Dynamic Energy Service Management at Home in a Secure Way

Reijo Savola, Pasi Ahonen, Mikko Rapeli, Anni Sademies, Jarkko Holappa, Timo Wiander, Kaarina Karppinen
VTT Technical Research Centre of Finland, Oulu, Finland

Abstract — Services and the technical infrastructures that enable them are showing a strong trend towards convergence and networking. The implementation of services is more and more often based on the use of telecommunication networks and databases. In addition, the management of electricity, water supply, district heating and gas services is on the threshold of a new era as the management systems become electronic, more versatile, more dynamic, and more international. In this paper, we analyse information security and privacy concerns in this new situation. Information security and privacy protection are important concerns for services that include payment functions and affect critical basic services such as water and electricity distribution.

Keywords — Energy services, information security management, digital convergence

I. INTRODUCTION

Subscription contracts and payments for electricity, water supply, district heating and gas have become commonplace for property owners and occupiers. For example, when a house is being built, a fixed amount of money according to the permitted building volume is paid to the local water utility for a water connection. Clear water and sewage are paid for according to use. District heating connections and heat consumption are similarly paid for. Issues such as choice of electric connection, applicability of connection size regarding customer use in all situations, as well as details of invoicing – like whether to choose a time-based or tariff-based invoicing – have to be agreed with companies in the field. Gas usage depends on cultural customs: in some countries the utilization of gas for household and property use has been minimal, but the situation is different in others.

As with the telecom industry, the distribution of electricity will be more comprehensively deregulated in Europe in the coming years. This will enable the development of ways of management for new kinds of dynamic and easy-to-use connections as well as the development of areas of business for the management of the ground energy distribution services. The goal of the deregulated energy field is to achieve better performance in the production and distribution of energy utilities by using the latest technology. For customers, this development means more accurate measuring of consumption, new ways for payment and easier competition among suppliers. The freedom of choice concerning electricity supply and diversification of energy supply services enabled by deregulation can already be seen in Finland, even if the deregulation process has been slower than thought. The situation is developing technically – for example, remote reading of electricity consumption is possible – but large-scale automation has not been achieved yet. This is partly due to the existing complicated
information systems and legislation that is restraining the development. Comprehensive field-specific standards do not exist, even if singular special standards like EDIEL [2] have been implemented. EDIEL defines electricity field message handling and is used for the exchange of the balance sheet status data.

Subscription to the services, and payment and changing subscription data are essential functions. The architecture is based on the use of common telecommunication networks and standardized protocols in a secure way. Common problems in these fields are the vast number and diversity of the required contracts, and deviations in the legislation and actors’ obligations in different countries. Cultural differences regarding service use and application also occur.

Where new technical management solutions in the field of electricity, water, district heating and gas supply are concerned, it must be noted that these fields are rather traditional and resistance to change can occur on both the customers’ and the companies’ side. Because of this, and the criticality of the services themselves, the new technical solutions have to prove their feasibility and usefulness in practise.

The main contribution of this work is an analysis of information security risks in electronic energy distribution services and a presentation of a new kind of architecture for the management of functions (energy, fluids, etc.) related to household and property administration and services.

The rest of the paper is organized in the following way. Section II discusses the convergence of energy services and Section III analyses their information security risks. Section IV presents the SHOPS architecture and authentication data management. Finally, Section V discusses future work and Section VI gives conclusions.

II. CONVERGENCE OF ENERGY HOME MANAGEMENT SERVICES AND INFORMATION SECURITY MANAGEMENT

The current trend is that services are becoming electronic, networked and convergent, both technologically as well as commercially. The implementation of services is more and more often based on the use of computer-based automation, databases and telecommunication networks – usually based on Internet protocols. This phenomenon has lead to a situation in which there can be a rather complicated network of actors behind the service. In order to ensure the reliability and security of this network, there is a need for comprehensive solutions beyond corporation boundaries.

One of the problems with closed environments has commonly been the lack of security thinking. A false sense of security is easily born when the whole network is handled by a single organization and no hostile parties are assumed to be located in the network. The main characteristics of the convergence threat can be seen as the switch-over from closed networks to open systems, which causes network traffic to spread in unplanned and untested ways. The data in converged systems is transferred between different network environments and a false message can cause problems in some networks because of system defaults or errors.

