Smart Grid Privacy and Security

Yan Zhang

Professor, University of Oslo, Norway

Learning Objectives

Throughout this lecture, it is aimed for the students to be able to

- **Learn the basic concepts related to smart grid privacy and security**
- **Learn several typical privacy issues, consequence and solutions in smart grid**
- **Understand several typical attacks, consequence and solutions in smart grid**

Industry Invited Talk Today

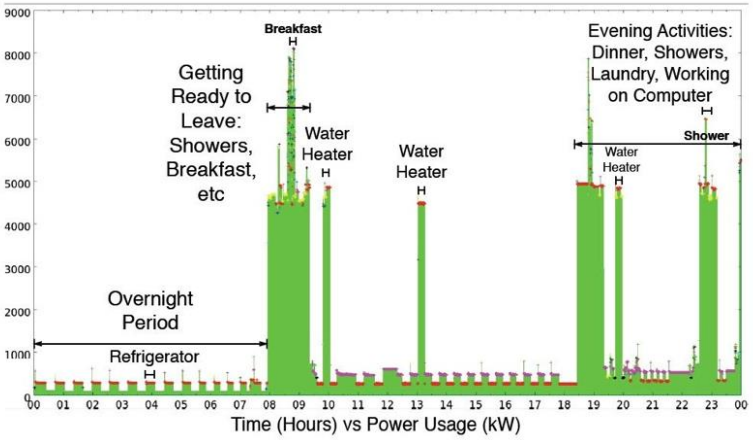
- **Speakers**: Jon Andreas Pretorius, *CIO, Hafslund Nett*

- **Title**: Smart Grid Cyber-Security: industry perspective

- **Hafslund**: Hafslund is the largest owner of power grids and the largest end-user seller of electricity in Norway.

Hafslund

Outline



Smart Grid Privacy

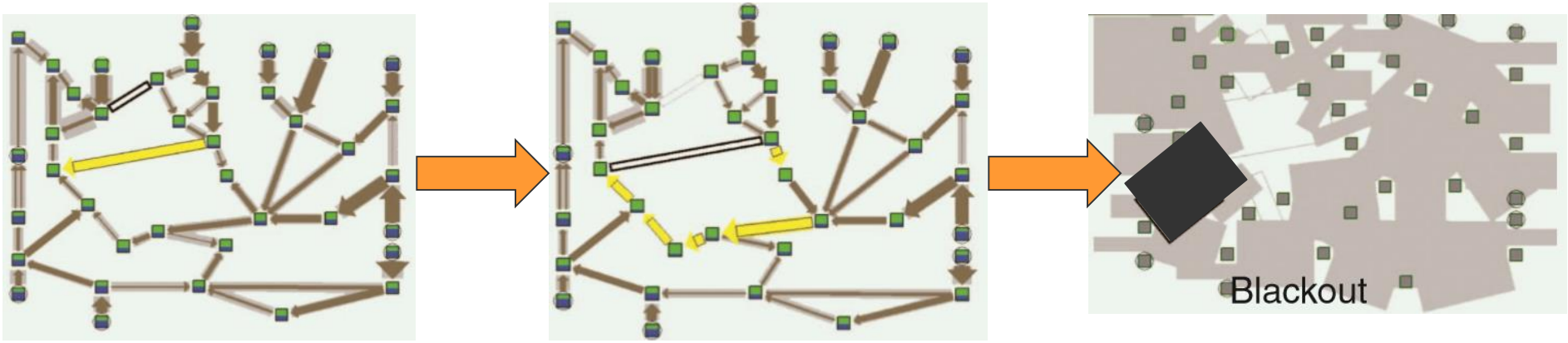
Smart Grid Security

SMART GRID CYBER-SECURITY: OVERVIEW

Security – two concepts

- **Physical Security**: this is the traditional "security" concept of power systems

  – cascading failure



Overloaded in yellow line

Load is spread to three lines nearby

Blackout in the area

- **Cyber Security**: technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access → **Our focus in this lecture**

Real-World Cyber Attacks in Smart Grid

- **Ukraine's power system:** Massive cyber attack occurred on Ukraine's power system in December 2015. More than ten thousand homes and facilities experienced a power outage for hours, even days. This attack was enabled by a malware called BlackEnergy installed on the control center computers.

- January 2003, computers infected by the Slammer worm shut down safety display systems at power plants in Ohio
- In 2008, there was evidence of computer intrusions into some European power utilities
- In 2010, Stuxnet worm provides an aggressive attack on control systems

In Norway

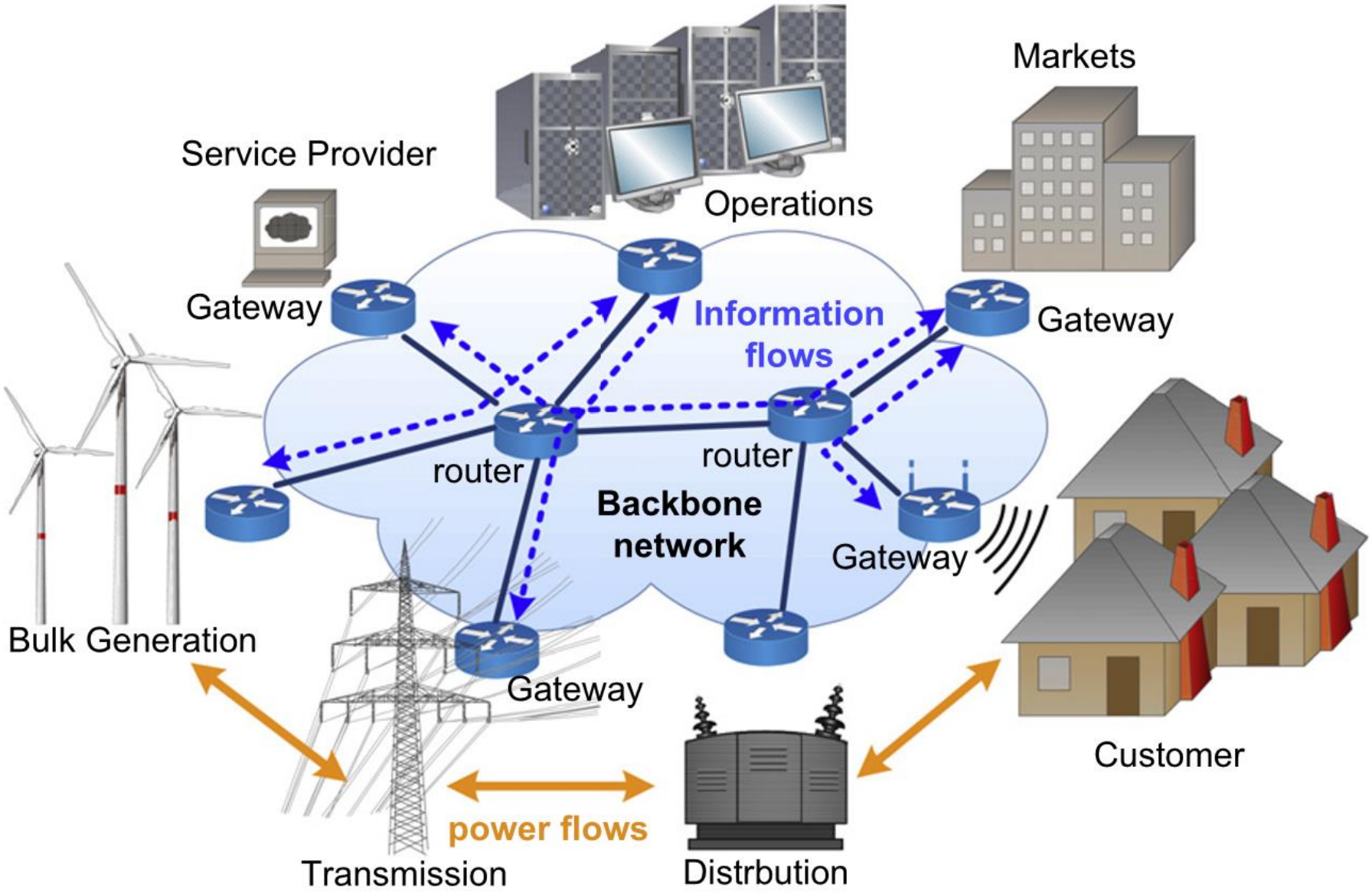
- **Norway has still not seen any serious cyber attacks that have taken out critical societal functions, as was witnessed in Ukraine during 2015**

- **But, “Around 80 per cent of all data traffic in Norway passes through Telenor. Every year, our security team deals with and averts thousands of cyber attacks and countless attempts at fraud, but it is impossible to stop them all,” says Hanne Tangen Nilsen (Telenor Norway’s Chief Security Officer)**

- **As an owner and operator of civic infrastructure, Telenor Norway has great responsibility. Hospitals, power companies and banks are highly dependent on Telenor infrastructure.**

telenor

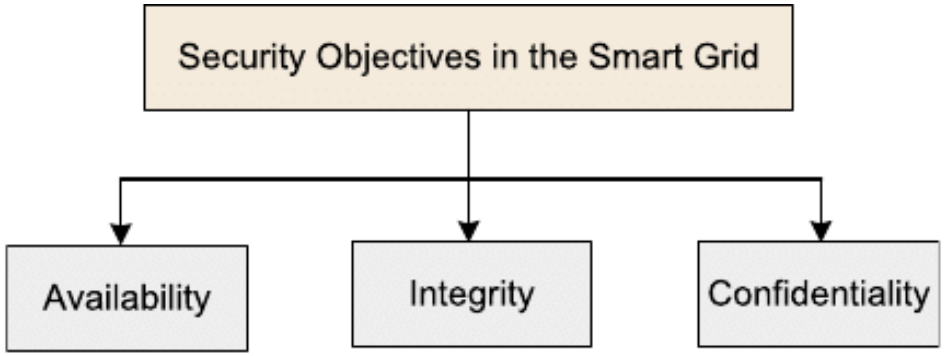
Information flow in smart grid in NIST reference model



Three Cyber Security Objectives in Smart Grid – NIST guideline

- **The cyber security working group in NIST released a comprehensive guideline for Smart Grid cyber security**
- **CIA (NOT Central Intelligence Agency): Confidentiality, Integrity, and Availability**

- Loss of ***availability***— disruption of access to or use of information or a system
- Loss of ***integrity*** — unauthorized modification of information
- Loss of ***confidentiality***—unauthorized disclosure of information



The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 (2010) 1–597.

