Smart Grid Privacy and Security

05.03.2026

Frank Eliassen

University of Oslo, Norway



Learning Objectives

Throughout this lecture, the aim is that the students to be able to understand:



Privacy and Security

the basic concepts related to smart grid privacy and security



Typical privacy issues

several typical privacy issues, consequence and solutions in smart grids



Typical security issues

several typical attacks, consequences and solutions in smart grid

Industry Invited Talk Today



Janne Hagen

Adjunct Associate Professor

Digital Security Group

Dept of Informatics

University of Oslo

Digital Security for Smart Grids

Outline



Smart Grid Cyber-security

Concept

CIA



Smart Grid Privacy

Load signature

Billing

Load monitoring



Smart Grid Security

Replay attack

Man-in-the-Middle attack

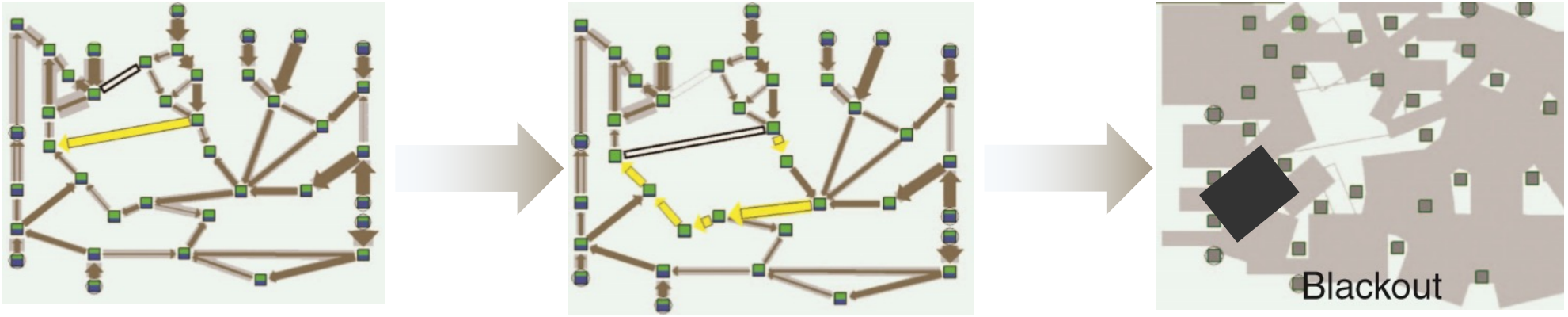
Integrity attack

01

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

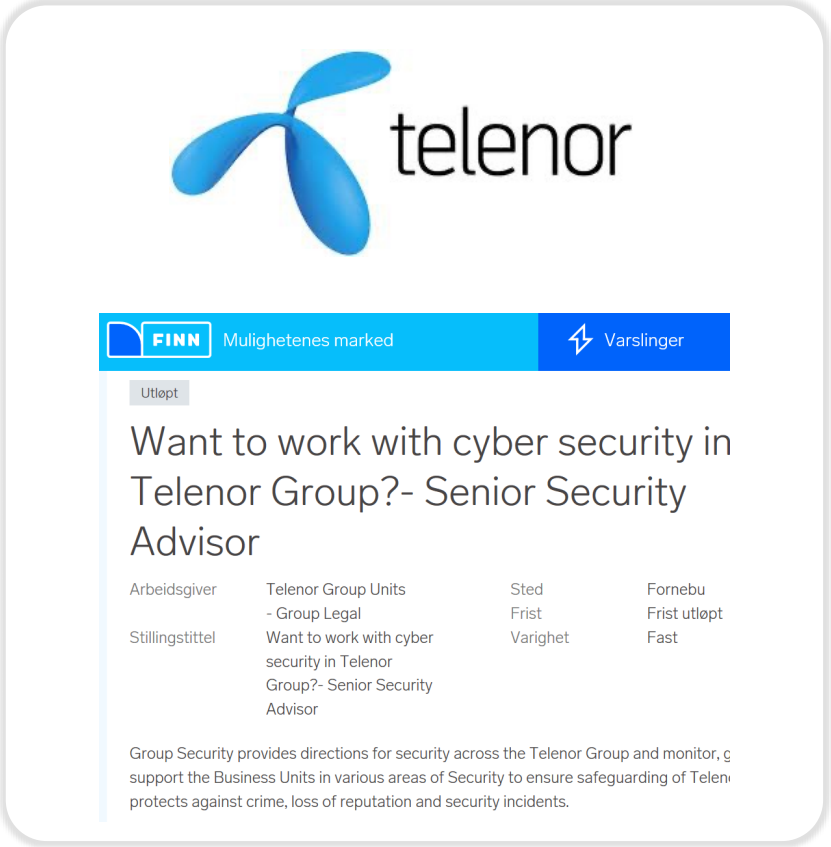
Overload is spread to three lines nearby

Blackout in the area

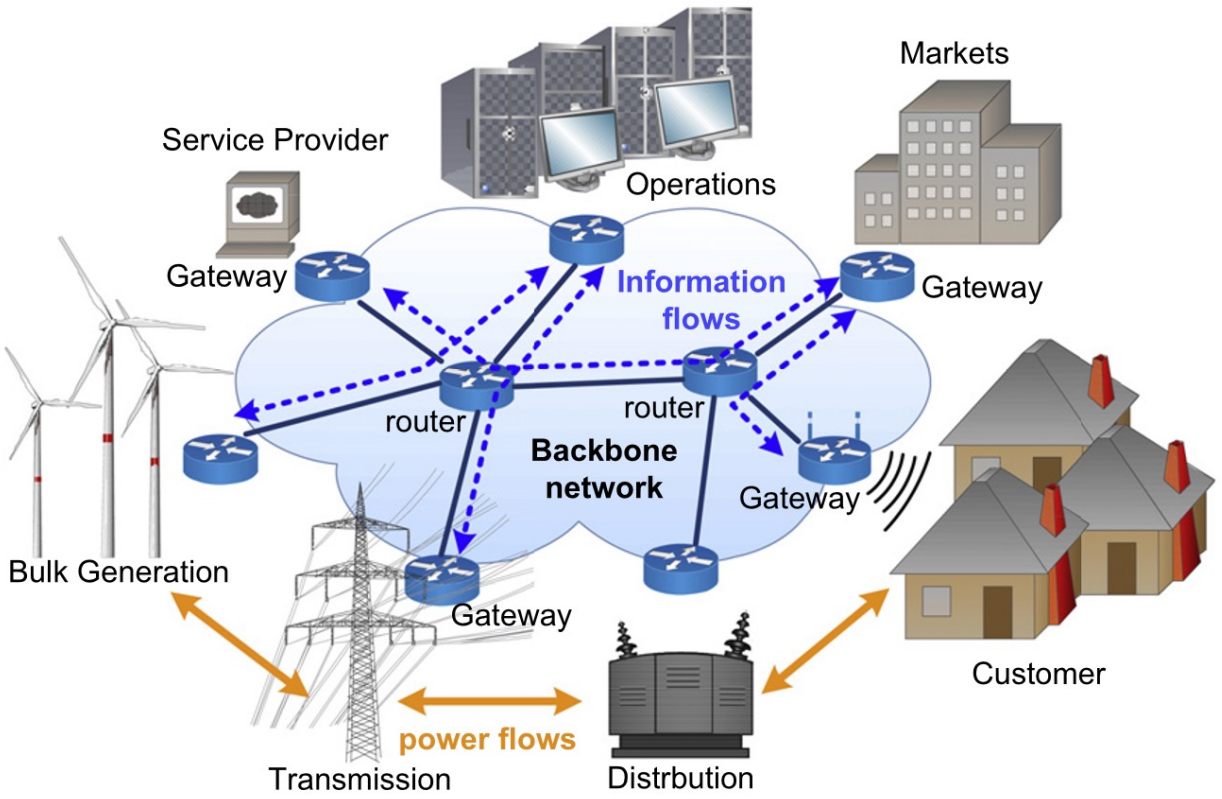
- Cyber Security: technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access → Our focus in this lecture

In Norway

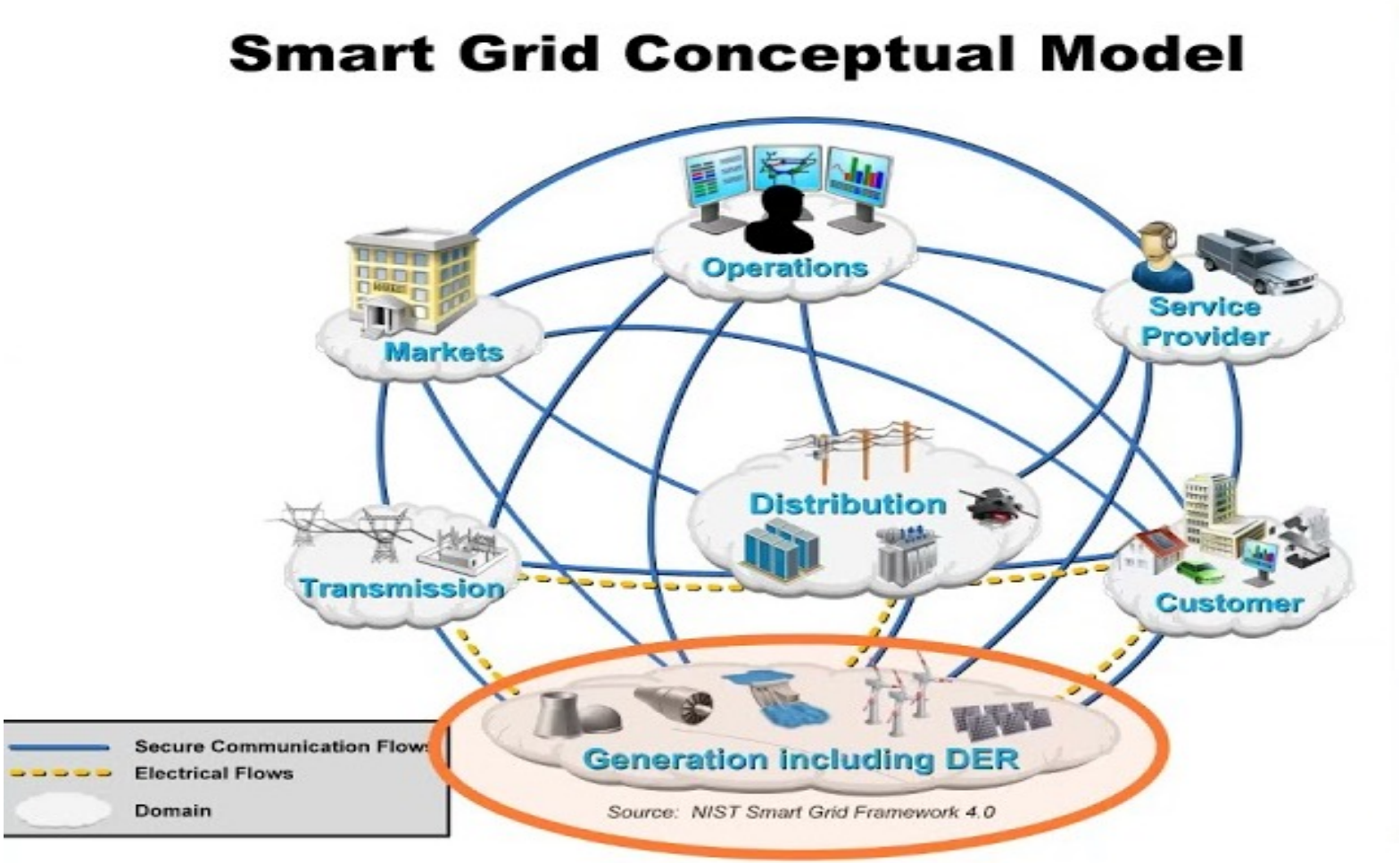
- Norway has not seen serious cyber attacks that have taken out critical societal functions
- But, “Around 80 per cent of all data traffic in Norway passes through Telenor. Every year, our security team deals with and averts thousands of cyber attacks and countless attempts at fraud, but it is impossible 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.