Since the beginning of the 1990s, IP protocol-based system solutions have been widely used in information transfer. The IP protocol’s main advantages are scalability, independency of physical network and reliability of routing model. The Internet consists of joined IP networks and connecting a physical device to the Internet means that it is
connected to the network using an IP protocol as a network layer for information transmission.

Despite its advantages, the TCP/IP protocol family is not very resistant by design. It has been designed to cope with hardware failures but not to act against attacks inside the network. In the design phase of TCP/IP it was assumed that all the devices in the network could be trusted, so security issues were left out. IP standards are still being developed but unfortunately this can also cause security problems. Several experimental techniques have been introduced and are being used in a way they were never meant for. In addition to increased reliability, the distributed management and routing techniques can also transfer faults to a widespread area. The burden of history is that IP networks were originally designed to be totally open. Table 1 lists some common information security threats connected to IP networks.

A satisfactory information security level can be problematic to find where different types of networks are used within convergence. For instance, the Internet is an open and uncontrollable system, whereas many networks that are connected to it, such as television and phone networks as well as production control systems, have been administrated in a closed manner. The problem in the closed systems is a lack of security-oriented thinking and actions. When a closed network has been administrated by one company and there do not appear to be any hostile parties in the network, it easily creates an impression of reliability and security. However, the security is questionable, when the system is connected to open networks, if the incoming Internet-type threats are not acted upon.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Internet threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreliable user action</td>
<td>The user name – password guessing by using dictionaries.</td>
</tr>
<tr>
<td></td>
<td>Eavesdropping on the unsecured connections in order to gather user names, passwords or other sensitive information.</td>
</tr>
<tr>
<td></td>
<td>Social engineering attacks in order to gather sensitive information (for example, asking for passwords on the phone).</td>
</tr>
<tr>
<td></td>
<td>Active content and plug-ins in web browsers can cause crashes, information leakage, spreading of viruses and malware, dialers calling to expensive foreign numbers, and privacy violations.</td>
</tr>
<tr>
<td>Insufficiencies of the network or the system (the user can be involved)</td>
<td>Faked network addresses in order to access sensitive information or avoid identification methods.</td>
</tr>
<tr>
<td></td>
<td>Connection hijacking in order to access sensitive information or break in.</td>
</tr>
<tr>
<td></td>
<td>Spoofing in order to defame the sender or break into the system.</td>
</tr>
<tr>
<td></td>
<td>Breaking into the system by taking advantage of the vulnerabilities in network programs.</td>
</tr>
<tr>
<td></td>
<td>Denial-of-service attacks, especially distributed attacks made with several devices.</td>
</tr>
</tbody>
</table>
Attacks against the DNS (Domain Name System) service, for example inserting faked information into the server cache, flooding it with faked replies or completely hostile DNSs. Resource-consuming spam, choking of the systems with a large amount of traffic, forged messages or header information and distribution of malware.

The implementation of different networks’ information security properties also differs considerably from one to another. If, for instance, a mobile phone network’s information security properties are to be utilized, one has to understand their restrictions, such as strong trust in the circuit-switched network elements, and a secure area must be implemented, which is often restricted to the air interface.

A good rule of thumb is that the applications’ TCP/IP data transfer has to be encrypted in public networks, for example, with the IPSec, TLS/SSL, SSH or SFTP protocols. Implementing information security solutions usually requires reasonable system resources. In practice, this means that the system requirements cannot be scaled just by concentrating on the core functions of the branch and applications; preparing for capacity requirements required by the information security properties is also sensible.

A common misconception is that information security problems could be totally solved with technical security solutions, such as encryption techniques, firewalls or anti-virus products. In reality, the technical solutions are an important part of information security management, but only a part of the solution. At best, functional technical information security solutions only transfer the original problem – for example from securing telecommunication to securing the encryption keys used in data traffic encryption – and the problems finally affect the behaviour of the users of the technical solutions, the end users, producers, employees, corporations and authorities.

The main objective of information security management is to implement a good and efficient information management way-of-conduct and to create a sufficiently basic level of security. Information security management is needed to protect against threats and damage caused by hardware and software faults, and natural events, as well as deliberate, negligent and accidental acts. Information security is based on the following three basic concepts:

- **Confidentiality** – information access and disclosure is limited to a set of authorized users, and access by or disclosure to unauthorized users is prevented.
- **Integrity** – the information and information resources are trustworthy, correct and up to date, and are not changed or destroyed by hardware or software faults, natural events or unauthorized acts.
- **Availability** – the information and services connected to them are available to authorized users.

