Vaasan yliopisto
UNIVERSITY OF VAASA

Österbottens förbund
Pohjanmaan liitto

Regional Council
of Ostrobothnia

Technical Report TR 5.3

Brief Report on Risks Associated with Customers' Access to Data – Insider Threat, and Ways to Protect Against Them

Vaasa Energy Business Innovation Center
VEBIC

Smart Energy Systems Research Platform
SESP

Bahaa Eltahawy

1 Description of the Case

In the current grid's implementation, data plays the most vital role since it is the enabler to the smartness level being added. Smart grid processes data collected from users' sides to get insights about their usage patterns and activities, and to prioritize/optimize operations in favor of providing the most adequate experience to users. Not only that, data would be used for internal processes too, and in many cases for commercial purposes. With these operations and advancements in mind, data criticality is no more questionable; however, the use of data goes with many doubts. As obvious, data here can play a second role, by revealing too much information about users, which leads to threatening and/or privacy invasion. Many standards, authorities, practices, and technologies are currently trying to solve for that issue: How data can be used to serve only for intended usage. In this brief report, we complete the work done with previous reports, and we focus more on the risks associated with data when being accessed by users or own employees.

2 Risk Assessment

Data would be always available at the operators' side, as they collect it for the operational purposes, and they hold full responsibility on processes and storage of data. Data access and critical information are protected and governed by many laws, standards, practices, and agreements. Once a customer signs for a service, he is entitled to follow these, and he gets acknowledged about acceptable and prohibited actions, alongside of his rights. This case is so idealistic and in many cases it can be worked around. For these, practices and security measures exist. Security measures are used to enforce protection regardless of any trials to break into the system or disobeying/violating the agreements. In reports **5.1** and **5.2**, these security measures were covered regarding networks and data storage.

With changes happening in this scenario, and with users holding control over data, security practices shifts to focus mainly on three aspects: Data security, Privacy, and Internal threat. It has been defined previously the following:

1. Data security ensures the integrity and consistency of data, protection in the form of confidentiality, and that data is always available to the right ones when necessary.
2. Privacy provides for absolute protection, by concerning advanced measures to protect the freedom of individuals from all sorts of unauthorized intrusion or the public's attention.

New to the list:

3. "An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business

> associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.”

Following the risk assessment criteria given in **Report 5.1**, the risks associated with users access to data would fall into one of two categories: accessing own data, and accessing others’ data. Accessing own data is how a user can monitor and control own information, settings, and preferences. This type of control is granted according to the service, as some services would allow viewing and monitoring only, while others would also allow editing. On the other hand, accessing others’ data is seen in terms of monitoring for equality, and transparency of services. This type of control does allow for editing on a hierarchical level only, i.e. higher level control.

Risks here would mainly include:

1. manipulation of data
2. destruction or removal of data
3. disclosure of sensitive data and Privacy

2.1 Data Manipulation

For own self, altering data could provide for misleading information, that would be the base for other forms of threats as repudiation, or if it is associated with settings then would give wrong results. For others’ data, the ability to view their data solely depends on its criticality, and the level of protection matching with it. Unless it is performed by operations, data modification of others is a severe security threat that shows shortage of access control protection, authentication, and accounting.

2.2 Data Destruction

Similarly, data destruction could affect operations that depend on data for their functionalities. This would tend to disrupt/disable services, and result with optimization and management issues. On a higher level, solely depends on the service, some services would allow for own data destruction upon termination of the service, while others would consider data belong to the service not to users; this follows the signed agreements. In the same manner, data destruction of others follows hierarchical control practices, in which same-level peers cannot such actions.

2.3 Sensitive Data Disclosure and Privacy

The worst case scenario could happen with the amount of information data can reveal about its owners. Here, data can be used to establish threats against individuals, by means of accessing it in trial of finding critical information or useful patterns to be used against its owners. These actions would depend on the level of data criticality, data visibility with others, data protection measures, and if data is in plain or anonymized. Confidentiality and Privacy are the most affected values out of such actions.

3 Data Protection

Previous reports extensively provided measures to protect data in all of its forms. Here, with users' access to data, the following measures need to be strengthened and highlighted more:

1. Effective and Enforced Security Policy
2. Hierarchical Encryption and Groupings
3. Least privileges Granted
4. Remote access monitoring for endpoint devices
5. Blockchain as a solution for consistent data distribution

3.1 Security Policy

Policies and procedures build the foundational practice for protection against threats. Policies should explicitly indicate the acceptable actions regarding data, the legal rights, and the measures taken to achieve protection. Practices will translate policies into implementable actions, specify technologies, processes, and skills required to get policies in action. Although these could be in place already, the main issue with policies and practices is effectiveness and enforcement. Policies and practices should be audited to make sure they are matching with the level of threat, and to rather ensure they are functional and working properly, as minor changes or deviation in a policy might render it unusable.

3.2 Hierarchical Encryption and Groupings

Hierarchical encryption targets data of users at different levels, or data with higher criticality. In brief, users would be classified according to their entitled services and features into different levels, and at each level encryption should be enforced. This will allow users (consumers, operators, analysts …) to only work with data at their level or other lower levels, but not a higher one. This would prevent peer to peer attacks targeting data breaches and manipulation. Additionally, some information are of higher criticality than others, e.g. personal or payment information, and thus it requires a different level of encryption. To facilitate these mechanisms, users and data should be set in functional groups that match the given criteria.

3.3 Least Privileges Granted

Separation of groups is the key to data protection of other groups. The more the groups and the separation criteria, the less is the breach surface in case it happens. One of the most concerns here is to provide for exactly the right functionality without any added ones. This goes with granting users the least privileges they would need to perform operations, and thus have tight data access control in place.

3.4 Remote Access Monitoring for Endpoint Devices

Endpoint devices normally reside out of the secure zone, and thus not all security measures would be applicable for them. These devices can perform operations or access data remotely, and with lower security profile in mind they can suffer from data breaches. Measures to be considered for this would include: enforcement of remote access security policy, continuous monitoring for remote access devices, and tunneling by means of VPNs for continuous encryption.

3.5 Blockchain as a Feasible Solution

The new and popular technology of Blockchain is handy to protect data among users while being distributed, thus protecting from many of the data breaches. Blockchain technology implements a distributed infrastructure for data, thus data does not reside at one place, but rather is shared equally among all peers. Additionally, with this implementation, encryption is in the core, thus data is only feasible to the ones who are entitled to it. Right configurations can specify the level of protection or privileges granted with data; as well data can be modified simultaneously at different locations, and stored in a distributed fashion which protectes against data destruction attacks.