RFID a její nebezpečí

O přednostech, významu a přínosech RFID již v současnosti nikdo nepochybuje, o čemž svědčí rozšiřující se spektrum jejího použití v nejrůznějších odvětvích průmyslu. V té souvislosti je nutné zkoumat i negativa provázející používání této rádiové techniky. O potenciálních nebezpečích je třeba nejen vědět, ale také jejich dopad minimalizovat.

Jakkoliv jsou přednosti identifikátorů a související komunikace na bázi RFID (*Radio Frequency Identification*) zřejmé, však se jich na světě používá již více než šest miliard, největším problémem jejich dalšího širšího používání je otázka bezpečnosti. Především obava z narušení automaticky snímaných, přenášených a ukládaných dat, a to nejen osobních údajů, ale také dat v logistice či výrobě, které by mělo sice různé, ale vždy nepříznivé důsledky.

S použitím RFID lze prostřednictvím rádiových vln automaticky identifikovat objekty, přesněji značky umístěné na objektu nebo živém organismu (člověku, zvířeti, rostlině). Nejčastější metodou vlastní identifikace je uložení sériového čísla produktu, popř. dalších informací, v mikročipu. Mikročip, k němu připojená anténa a jejich nosná podložka dohromady tvoří tzv. transpondér, štítek či značku (*tag*) RFID. Díky anténě může čip vyslat identifikační údaje snímači (čtečce), který je převede do vhodné formy pro další počítačové zpracování.

RFID díky své radiokomunikační podstatě a paměťovým možnostem nabízí mnohem více než pouhou identifikaci, totiž sledování pohybu a změn stavu „sledovaného“ objektu. Chytré „věci“ získávají díky výpočetním schopnostem určitou nezávislost, a tím možnost reagovat na podněty přicházející z okolí. Značky RFID přeměňují běžné objekty denní potřeby na síťové uzly, které posílají svá identifikační a stavová data do databází a ukládají si nové informace podle potřeb.

Z uvedených vlastností RFID plynou také první otazníky nad její bezpečností. V první řadě mnoha spotřebitelům vadí v principu možnost, že by prostřednictvím značek použitých na různých předmětech mohli být sledováni doslova na každém kroku, popř. že by tyto značky dokázaly sdělit i něco z jejich soukromí (např. preference zboží, stravovací návyky). Data nasbíraná prostřednictvím RFID lze přenášet, ukládat a dále zpracovávat, což vyvolává další obavu. Co se s údaji soukromého charakteru, tedy s údaji svázanými s danou osobou, může dít dál? Kdo s nimi může pracovat, k čemu je může využívat? Nelze je ukrást, modifikovat, či dokonce zneužít? I když toto nebezpečí nesouvisí výhradně s RFID, ale spíše se zacházením s citlivými údaji, je třeba se i jím pečlivě zabývat, jinak by přijatelnost RFID pro spotřebitele a uživatele nebyla velká.

Ochrana soukromí

Obava z narušení soukromí a strach z potenciálního zneužití osobních údajů jsou v současném světě oprávněně velice silné. Požadovaná úroveň ochrany soukromí souvisí nejen s technickými možnostmi, ale také s otázkami regulace (přístup k informacím), trhem a socio-ekonomickým prostředím.

Specifickým požadavkům na RFID s ohledem na ochranu soukromí a dat se po mnoho let věnuje také Evropská komise, která v květnu letošního roku vydala doporučení [1] týkající se mj. informovanosti uživatelů, transparentnosti používání a možnosti bezplatné deaktivace, popř. odstranění štítků RFID při jejich užití v maloobchodě (pokud si kupující nepřeje jinak). Doporučení vyplývá z dlouhého procesu konzultace s veřejností (IP/06/289) na téma RFID, kterou komise zahájila v roce 2006. Průzkum ukázal, že téměř polovina respondentů se domnívala, že metody používané k ochraně soukromí by měly být při použití RFID povinné. Více než 60 % respondentů také bylo přesvědčeno o tom, že značky připevněné na spotřební zboží by měly být po nákupu automaticky deaktivovány.