In addition, the following security functions are essential for information security management:

- Detection, prevention and avoidance of malpractices,
- Countermeasures, survivability and intimidation.

Controls can be created in order to implement security functions in the information system: policy, method, practice, or a device or programmed mechanism.
Information security management sets various requirements for networks, servers, hardware, software and methods. Simultaneous handling and adequate management of all of these is challenging, sometimes even impossible, and rather depends on the application area. Acting in a secure way requires constant recognition, management and minimizing of risks [5].

III. RISKS OF ELECTRONIC ENERGY DISTRIBUTION SERVICES

Taking care of information security places various requirements on networks, servers, hardware, software, systems and procedures. To be able to employ and manage them simultaneously is difficult, sometimes even impossible, and is directly related to the corresponding application area. This means that in order to have a functioning system, the risks to the current situation have to be identified, managed and minimized.

A. Industry-Specific Risks

When industry-specific information security solutions are being developed, it is important to conduct as comprehensive risk analysis as possible covering that specific industry. Risk lists can easily become excessively long and the threats are strongly dependent on each other. General threats or even information security threats targeting a certain system can never be conclusively handled in any development project, so it is good to be prepared for changes concerning the threats and their technical solutions.

Even the risk identification phase at an adequately accurate level requires at least a good understanding of the application area, the technical system and the different interdependencies. In addition, improving the understanding of the application area and technical solutions induces an understanding of the new threats and vulnerabilities that have to be acted upon during the system’s use and maintenance.

Examples of industry-specific risks related to electricity subscription and payment include:

- The electricity consumption address is incorrectly registered,
- It is not possible to deliver electricity to the consumption place on the agreed terms,
- The wrong service is delivered (e.g. general electricity),
- The electricity is not delivered at the agreed time,
- The payment has gone to the wrong electricity company,
- An incorrect amount of money has been paid,
- The electricity is switched off for no reason, and
- Excessive invoicing costs.

B. Risks Similar to Other Networked Services

Electronic energy distribution services include very similar general and information security risks as other networked services [1]:

- The complexity of the terminals and the number of interfaces increases, leading to reduced reliability of the software and growth of the surface that is subject to vulnerabilities,
• No preparations are made for networks in information systems being connected to each other, for example a closed IP network getting connected to an open IP network,
• The user logs in to a false (e.g. hoax) service or the service does not authenticate the user correctly.
• A payment transaction or submission cannot be considered indisputable (e.g. claimed that a child has been playing with the computer),
• The level of information security may decrease when new updates or features are added to the system or its parts – on the other hand, if the programs are not updated, the closed system they are in is exposed to the threats that would have been fixed a long time before in an open network system,
• The user information spreads due to unprotected and careless actions, and
• In some points of the value chain there are unreliable actors that endanger information security, privacy protection or financial shelter.
• The system is not sufficiently easy to use or compatible with other corresponding systems, such as payment systems.
• The information system development and administration can be too complicated to be secure.
• The legislation obligations are not familiar enough, or it is too difficult to quickly to correspond to new legislation.

From the service developer’s perspective, a new financial risk is the investigation of the non-repudiation of transactions, which can be laborious and prolonged, and can cause loss of income. It is important to define and state inform beforehand how a service user is responsible for the expenses that criminal activity such as stealing a mobile device or fraud can cause via use of the service. It is the user’s duty to be aware of who is using his/her device and how – and to inform the responsible quarters if he/she no longer possesses the device.

There can be threats and problems in each phase of the system and service development. Threats can be generated during the design phases by situations where a certain technology is used even though the risks are big in that technology – or automation is not exploited. The core phases are the requirement specification and system design phases. The implementation phase can incorporate various problematic issues - e.g. software bugs and wrong kinds of connections between modules. Threats are also generated by the supporting systems. These threats are due to weak programming languages and weak development tools – both of which can be trusted too much. Threats can be generated during the system design by wrong assumptions regarding the system environment and human behavior, as well as faulty models and simulations. It is possible to carry out the wrong kind of testing during the implementation analysis phase and there can be errors in software debugging practices. Some general problems in development are a lack of capable human resources (e.g. slowness in absorbing new maintenance practices), rush and defective documentation.

