Security Challenges For Expanding E-governments' Services

Izzat Alsmadi

Yarmouk University
ialsmadi@yu.edu.jo

Abstract

In the scope and vision of using and expanding the types of services e-government portals can offer to citizens, one of the major challenges and possible barriers is the security concern. Unlike typical websites that include largely data to browse and download, such portals are expected to have sensitive private personal data about country citizens. The threat of possible intrusion or identity theft is high and may cause serious consequences.

This paper proposes a multilevel security layered architecture for e-government websites based on the data access privileges. The paper evaluates the current security status of selected e-government portals in Jordanian e-government suite of websites. The focus of the evaluation is on possible vulnerabilities in securities and possible candidate threats. The study focuses on showing the weaknesses and problems that face the expansions of e-government services in Jordan to be fully active in the e-business to provide services to citizens throughout the Internet. The study makes some recommendations on how to approach such problems.

Keywords: *E-government, e-business, security, vulnerability, and e-commerce*

1. Introduction

Many countries around the world are continuously trying to expand their utilization of the Internet services. They are trying to facilitate using the Internet as an alternative for selling, buying, and communicating with individuals or business in person. Providing such services without the need for the physical present of individuals can make such services and transactions much more convenient to citizens.

In countries that have long time utilization of the Internet services such as USA, perhaps e-government initiatives may not be that much compelling due to several factors. The first one is that a large number of companies provide services through the Internet and such services are used frequently by individuals. For examples, people buy books online in the US more than buying them from actual stores. In fact, even traditionally known book sellers' outlets are expanding their business to cover selling, or buying online. The second reason is that the required infrastructure for e-business transactions is well established, tested, and evaluated. As we will explain later on, such requirements can be divided in several aspects that include, legal, technical, and cultural aspects. Another factor is that people in the US with a wide spectrum based on their age, location, level of education, etc use, respect and trust using online business transactions.

If we take one aspect which is: e-banking, it can be considered as a sub category of e-businesses. It focuses in providing all bank services for users online. This may include: checking balance, authorize funds to third parties, check account history, pay for items that they bought online, or transfer money from bank account to another.

E-Banking has been provided for the last several years by the main commercial banks in Jordan. The e-services include: Internet banking, shopping, WAP banking, transfers, e-cards, ATM, e-transactions, bank to bank transfers. [12]. A new Electronic Transactions Law supporting e-commerce and e-banking was drafted and passed in January 2002. However, a comprehensive set of supportive regulations is still missing and needs to be worked out through joints efforts from the Ministry of Information and Communications Technology, the Ministry of Industry and Trade, and the Central Bank of Jordan. Jordan's Electronic Transactions Law, based on UNCITRAL model law, is a sleeping beauty that can only be awakened with the proper supportive regulations, instructions, and institutions in place. Under the current law, an electronic signature has no evidentiary power until it is authenticated by a certification authority. The absence of certification bodies and a secure public key infrastructure (PKI) are major impediments to the creation of an effective e-contracts/e-transactions environment in Jordan. Furthermore, the Central Bank of Jordan is empowered by the Electronic Transactions Law to issue regulations on the electronic transfer of funds and methods of payments, but no regulations or instructions authorizing such transactions have been issued to date. Regulations that will be adopted will be authorizing:

(a) Digital certificates;

(b) Licensing and regulating certification authorities;

(d) National digital identity;

(e) Foreign certification authorities.

Based on United Nations Commission on International Trade model law (UNCITRAL), Jordan's Electronic Transactions Law recognizes the equivalency of electronic signatures, documents, data, and transactions as having the same the legal status as original versions. In addition, the law grants the Central Bank of Jordan the authority for regulating the electronic transfer of funds and also sets penalties for any crime committed through electronic means. The crucial next step in implementing this law is to establish the infrastructure and institutions necessary for certifying and processing transactions. [13]

Digital identification is increasingly evolving in use and importance as a method to safely identify humans or entities especially through on-line business transactions. Through history, several techniques are used to uniquely identify individuals. Up to date, writing signatures are significant and required to verify that the person filling an application for example, is the same person he or she claims to be. Biometric signatures such as finger prints, iris patterns of the eyes, retina scans, DNA, voice prints, facial features, etc. are important and are able to uniquely identify an individual. However, none of those signatures can be conveniently implementing on-line to complete a transaction in a short time with a reasonable cost.

Public Key Infrastructure (PKI) is a set of technologies and security policies used to issue, revoke, and manage digital certificates and key pairs [7].

