AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Attack Vectors to Metering Data in Smart Grids under Security Constraints

The 1st IEEE International Workshop on Methods for Establishing Trust with Open Data
Izmir, Turkey | July 16, 2012

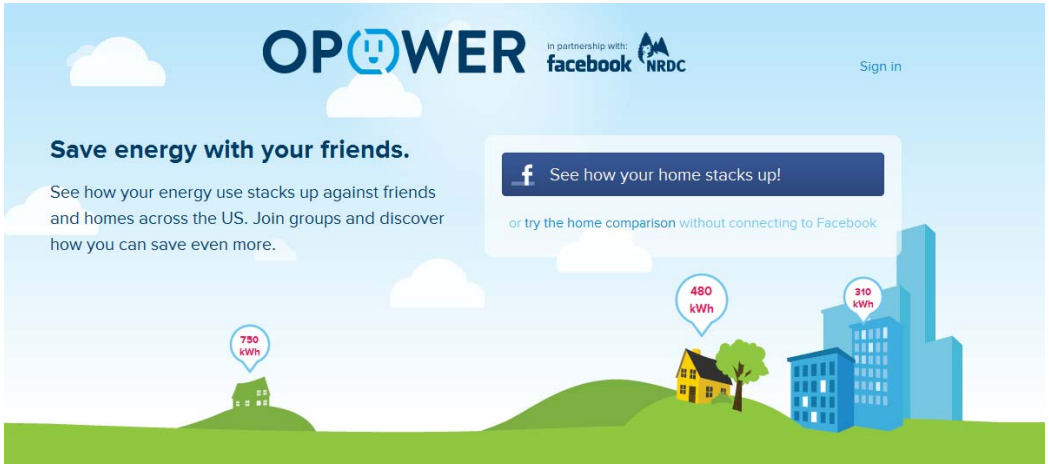
Florian Skopik and Zhendong Ma

Smart Grid

An electricity network that integrates the behavior and actions of all users connected to it - generators, consumers, or both – to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety [3].

[3] European Regulators Group for Electricity and Gas, *Position paper on Smart grids*, 2010