The level of information security often changes during updates and interconnection of components. Moreover, there are threats in disposal of services, like a premature shutdown of required components and a hidden dependence on a non-existent older version. A big threat is lack of security awareness on the part of the developers. Other threats include the short-lived operation of a stakeholder, resource allocation problems and an insecure service development process.
C. Categorization of Risks

In order to ease handling, risks can be categorized according to different types of parameters, such as criticality and sensitivity. In addition to recognizing general and field-specific risks, the threat classification and analysis can also be based on the detection of different dimensions of security, such as confidentiality, integrity, availability and authentication. Examples of defective solutions for the different dimensions of information security management include:

- **Confidentiality**: confidential customer data, such as old invoicing and pricing data or consumption profile, end up with a new electricity retailer,
- **Integrity**: defective verification of data integrity may lead to a transfer of false measurement data, or misrepresentation of given account data,
- **Authentication**: if authentication of identification of the user and the service is not implemented correctly, the service can be accidentally ordered from a wrong place, or the user may indicate a wrong payer for the service.

D. Preparing for Risks

After the information security risks are detected it is good to attach estimates of their implementation probabilities and losses caused by the implementation to them, just as is being done in risk management. After this one can analyze which threats it is reasonable to pay more attention to in order to minimize possible losses. Especially important – even though difficult – is to define the value of the information. For example, important data on the money and material flow are far more important for the corporation’s core business than employees’ personal email, unless the email is moving the data. Disturbances in the core business will directly affect the company result, so investment should be made in its protection.

One somewhat hidden problem is that different actors estimate the value of information in different ways. For example, information that is valuable to the end user, such as names, addresses and social security numbers, can be almost worthless from the service providing company’s point of view. In this situation the company does not consider protection of clients’ information important without separate legislation requiring it. The same applies to actions between companies, especially when the companies handle information on a third party – such as credit card information. However, there is quite extensive legislation concerning companies and consumers in Europe that protects consumer and obligates companies, whereas legislation concerning actions between companies is lacking.

One way to proceed with risk analysis is the following:

- **Define the purpose of the risk analysis**: What is the benefit of this analysis?
- **Define the type of risk**: What kinds of risks are sought (e.g. information security risks, personnel risks...)?
- **Analyze the domain**: How is the analyzed system delimited? Who and what are included in the system and how do they affect the system? What assets must be protected (concrete or immaterial)?
• **Identify risks and risk sources:** What kinds of risks related to the assets can exist in the system? In what ways can the risk be caused? Could these sources of risk be classified?
• **Make a risk path:** Build a sequential event path from the source event to the realized risk.
• **Assess the risk’s criticality level:** How critical is the risk?
• **Assess the risk’s sensibility level:** Who should be informed when the risk is realized?
• **Dependencies between risks:** Are there any common causes or consequences between different risks? Could the same kinds of risks be integrated?

These phases are not necessarily consecutive; they can be reverse or cyclic depending on the progress of the analysis and achieved benefits.

IV. SHOPS SYSTEM

The SHOPS (Smart Home Payment Systems) [5, 6] research project (part of the Eureka-ITEA cluster) defines the general architecture, and enables the use of different types of electronic terminals for the management of functions related to household and property administration and services.

A. **Authentication Data Management**

The service chain has to efficiently and securely manage who has access to the network and services, from where and what kind of actions can be performed. If this is neglected, part of the information security can be jeopardized. In services related to energy distribution that are targeted at end users, the user identity encompasses a lot of information, whose confidentiality and integrity has to be maintained for legislative reasons. When the customer changes the electricity retailer, the information passing from one electricity retailer to another requires implementing value chains according to the law and business models, including the technical solutions. These technical solutions include the user identity management and related data which can be implemented with, for example, Liberty Alliance [3] standards. The Liberty Alliance project is working on an open technical standard that enables the implementation of authentication data management and Single Sign-On (SSO) for several services.
Many existing services use a user ID and password for user authentication in the network. In the Liberty architecture those service providers that have the necessary commercial contracts can belong to the same federation, in which case they can share authentication data with each other, as long as the user allows that. Liberty also aims to maintain the compatibility in older software and hardware systems and to be platform and hardware independent.

Single sign-on is a way of managing the user authentication in a centralized manner when the user wants to use several service providers’ services. This is beneficial from the service provider’s point of view as the changes to the information security properties of the authentication service can be done in one location and the users do not have to remember several passwords and user logins. On the other hand, the administration can manage the authentication data through one connection, from where the changes are updated to all the services, using a single sign-on. The single sign-on server keeps track of the login attempts. This reduces the service provider’s efforts, as there is no need to consider access control–related collection of the log files in the design stage.

