Wireless M-Bus: Kdo ví, že perete?

V poslední době se stále více prosazují dálkové odečty spotřeby energií v domácnostech. Časté odečty mohou vést k prozrazení řady detailů o chodu domácnosti. Proto stanoviska Úřadu pro ochranu osobních údajů i pracovní skupiny zřízené podle článku 29 (Article 29 Data Protection Working Party, dnes Evropský sbor pro ochranu osobních údajů – European Data Protection Board) dbají na ochranu soukromí danou Listinou základních práv a svobod a prováděcí legislativou, zejména obecným nařízením o ochraně osobních údajů. Na trhu se však objevují řešení pro odečty spotřeby vody a tepla, které nejsou v souladu s obecným nařízením o ochraně osobních údajů. Cílem tohoto článku je upozornit na tento problém a přinést doporučení na zlepšení situace.

dálkové odečty smart metering Wireless M-Bus GDPR soukromí

Za dodávky spotřebované energie je potřeba řádně zaplatit. Domácnosti obvykle platí zálohy. Dodavatelé energií provedou po určitém čase (např. v ročním intervalu) odečet stavů elektroměrů, vodoměrů, plynoměrů, měřidel tepla apod. Následně vystaví vyúčtování, vrátí přeplatky či požadují nedoplatky.

Historicky se odečty provádějí vizuálně. Zaměstnanec dodavatele, zmocněnec bytového družstva či SVJ přijde k měřiči a opíše stav. Takové zpracování odečtů má však své nevýhody, např. riziko chyb v opisu údajů. V bytových domech by měly být odečty prováděny v co nejmenším časovém rozestupu, aby se předešlo vzniku přebytků a ztrát oproti hlavnímu domovnímu měřiči. Často je však komplikované zajistit, aby byly navštíveny všechny byty v krátkém časovém období, protože jednotliví obyvatelé mohou být mimo domov. Proto se v poslední době prosazují chytrá měřidla (smart meters).

Tento článek se zabývá využitím protokolu Wireless M-Bus popsaného normou ČSN EN 13757 pro dálkové odečty. Wireless M-Bus je optimalizovaný pro přenos dat chytrých měřidel bezdrátovým způsobem jak formou jednosměrného čtení dat (člověkem či trvalou infrastrukturou, tzv. automatic meter readout – AMR), tak pomocí obousměrné komunikace (trvalá infrastruktura označovaná jako advanced metering infrastructure – AMI). Wireless M-Bus bývá nasazen v některých řešeních nabízených pro potřeby bytových domů, např. pro

odečet spotřeby vody či tepla. Pro doplnění kontextu týkajícího se inteligentního měření doporučujeme článek Legislativní požadavky na fungování a ochranu systémů inteligentního měření [11], který vyšel v DSM v čísle 2/2017.

Dodavatelé by měli budoucím provozovatelům poskytovat dostatek informací o nabízeném systému a právních dopadech jeho nasazení, což se však ne vždy děje. Např. odběratel nemusí dostat informaci, že údaje o spotřebě energií zpracovávané chytrými měřidly jsou osobními údaji dle obecného nařízení o ochraně osobních údajů, viz stanovisko 1/2014 Úřadu pro ochranu osobních údajů [14], stanovisko 12/2011 Article 29 Data Protection Working Party (WP29) [2] i normy ČSN EN 13757. Z této povahy údajů se pak odvíjí sada právních povinností správce i zpracovatele těchto dat, kterými legislativa cílí na ochranu soukromí osob, jichž se týkají údaje o provozu odběru energií v domácnosti (slovy právní úpravy subjekty údajů).

Jak funguje Wireless M-Bus?

Wireless M-Bus je navržen pro minimalizaci spotřeby elektrické energie, protože měřidla používající Wireless M-Bus často nemají přístup k trvalému zdroji elektrické energie (umístění na stoupačkách či topných tělesech) a musejí používat baterii.