Smart Energy Community Portal



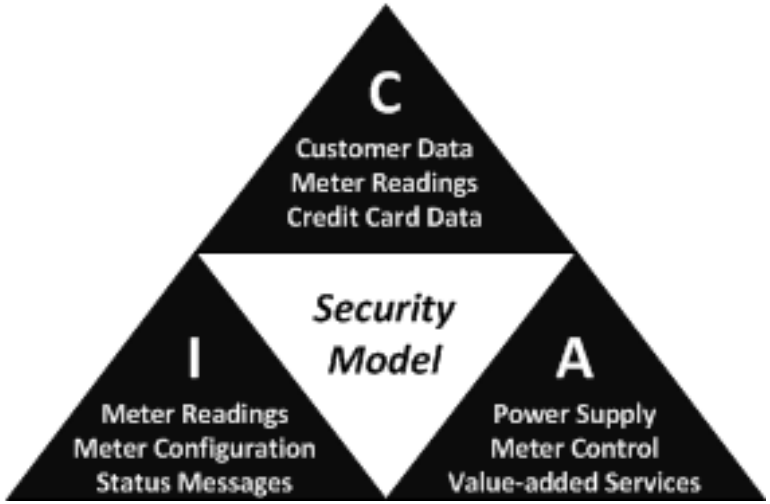
[source] www.opower.com

[source] smartenergygroups.com

Stakeholders

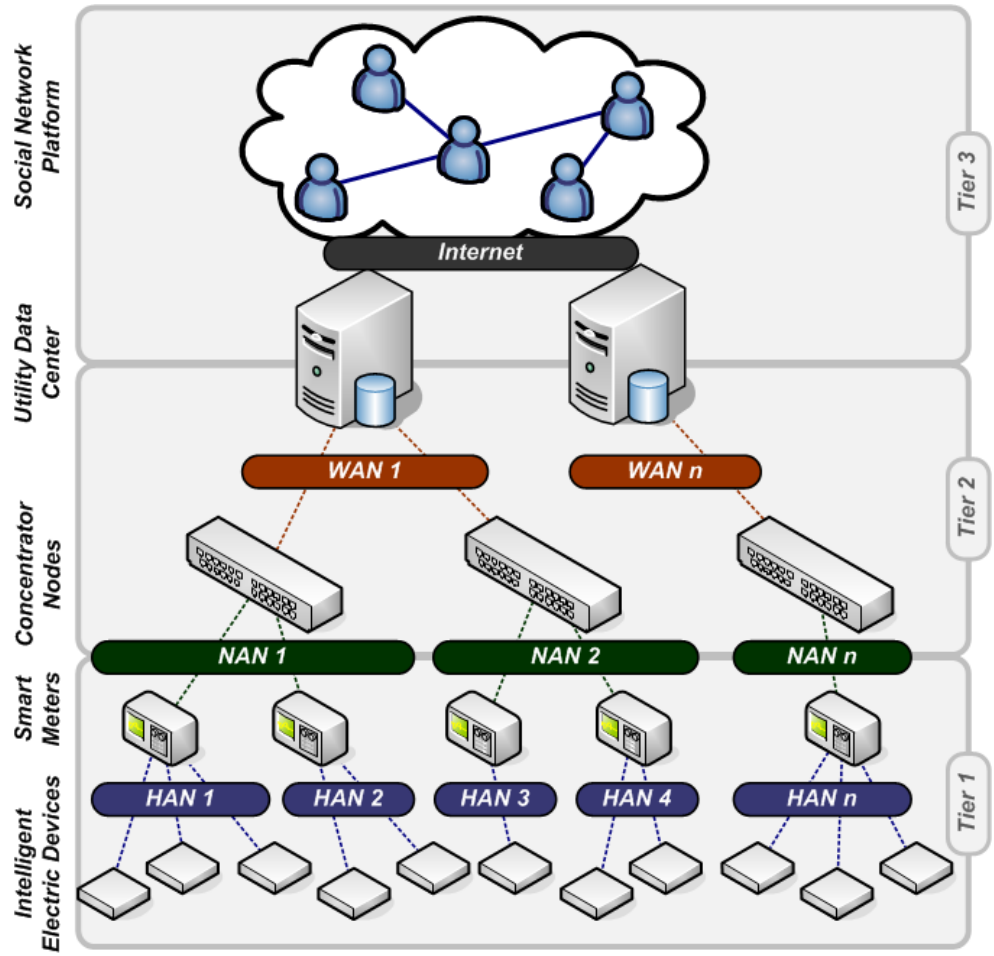
- **Energy Providers** use aggregated data to estimate midterm energy requirements of customers.
- **Grid Operators** real-time metering data to ensure the smooth operation of the network (e.g., detect and compensate local overloads).
- **Billing Companies** demand for accurate consumption data to implement envisioned flexible price models.
- **Third-party Services Provider** are used to generate consumption profiles and potentially compare them within so-called “energy saving communities”
- **Governmental Agencies** might demand access in preparation of lawsuits.