Information flow in smart grids according to NIST (National Institute of Standard and Technology, USA) reference model

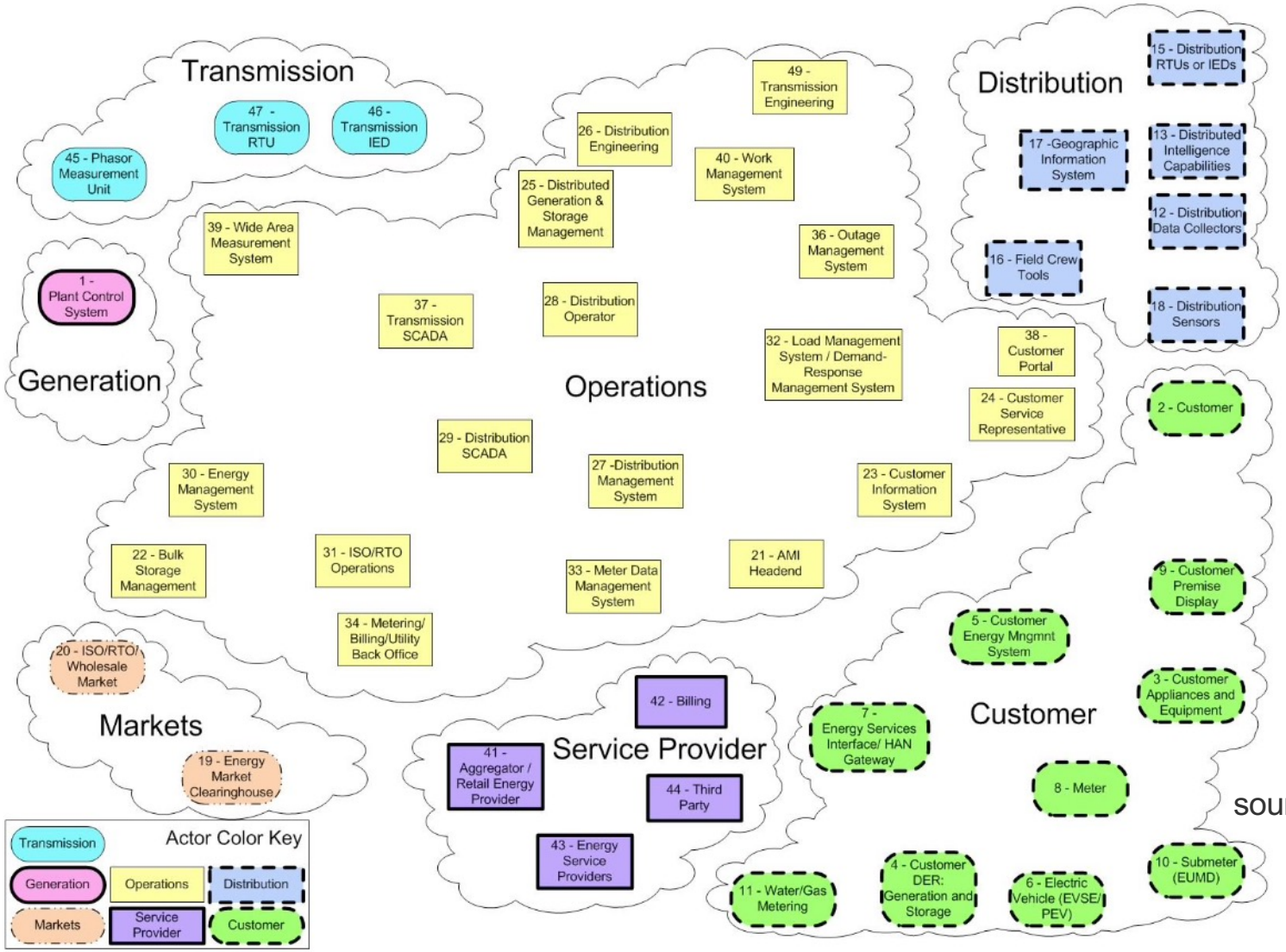


NIST (National Institute of Standards and Technology, USA**)**



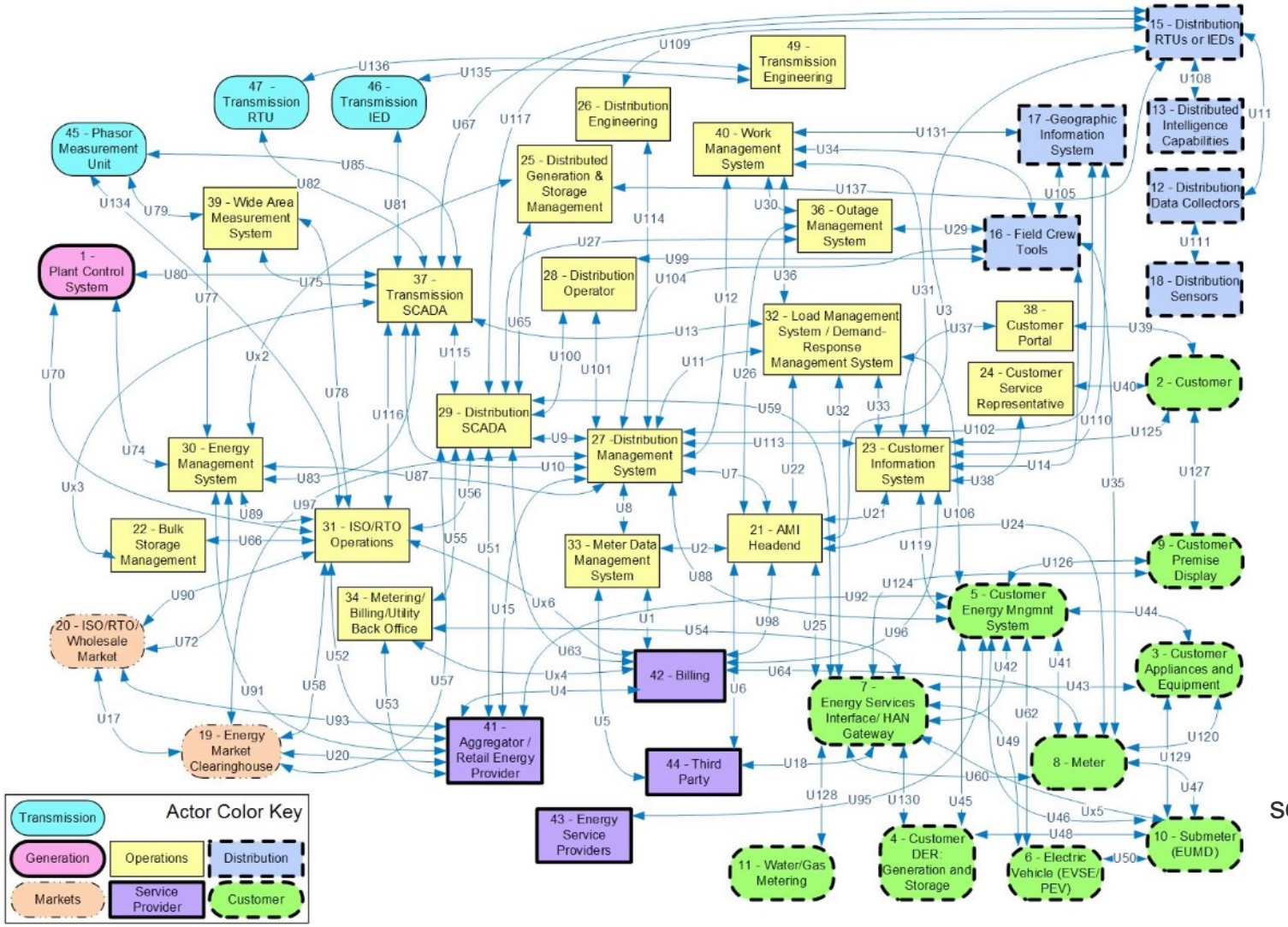
Interaction between Smart Grid domains through information and energy flow

Actors within each of the Smart Grid domains



source: NISTIR 7628 Rev 1, 2014

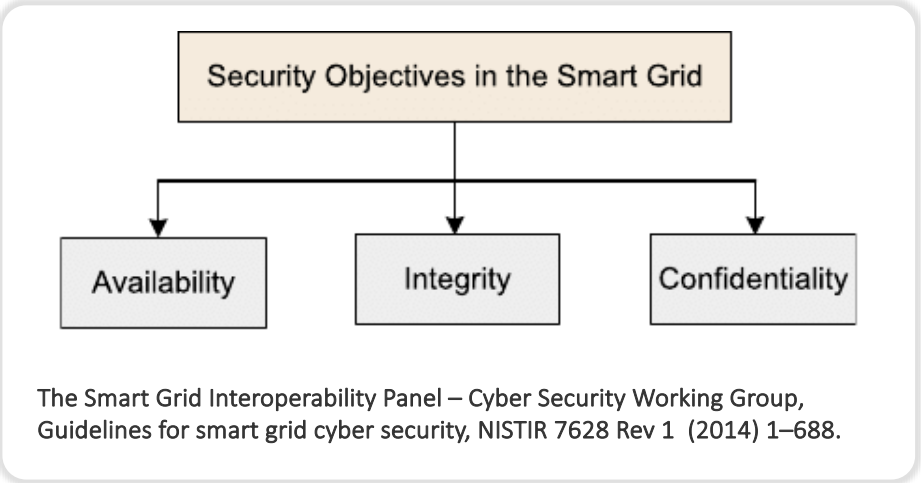
Information exchange between Actors in the Smart Grid domains



source: NISTIR 7628 Rev 1, 2014

Three Cyber Security Objectives in Smart Grids – 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



The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 Rev 1 (2014) 1–688.

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

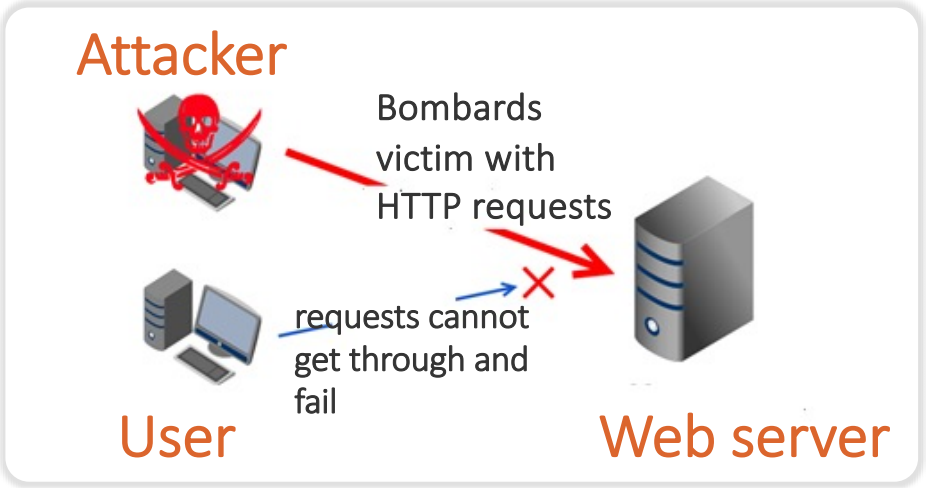
Availability

- Availability: Ensuring timely and reliable access to and use of information in Smart Grids. 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 or wrong price information can adversely affect power demand.
  - Availability of commands: important for turning a meter back on after completing the payment of an electricity bill.

Availability Attack – an example

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



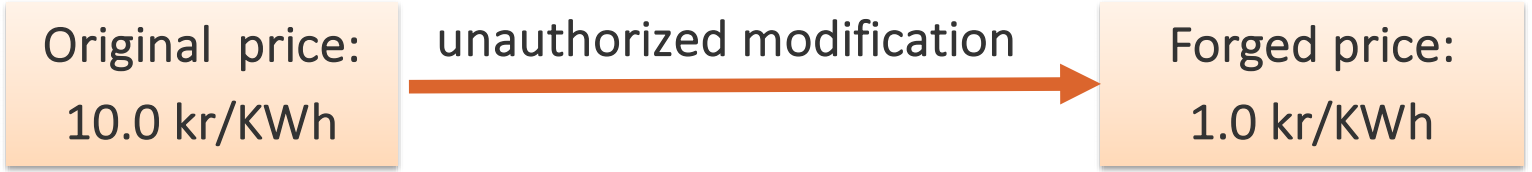
- An old DoS attack: *ping –t 0.01 –l 500 129.240.171.52*

UiO IP address

- -t: the time (sec.) used to repeat the ping recursively
- –l: the packet size in byte.
- Vary these parameter values in order to make your attack more intense. The larger the –l value and the smaller the –t value, the higher the attack intensity will be.

Integrity

- Integrity: 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 of information and can induce incorrect decision regarding power management. Violation of integrity may cause safety issues, e.g., equipment or people may be harmed.



The operator wants to set a high price to discourage energy usage from users

The forged price is very low, and the users take advantage of the price and use more electricity

- Q: any consequences after price changes?

Integrity Attacks – an example

- Electricity theft: meters are tampered with, and violators are not charged for the electricity actually used. The Cyber Intelligence Section of 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 unstable, why?

