Chytrá měřidla v domácnosti: hrozba, nebo zdroj informací pro vyšetřování?

Libor Polčák
2019-09-09

Chyté měřidla (smart meters)

- Umožňují *dálkové* čtení stavu
  - Prevence chybného opisu stavu
  - Čtení všech měřidel ve *shodný* čas
  - Není nutná spolupráce majitele domu/bytu
- Doporučení Komise ze dne 9. března 2012 o přípravách na zavedení inteligentních měřicích systémů (2012/148/EU)
  - Připravovaná směrnice EU o společných pravidlech pro vnitřní trh s elektřinou

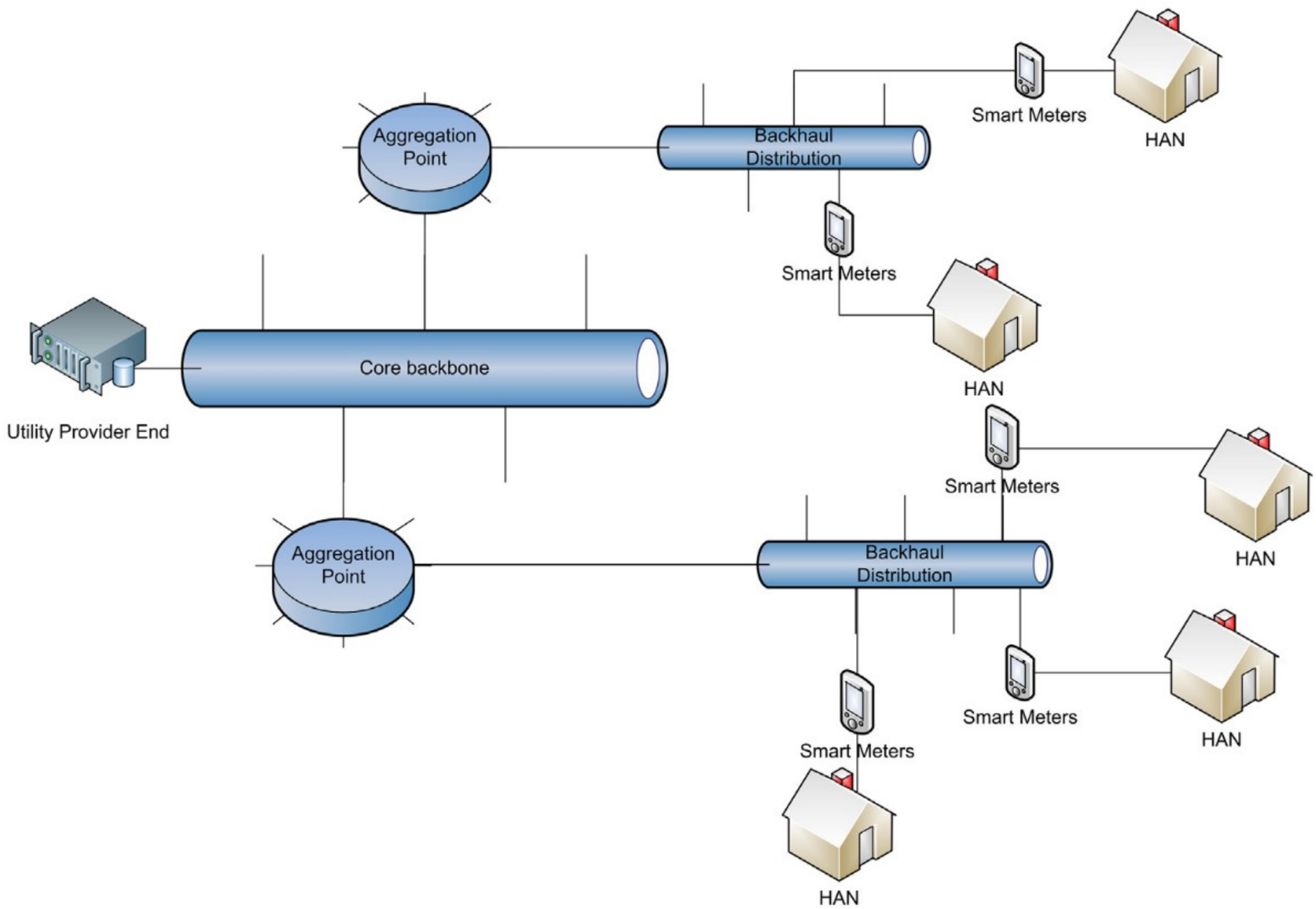
AMR vs. AMI

automatic meter readout (AMR)

advanced metering infrastructure (AMI)

