The Future of e-Commerce Security

Pita Jarupunphol* and Wipawan Buathong*

ABSTRACT

The growth of e-commerce clearly relies upon a strong support from consumers and merchants. Since security of sensitive information is an issue of concern to e-commerce consumers, it is vital to have security criteria and mechanisms in order to address this issue. Recently, there have been several secure e-commerce applications invented to fulfil e-commerce end-user security requirements. Many of these applications, however, have not really taken on because they fail to meet e-commerce end-user implementation requirements. For successful implementation of secure e-commerce applications, there is a need of coordination between e-commerce application developers and e-commerce end-users. Currently, it can be seen that this requirement has not yet been achieved. The more security requirement is fulfilled, the less systems meet implementation requirements. This paper considers current situation and the future of e-commerce security.

KEYWORDS: electronic commerce (e-commerce), ecommerce end-users, software developers, security requirements, implementation requirements, secure e-commerce applications.

1. BACKGROUND

It is clear that many public/private sectors have already adopted e-commerce technologies in order to provide their organisations and communication partners with a number of benefits. However, several factors must also be taken into an account when implementing e-commerce requires, since sensitive and financial information must rely upon Internet technologies generally considered as untrusted environment.

Nowadays, there have been several secure e-commerce applications invented to fulfil e-commerce end-user security requirements. Many of these applications, however, have not really taken on because they fail to meet e-commerce end-user implementation requirements [1, 2, 3, 4]. For successful implementation of secure e-commerce applications, there is a need of coordination between e-commerce application developers and e-commerce end-users. Currently, it can be seen that this requirement has not yet been achieved. The more security requirement is fulfilled, the less systems meet implementation requirements. In this paper, a number of security and implementation aspects of secure payment mechanisms for e-commerce, including PKI and trusted computing have been discussed.

2. e-Commerce security: the end-user perspective

As can be seen in a number of literatures [3, 5, 6, 7, 8], e-commerce security means different things to the various parties involved in a transaction. In addition, the level of security requirement is unpredictable, since it is strongly dependent upon e-commerce end users. In this section, we summarise e-commerce security from an end-user perspectives based on a number of literatures as follows.

2.1 Security as a key enabler

It is widely accepted that the growth of e-commerce depends on how much the public trusts online transactions [3]. In this context, security is potentially a key enabler to the growth of e-commerce.

2.2 Security as a promotional tool

Currently, security has been used by many e-commerce organisations to promote their e-commerce systems and also in accordance to the previous perspective. Thus security can be a positive factor for the organisations implementing it.

2.3 Security as an excuse

As has already been discussed in [1, 2, 3, 6, 7, 8], e-commerce end-users claim to be concerned about the security of e-commerce transactions. However, when an effective secure e-commerce application, developed based on security requirements, was proposed (i.e. SET), implementation issues became an insurmountable barrier to its adoption. Even though the application is usable, the end-users have opted for a much simpler and less secure solution, i.e. SSL/TLS, that requires minimal effort to implement.

2.4 Security as a sensational topic

While security can be used to promote the reputation of an e-commerce organisation, it is often treated by the media in a sensational way in order to attract public attention [9].

2.5 Security as a replacement tool

Unlike traditional shopping methods, e-commerce is a non face-to-face shopping method in which the consumer and merchant must trust each other without having the usual security assurances derived from a face-to-face interaction. When used to protect an e-commerce transaction, cryptographic security measures can replace the security elements found in traditional shopping methods, but that are missing in e-commerce. For example, a digital signature can replace a traditional signature, and a digital certificate can replace credentials (documents, tokens or plastic cards) held by end-users.

2.6 Security as a risk prevention method

While there are a number of risks associated with Internet e-commerce, security can be used as a tool to prevent or minimise such risks.

3. Classifying e-commerce security

It can be seen that there have been many technical and managerial issues concerning e-commerce security since after the emergence of this alternative marketing approach. In this section, we identify e-commerce security into four major domains.

* Department of Informatics, Faculty of Science and Technology, Phuket Rajabhat University

3.1 Physical world

E-commerce security relies upon the proper configuration of physical devices, such as firewalls, web servers, etc. If these physical devices are improperly configured, ecommerce systems may become a target for fraudsters, who can search for vulnerabilities arising from misconfiguration of physical devices.