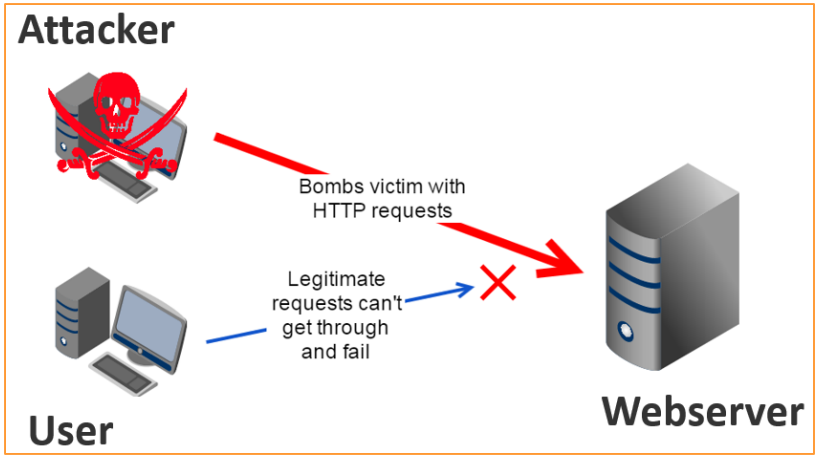
Availability

- **Availability: Ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid. This is because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.**

- **Availability of critical information is very important**
  - **Availability of price information: critical due to serious financial and possibly legal implications. Moreover, outdated price information can adversely affect power demand.**
  - **Availability of commands: important for turning a meter back on after completing the payment of an electric bill.**

Availability Attack – an example

- Denial-of-Service (DoS) is a typical attack targeting availability
- DoS attempts to stop or prevent a legitimate user from accessing service or a system. The attacker may flood a web server with so many requests that the server shuts down or simply cannot handle legitimate request.



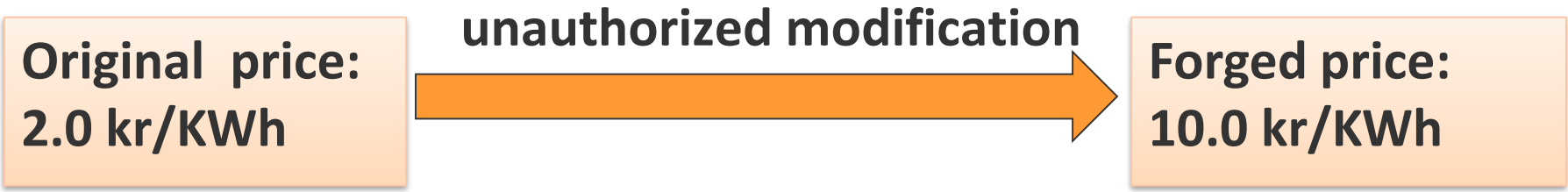
- **An Old DoS attack**: `ping -t 0.01 -l 500 129.240.171.52`

UiO IP address

- -t is the time (sec.) used to repeat the ping recursively
- –l is the packet size.
- Vary these digits in order to make your attack more efficient. The more the –l and less the –t, the higher will be the attack intensity.

Integrity

- Integrity refers to preventing undetected modification of information by unauthorized persons or systems.
- **Target:** either customer's information (e.g., pricing information) or network operation information (e.g., voltage readings, control commands). Such attacks attempt to deliberately modify the original information in order to corrupt critical data exchange in the smart grid.
- **Consequence:** A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management. Violation of integrity may cause safety issues, that is, equipment or people may be harmed.



- **Q:** any consequences after price changes?

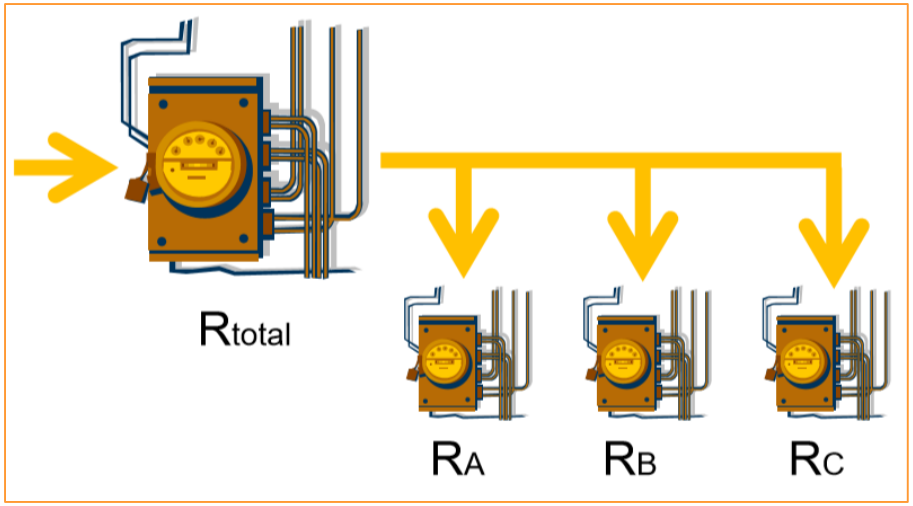
Integrity Attacks – an example

- **Electricity theft: meters are tampered and violators are not charged for the electricity actually used. Cyber Intelligence Section of the FBI reported that smart meters were hijacked in Puerto Rico, causing electricity theft amounting to annual losses for the utility estimated at $400 million**

- **Q: smart grid may become instable, why?**
- **An attacker may be possible to destabilize a real-time electricity market system by compromising smart meter consumption readings, causing suppliers to modify the electricity price accordingly.**

Cyber Intelligence Section: Smart grid electric meters altered to steal electricity (May 2010), http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

Integrity Attacks – an example - defense



- **Add a feeder meter for a group of houses**
- **Sum all house readings:** $R_A + R_B + R_C$
- **Compare with feeder meter** R_{total}
- **Readings should be about the same** $R_{total} = R_A + R_B + R_C$

Q: in what condition, we can say that there is electricity theft? Can we trace back the person who is stealing electricity?

$$R_{total} \gg R_A + R_B + R_C$$

Confidentiality

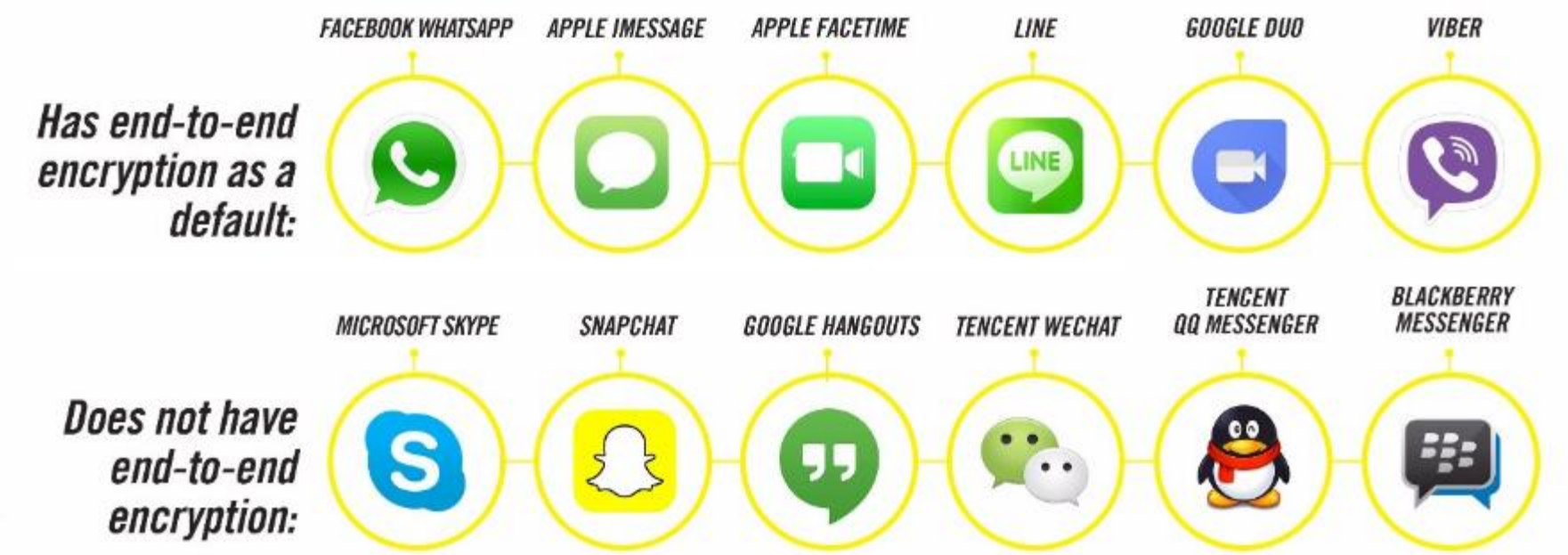
- **Confidentiality: set of rules that limit access or place restrictions on disclosure of some information, e.g., by means of encryption. Confidentiality ensures that access to information is restricted to authorized entities, e.g., bank account statements, personal information, credit card numbers, trade secrets, government documents.**

- **Encryption is a fundamental approach for information confidentiality. Encryption ensures that only the right people can read the information. A typical example is HTTPS (HTTP over SSL/TLS), a security protocol for communications over the Internet.**

- **Access control: another way to ensure information confidentiality to restrict access to sensitive information.**

Confidentiality – an example

- **End-to-end encryption: end-to-end encryption basically means that only a sender and the recipient of a particular message can see one another's messages. In essence, the messages cannot be decoded during transmission by outsiders or even the maker of the application.**



Source: Amnesty international, amnesty.org

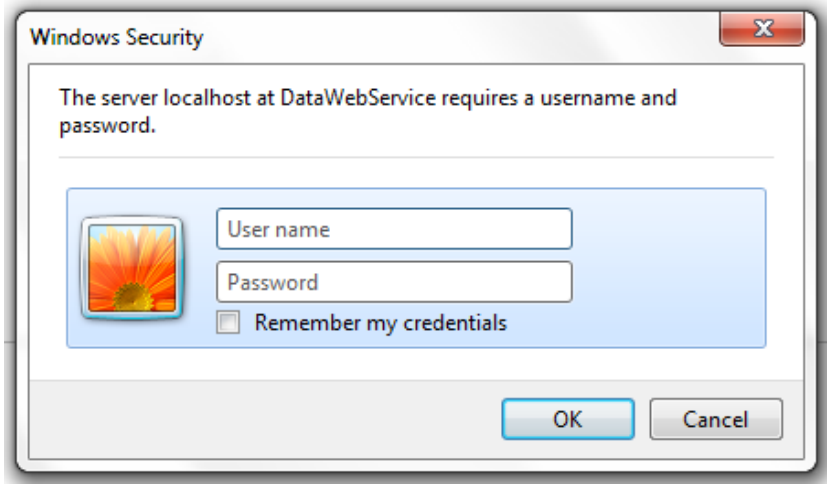
Many more requirements - Privacy

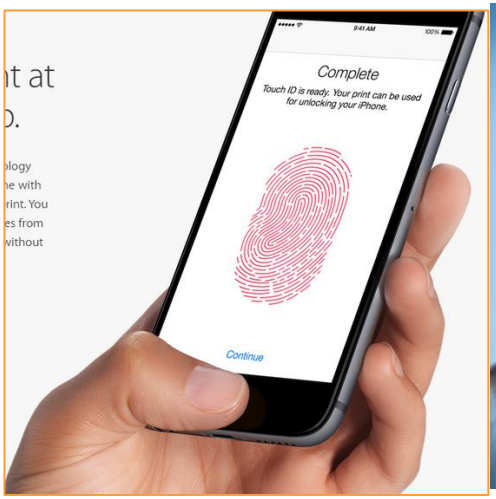
- Privacy (or information privacy, data protection): utilize the private data while protecting individual's privacy and their personally identifiable information.
- General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas .
- "Personal data is defined as any information and assessments that may be linked to a natural person" - The Norwegian Data Protection Authority

healthcare records, financial reports, education, tax reports, web-surfing behavior and many more

Authentication

- Authentication is concerned with determination of the true identity of a communication system participator and mapping of this identity to a system-internal principal (e.g., valid user account) by which this user is known to the system.
- Most security objectives, most notably authorization, distinguish between legitimate and illegitimate users based on authentication.
- Authentication approaches: username-password; biometric authentication (e.g., fingerprint, face)





Mutual Authentication

- Mutual authentication: network authenticates mobile phones; and at the same time mobile phones will authenticate networks
- Mutual authentication provides enhanced protection against false base station attacks by allowing the mobile phone to authenticate the networks

13.12.2014 - Oslo

Aftenposten Discovers Spying Equipments outside Norway Parliament and Prime Minister Residence

Aftenposten reports they have detected a number of false base stations placed around central Oslo, which can monitor the movements of top politicians and flood of data from mobile phones.