Nasazení v distribuční síti

R. Rashed Mohassel et al./Electrical Power and Energy Systems 63 (2014) 473–484

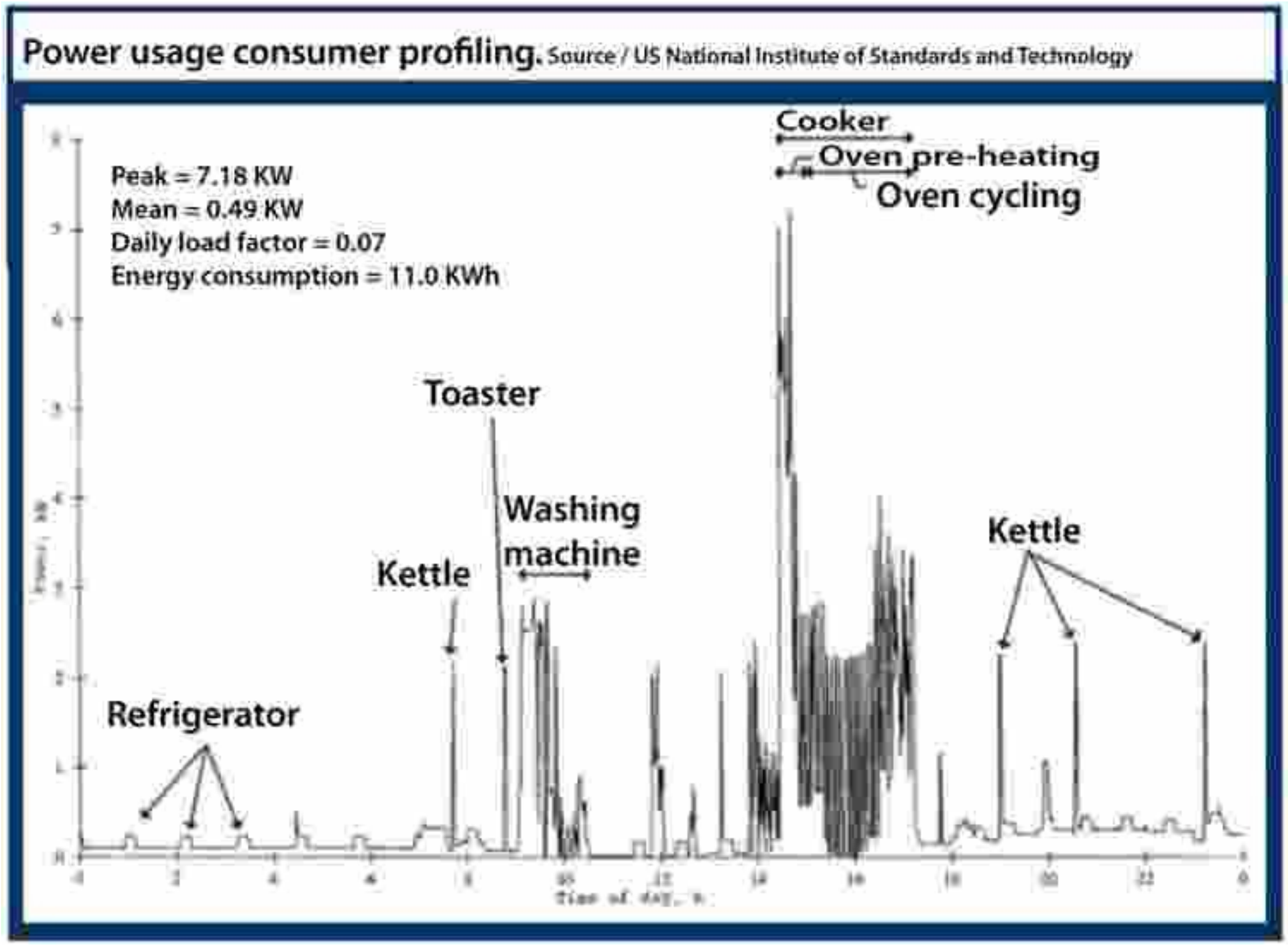


Výhody

- Odběratelé s chytrými měřidly mají nižší spotřebu vody/elektřiny (varinta AMI, zobrazování grafů spotřeby)
- Brzká detekce úniků vody a jiných problémů sítě (AMI)
- Snížení ceny odečtů (především AMI)
- Lepší analýza chování spotřebitelů → predikce využití sítě (AMI)
- Prevence proti podvodům (AMI)

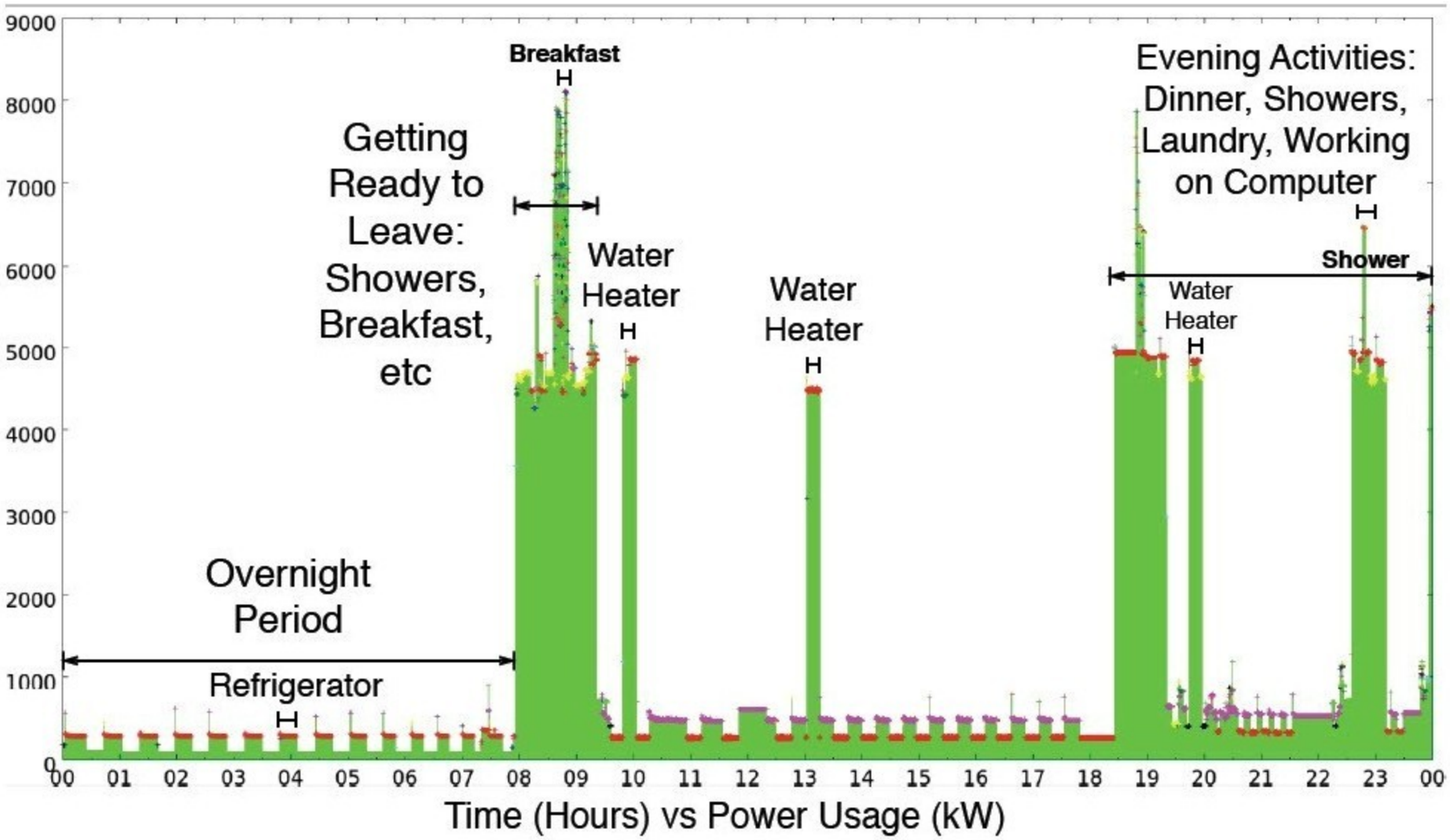
Náhled na dění v domácnosti
Výhoda? Nevýhoda?