Komunikaci protokolem Wireless M-Bus zahajuje vždy měřidlo. To v pravidelných intervalech (1) aktivuje vysílač, (2) zašle naměřená data bezdrátovým přenosem do všech stran v naději, že se informace dostane ke sběrnému zařízení, a (3) okamžitě (jednosměrný přenos, AMR) nebo s drobným odstupem (s možností navázání obousměrného přenosu, AMI) deaktivuje vysílač a šetří elektrickou energii. Sběrné zařízení má trvale aktivovaný přijímač, protože se předpokládá, že je buď trvale připojeno ke zdroji energie, nebo je možné je pravidelně dobíjet. Výhodou jednosměrné varianty je, že měřidlo nepotřebuje žádný přijímač a obvody eliminující přeslechy a odrazy vznikající při bezdrátových přenosech. Zvolený postup také redukuje množství kolizí hrozících při vysílání více měřidel současně.

Ve variantách AMR a AMI je v bytovém domě vybudovaná infrastruktura zahrnující trvale umístěná sběrná zařízení a další zařízení zajišťující přenos dat ke zpracovateli (např. s využitím brány s připojením k Internetu). Koncový odběratel má možnost sledovat spotřebu např. v informačním systému zpracovatele dat. Dle stanoviska 1/2014 Úřadu pro ochranu osobních údajů [14] je však zapojení do systému pro každého spotřebitele dobrovolné na základě odvolatelného a informovaného souhlasu či podpisu smlouvy o volitelné službě.

Při zpracování odečtů pracovníkem správce či zpracovatele údajů pomocí přenosného zařízení pro účely vystavení vyúčtování přijede odečítající pracovník na místo nasazení chytrých měřidel a provede odečet tak, že se dostane do míst, kam sahá signál měřidel. Po získání dat pracovník odejde a po zpracování přečtených dat je možné vystavit vyúčtování služeb.

K možnosti rychlého odečtu je nutné, aby měřidla zasílala data poměrně často. Autor článku se setkal se systémem, kdy dochází k přenosům stavu měřidel každých 80 sekund v pondělí až pátek přibližně 12 hodin denně. V ostatním čase (v noci pondělí až pátek, soboty a neděle) dochází k přenosům stavu měřidel přibližně každých 300 sekund.

Jednosměrná varianta protokolu Wireless M-Bus trpí neduhem nemožnosti ovlivnit přenášená data. Ať je či není

přítomno čtecí zařízení, obsah zprávy je vždy shodný. Proto je potřeba dbát na minimalizaci přenášených dat, aby byla naplněna stěžejní zásada obecného nařízení o ochraně osobních dat, čl. 5 odst. 1 c). Pokud nedojde k explicitnímu souhlasu subjektu údajů nebo k uzavření smlouvy o předávání průběžných naměřených hodnot, měla by měřidla zasílat jen data podstatná pro výpočet vyúčtování, jinak je ohroženo soukromí obyvatel domu. Samotná norma ČSN EN 13757 upozorňuje na existenci rizik spojených s detailním monitorováním spotřeby a požaduje, aby si organizace provozující systémy založené na této normě vypracovaly mechanismy vyhodnocující a předcházející rizikům na dopady soukromí. WP29 doporučuje zasílání stavu jen tak často, jak je potřeba [2] – v případě ročně vystavovaného vyúčtování by se tedy jednalo o hodnotu zaznamenanou na přelomu roku.