3.2 Digital world

E-commerce security relies on various mechanisms applied to physical devices in order to provide e-commerce security services. For example, cryptographic mechanisms can be used to provide e-commerce systems with confidentiality, integrity, and authentication. Some of these mechanisms can offer varying levels of security. For example, the SSL/TLS protocol can employ encryption with 40 to 128 bit key lengths. E-commerce end-users can choose the most appropriate method to address the security issues.

3.3 Operational world

Effective deployment of security mechanisms to protect e-commerce transactions requires end-users to have sufficient knowledge and skills to use them properly. In addition to skills and knowledge, e-commerce security relies to some extent on the trustworthiness of the end-users, in spite of the fact that not everyone online can be completely trusted.

3.4 Social world

E-commerce is based upon trust relationships between merchants and consumers. Since trust relationships can be influenced by many factors, such as membership of a social system, the level of trust in e-commerce varies widely. This is inevitable since trust relies upon human factors that can be highly volatile. In [7, 9] culture, familiarity, and the influence of members of a social system can affect ecommerce end-user perceptions.

4. Computing and communications speed and the future of e-commerce security

We next discuss how the future of e-commerce security is likely to be affected by the continuing rapid growth in computing and data communications speed.

The speed and availability of both computer processing and data communications continues to increase, enabling the provision of ever more complex applications. In this connection it is interesting to note that the speed of a 2001 personal computer is comparable to that of a 1990 supercomputer [10]. In addition, it can be seen that the speed of a personal computer at the present time is much higher than that of a 2001 personal computer. These increasingly complex applications are typically designed to facilitate their operation by the majority of unsophisticated end-users, who require something both effective and easy to use. This means that the true complexity of what is being undertaken on behalf of the end user is often hidden, which is potentially dangerous, not least because the end user will have no conception of the possible risks involved in using the application.

The rapid increases in computing and communications speed also mean that malicious parties can exploit them to penetrate information security systems, including those based on cryptographic techniques.

It is thus important to assess the impact of increasing computing and communications speeds on the future of ecommerce security.

4.1 Computer processing speed and e-commerce security

Security in the e-commerce world almost inevitably relies on the use of cryptographic techniques to protect data transferred across unreliable communications channels such as the Internet. The continued growth in computing power and availability has meant that cryptographic techniques considered secure 20 years ago, such as DES, are clearly no longer adequate. The effect of the growth in both the number and power of personal computers is dramatically exemplified in the 'records' for the bit lengths of RSA moduli factored using general purpose PCs cooperating across the Internet, as given in Table 1.

This means that systems implemented today, and designed to last for a number of years, must take into account the continuing likely growth in power available to cryptanalysts. A number of experts have predicted the likely lifetimes of a range of RSA key lengths — see Table 2.

Similar remarks apply to symmetric cryptosystems, although AES using a 128-bit key appears likely to be sufficiently secure for many years to come [11] (unless, of course, there is a breakthrough in cryptanalysis).

While DES was cracked few years ago, AES is claimed to be an unbreakable cryptographic algorithm for 20 years lifetime [11]. However, since searching for a valid key depends on how fast computer can perform, it is important to consider Moore's law [12] indicating that the computer speed increase double every couple of years. In addition to the double increase of the computer speed, the price of computer hardware also rapidly reduces. According to a research at Intel Silicon, an exponential growth in the number of transistors per integrated circuit observed by Moore has been maintained. Table 3 shows that the number of transistors has been growing every couple of years at double rate.

However, we realise that cracking AES is still not realistic even though the computer speed is faster than the current speed ten times. Our concern is that will cryptographic mechanisms used in Internet e-commerce always use AES to secure data communication, since various approaches have been invented to break cryptographic algorithms from time to time. For example, the grid computing technique that was successfully used to break DES few years ago is still a serious issue to consider. With the integration of all modern computers, the security of sensitive information during data transmission appears to be at risk. Of course, once the secure risk is exposed, consumer trust in Internet e-commerce security will be uncertain.