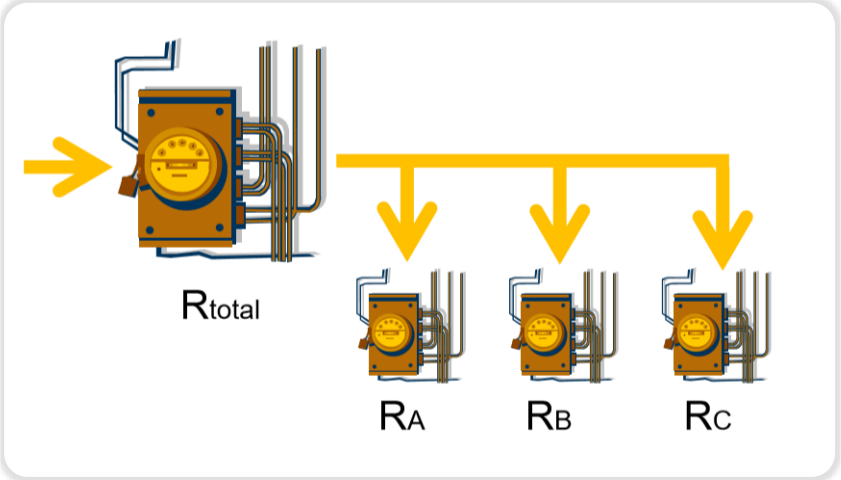


- It may be possible for an attacker to destabilize a real-time electricity market system by compromising smart meter consumption readings, causing suppliers to modify the electricity price accordingly.

Ref. 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 of 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 $R_{total} = R_A + R_B + R_C$



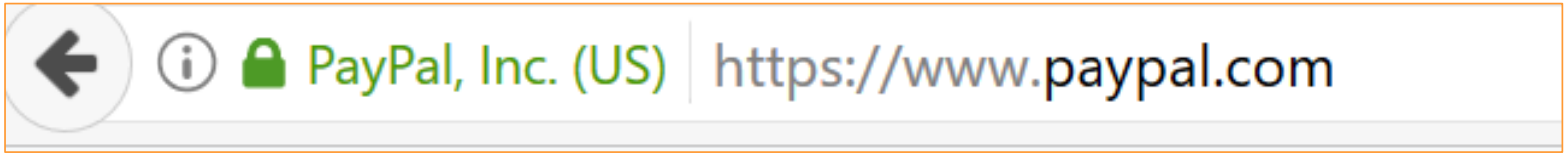
Q: What is the condition for that there is electricity theft?

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

Confidentiality

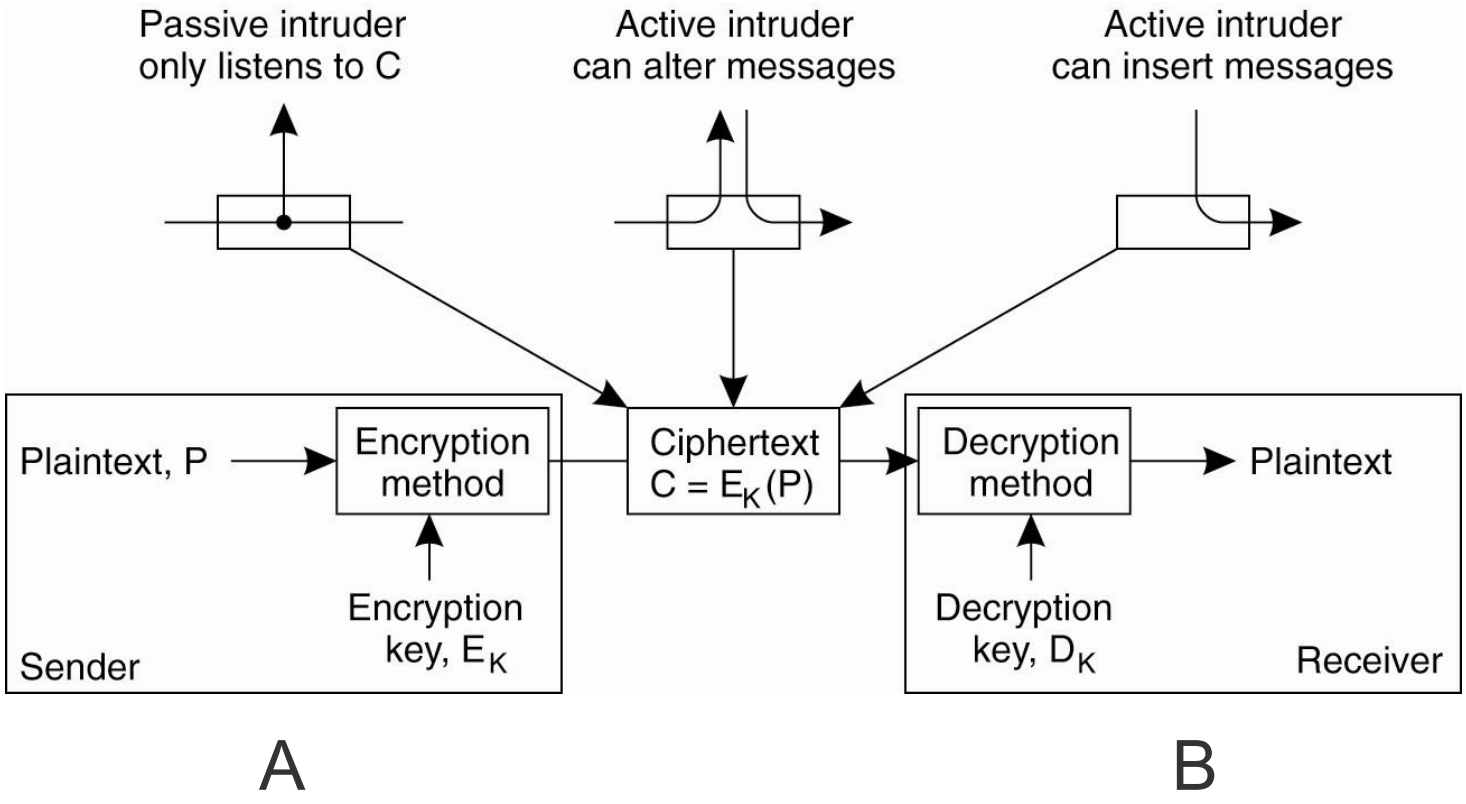
- Confidentiality: Confidentiality ensures that access to information is restricted to authorized entities, e.g., bank account statements, personal information, credit card numbers, trade secrets, government documents.

- 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.



Cryptography

Intruders and eavesdroppers in communication.

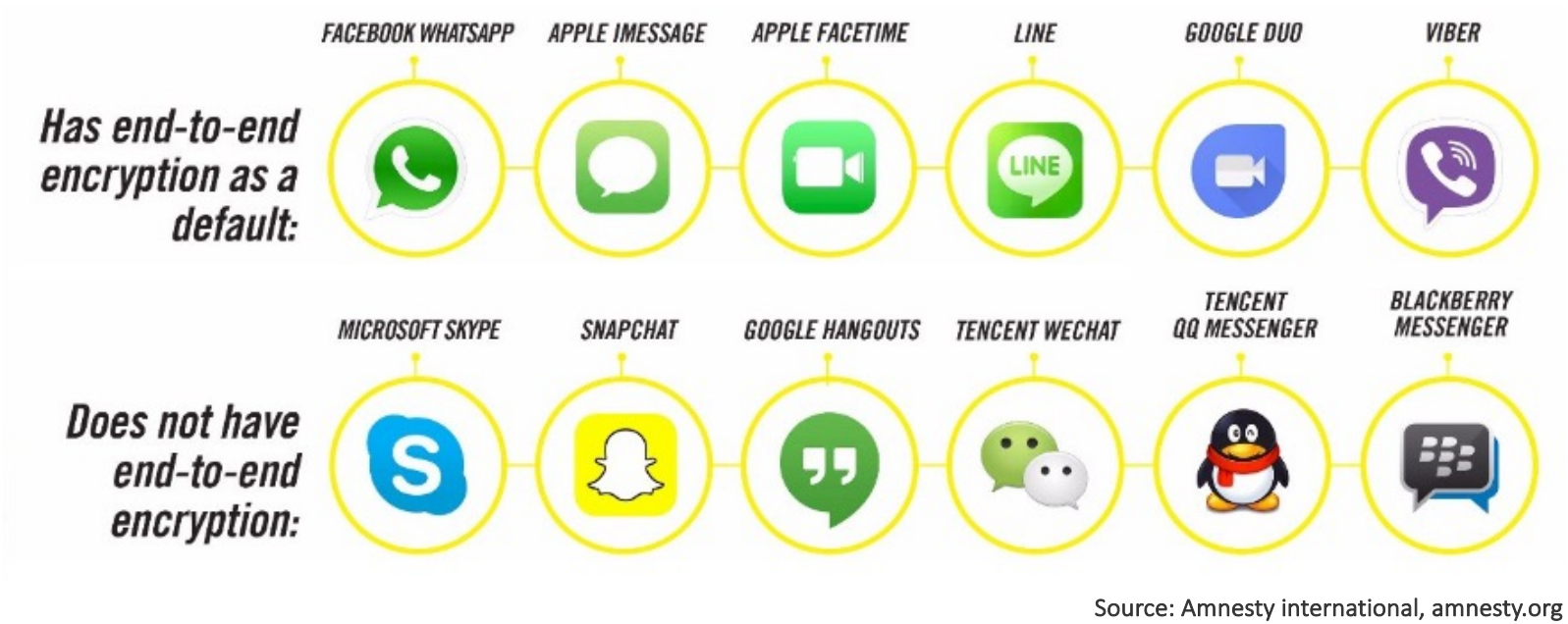


- **Symmetric key encryption:** Secret key is shared by A and B: $K_{A,B}$
- **Asymmetric key encryption (public key encryption):** two different keys used to encrypt and decrypt data: the public and private key
  $K_{A,\,pub}$ $K_{A,priv}$
  $K_{B,pub}$ $K_{B,priv}$

source: Tanenbaum & Van Steen, Distributed Systems: Principles and Paradigms, 2e, (c) 2007 Prentice-Hall, Inc.

Confidentiality – an example

- End-to-end encryption: only a sender and the recipient of a specific message can see one another's messages. 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 personal 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 .
- California Consumers Privacy Act (CPA): effective from jan. 2020. Fine: 7500USD/California customer
- "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

GDPR (external) accountability

- **Giving consent**: to processing of personal data for *specific* purposes
- **Transparent data collection**: be clear and open with individuals about how their information will be used to enable *informed choices*
- **Minimal data collection**: limit data collection to what is necessary for the purpose of data processing
- **Online access to own data**: via a secure remote system
- **Export of own data**: in a commonly used machine-readable format (right to data portability, right to be forgotten)
- **Granular choice over own data**: what data, category of data, time and frequency of data capture, giving access to parts of the data;
- **Limit data distribution**: who can use the data and how; and keep raw data as close to the source as possible (recommended)
- **Permit local control**: allowing individuals to review the results of processing operations prior to «publication» or distribution (cf previous point)

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.