Security Threats in e-Government

Both security threats and solutions are similar in implementation in the scopes of e-Commerce and e-Government. However, in the scope of e-Government, almost all data are more security-sensitive (i.e. relative to e-commerce data). This can be seen when considering that the consequences of misuses of stored personal citizen data are more important than those in the scope in e-commerce. Typical citizens, especially those who don't use the Internet frequently, feel vulnerable when using e-Government services. They expect to have security measures which provide subjective mutual trust. In developed countries such as Jordan, typical citizens are not well familiar with Internet services and initially they may have little confidence that their personal information can be communicated through websites safely. However, due to the fact that those services are available online and that they don't need to waste hours or days visiting governmental offices to renew a license, apply for a birth certificate, see their job applications' status, etc. Additionally there are important several differences between e-Commerce and e-Government websites which influence the security context and the existence of different threats.

Technical Security Threats

There are several technical security aspects that should be evaluated to judge if a website is ready for e-business transactions. From a technical viewpoint, Saarenpää et al [18] have defined at least 20 different threats related to data security particularly in websites or e-transactions. Examples of some of those requirements include:

- Unauthorized information access. This can have several types where users may not have authorization at all and yet they were able to access websites' resources. They may also have limited authorization but expands, illegally their authorizations (e.g. privilege escalation).
- Loss of integrity (e.g. unauthorized modification). Through illegal access, users were able to tamper or modify data that they are not supposed to modify.
- Loss of availability. A famous websites' attack (Denial Of Service, DOS, may prevent websites' users from some or all of services available for users. This can be intentional through flooding the website with frequent requests from one or different sources. It can also be unintentional when websites receive several requests from actual users.
- Data exploitation. Websites that host personal or critical information are liable to protect those information with due protections. The amount, types and levels of those protection may vary depending on the environment, threats types, users' types and the types of assets or data they are protecting. The levels of data utilization are divided into: see, use, access, modify, publish, and destroy. Each one of those data utilization levels has its own types of threats. Privilege escalation threats raise a user privilege from one of those to another (which is usually higher).
- Authentication or accountability problems. Web sites administrators, owners, or power users are allowed to add new users, delete existed users, and raise users' privileges' from one level to another.

One of the real challenges for websites offering services, is that intruders can be internal and/or external. The methods to prevent internal possible intrusions maybe different or even contradict with those to prevent external intrusion.

Threats can be also defined in terms of vulnerabilities. A weak website with several known weaknesses or holes is seductive for external and internal intruders.

Security in the virtual world (i.e. the web) is more challenging relative to security and identity verification physically or in reality. This is due to the fact that users are expected to verify their identity to data holders digitally through providing certain information that can verify to the data holder their identity.

Threats can be also defined based on passive and active where passive threats are “silent” threats that are difficult to detect. In some other definitions for passive threats, they are those that can be detected but not prevented. Many complicated malwares act in a stealth mode to deceit the antivirus, firewall or any protection system.

Non-technical Security Threats

E-government transactions have their own unique features that distinguish them from e-business transactions. The amount of flexibility available in the e-business for users to select the business they want to deal with, the items they want to buy or sell are more flexible and open relative to those services available for citizens in the e-government transactions. Requirements and conditions for performing such transactions are also more complex in the e-business relative to e-government. For example, for a user to be qualified for a new driver license renewal, the user needs to verify and have certain conditions and criteria for such process to be initiated or completed. However, this may not be the case for a user who is accessing www.amazon.com or www.ebay.com to buy/sell a book or an item.

Making profit or revenue is another major distinguishing factor between e-government and e-business websites. An e-government portal is not completely revenue oriented in comparison with those of businesses. As a result marketing and customer service schemes should be different. For example, an e-government portal is not concerned with directing customers to items of higher prices, etc. They should provide information for citizens that can help them understand their needs and instructions.

Legal requirements and regulations are and can be different for those in the two sections. In a previous paper [19], we divided requirements for having an effective successful e-business infrastructure into three major elements: legal, software, network and hardware perspectives. In each one, we showed the main attributes that a website or an e-business should have and be verified against for e-readiness compliance. As an e-government project will provide a large number of important services to citizens that are expected to touch all or most citizens, verifying all requirements is important and necessary.

