Review of Security and Privacy Issues in e-Commerce

Mehrdad Ghayoumi
University of Art
Tehran, Iran
mehrdad@ghayoumi.com

Abstract—Privacy: the control over one’s personal data — and security—the struggled access to the data by unauthorized other, are two critical problems for e-commerce consumers. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both. This paper reviews the review for privacy and security respectively. We study privacy from social psychological, organizational, technical, and economic perspectives.

Keywords— Privacy, Security, E-Commerce, Issues, Technology, Society.

I. INTRODUCTION

General and public communication, and the benefits of information technologies are rapidly changing our society, economy, and the way we are doing business and in the general our life. Digital business (e-Commerce) means doing business electronically, both within enterprises and externally, using computer networks or telecommunications. The current state of e-commerce is a good example that the supporting technology has not yet reached its full potential. In 1999 Forrester Research predicted a volume of US$ 184 billion of US online retail sales in 2004 [1] whereas the actual value is only approximately US$ 69 billion [2], representing a big gap of almost 167%. One of the major reasons for the gap between predicted value and actual development that has been suggested by the research community and backed by many studies is simply the lack of trust, privacy and security in digital business. There are many software which try to increase the human securities such as biometric software [47]. A complete review is here[48].

In order for digital business to reach its full potential the obvious conclusion is that either companies involved need to increase the level of confidence and trust provided by them to their customers or technologies need to be created having strong built-in features to protect the individuals’ privacy and the security of the digital business transaction[3], [4]. As much as the privacy and security goes higher the usage and the user number goes higher and going to this way, save the energy and time. It can be affected on many thing even on the all types of the energy. This can be even effect on the environment and the green earth. Even assume we have not this and the users does not use it too much, then it make the wasting too much [5].

There are many architecture for satisfying the privacy and security in digital business especially in the e-Commerce. They discussed a dynamic interface that applies Role Based Access Control (RBAC) policies as the output of policy analysis and limits the amount of information that users have access to according to the policies defined for roles. And presenting a dynamic model that adjusts users’ security policies based on the level of trust that they hold and use machine learning beside the trust manager component that helps the system to adapt itself, learn from the user’s behavior and recognize access patterns based on the similar access requests and not only limit the illegitimate access, but also predict and prevent potential malicious and questionable accesses. [24, 25 and 26].

The growth of Internet usage in some countries is also raising concerns about privacy. The qualities that make computer networks such powerful tools for improving efficiency and living standards also give them amazing power to collect, store, or distribute medical data, financial data, and other personal or biographical information. Many individuals and consumer groups are calling for new privacy safeguards for the Internet and other computer networks. Personal information that may be of interest to businesses or people with malevolent aims is generated whenever people surf the Internet.

Companies, for example, are able to learn a great deal about web surfers who visit their websites. Using tracking devices known as “cookies,” companies are able to track purchases and gather personal data. They can use this information to target their marketing efforts at individual consumers or groups of consumers. While some may welcome increased attention to their consumer needs, others may consider it an invasion of their privacy. There is also growing concern about what on-line and conventional stores do with the purchasing or personal data they collect during transactions. Under pressure from consumers, some stores have recently begun to develop privacy policies, but consumer groups say many of these policies fall short [9].

Finally, patients and consumer want to set rules for the sharing of personal medical data. In each of these areas, it will be difficult to slowdown a balance between protecting privacy and ensuring a flow of information and data that can improve quality of life. The same Internet-based tools that can improve education, health, and governance can also cause considerable damage when used for purposes of theft or fraud.

Companies and individual computer users are being increasingly affected by computer viruses and schemes to steal

data or computer identities [10]. Companies are spending enormous amounts of time and money to protect their networks and their data. Recent polls suggest that two thirds of American companies have experienced some form of "cyber-disruption." [11].

In this paper we are discussing the major issues involved. We will start with a general discussion on trust issues, followed by a discussion on the general meaning of privacy and privacy enforcing technologies and will conclude with the current major fields related to providing the security of the underlying technical infrastructures for digital business [17], [18].

The rest of the paper is organized as follows. Security concept, such as technology and social issues are present in the Section 2. Section 3 demonstrates an overall in privacy and technologies and issues. Economic issues in general are presented in Section 4 and the last section concludes the paper.

II. SECURITY

Security is a major concern for e-commerce sites and their clients. Users fear the loss of their financial and secured personal data, and e-commerce sites fear the financial losses associated with break-ins and any other types such this [15]. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Here we mention to the 6 dimensions of e-commerce security:

- **Integrity**: prevention against unauthorized data modification
- **Nonrepudiation**: prevention against any one party from reneging on an agreement after the fact
- **Authenticity**: authentication of data source
- **Confidentiality**: protection against unauthorized data disclosure
- **Privacy**: provision of data control and disclosure
- **Availability**: prevention against data delays or removal

A. Security Technologies

There are many technologies, including cryptographic solutions that can ease the above weaknesses. For a more complete description of each technology, see [13], [16]. In the mass media, the most visible security technologies are the encryption algorithms. For a general introduction to these technologies see [21], [27]; a popularization can be found in [28]. Two classic textbooks are [22], [29], and encyclopedic compendia include [31].