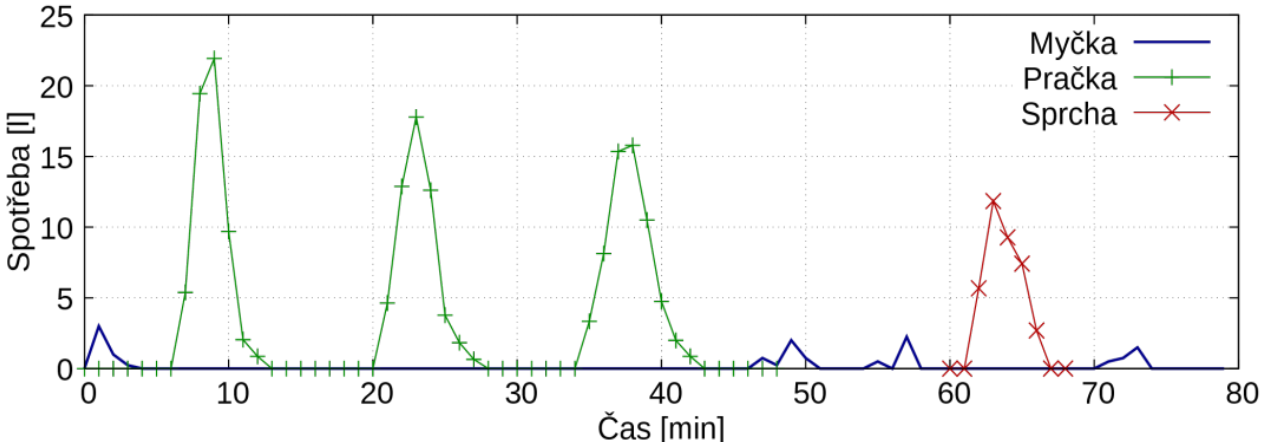
Vzhledem k tomu, že měřidla mění frekvenci zasílání zpráv v závislosti na dni v týdnu a denní době, musejí mít přehled o čase. Je tedy v současných technických možnostech splnění požadavku minimalizace dat na přenos hodnoty měřidla na roční bázi: ve všech přenosech se po celý rok přenáší stejná hodnota.

V případě nasazení obousměrné varianty (typicky pouze AMI) je možné minimalizace přenášených dat docílit i tak, že se aktuální stav neposílá v pravidelně zasílaných zprávách, ale až na vyžádání čtecím zařízením. V této variantě měřidlo zasílá zprávy signalizující svou připravenost přijímat pokyny. Čtecí zařízení se autentizuje a vyšle požadavek na čtení stavu jen při vzniku zákonné potřeby odečtu, např. jednou ročně, při stěhování, na základě smlouvy uzavřené se subjektem údajů apod. Vzhledem k tomu, že se obousměrná varianta obvykle nepoužívá při variantě AMR, autor článku očekává, že toto řešení je aplikovatelné v menším množství odečtů založených na protokolu Wireless M-Bus.

Jak měřidla narušují soukromí?

Tématem zneužití dat produkovaných měřidly spotřeby vody a elektrické energie bez minimalizace přenášených stavů se obšírně zabývá dostupná literatura. I když se většina článků zaměřuje na měřidla elektrické energie, některé se věnují i měřidlům vody [3, 4, 5, 8, 13].

Nejběžnějším tématem popisovaným v literatuře, např. [5, 8, 14], je téma detekce přítomnosti a nepřítomnosti osob. Při spotřebě vody je zpravidla také přítomen někdo, kdo vodu spotřeboval. Při dlouhodobém sledování spotřeby domácnosti je možné zjistit opakované časy, kdy nikdo v domácnosti není [8]. Taková informace je využitelná pro nevyžádaný komerční kontakt či rovnou kriminální činnost (krádeže, stalking).



Obr. 1: Spotřeba vody při využití pračky, myčky a sprchování s využitím dat výzkumu CSIRO [1]

Chen a kol. [4] úspěšně identifikovali domácí aktivity spojené s využíváním vody (sprchování, praní prádla) s využitím měřidel zasílajících stav vodoměru v 15minutových intervalech. Obr. 1 ukazuje spotřebu vody při využití pračky, myčky a sprchování.

Některá zařízení také mohou mít specifický průběh spotřeby [8, 7, 9, 6]. Např. konkrétní typ pračky spotřebuje s určitým programem určité množství vody, přičemž voda se napouští s rozestupy specifickými pro dané zařízení. Toho je možné využít při výběru budoucí oběti vykradení, profilování pro marketingové účely apod. Některé nemoci trávicí soustavy jsou spojené s častějším navštěvováním toalety. Vzhledem k tomu, že má splachovací nádrž toalety v každém bytě nějakou konkrétní kapacitu, je možné z aktuální spotřeby odvodit návštěvy toalety. Comcast chce v roce 2020 uvést na trh zařízení, které bude odhadovat zdravotní stav na základě několika vstupů včetně návštěv toalety [12].