Sledování dění v domácnosti



NISTIR 7628, Guidelines for Smart Grid Cyber Security

Sledování dění v domácnosti

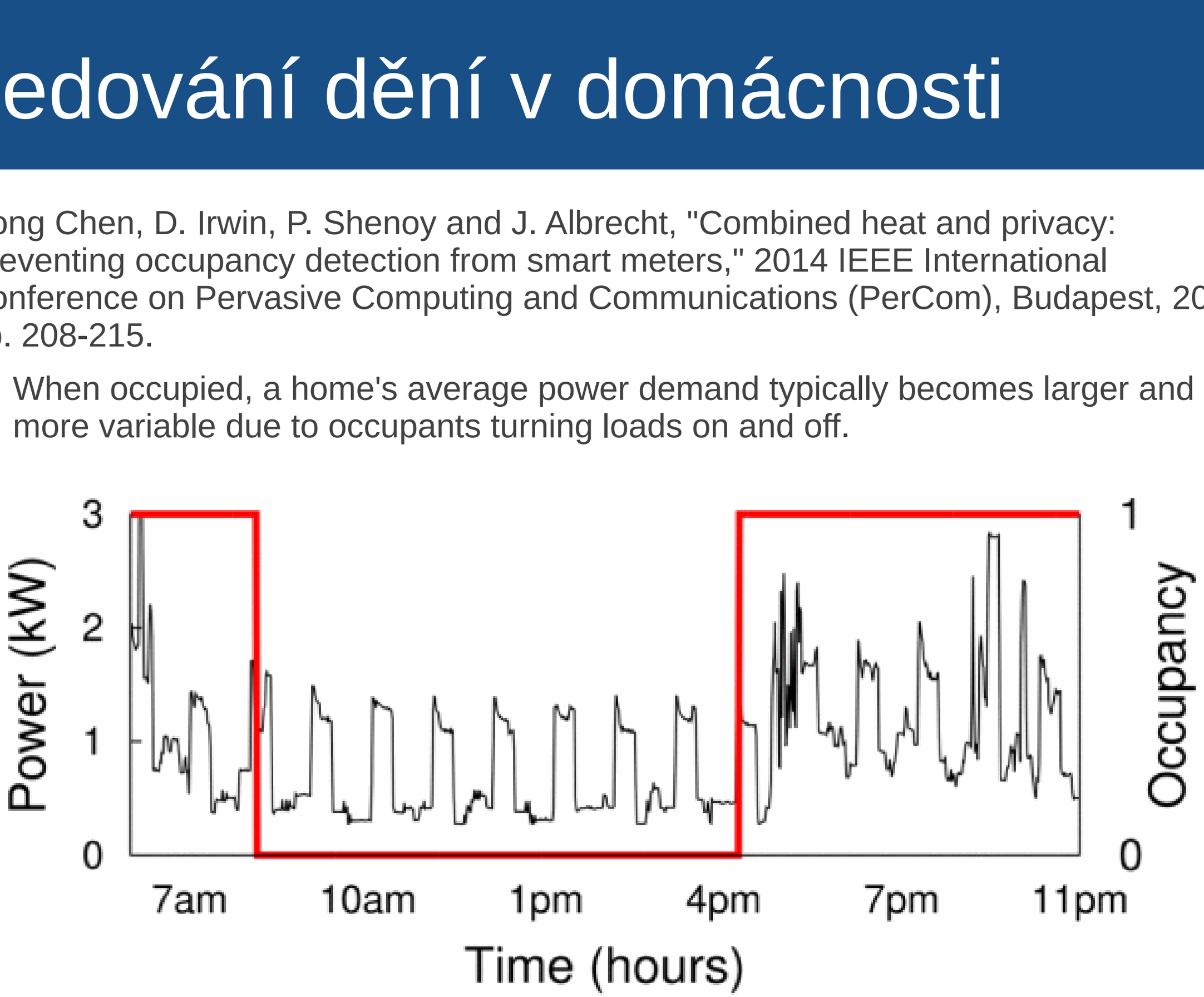


Without detailed knowledge of appliance signatures, intuitive observation with power consumption variations indicates human activity.

Credit: "Private Memoirs of a Smart Meter," Molina-Markham, et.al., 2nd ACM Workshop On Embedded Sensing Systems For Energy-Efficiency In Buildings (BuildSys 2010), Zurich, Switzerland, November 2, 2010.

Sledování dění v domácnosti

- Dong Chen, D. Irwin, P. Shenoy and J. Albrecht, "Combined heat and privacy: Preventing occupancy detection from smart meters," 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), Budapest, 2014, pp. 208-215.
  - When occupied, a home's average power demand typically becomes larger and more variable due to occupants turning loads on and off.