Public key infrastructure (PKI) systems are one such encryption technology [23]. Important PKI-based secure protocols include the retail mechanism Secure Socket Layer (SSL) [32], [33] and the interbank standard suite, ANSI X9 [6], [34]. The PKI is a flexible key-distribution system in which every participant carries two cryptographic keys, one for encryption and one for decryption; together these two keys make up what is called an asymmetric key pair [35], [36]. The encrypting key is published to the world and is called the participant’s public key. The decrypting key is called the private key. The system is characterized by mathematical elegance, efficient scaling features, and theoretically based security guarantees. A performance advantage of PKI is that it does not require a centralized, highly available intermediary for every secured transaction; however, this also makes it difficult to know when another party's key has been stolen or otherwise compromised. As such, PKI often requires a centralized, highly available intermediary for key management, and especially for prompt notification about revoked key-pairs [37]. This issue, the revocation problem, is still unsolved [38], despite the best effort to date [39].

A digital signature is the salient application of public-key cryptography, and is an analog of a handwritten signature. A digital signature is a cryptographic tag that only one author can calculate; the tag can be combined with any kind of data that the author might create; and the tag's validity can be checked by anyone who can access the data. This combination of authored content with the author's identity serves the same purpose as applying one's signature to a paper document; a digital signature can be used to sign contracts, to provide authenticity of an electronic distribution, or to prove identity for access.

B. Social and Organizational Issues in Security

Security, however, is not just a matter of technology; implementing technology without the proper organizational processes will not solve security problems [27]. There are a number of critical social and organizational issues with security. The first is that the weak link in security is often users or employees and the second is software engineering management, or managing how security technology is deployed. The third is the development of adequate organizational processes for risk management, separation of duties, and development of security policies, access control, and security assurance. The ability for hackers to obtain critical authenticity data is well known; it is often called “social engineering”. There is research work on understanding user’s mental models and motivations, but little on how to deal with the problem. Even keeping up-to-date with all security advisories and security patches is difficult, arguing that merchants should be conservative about undertaking complicated, heterogeneous deployments [30].

III. PRIVACY

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher [40] reported "Forty-one percent of Web buyers surveyed last year by Forrester Research of Cambridge, Mass., said they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely.”

A Business Week/Harris Poll found that over forty percent of online shoppers were very concerned over the use of personal information, and 57% wanted some sort of laws regulating how personal information is collected and used [41]. Similarly, Culnan [42] argued that privacy concerns were a critical reason why people do not go online and provide false
information online. Why this concern about privacy? The answer is simple. As of 1998, the FTC found that the majority of online businesses “had failed to adopt even the most fundamental elements of fair information practices. Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses.

The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce. Tackling privacy, however, is no easy matter. If nothing else, privacy discussions often turn heated very quickly. Some people consider privacy to be a fundamental right; others consider it to be a tradable commodity.

Detailed arguments about the historical progression of privacy can be found, for example, in [43]. We have these types of the privacy:

- **Privacy of the person**: It encompasses the right to keep body functions and body characteristics private;
- **Privacy of behavior and action**: It includes sensitive issues such as sexual preferences and habits, political activities and religious practices;
- **Privacy of communication**: It aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to email messages;
- **Privacy of data and image**: It includes concerns about making sure that individuals’ data is not automatically available to other individuals and organizations and that people can “exercise a substantial degree of control over that data and its use”;
- **Privacy of thoughts and feelings**: It refers to the right not to share their thoughts or feelings or to have those thoughts or feelings revealed. Individuals should have the right to think whatever they like;
- **Privacy of location and space**: It means individuals have the right to move about in public or semi-public space without being identified, tracked or monitored;
- **Privacy of association**: It is concerned with people’s right to associate with whomever they wish, without being monitored.

There are some security requirements:

- Authentication of merchant and consumer
- Confidentiality of data
- Integrity of data
- Non-repudiation

A. Privacy Technologies

Clark [19] divides the technologies in question into 4 groups. Clarke argues there are technologies used for surveillance, the technologies for forming agreements about the release of private data, the technologies for labeling and trust, and privacy-enhancing technologies (PETs). The technologies for surveillance and for data capture are used by companies for business purposes, but they have the side effect of endangering personal privacy. These include generating data trails, data warehousing and data mining, and biometrics. Many of these technical mechanisms can lead to consumer profiles that “are no longer based only on the individual’s dealings with a single organization, because their data is shared by multiple merchant. Balancing these tracking mechanisms are privacy enhancing technologies (PETs), which attempt to defeat or neutralize the surveillance or tracking technologies. Basic PETs include cookie managers and personal firewalls.

