Review chapter for the New Economy Handbook (Jones, ed.), in press

Privacy and Security Issues in E-Commerce

Mark S. Ackerman and Donald T. Davis, Jr.

Privacy – the control over one's personal data – and security – the attempted access to data by unauthorized others – are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both. This chapter reviews the current state of the art and the relevance for privacy and security respectively. We examine privacy from social psychological, organizational, technical, regulatory, and economic perspectives. We then examine security from technical, social and organizational, and economic perspectives.

1 Privacy

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher [2001] 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. (pp. 20-21)." 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 [Harris Poll 2000]. Similarly, Culnan [2000] 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. ([Culnan 2000], p. 8)." Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses [Culnan and Armstrong 1999]. 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 [Davies 1997] and [Etzioni 1999]. (Even these historical accounts have sharply differing viewpoints. For example Etzioni argues that privacy is societally illegitimate or infeasible, while Davies argues that it has become a squandered right.) For the purposes of this article, we will explore the potential space of privacy concerns, not privileging any particular viewpoint. In our view, both consumers and businesses may have legitimate viewpoints, sometimes conflicting. This is in the nature of most societal issues. We also restrict ourselves to the privacy issues that accrue in electronic commerce; we omit, for examples, the issues emerging from vehicle tracking chips, the wholesale monitoring of telephone and other communication mechanisms, and image recognition from public cameras (see [Froomkin 2000] for other examples).

Culnan [2000], following Westin, defines privacy as “the ability of an individual to control the terms under which their personal information is acquired and used.” An individual’s privacy, as such, is always in an inherent state of tension, since it must be defined in conjunction with capabilities of others to transact business and even to control their own privacy. As Clarke [1999] noted, privacy may have to be traded off in certain transactions, such as the access to credit or to maintain the quality of health care. Indeed, societal needs may also transcend an individual’s privacy concerns, as in the case of public health.

Nonetheless, individuals as e-commerce consumers, even with its inherent tradeoffs, still wish to control their personal information. Goffman [1961] noted that people must control their presentation of self, their face, to others. People need to be able to control what others think of them, and find it disconcerting when they cannot. Even more, people find it disconcerting when the rules of everyday conduct appear to change, as they can with new technologies. In these situations, people may feel that they have been unfairly treated or that they have not received proper notice [Culnan 2000].

Besides “privacy”, a number of terms -- such as notice, choice, identification, digital persona, authentication, anonymity, pseudonymity and trust -- are used in privacy discussions. However, because of space limitations we cannot hope to carefully to define each. See [Clarke 1999] for a useful introduction. Note, however, that there is a vigorous research debate surrounding many of these concepts.

1.1 Social and business issues

Why is privacy of concern to e-commerce? We believe this concern stems from a new technical environment for consumers and businesses, the resulting data flow with substantial benefits to businesses and consumers, consumer concerns in this new environment, and regulatory attempts to govern this environment. It is important to understand each one of these, and to understand the tradeoffs. Privacy as a business issue is extremely sensitive to changes in the surrounding context. Changes in people’s expectations (such as when they become accustomized to data transfer in commercial settings) or in regulatory governance (such as new laws, governmental regulations, or even case law in the US) 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 ameliorate 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, shopping patterns, 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 [Dhillon and Moores 2001]. 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. The data are valuable for reuse, for example, in finding potential sales to existing customers. As well, the data are also valuable to aggregators (who may look for other personal trends and patterns) or for other types of resale. Indeed, reuse and resale are simultaneously both potential opportunities and problems. “Ironically, the same practices that provide value to organizations and their customers also raise privacy concerns (p. 5).” [Culnan and Armstrong 1999]

From the viewpoint of customers, many e-commerce sites have done foolish things with their customers’ data [Fisher 2001]. Consumers’ opinions in this have been confirmed by media stories of particularly egregious privacy failures and public relations nightmares. Broadly speaking, consumers are merely 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 [Light 2001].

Culnan and Armstrong [1999] make the argument that consumers have two kinds of privacy concerns. First, they are concerned over unauthorized access to personal data because of security breaches (see below) or the lack of internal controls. Second, consumers are concerned about the risk of secondary use – the reuse of their personal data for unrelated purposes without their consent. This includes sharing with third parties who were not part of the transaction in which the consumer related his or her personal data. It also includes the aggregation of a consumers’ transaction data and other personal data to create a profile. Smith, Milberg, and Burke [1996] 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.