Security Principles and Protectoin Objectives

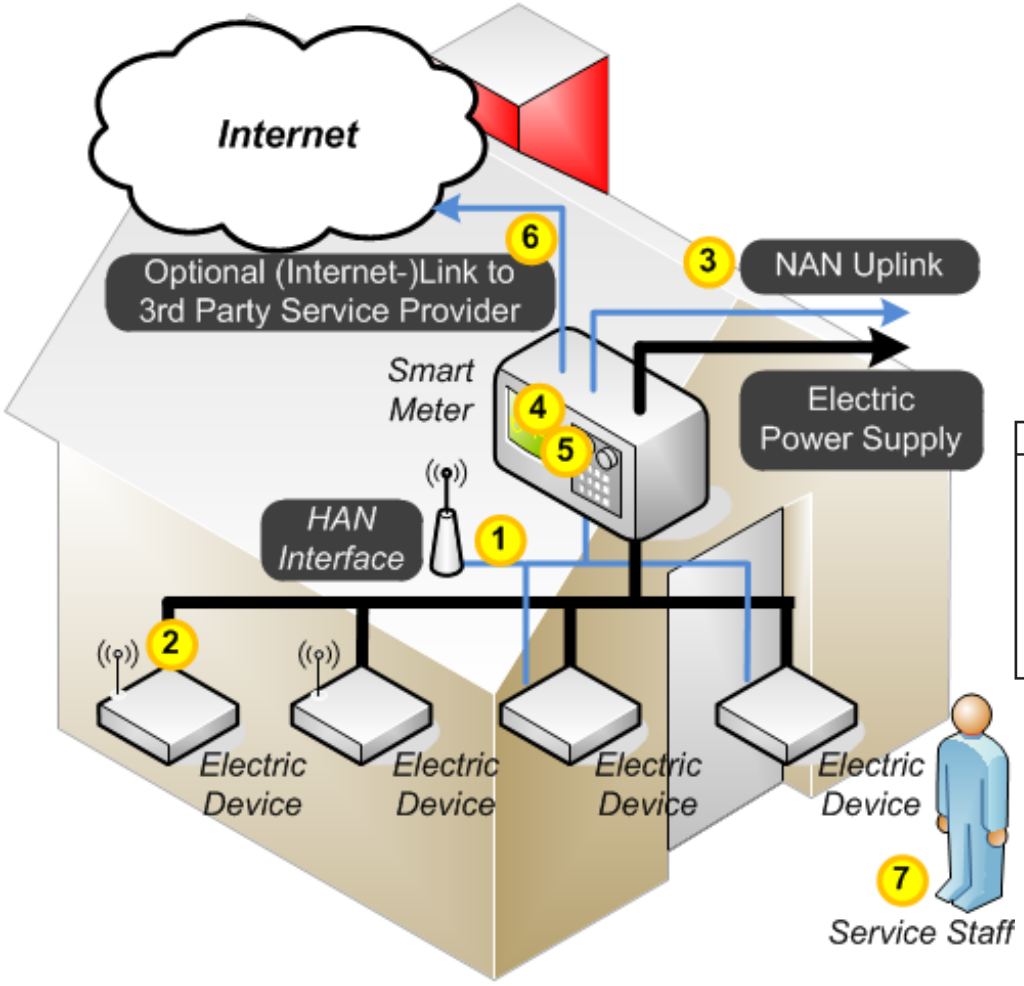


- Availability of the the Power Grid
- Legitimate Power Consumption and Delivery
- Privacy of Consumers