Ze spotřeby vody během svátků a v průběhu přípravy na ně je možné v datech produkovaných měřidly objevit specifické vzory týkající se náboženského vyznání. Např. rozdílný termín římskokatolických a pravoslavných Vánoc a Velikonoc se promítne v různé termíny velkého úklidu domácnosti a v různé termíny přípravy pokrmů náročných na množství ušpiněného nádobí. Jak úklid domácnosti, tak umývání nádobí se promítne do množství spotřebované vody.

Lisovich a kol. [8] upozorňuje, že v přítomnosti sledování více zdrojů dat (elektřina, voda, plyn aj.) je možné data navzájem porovnávat a odvozovat další informace. Např. zapnutá pračka spotřebovává nejen vodu, ale i elektřinu. Při nasazení jak měřidel tepla, tak měřidel vody si může být pozorovatel provozu měřidel jistější v určení svátečních příprav. Viděl by zvýšené používání trouby (formou nižšího odběru tepla) i zvýšené množství spotřebované vody.

Zabezpečení dat

Na realizaci útoku na systém bezdrátových odečtů není potřeba drahé softwarové a hardwarové vybavení. Kromě

obyčejného notebooku, Raspberry Pi či podobného zařízení stačí vlastnit jen přijímač podporující Wireless M-Bus, který je možno zakoupit již v ceně okolo 2 500 Kč. Autor článku prakticky ověřil, že takový přijímač umožňuje v prostředí panelového domu a okolí záchyt až na 40 m. Rouf a kol. [10] vyzkoušeli, že s použitím vhodné antény a zesilovače je možné zachytávat data na delší vzdálenosti. Potřebné programové vybavení je možné na Internetu stáhnout zdarma včetně zdrojových kódů[1]. K dispozici jsou také nástroje pro podvržení dat [3].

ČSN EN 13757-1:2015 doporučuje vypracovat analýzu bezpečnostních hrozeb a v návaznosti zvolit vhodné zabezpečení dat pro zajištění soukromí, integrity a autentizace, např. pomocí ČSN ISO/IEC 27033 a ČSN ISO/IEC 15408. Také vyžaduje použití unikátního klíče s doporučením na jeho průběžnou obměnu. Klíč nesmí být odvozen z jiných dat, jako je číslo měřidla. Stanovisko WP29 vyžaduje šifrovaný přenos mezi koncovými zařízeními (end-to-end) [2]. Tomuto stanovisku odporuje služba AMR, pokud jsou odečty spotřeby přenášené přes Internet v nezabezpečené podobě.

Při nasazení v bytových domech se nedá očekávat, že správce domu (SVJ, bytové družstvo) v roli správce osobních údajů (při rozpočítávání spotřeby vody a tepla) ve smyslu obecného nařízení o ochraně osobních údajů bude mít dostatečnou znalost norem, bezpečnostních zvyklostí, šifrovacích mechanismů apod. Aplikováním článků 24, 25 a 32 obecného nařízení o ochraně osobních údajů vzniká provozovateli systému povinnost zajistit zabezpečení dat. Je proto nanejvýš vhodné, aby dodavatel systému nabízel služby zajišťující bezpečnost systému, např. formou smlouvy o dohledu nad provozovanými zařízeními a jejich souladem s aktuálním stavem daným normami a veřejně publikovanými útoky [3].

[1] Např. https://github.com/CBrunsch/scambus, https://github.com/weetmuts/wmbusmeters

Závěr

Wireless M-Bus je určen pro použití v prostředí omezeného přísunu elektrické energie, pro měřidla fungující na baterie. Spotřeba elektrické energie je redukována tím, že komunikační obvody měřidla většinu času spí. Probouzejí se pouze v době určené pro vysílání. V jednosměrné variantě se komunikační část měřidla po zaslání dat okamžitě uspí. V obousměrné variantě se po zaslání dat na krátkou dobu aktivuje přijímač. Samotný standard ČSN EN 13757-4 specifikuje maximální délku periody zasílání dat jako 15 minut či 2 hodiny podle typu přenosu. V praxi se pro pohodlnější dálkový odečet používají hodnoty v jednotkách minut.