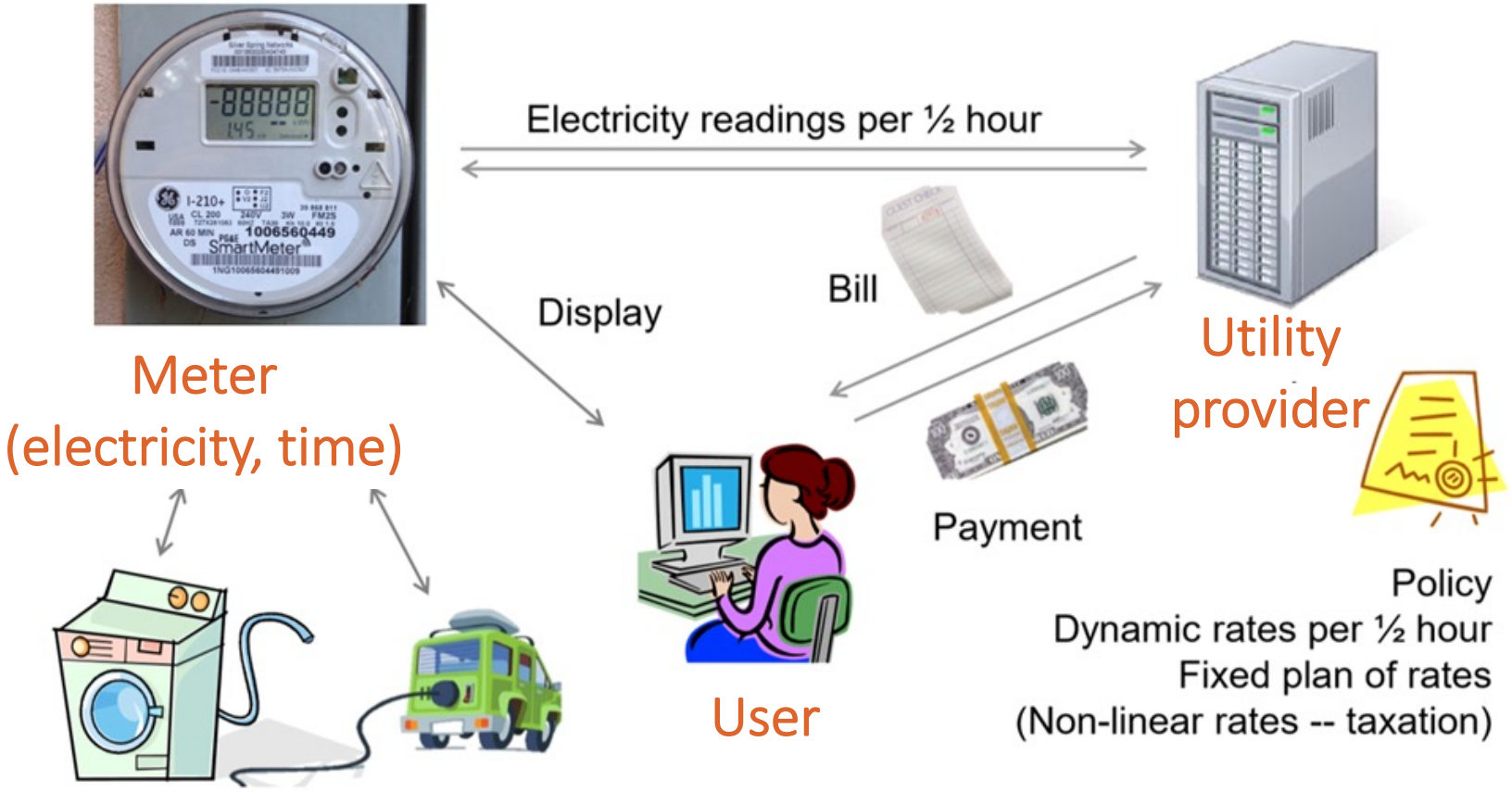


- Q: is mutual authentication used in 4G/5G?
- Q: should we perform mutual authentication when an Electric Vehicle is charging battery?

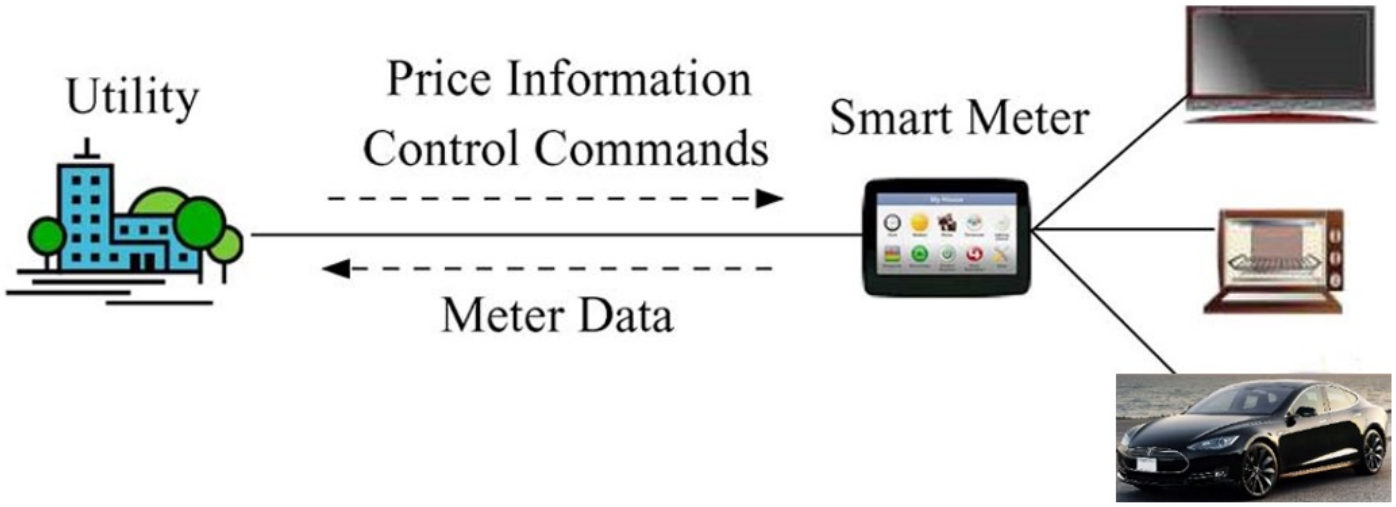
02

SMART GRID PRIVACY

Privacy is very much related to smart metering



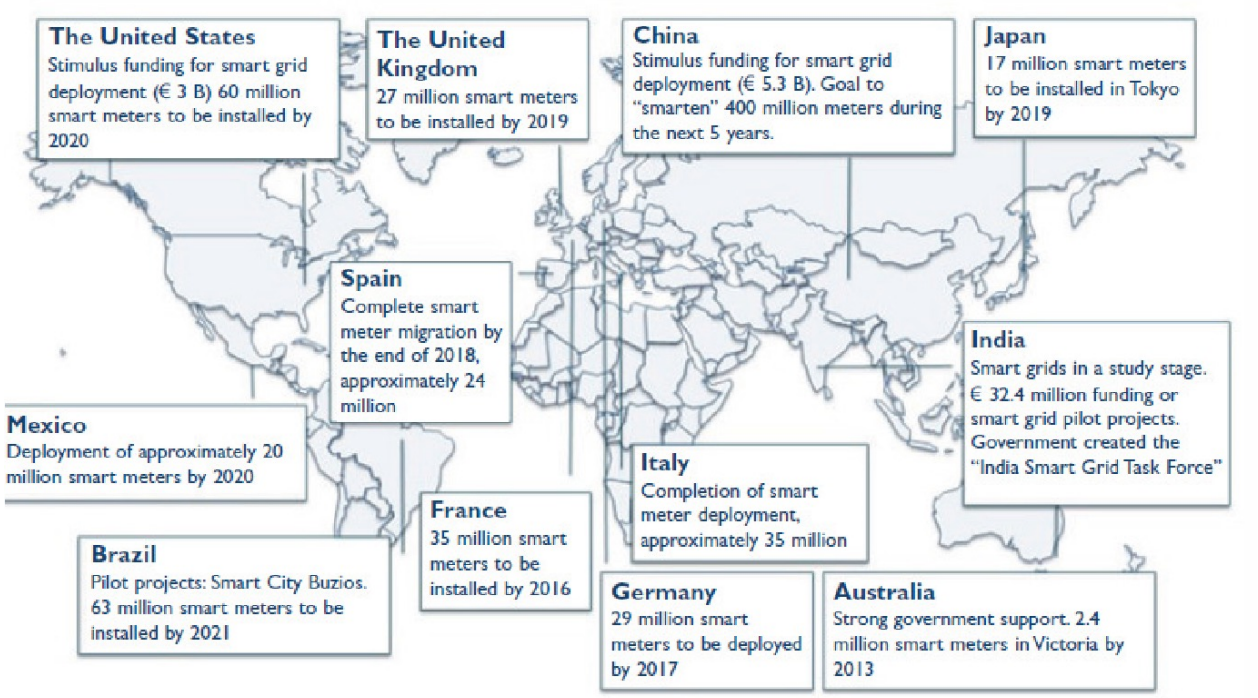
Important information exchange through smart meters



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

Smart Meters Deployment around the World

- Netherlands: April 2009, declined a bill which would require the installation of smart meters in residences: privacy issues as the main concern measure. Today: approaching 90% penetration.
- Germany: decided against a nation-wide deployment of smart meters due to privacy and cost issues in 2016. Still the case.
- As per 2022: 13 of the 27 EU countries have completed smart metering rollouts.
  Why could that be?



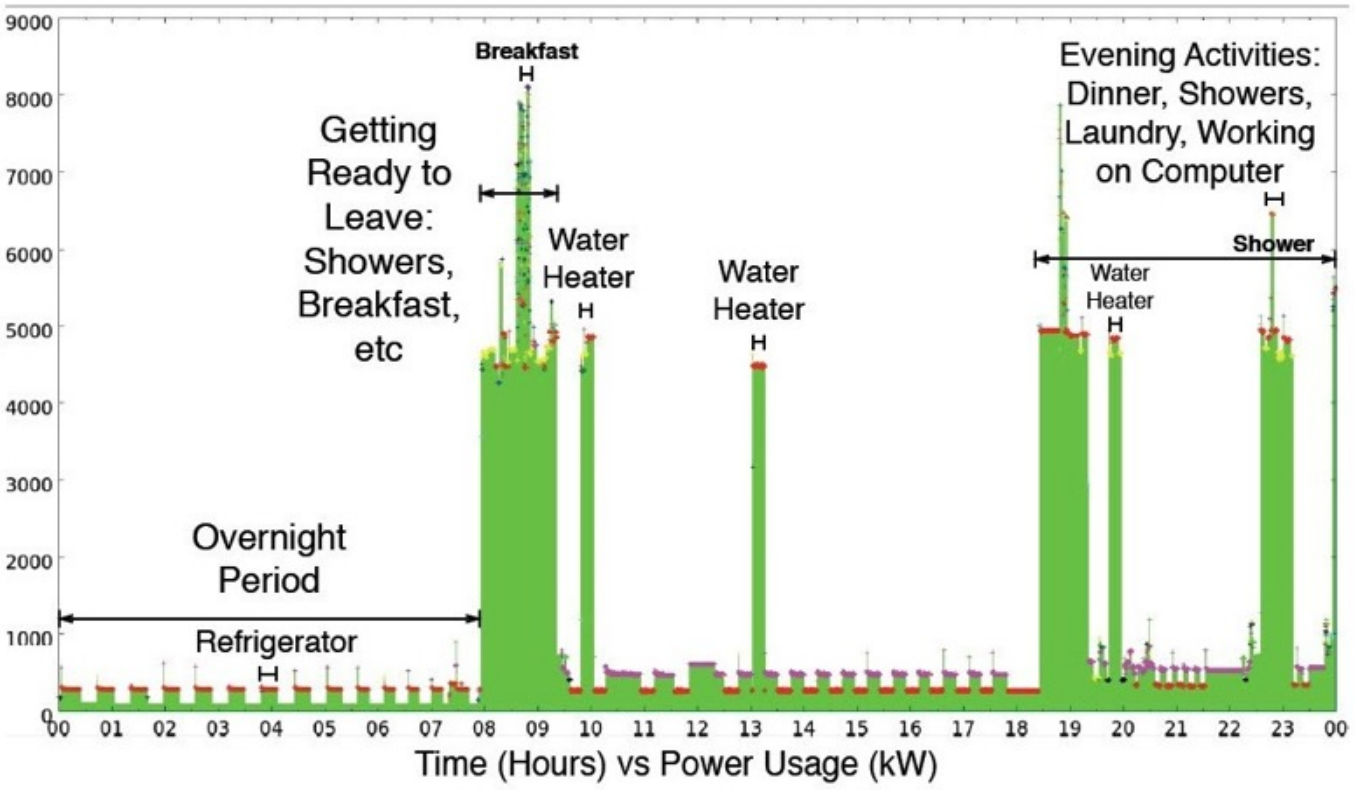
Source: Frost & Sullivan analysis

Privacy Concerns at End-users

- Smart Meters: Information regarding energy use will be collected from the home and may be able to relate information about specific types of appliances being used at specific time.
- Fine-grained meter reading: one essential technology of smart grids is fine-grained meter reading within a very short period (15min or shorter) 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 a centralized data center. Fine-grained meter readings may cause serious privacy issues.
- Load signatures: potentially indicate when you are home and whether you are cooking, watching television, or using other electronic devices.

Load Signature

Power Usage (kW)



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

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

What Could Power Usage Information Reveal?