4.2 Data communications speed and e-commerce security

Apart from the extremely fast growth of computer speed, the Internet traffic has also increased tremendously from time to time. In [13] the Moore's Law has been applied to analyse

the growth of Internet traffic by the authors. Although there is no precise conclusion that whether the Internet traffic growth rate is 3 times or 4 times every year, it is sufficient for any businesses or individuals to know that its growth is at least more than double. For example, the traffic of Internet backbones in US increased from 1,500 terabytes in 1995 to between 20,000 and 35,000 terabytes in 2000.

The availability of low-cost network bandwidth is also continuing to grow very rapidly. For general Internet users, broadband Internet access, as provided by ISDN and ADSL, is rapidly growing in popularity amongst the public. The bandwidth of a broadband connection is much greater (up to 20 times faster) than that of a modem connection, which only offers up to 56 kb/s. From NUA Internet surveys5 of March 2003, it was predicted that over 41 million European households will be accessing the Internet using high-speed broadband connections by 2006. A recent survey of February 2005 conducted by eMarketer has proved that the prediction was correct. It shows that broadband Internet users in the US increased from 71.5 millions in 2003 to 86.5 millions in 2004. In addition, it predicted that the US broadband Internet users will reach 157.3 millions by the end of 2008 while dial-up Internet users will decline to 31.2 millions.

According to a national survey of November 2005 regarding mode of access to the Internet of Thai people conducted by National Electronics and Computer Technology Center (NECTEC), the rate of ADSL Internet users increased sharply from 1.6% to 43.1% during the period 2003-2005. In comparison to the rate of dial-up Internet users that went down from 54.3% to 30.9%, it implies that broadband Internet connection in Thailand will continue to dominate dial-up Internet connection for many years to come.

Table 1. *The bit lengths of RSA numbers factored using general purpose PCs [14]*

Years	Lenght (decimal digits)	Number	Who	Method	Hardware
1970	39	$2^{128}+1$	Brillhart/Morrison	CFRAC	IBM Mainframe
1978	45	$2^{223}-1$	Wunderlich	CFRAC	IBM Mainframe
1981	47	$2^{225}-1$	Gerver	QS	HP-3000
1982	51	$5^{91}-1$	Wagstaff	CFRAC	IBM Mainframe
1983	63	$11^{93}+1$	Davis/Holdridge	QS	Cray
1984	71	$10^{71}-1$	Davis/Holdridge	QS	Cray
1986	87	$5^{128}+1$	Silverman	MPQS	LAN Sun-3s
1987	90	$5^{160}+1$	Silverman	MPQS	LAN Sun-3s
1988	100	$11^{104}+1$	Internet	MPQS	Distributed
1990	111	$2^{484}+1$	Lenstra/Manasse	MPQS	Distributed
1991	116	$10^{142}+1$	Lenstra/Manasse	MPQS	Distributed
1992	129	RSA-129	Atkins	MPQS	Distributed
1996	130	RSA-130	Montgomery	GNFS	Distributed
1998	140	RSA-140	Montgomery	GNFS	Distributed
1999	155	RSA-512	Montgomery	GNFS	Distributed
2003	160	RSA-160	Bahr et al.	GNFS	Distributed
2003	174	RSA-576	Franke	GNFS	Distributed

Table 2*. The likely lifetimes of cryptographic key lengths. Source: RSA Laboratories — TWIRL and RSA Key Size*

Protection Lifetime of Data	Present - 2010	Present - 2030
Minimum secretkey length	80 bits	112 bits
Minimum RSA key length	1024 bits	2048 bits

While the rapid growth of computing speed can have either a positive or negative effect on e-commerce security, the sharp increase in Internet communications capabilities appears to have solely beneficial effects for both end-users and e-commerce generally. Some obvious benefits from using high-speed Internet connections are as follows.

- Internet users are now able to conduct e-commerce transactions much more quickly than with previous connection methods.
- Internet users are much less likely to encounter situations where their browsers do not respond quickly enough when searching for Internet products or services, or do not respond quickly after the payment button has been clicked.
- Merchants can enhance their web sites with more complex features in order to make them look more attractive.
- Merchants can more easily provide Internet users with statements regarding consumer confidentiality [7, 8].