For the legal perspective, which is the main one of the three perspectives that can guarantee the failure or the success of an e-government initiative, government is expected to produce proactive regulations to protect a business transaction and make clear possible consequences and liabilities on all e-business transaction members in case of any shortcoming, misuse or failure. For example, the speed of executing a legal case in such environment should be quick and if cases in the e-business transactions will take months or years or process, no one will be tempted to be part of such transactions. Security, convenience and performance, are three main beams that set at the core of e-business transactions in which a failure or a shortcoming of one beam may risk the falling of the whole process. The challenge is that fulfilling the requirements of one beam may conflict or even contradict with another. For example, it is widely known that security and performance are always competing requirements where improving one of them may come at the cost of the other one.

Transparency is one of the related attributes to security where it measures the reliability, visibility and the reality of the activities that an e-government entity or website is providing. However, the amount of exposed information, specially through the website, may contradict with some of the security requirements in that possible intruders of unauthorized individuals may abuse, disclose or miss use such information. For example, will providing, the phone number, emails, and full names of ministers, or official employees especially at high rank improve transparency at the cost of security? How can we draw the line between those competing requirements in the goal of improving the overall stance of such website and improve e-readiness ?!

Each e-government outlet or website should clearly define their services and audience in terms of the data levels that we described earlier; see, use, access, modify, disclose and destroy. For example, a website or a service that is solely informative to all providing announcement (i.e. the first data level, see) can have a very basic security level as its information is of a broadcasting level for all those who are interested and hence there is no real security concern for such information to be , possibly, edited, disseminated, etc. However, this is not the case for the most of the other levels of data privileges.

Most surveyed papers in this scope focus on proposal for security aspects at the authentication level to verify the user eligibility to enter a website or not. Those papers takes into consideration the user, software, network or hardware level security. This paper focuses on elaborations of authorization levels of security. In other words, after a user is authenticated, security measures should be able to tell how much privileges a person have and what type of assets, pages, etc, they can see, edit, etc.

2. Related Work

Security has been widely recognized as one of the main obstacles to the adoption of Internet services and it is considered an important aspect in the debate over challenges facing Internet banking. The evaluation of websites E-readiness is a complex and dynamic problem involving many factors, and because of the subjective considerations and the ambiguities involved in the assessment, Fuzzy logic (FI) model can be an effective tool in assessing and evaluating of an e-commerce security performance and quality [11].

One of the major requirements for e-businesses in general is the ability to handle payments online. In order to an e-business to be fully executed online, users should be able to search, select, pay and order items to be shipped to their local address. The first two elements can be implemented using typical web technologies (which is not a real barrier). However, in many countries around the world (as in Jordan), the last two (i.e. online payments and shipping) are still premature and require major improvements.

One of the widely used techniques to secure online transactions is the usage of digital certificates. In digital certificates, users are identified by the information embedded in their machines, and verified by mutually trusted third party entities called Certification Authorities (CA) (such as Thawte or Verisign). The CA guarantees that the website operating is who it claims to be [8].

CA issues and manages digital certificates. They are third party trusted entities to authenticate sellers to buyers, banks to customers, email servers to email users, etc. In general, you are not supposed to expose any personal or financial information in any website that does not have a valid certification.

There are some requirements for any company or entity that wish to become a certificate authority who issues certificates to clients. As a hardware requirement, digital certificates are usually created by certificate servers such as Cisco IOS, Microsoft certificate server, EverLink, etc. CA's should make sure that their certificate database is secured from being accessed or hacked by invaders.

There are several forms of digital certificates. In this one type of certificates, software companies send their keys (public keys) to their customers. Customers will return back a certificate that combines the software company's public key with their private key (which includes specific information taken from their computers to include unique identifiers that distinguish a computer from all other computers). This information may include MAC addresses, IP address, CPU and hard drive unique identifiers, etc. The digital certificate will be encrypted so that its information will not be readable if retrieved by unauthenticated users. It can be understood only by those who issued it.

Table 1 shows the number of websites that have digital certificates in Jordan relative to several countries in Middle East (ME) and the world. Clearly Jordan is falling behind relative to both. Most of those websites that use and need website in Jordan are hotels.

Table1. Number of Certified Websites in some ME Countries [6].

Country	No. of servers certified	Country	No. of servers certified
USA	250558	Lebanon	38
UK	31870	Iran	26
Turkey	1528	Jordan	26
Israel	1221	Morocco	24
UAE	222		
KSA	90	Qatar	17
Kuwait	83	Tunisia	16
Egypt	46	Oman	8
Bahrain	44	Algeria	4

There have been several unsuccessful trials by local companies to establish certificate authorities in Jordan [9]. They may be were having problems getting the right authentication and trust from government and private sectors. As an alternative, Jordan government, represented by any entity or ministry such as Jordan Ministry of Information and Communications Technology (MOICT) can be a certificate authority that will authenticate certificates for all those who are requesting to have them. Currently MOICT is acting as the CA (through its electronic commerce or sale department). Many websites or business in Jordan who need and provide e-services is using International CAs such as VeriSign and Thawte.