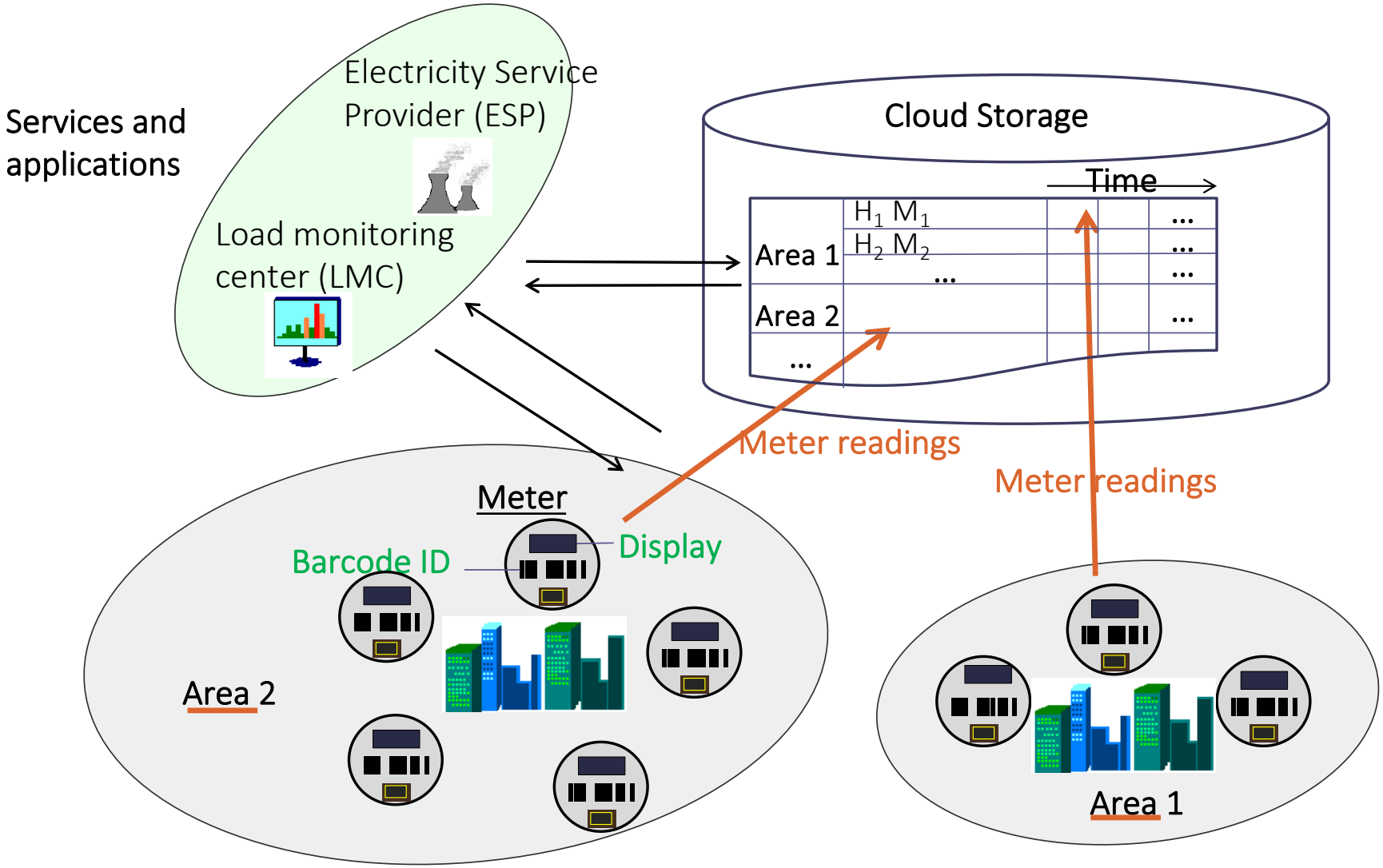
Applications/Services, Questions?		Energy usage pattern
Safety services Q: Are you on vacation?		Yes: No power events for some days No: random power events in a day
Health services Insurance services Q: Did you get a good night's sleep?		Yes: No power events overnight for at least 6 hours No: Random power events overnight
House renting Q: 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

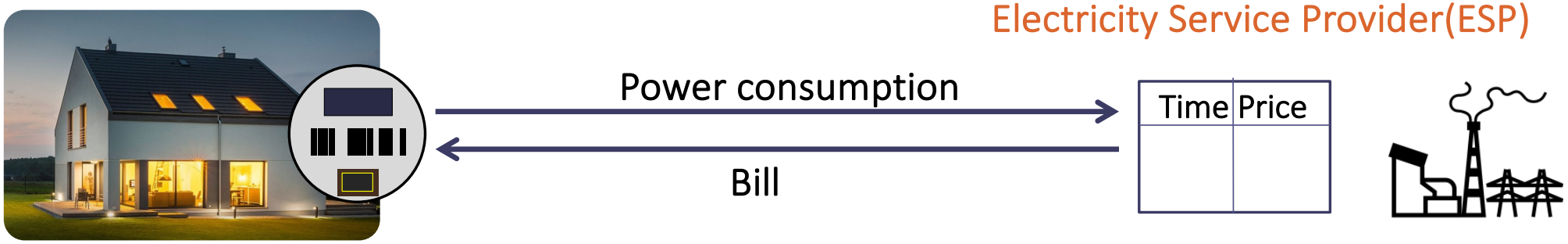
Who wants smart meter data?	How could the data be used?
Utilities	To monitor electricity usage and load; to determine bills
Advisory companies	To promote energy conservation and awareness
Insurance companies	To determine premiums based on unusual behaviors that might indicate illness
Marketers	To profile 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 energy consumption data every few minutes?

Billing Application and Load Monitoring Application

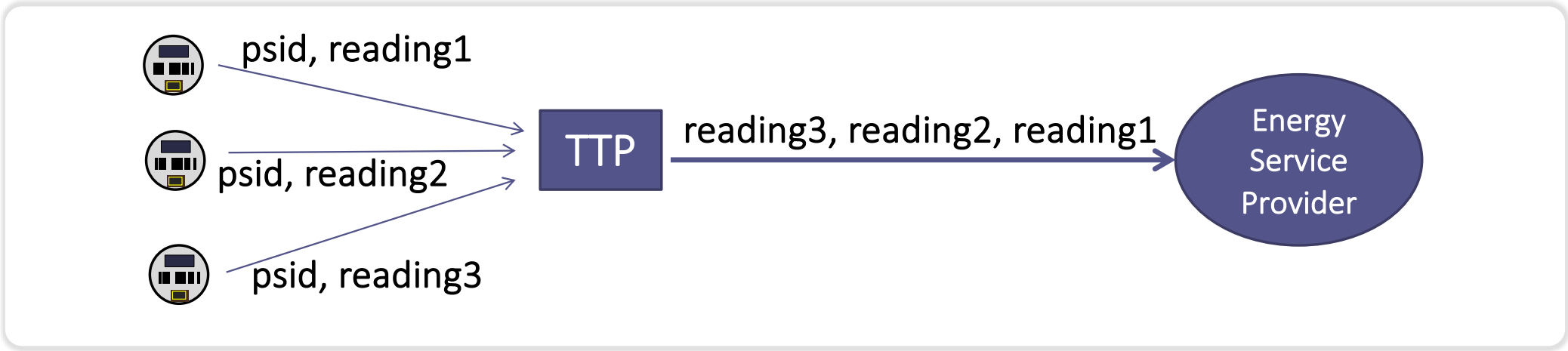


Automatic Billing – we do not need meter readings every minute



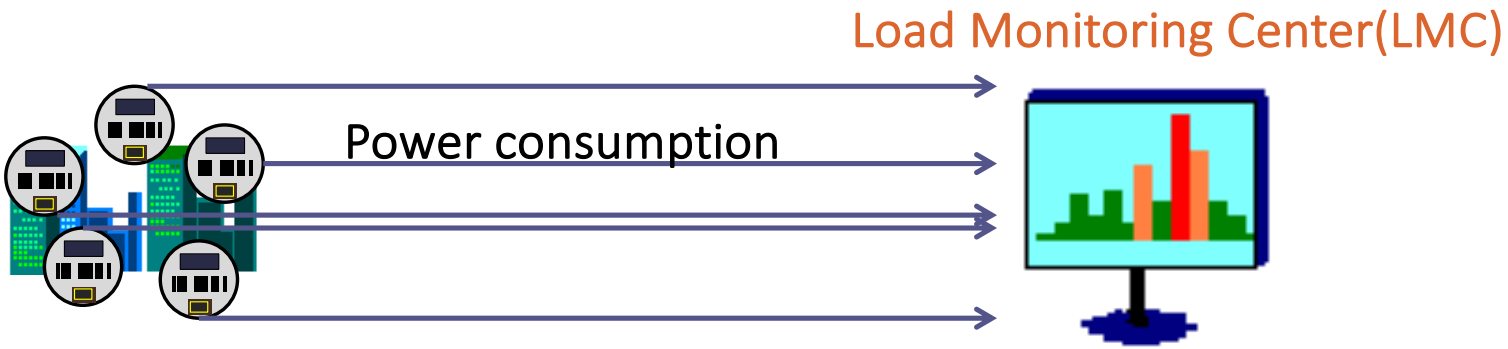
- Automatic Billing: In billing applications, the electricity service provider only needs the amount of power consumption per hour to compute a bill.
- For example, in Ontario, Canada, the bill service during winters only needs the consumption data over two hours in an on-peak time period, six hours in a mid-peak time period, and 12 hours in an off-peak time period.

Privacy-preserving Automatic Billing (a proposal)



- Trusted third party (TTP) computes the bill, e.g., a module in a grid operator system
- Anonymization – Instead of a user's real ID, a pseudonym (a fake ID, denoted by psid in the illustration above) 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.

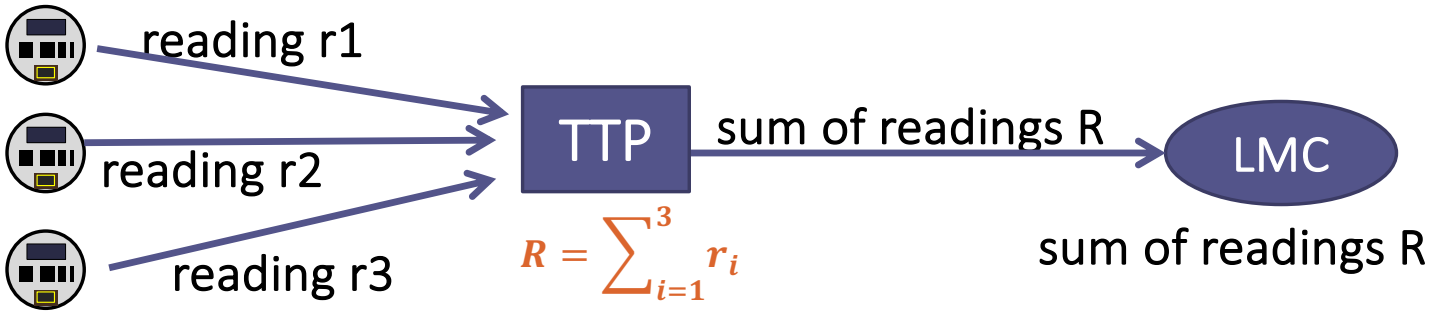
Load Monitoring - we do not need meter reading every minute



- 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

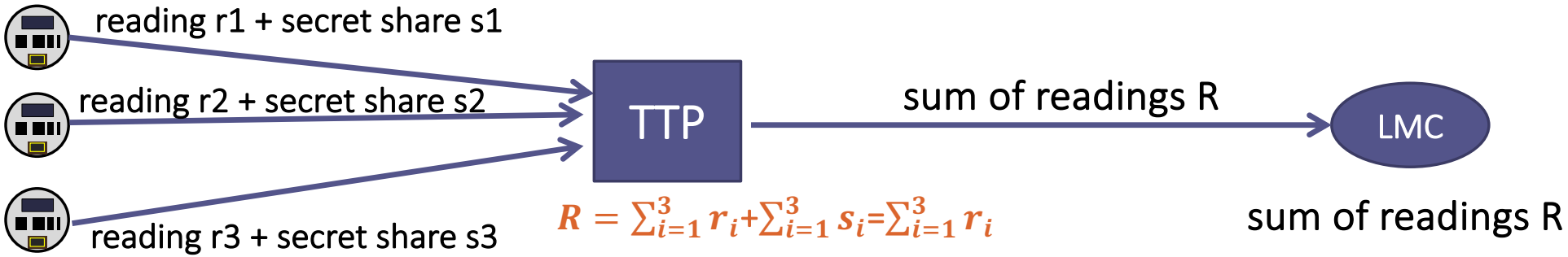
- Aggregation: data from individual users are aggregated and only the aggregated data are sent to the receiver.
- Privacy-preserving aggregation: the aim is for the LMC to receive the sum of readings from multiple meters without learning the readings themselves. Alternatively, the LMC only gets an aggregated result of meter readings while individual meter reading remains private.
- Q: any disadvantages of using this scheme?



- May not be scalable when there are 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?)