Dodavatelé systémů chytrých měřidel by měli své zákazníky seznámit s principem fungování nabízených systémů (obzvlášť pokud automaticky přenášejí odečítaná data i bez přítomnosti oficiálního čtecího zařízení) a průběžně doporučovat modernizaci systému v reakci na nové normy či útoky, např. formou placené služby. Součástí takové služby by mělo být zajištění správného zacházení s klíči popsanými v ČSN EN 13757 včetně minimalizace množství osob se znalostí sdíleného klíče, což není např. výrobce zařízení. Pokud se dodavatel systému stane zpracovatelem vyúčtování, měl by si smluvně se správcem rozdělit zodpovědnost: kdo zodpovídá za přenosy, jejich obsah a zabezpečení?

Měřidla by měla přenášet minimální množství potřebných údajů. WP29 upozorňuje, že zařízení by měla ve výchozím nastavení dbát na ochranu soukromí [2]. Stanovisko

1/2014 Úřadu pro ochranu osobních údajů vyžaduje, aby přenosy byly přiměřené a nezbytné [14]. Získání podrobností o soukromí uživatelů bytů lze velmi efektivně zamezit prostým splněním zákonného požadavku na minimalizaci osobních údajů. V případě jednosměrné varianty chytrých vodoměrů stačí nastavit vysílání jediné hodnoty relevantní pro samotný účel měření – a to hodnoty spotřeby vody ke konci roku. U obousměrné varianty je možné zasílat aktuální stav až jako odpověď na požadavek ze strany čtecího zařízení. Měřidlo může vysílat v časové frekvenci umožňující pohodlný odečet za předpokladu, že se po celý rok bude přenášet jedna hodnota nebo se bude aktuální stav zasílat až po autorizaci oficiálního sběrného zařízení (obousměrná varianta). V případě mimořádného odečtu stavu vodoměru se dá předpokládat osobní účast zainteresovaných (typicky při nájmu, převodu bytu) a vizuální odečet stavu vodoměru bude komfortnější i vhodnější.

Dodavatelé by měli společně s měřidly dodávat i posouzení dopadů dle čl. 35 obecného nařízení o ochraně osobních údajů (tzv. DPIA)[2]. Vysoké riziko pro subjekty údajů plyne z vysoké citlivosti údajů produkovaných měřidly. Vypracování DPIA je obzvláště důležité při plánovaném plošném nasazení dálkových odečtů, tedy bez možnosti subjektu údajů prosadit svá práva.

Evropská komise vydala doporučení týkající se využívání inteligentních měřících systémů v distribuci elektřiny a plynu[3]. Z něho vychází i připravovaný text směrnice EU o společných pravidlech pro vnitřní trh s elektřinou[4], který obsahuje možnost koncového odběratele požádat o přístup ke standardizovanému lokálnímu či dálkovému přístupu. Provozovatelé systému založeného na protokolu Wireless M-Bus by měli zvážit poskytnutí klíče pro čtení dat z měřidel. Koncoví odběratelé by tak mohli data produkovaná měřidly využít pro své účely, případně si ověřit, jaká data o nich měřidla přenášejí.

Libor Polčák
polcak@fit.vutbr.cz

Ing. Libor Polčák, Ph.D.

Působí na Fakultě informačních technologií Vysokého učení technického v Brně, kde také vystudoval. V rámci výzkumné skupiny počítačových sítí se dlouhodobě zabývá bezpečnostním výzkumem.

Tento příspěvek vznikl za podpory projektu VI20172020062 financovaného Ministerstvem vnitra ČR. Na přípravě článku se cennými radami podílela JUDr. Ing. Helena Svatošová.