It has been largely shown that the national e-readiness has a positive impact on e-commerce diffusion. There were also significant country effects, such that US firms had significantly higher scope of use than firms from other countries [14].

Several researchers studied e-commerce decisions and impacts on different countries. Example of which is the paper [15] which studies such case in Taiwan by describing the degree to which various organizational, industrial, governmental and cultural factors influence B2B ecommerce adoption decisions in Taiwan. Cultural tendencies are shown to have an effect on B2B e-commerce adoption decisions in an indirect manner.

In another similar paper, Liao et al found that individual expectations regarding accuracy, security, network speed, user-friendliness, user involvement and convenience were the most important quality attributes in the perceived usefulness of Internet-based e-retail banking [16]. E-banking system may include: ATMs, phone banking, Internet banking and mobile banking. In small homogenous countries, advanced infrastructure and banking, the logistics, communications, and payment costs associated with ordinary and Internet-based shopping tend to be low and similar.

Many banking studies conducted during the past years which find that TAM is a powerful, highly reliable, valid and robust predictive model that may be used in a variety of contexts [17]. While customer behavior is well described by economic and marketing theories, great evidence suggests that technology-related variables have become as important as traditional factors in predicting online users' behavior. The customer's perception of security on blogs refers to the perceived degree of protection against threats such as third-party network attacks.

In a more focused scope, Wimmer and Bredow proposed a holistic approach for security solutions to e-governmental portals [20]. They discussed commonalities and differences between an e-business and an e-government website. Their security model analyses possible threats in e-government based on several aspects such as the domain, level of electronic processing and abstraction layers.

3. Goals and Approaches

The main focus on this paper is to evaluate and propose data authorization and access level privileges based on data access levels. In the first section, we will elaborate on the proposed security model based on data access levels for e-government websites.

A V or onion like model for security protection in e-government portals.

Based on the data visibility levels that we mentioned earlier for users of e-government websites, we proposed a V model for security prevention and protection. The Data in the back end is the main asset that those websites must protect. Users can have access , remote and local, to those data based on their privilege. The same model can be applied using some other aspects of security. For example, we can use the OSI network model layers (i.e. application, presentation, session, transmission, network, data link and physical layers) to similarly layer security aspects based on those layers. In another approach, user privileges (i.e. guest, user, power user, administrator, etc) can be used as the base to layer this model. However, for websites in general and e-government websites in particular, we believe that layering such architecture based on data access or privileges or more relevant and simple to apply. This can be particularly applicable if website is design based on Service Oriented Architecture (SOA); a design architecture that can smoothly deal with such security modeling approach.

We will elaborate on the data access and protection levels we described earlier. It should be mentioned that the data privilege security focused on the authorization level security. This means that an earlier authentication level security should be implemented. The authentication security measures come first to make sure whether a user is allowed to access a system or a resource in general or not. While the authorization level security measures check, after authentication, if such user has the enough privilege to perform one of the data level available services described in Figure 1. This role or service based access control can be implemented along with the SSO service to read all user authorization or privilege levels as soon as they log in to the e-government website.

1. The reason for focusing on the data access level and making the whole security model oriented based on those attribute is that ultimately all rights, privileges and security measures especially on e-government websites aim at known the person, or the entity that is trying to access the system and what are the resources they are intended to see or use. For the website, the main resources at hand are the web pages, and the data behind them. If for each one of those two elements, we specify users and data access privileges (e.g. as shown in Figure 2), we can provide a simple and easy to implement security model. Such model can be connected with the SSO service that is activated as soon as the user accesses the system. Figure 2 shows a simple and generic way in which such data level authorization can be implemented and propagated through different users, and components.