Smart Metering Infrastrucutre: a layered model

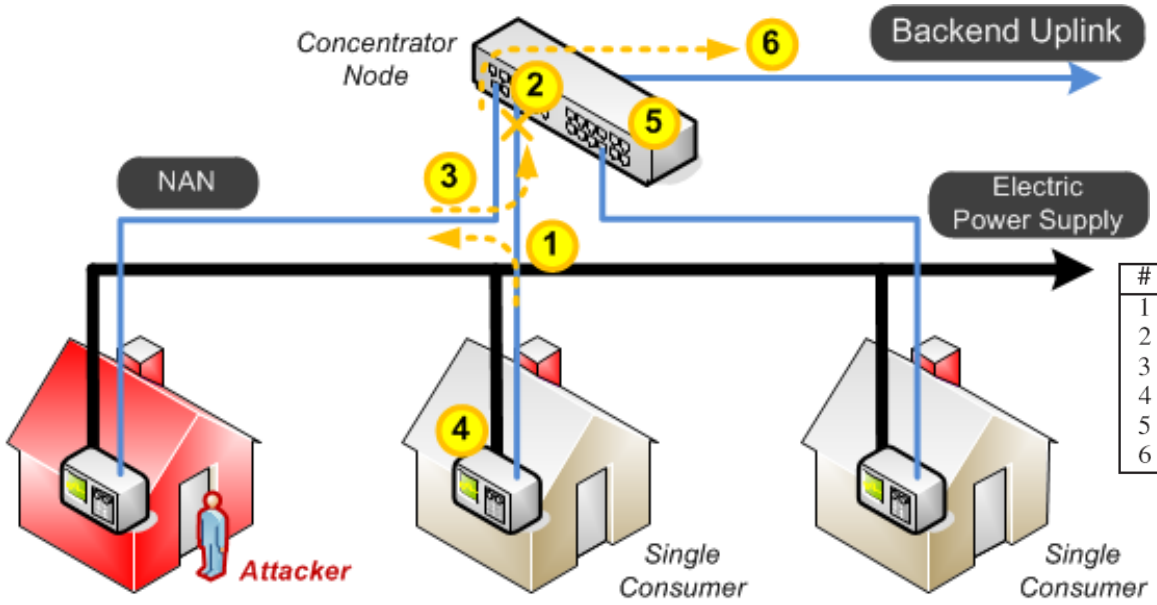


Tier 1 Threats: Smart Meter Attack Vector



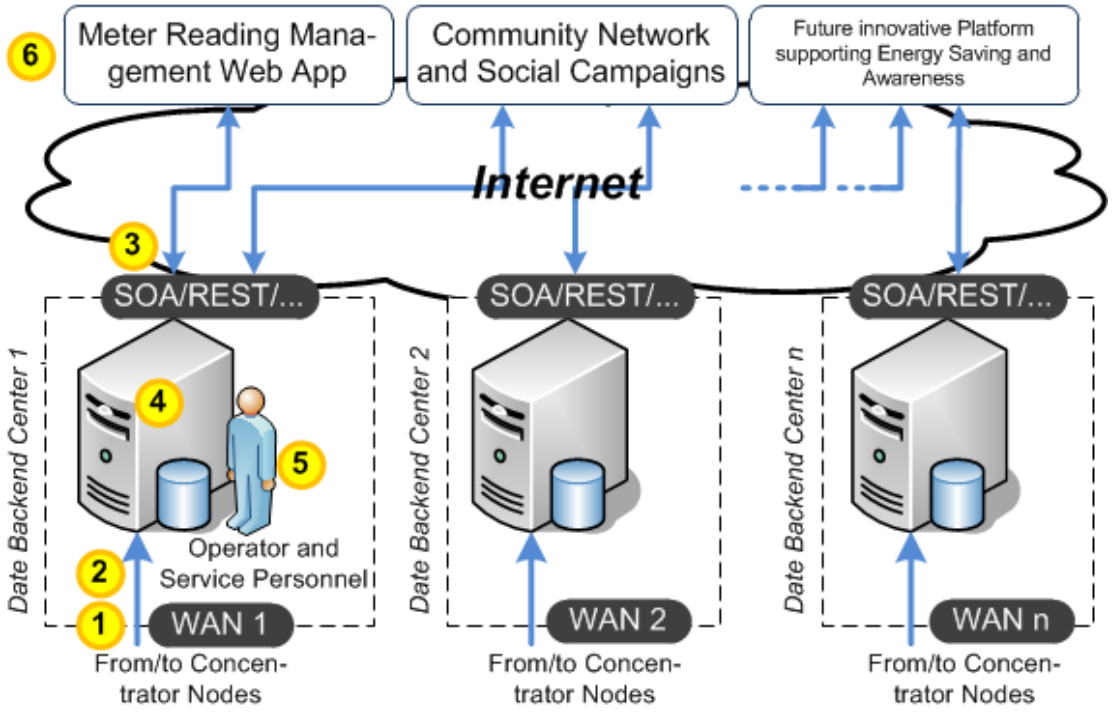
#	attack action	estim. effort	c	i	a
1	HAN sniffing	low – medium	x		
2	HAN message tampering	medium – high		x	x
3	sm. meter NAN shielding	low			x
4	sm. meter false reporting	high		x	
5	sm. meter swapping	low		x	
6	configuration manip.	medium	x		x
7	social engineering	n/a	x	(x)	x

Tier 2 Threats: Electric Utility Attack Vector



#	attack action	estim. effort	c	i	a
1	NAN sniffing	medium – high	x		
2	NAN comm. blocking	medium			x
3	NAN msg. tampering	high		x	x
4	neighbor meter DoS	high			x
5	concentr. node DoS	medium			x
6	utility data center intr.	very high	(x)	(x)	(x)

Tier 3 Threats: Web Services Attack Vector



#	attack action	estim. effort	c	i	a
1	WAN sniffing	n/a	x		
2	data backend DDoS (WAN)	n/a			x
3	data backend DDos (Internet)	n/a			x
4	data backend intrusion	n/a	x	x	x
5	data theft through social eng.	n/a	x		
6	attacks against Web Apps	low-medium	x	x	x

Security Recommendatoins

- Physical robustness and tamper resilience of smart meters and concentrator nodes in order to hinder numerous hardware hacks and attacks.
- Authentication of users and devices using strong passwords, digital certificates and signatures.
- Authorization of users and devices to grant them least privileges to access resources and services.
- Encryption of communication data and user data in the utility data center.
- Integrity and plausibility checks of data, such as meter readings, grid status messages, and network traffic.
- Training of technicians and service staff to prevent social engineering.