UNIVERSITY OF SOUTHERN CALIFORNIA

Semester Project

Fall 2015 INF 522 – Policy

Course Instructor:
Prof. Dr.Tatyana Ryutov
USC Information Sciences Institute
4676 Admiralty Way,
Marina del Rey, CA 90292

Project by:
Sandeep Kadagathur Vadiraj
Masters in Cybersecurity
USC ID: 8998-3394-34

EXECUTIVE SUMMARY:

In the world of computer security, mechanisms to implement the policy are always changing. The deeper understanding of the security policy gives us an understanding that the security is the fundamental aspect of the design of a system and is not a, add on feature. The security policies when implemented properly can protect the triads of information security i.e. Confidentiality, Integrity and Availability. Accurately applied, information security principles may help incident handlers reduce the number of attacks on the infrastructure, or address privacy issues of information collected by the smart-grid infrastructure.

This document is intended as a recommendation document for the exchange and processing of actionable information gained from the smart-grid infrastructure. The report is relevant to designers and implementers in all types of organizations adopting Smart-grid infrastructure. The goal for this report was to touch on a wide variety of challenges that should be addressed in the area of protecting privacy of the data obtained from the smart-grid technology in accordance with the California Law AB-1274. Another goal of the report is also to outline the security policies to the human language policies provided by the law.

The Smart Grid brings with it many new data collection, communication, and information sharing capabilities related to energy usage, and these technologies in turn introduce concerns about privacy. Privacy relates to individuals. Four dimensions of privacy are considered: (1) personal information—any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity; (2) personal privacy—the right to control the integrity of one's own body; (3) behavioral privacy—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and (4) personal communications privacy—the right to communicate without undue surveillance, monitoring, or censorship. This project report will highlight the security policy implementation in the smart-grid system, to enforce and implement the California law AB-1274.

INDEX:

INTRODUCTION:

A smart grid is a system which includes a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficiency resources. Electronic power conditioning and control of the production and distribution of electricity are important aspects of the smart grid. Thus, it becomes one of the nation's high value assets for guarding against the attack by the adversaries. The high-level overview of the smart-grid is as shown by Figure 1.

Cybersecurity applied to Smart-grid infrastructure must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, terrorists, and other adversaries, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Security must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition. Systems for critical applications need to withstand cyber security events with no loss of critical function.

