„Smart Meters” a Cyberbezpieczeństwo

Przemysław Kubiak

Politechnika Wrocławska

IATI Cybersecurity Academy, 25 luty 2016

Konspekt prezentacji

- Uzależnienie społeczeństwa od dostaw energii elektrycznej
- Potrzeba wprowadzenia „smart meters”
- Pozytywne aspekty wprowadzenia inteligentnych liczników
- Zagrożenia
- Luki bezpieczeństwa znalezione w przykładowym liczniku (Black Hat 2014)
- Proces budowy wymagań - CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids
- Przykładowe wymagania - Niemcy
- Specyfikowanie wymagań w Polsce

Uzależnienie społeczeństwa od dostaw energii elektrycznej

Sieć generacji i dystrybucji energii elektrycznej jest jednym z najbardziej krytycznych komponentów infrastruktury. Jeśli ona przestaje działać, w krótkim okresie czasu społeczeństwo przestaje normalnie funkcjonować.

- 1996, Auckland, Nowa Zelandia: sześciotygodniowa przerwa w dostawie energii do głównej dzielnicy biurowej; 60 000 z 74 000 pracowników musiało pracować z domu lub z biur o zmienionej lokalizacji, a mieszkańcy 6000 apartamentów wyprowadzili się z nich na ten okres
- . . .

Uzależnienie społeczeństwa od dostaw energii elektrycznej

- . . .
- Maj 1999, operacja ALLIED FORCE przeciwko Serbii. Po przeprowadzeniu ataków z wykorzystaniem bomb BLU-114/B (bomba grafitowa) 70% obszaru kraju było bez prądu
- Podobnie w trakcie wojny z Irakiem (operacja DESERT STORM) instalacje przesyłu i dystrybucji prądu okazały się celem lotnictwa USA.

Bomba grafitowa – w trakcie detonacji rozsypuje włókna grafitowe, które tworzą chmurę przewodząca energię elektryczną. Bomba zdetonowana nad transformatorami lub liniami przesyłowymi powoduje natychmiastowe przepięcia i niszczenie infrastruktury (fot. z [4]).

Potrzeba wprowadzenia „smart meters”

System dostaw energii staje się coraz bardziej skomplikowany, rośnie liczba generatorów, oraz:

- Różne rozwiązania mają różne charakterystyki: np. koszt budowy elektrowni jądrowej jest wysoki, natomiast koszt jej użytkowania jest relatywnie niski, dlatego ekonomicznie uzasadnione jest użytkowanie jej na maksymalnej mocy.
- . . .

Potrzeba wprowadzenia „smart meters”

- . . .
- Elektrownie węglowe maja zwykle dłuższy czas rozruchu, co utrudnia ich zastosowanie do kompensacji szczytowego zapotrzebowania na moc, które jest okresowe (największe zapotrzebowanie jest rano i wieczorem).
- Turbiny gazowe są bardziej elastyczne (krótszy rozruch), ale koszt energii jest wyższy.
- Jeśli pobór prądu jest za duży, lub dostawca energii nie dysponuje elektrowniami, wówczas kupuje energie na wolnym rynku.

Potrzeba wprowadzenia „smart meters”

- Generatory energii odnawialnej dodatkowo komplikują sytuację (ilość energii osiąganej z elektrowni pływowych jest przewidywalna, z elektrowni słonecznych już mniej, z elektrowni wiatrowych najmniej przewidywalna). W niektórych krajach (np. w Niemczech) dostawcy energii są zobowiązani akceptować energię odnawialną, tzn. przyjmować ją w swoją sieć dystrybucji.

Potrzeba wprowadzenia „smart meters”

Dostawcy energii są zainteresowani:

- Precyzyjnym przewidywaniem zapotrzebowania na energię (ułatwienie planowania wykorzystania zasobów)
- Zmianą zachowania odbiorców energii: by starali się zużywać energię w sposób bardziej jednostajny, obniżając zapotrzebowanie w godzinach szczytowego poboru mocy.

Potrzeba wprowadzenia „smart meters”

- Typowy miernik poboru mocy zapewnia tylko dwie taryfy: standardową i nocną.
- Z drugiej strony ceny energii elektrycznej na wolnym rynku ustalane są z dużo większą rozdzielczością. Np. w Wielkiej Brytanii ceny energii na kolejną dobę ustalane są z osobna dla każdego z 48 półgodzinnych okresów. Na innych rynkach ceny różnicowane są z dokładnością do godziny lub 15 min.

Potrzeba wprowadzenia „smart meters”

- Trudno jest zmienić obecne zachowanie odbiorcy, jeśli nie jest on bezpośrednio zależny od cen rynkowych energii.
- Stąd pomysł by informacja o zużyciu energii przez jej odbiorcę była osiągalna z tą samą rozdzielczością, z jaką ustalane są jej ceny rynkowe.
- Dodatkowy czynnik: taryfy prepaid (możliwość zdalnego przełączenia w przypadku zalegania z opłatami za energie).