[2] Pro oblast inteligentního měření existuje šablona Data protection Impact assessment template for smart grid and smart metering environment, https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment

[3] Doporučení Komise ze dne 9. března 2012 o přípravách na zavedení inteligentních měřicích systémů (2012/148/EU), https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32012H0148 distribuce plynu a elektřiny

[4] Directive of the European Parliament and of the Council on common rules for the internal market in elektricity, http://eur-lex.europa.eu/resource.html?uri=cellar:c7e47f46-faa4-11e6-8a35-01aa75ed71a1.0014.02/DOC_1&format=PDF

POUŽITÉ ZDROJE

[1] Sources of critical contaminants in domestic wastewater: contaminant loads from household appliances. Technická zpráva, 2008, CSIRO: Water for a Healthy Country National Research Flagship. Dostupné online na https://www.researchgate.net/publication/242137154_Sources_of_critical_contaminants_in_domestic_wastewater_contaminant_loads_from_household_appliances.

[2] Article 29 Data Protection Working Party: Opinion 12/2011 on smart metering. 2011, dostupné online na https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf.

[3] BRUNSCHWILER, C.: Wireless M-Bus Security. Whitepaper Black Hat USA 2013, 2013, https://www.compass-security.com/fileadmin/Datein/Research/Praesentationen/blackhat_2013_wmbus_security_whitepaper.pdf.

[4] CHEN, F.; DAI, J.; WANG, B.; aj.: Activity Analysis Based on Low Sample Rate Smart Meters. In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, NY, USA: ACM, 2011, ISBN 978-1-4503-0813-7, s. 240–248. URL http://doi.acm.org/10.1145/2020408.2020450

[5] EROL-KANTARCI, M.; Mouftah, H. T.: Smart grid forensic science: applications, challenges, and open issues. IEEE Communications Magazine, ročník 51, č. 1, 2013: s. 68–74, ISSN 0163-6804.

[6] HURRI, P.; NEUVO, N.; MIKKOLA, T.; aj.: Smartgrid energy-usage-data storage and presentation systems, devices, protocol, and processes including a visualization, and load fingerprinting process. US Patent US8949050B2 přiřazený BASEN CORP.

[7] KELLY, D. A.: Disaggregating Smart Meter Readings using Device Signatures. 2011, diplomová práce, Imperial College London, http://www.doc.ic.ac.uk/teaching/distinguished-projects/2011/d.kelly.pdf.

[8] LISOVICH, M. A.; Mulligan, D. K.; Wicker, S. B.: Inferring Personal Information from Demand-Response Systems. IEEE Security Privacy, ročník 8, č. 1, 2010: s. 11–20, ISSN 1540-7993.

[9] VAN MEGEN, F.; MUELLER, U.: Classifying devices by fingerprinting voltage and current consumption. US Patent US20110313582A1 přiřazený Microsoft Technology Licensing LLC, https://patents.google.com/patent/US20110313582A1/en.

[10] ROUF, I.; MUSTAFA, H.; XU, M.; aj.: Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, New York, NY, USA: ACM, 2012, ISBN 978-1-4503-1651-4, s. 462–473.

[11] STUPKA, V.; PITNER, T.: Legislativní požadavky na fungování a ochranu systémů inteligentního měření. Data Security Management, ročník XXI, č. 2, 2017, ISSN 1211-8737.

[12] WELCH, C.: Comcast is reportedly developing a device that would track your bathroom habits. 2019, dostupné online na https://www.theverge.com/2019/5/21/18634466/comcast-health-monitoring-speaker-amazon-echo.

[13] WIGAN, M.: User Issues for Smart Meter Technology. IEEE Technology and Society Magazine, ročník 33, č. 1, 2014: s. 49–53, ISSN 0278-0097.

[14] Úřad pro ochranu osobních údajů: Stanovisko č. 1/2014 – Chytré měření a ochrana osobních údajů. 2014, dostupné online na https://www.uoou.cz/stanovisko-c-1-2014-chytre-mereni-a-nbsp-ochrana-osobnich-udaju/d-7067/p1=1099.