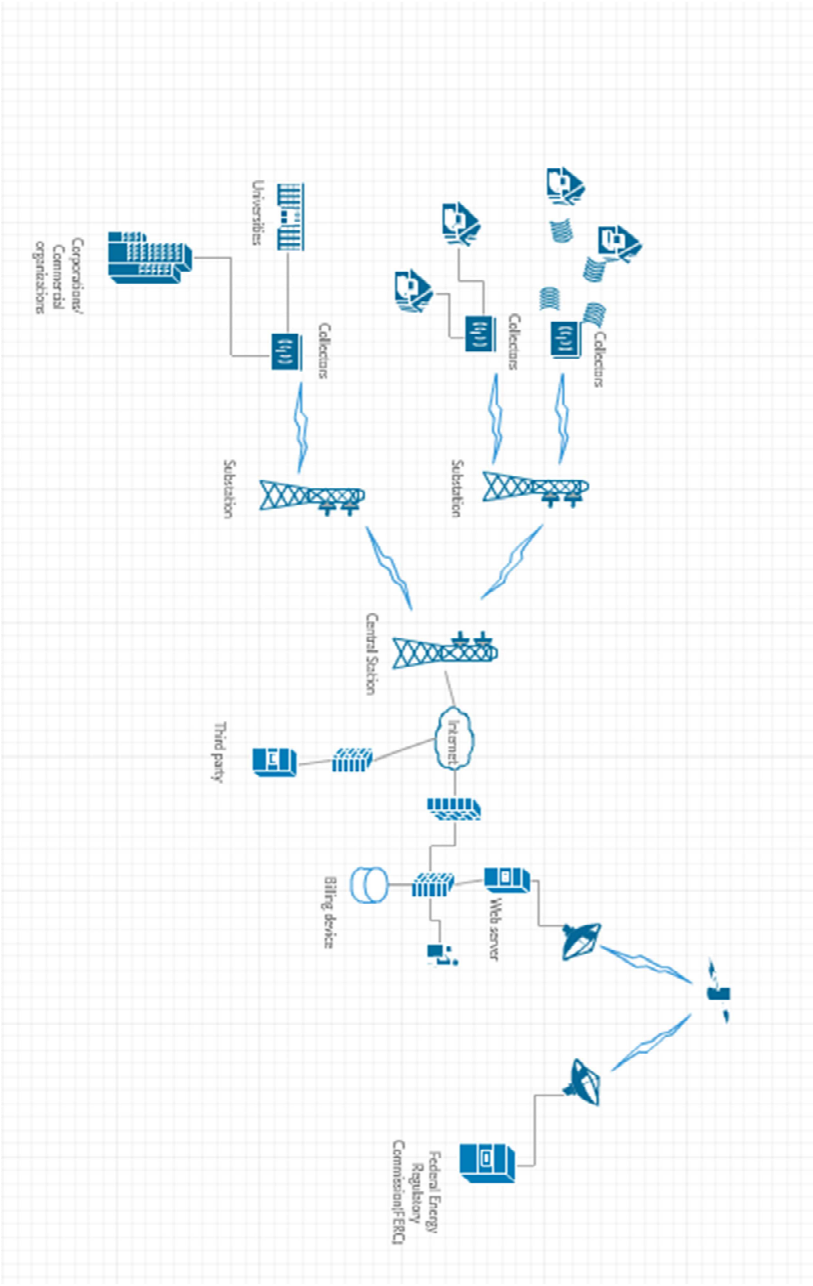
To help support the modernization of the Nation's electric system consistent with Title XIII of the Energy Independence and Security Act of 2007, the Federal Commission is focusing on issues associated with a smarter grid. Smart Grid advancements will apply digital technologies to the grid, and enable real-time coordination of information from generation supply resources, demand resources, and distributed energy resources (DER). The Commission's interest and responsibilities in this area derive from its authority over the rates, terms and conditions of transmission and wholesale sales in interstate commerce, its responsibility for approving and enforcing mandatory reliability standards for the bulk power system in the United States, and a recently enacted law requiring the Commission to adopt interoperability standards and protocols necessary to ensure smart-grid functionality and interoperability in the interstate transmission of electric power and in regional and wholesale electricity markets.

Based on the necessities expressed by the federal agencies many state legislatures passed legislation for guarding the critical Smart-grid infrastructure and also the information obtained from deploying the infrastructure. At least 13 states considered 31 bills this session that address smart grid technology. Seven states—California, Illinois, Maine, New Hampshire, Ohio, Oklahoma and Vermont—enacted legislation on the issue.

Six states are considering or enacted laws to promote smart grid deployment: Illinois, Massachusetts, New Jersey, New York, Ohio and Vermont. Illinois enacted S.B. 1652 to promote investment in a Smart Grid Advanced Metering Infrastructure Deployment Plan. The new law also created a Smart Grid Advisory Council to advise and work with participating utilities on plan development and implementation.

Ohio enacted S.B. 315 to encourage innovation and market access for cost-effective supply and demand-side retail electric service, including smart grid programs. Vermont's S.B. 78 (enacted) established policies and programs to help facilitate state-wide smart grid deployment by the end of 2013.