A new area of research includes the so-called labeling protocols, such as the MIT/World Wide Web Consortium’s Platform for Privacy Preferences (P3P) [20, 21, and 22]. P3P allows sites to describe their data handling policies and permits users to describe their preferences for releasing private data. Other technologies, such as those to help users understand predetermined terms or even contract related fraud, will also emerge. Ackerman and Cranor [1] outline one such technology.

If we would like to talk about the security of site some major point can be consider such as:

- Choose a secure ecommerce platform.
- Use a secure connection for online checkout—and make sure you are PCI compliant.
- Don’t store sensitive data.
- Employ an address and card verification system.
- Require strong passwords.
- Set up system alerts for suspicious activity.
- Layer your security.
- Provide security training to employees.
- Use tracking numbers for all orders.
- Monitor your site regularly and make sure whoever is hosting it is, too.
- Perform regular PCI scans.
- Patch your systems.
- Make sure you have a DDoS protection and mitigation service.
- Consider a fraud management service. "Fraud does happen”.
- Make sure you or whoever is hosting your site is backing it up and has a disaster recovery plan.

B. Social and Business Issues in Privacy

Privacy as a business issue is extremely sensitive to changes in the surrounding context. Changes in people’s anticipations or in regulatory governance can dramatically alter business issues.
and possibilities. Below is an overview of the research and business issues. This will include the consumers’ concerns, technical issues, and regulatory attempts to improve privacy concerns. In this examination, our attempt is not to predict what will happen or should happen, but to present issues to guide further research and business activity. Clearly, there are many business opportunities in the changing technical environment.

The use of digital systems allows data capture at a much larger rate and scope than previously; e-commerce sites could potentially collect an immense amount of data about personal preferences, patterns of information search and use, and the like about consumers, especially if aggregated across sites. Not only is it easier than ever to collect the data, it is also much easier to search these data. New computational techniques allow data mining for buying patterns and other personal trends.

These data can be used to personalize a customer’s e-commerce experience, augment an organization’s customer support, or improve a customer’s specific e-site experience. From the viewpoint of customers, many e-commerce sites have done irrational things with their customers’ data. Consumers’ opinions in this have been confirmed by media stories of particularly privacy failures and public relations nightmares. Broadly speaking, consumers are just confirmed in their opinions by the media. As mentioned, few consumers trust companies to keep their data private.

In one survey, 92% of respondents indicated that even when companies promised to keep personal data private, they would not actually do so. Culnan and Armstrong [44] make the argument that customers have two types of privacy concerns. First, they are concerned over unauthorized access to personal data because of security breaches or the lack of internal controls. Second, consumers are concerned about the risk of secondary use. This includes sharing with third parties who were not part of the transaction in which the customer related his or her personal data. It also includes the combination of a consumers’ transaction data and other personal data to create a profile.

Smith, Milberg, and Burke [45] raise two additional concerns based on Delphi studies, general concerns about personal data being collected and concerns over one’s inability to correct any errors. A persistent finding, over several decades, is that it is fruitful to consider US consumers not as a general block but as consisting of 3 groups: privacy fundamentalists, the pragmatic majority, and the marginally concerned.

These groupings have been consistent across studies. In Ackerman et al., [1] these groups were 17%, 56%, and 27% of the sample respectively. In [1], the concerns of pragmatists were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on Web sites. Another interesting finding, also quite persistent, is that there is a large gap between most people’s stated preferences and their actual behavior. While this is often the case in social studies [12], it is of particular interest here.

IV. ECONOMIC ISSUES

The above presented security either as a technical authoritative or as a set of social and organizational issues; however, it must be stressed that security for both user and site needs an analysis with the proper weighing of potential risk. More importantly, as Anderson points out, security engineering is a matter of control and power as well as access [7, 8]. Security mechanisms can be used to manage compatibility and attempt to control network effects governing the adoption of new or potentially replacing technologies [46].

V. CONCLUSION

In summary, privacy and security are still ongoing research. There have been some exciting and important findings, however, in the last five years that stand key consequences for e-commerce sites and clients. Privacy is now understood, by many, to be a social structure with potentials the largest consideration. Yet, privacy is also considered a public issue by controllers, who have nonetheless largely allowed technology to unfold to date. Security is now understood to be largely imperfect. Important technical developments have been deployed in the last ten years; however, it is clear that organizational policies may play as an important a role in site security. Looking for the security and privacy issues and try to solve them are the main concern for most companies and organization which the most important things which they have is their information and they vulnerable. Here, we had a brief review on its issues and present some solutions.

REFERENCES


[18] Clarke, Roger,. Introduction to Dataeaveillance and Information Privacy, and Definition of Terms,1999.