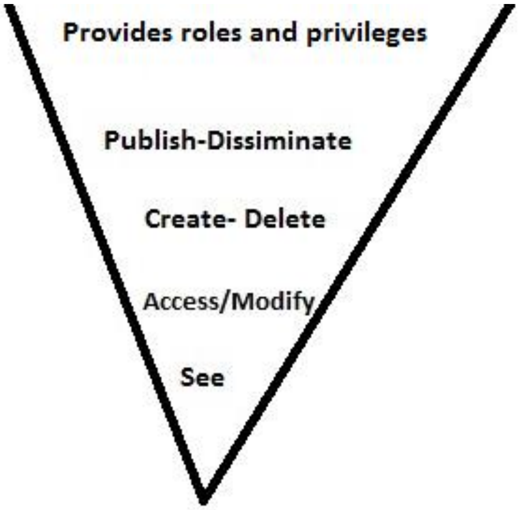
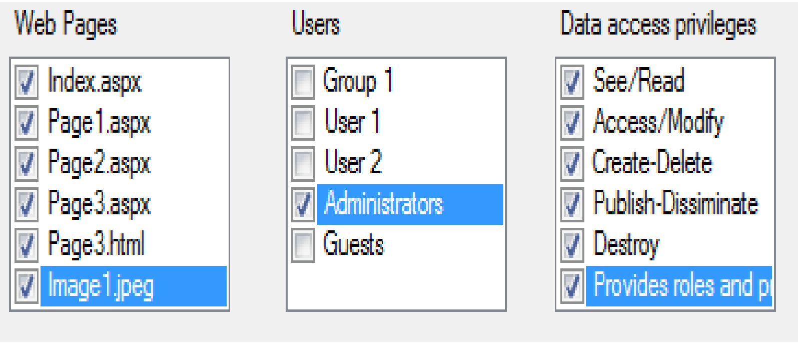


Figure 1. Data Visibility Levels for Websites' Data

1. The "see/read" level. This is the first and lowest level (based on privilege). Although by default, the lowest possible user privilege (e.g. guest) can have such level, however, visibility is not always guaranteed specially for some private pages that can be only seen by one or a limited number of intended users.



Web Pages

☑ Index.aspx
☑ Page1.aspx
☑ Page2.aspx
☑ Page3.aspx
☑ Page3.html
☑ Image1.jpeg

Users

□ Group 1
□ User 1
□ User 2
☑ Administrators
□ Guests

Data access privileges

☑ See/Read
☑ Access/Modify
☑ Create-Delete
☑ Publish-Dissiminate
☑ Destroy
☑ Provides roles and p

Figure 2. A sample approach for security implementation in e-government websites

The triple components security approach (i.e. web page, user, data privilege) can be defined on the micro or the macro level. This means that we can set general roles that are applied to a user or a certain group of users. Nonetheless a micro level security role can override (usually downward) a role in the macro level.

2. Access/modify

On this level, the user can read and modify on the page that they are visiting. For example, in this level, a citizen is allowed to submit an application to renew a driving license. A user may not have such privilege if they are visiting users who do not fulfill initial preconditions or constraints. For example, the user may open and download such form, however, in order to submit this page (i.e. a modify privilege), they have to fulfill all or some major fields in that form. This shows that a privilege can be raised on the fly once a precondition is fulfilled.

3. Create/delete

Users usually are not allowed to create a new page, table, a file, or any website object. Such privilege is given to data owners or e-government websites' employees.

4. Publish/disseminate

A user who can read or write a web page, may not be allowed to distribute such information. Such privilege should be given a separate privilege level. Many websites read announcements and post them on their own websites. In some cases, this may need to have clear acknowledgement from the data owner to ensure authenticity of the data.

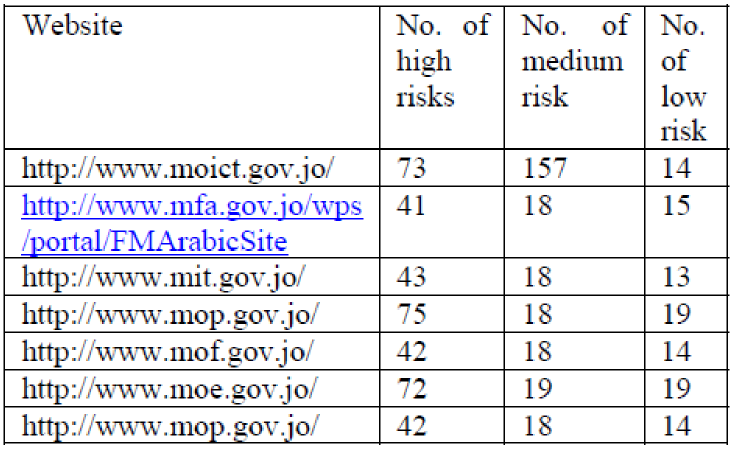
5. Provide rules/services

A data owner or administrator can add new users, delete current users. They can also modify users privileges. At the end, data owners themselves are users just like the typical citizens.