Pozytywne aspekty wprowadzenia inteligentnych liczników

- Zaadresowanie potrzeb dostawców energii.
- Potencjalna możliwość komunikacji miernika poboru mocy z urządzeniami elektrycznymi w domu: użytkownik mógłby programować np. pralkę lub zmywarkę, by realizowała program dopiero w momencie, w którym koszt energii jest niższy od pewnego progu, lub jest np. najniższy.

Zagrożenia

- W przypadku przejęcia kontroli nad miernikiem - możliwość wysyłania zafałszowanych danych, lub możliwość przejścia z trybu prepaid do trybu zwykłego.
- W przypadku utraty poufności danych przesyłanych z miernika do dostawcy energii – możliwość odczytu informacji o porach aktywności użytkowników (a w przypadku zmiany oprogramowania miernika – możliwość identyfikowania niektórych urządzeń)

Zagrożenia

- W przypadku możliwości uwierzytelniania własnej komunikacji do miernika (utrata integralności komunikacji przez miernik) możliwość złośliwego wyłączenia prądu, lub przełączenia w tryb prepaid.
- W przypadku masowego przejęcia mierników – możliwość masowego wyłączenia prądu, oraz (poprzez zmianę kluczy lub oprogramowania) uniemożliwienie zdalnej naprawy sytuacji przez dostawcę energii – skutek: paraliż systemu.

Luki bezpieczeństwa znalezione w przykładowym mierniku

- Przebadano losowy miernik z rynku hiszpańskiego, wyniki omówiono na konferencji Black Hat 2014.
- Mikroprocesory obecne na tym mierniku nie mają pamięci wewnętrznej (w szczególności procesor odpowiedzialny za szyfrowanie komunikacji): klucze i firmware osobnych kościach pamięci trwałej
- Otwarty port do debugowania urządzenia.

Luki bezpieczeństwa znalezione w przykładowym mierniku

- Stąd możliwość analizy zachowania się miernika (reverse engineering) oraz znalezienia kluczy kryptograficznych.
- Zastosowano jedynie symetryczny algorytm szyfrowania AES-128.
- **Klucz jest taki sam dla wszystkich urządzeń!!!**
- Po odczytaniu klucza możliwość wymiany oprogramowania (firmware’a) na własne.
- **Możliwość realizacji wszystkich ww. zagrożeń.**

Właściwe jest pytanie: jakie wymagania obecnie mają spełniać inteligentne liczniki?

Proces budowy wymagań - CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids

- W 2011 Komisja Europejska oraz Europejskie Stowarzyszenie Wolnego Handlu wydało tzw. „Smart Grid Mandate M/490” na opracowanie metodologii/podstaw dla opracowywania/rozwijania standardów dla „smart grid”.
- W odpowiedzi trzy europejskie organizacje standaryzacyjne zawiązały grupę koordynacyjną: CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG).
- Z końcem 2012 roku ww. mandat został przedłużony do końca 2014r.
- Do końca 2014 SG-CG opracowało zbiór dokumentów [6], wśród których jest raport „Smart Grid Information Security”.

Proces budowy wymagań - CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids

SG-CG Smart Grid Information Security to

- Wysokiego poziomu dokument, tworzony zgodnie z metodologią analizy ryzyka.
- Patrzy całościowo na architekturę wytwarzania, dostaw i konsumpcji energii.
- Wyróżnia kluczowe dla bezpieczeństwa komponenty ww. architektury.
- W kontekście bezpieczeństwa zaleca stosowanie właściwego dla infrastruktury krytycznej podejścia obejmującego nastepujące aspekty: . . .

Proces budowy wymagań - CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids

W kontekście bezpieczeństwa zaleca stosowanie właściwego dla infrastruktury krytycznej podejścia obejmującego nastepujące aspekty:

- Zarządzanie bezpieczeństwem i ryzykiem.
- Zarządzanie cyklem życia komponentów infrastruktury oraz procedur operacyjnych.
- Procedury odpowiedzi na incydenty, zarządzanie wymianą informacji.
- Plan ciągłości działania.
- Bezpieczeństwo fizyczne, sieciowe.
- Określanie zakresu odpowiedzialności.
- Audyt, treningi, . . .

Przykładowe wymagania - Niemcy

- W Niemczech Ministerstwo Gospodarki i Energii zobowiązało Federalne Biuro ds. Bezpieczeństwa Informacji (Bundesamt für Sicherheit in der Informationstechnik) do wytworzenia specyfikacji dla komponentów inteligentnego systemu pomiarowego, które bezpośrednio współpracują z licznikiem (brama - smart meter gateway).
- Powstała specyfikacja techniczna BSI TR-03109 oraz dwa „protection profiles” (PP) - PP dla bramy i dla modułu kryptograficznego bramy.