Sledování dění v domácnosti

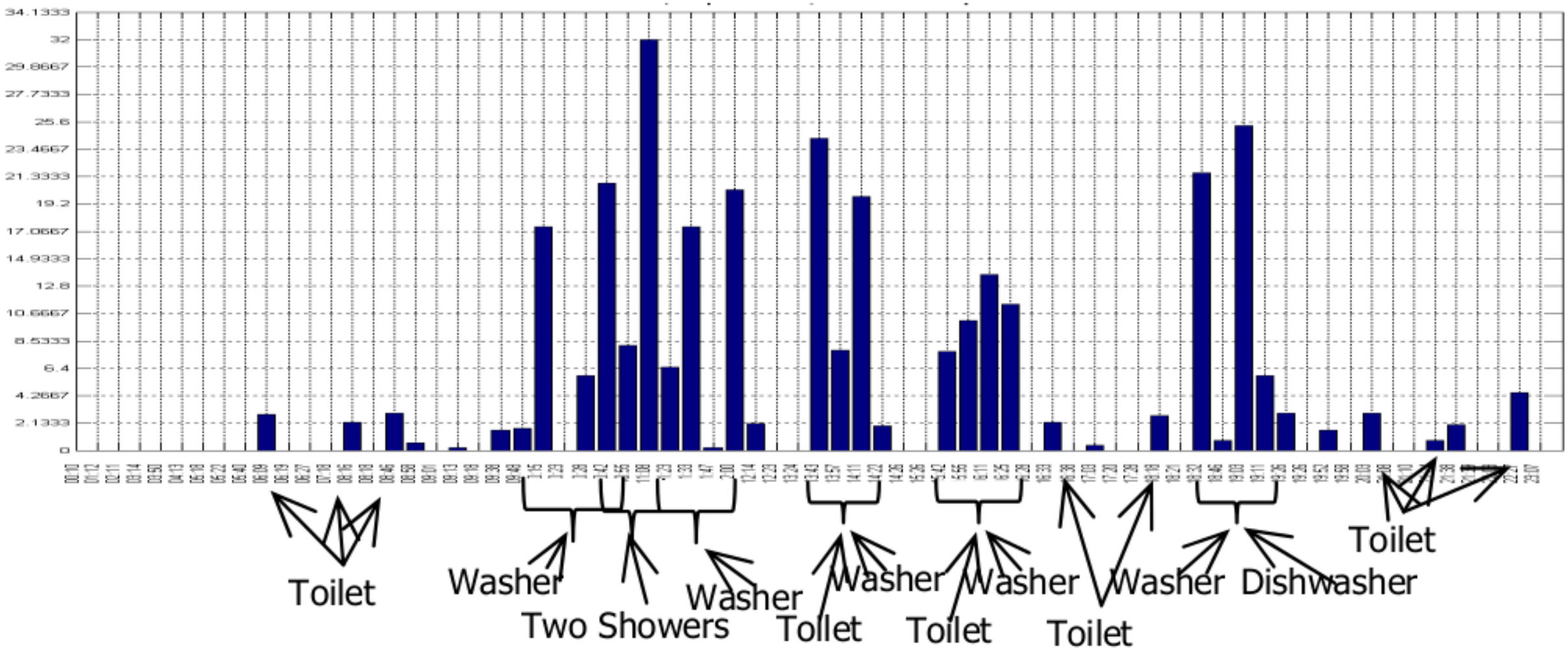
Smart meter hacking can disclose which TV shows and movies you watch

https://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/

http://www.youtube.com/28c3#p/u/54/YYe4SwQn2GE

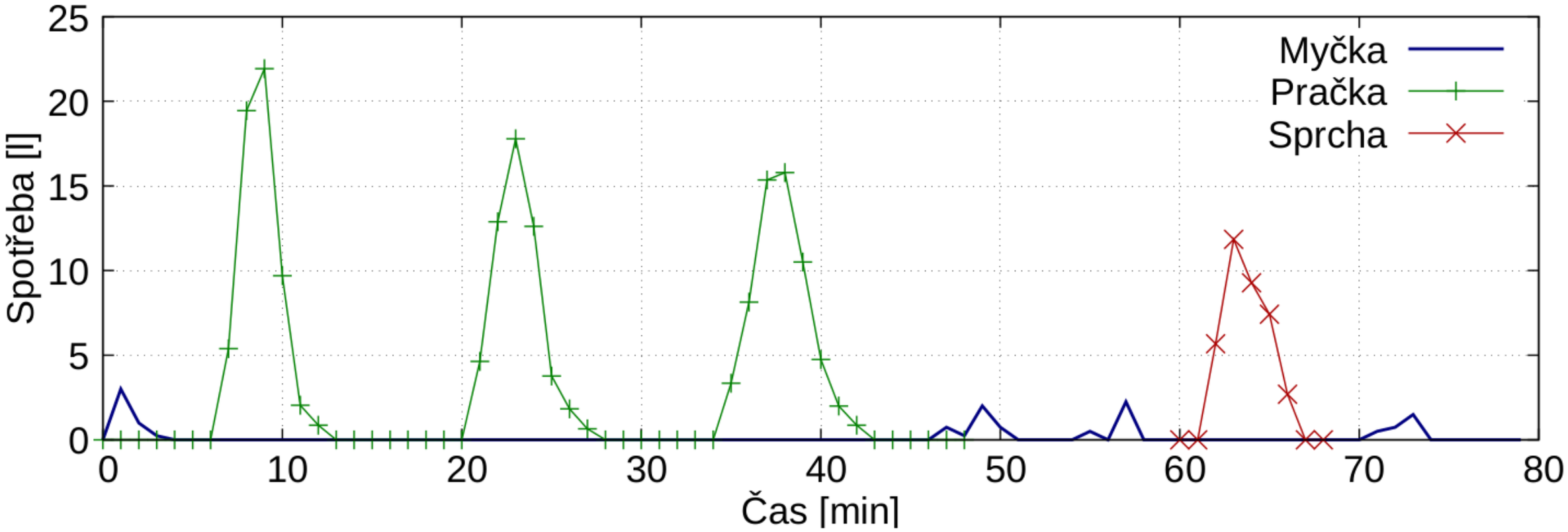
V tomto případě se měřiče zasílaly elektrickou spotřebu v 2s intervalech