- **Q:** are we using mutual authentication in 4G?
- **Q:** shall we perform mutual authentication when an Electric Vehicle is charging battery?

SMART GRID PRIVACY

Privacy is very related to smart metering

Meter
(Electricity, time)
(Gas, time)

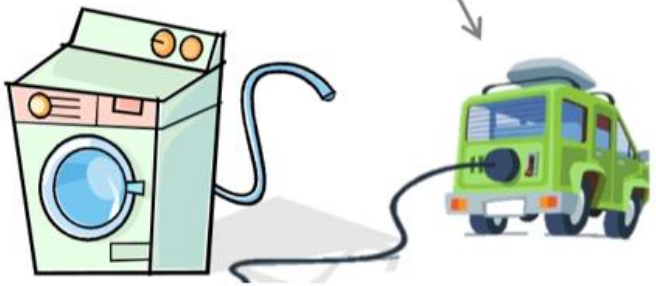
Electricity readings per ½ hour

Display

Bill

Payment

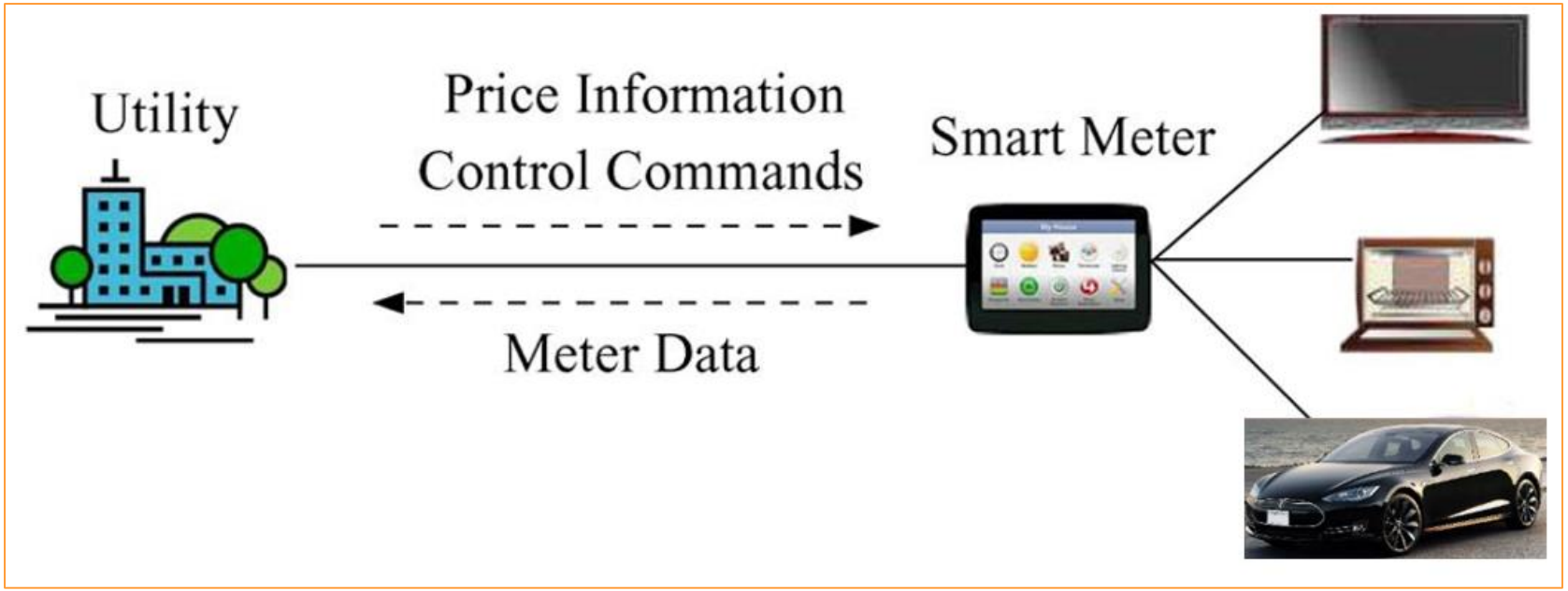
Utility
Provider



User

Policy
Dynamic rates per ½ hour
Fixed plan of rates
(Non-linear rates -- taxation)

Important information exchange through smart meters



- Information flows to/from a smart meter including
  - price information
  - control commands
  - meter data (e.g., electricity consumption)

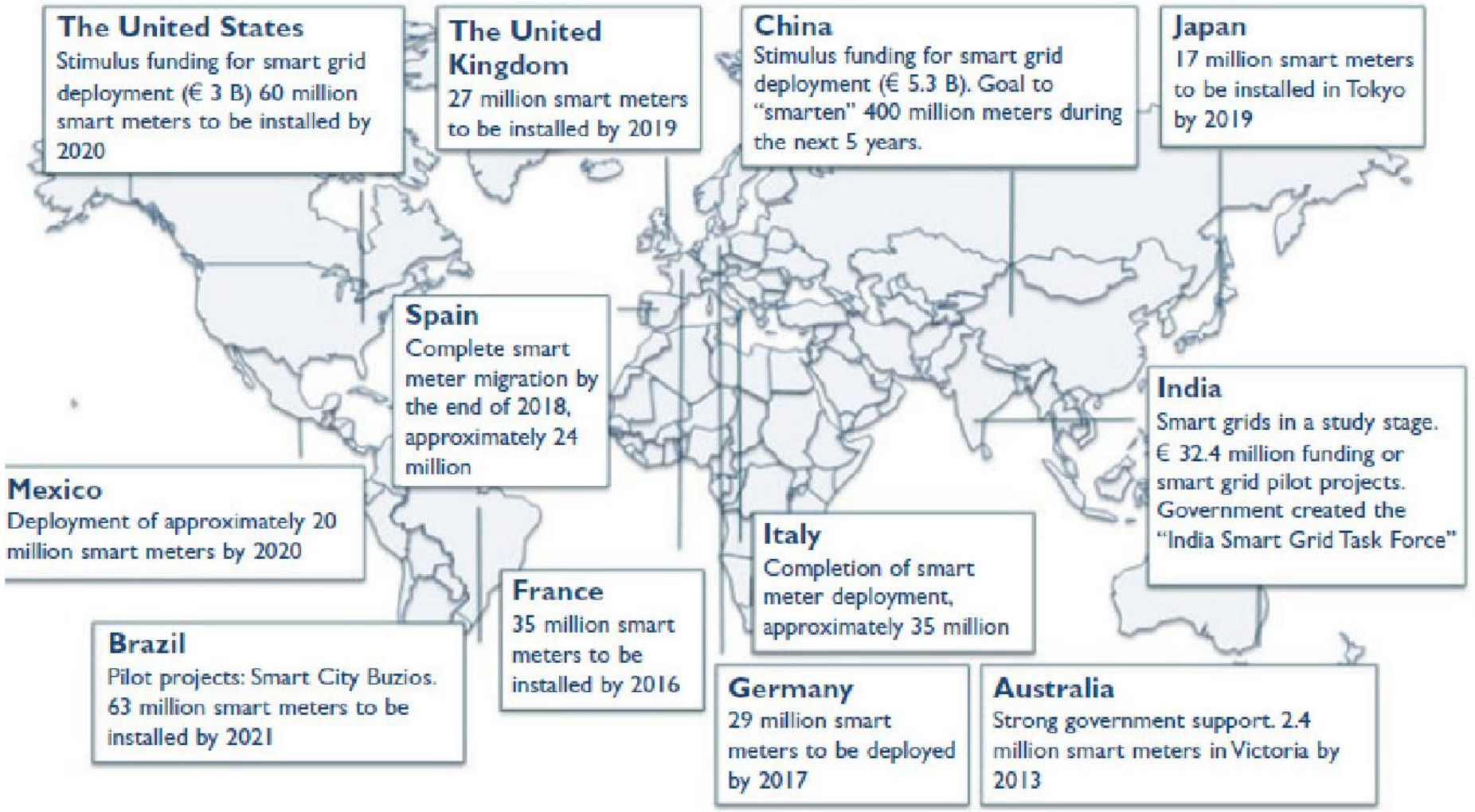
Smart Meters Deployment Plan in Europe

- **Norway: decided that all customers in Norway will receive new smart meters by 1 January 2019.**
- **European Union: The European Parliament proposed that 80% of electricity customers have smart meters by 2020.**
- **England: The Government has announced plans to install a smart meter in every home in England by 2020.**

However

- **Netherlands: April 2009, First Chamber declined a bill which would require the installation of smart meters in residences. Chamber cited privacy issues as the main concern measure**
- **Germany: decided against a nation-wide deployment of smart meters due to privacy and cost issues in 2016**

Smart Meters Project around the World



Source: Frost & Sullivan analysis

Privacy Concerns – different applications

- At your home
  - Appliances and devices may communicate with one another to use electricity more efficiently.
  - Consumers or others may remotely control temperature and other appliances.
- Remote Connection / Disconnection of Meter
- Demand Response and Pricing
  - Customers will respond to real-time pricing signals.
- Marketing Use of Data
- 3rd Party Application Developers
  - Device-makers may seek access to data to provide in-home tools for better monitoring of electricity use.