Figure 1: High level overview of the Smart-grid



Types of interaction with the system:
With Smart Grid technology people will be able to: And they will do it by: Understand how their household uses energy, manage energy use better, and reduce their carbon footprint.
1) Logging into their energy use account and seeing how much energy they are using in real time, and as compared to their neighbours, as reported by smart meters installed at each household.
2) Using smart devices, such as a smart thermostat that shows minute-by-minute price of energy. The thermostat could be programmed to make decisions about the house's heating and air conditioning levels. If the price of energy is high, and no one is home, the thermostat could be set to adjust automatically to use less energy. Smart appliances could also be programmed to run when energy is cheaper, such as a dishwasher running at night.
3) At peak energy usage times, allowing the utility to lower energy consumption of smart devices, such as adjusting a house's air conditioner by a few degrees. Control expenditure on electricity. 1) Accessing their account balance, and seeing how many units are being used per day, and which appliances are costing the most money.
2) Taking advantage of energy saver plans offered by the utility to keep energy use in line with a person's budget. For example, if a heat wave hits and the price of electricity peaks, the individual could be notified that they may exceed their budget. The individual would then be in control regarding whether the utility could adjust the temperature of the air conditioning a few degrees when peak energy consumption occurs. Experience fewer and shorter power outages, and to be notified when the power will come back on.1) having the Smart Grid pinpoint the location of the outage and dispatch workers to the scene immediately. Power will be routed around the outage, so that fewer individuals are affected by the power outage.
2) Signing up to receive alerts when the power goes out via text message to a mobile phone regarding when the power will be back on. Additional messaging services could provide alerts regarding
a loved one's energy restoration time. Control energy devices in the home. 1) Tying all energy devices that give energy back to the grid, such as a plug-in hybrid vehicle and solar panels, to a central household control which provides up-to-the-minute indication of energy use.
2) Monitoring whether their home is using more energy than it is producing, and adjusting devices so they use less energy. The smart meter tracks this activity, and any surplus in energy shows up as a credit on the person's utility bill.3) Controlling smart devices and account information over the Internet, allowing individuals to monitor and adjust their house's energy usage remotely.

1. NIST Guidelines for Smart Grid Cyber Security

1.1 Information that can impact the privacy of the customer:

Here are some of the identify information available within the Smart Grid that can impact privacy if not properly safeguarded

1. Name and address of the consumer, the account number of the smart -grid.
2. Smart meter number itself can be used to make a map as to which house it is connected and other characteristics such as their usage behaviors and so on.
3. The Datalink Layer headers such as the MAC address on Ethernet media or the DLCI numbers in a serial interface media. If the attacker is passively monitoring connecting to the same LAN of the smart-grid he might be able to trace it back to the user. But, this information makes no-sense if the user is on a different network as the MAC's are only transmitted within the LAN.

4. The IP address of the subscriber is another crucial piece of information which can impact privacy. The IP addresses are unique if the smart-grid is using public IP addresses to connect to the Power and Water Department monitoring and billing stations.
5. The billing information of the user itself can be private information.
6. Real time power consumption that the smart-meter gathers reveals information about the device like for example it provides the electronic signature of the devices that are being used.
7. Smart grid in business environment may reveal the machines that are running, the amount of hours the machines are running and even the personal information.
8. The lifestyle of the consumer is another important privacy factor as it reveals information like when the user is at home or when he is away and so on.

1.2 Privacy preserving guidelines.

Information that is to be protected according to California AB-1274 policy:

1. Existing law prohibits, except as specified, an electrical corporation or gas corporation, and a local publicly owned utility, from sharing, disclosing, or otherwise making accessible to a third party a consumer's electric or gas usage that is made available as a part of an advanced metering infrastructure, including the name, account number, and residence of the customer (data). Existing law requires the electrical corporation or Gas Corporation, and a local publicly owned utility, to use reasonable security procedures and practices to provide a consumer's unencrypted data from unauthorized access, destruction, use, modification, or disclosure.
2. Existing law makes the wilful obtaining of personal identifying information, as defined and use of that information for any unlawful purpose, a felony or misdemeanour. Existing law authorizes a person that has been injured as a result of a violation of this prohibition to bring an action against a claimant, as defined, to establish that they are a victim of identity theft, in connection with the claimant's claim against that person and to bring a cross-complaint if the claimant has brought an action to recover on a claim against the person. A person who proves that he or she is a victim of identity theft by a preponderance of evidence is entitled to a judgment providing for actual damages, attorney's fees, and costs, and any equitable relief that the court deems appropriate.
3. This bill would prohibit a business from sharing, disclosing, or otherwise making accessible to any third party a customer's electrical or natural gas usage data without obtaining the express consent of the customer and conspicuously disclosing to whom the disclosure will be made and how the data will be used. The bill would require a business and a non-affiliated third party, pursuant to a contract, to implement and maintain reasonable security procedures and practices to protect the data from unauthorized disclosure. The bill would prohibit a business from providing an incentive or discount to the customer for accessing the data without the prior consent of the customer. The bill would require a business to take reasonable steps to dispose that customer data within its custody or control when the data is no longer to be retained by the business, as specified. The bill would authorize a customer to bring a civil action for actual damages not to exceed $500 for each wilful violation of these provisions.