Sledování dění v domácnosti



Feng Chen, Jing Dai, Bingsheng Wang, Sambit Sahu, Milind Naphade, and Chang-Tien Lu. 2011. Activity analysis based on low sample rate smart meters. In Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '11). ACM, New York, NY, USA, 240-248. DOI: https://doi.org/10.1145/2020408.2020450

Sledování dění v domácnosti



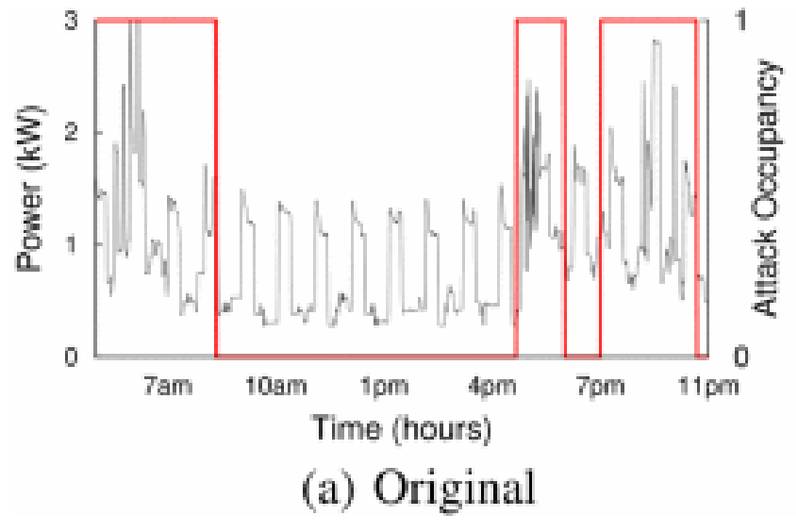
Spotřeba vody při využití pračky, myčky a sprchování s využitím dat výzkumu CSIRO.

Sources of critical contaminants in domestic wastewater: contaminant loads from household appliances. Technická zpráva, 2008, CSIRO: Water for a Healthy Country National Research Flagship.

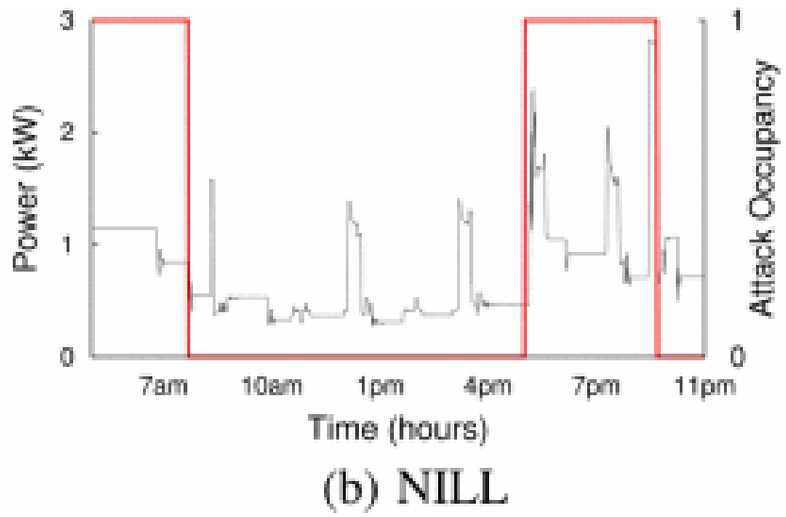
Výzkum v oblasti prevence úniku dat

- Využití baterií
  - M. Backes and S. Melser, "Differentially Private Smart Metering withBattery Recharging," IACR Cryptology, no. 183, April 2012.
  - G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda,"Privacy for Smart Meters: Towards Undetectable Appliance LoadSignatures," in SmartGridComm, October 2010.
  - S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting ConsumerPrivacy from Electric Load Monitoring," in CCS, October 2011.
  - W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel,"Minimizing Private Data Disclosures in the Smart Grid," in CCS,October 2012.
  - K. Armel, A. Gupta, G. Shrimali, and A. Albert, "Is Disaggregationthe Holy Grail of Energy Efficiency? the Case of Electricity," EnergyPolicy, vol. 52, no. 1, January 2013.
  - M. Zeifman and K. Roth, "Nonintrusive Appliance Load Monitoring:Review and Outlook," IEEE Transactions on Consumer Electronics,vol. 57, no. 1, February 2011.
- Využití ohřívač vody
  - Dong Chen, D. Irwin, P. Shenoy and J. Albrecht, "Combined heat and privacy: Preventing occupancy detection from smart meters," 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), Budapest, 2014, pp. 208-215.