Beyond the research literature describing a general anxiety (and its extent), there is some research literature providing more detail. 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 [Westin 1991]: privacy fundamentalists, the pragmatic majority, and the marginally concerned. These groupings have been consistent across studies (e.g., [Ackerman, Cranor, and Reagle 1999], [Spiekermann, Grossklags, and Berendt 2001]). (Spiekermann et al. divided the pragmatics into those who were considered with revealing their identity and those who were more concerned about making their personal profiles available.) In Ackerman et al., these groups were 17%, 56%, and 27% of the sample respectively. Spiekermann et al. noted a larger group of privacy fundamentalists and fewer marginally concerned in Germany. The groups differ significantly in their privacy preferences and attitudes. The marginally concerned group is mostly indifferent to privacy concerns; privacy fundamentalists, on the other hand, are quite uncompromising about their privacy. The majority of the US population, however, is concerned about its privacy, but is willing to trade personal data for some benefit (e.g., customer service). Nonetheless, consumers still want adequate measures to protect their information from inappropriate sale, accidental leakage or loss, and deliberate attack [Dhillon and Moores 2001]. In [Ackerman, Cranor, and Reagle 1999], 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 ([Ackerman, Cranor, and Reagle 1999], [Spiekermann, Grossklags, and Berendt 2001]). While this is often the case in social studies [Bernard 2000], it is of particular interest here. It is not yet known, however, whether this gap is permanent, in that it is unlikely to change, or is the symptom of people's frustration with current technologies.

1.2 Technologies for privacy

The next consideration is technology. A number of technologies have altered the current privacy debates. Clark [2001] divides the technologies in question into 4 groups. Clarke argues that there are technologies used for surveillance, the technologies for forming agreements (contracting) 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 merchants…. [Clarke 2001]"

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. Other PETs attempt to provide genuine anonymity, and include anonymous remailers (e.g., Mixmaster) and digital cash (e.g., ECash). An active area of research and development are systems to provide non-traceable identifiers (e.g., ZKS Freedom, AT&T Crowds, anonymizer.com, anonymous remailers). Yet other PETs, which Clarke calls "gentle PETs", try to balance privacy and accountability. These include systems to provide some level of pseudonymity, allowing users to hide behind the pseudonyms but allowing actions to be traced back to a person if necessary. In addition, privacy seals (e.g., from TRUSTe or the Better Business Bureau) indicate that the company follows the privacy practices stated on their web site.

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) [Cranor and Reagle 1998, Cranor 2002, P3P 2002]. P3P allows sites to describe their data handling policies (P3P statements) and permits users to describe their preferences for releasing private data (P3P preferences). As sites label themselves with P3P and as user clients (such as Internet Explorer) handle P3P statements and preferences, it will be possible to create technologies to form contracts for the release of private data. Other technologies, such as those to help users understand contractual terms or even contract-related fraud, will also emerge. Ackerman and Cranor [1999] outline one such technology. Their browser-based agents watch for privacy violations, privacy scams, and the like on behalf of the user.

1.3 Regulation, economic issues, and privacy co-design

The final consideration is regulation. In this, we include the varying governmental attempts, whether by law or by decree, to regulate this new environment on behalf of their citizens. It also includes emerging legal precedents and case law for governing privacy in cyberspace. Currently, regulation is a warren of overlapping and conflicting attempts. Fortunately, these attempts are slowly consolidating. (Around 1997, it was thought possible that even municipalities might have their own, specific privacy regulations, holding ISPs and web services responsible for any violations.) Nonetheless, currently, there are wide differences between the United States and the European Union. To continue e-commerce, there has emerged a notion of "safe harbor" internationally, although it is not known how long this will continue.

In the US, privacy is largely a matter of economics, with the admonition that caveat emptor is the rule for consumers. Once data are provided by an individual to an e-commerce or anyone else, all rights to that data are lost. US consumers have no recourse, which may result in surveys' showing a lack of trust. A company can use that data in any way, including selling the data to third parties for subsequent reuse. There are, however, specific areas of greater protection, for example in medical records. In addition, the Federal Trade Commission (FTC), which regulates consumer and inter-state trade in the US, has taken upon itself to take particularly egregious privacy cases to court. For example, the FTC has taken large companies to court when they have violated their own sites' privacy statements. While many researchers and analysts (e.g., [Reidenberg 1999], [Culnan 2000]) have argued that self-regulation has largely failed, it is unlikely that there will be significant change under the current US administration. It is possible, however, that greater penalties may accrue to companies violating their own privacy statements.