2. Information protection policies according to law AB-1274:

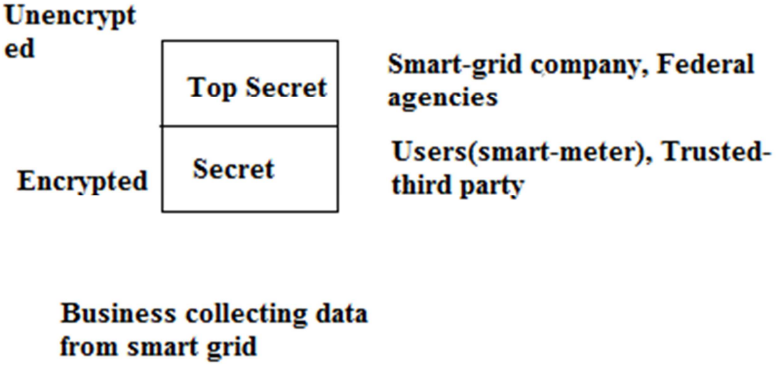
1. The important data items which has to be protected without the loss of the privacy is the user data such as the metered information and their personally identifiable information..

2. The businesses can disclose the data after the consent of the customer to a trusted third party who takes the same precaution in safeguarding the privacy of the users.
3. The data in transit or stored should not be tampered. Both the confidentiality and the integrity of the data have to be preserved.

3. <u>Mapping of Human Language Policy to access control policy -</u>

1. Human-Language Policy - Unless otherwise required or authorized by federal or state law, a business shall not share, disclose, or otherwise make accessible to any third party a customer's data without obtaining the express consent of the customer and conspicuously disclosing to whom the disclosure will be made and how the data will be used.

MAC implementation for the confidentiality can be done using only two security levels namely Top secret and secret level. At the secret level the data is in scrambled form and in the top secret level the data is in clear text. The business utilities that require the data for billing, diagnostics of the smart-grid will have the privilege of accessing all data in clear text and users and trusted party will have access to the secret level only. Separate key is shared to each customer to decrypt and access only their portion of data.

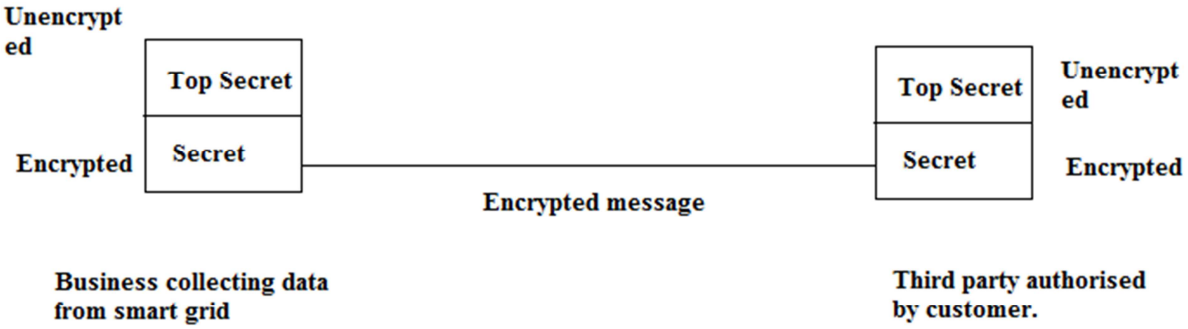


DAC is used to implement need to know model to provide the confidentiality and privacy. In general confidentiality is provided by the regular DAC with the (rwx) access but since the privacy is involved notice how the access rights vary for the third party. Capability of the third party is based on the rights he has obtained from the customer.

Agent\Records	Customer A	Customer B		Customer N
Business	rw	rw	rw	rw
Federal\State Agency	rw	rw	rw	rw
Third party	Customer granted rights and ORCON then r	Customer granted rights and ORCON then r	Customer granted rights and ORCON then r	Customer granted rights and ORCON then r

