických hrozieb, odpoveď by isto nebola jednoznačná. Všetci vieme, že absolútne zabezpečenie akéhokoľvek systému neexistuje. Riziká, ktoré v rámci konkrétnej softvérovej aplikácie vznikajú, môžu byť eliminované len na určitú tolerovateľnú úroveň, a to platí aj pre kryptografické mechanizmy. Možno ešte konštatovať, že metódy kryptografie a kryptoanalýzy sa na rozdiel od iných vedných disciplín menia omnoho dynamickejšie, preto je potrebné sledovať vývoj v tejto oblasti a výber bezpečnostných mechanizmov viazať na konkrétnu aplikáciu po podrobne vykonanej analýze rizík.

Príspevok vznikol s podporou edukačnej grantovej agentúry Slovenskej republiky (KEGA) číslo: 024ŽU-4/2012: Modernizácia technológií a metód vzdelávania so zameraním na oblasť kryptografie pre bezpečnostne kritické aplikácie.

Literatúra:

[1] ÅKERBERG, J. et al.: *Efficient integration of secure and safety critical industrial wireless sensor networks*. In: *EURASIP Journal on Wireless Communications and Networking*, 2011 [on-line]. [cit. 23. 12. 2013]. URL: <http://jwcn.eurasipjournals.com/content/2011/1/100>.

[2] FRANEKOVÁ, M. a kol.: *Komunikačná bezpečnosť priemyselných sietí*. Monografia, EDIS ŽU Žilina, 2007. ISBN 978-80-8070-715-6.

[3] STN EN 50159: *Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Komunikácia súvisiaca s bezpečnosťou v prenosových systémoch*. SÚTN, Bratislava, 2010.

[4] IEC 61784-3: *Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CPF3*. 2010.

[5] TREMLET, CH.: *Priemyselné systémy potrebujú dodatočnú ochranu pomocou bezpečnostných integrovaných obvodov*. ATP Journal, 1/2013.

[6] FIPS PUB 197: *Advanced Encryption Standard (AES)*. 2001.

[7] VAUDENAY, S.: *A Classical Introduction to Cryptography. Applications for Communications Security*. Springer, 2006. ISBN 0-387--25464-1.

prof. Ing. Mária Franeková, PhD., katedra riadiacich a informačných systémov, Elektrotechnická fakulta Žilinskej univerzity v Žiline (maria.franekova@fel.uniza.sk)

Výzkumné projekty podpořené Nadací ČVUT Media Lab

Začátkem prosince 2013 byl uspořádán již šestý ročník workshopu nadace ČVUT Media Lab. Bylo velmi povzbudivé seznámit se s výsledky projektů, které vznikly s podporou této nadace. Nadpoloviční většinu tvořily projekty vzniklé z iniciativy eClub ČVUT, již nadace od počátku podporuje. Iniciativa eClub ČVUT pod vedením Jana Šedivého z katedry kybernetiky ČVUT v Praze se zaměřuje na propojování studentských nápadů se světem podnikání. Skutečnost, že v letošním ročníku pochází větší počet projektů z líhně této iniciativy, jen dokládá, že eClub ČVUT si našel cestu nejen ke studentům, ale i k podnikatelům.

Stejně jako v předchozích letech, i v roce 2013 vzrostl počet projektů podpořených nadací ČVUT Media Lab. Rok od roku také narůstá množství nápadů, které již byly uvedeny do praktického života. Jako letošní příklad může sloužit trojice projektů podpořená iniciativou eClub ČVUT. Projekt pod názvem APEMAN boards se úspěšně zabývá výrobou speciálního typu skateboardů, tzv. longboardů, z materiálu na bázi uhlíkových vláken. Studenti zapojení do projektu BlindShell zase vyprojektovali rozhraní dotykového telefonu pro nevidomé. Třetím realizovaným studentským nápadem je služba Mixturam, která umožňuje zákazníkům určit si složení potravinových doplňků podle svých potřeb. Tento studentský projekt sklízí úspěchy na domácím trhu a jeho tvůrci přemýšlejí o expanzi do zahraničí.

Nejeden projekt je založen na využití informační techniky v oblastech, kde to ještě před několika lety nebylo myslitelné. Mezi aplikacemi pro chytré telefony a tablety se objevují nejen hry, ale i kreslení či výuka psaní. Jednoduchá aplikace LearnToWrite velmi přístupnou formou otevírá svět IT malým školákům i předškolákům.

Tradičními účastníky workshopu Nadace ČVUT Media Lab jsou tvůrci studentské formule CTU CarTech. Tentokrát se rozhodli navrhnout a vyrobit měnič k řízení synchronního motoru s permanentními magnety. Sériově vyrobený kus totiž selhal v nejméně vhodném okamžiku a tato závada přinutila studentské závodníky předčasně ukončit sezonu.

Dalším zajímavým projektem, jenž byl v rámci workshopu prezentován již podruhé, je 6ixtenRobot (Fakulta strojní ČVUT v Praze), tentokrát jeho verze 2.0. Cílem projektu je vytvořit multifunkční robotický podvozek schopný pohybu v těžkém terénu a zároveň vybavený mechanismem pro „chůzi“. Podvozek (*obr. 1*) by mohl být použit u invalidních vozíků ke zlepšení jejich schopnosti pohybovat se např. v bariérových částech města.

Další informace o činnosti nadace a možnostech její podpory ze strany průmyslových podniků lze nalézt na webových stránkách www.cvutmedialab.cz a www.eclub.cvutmedialab.cz.

(ev)