In contrast, "Privacy rules are strikingly different in the European Union, and the differences threaten to hamper the ability of US companies to engage in transactions with European Union countries without risk of incurring penalties ([Fjetland 2002], p. 54)." Europeans must unambiguously give consent after being informed as to why the information will be used; this is not the case in the United States. According to European Union rules, consumers must be informed of the entity collecting the data, purposes of the processing, recipients of the data, and any rights they (the customers) have. Furthermore, one must ask for specific consent for "sensitive information" (person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual preference). Unlike in the US, European customers can have incorrect, or unlawfully processed data corrected, blocked, or erased, and consumers can even require that third parties who have seen incorrect data be notified.

The extent to which European Union privacy rules hold for companies is unclear. Technically, not only do the European Union rules apply to European Union citizens, they also apply even if the customer is outside the European Union if the data will be processed within the European Union. The onus is on the data user (i.e., the company or electronic commerce site), and the penalty can be the blockage of data transfers to the offending company. Currently, however, these European Union rules are suspended for American and international companies, and little if any enforcement is occurring for European Union companies. Not even all European Union countries have complied [Fjetland 2002]. As a "safe harbor", which has been the point of contention between the US and European Union governments, US and international companies must merely embrace a substantially diluted version of the privacy standards.

Thus far, we have largely examined privacy from a sociological stance; that is, as socially constructed expectations and sets of norms and regulations. Privacy can also be as an economic good. There has been considerable research recently in examining a marketplace for personal data. A general analysis of markets for data, including personal data, can be found in [Shapiro and Varian 1999]. An example of potential economic mechanisms for privacy data markets, including negotiation protocols, can be found in [Cranor and Resnick 2000].

Very recently, researchers have moved towards advocating approaches towards privacy that combines technology, regulation, and social change. The technologies may include economic mechanisms. Increasingly, privacy is considered a complex social phenomenon with interactions among new technologies, regulatory structures, and citizens' perceptions of privacy and social norms. Reidenberg [1999] and Cranor and Reagle [1998] have argued that e-commerce privacy requires a combination of law and technology, and Ackerman, Darrell, and Weitzner. [2002] have argued that solutions for privacy must simultaneously consider technology, social structures, and regulation in a co-design space.

2 Security

As mentioned, security is also a major concern for e-commerce sites and consumers alike. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved. We cover each in turn.

2.1 Security vulnerabilities in electronic commerce

There are many points of failure, or vulnerabilities, in an e-commerce environment. Even in a simplified e-commerce scenario – a single user contacts a single web site, and then gives his credit card and address information for shipping a purchase – many potential security vulnerabilities exist. Indeed, even in this simple scenario, there are a number of systems and networks involved. Each has security issues:

- A user must use a web site and at some point identify, or authenticate, himself to the site. Typically, authentication begins on the user’s home computer and its browser. Unfortunately, security problems in home computers offer hackers other ways to steal e-commerce data and identification data from users. Some current examples include a popular home-banking system that stores a user’s account number in a Web “cookie” which hostile web-sites can crack [Graves and Curtin 2000]; ineffective encryption or lack of encryption for home wireless networks [Borisov, Goldberg, and Wagner 2001]; and, mail-borne viruses that can steal the user's financial data from the local disk [Roberts 2002] or even from the user's keystrokes [Neyses 2002]. While these specific security problems will be fixed by some software developers and web-site administrators, similar problems will continue to occur. Alternatives to the home computer include Point-of-Sale (POS) terminals in brick-and-mortar stores, as well as a variety of mobile and handheld devices.

- The user’s web browser connects to the merchant front-end. When a consumer makes an online purchase, the merchant's web-server usually caches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit-card fraud. Further, such archives often hold 90 days' worth of customers' orders. Naturally, hackers break into insecure web servers to harvest these archives of credit card numbers. Several recent thefts netted 100,000, 300,000, and 3.7 million credit-card data, respectively. Accordingly, an e-commerce merchant's first security priority should be to keep the web servers' archives of recent orders behind the firewall, not on the front-end web servers [Winner 2002]. Furthermore, sensitive servers should be kept highly specialized, by turning off and removing all inessential services and applications (e.g., ftp, email). Other practical suggestions to secure web servers can be found in [Tipton and Krause 2002], [Garfinkel 2002], and [Garfinkel, Schwartz, and Spafford 2003], among many others.

- The merchant back-end and database. A site’s servers can weaken the company's internal network. This not easily remedied, because the web servers need administrative connections to the internal network, but web server software tends to have buggy security. Here, the cost of failure is very high, with potential theft of customers’ identities or corporate data. Additionally, the back-end may connect with third party fulfillment centers and other processing agents. Arguably, the risk of stolen product is the merchant's least-important security concern, because most merchants' traditional operations already have careful controls to track payments and deliveries. However, these third parties can release valuable data through their own vulnerabilities.