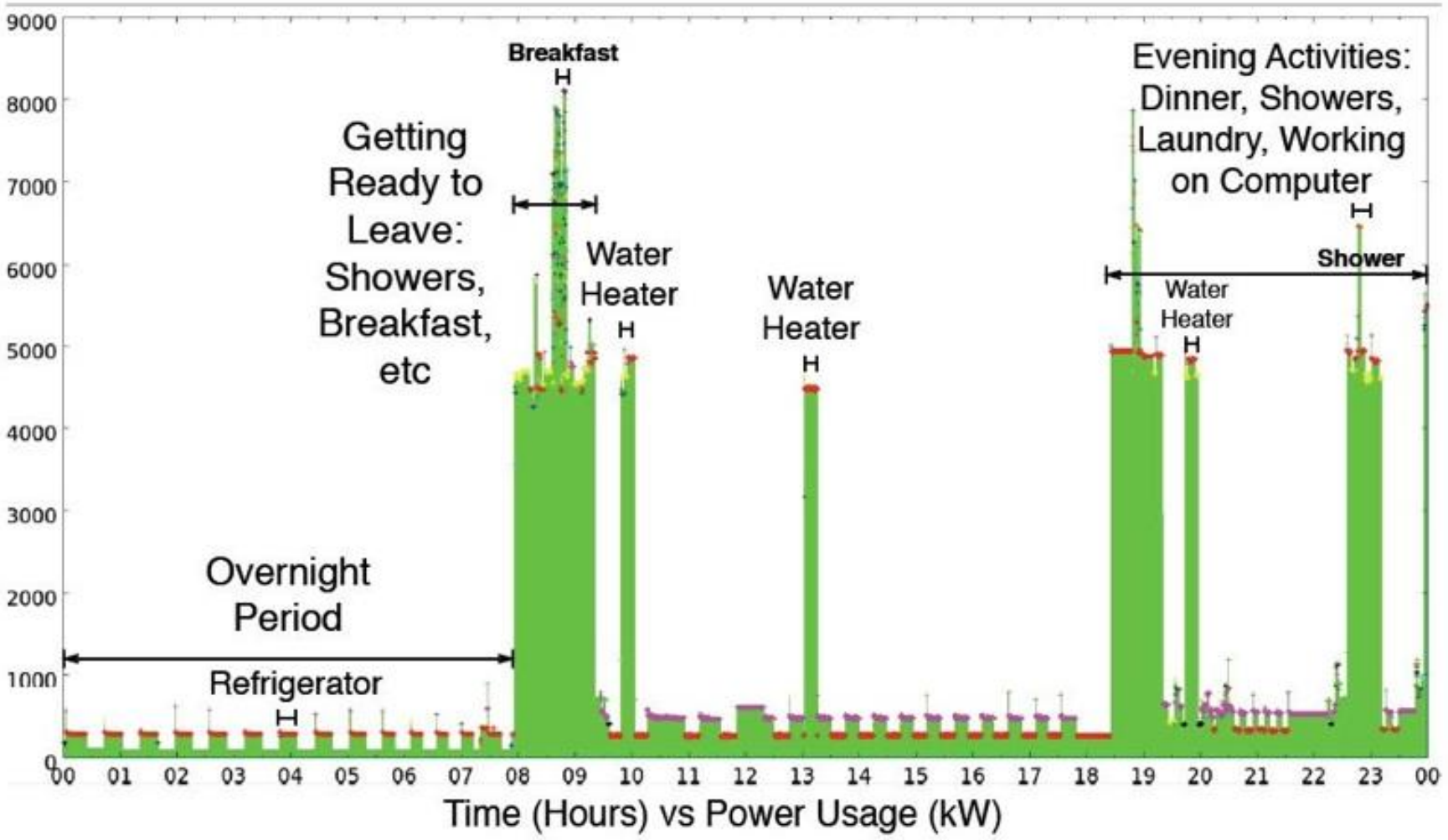
Privacy Concerns at End-users

- **Smart Meters: Information regarding energy use will be collected from the home and may be able to relay information about specific types of appliances being used at specific moments in time.**

- **Fine-grained meter reading: one essential technology of smart grids is fine-grained meter reading within a very short period (15min or fewer) per household. However, meter readings of a household reveal detailed information about daily activities of the household and used appliances during a specific time period. The smart metering data is normally saved in centralized data center. Fine-grained meter readings may cause serious privacy issues.**

- **Load signatures: could potentially indicate when you are home and whether you are cooking, watching television, or using other electronic devices.**

Load Signature



Molina-Markham A, Shenoy P, Fu K, Cecchet E, Irwin D. "Private memoirs of a smart meter", BuildSys 2010.

- **Smart meter data may be used to determine device usage in the home.**

What Could Power Usage Information Reveal?

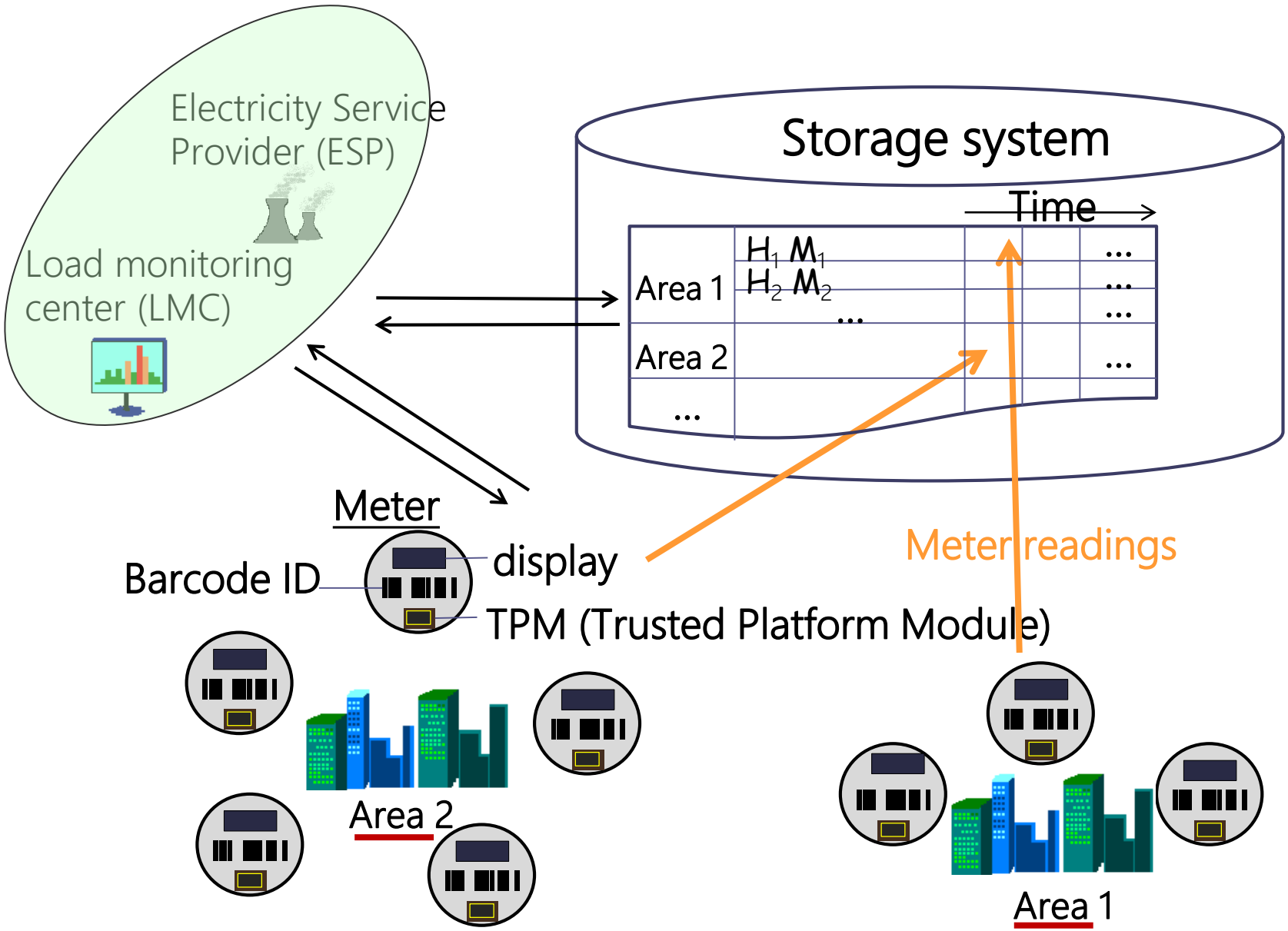
Applications/Services, Questions?		Energy usage pattern
Health services Insurance services Typical question: Did you get a good night's sleep?		Yes: No power events overnight for at least 6 hours No: Random power events overnight
Safety services Typical question: Are you on vacation?		Yes: No power events for some days No: random power events in a day
House renting Typical question: How many people live there? When did you have a party?		High power usage one day Your landlord have great interest to know: You have contract to have one person in the apartment, but in fact two persons in the apartment

Potential Risks

Who wants smart meter data?	How could the data be used?
Utilities	To monitor electricity usage and load; to determine bills
Advisory companies	To promote energy conservation and awareness
Insurance companies	To determine premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify best times for a burglary, or valuable appliances to steal

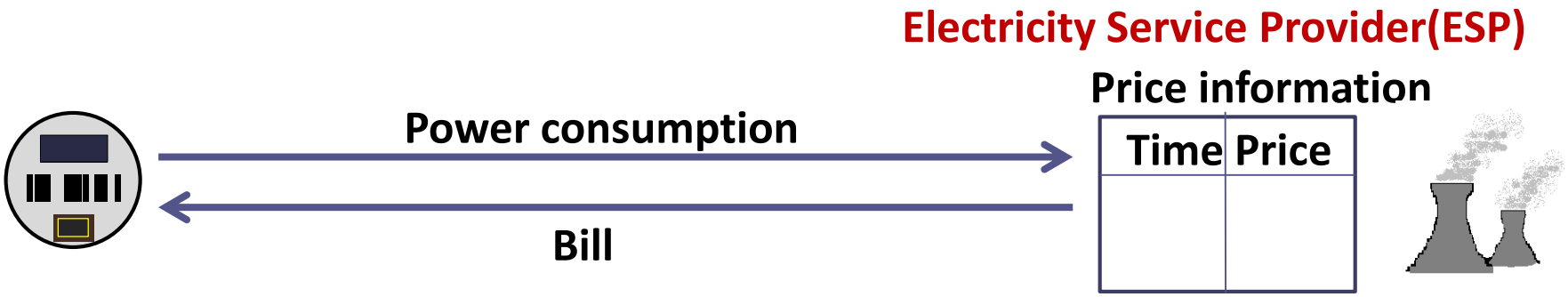
- **Q: do we always need minute-scale energy monitoring?**

Bill Application and Load Monitoring Application



TPM (Trusted Platform Module): holds key information to ensure data integrity

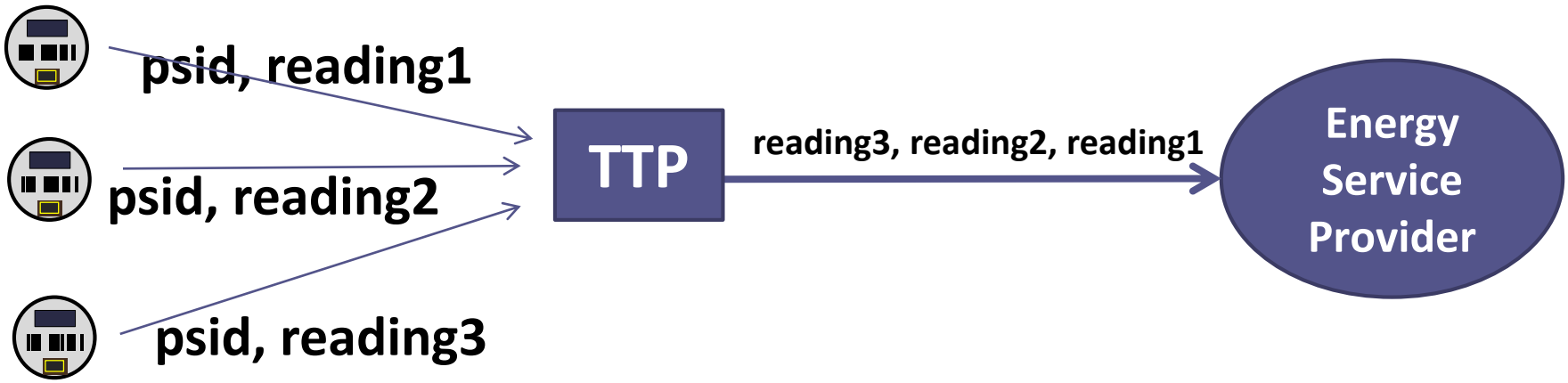
Automatic Bill – we do not need minute granularity of meter readings



- Automatic Bill: In billing applications, the electricity service provider only needs the amount of power consumption per hour to compute a bill.