Nevertheless, there are also serious consequences of the rapid growth in data communication capabilities on the future of e-commerce security. The continuing growth in computing and data communications speeds will facilitate distributed attacks of various types. This includes Denial of Service attacks as well as distributed cryptanalysis. In the latter context, the Grid computing techniques [10, 15], that require high-speed data communications to support network resource sharing environments, may eventually have serious implications.

5. Emerging security technologies

We now review certain recently developed technologies that appear likely to have an impact on the future of ecommerce and its security.

Table 3. *The growth in the number of transistors per integrated circuit.*

Processor Types	Years of introduction	Transistors
4004	1971	2,250
8008	1972	2,500
8080	1974	5,000
8086	1978	29,000
286	1982	120,000
386TM processor	1985	275,000
486TM DX processor	1989	1,180,000
Pentium	1993	3,100,000
Pentium II	1997	7,500,000
Pentium III	1999	24,000,000
Pentium IV	2000	42,000,000
Itanium	2001	300,000,000
Projected Roadmap	2007	1,000,000,000

5.1 The Liberty Alliance Project

The Liberty Alliance Project6 involves a number of wellknown public/private sector companies, including computer/IT related and mobile phone companies as well as financial institutions. The objective of Liberty is to support trust, commerce, and communications on the Internet. The project has produced a series of specifications, the latest version of which were published in [16, 17], for a service known as Internet single sign-on. The Liberty model for a single sign-on involves two types of service-providing entities, as follows.

- Service providers are organisations that offer Webbased services to users. This includes all types of ecommerce merchants.
- Identity providers are organisations that provide an identity verification service to Service providers. An Identity provider will authenticate an end-user, using stored user credentials, and can then vouch for the correctness of the user identity to one or more Service providers; this means that users do not need to possess the means to authenticate to every individual Service provider.

Within the LAP-based transaction, end-users are required to provide and authenticate their identities via either an identity provider or a service provider. When the user visit the company Website of a affinity group member, the company will notice that whether the user has already visited other Websites of the group member. In the meantime, the user will be asked to federate his/her identity with other affinity group members. Besides these processes, the LAP uses a single-sign on technology to facilitate the user for his/her next visit. As a consequence, the user no longer need to authenticate several times when connecting to any affinity group members after once the user has already authenticated his/her identity with a affinity group member.

The objectives of the LAP are as follows.

- Enable consumers to protect the privacy and security of their network identity information
- Enable businesses to maintain and manage their customer relationships without third party participation
- Provide an open single sign-on standard that includes decentralised authentication and authorisation from multiple providers
- Create a network identity infrastructure that supports all current and emerging network access devices

It can be seen that LAP does not emphasise security in e-commerce transactions, but deals with how entities in e-commercecan trust each other without third-party interference. In addition, the LAP scheme does not require consumers to provide their personal information to every web site that they visit once the consumer has already registered with either service providers or identity providers. This is very useful for most consumers who are so concerned about their privacy.

5.2 The Trusted Computing Group (TCG)

The Trusted Computing Group (formally known as the Trusted Computing Platform Alliance or TCPA) [18, 19] is a broadly-based industry working group including a number of well-known hardware/software organisations, such as, HP, IBM, Intel and Microsoft.

In a recent TCG specification [20] it is stated that concerns about the security of communications, transactions, and wireless networks are inhibiting the realisation of the benefits associated with pervasive connectivity and electronic commerce. The purpose of TCG is to develop, define, and promote open, vendor-neutral industry standard specifications for trusted computing. These include hardware building block and software interface specifications across multiple platforms and operating environments. Use of these standards will help users keep the data and digital identities on their systems more secure from external software attack and physical theft.

Microsoft's Next-Generation Secure Computing Base (NGSCB) [21, 22] is a good example of a TCG architecturebased product that seems to be destined to play an important role in the future of computer and communications security. NGSCB is a new security technology for the Microsoft Windows

platform that uses TCG-compliant hardware in conjunction with a secure software system to give end-users new kinds of security and privacy protection.

As a consequence, the TCG architecture would appear to have the potential to be beneficial to the future of ecommerce security, since it provides the means to address many of the potential e-commerce security risks.

5.3 XML Key Management Specification (XKMS)

The Extensible Markup Language (XML) specification [23], describes a class of data objects called XML documents, and partially describes the behavior of computer programs which process them. XML is an application profile for (i.e. a restricted form of) the Standard Generalized Markup Language or SGML [24]. By definition, XML documents are also SGML documents.

XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure of a document [23]. XML has a structure that is designed to be readily understood, and has a fixed set of markup options [25].

XML is increasingly being used by Internet e-commerce web sites, since it supports emerging Internet technologies such as theWeb Services architecture. This latter concept is based on core standards that allow entities to communicate with each other, including UDDI (Universal Description, Discory, and Integration) for describing the services, WSDL (Web Services Description Language) for establishing communication using HTTP, and SOAP (Simple Object Access Protocol) for exchanging communications between entities encapsulated within HTTP. Apart from these core standards, XML is also used by the Web Service architecture, examples of which include the recently lunched .NET platform and the Java-based 'J2EE' environment. Although the relative usefulness of these two web servicesbased products remains a matter for debate [27, 28] (some claim that .NET is much easier to use, and applications can be developed more quickly, whilst others recommend J2EE because of its greater flexibility), web services undoubtedly offer benefits in addressing interoperability issues among different product platforms.

XKMS is another Web Service that provides an interface between an XML application and a PKI [29]. Some writers have questioned [30] whether Internet e-commerce needs PKI, since XML also provides similar security services, including XML digital signatures, XML encryption, and XML key management services. However, it is generally agreed that PKI is still required for e-commerce security for two main reasons [30]: many applications that use PKI are not Web services, and PKI is the *only* choice available for connecting business relationships to keys and identities when more than one domain is involved.

XKMS transfers complex processing tasks from the client application to a Trust Service that facilitates the deployment of PKI. The XKMS protocol is currently being standardised by a World Wide Web Consortium work group, co-chaired by Baltimore Technologies.

XKMS can help to support PKI-based e-commerce in several ways [29]. Firstly, it requires a very small client footprint that make PKI much simpler to implement. Secondly, the XML syntax greatly simplifies PKI implementation.

6. Trends in e-commerce security

In this section, we conclude by considering key trends in the provision of security for e-commerce.

6.1 Data Transmission Security

SSL/TLS has long been used in Internet prior to the emergence of e-commerce, since it is effective in providing security during data transmission. After e-commerce had been introduced to the public, this standard mean was still used in most e-commerce organisations to ensure that all sensitive information transmitted remain confidential and integral. This is not only 'ready to use' features of SSL/TLS, but also consumer risk perceptions in which data transmission is often considered as the weakest link. Numerous consumers are concerned that their financial information will be stolen during data transmission.

6.2 Transaction Security

After this trend, a number of security mechanisms have been invented from time to time in order to fight against potential fraud associated with online shopping. In the meantime, several types of fraudulent techniques have been developed and used by malicious people, who want to gain access to sensitive information of cyberspace community. As a result, focusing on data transmission security is insufficient to address several major concerns, since e-commerce transaction security involves wider scopes in which any potential risks in e-commerce transaction security must be addressed.

6.3 Software Usability

We have mentioned earlier that implementation issues of SET are because the software developers too focussed on technical aspects based on e-commerce end-user security concerns. Every designing process seems to be carried out by a group of people who expertise in security software development fields. This is similar to the early stage of software design and development when end-users used the products mainly designed by software developers [31]. However, when the users found that the product is very difficult to use, it is infeasible for the less usability product to compete with others.

6.4 Software Implementation

After SET failures, implementation requirements have become another major concern to security software developers, since it was found that security requirements alone could not be used as main perspectives for designing the softwares. A number of security mechanisms invented for secure e-commerce transactions during these periods of time are mutually designed from major security and implementation aspects, i.e. the efforts on SET extensions and invention of

the 3D e-payment architecture [4, 32]. As we mentioned before, even thought SET is now much easier to use, it is still not convincing for end-users whose implementation requirements are getting very hard to achieve.

6.5 Trusted-Based Computing Environment

As can be seen earlier, several upcoming security mechanisms for e-commerce are designed to increase trust relationships in Internet community not just secure Internet e-commerce transactions. Most mechanisms require all entities involved in Internet communication to be trusted and verified. In the meantime, the mechanisms must be easily implemented by the entities. For example, using the LAP scheme, consumers need to register to either service providers or identity providers, so that the LAP members can verify them. In addition, consumer can also verify service provider and identity providers under the LAP verification chain. In addition to LAP, all computing elements used within the scheme must also be verified in order to ensure that there are no flaws associated with the communication security in TCPA. In the XKMS web services, all entities involved will be verified, since XKMS provides essential services in which XML and PKI can be integrated.