This is a simplified model of an e-commerce architecture; yet even in its simplicity, there are a number of security problems. Note that encrypted e-commerce connections do little to help solve any but network security problems. While other problems might be ameliorated by encryption, there are still vulnerabilities in the software clients and servers that must use the data. We will discuss the implications of these vulnerabilities below – users who may themselves release data or act in ways that place sites at jeopardy, the constant pressure of new technologies and the resulting constant threat of new vulnerabilities, as well as the requirements for critical organizational processes. However, before discussing potential requirements for e-commerce sites and their consumers, it is important to survey potential security technologies

2.2 Security technologies

There are many relevant technologies, including cryptographic technologies that can mitigate the above vulnerabilities. However, none is comprehensive or airtight by itself. Accordingly, we next present a brief overview of the major technologies, also considering the advantages and disadvantages of each. For a more complete description of each technology, see [Bishop 2003].

In the mass media, the most visible security technologies are the encryption algorithms. For a general introduction to these technologies see [Treese and Stewart 1998]; a popularization can be found in [Levy 2001]. Two classic textbooks are [Denning 1983] and [Koblitz 1994], and encyclopedic compendia include [Schneier 1996] and [Menezes, Van Oorschot, and Vanstone 1996].

Public key infrastructure (PKI) systems are one such encryption technology [Adams et al. 2001, CCITT 1988, Housley et al. 2002, Polk, Housley, and Bassham 2002]. Important PKI-based secure protocols include the retail mechanism Secure Socket Layer (SSL) [Dierks and Allen 1999, Rescorla and Schiffman 1995] and the interbank standard suite, ANSI X9 [American National Standards Institute 1994, RSA Security 2003a]. 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* [Diffie and Hellman 1976, Rivest, Shamir, and Adelman 1978]. 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 [Adams and Farrell 1999]. This issue, the *revocation problem*, is still unsolved [Davis 1996, Davis 1998], despite the best effort to date [Myers et al. 1999].

A digital signature [Rabin 1978, Rivest, Shamir, and Adelman 1978] is *the* salient application of public-key cryptography (and by extension, of PKI), 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 (e.g., financial, entertainment, medical); 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. While e-commerce digital signatures have been much anticipated, they have been little adopted to date. There is still substantial research potential in understanding the legal and economic issues involved in the lack of widespread adoption of digital signature-based electronic commerce.

In symmetric key systems, on the other hand, the same key is used for both encryption and decryption, so it must always be guarded as a secret. For e-commerce applications, the principal examples of symmetric key systems are the ciphers DES [NIST 1993], AES [NIST 2001], and RC4 [RSA Security 2003b], as well as Microsoft's Hailstorm authentication system (formerly PassPort). As advantages, symmetric key cryptography runs orders of magnitude faster than public key cryptography.

These ciphers can be used in a variety of ways. As noted above, the technical challenge in authenticating users is that the identifying information must remain private but the Internet is a public broadcast medium. Cryptography meets this challenge by guaranteeing that the subscriber's identifying information cannot be stolen, copied, or replayed by others. It was once supposed that most users would use public-key cryptography to authenticate themselves. However, very few end users possess public key certificates currently, because certificates are expensive. Instead, web users use a variant of SSL in which users identify themselves with passwords instead of with digital signatures. A second way in which e-commerce sites validate users' passwords is with HTTP cookies. Cookie-mediated authentication, however, is very insecure [Dawson 1998, Festa 1998]. Symmetric key cryptography offers more security than password-mediated authentication with more favorable key management tradeoffs than PKI affords, but as noted above, the key must be tightly guarded.

Other technologies can be used to perform both authentication and data protection. For example, smart cards [Rankl and Effing 1997] can be used to store data about the bearer of the card, including financial data, medical records, identification credentials. Because those data are so sensitive, it is critical to store the associated encryption keys in tamper-resistant hardware. Further, the smartcard shouldn't ever have to share the bearer's personal data or his keys with a POS terminal, otherwise the bearer's privacy and keys could be compromised. In practice, this means putting a computer processor and cryptographic hardware on the card, along with the encryption keys. A further advantage is that smartcards can allow POS transactions to be more intricate, because all the user's data is always available. This architecture can also avoid the centralized storage of personally sensitive data, and supposedly demands less trust of the consumer to a centralized authority to husband the data properly. Smartcards have the disadvantage that every promise of tamperproof packaging has been shown false [Anderson and Kuhn 1996, Anderson and Kuhn 1997]. Smartcards saw early and widespread deployments in Europe, especially in Germany, Benelux, and France, but not in the U.S. The reason for smart cards' adoption failure in the US remains unclear.