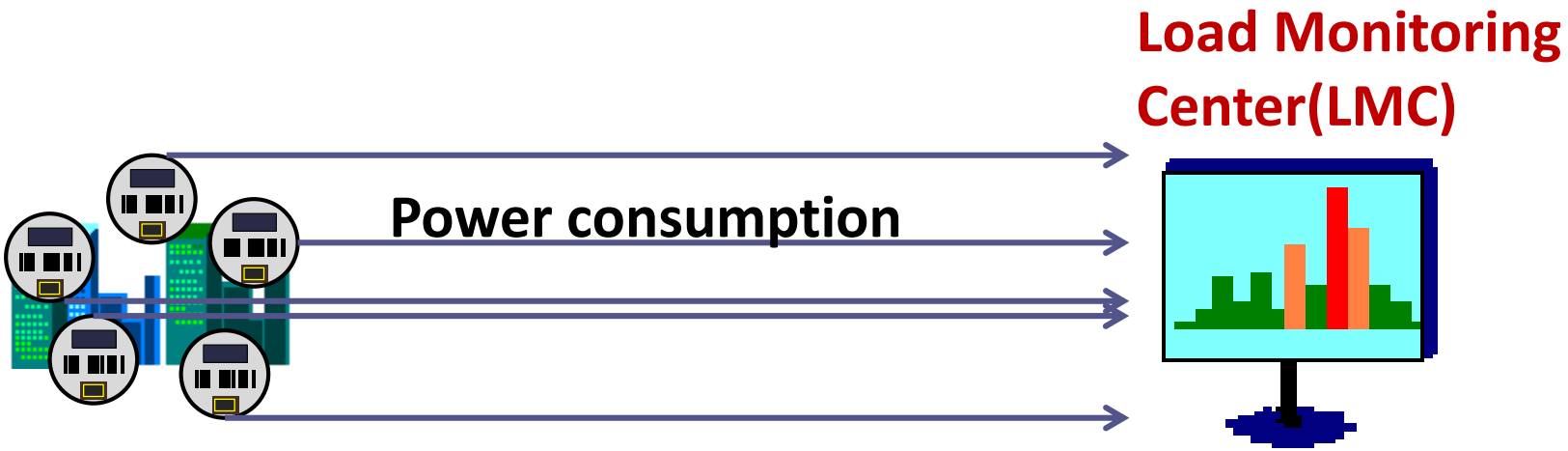
Privacy-preserving Automatic Bill

- Trusted third party (TTP) computes the bill, e.g., module in a grid operator
- Anonymization – Instead of a user's real ID, a pseudonym (a fake ID, denoted by psid in the illustration below) is attached to the data. Thus, the receiver do not know to which individual the received data belong. Daily (or hourly) power consumption remains anonymous, user identity is only used at the end of each billing period when presenting all consumed credentials together.
- **Q:** any disadvantages of this scheme?



- May have large volume of data; Complex accounting service

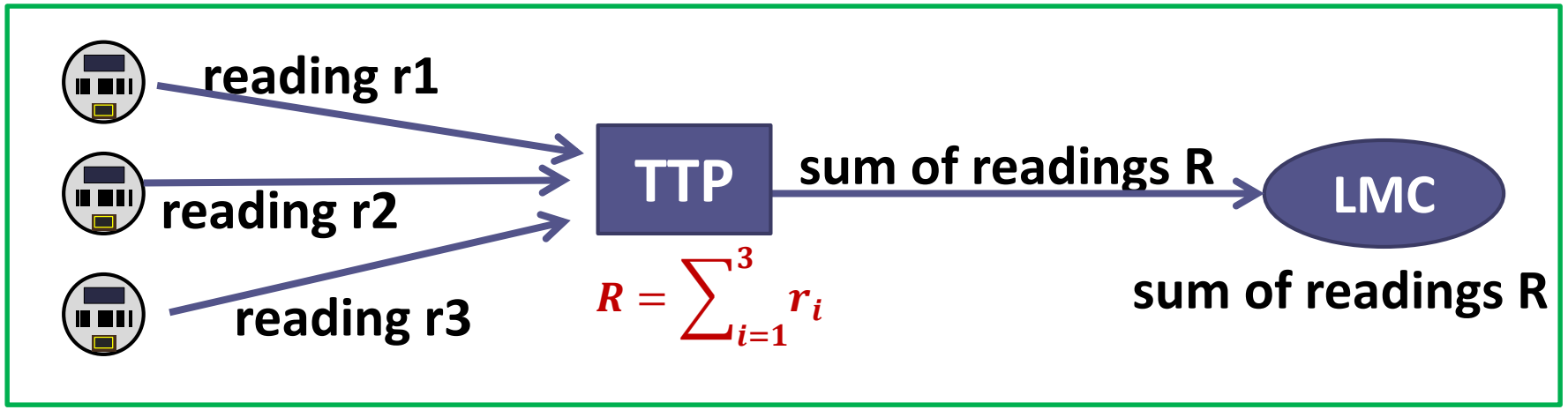
Load Monitoring - we do not need minute granularity of meter readings



- Load Monitoring: the load monitoring center (LMC) collects the amount of electricity usage over a local area in order to monitor current activities of the power grid.
- LMC only needs the total power consumption over the area at recent time units.

Privacy-preserving Load Monitoring

- Aggregation: The data from individual users are aggregated and only the aggregated data are sent to the receiver.
- Privacy-friendly aggregation: the aim is for a utility to reveal the sum of readings from multiple meters without learning the readings themselves.
- **Q:** any disadvantages of using this scheme?



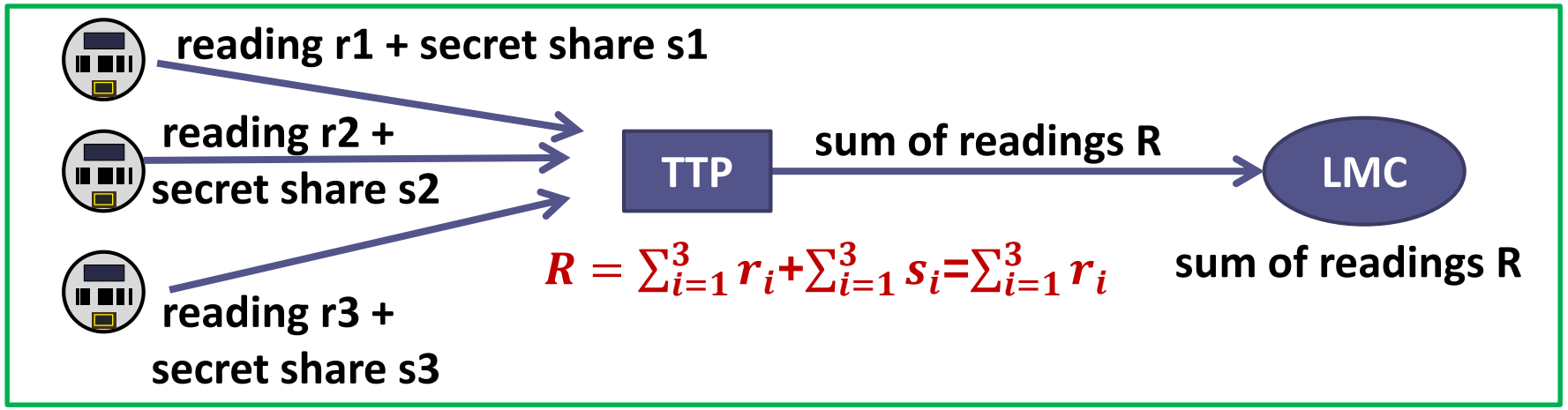
- May not be scalable when there are too many users in an area
- Need a Trusted Third Party (TTP) to aggregate data

Privacy-preserving Load Monitoring – secret shares

- Each reading is added by secret share which is a random number. The sum of all secret shares (s1, s2, s3) is zero (i.e. s1+s2+s3 = 0), e.g., s1=0.1, s2=0.4, s3=-0.5.

- When the readings are summed, shares cancel out and the output of LMC is the sum of metering readings

- **Q:** any disadvantages of using this scheme?



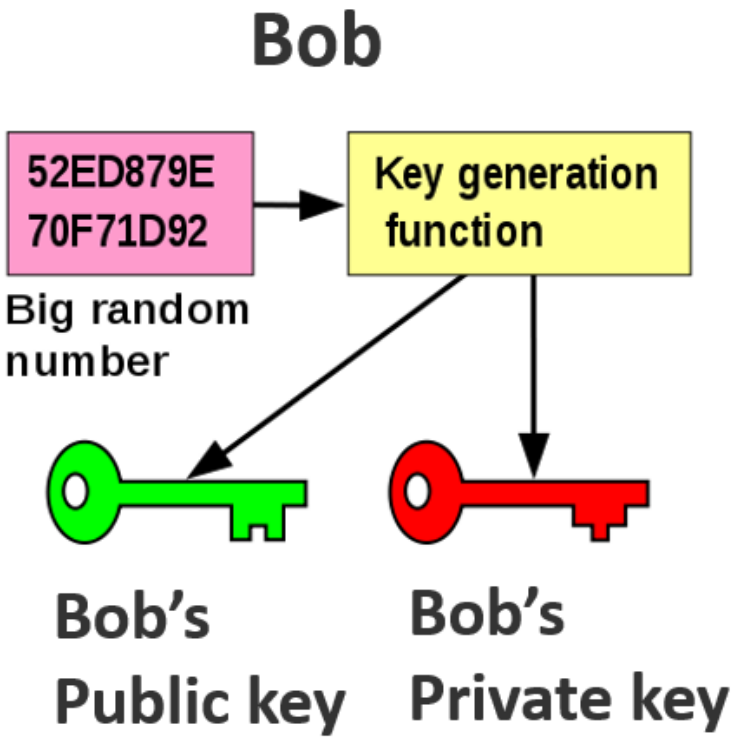
- These protocols are very efficient but suffer from inflexibility: the groups of meters that can be aggregated are static, and missing readings prevent the computation of the aggregate. Need a trusted third party (TTP) to aggregate data **(Q: what if TTP is not trusted?)**

Untrusted TTP: We Need Public Key and Private Key

- Bob has two keys: public key and private key (basically long random numbers). An example of a Public Key:

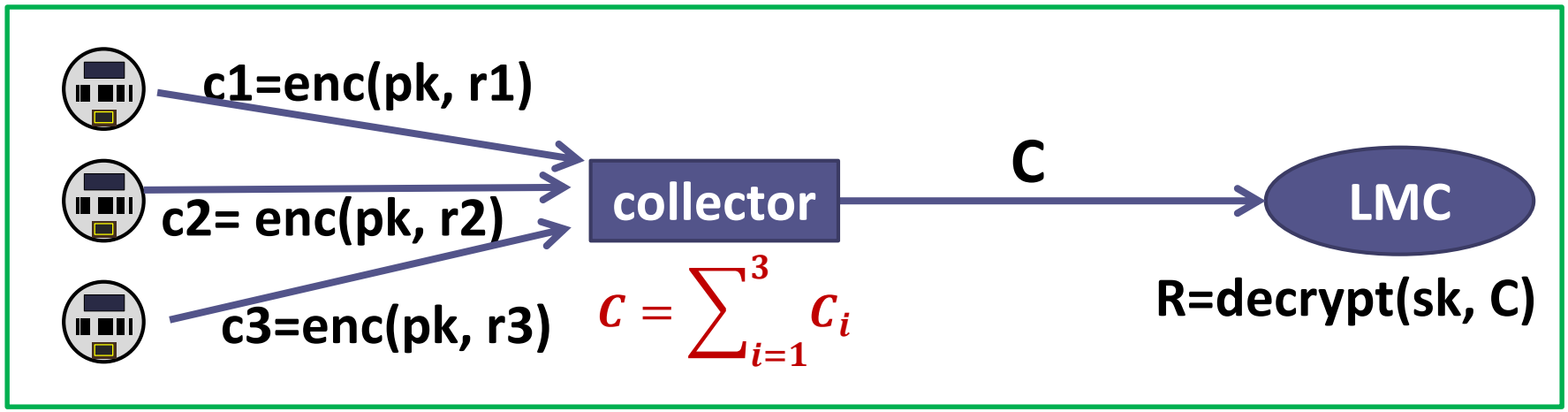
```
3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069
EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F
BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673
CA2B 4003 C266 E2CD CB02 0301 0001
```

- Public Key: available to everyone via a publicly accessible directory
- Private Key: confidential to its owner, i.e., Bob
- The key pair is mathematically related, a message encrypted with a Bob's public key cannot be decrypted by anyone, except Bob possessing with his private key.