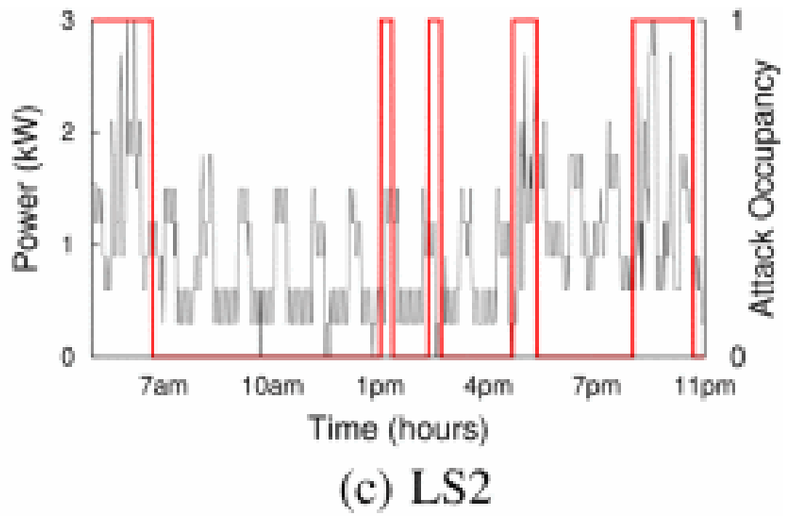
Výzkum v oblasti prevence úniku dat



(a) Original

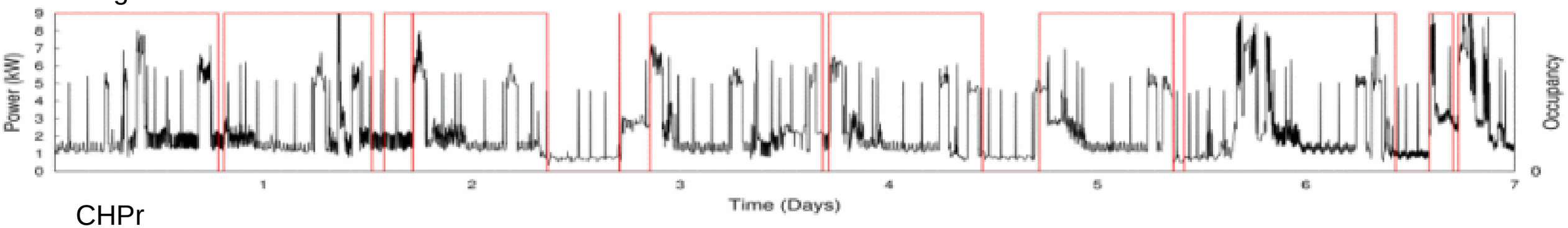


(b) NILL

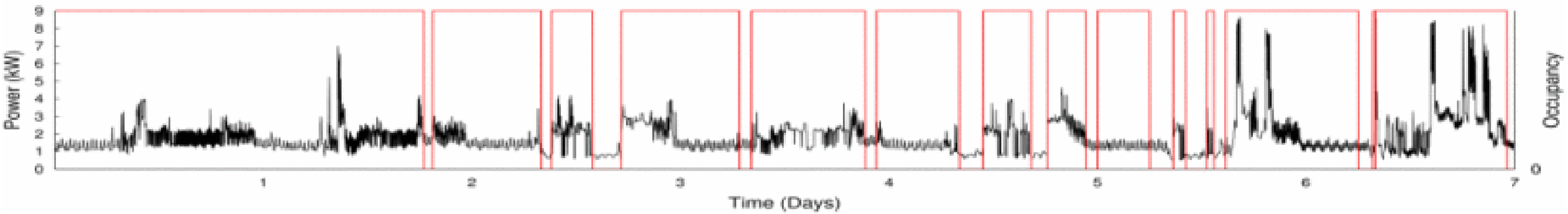


(c) LS2

Original:



CHPr



Výpočet účtu s ohledem na soukromí

- Alfredo Rial, Markulf Kohlweiss and George Danezis. M.: Privacy-preserving smart metering revisited. Int. J. Inf. Secur. (2018).
  - Alfredo Rial and George Danezis: Privacy-Preserving Smart Metering. ACM Workshop on Privacy in the Electronic Society (WPES 2011)
- Měřidlo podepisuje naměřené hodnoty a poskytuje je šifrované sdíleným klíčem s uživatelem
- Uživatel na svém zařízení dešifruje naměřené hodnoty
  - Na základě dodané cenové politiky spočítá účet
- Dodavatel může verifikovat, že dodaná cena je spočítaná správně
- Mechanismus podporuje rozšíření pro předvídání spotřeby, vyhledávání podvodů, profilování apod.

Legislativa – přísná při zpracování

- Obecné nařízení o ochraně dat (aka GDPR)
  - Article 29 Data Protection Working Party: Opinion 12/2011 on smart metering.
    - Article 29 Data Protection Working Party: Opinion 8/2014 on Recent Developments on the Internet of Things.
  - Úřad pro ochranu osobních údajů: Stanovisko č. 1/2014 - Chytré měření a ochrana osobních údajů. 2014
    - Čtení hodnoty je možné jen:
      - s explicitním souhlasem
      - po uzavření smlouvy vyžadující časté odečty
  - Šablona pro posouzení dopadů DPIA:
    - 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
- Doporučení a směrnice EU/komise zdůrazňují dopady na soukromí a požadují aplikaci obrany – šifrování apod.

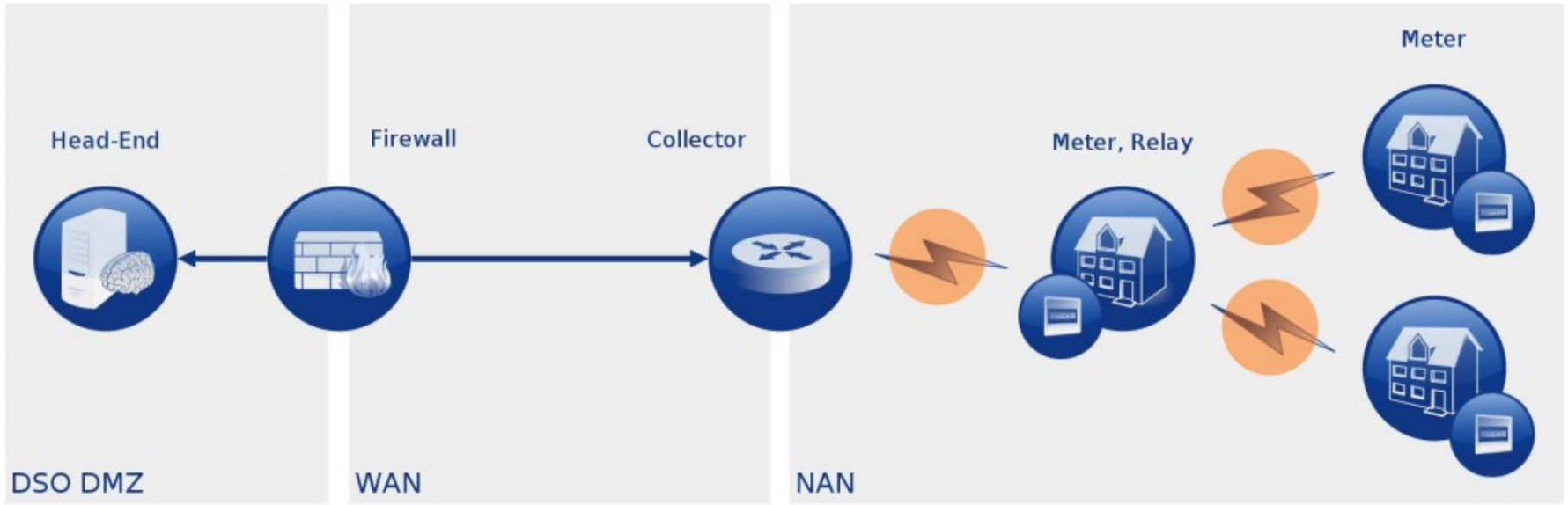
Wireless M-Bus
Dálkové odečty nabízené i v ČR