Similarly, cryptographic technologies can be used in various points in the payment system [Neuman and Medvinsky 1998]. The majority of Web transactions are currently SSL-protected credit card transactions. However, many other mechanisms have been proposed for handling electronic payments. Digital cash and networked payments (e.g., [Chaum 1985] purport to bring anonymous electronic transactions to e-commerce; that is, like currency and unlike credit cards, digital cash cannot be traced to any specific individual. Thus, a consumer might buy electronic data or a digital service without revealing his identity to the merchant, and without revealing his purchases to a financial clearinghouse. There are many digital cash variants, but Chaum's version was the archetype, using digital signatures and encryption to simulate the issuance of paper currency with serial numbers. In some variants, this currency can be given to others while not having the side effects of allowing counterfeiting, duplication, or double-spending. Micropayment schemes, such as MilliCent [Glassman et al. 1995] are systems for transferring extremely small payments, perhaps fractions of cents, for Internet goods (often information goods). The goal in this case is to enable the creation of markets for small quantities of data and services, such as per-article newspaper subscriptions. Despite these interesting social and technical advantages, these sophisticated digital payments schemes haven't thrived, for a variety of reasons. Shirkey [2000] has provided sharp arguments on why micropayments have not caught on: the history of communication markets shows that users greatly prefer simple and predictable pricing schemes. The Mondex anonymous payments system has been successful in Europe, but cryptographers have raised questions about Mondex's security [Brehl 1997]. Similarly, PayPal, a payment intermediary, has been financially successful but has been plagued by repeated problems with fraud [Jonas 2002]. Indeed, Stefan Brands, a cryptographer specializing in the design and analysis of digital cash systems, noted in 1996 that of the digital cash issued in European pilot deployments, 10% had been lost to fraud [Brands 1996].

Recently, the entertainment and mass media industries have invested much effort in digital watermarking technology [Delaigle, De Vleeschouwer, and Macq 1996]. Here, the technical goal is to find ways of cryptographically tagging electronic content (especially images and audio) in a way that is recognizable, non-forgeable, and nonremovable. The business goal is to enable firms to detect unlicensed distribution or re-sale, in hope of firms being able to distribute content electronically and safely. The watermark tag is generally designed to be invisible or unobtrusive. This is still an active area of research, as all proposals to date have been successfully attacked [Craver et al. 2001]. Currently, the entertainment industry is using the Digital Millennium Copyright Act of 1998 (DMCA) to bolster with law the technical weaknesses of digital watermarking proposals, by making it illegal in the US to remove or forge such protections [Lazowska 2001].

2.3 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 [Treese and Stewart 1998]. 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, rather than the technology per se [Anderson 1994]. The second is software engineering management, or managing how security technology is deployed [Anderson 2001a]. The third is the development of adequate organizational processes for risk management, separation of duties, development of security policies, access control, and security assurance.

A persistent problem is users' differing and incorrect models of security and their seeming inability or unwillingness to adhere to critical security policies and guidelines. Not only do users not understand what they need to do, they often will not take the precautions necessary for the security technologies to work effectively [Davis 1996]. For example, users may store passwords in unencrypted files on vulnerable machines or employees may divulge their passwords to third parties. The ability for hackers to obtain critical authenticity data is well known; it is often called "social engineering" [Mitnick and Simon 2002]. Currently this is an open research area. There is research work on understanding user's mental models and motivations (e.g., [Adams and Sasse 1999], [Friedman et al. 2002]), but little on how to deal with the problem. We suggest that a networked application cannot offer full measures of connectivity, security, and ease-of-use, all at the same time; there seems to be an intrinsic trade-off here, and some sacrifice is unavoidable. Until security vendors achieve the necessary delicate balance of all three desiderata, effective e-commerce security will remain a problem.

A second problem is that software management is a substantially larger problem with security than with many other types of software. As mentioned, hackers constantly discover new vulnerabilities in both new and existing systems. Standards and protocols are in a state of constant turmoil. 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 [Schneier 2001]. Indeed, since many merchants' e-commerce applications rely on client-side security features, it is important to remember that security holes tend to be very version-specific, making the software portability problem even worse. In addition, assessment of new security-relevant technologies is at once urgent and quite difficult. It is particularly hard to determine which technical proposals will succeed, but to be competitive and to avoid embarrassment, firms can't afford to wait for standards to settle, before beginning to build and deploy security solutions. Finally, in software management, security programmers are a limiting resource. There is currently a dearth of programmers who understand security, and the software they write usually is subtle and hard to maintain, but naturally, security specialists don't want to be boxed in to dead-end software maintenance jobs. Thus, security products are often poorly maintained, with old security holes re-appearing from time to time.