Aggregation with collector which may not be trusted

- Load monitor center (LMC) has two keys: public key and private key. Each smart meter encrypts (enc(.) in the illustration) its data with the public key (pk in the illustration) and sends the ciphertext to the collector.
- The collector aggregates the received ciphertexts and sends the aggregated ciphertext to load monitor center.
- The load monitor center decrypts the aggregated ciphertext with its private key (sk in the illustration) to obtain the aggregated data of all smart meter readings.



SMART GRID SECURITY

We focus on three attacks

- Replay Attack
- Man-in-the-Middle Attack
- Integrity Attack

Our Focus

- False Data Injection Attack
- Virus
- Backdoor
- Logic bomb
- Trojans
- And many more...! You can google

Replay Attack

- Replay attack is based on interception of smart grid's usage pattern. The replay attacks can easily be realized since the utility company cannot manage every smart meter distributed in a very large area.
- The attacker can intercept the smart meters to observe the reported data for a certain amount of time.

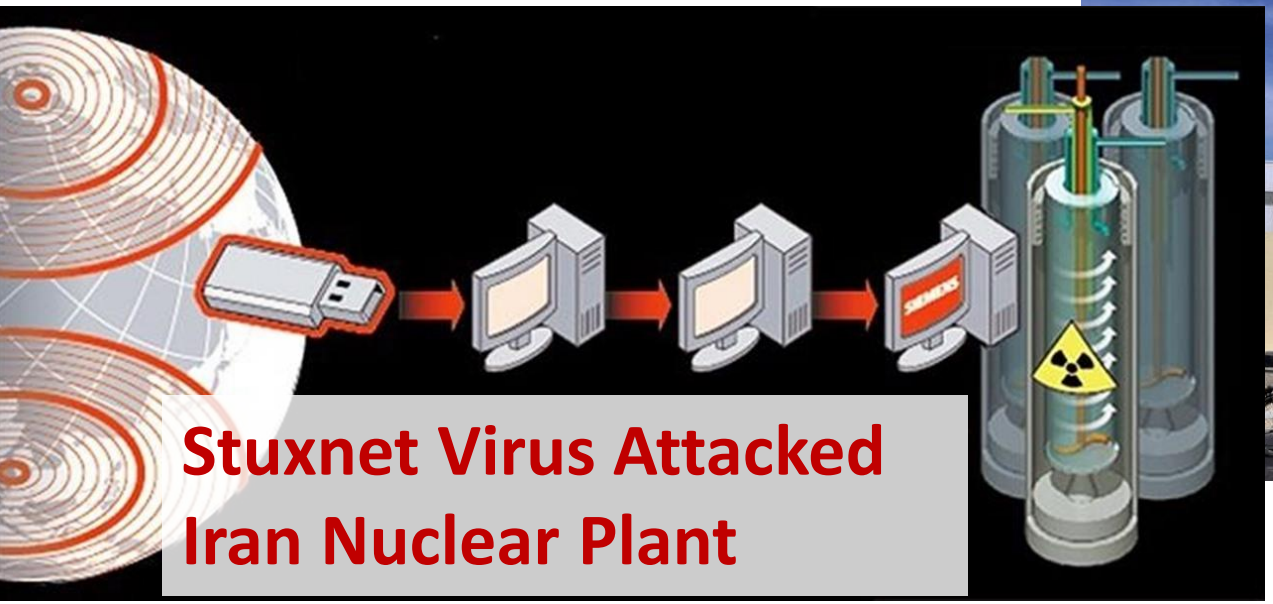
Replay Attack

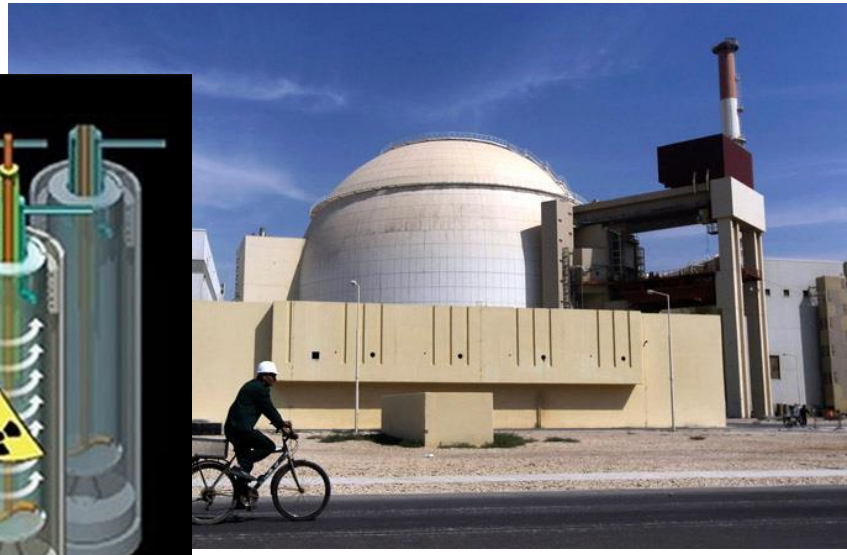
- The attacker replays (or retransmits) the data to smart grid control center.
- Attacker can make customers' smart meters out of order by injecting incorrect data (e.g., energy consumption data) to the system, which may lead to incorrect energy price or inaccurate prediction.

Replay Attack

- In order to launch such an attack the adversary needs to
  - capture and analyze the data transmitted between appliances and smart meters to gain the customer's characteristics of power usage
  - inject false control signals into the system; and lead to power system instability
- The aim of the replay attack is:
  - to steal energy by changing idle equipment's status to busy state in order to reroute the power to another place
  - cause physical damage to the system

Replay Attack – an example





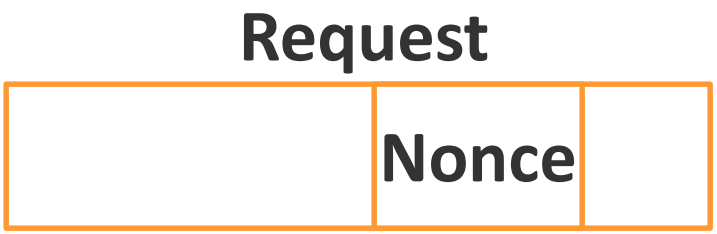
- Stuxnet is 500KB computer worm and allegedly designed in a joint effort by USA and Israel as a cyberweapon against Iranian nuclear facilities.
- Stuxnet targets power supplies used to control the speed of a motor in nuclear centrifuges. The malware intercepts commands sent to the power supply from the Siemens industry control software, and replaces them with malicious commands to control the speed of a motor, varying it wildly. This can destroy the centrifuges and impair uranium enrichment.

Defending Replay Attack – adding timestamp and sequence number

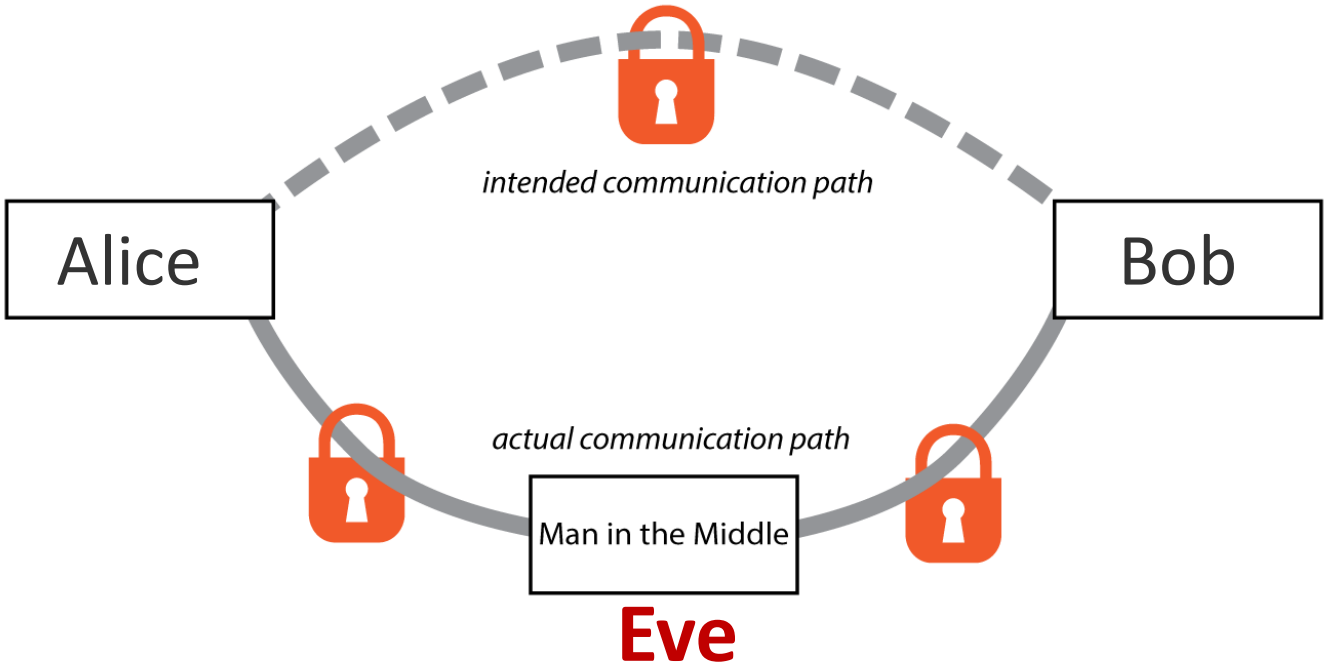
- Put a time stamp in each message to ensure that the message is “fresh”
  - Do not accept a message that is too old
  - Place a sequence number in each message
  - Do not accept a duplicated message

Defending Replay Attack – adding random noise

- Add random noise in request-response
  - Sender of request generates a nonce (random number)
  - Places the nonce in the request
  - Server places the nonce in the response
  - Neither party accepts duplicate nonce