Vulnerability Evaluation

Websites' security evaluation includes evaluating websites against several rules and measures. There are several commercial, free and open source tools that can be used to perform websites security evaluation. Examples of those websites include: Wikto, Acunetix web vulnerability scanner, CGI, and NStalker. Table 2 shows a security survey on selected Jordanian e-government websites to scan for possible weaknesses or vulnerabilities.

Table 2. No. of Risks in Selected Jordanian e-government Websites [18]



Website	No. of high risks	No. of medium risk	No. of low risk
http://www.moict.gov.jo/	73	157	14
http://www.mfa.gov.jo/wps/portal/FMArabicSite	41	18	15
http://www.mit.gov.jo/	43	18	13
http://www.mop.gov.jo/	75	18	19
http://www.mof.gov.jo/	42	18	14
http://www.moe.gov.jo/	72	19	19
http://www.mop.gov.jo/	42	18	14

Table 3 shows also the overall evaluation of the selected e-government websites in Jordan from security perspectives. All previously mentioned tools were used in the evaluation and the total number of weaknesses is added to the table. R1,R2,R3 are High, Medium and Low risks respectively. To study the impact of security measures on performance, the total time it takes tools for security evaluation was added to the table.

Table 3: Security Evaluation for Selected e-government Websites in Jordan.

Website	R1	R2	R3	Time Sec
1	0	6	0	7320
2	0	5	0	18000
3	26	36	0	6530
4	0	2	0	16980
5	0	0	0	14650
6	0	12	0	9760
7	92	58	7	24360
8	242	51	3	12323
9	68	50	27	287
10	41	2	0	6520
11	12	12	3	93172
12	0	2	0	12
13	59	42	3	2300

Table 3 shows that there is a large variation between the different websites in terms of size and vulnerabilities. Some websites have very large websites with lots of documents and details while other websites are using the website for providing only basic information.

E-readiness

This is an e-commerce related metric that ability to use information and communication technologies (ICT) to develop a country economy and to foster its welfare. There are many attributes that affect e-readiness ranking related to the ICT such as Internet, connectivity, legal, social and environmental factors. In 2009, Jordan is ranked 50 out of 70 countries studied which show some improvements over the past years. The e-readiness score out of 10 was 4.92. Relative to Middle East countries, it is ranked fourth after Israel, UAE and Turkey.

Other studies also show while Jordan progressed very well in some aspects of e-readiness related to the spread of the Internet, however, for those related to legal perspectives, many future steps are still needed to regulate and protect online transactions.

Citizens' Digital Identities

Problems such as identity theft are far more destructive in e-government transactions. For example, an identity theft that causes a person to buy a laptop under the name of another person is less complicated than that which causes a person to issue a driving license under another individual name. It maybe necessary on the long run for any e-government initiative to initiate a digital certificate for each citizen in the same manner that they provide them a personal identity card or passport. Digital entities may also added to those major citizen identity verification documents where such documents can be encoded with those digital identities and citizens can enter those digital identities whenever they used an e-government service.

Security Policies

Policies and permissions are important dimensions of security for social networks. In the service oriented architecture of the web, it is important to autonomously differentiate between users, data providers and service providers.

Permission is a term that is related to the terms: authentication and authorization. Authentication indicates whether a user has access to the particular system, service or not. However authorization gives further details to specify if a user is allowed to access a system what is the authorization or permission level of access that he or she can have. Typical permissions in social networks include: Only the subject person, Everyone, Individual Friends (and NOT individual friends), All Friends (1st level connections), All Friends of Friends (2nd level connections), All Groups, Some Groups (and NOT some groups). However, in e-government websites, policies should be distributed based on the types and privileges of users for the e-government website. Figure 3 shows the ontology for ODRL asset model. This class or ontological diagram shows the major elements of this model which are the policy, asset, party, subject, role, permission, duty, prohibition, action and constraint. There are several examples of projects that implement ODRL for digital rights managements and permission [21].