User and employee limitations as well as the chronic problems of software management suggest that organizations need to have a set of organizational processes in place to assess security vulnerabilities, manage their risk, and contain intrusions [Bishop 2003, Treese and Stewart 1998]. (One is again referred to applied security publications, such as [Garfinkel 2002, Tipton and Krause 2002], for the details of specific policy and process recommendations.)

Organizational processes can offer important security protections. By creating a chain of responsibility and the proper separation of duty, organizations can be protected against intrusions as well as criminal insiders. Organizations must consider and insist upon policies for confidentiality of data as well as the integrity of the data; that is, there must be policies in place to prevent both the leakage and the corruption of data [Bishop 2003]. Organizations must strive to create processes for determining access control to sensitive data, how intrusions or break-ins will be contained, and levels of risk [Tipton and Krause 2002] and assurance. (See [Bishop 2003] for a discussion of formal methods in security assurance.)

Without the necessary technologies and organizational processes in place, merchants stand to lose just as much as consumers, proportionally, if an e-commerce deployment is insecure. Security breaches are newsworthy, and a merchant must be able to protect customers' identities, financial data, and shopping choices from exposure, so as to avoid alienating loyal customers.

Moreover, an underappreciated risk is that an insecure e-commerce server can undermine corporate regulatory compliance. In the US, this risk is particularly important for financial systems, because securities laws require brokerages to keep extensive archives of internal communications, and to prevent even insiders from accessing certain documents. An insecure e-commerce deployment can cause a financial institution to leak information in actionable ways, can allow insiders to cover up misdeeds, or can even allow insiders to generate falsified audit-logs of non-existent transactions.

2.4 Economic issues

Again, an understanding of security would be incomplete without an analysis of the underlying economic issues. The above presented security either as a technical imperative or as a set of social and organizational issues; however, it must be stressed that security for both consumer and site requires 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 [Anderson 1994, Anderson 2001b]. Security mechanisms can be used to govern compatibility and attempt to control network effects governing the adoption of new or potentially replacing technologies [Shapiro and Varian 1999]. Indeed, Anderson argues that security technologies are often deployed as much for risk reassignment as risk reduction. An excellent collection of links to economics-based analyses of security is http://www.cl.cam.ac.uk/~rja14/econsec.html.

3 Conclusion

In summary, privacy and security are still ongoing research problems. There have been some interesting and significant findings, however, in the last five years that bear important consequences for e-commerce sites and consumers. Privacy is now understood, by many, to be a social construction with expectations the largest consideration. Yet, privacy is also considered a public issue by regulators, who have nonetheless largely allowed technology to unfold to date. Security is now understood to be largely imperfect, the continual cat-and-mouse game of security expert and hacker. Important technical developments have been deployed in the last five years; however, it is clear that organizational policies may play as an important a role in site security. Finally, detailed economics- and sociologically- based analyses are beginning to find their way into the published literature, and we expect that these studies will bring greater clarity and proficiency to admittedly murky areas.

References

Ackerman, Mark S., and Lorrie Cranor. 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99)* : 258-259.

Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce* : 1-8.

Ackerman, Mark S., Trevor Darrell, and Daniel J. Weitzner. 2002. Privacy in Context. *Human-Computer Interaction*, 16 (2-4) : 167-176.

Adams, Anne, and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Communications of the ACM*, 42 (12) : 40-46.

Adams, C., and S. Farrell. 1999. Internet X.509 Public Key Infrastructure certificate management protocols. Internet RFC 2510.

Adams, C., P. Sylvester, M. Zolotarev, and R Zuccherato. 2001. Internet X.509 Public Key Infrastructure data validation and certification server protocols. Internet RFC 3029.

American National Standards Institute. 1994. Accredited Standards Committee X9 Working Draft: Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman. ANSI X9.42-1993.

Anderson, Ross. 1994. Why Cryptosystems Fail. *Communications of the ACM*, 37 (11) : 32-40.

Anderson, Ross. 2001a. *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: John Wiley & Sons.

Anderson, Ross. 2001b. Why Information Security is Hard - An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*

Anderson, Ross, and M. Kuhn. 1996. Tamper Resistance - A Cautionary Note. *Proceedings of the Second USENIX Workshop on Electronic Commerce* : 1-11.

Anderson, Ross, and M. Kuhn. 1997. Low Cost Attacks on Tamper-resistant Devices. *Proceedings of the Security Protocols, 5th International Workshop* : 125-136.