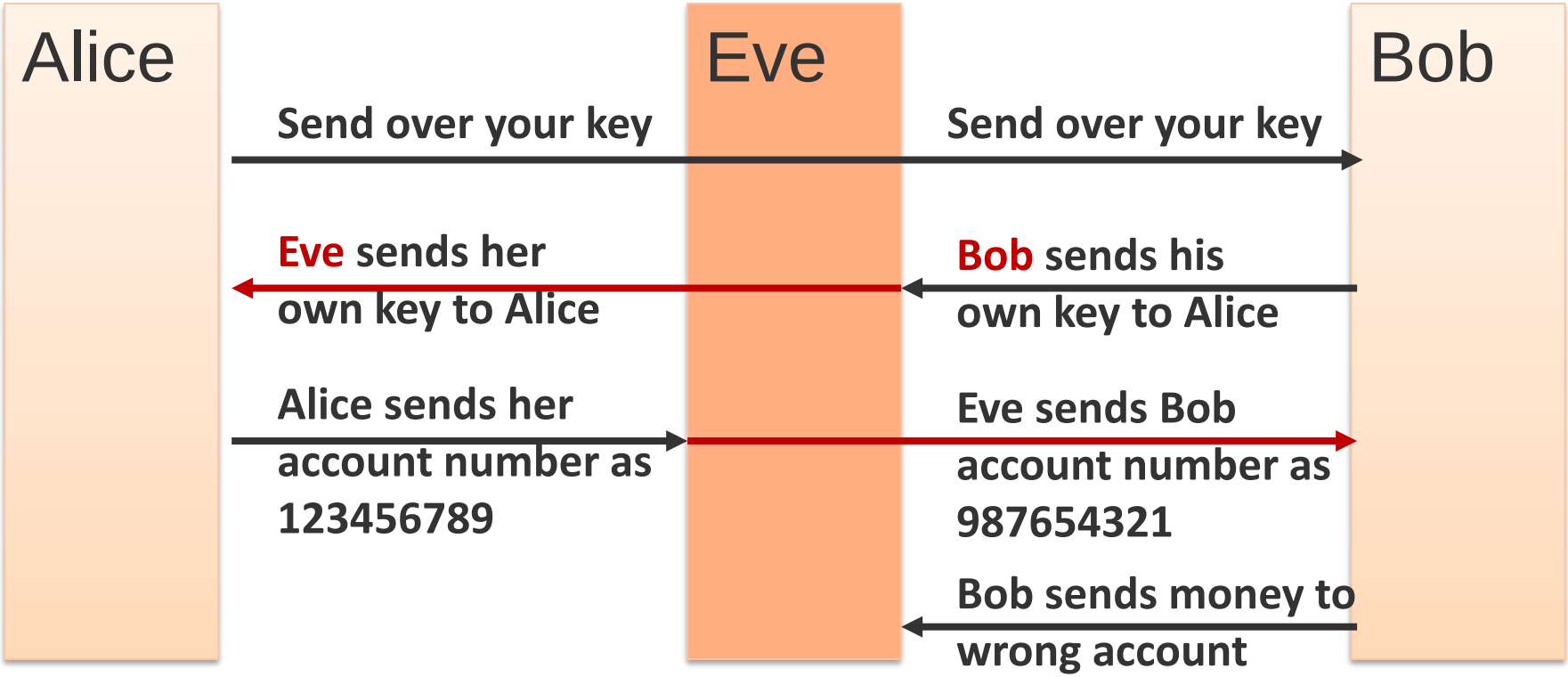
Man-in-the-Middle Attack – in general



- **Alice thinks her communication with Bob is secure, but actually a man-in-the-middle Eve is eavesdropping on the conversation. Eve impersonates two communication nodes and makes them believe that they are talking together.**

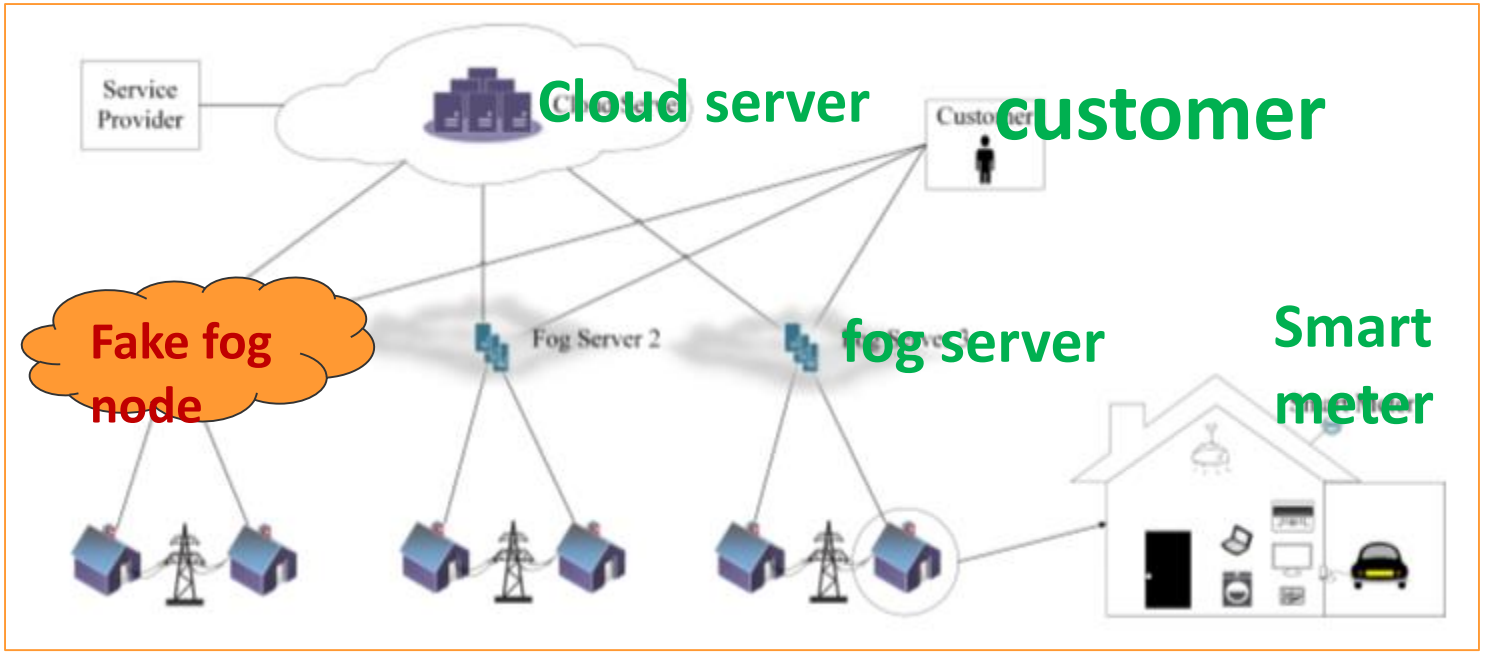
- **Alice and Bob think their communications are end-to-end encrypted when actually there is an eavesdropper Eve who is removing the encryption, examining (or modifying) the unencrypted content then re-encrypting it before passing it to.**

Man-in-the-Middle Attack may result in financial loss



- Eve impersonates both sides of the conversation to gain access to funds. Eve intercepts a public key and can transpose her own credentials to trick Alice/Bob into believing they are talking to one another securely.
- Very common in wireless communications. One typical solution is to enforce a secure wireless authentication protocol, e.g., WPA2 (Wi-FI Protected Access 2)

Man-in-the-Middle Attack in Smart Grid with Fog Computing



- Gateways serving as fog nodes may be compromised or replaced by fake ones. Private communications of victims (individual users, block of houses) will be hijacked once the attackers take the control of gateways.

- This attack happens when the adversary intercepts network data (e.g., switch states) and meter data, fabricates part of these, and forwards the modified version to the control center.

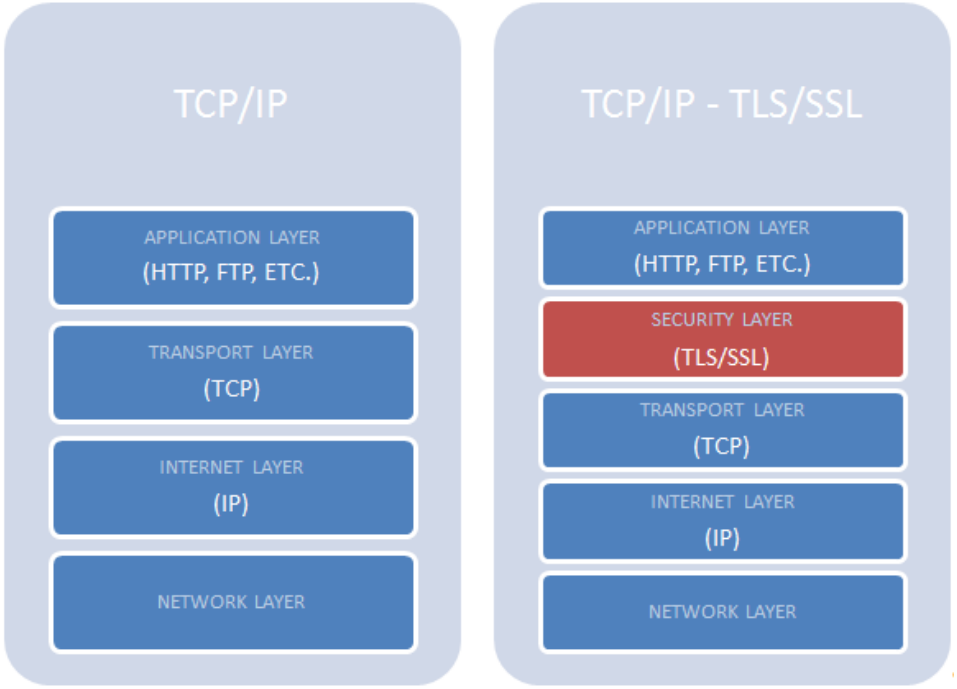
Man-in-the-Middle: Consequences

- The adversary can mislead the control center that the grid is operating under a topology different from that in reality.

- Such an attack, if launched successfully and undetected by the control center, will have serious implications:
  - A grid that is under stress may appear to be normal to the operator. This delays the deployment of necessary measures to ensure stability.
  - Grid operating normally may appear to be under stress to the operator. This causes load shedding and other costly remedial actions by the operator.