AMI s bezdrátovými prvky

Intro – Smart Metering

COMPASS SECURITY

Metering Infrastructure Blue Print



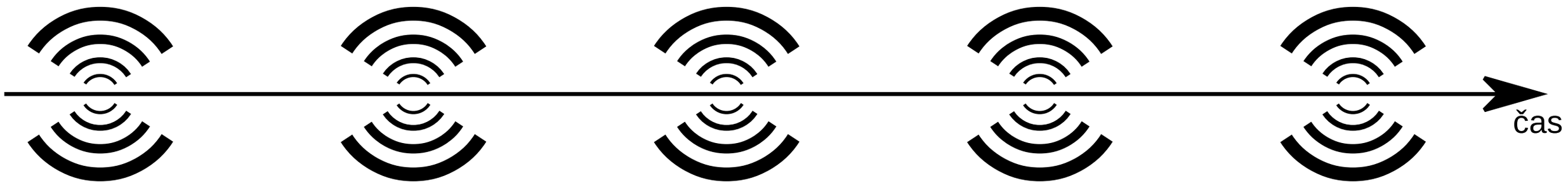
Legend

- DSO Distribution System Operator
- NAN Neighbourhood Area Network
- Wireless M-Bus

nesfit

Wireless M-Bus

- ČSN EN 13757
  - 4. část: bezdrátové sítě
- Minimalizace spotřeby energie a ceny zařízení
  - Často není měřidlo u zdroje el. energie (stoupací šachty, radiátor)
  - Komunikaci vždy začíná měřidlo
  - U dvousměrné varianty může protistrana vyžádat další informace (po omezenou dobu)



WM-Bus: maximální perioda zasílání

- Specifikuje ČSN EN 13757 podle varianty protokolu

Mód	Maximální perioda
T, C	15 min
S	120 min
R, N, F, H	24 h

- V praxi 80s, 120s, 300s apod.

Normy ČSN EN 13757

- Upozornění, že přenášená data mohou být považována za osobní data
  - Je nutné se vypořádat legislativou (EU/národní)
- Provedení bezpečnostní analýzy podle ISO/IEC 27033 a ISO/IEC 15408

Jak to chodí v praxi?

- Nabídka chytrých měřičů
  - *ochrana soukromí uživatelů – odečet bez vstupu do bytu*
  - Informace o využití Wireless M-Bus
    - Chybí informace o částých přenosech aktuálních hodnot
    - Chybí informace o zabezpečení
    - Na webu chybná informace o přenosech (po-pá 8 -18 hod.)
  - AMI: zabezpečení při přenosu přes Internet?
  - Chybí DPIA, bezpečnostní analýza
- Skutečný stav
  - Přenos po-pá ?-19 hod.: každých ~80s
  - Jindy: každých ~300s
  - Zabezpečení AES se sdíleným klíčem (data od měřidla)
    - Sílá klíče předmětem dalšího výzkumu

Využití a zneužití dat, útoky

Využití: kontrola dodržování zákonů

- V Ohio potvrzení pěstíren Konopí
  - Specifická spotřeba el. energie
- Detekce přítomnosti osob
  - El. energie, voda
  - Dodržování léčebného režimu při dočasné pracovní neschopnosti
- Ochrana autorských práv
  - Televize/monitor zobrazuje film, který je zatím pouze v kinech
- AMI s nešifrovaným přenosem přes Internet

Možná omezení

- Article 29 Data Protection Working Party: Opinion 03/2013 on purpose limitation
  - Example 20: Smart metering data used for tax purposes and to detect indoor cannabis factories
    - Such use may not be reasonably expected by the data subjects
    - Therefore, it could only be permissible, subject to the strict conditions set forth in ~~Article 13 of the Directive~~ → čl. 23 GDPR
- Právo Unie nebo členského státu může prostřednictvím legislativního opatření (autorizovat) s cílem zajistit … prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;
  - Otázka, jestli takové právo existuje

„Neočekávaná“ využití

- Sousedský stalking
- Příprava na vykradení
  - Hledání specifických křivek odběru → databáze zařízení → odhad finanční situace oběti
- Marketing
  - Detekce pokažených zařízení
  - Cílený prodej podle výskytu konkrétních zařízení

DOS a útoky na infrastrukturu

- Organizované/neorganizované útoky na infrastrukturu
  - Některá měřidla umí i vzdáleně odpojit odběrná místa
- NERC: Lessons Learned
  - Útok na energetickou infrastrukturu v USA z 5.3.2019