Bernard, H. Russell. 2000. *Social Research Methods: Qualitative and Quantitative Approaches.* Newbury Park, CA: Sage.

Bishop, Matt. 2003. *Computer Security*. New York: Addison-Wesley.

Borisov, N., I. Goldberg, and D. Wagner. 2001. Intercepting Mobile Communications: The Insecurity of 802.1. *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking* : 180-189.

Brands, Stefan. 1996. Electronic Cash. Invited talk, RSA Cryptographers' Colloquium.

Brehl, B. 1997. Security of `Cash Cards' Questioned. *Toronto Star*, October 6, 1997, E1-2.

CCITT. 1988. Recommendation X.509: The Directory - Authentication Framework. Data Communications Network Directory, Recommendations X.500-X.521.

Chaum, David. 1985. Security Without Identification: Transaction Systems To Make Big Brother Obsolete. *Communications of the ACM*, 28 : 1030-1044.

Clarke, Roger. 1999. Introduction to Dataveillance and Information Privacy, and Definition of Terms. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Clarke, Roger. 2001. Of Trustworthiness and Pets: What Lawyers Haven't Done for e-Business. http://www.anu.edu.au/people/Roger.Clarke/EC/PacRimCL01.html.

Cranor, Lorrie, and Joseph Reagle. 1998. The Platform for Privacy Preferences. *Communications of the ACM*, 42 (2) : 48-55.

Cranor, Lorrie F. 2002. *Web Privacy with P3P*. Cambridge: O'Reilly & Associates.

Cranor, Lorrie Faith, and Paul Resnick. 2000. Protocols for automated negotiations with buyer anonymity and seller reputations. *Netnomics*, 2 : 1-23.

Craver, S., J. McGregor, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. Wallach, D. Dean, and E Felten. 2001. Reading Between the Lines: Lessons from the SDMI Challenge. Unpublished manuscript, to have been presented at the Fourth International Information Hiding Workshop, http://cryptome.org/sdmi-attack.htm.

Culnan, Mary J. 2000. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy and Marketing*, 19 (1) : 20-26.

Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1) : 104-115.

Davies, Simon G. 1997. Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In *Technology and Privacy: The New Landscape*. Edited by P. Agre and M. Rotenberg. 143-165. Cambridge, MA: MIT Press.

Davis, Don. 1996. Compliance Defects in Public-Key Cryptography,. *Proceedings of the 6th Usenix Security Symposium* : 171-178.

Davis, Don. 1998. Non-linear Complexity of Revocation-checking. Post to the Cryptography Mailing List, Nov. 11, 1998. http://world.std.com/~dtd/compliance/revocation.html.

Dawson, K. 1998. JavaScript Privacy Bugs Hit Netscape, Then Microsoft. *Tasty Bits from the Technology Front*, October 12, 1998,

Delaigle, J-F., C. De Vleeschouwer, and B. Macq. 1996. Digital Watermarking. *Proceedings of the Conference 2659 - Optical Security and Counterfeit Deterrence Techniques* : 99-110.

Denning, D. 1983. *Cryptography and Data Security*. New York: Addison-Wesley.

Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37.

Dierks, T., and C. Allen. 1999. The Transport Layer Security Protocol. Internet RFC 2246.

Diffie, W., and M. Hellman. 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22 (6) : 644-654.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

Festa, P. 1998. Navigator Still Has Bug Problem. *CNet News.com*, October 7, 1998,

Fisher, Susan. 2001. Privacy By Design. *InfoWorld*, 23 (27) : 20-22.

Fjetland, Michael. 2002. Global Commerce and the Privacy Clash. *Information Management Journal,* 36 (1) : 54-58.

Friedman, Batya, David Hurley, David C. Howe, Edward Felten, and Helen Nissenbaum. 2002. Users' Conceptions of Web Security: A Comparative Study. *Proceedings of the ACM Conference on Human Factors and Computers (CHI'02)* : 746-747.

Froomkin, A. Michael. 2000. The Death of Privacy? *Stanford Law Review*, 52 : 1461-1543.

Garfinkel, Simson. 2002. *Web Security, Privacy and Commerce*. Cambridge, MA: O'Reilly and Associates.

Garfinkel, Simson, Alan Schwartz, and Gene Spafford. 2003. *Practical Unix Internet Security*. Cambridge, MA: O'Reilley.

Glassman, S., M. Manasse, M. Abadi, P. Gauthier, and P. Sobalvarro. 1995. The MilliCent Protocol For Inexpensive Electronic Commerce. *Proceedings of the Fourth International World Wide Web Conference*

Goffman, Erving. 1961. *The Presentation of Self in Everyday Life*. New York: Anchor-Doubleday.