Customer A	r	-	-	-
Customer B	-	r	-	-
….	-	-	-	-
Customer N	-	-	-	r

The implementation of this legislation requires different security levels at-least two security levels to be implemented to store the consumer's data collected from implementing the smart grid technology.
First is that the Encrypted text obtained from the smart meters to the utility which has to be stored in the encrypted data storage and second is the clear text data for billing, monitoring and maintenance. The clear text data here assumes the nature of top-secret data and the encrypted data is secret data. The level of the top-secret data is transformed to secret data only by the process of cryptography.
The integrity part of the policy can be implemented based on the BIBA's integrity model (no write up and no read down). For the integrity labels the smart-meter is given Top secret label, including super-users (who may want to make correction) and all other entities including the business storage servers and the third party sites are made Secret-level. So, any data coming out of the smart-meter (TS) is passed on to the business storage servers(S) and the third party(S). Thus nobody will be able to tamper the integrity of the data.
2. Human Language Policy - A business that discloses data, with the express consent of the customer, pursuant to a contract with a non-affiliated third party, shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the data from unauthorized access, destruction, use, modification, or disclosure.
The business to business sharing of user's smart meter information requires that the same level of security policies to be applied by the later business as well. This is the direct implementation of Originator Control access control (ORCON)[2] so that the same right of the originator file passes on to the receiver of the file. Since the same type of access policies needs to be maintained at the third party site the data transfer from the Billing Company's site to the third party site should be trustworthy. We need to have trusted network interconnect (TNI) to protect the transfer.



The system in the business collecting the data from the smart-grid has only two mandatory access control levels and hence is of the standard of B1 level system and due to the ORCON policy and protection of privacy stipulated by the law the third party implements the same standard of the security (B1)[5] in his

system. Now to maintain the overall security of the systems interconnected we will have to send the message from Business to Third party in an encrypted manner.

3. Human Language Policy - A business shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the data from unauthorized access, destruction, use, modification, or disclosure.
The reference monitor concept enforces steps like authentication to map each individual user to the subject. The authentication procedures should again be non bypassable meaning the passwords sent over the network should not be in clear text, they should implement best encryption algorithms such as a minimum of AES-128 bit to encrypt the passwords. The passwords stored on the machine should again be hashed with the salt to randomize.
Since, the present day machines are not formally verified unlike Multics, the system administrators need to patch the systems on a regular basis. Even then these systems are vulnerable to zero-day attacks and the administrators need to keep a watch on these.
The policy also requires the integrity of the information. The information obtained from the smart meters might be subject to modification due to noise in the environment or by usurpation by the attackers so it is necessary to add checksums to each of the packets sent by the smart-meter to the utility. The data sent by the smart meter need to use Public-private key to share the data between the two end-points as the signing of the data sent by individual keys would verify the integrity of the sender (Smart-meter). Apart from the threats to the data in transit the data stored in the database of the utility might also be subject to modification so during the design of the system itself it is necessary to add hashes to keep track of the value of the data.
4. Human Language Policy - A business shall not provide an incentive or discount to the customer for accessing the data without the prior consent of the customer.
This requires that the business that is collecting the data from the smart-grid on behalf of the government should actually protect the privacy of the customer; it is collecting the information from. This is because smart-grid provides enough information to map the activities of the users to the power and energy consumption patterns. The businesses can make unfair deals with the third parties by selling the user behavior patterns. To prevent this from happening, the Law mandates for the customer's signature as a constraint for the third party sharing of the data.
5. Human Language Policy - A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer data within its custody or control when the records are no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the data in those records to make it unreadable or undecipherable through any means.[1]
The data collected from the smart-grid may be very sensitive in nature. The data acquired might include the customer's Personally Identifiable Information such as the name, address, telephone numbers, email-ids, social security numbers(SSN) or even financial details like the bank details, the credit card numbers and so on. After a data has lost its importance it is very important to sanitize the data, before disposal. The NIST SP 800-88 Rev. 1 has a separate set of guidelines on ways to sanitize different types of data storage. Some of the best practices for each of different types of data storage are –

Method	Description
Clear	The sanitization is done by overwriting the existing memory locations by data which are non-sensitive.
Purge	Apply media specific technique such as pulverizing, degaussing, cryptographic erase etc.
Destroy	There are two options – 1. Disintegrate, Pulverize, Melt, and Incinerate and 2. Shred

The smart-grid contains the history of trends of power and water usage of the customers and much other sensitive information. So, it is advisable to adapt the best sanitization practices of the industry i.e. destroy the hard-drive or the data storage completely such that it will not be able to reconstruct even at research labs.