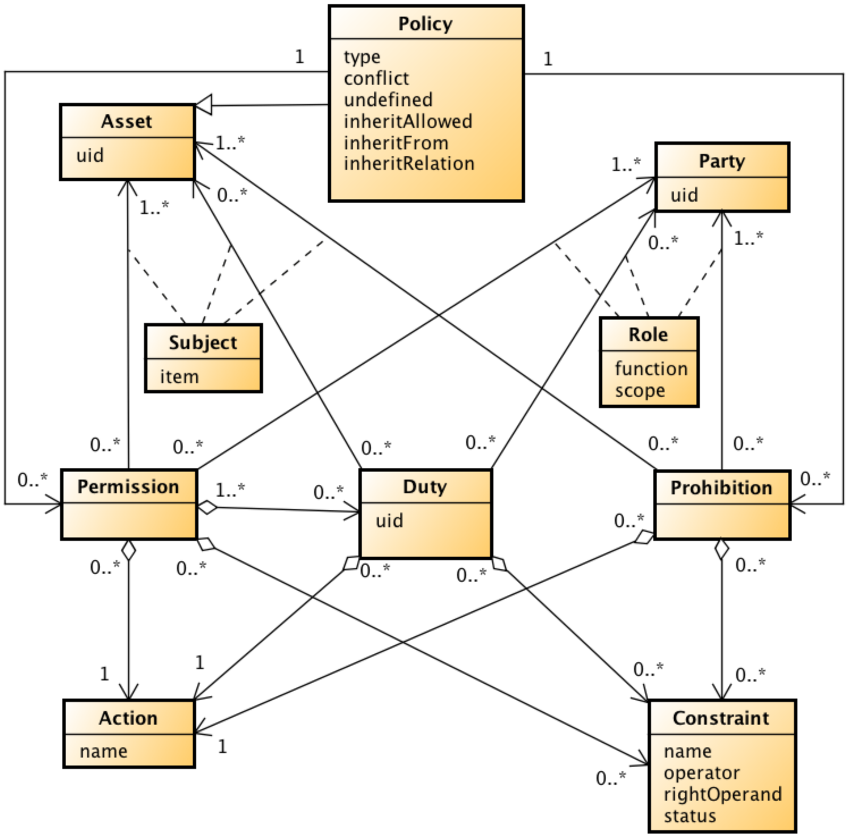


Figure 3. ODRL Asset Model Ontology [21].

For each web page in a website (i.e. asset in Figure 3), all elements should be specified based on the ODRL ontology. Table 2 shows an example of a policy for a web page.

Table 2. Driver License Renewal Page

Asset	Driver license renewal page (DLNew.aspx)
Policy	Policy: policy1, ID:2000
Subject	Allow citizens to submit a form to renew their driving license
Permission	A citizen should be able to login using a valid social security or identification number
Role	Citizens, employees, and administrator
Party	Group driver license generation is not allowed
Duty	Create new form, pay fees, etc.
Prohibition	Special licenses cant be submitted through this form.
Constraint	Check for duplication, expired license, etc.

4. Summary and Conclusion

E-government initials are intended to help citizens communicate with the government and government officially more easily and conveniently relative to personal visits for actual government offices. In this paper, we introduced a security model for e-government websites based on data access levels. Data, web pages and all other types of resources are the assets that users visit those websites for. As such, all other security tools support this backend goal. This represents a focus on the access authorization or privilege levels. Previous authentication or identity verification levels come before authorization to verify a citizen or user and their identity. Data access levels come at the second stage after assuming that an individual is, generally, allowed to access this website. It takes this further to identify what types of resources they have access to and what level of privilege they have on those resources.

Implementing this scheme with a single sign one service, can help both citizens and data owners in making the process of data access simple, smooth and fast. While such scheme is specified at the page, table or file level, however, since a single sign on approach can propagate such privileges across pages, it is expected that such scheme will not cause any slowdown in page loading or data retrieval.

It was strange to know that in many Middle Eastern countries, people use Internet services more than Jordan despite the fact that Jordan is ranked high in Internet readiness relative to those countries. Perhaps the government is only focusing on major cities relative to Internet education or in educating citizens about the types of services available online. In some other cases, other cultural or trust barriers may block the usage of e-government services.

We classified the factors that may affect how much people use and trust online websites or service into different categories. Some e-government websites themselves don’t use encryption or digital certificates although they provide sensitive or personal information. Jordan has no local Certificate Authority (CA) yet, despite the fact that MOICT is trying since years to have a department dedicated for that purpose.

Customers in Jordan need to trust and use online services. It seems that several e-government websites are offering services online. However, traffic analysis for those websites showed that they have a small number of users (i.e. daily, weekly, monthly). Either they are not promoting enough for such services, or customers do not trust such services or lack enough information about risks and problems. Jordan does not lack the infrastructure for the Internet and the Internet services are provided all over the country with good speed and relatively low cost. General trends of Jordanian citizen’s usage of the Internet indicate that their focus is largely on the entertainment sectors. We need to understand and learn the real benefits of the Internet and utilize it for the best purposes it meant to be.