V březnu 2007 již bylo zřejmé, že se oblast využívání RFID neobejde bez další akce směrované právě na ochranu soukromí a dat, k čemuž Evropská komise vydala své prohlášení (IP/07/332). K tomu ještě přispělo vyhlášení základních práv EU (*Charter of Fundamental Rights of the European Union*) na konci roku 2007. Cílem současného doporučení, které však mělo být vydáno již vloni, je, aby všichni zainteresovaní v procesu návrhu, výroby a zejména použití RFID respektovali základní práva jednotlivce na ochranu osobních dat a soukromí.

Provozovatelé RFID mají poskytovat jednoznačné informace o sobě (kdo), popis využití RFID (co a proč), zda značka sbírá nebo zpracovává údaje spojené s identifikovatelnou osobou a jakými opatřeními je zamezeno případnému ohrožení soukromí uživatele (jak). Všechny tyto informace mají být široce dostupné (např. web, letáky) a srozumitelné pro spotřebitele. Dále mají provozovatelé viditelně označit přítomnost snímačů RFID (např. u vchodu do obchodu) a odkaz na získání dalších informací.

Doporučení jasně ukazuje, že zákazníci musí vědět, zda jimi nakupované zboží obsahuje čipy RFID. Kromě toho by měly být tyto čipy automaticky deaktivovány ihned po nákupu zboží, a to zdarma, pokud sám zákazník jasně nepožádá, aby byl čip ponechán funkční. S touto součástí doporučení ale mají mnozí problém, protože automatickým vypnutím čipů lze přijít o mnoho funkcí spjatých se značkami RFID po vlastním nákupu, mj. o možnost úsporné recyklace zakoupeného produktu či správy záručních a servisních zásahů. Současně to znamená zátěž pro maloobchod, protože je třeba počítat s tím, že zákazník může uplatnit svůj názor na deaktivaci u každé jednotlivé značky (transpondéru) RFID.

Doporučení [1] dále uvádí, že při zpracování údajů spjatých s identifikovatelnými osobami musí provozovatelé nejprve posoudit dopad takového procesu na soukromí spotřebitelů (*Privacy Impact Assessment* – PIA) a posouzení předložit nejméně šest týdnů před zavedením daného systému místnímu úřadu pro ochranu dat. Obsah kritérií pro PIA není v samotném doporučení Evropské komise stanoven, ale organizace GS1 EPCglobal již na doporučeném seznamu pracuje.

Doporučení [1] není mandatorní, jak ostatně jeho titul napovídá, ale nezůstane pouze papírovým dokumentem: do dvou let musí jednotlivé členské státy sdělit, jakým způsobem je hodlají vnést do praxe. Do tří let pak Evropská komise bude informovat o realizaci doporučení a o výsledcích analýzy jeho dopadu na podniky a veřejné úřady a samozřejmě na občany.

Komisařka pro informační společnost a média Viviane Redingová se v souvislosti s RFID zmínila také o problematice Internetu věcí (*Internet of Things*), k níž se den před vydáním doporučení konal samostatný workshop v rámci významné mezinárodní konference *The Future of the Internet: Europe moving forward*, zorganizované akademickým a výzkumným sdružením Cesnet letos v Praze. Internet věcí má využívat senzory a RFID pro propojení neživých objektů a doplnit tak komunikační prostor, v němž zatím působí na internetu především živí uživatelé. Komisařka uvedla, že podle odhadu expertů by zavedení RFID mělo do roku 2016 vytvořit trh o velikosti asi 30 miliard eur. Jen v minulém roce se prodalo 2,2 miliardy značek RFID, z toho třetina v Evropě.

Technická nebezpečí

Vedle zranitelnosti osobních dat existují při používání RFID ještě další nebezpečí. Některá plynou ze samotné metody: u RFID jde o zranitelnost rádiové komunikace a transpondérů. To jsou však jen nejnižší vrstvy síťové komunikace (fyzické a spojové), k nimž se ještě přidávají další hrozby na vyšších vrstvách, tedy od síťové až po aplikační. Za cel-

kem oprávněného předpokladu většího využití síťového protokolu IP i pro komunikaci mezi zařízeními pro RFID (zejména v rámci Internetu věcí) je pak třeba počítat v podstatě se všemi potenciálními útoky známými ze sítí používajících IP.