(g) The provisions of this section do not apply to an electrical corporation, a gas corporation, or a local publicly owned electric utility or a business that secures the data as a result of a contract with an electrical or gas corporation or a local publicly owned electric utility under the provisions of subdivision (e) of Section 8380 or subdivision (e) of 8381 of the Public Utilities Code.

The provisions of subdivision (e) of section 8380 or subdivision (e) of 8381 of Public Utilities Code states that the user's consent for the usage of their PII collected from the smart-grid to a business is non-transferable. The agreement of the business with a third party will not allow that the party gets the consent from the user's without themselves signing up for the third party services.

4. <u>The other requirements not covered by access control policy</u>

Access control policy can identify the subjects and provide access to objects within the reference monitor abstraction model (smart grid network) however it cannot guarantee the service will be available to all the users all the time. Apart from this the QoS, User experience etc.; will vary. So the availability is one of the requirements not covered by access control policy.

The confidentiality of data stored can be protected by the access control policy. However the confidentiality of the data in transit between the two systems is another important aspect that access control policy cannot ensure. The confidentiality of data in transit is provided by the encryption mechanisms.

The access control policy can provide the integrity to the data by ensuring read only access. This prevents illegal writing of the object but again may not provide the copy or the deletion of the object. The object might include the user records. Access control policy cannot guarantee the integrity of the source. Like if we have two or more number of users who can write to an object then without any additional mechanisms such as logging, the access control policy cannot ensure the integrity of the data.

5. Potential threats to the protected information

1. Illegal data modification - The data stored on the system may be modified by the users working at the smart-grid metering facility. Special mechanisms must be ensured to limit the data modification. It is important to note that at least few of the privileged users at least have the ability to modify the data. Because sometimes the dispute may arise from the customer stating faulty reading so if it is to be corrected we will require one or more persons to modify the information.
2. Illegal sharing of the user information - We have created a secure policy and mechanisms to enforce such policies, even then we have to place trust on the operators of the smart-grid facility. A disgruntled employee or an employee deceived by social networking may go on to reveal the customers classified data.
3. Fabrication of data - This is usurpation of data. Creating false user information from the smart-meters and faking it as the original packets. The server stores the packet as original packet. So, there must be mutual authentication between the client (smart-meter) and the server before the data is exchanged. This prevents false packets from making any changes to smart-grid data.
4. Denial of access to the stored information - The rightful access to the stored access should be allowed or be available all the time. There are various techniques like Denial of service (DoS) or Distributed Denial of Service (DDoS) attacks where a group of boots start requesting the service to prevent the legitimate service from being serviced.

6. Threat space addressed by the law AB-1274

AB-1274 [2] will address parts such as the Confidentiality, Integrity and Privacy of the consumer data. However the law does not speak of the availability of the smart-grid infrastructure. It does not put any strict responsibilities on the Businesses as to what did needs to be available all the time.

Prior to AB 1274 there were no laws or burden on the businesses to protect the privacy of its customers

Due to this new law since the penalty set by the law is high the businesses have taken the privacy of its customer data seriously.

To enforce the privacy we have to the policy makers have to implement mechanisms with tougher confidentiality requirements. The smart-meters are made to transfer the data using AES level encryption

The access to the stored data is provided only to the authorised users. Thus, the confidentiality component is addressed by the law.

To prevent any accidental damage to the stored data only the smart-meters are put in the highest category for the integrity label. So, only it can write to the server with lower integrity label. Thus the integrity space of the threat is also addressed by the law.

7. Recommendations of additional controls to cover the threat space effectively

1. Make accountability law more elaborate and specific based on case to case basis. The businesses cannot always be held responsible for the disclosure of the user's private information. However, the businesses must be penalised if they are not practicing the industries best practices.

2. Make availability of the smart-grid a top priority and set clear benchmarks. Develop elaborate plans on who has to take the responsibility for the availability of the system. If the privacy is lost then a user's information private information is lost. However, if the availability to the system is lost, then the control to the smart grid is lost.

3. Also, as a precaution mandate the businesses to come with a backup plan to keep the grids from failing even in the case of being under attack.