The government should have laws and regulations for online transactions to protect online users from any risks or problems. This can increase citizen's trust in using online services. Jordan Internet infrastructure is strong and capable of handling the construction of a trusted network. The private sector should take the lead in PKI and digital identity infrastructure. Once such infrastructure is established, many of those related and dependent industries can exist and provide an important economical input to the national revenue.

References

[1] "Secure computing corporation. Digital certificates". <http://www.securecomputing.com/gateway/digital_certificates.cfm>. 2008.

[2] Conjecture corporation. "What are digital certificates". <http://www.wisegeek.com/what-are-digital-certificates.htm. 2008>.

[3] Comtrust. <http://www.comtrust.co.ae-/docs/contactus.htm>. 2008.

[4] WISekey, http://www.wisekey.com/press/-jordan32002.htm>. 2002. 2008.

[5] "Jordan e-government program, e-Government strategy". <http://www.moict.gov.jo/moict/>e_gov_strategy/eGovernment%20Strategy.pdf>. 2006. 2008.

[6] "Netcraft, Certificate services". < http://news.netcraft.com/SSL-Survey/CMatch/certs>. 2006. 2008.

[7] "Secure computing corporation. Digital certificates". <http://www.securecomputing.com/gateway/digital_certificates.cfm>. 2008.

[8] "Conjecture corporation. What are digital certificates". http://www.wisegeek.com/what-are-digital-certificates.htm. 2008.

[9] "Comtrust ties up Jordanian company ESKADENIA. AME Info". <http://www.ameinfo.com/26458.html>. 2003. 2008.

[10] Aburrous, M.; Hossain, M.A.; Thabatah, F.; Dahal, K, "Intelligent Quality Performance Assessment for E-Banking Security using Fuzzy Logic". "National profile for the information society in Jordan, United Nations Economic and Social Commission for Western Asia". (ESCWA).2005

[11] "Profile of the information society in the Hashemite kingdom of Jordan, united nations Economic and Social Commission for Western Asia" (ESCWA).2003.

[12] Gibbs, Jennifer L. and Kenneth L. Kraemer. 2004. "A Cross-Country Investigation of the Determinants of Scope of E-commerce Use: An Institutional Approach. Electronic Markets". 14(2):124-137.

[13] Thatcher, Sherry; Foster, William; and Zhu, Ling, 2006. "B2B e-commerce adoption decisions in Taiwan: The interaction of cultural and other institutional factors, Electronic Commerce Research and Applications", Volume 5, Issue 2, Pages 92-104

[14] Liao, Ziqi and Cheung, Michael Tow, 2002 "Internet-based e-banking and consumer attitudes: an empirical study, Information & Management", Volume 39, Issue 4, January 2002, Pages 283-295.

[15] Yousafzai, Shumaila, Y.; Pallister, John G.; and Foxall, Gordon R., 2003, "A proposed model of e-trust for electronic banking, Technovation", Volume 23, Issue 11, Pages 847-860.

[16] Saarenpää, A., Pöysti, T., Sarja, M., Still, V., Balboa-Alcoreza, R., "Data Security and Law: Perspectives on the Legal Regulation of Data Security. Executive Summary in English of the Research Report published by the Ministry of Finance under the itle "Tietoturvallisuus ja laki, näkökohtia tietoturvallisuude oikeudellisesta sääntelystä", 1997,

[17] http://www.urova.fi/home/oiffi/julkaisut/datasec.htm[5/6/2001].

[18] Izzat M Alsmadi, Ikdam Alhami, and Hisham Alsmadi, "The Requirements for Building an E-commerce Infrastructure", , International Journal of Recent Trends in Engineering (IJRTE), ISSN 1797-9617, Volume 2, Number 2, November 2009, http://www.academypublisher.com/ijrte/vol02/no02/index.htm.

[19] Maria Wimmer and Bianca Bredow, "A Holistic Approach for Providing Security Solutions in e-Government", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[20] Michael Mrissa, Salah-Eddine Tbahriti, and Hong-Linh Truong. "Privacy model and annotation for DaaS", ECOWS2010, IEEE Computer Society, 1-3 December, 2010, Ayia Napa Cyprus.

Authors

Izzat Alsmadi is an assistant professor in software engineering. He got his phd from NDSU, Fargo, ND in 2008. He is working in the computer information system department at Yarmouk University, Irbid, Jordan. His research interests are focused on software testing and metrics.