Przykładowe wymagania - Niemcy

BSI TR-03109 - rozległa dokumentacja:

- Specyfikacja techniczna dla bramy (smart meter gateway).
- Specyfikacja techniczna dla modułu kryptograficznego bramy.
- Zalecenia kryptograficzne dla bramy.
- Specyfikacja Infrastruktury Klucza Publicznego dla bramy.
- Specyfikacja techniczna dla adaptera komunikacyjnego.
- Specyfikacje testów dla bramy, modułu kryptograficznego oraz dla adaptera komunikacyjnego.

Przykładowe wymagania - Niemcy

Protection Profiles:

- Szczegółowe dokumenty określające wymagania bezpieczeństwa w sformalizowany sposób.
- Określają założenia środowiska, w którym działają komponenty.
- Opisowo pokazują, z jakich celów/przesłanek wynikają formalne warunki bezpieczeństwa.

Specyfikowanie wymagań w Polsce

- W kietniu 2015 Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT) wystosowała list do Ministra Gospodarki – propozycję zarządu KIGEiT dotyczącą iteroperacyjności urządzeń pomiarowych w sieciach smart grid.
- Propozycja wskazuje na konieczność pilnego określenia warunków technicznych dla liczników zdalnego odczytu (smart meters) tak by wynikowy system m.in.:
  - pozwalał na rozwój sieci smart grids w oparciu o otwartą architekturę,
  - miał jednoznacznie zdefiniowaną komunikację z bramą domową,
  - spełniał wymogi bezpieczeństwa teleinformatycznego w sieciach SG w oparciu o otwarte standardy,
  - zapewniał interoperacyjnosć.
- Ponadto KIGEiT proponuje powołanie zespołu ds. Smart Grids oraz Pełnomocnika Rządu ds. sieci inteligentnych.

Specyfikowanie wymagań w Polsce

- Jednocześnie 11 marca 2014 r. na stronie Urzędu Regulacji Energetyki do dyskusji publicznej został wystawiony projekt Wzorcowej Specyfikacji Technicznej dla postępowań przetargowych na dostawę infrastruktury licznikowej dla systemów AMI (Advanced Metering Infrastructure). W dniu 25 maja 2015 r. została opublikowana aktualna wersja dokumentów.
- Dokument w kontekście protokołów i komponentów kryptograficznych jest dużo mniej szczegółowy niż specyfikacja BSI.

- **Projekt wzorcowej specyfikacji polega na konsultacjach społecznych jako na mechaniźmie opracowywania architektury bezpieczeństwa dla podsystemu elektronicznego wchodzącego w skład infrastruktury krytycznej**.
- Kto może sobie pozwolić na przeznaczenie zasobów koniecznych do przeprowadzenia niezbędnych analiz i wypracowania architektury ww. systemu na zasadzie konsultacji społecznych?
- Przykładowe pytanie dot. bezpieczeństwa oraz pytanie dot. interoperacyjności:
  - Zgodnie ze specyfikacją możliwa ma być zdalna aktualizacja oprogramowania liczników i koncentratorów, przy czym serwer udostępniający to oprogramowanie ma się uwierzytelniać. Czy poza wykonaniem protokołu uwierzytelniania serwera licznik ma weryfikować, czy nowa wersja oprogramowania jest podpisana? Gdzie we wzorcowej specyfikacji jest taki wymóg?
  - Jakie algorytmy weryfikacji podpisu ma wspierać licznik w komunikacji z adapterem HAN?

Źródła

1. Ross Anderson, Shailendra Fuloria: Who controls the off switch? Smart Grid Communications (SmartGridComm) 2010
2. Alberto Garcia Illera, Javier Vazquez Vidal: Lights Off! The Darkness of the Smart Meters, Black Hat 2014
   `https://www.youtube.com/watch?v=Z_y_vjYtAWM`
3. Christopher Laughman, i in.: Power Signature Analysis, IEEE Power & Energy magazine 2003
4. CBU-94 Blackout Bomb, BLU-114/B Soft-Bomb
   `http://fas.org/man/dod-101/sys/dumb/blu-114.htm`
5. Tobias Jeske: Privacy Preserving Smart Metering Without a Trusted Third Party, Security and Cryptography (SECRYPT), 2011

Źródła

6 CEN-CENELEC-ETSI Smart Grid Coordination Group: http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

7 Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03109

8 Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (KIGEiT): Propozycja zarządu KIGEiT dotycząca interoperacyjności urządzeń pomiarowych w sieciach Smart Grids http://www.kigeit.org.pl/FTP/kl/SIS/150428_Wniosek_interoperacyjnosc_pomiarow_SG.pdf

9 Urząd Regulacji Energetyki: Projekt Wzorcowej Specyfikacji Technicznej dla systemów AMI (2015)

10 BSI: Protection Profile for the Gateway of a Smart Metering System and Protection Profile for the Security Module of a Smart Meter Gateway

Dziękuję za uwagę!