Na místě jsou obavy především z útoků typu neautorizovaného připojení (*spoofing*), odposlechu existujícího rádiového spojení mezi autorizovaným snímačem a značkou RFID a útoků vedoucích k odmítnutí služby (DoS).

Útokům prvního typu lze zabránit zakrytím značky ochranným materiálem, který se odkryje pouze pro autorizované čtení. Dalším stupněm ochrany je identifikační číslo (známé PIN), které je třeba zadat na snímači před otevřením vlastní rádiové komunikace v rámci autentizace. Při přenosu dat je možné použít šifrování na rádiovém kanálu.

Značky jako elektronické prvky mohou být teoreticky zničeny působením velmi silného elektromagnetického pole, což ale vyžaduje výskyt útočníka v blízkém okolí cíle, a (mechanická) ochrana je tedy poměrně snadná. Stejné nebezpečí hrozí i ve výrobních procesech, kde je nutné zajistit, aby se čipy RFID nedostávaly do míst s velkou intenzitou (elektro)magnetického pole.

Data, s nimiž se v rámci systémů RFID pracuje, jsou jednak získávána a přenášena do databáze, kde musí nastoupit potřebná úroveň ochrany uložených dat, a jednak jsou uložena v čipu RFID. Maximálním stupněm ochrany jsou v tomto případě čipy určené pouze ke čtení, které jakoukoliv modifikaci dat nedovolují.

„RFID vytváří základ pro lepší a bezpečnější zdravotní péči, významně zlepšuje řízení dodavatelských řetězců, zlevňuje monitorování životního prostředí a přispívá tak k udržitelnému rozvoji společnosti a k její čistší budoucnosti. K tomu, abychom mohli těžit z výhod RFID a přitom ji dali občanům, spotřebitelům i podnikatelům do rukou jako transparentní nástroj, který bude plně pod jejich kontrolou, je potřebný proaktivní celoevropský přístup."

Viviane Redingová,
komisařka pro informační společnost a média

V mnoha případech ale úlohy vyžadují možnost přepisovat uložená data. Krátká vzdálenost potřebná pro komunikaci se značkou je pro ochranu před modifikací dat v čipu předností.

Jedním z komunikačních protokolů používaných pro RFID je NFC (*Near Field Communication*), protokol pro obousměrnou rádiovou komunikaci na velmi krátkou vzdálenost v pásmu 13,56 MHz. Na základě specifikací průmyslového sdružení NFC Forum (využívajících normy ISO 18092, ECMA a ETSI pro chytré karty) lze realizovat bezpečné bezdotykové transakce (pouhým přiblížením, i přes překážku z nekovového materiálu) mezi zařízeními s podporou NFC (typicky bezkontaktní karty, čtečky nebo značky RFID).

Bezkontaktní karty nemusí být ani kartami; jde u nich především o čip a rádiovou složku, bez přísné vazby na plastovou kartu. Čipy lze uplatnit v mnoha jiných malých zařízeních, jako jsou mobilní telefony nebo přívěsky ke klíčům. Jejich použití je mnohostranné zejména při platbách i při identifikaci (např. placení mýtného, identifikační karty či pasy s biometrickými údaji). O to důležitější je právě zde ochrana uložených a přenášených dat.

Bezpečnost bezkontaktních karet je i přes závislost na bezdrátové komunikaci velká. Lze provádět vzájemnou autentizaci mezi snímačem a uživatelem, takže se k uloženým datům na čipu nedostane nikdo neoprávněný. Dále lze přenášená data šifrovat, aby ani jejich nepravděpodobný odposlech nepřinesl útočníkovi užitek. Karta je navíc aktivní jen po velmi omezenou dobu (ověření identity a další jednoduché transakce do 100 ms), kdy se přiblíží ke snímači, a fyzický prostor pro odposlech je také minimální.