The single sign-on process includes three parties: Identity Provider, (IdP), the user (Principal) and the service exploiting the single sign-on (Service Provider, SP). At first, the principal requests a www page from the service provider (Stage 1 in Figure 1). The service requires user authentication, which is implemented as a single sign-on system (Stage 2). The user is redirected (HTTP Redirect) to the single sign-on server, which the user sees as a login window (Stage 3) and the user logs in (Stage 4), if has not yet been done. The server responds by using a cookie or by creating an authentication ticket, which is delivered to the original service provider (Stage 5). The service provider and the
authentication server ensure the data of the authentication ticket, after which the user is authenticated and is ready to use the service. If the user wants to use some other single sign-on service, the service notices that the login has already been accepted and the service use may start immediately.

B. SHOPS Architecture

The SHOPS architecture primarily uses standardized solutions and the functionality can mostly be implemented with software – see Figure 2 for the SHOPS system architecture demonstrator concept.

The actors in the SHOPS system are: (1) end user, (2) retailer, (3) distributor, (4) supplier, (5) payment broker and (6) telecom operator. The actors can be formed according to the communication hierarchy, which describes the communication between them – see Figure 3.

![Fig. 2: SHOPS Demonstrator](image-url)
The consumer can subscribe for time-limited electricity delivery from the service provider and pay for it either in advance or afterwards. The subscription can be done using different kinds of terminals and it can cover various services.

The SHOPS research project exemplary application enables real-time follow-up of electricity consumption data in a secure way. The service providers the consumer sees use Liberty standard protocols and have combined their existing user authentication methods in a Liberty federation. This enables the user, according to his/her choice, to combine the authentication methods used in several services and utilize a single sign-on for all the services of the federation.

The electricity meter and the background system are traditional closed systems. The HTTP server is written with Python that is offering the service and applications running in the server. The server combines the data from the electricity meter and background system with the signed-on user. User signing and verification are taken care of by the Liberty standard-compliant Service Provider (SP), which redirects (HTTP Redirect) the user to authenticate in Identity Provider (IdP), which, in the test environment, has been implemented with a LASSO library [4]. LASSO is an open C source code library whose aim is to implement Liberty Alliance standards. Service use and Liberty sign-on use HTTP 1.0 and HTTP 1.1 protocols. In addition, the user connections between the application and the Liberty components have been protected with TLS protocol (Transport Layer Security) and the user verifies the servers with certificates.

According to the Liberty standard, the Service Provider (SP) and Identity Provider (IdP) exchange the XML-based SAML messages (Security Assertion Markup Language) needed in user authentication with the SOAP protocol (Simple Object Access Protocol). The TLS-protected and certificate-verified HTTP acts as the transport layer.

Because the service’s user interface only requires HTML, HTTP and TLS support, the service functions with several different terminals, such as PC, palmtop computer, mobile
phone or digital TV. Due to the features of the digital TV and mobile phone browsers, the service use may also require also the use of proxies, but the Liberty standards have considered this already.

V. FUTURE WORK

In the future phases the exemplary application will be extended so that the user authentication could happen using several methods allowed by Liberty, such as electronic ID cards. In addition, the Liberty architecture’s application development is supposed to be documented and simplified. There are plans to extend the application-dependent functionality so that electricity distributor change would be possible, for example. This is challenging because changing the distributor encompasses many contract-related and legislative obligations that have to be taken into account in the solution.

VI. CONCLUSIONS

Energy distribution services, as well as other home services, will become electronic, more dynamic and easier to configure and manage. Information security concerns for services like this that include payment functions and affect critical basic services such as water and electricity distribution.

Satisfactory information security management of networked services requires a comprehensive understanding of the value networks of the service, the technical infrastructures used, and the cross-relationships between the risk factors.

Threats due to digital convergence can be partially mitigated by experience gathered from implementation and network security in the Internet world. A lot of trouble can be avoided if the lessons learned can be exploited when developing new software, interfaces and networks.

The SHOPS research project exemplary application enables real-time follow-up of electricity consumption data in a secure way. According to his/her choice, the user can combine the authentication methods used in several services and utilize a single sign-on for all the services of the federation.

REFERENCES


SHOPS (Smart Home Payment Services) Eureka ITEA Project: http://www.shops-itea.org/Shops/Home.html.