Graves, P., and M. Curtin. 2000. Bank One Online Puts Customer Account Information At Risk. http://www.interhack.net/pubs/bankone-online.

Harris Poll. 2000. Online Privacy: A Growing Threat. *Business Week,* March 20, 2000, 96.

Housley, R., W. Polk, W. Ford, and D. Solo. 2002. Internet X.509 Public Key Infrastructure certificate and Certificate Revocation List (CRL) profile. Internet RFC 3280.

Jonas, J. 2002. PayPal's Tenuous Situation. http://catless.ncl.ac.uk/Risks/21.92.html#subj6.

Koblitz, N. 1994. *A course in number theory and cryptography*. Berlin: Springer-Verlag.

Lazowska, E. 2001. Overview of CRA and Felten et al. http://lazowska.cs.washington.edu/felten/FeltenOverview.pdf.

Levy, Steven. 2001. *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*. New York: Viking.

Light, David A. 2001. Sure, You Can Trust Us. *MIT Sloan Management Review*, 43 (1) : 17.

Menezes, Alfred J., Van Oorschot, Paul C., and Scott A. Vanstone. 1996. *Handbook of Applied Cryptography*. New York: CRC Press.

Mitnick, Kevin D., and William L. Simon. 2002. *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley and Sons.

Myers, M., R. Ankney, A. Malpani, S. Galperin, and C. Adams. 1999. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Internet RFC 2560.

Neuman, B. Clifford, and Genyady Medvinsky. 1998. Internet Payment Services. In *Internet Economics*. Edited by L. W. McKnight and J. P. Bailey. 401-416. Cambridge, MA: MIT Press.

Neyses, J. 2002. Higher Education Security Alert From the U.S. Secret Service: List of Keystroke Logging Programs. http://www.unh.edu/tcs/reports/sshesa.html.

NIST. 1993. Data Encryption Standard. FIPS PUB 46-2. http://www.itl.nist.gov/fipspubs/fip46-2.htm.

NIST. 2001. Advanced Encryption Standard (AES). FIPS PUB 197. http://csrc.nist.gov/encryption/aes/.

P3P. 2002. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. MIT/World Wide Web Consortium. http://www.w3.org/TR/P3P/.

Polk, W., R. Housley, and L. Bassham. 2002. Algorithms and Identifiers For the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet RFC 3279.

Rabin, M. O. 1978. Digitalized Signatures. In *Foundations of Secure Computation*. Edited by R. Lipton and R. De Millo. 155-166. New York: Academic Press.

Rankl, W., and W. Effing. 1997. *The Smartcard Handbook*. New York: John Wiley.

Reidenberg, Joel R. 1999. Restoring Americans' Privacy in Electronic Commerce. *Berkeley Technology Law Journal*, 14 (2) : 771-792.

Rescorla, E., and A. Schiffman. 1995. The Secure HyperText Transfer Protocol. Internet Draft, version 1.1.

Rivest, Ron, A. Shamir, and L. Adelman. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2) : 120-126.

Roberts, P. 2002. Bugbear Virus Spreading Rapidly. *PC World Online*, Ocotober 2, 2002,

RSA Security. 2003a. What Are ANSI X9 Standards? Cryptography FAQ, http://www.rsasecurity.com/rsalabs/faq/5-3-1.html.

RSA Security. 2003b. What Is RC4? Cryptography FAQ, http://www.rsasecurity.com/rsalabs/faq/3-6-3.html.

Schneier, B. 1996. *Applied Cryptography*. New York: John Wiley & Sons.

Schneier, B. 2001. The Security Patch Treadmill. *Crypto-Gram Newslette*, Mar 15, 2001, http://www.counterpane.com/crypto-gram-0103.html#1.

Shapiro, Carl, and Hal R. Varian. 1999. *Information Rules*. Cambridge, MA: Harvard Business School Press.

Shirkey, C. 2000. The Case Against Micropayments. O'Reilly OpenP2P.com, Dec. 19, 2000, http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, June : 167-196.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. *Proceedings of the ACM Conference on Electronic Commerce* : 38-46.

Tipton, Harold, and Micki Krause. 2002. *Information Security Management Handbook*. New York: CRC Press.

Treese, G. Winfield, and Lawrence C. Stewart. 1998. *Designing Systems For Internet Commerce*. New York: Addison-Wesley.

Westin, Alan F. 1991. *Harris-Equifax Consumer Privacy Survey 1991*. Atlanta: Equifax, Inc.

Winner, D. 2002. Making Your Network Safe for Databases. *SANS Information Security Reading Room*, July 21, 2002,