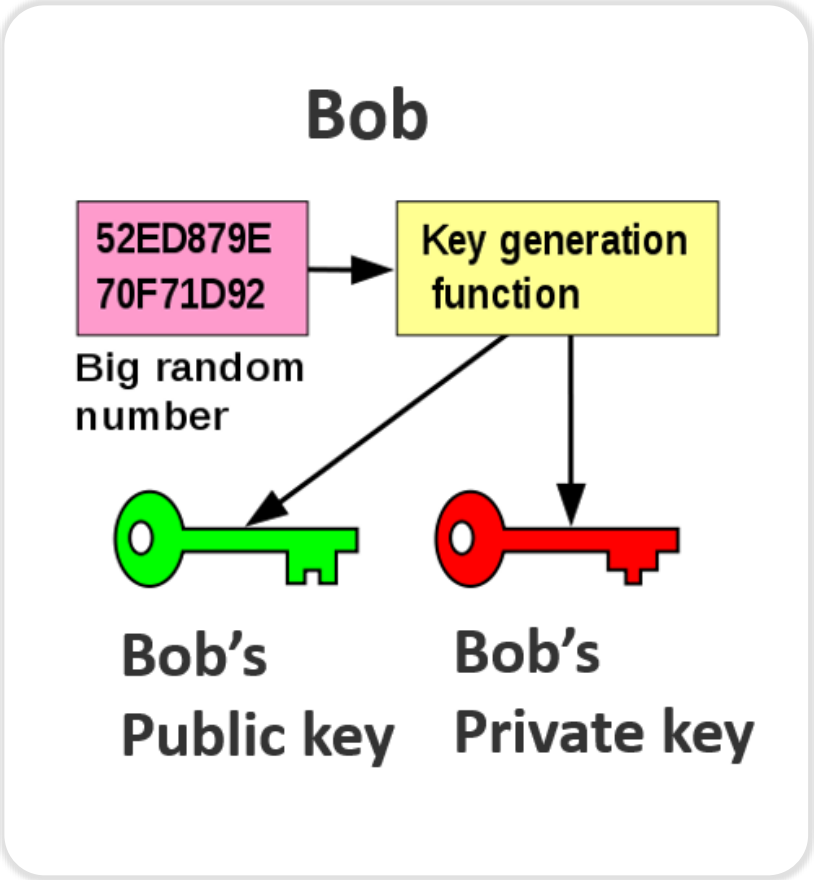
* Danezis et al, Smart Metter Aggregation via Secret-Sharing, SEGS´13, 2013, Bdrlin, Germany

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:

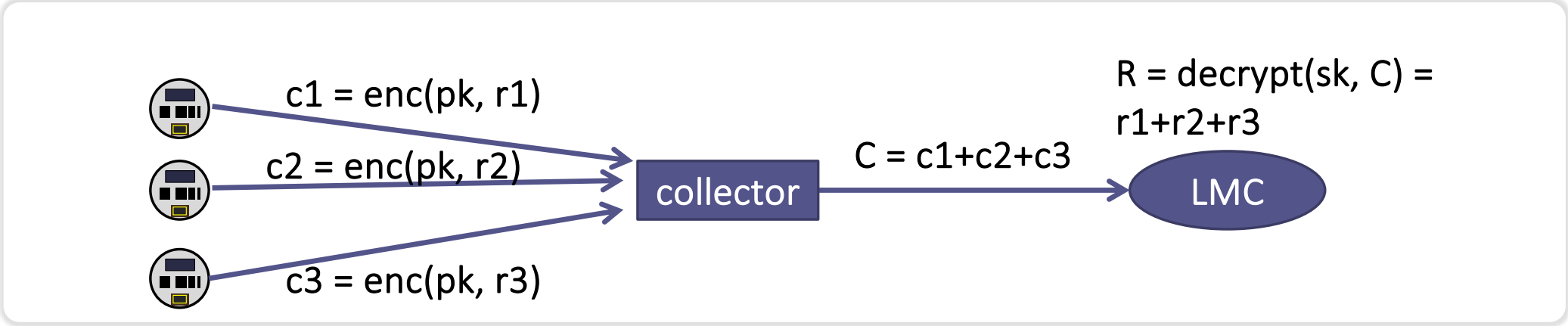
```
3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97
FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F
922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266
E2CD CB02 0301 0001
```

- Public Key: available to everyone via a publicly accessible directory and is typically stored on a public key infrastructure server
- 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 is trusted and 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 (the sum of the ciphertexts) to the load monitor center. The load monitor center decrypts the aggregated ciphertext with its own private key (sk in the illustration) to obtain the aggregated data of all smart meter readings.
- If you have interest to know more, check: homomorphic encryption (HE) system with additive homomorphic property



https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption

03

SMART GRID SECURITY

We focus on three attack types

- 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

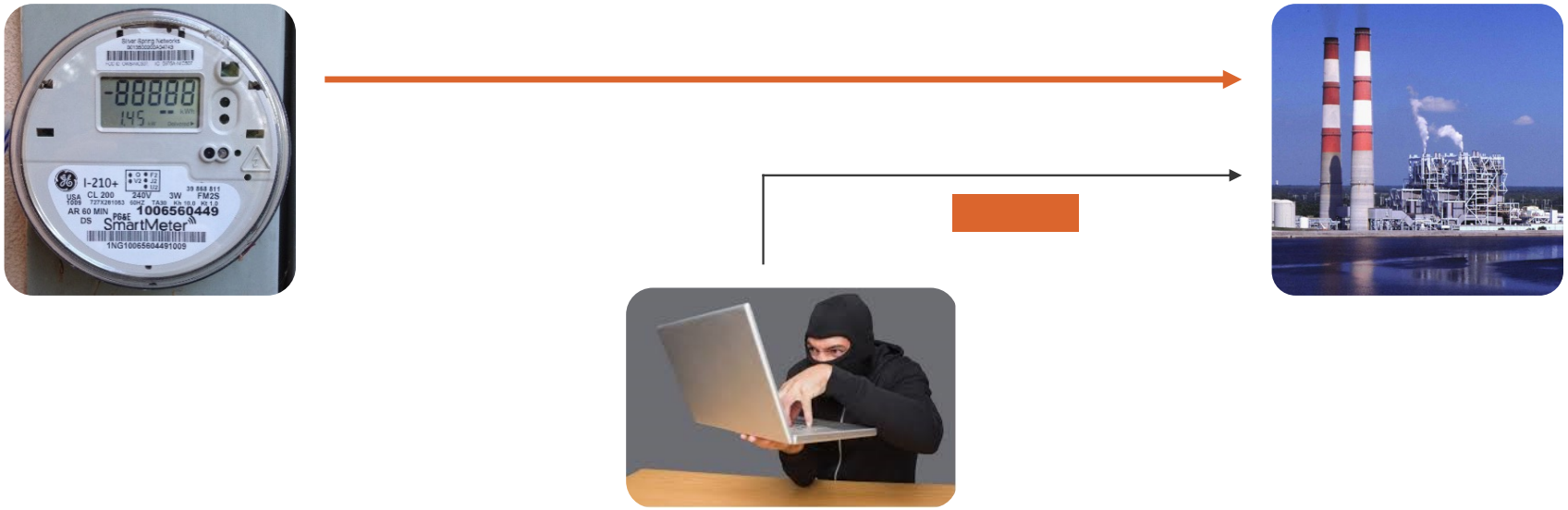
Replay Attack



- A 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

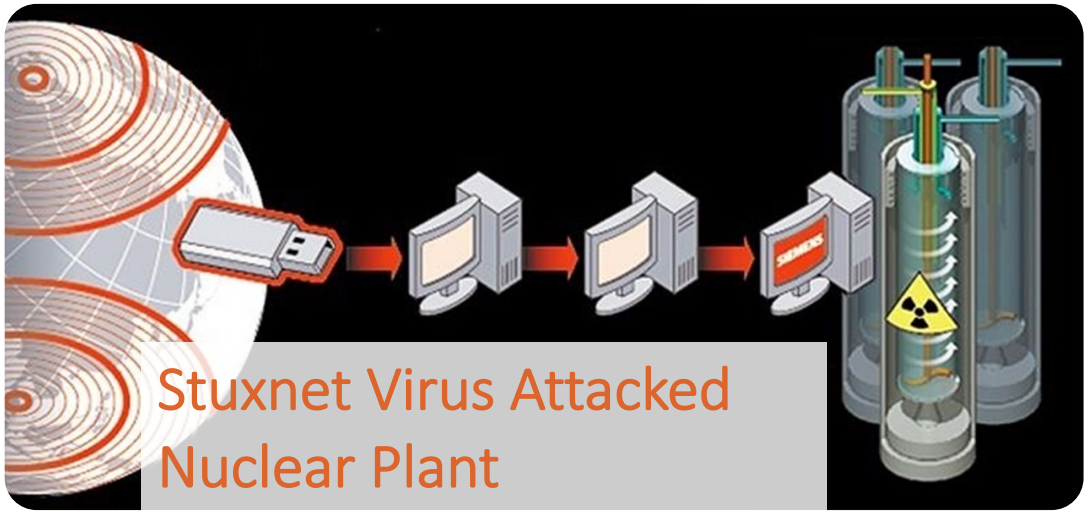


- The attacker replays (or retransmits) the data to smart grid control center.
- The attacker can make customers' smart meters appear out of order by injecting incorrect data (e.g., energy consumption data) to the system, which may lead to incorrect energy price or inaccurate prediction.

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; that could lead to power system instability
- The aim of the replay attack could be:
  - cause physical damage to the system
  - to steal energy: the valid energy consumption data is maliciously retransmitted with incorrect data

Replay Attack – an example



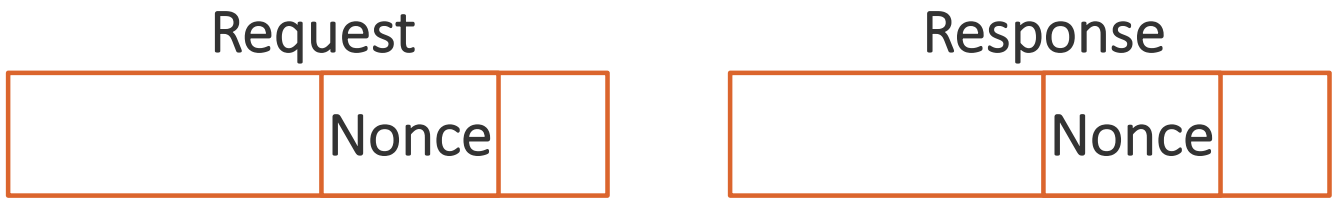
- Stuxnet is 500KB computer worm and allegedly designed as a cyberweapon against nuclear facilities.
- Stuxnet targets power supplies used to control the speed of a motor in nuclear centrifuges. The malware intercepts commands sent to the power supply from the Siemens industry control software and replaces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

Defending against Replay Attacks – adding timestamp and sequence number



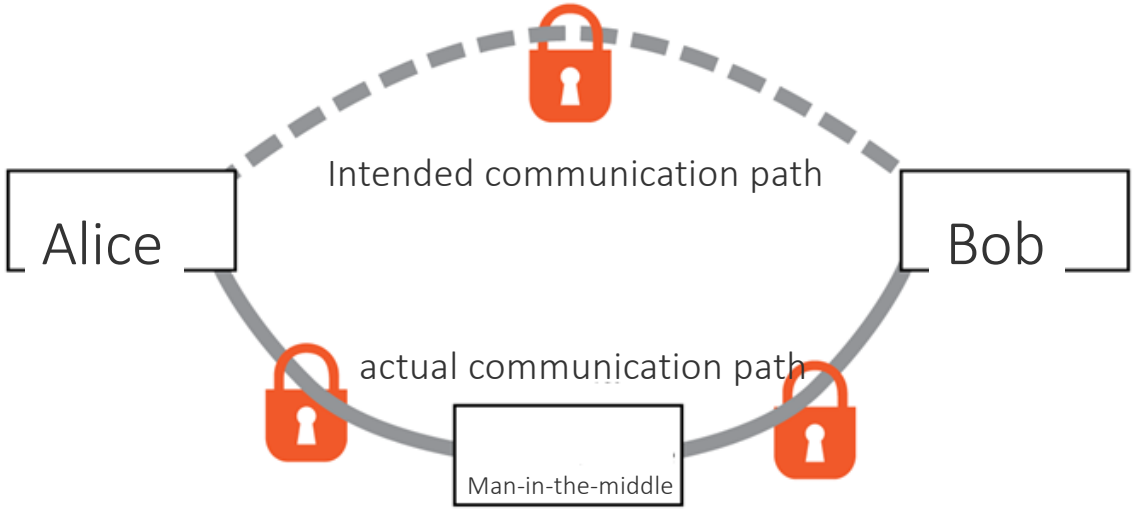
- Put a time stamp in each message to ensure that the message is “fresh”
  - Do not accept a message that is too old
  - Place a sequence number in each message
  - Do not accept a duplicated message

Defending against Replay Attacks – adding random noise



- Add random noise in request-response interactions
  - 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