8. Comparison of current best practices with the protection afforded by the high assurance trusted systems

8.1 Important multics security features:

Discretionary Protection [6]
Discretionary access control (DAC) policy for all the subjects and objects.
Require identification & authentication
Auditing capable of tracking each individual's access or attempt to each object
More stringent security testing
Mandatory access control (MAC) for specific sets of objects
Each controlled object must be labelled for a security level & that labelling is used to control access
Security testing requirements more stringent
Informal security model for both hierarchical levels and non-hierarchical categories informal security model shown consistent with its axioms
MAC for all objects
Labelling expanded
Trusted path for login
Requires use of principle of least privilege
Covert channel analysis
Configuration management
Formal model of security policy proven consistent with its axioms
Thus the multics clearly has good set of security features implemented in its design and development. However the commercial systems are generally evaluated at level C2 in TCSEC.

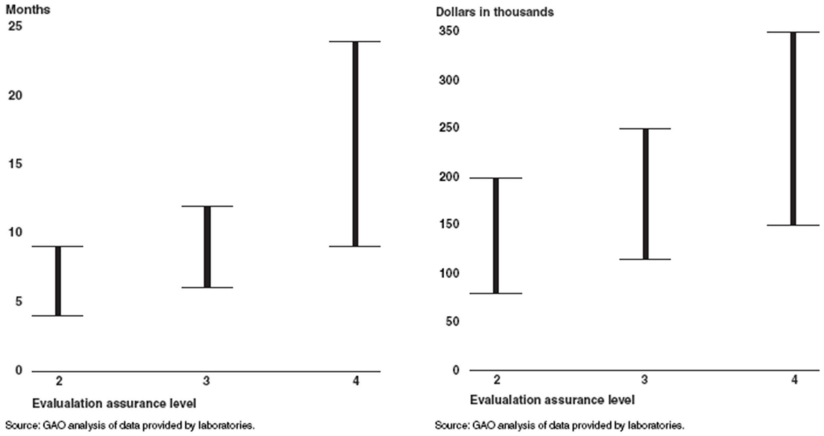
8.2 Features commercial systems exhibit

DAC [6]
Require identification & authentication
Auditing capable of tracking each individual's access or attempt to each object
More stringent security testing

8.3 Differences between trusted high assurance system and the current best practices

1. The main difference of commercial systems from Multics is that they are not subjected to covert channel analysis, so the systems are susceptible to subversion. To overcome the subversions, the commercial systems have come up with several best practices like Defence in depth i.e. having layers of security, having multi-vendor devices instead of relying on one particular vendor. This is done so that an unpatched vulnerability should not let the attacker to gain access through the entire network.
2. The Multics OS and software are shown to be secure formally meaning vulnerabilities are non-existent on the system. However, the commercial systems have no such proof of security. Hence, their security is often based on penetrate and patch approach. They are subject to zero day vulnerabilities.

3. The Multics and other OS which implement MAC are not susceptible to attacks by viruses like Trojan horses. However, the conventional systems have software mechanisms like DAC to enforce the access-controls are susceptible to changes by Trojan horses. This requires additional investment on software like antivirus.
4. In the commercial systems each function of the reference monitor is handled by different systems whereas the trusted high assurance systems implement all of the of the reference monitor functions in itself. Example is that we have separate dedicated devices to perform authentication like RADIUS or the Kerberos servers. For auditing we have SNMP servers or log servers in place. But, in high assurance system it is a complete system providing all the features in the same device.
5. Development of high assurance systems require huge spending of money and also time and effort of people. Another main problem in development of such systems are the developers of such system must also have the clearances to work in Top Secret and Secret environments which is harder to get for all the users. The figure below shows the estimation of time and cost for the development of systems from EAL2 to EAL4. [7][8]



References:

1. NIST Special Publications 880 - Data sanitization. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
2. California Legislation Assembly bill no. 1274(AB-1274).
3. Computer Security : Art and Science by Matt Bishop
4. University of Southern California INF522 Policy class lecture slides by Prof. Dr. Tatyana Ryutov.
5. National Computer Security Center (NCSC) NCSC-TG-005
6. Trusted Network Interpretation Environments Guideline (TNI) the Red book NCSC-TG-011
7. Department Of Defense Trusted Computer System Evaluation Criteria(TCSEC) 12/26/1985 by MITRE and NCSC http://csrc.nist.gov/publications/history/dod85.pdf
8. INFORMATION ASSURANCE National Partnership Offers Benefits, but Faces Considerable Challenges article by U.S GAO office http://www.gao.gov/new.items/d06392.pdf