Man-in-the-Middle: Defense

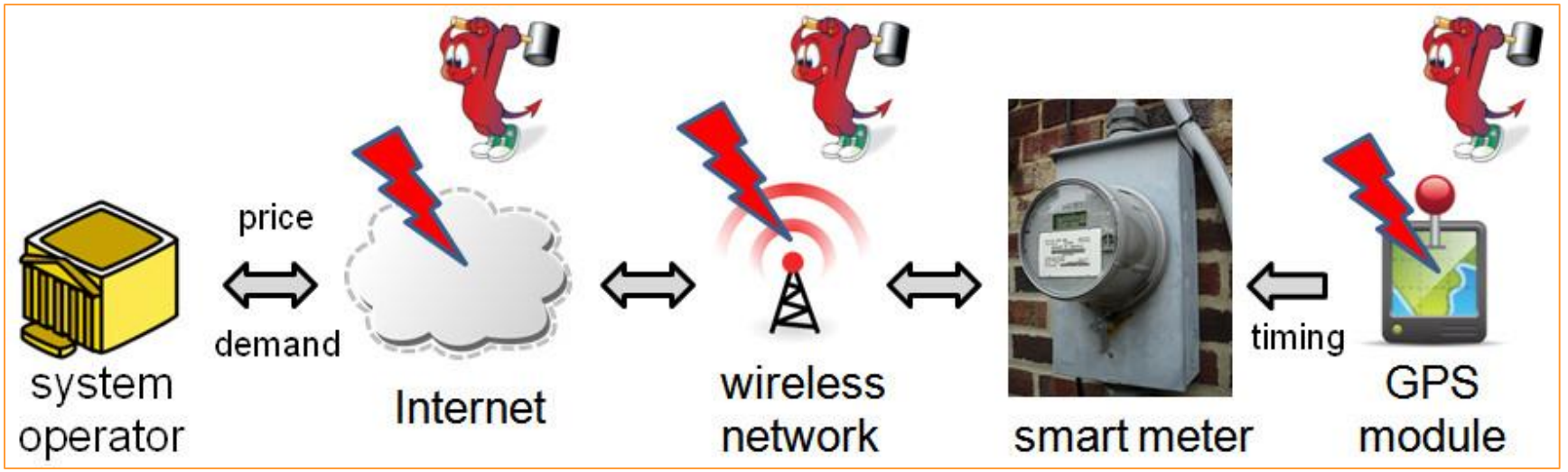
- Man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other.
- Two crucial points in defending against the attack are **authentication and encryption**. We need to ensure that information from our devices will indeed go to the intended recipient.



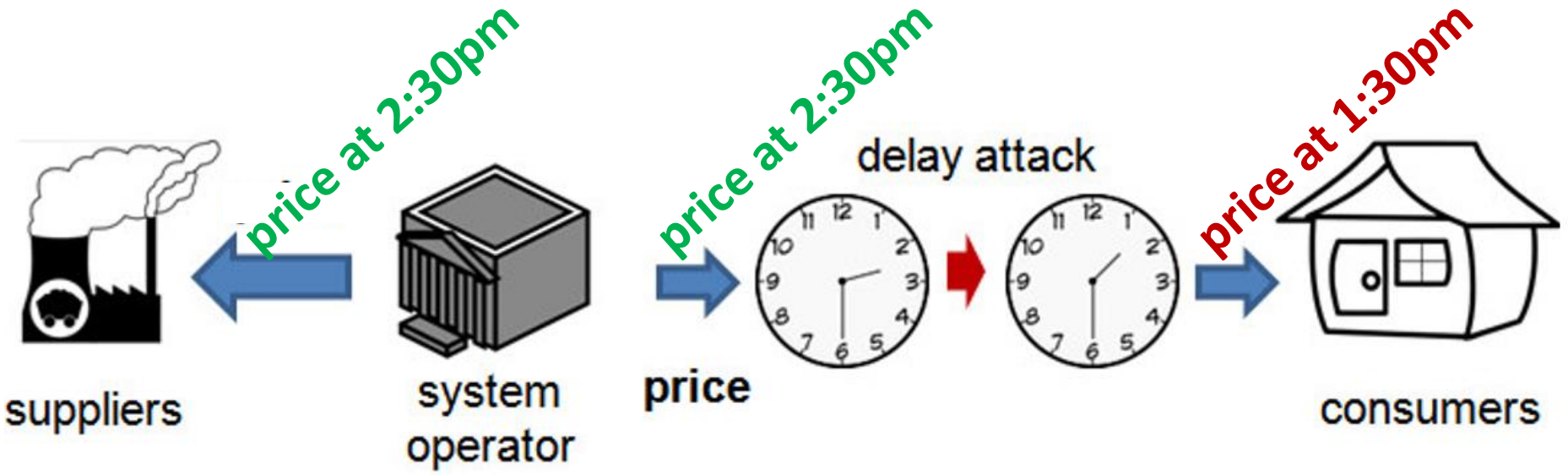
- SSL (Secure Socket Layer) and HTTPS (HTTP over SSL) is the standard for creating this virtual trust and establishing secure communication between devices.

Integrity Attacks on Real Time Pricing (RTP)

- We consider integrity attacks on the price received by consumers. Small malicious modifications to the price signals can be iteratively amplified, causing inefficiency and even severe failures such as blackouts.
- Delay attacks: The compromised price is an old price.



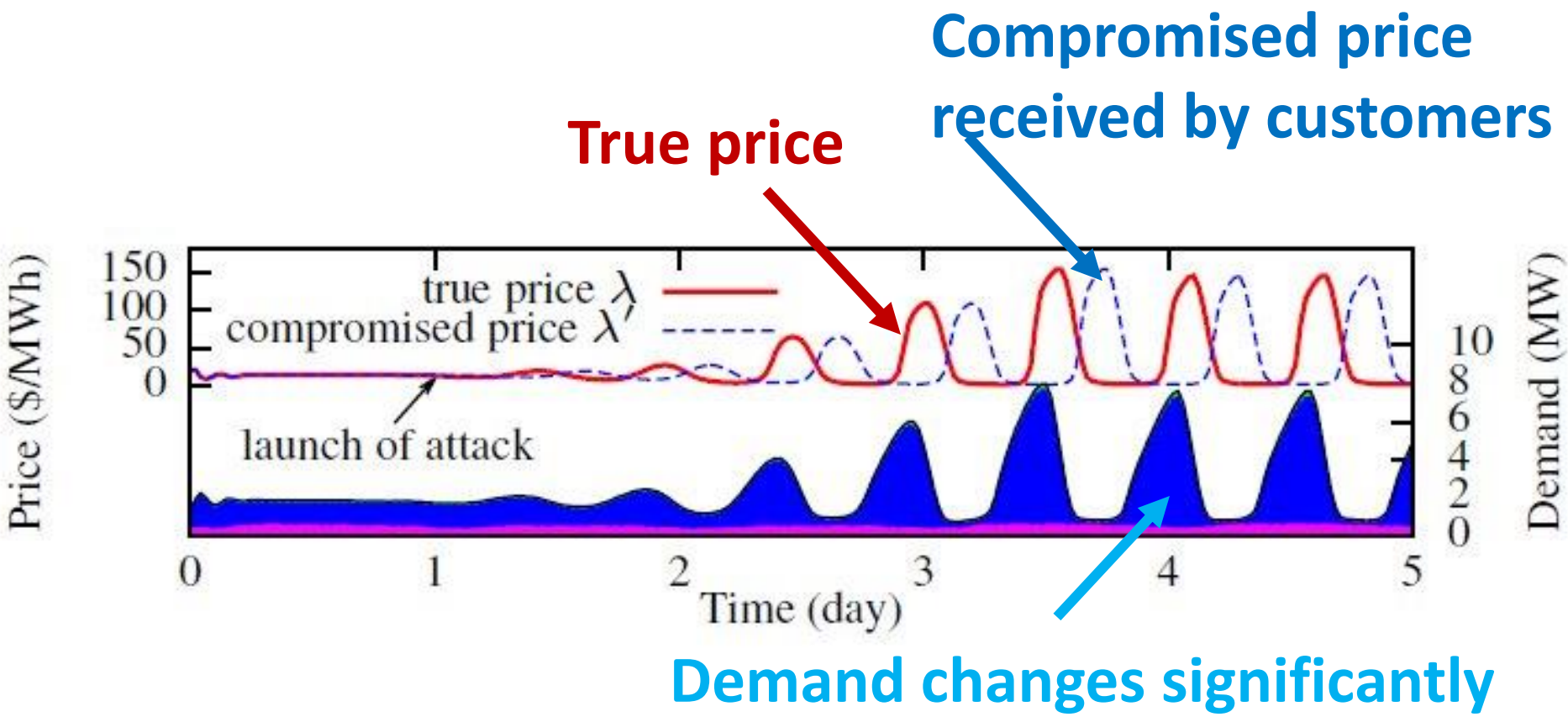
Integrity Attack – delay attack



- The delay attack can be launched by modifying the smart meters' internal clocks. Attacks on the clocks can be realized by compromising the vulnerable time synchronization services in smart grids. Current commercial smart meters synchronize their clocks by either built-in Global Positioning System (GPS) receivers, which has been shown to be vulnerable to realistic attack methods.

- Smart meters typically assign a memory buffer to store received prices. When a smart meter's clock has a lag, it will store newly received prices in the buffer and apply an old price for the present.

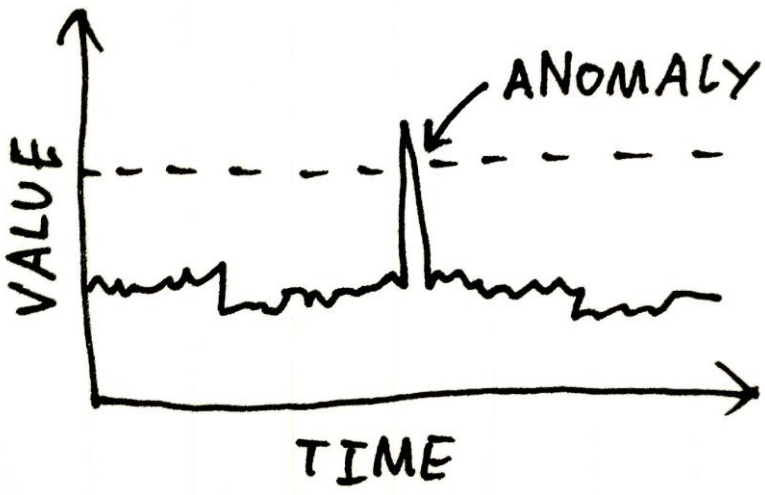
Results under the delay attack.



- A small error between demand and supply is amplified iteratively along the control loops, after the launch of the attack

Defending Integrity Attack: rule-based approaches

- **Main idea**: integrity attacks would result in abnormal state estimations (e.g. energy demands) , we can apply anomaly detection techniques.
- **Rule-based mechanisms**: typically exploit static thresholds to identify anomalies. When the value of a raw data input exceeds the thresholds, this value is regarded anomalous.



- Advantage: these schemes introduce very low overhead to the system
- Disadvantage: they fail to adapt to valid changes in the environment. Furthermore, a high level of professionalism is required to manually maintain detection thresholds.

MORE CONSIDERATIONS…

Charging Electric Vehicles (EV)

- When connected to a charging station, the EV's charging profile must always be monitored. EV itself must also properly respond to command signals coming from the charging station.
- It is important that such commands come from an authentic charging station and reach the required EV unaltered.

- In a typical charging scenario, an EV arrives at a charging station and requests a charging session. As stated by IEC 15118, each EV must have a secret key stored in its ECU (*Electronic Control Unit)*.
- If the control station verifies the car's key through wireless communication, the charging process can be compromised by a Man-in-the-Middle attack. **(Q: are you able to see Man-in-the-Middle attack here?)**

Man-in-the-Middle for Electric Vehicles

- A registered car with a valid key performs the authentication process. The **stolen car** eavesdrops on the conversation between the charging station and the registered car. The power goes to the stolen car.

References

- **Y. Yan et al., “A Survey on Cyber Security for Smart Grid Communications”, IEEE Communications Tutorials & Surveys, vol. 14, no.1, 2012**