Komunikaci aktivních značek RFID se poměrně nedávno začala věnovat také organizace IEEE, v níž je v rámci výboru pro malé bezdrátové sítě (*Wireless Personal Area Network* – WPAN) založena nová skupina 802.15.4f. Úkolem skupiny je definovat novou fyzickou vrstvu pro aktivní značky RFID splňující zásadní požadavky na velmi malou spotřebu energie a malý vysílací výkon, komunikaci jednosměrnou i obousměrnou, velkou hustotu (tisíce) značek vyžadující síťové mechanismy zamezující zahlcení v síti. Nová norma rovněž musí zajistit autentizaci a zamezit rušení s jinými rádiovými technikami. Návrh normy by měl být dokončen již příští rok a měl by přispět k otevřenosti systémů RFID, protože konkrétní realizace jsou zatím stále velmi často založeny na firemních řešeních specifických požadavků.

V diskusi o technických nebezpečích RFID nelze opomenout ještě jednu zvláštní kategorii nebezpečí související s vyzařovacím výkonem, použitým kmitočtem a s nimi souvisejícím rušením s jinými rádiovými technikami. To je třeba zkoumat a vyloučit zejména v nemocnicích, kdy potenciální rušení s jinou elektronikou, na jejíž správné činnosti může záviset i lidský život, může mít fatální následky. Jinak vyzařování v systémech RFID je na nepoměrně nižší úrovni než u mobilních telefonů a komunikace je také výrazně méně častá, takže zdraví uživatele-spotřebitele principiálně není v tomto směru ohroženo ani v případě značek RFID nacházejících se v bezprostřední blízkosti těla (např. na oblečení).

Rozum do hrsti

Nepřátelé RFID – puritáni v otázkách osobní bezpečnosti – se snaží představit RFID jako špatnou techniku. Techniku samu o sobě ale nikdy nelze označit za dobrou nebo špatnou, protože každou je možné s trochou podlosti zneužít. Pokud se však budou dodržovat dobře nastavená pravidla ochrany soukromí a bezpečnosti rádiové komunikace, RFID se rozhodně ještě více osvědčí a rozšíří jako užitečná technologie v různých oblastech a skutečně otevře cestu ke komunikaci objektů nejen v uzavřených systémech, ale i po internetu budoucnosti.

Literatura:

[1] Commission of the European Communities: *Commission recommendation of 12. 5. 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* [on-line]. Dostupné z <http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf>, 2009 (cit. 30. 6. 2009).

[2] Commission of the European Communities: *Radio Frequency IDentification and the Internet of Things* [on-line]. Dostupné z <http://ec.europa.eu/information_society/policy/rfid/index_en.htm>, 2009 (cit. 30. 6. 2009).

[3] European Commission: *From RFID towards the Internet of Things* <http://www.iot-visitthefuture.eu/>, 2008 (cit. 30. 6. 2009).

[4] –: *BRIDGE Project (Building Radio Frequency Identification solutions for the global Environment)* [on-line]. Dostupné z <http://www.bridge-project.eu/>, BRIDGE 2009 (cit. 30. 6. 2009).

[5] –: *SMART Project (Intelligent integration of supply chain processes and consumer services based on unique product identification in a networked business environment)* [on-line]. Dostupné z <http://www.smart-rfid.eu/>, Eltrun Research Center, 2007 (cit. 30. 6. 2009).

[6] –: *RACE NetworkRFID (Raising Awareness and Competitiveness in Europe)* [on-line]. Dostupné z <http://www.race-networkrfid.eu/>, RFID in Europe 2009 (cit. 30. 6. 2009).

Odkazy na internet:

http://www.epcglobalinc.org/ (GS1 EPCGlobal)
http://www.rfid-epc.cz (portál pracovní skupiny RFID-EPC při GS1 Czech Republic)
http://www.nfc-forum.org/ (NFC Forum)
http://www.etsi.org (ETSI)
http://www.ieee802.org/15/pub/TG4f.html (IEEE 802.15.4f Active RFID)
http://www.rfidjournal.com (RFID Journal)
http://www.rfid4u.com (RFID4U)
http://www.autoidlabs.org/ (Auto-ID Labs)
http://m2mxml.sourceforge.net/ (projekt M2MXML)
http://www.m2mmag.com/ (M2M Magazine)
http://www.fi-prague.eu/.(Future of the Internet Conference, Prague 2009)

Ing. Rita Pužmanová, CSc., MBA
(rita@ieee.org)