Problem Statement

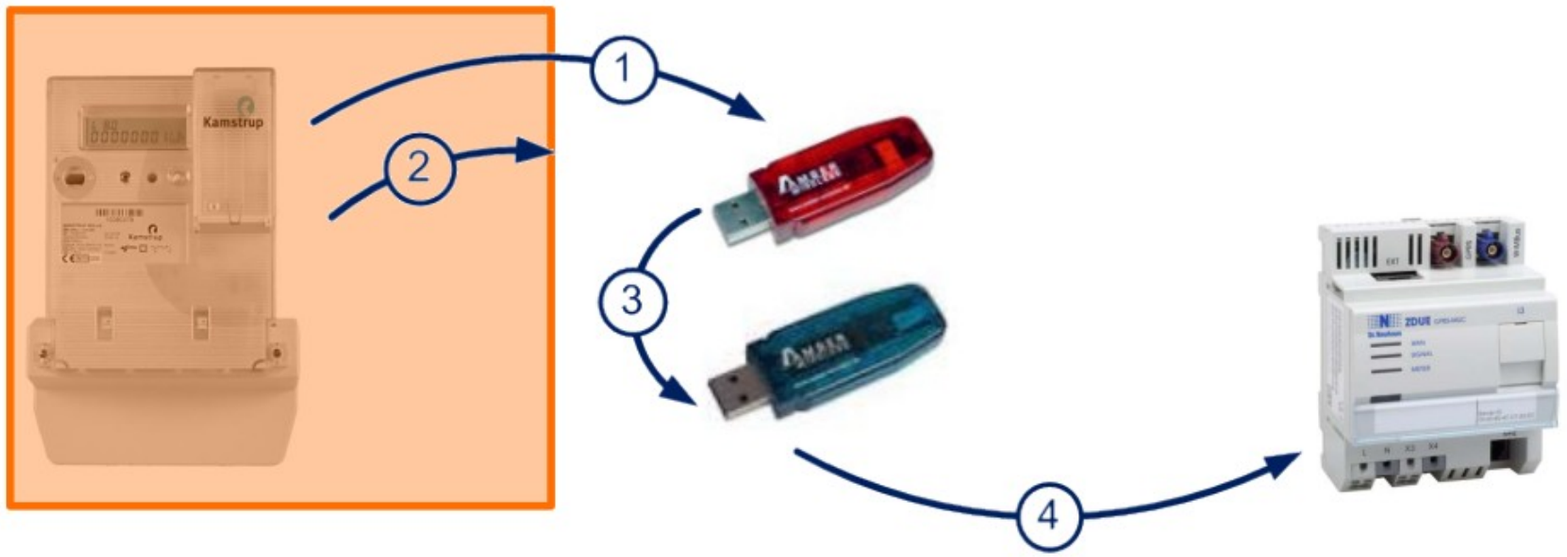
A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. This resulted in a denial of service (DoS)[1] condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center.

  - Zranitelnost firewallů dávno známá, opravená, veřejné exploity

Útoky na WMBus

Issues with Packet Replay

Shield and Replay I



- Capture messages from original device
- Shield device and replay messages

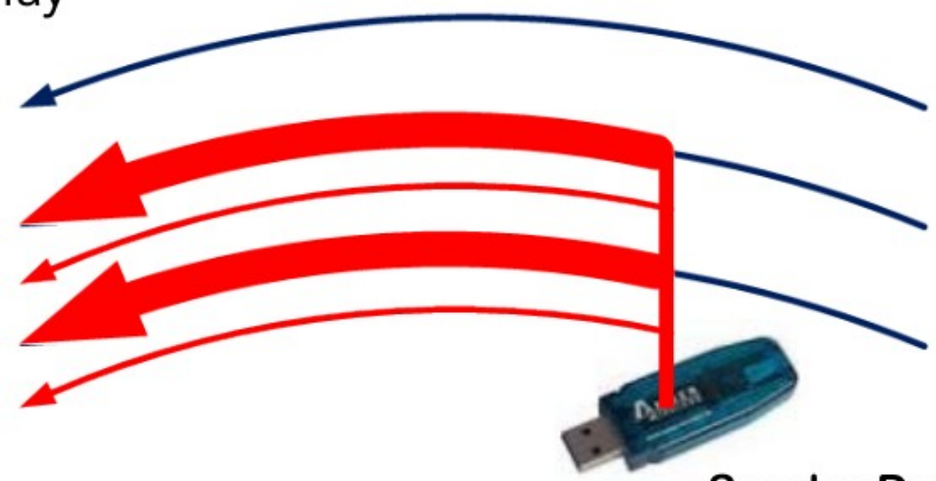
Útoky na WMBus

Issues with Packet Replay

COMPASS SECURITY

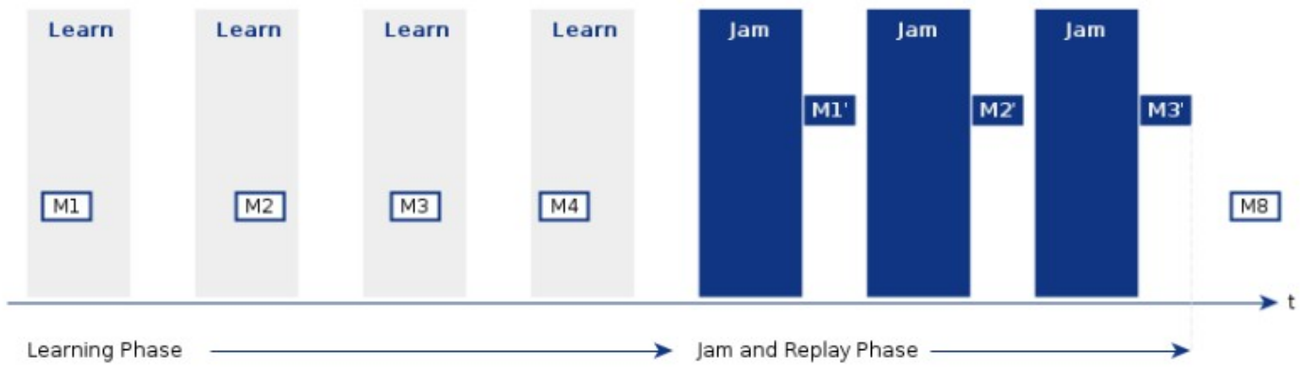
Jam and Replay

Collector



Sender Device

Meter



Děkuji za pozornost