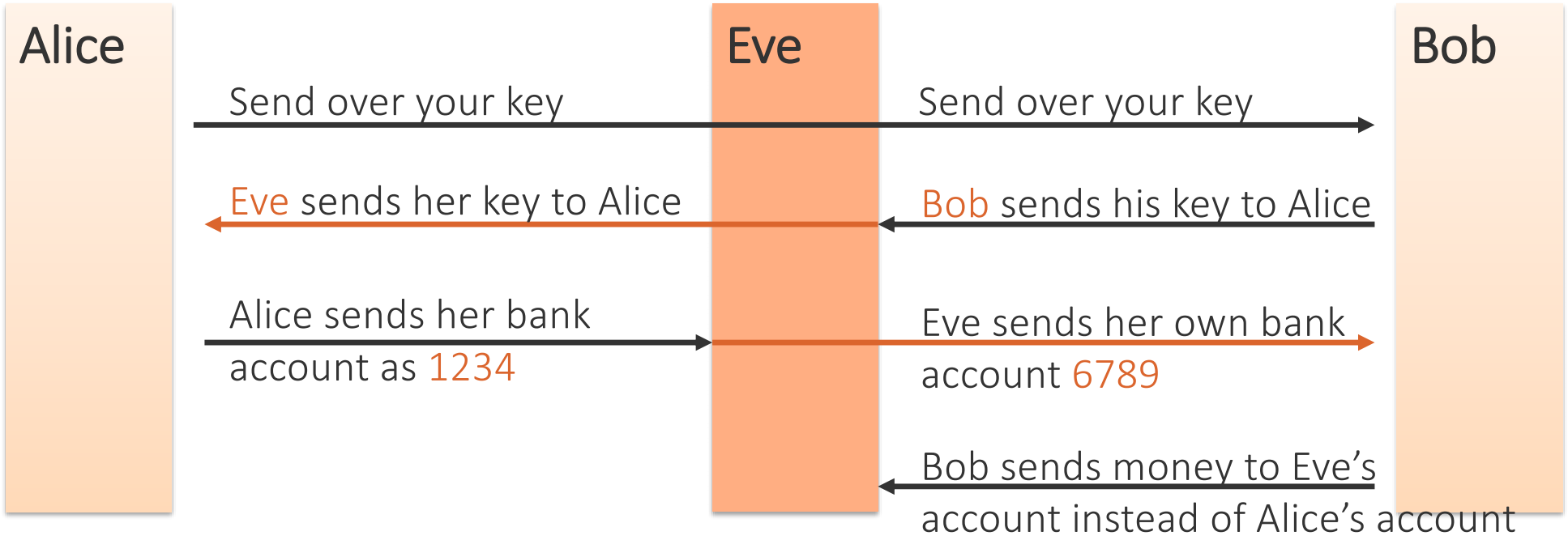
Man-in-the-Middle Attack – in general



- 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.

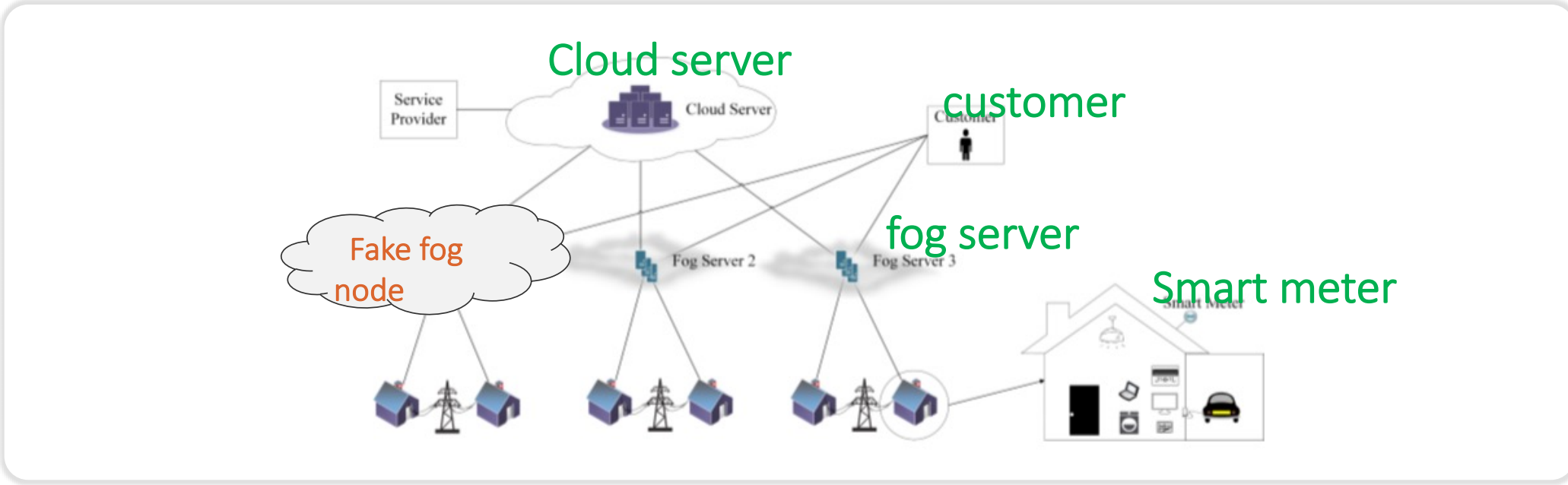
- Alice and Bob think their communications are end-to-end encrypted when actually there is a **perpetrator (Eve) positioned in a conversation between a user and an application either to eavesdrop or to impersonate one or both of the parties, making it appear as if a normal exchange of information is underway**. Eve removes the encryption, examines (or modifies) the unencrypted content then re-encrypting it before passing it on.

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.
- 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.

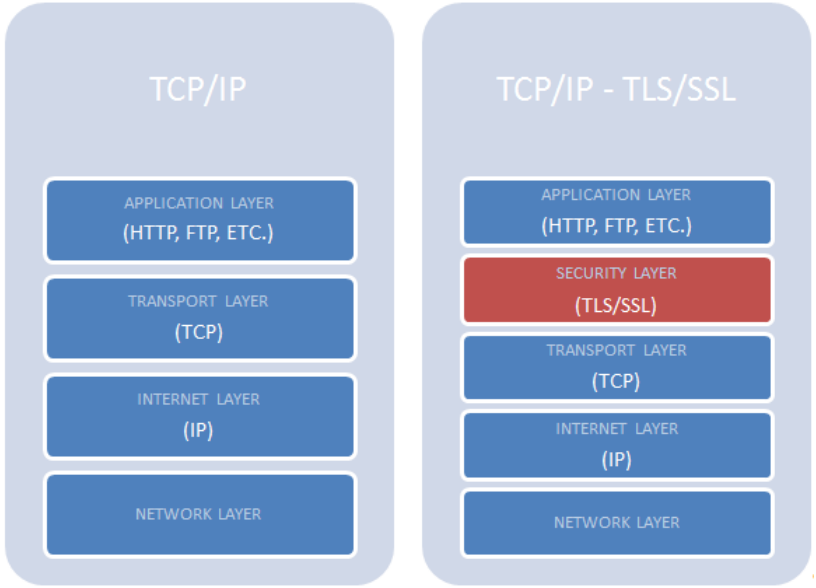
Man-in-the-Middle: Consequences

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

- If such attack launched successfully and undetected, the smart grid have the following problems.
  - Stability: a power grid that is under stress may appear to be normal to the operator. This delays the deployment of necessary measures to ensure stability.
  - Cost: a power grid operating normally may appear to be under stress to the operator. This causes costly remedial actions by the operator.

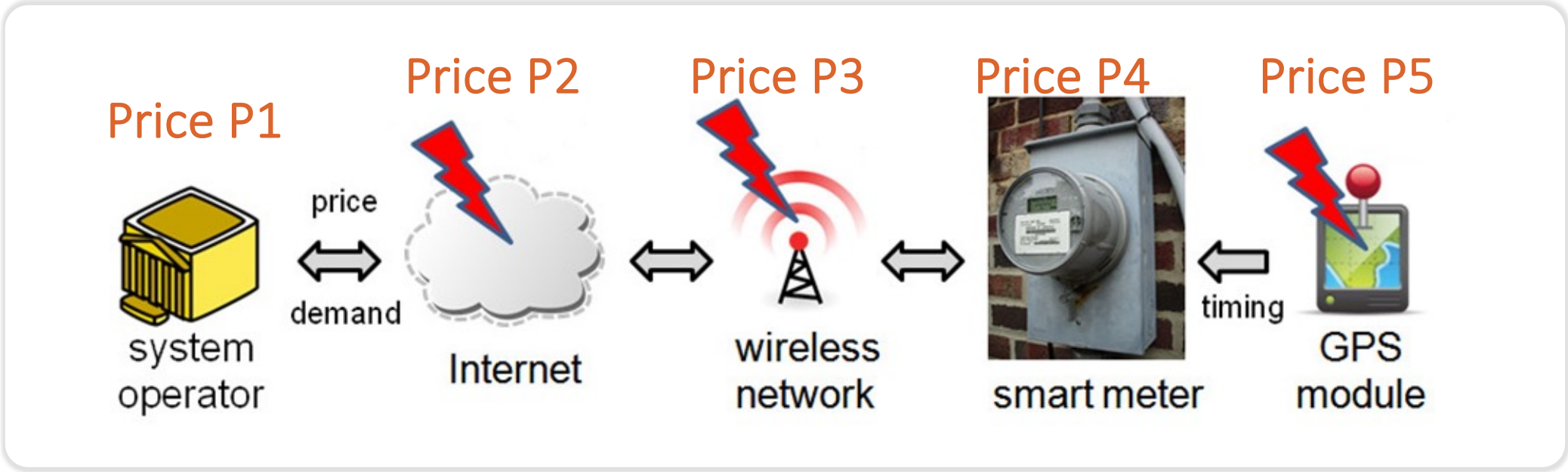
Man-in-the-Middle: Defense

- 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.

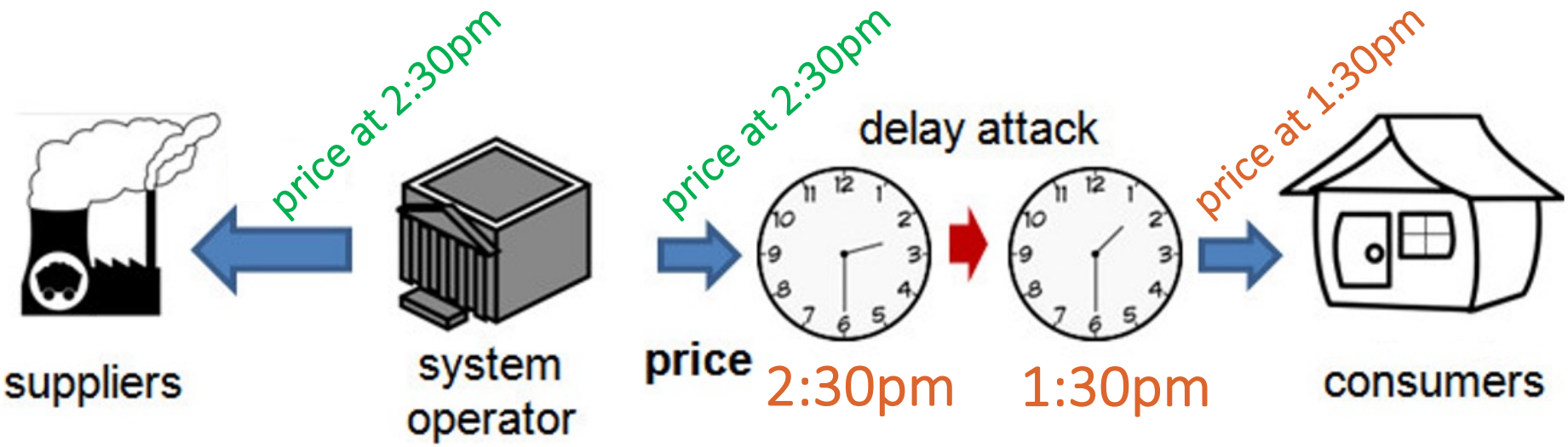
Integrity Attacks on Real Time Pricing (RTP)



- 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 blackouts.

- Delay attacks: the compromised price is an old price.

Integrity Attack – delay attack

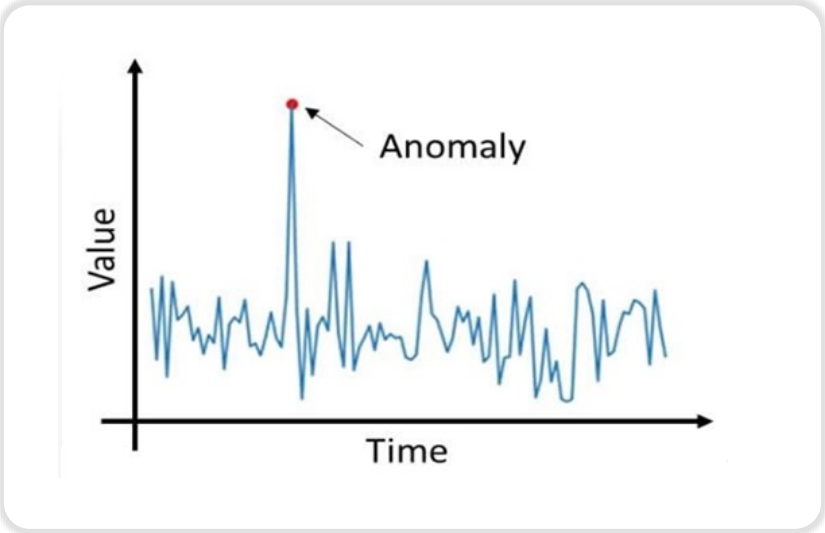


- The delay attack can be launched by modifying the smart meters' internal clocks. Attacks on the clocks can be realized by compromising the vulnerable time synchronization services in smart grids. Current commercial smart meters synchronize their clocks by built-in Global Positioning System (GPS) receivers,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

Defending against Integrity Attacks: 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 threshold, this value is regarded anomalous.

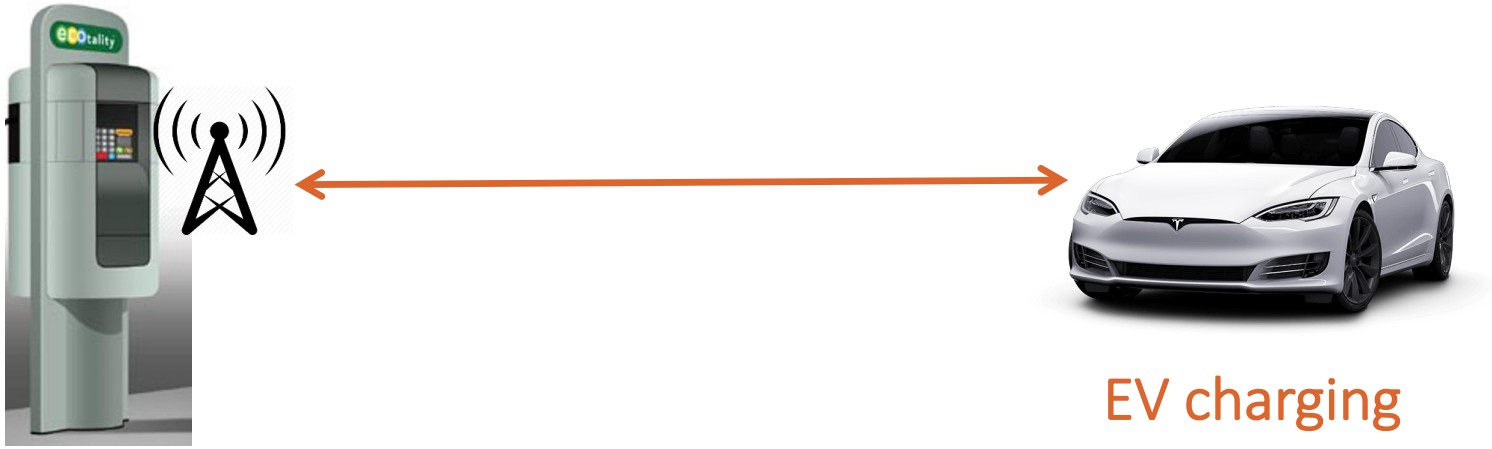


- Advantage: these schemes introduce very low overhead to the system
- Disadvantage: they fail to adapt to valid changes in the environment. Furthermore, a high level of professionalism is required to manually maintain detection thresholds.

04

MORE CONSIDERATIONS…

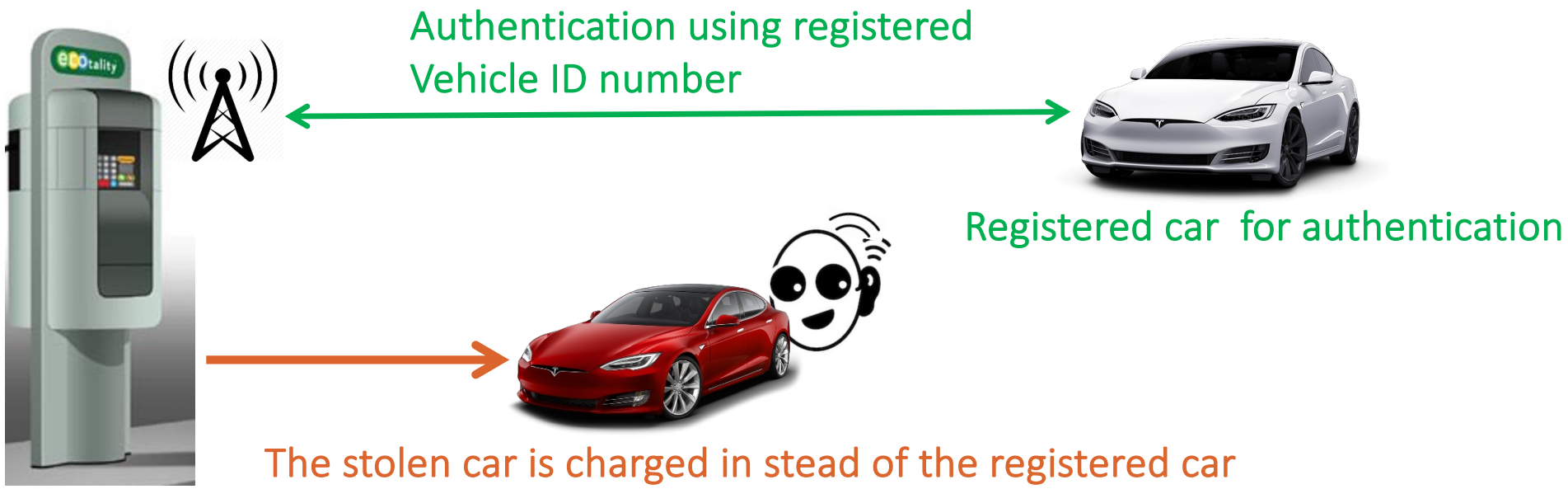
Charging Electric Vehicles (EV)



- In a typical charging scenario, an EV arrives at a charging station and requests a charging session. As stated by the standard IEC 15118, each EV must have a secret key stored in its ECU (*Electronic Control Unit)*.

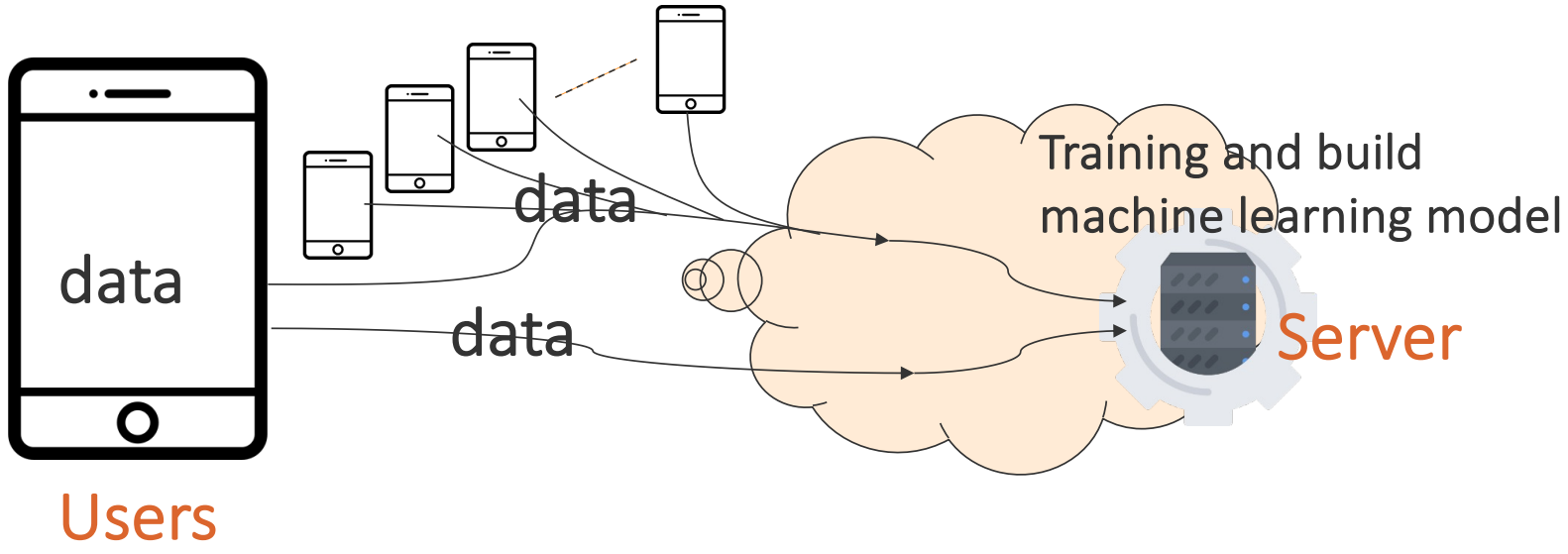
- If the control station verifies the car's key through wireless communication, the charging process can be compromised by a Man-in-the-Middle attack. (Q: please imagine the Man-in-the-Middle attack here?)

Man-in-the-Middle for Electric Vehicles



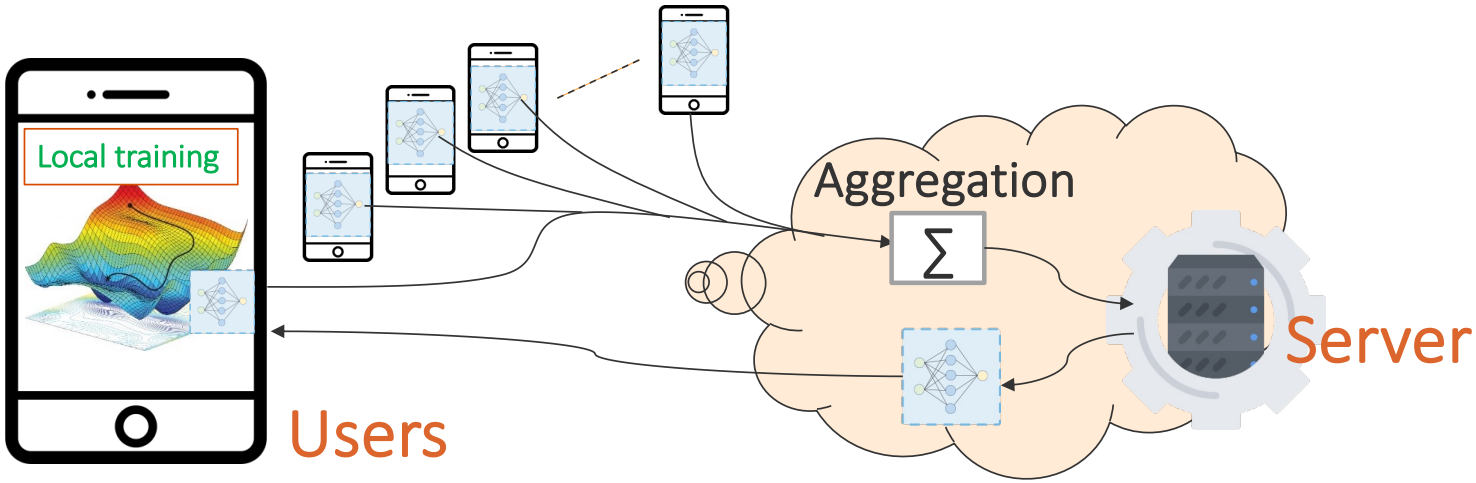
- A registered car with a valid key performs the authentication process. The stolen car eavesdrops on the conversation between the charging station and the registered car. The power goes to the stolen car instead of the registered car.

Current machine learning approach



- Machine learning: training on centralized datasets. Data should be sent to the central server. Users' private data (e.g., health record, location data) may be disclosed.
- Q: Please suggest a new solution that can protect users' private data in machine learning

Federated learning: concept



- Data owners train local machine learning models.
- Devices only transmit the model parameters to the server, not the raw data. The users' private data are kept locally in their own device.

References

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

- NISTIR 7628 Rev 1, Guidelines for Smart Grid Security Vol. 1, 2014
  http://dx.doi.org/10.6028/NIST.IR.7628r1