7. Conclusions

As has already been discussed, security means different things to different parties. We have therefore attempted to classify the main aspects of security from an end-user perspective. It can be seen that computing and data communications capabilities steadily increase, and both of these increases have a potentially significant impact on e-commerce and its security. More powerful and more numerous computers, advances in distributed computing (as exemplified by the Grid), all combined with steady advances in cryptanalytic techniques, mean that key lengths need to be increased over time; indeed, all aspects of security for an ecommerce system need to be subjected to continuous review.

Furthermore, we have also examined three areas in which new technologies may play a significant role in the future of e-commerce and its security. It is to be hoped that developers of e-commerce security solutions will take on board the lessons of past failures and will ultimately develop security solutions which are both robust and easy to implement and use. Once this goal has been reached, whether or not e-commerce end-users understand e-commerce security can perhaps be ignored, since it is sufficient for end-users to know that the e-commerce system is secure, i.e., they will not need to understand how security in e-commerce is implemented. This fits with Odlyzko [33] who argues that when people use security features '[t]hey do not have to know anything about the complicated algorithms that were used. Similarly, to drive over a bridge, all we need is an assurance that it is safe, and we do not require personal knowledge of the materials in the bridge'.

References

[1] P. Jarupunphol and C. J. Mitchell. Failures of SET implementation: What is amiss? In *Proceedings of 7th Asia- Pacific Decision Sciences Institute Conference 2002. ISSN:1539-1191*. National Institute of Development Administration, July 2002.

[2] P. Jarupunphol and C. J. Mitchell. Implementation aspects of SET/EMV. In J. L. Monteiro, P. M. Swatman, and L. V. Tavares, editors, *Towards the Knowledge Society: eCommerce, eBusiness and eGovernment, The 2nd IFIP Conference on e-commerce, e-business and e-government, IFIP I3E 2002*, pages 305–315. Kluwer Academic Publishers (IFIP Conference Proceedings 233), Boston (2002), October 2002.

[3] P. Jarupunphol and C. J. Mitchell. Measuring SSL and SET against e-commerce consumer requirements. In *Proceedings of the International Network Conference (INC 2002)*, pages 323–330. Plymouth University Press, July 2002.

[4] P. Jarupunphol and C. J. Mitchell. Measuring 3-D Secure and 3D SET against e-commerce end-user requirements. In *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*, pages 51–64. National University of Ireland, Galway, June 2003.

[5] A. Bhatnager, S. Misra, and H. R. Rao. On risk, convenience, and internet shopping behaviour. *Communications of the ACM*, 43(11):98–106, November 2000.

[6] P. Jarupunphol and C. J. Mitchell. Actual and perceived levels of risk in consumer e-commerce. In *Proceedings of 2nd International We-B Conference*, pages 207–216. Edith Cowan University Press, November 2001.

[7] P. Jarupunphol and C. J. Mitchell. Consumer risk perceptions in e-commerce. In *Proceedings of UKAIS 2002*, pages 308–315. Leeds Metropolitan University, April 2002.

[8] P. Jarupunphol and C. J. Mitchell. The future of SET. In *Proceedings of UKAIS 2002*, pages 9–17. Leeds Metropolitan University, April 2002.

[9] P. Jarupunphol and C. J. Mitchell. E-commerce and the media — influences on security risk perceptions. In W. Cellary and A. Iyengar, editors, *The 1st IFIP Workshop on Internet Technologies, Applications and Societal Impact, WITASI '02*, pages 163–173. Kluwer Academic Publishers (IFIP Conference Proceedings 232), Boston (2002), October 2002.

[10] I. Foster. The Grid: A new infrastructure for 21*st* century science. *Physics Today*, 55(2):42–47, February 2002.

[11] F. Piper. Some trends in research in cryptography and security mechanisms. *Computers and Security*, 22(1): 22–25, January 2003.

[12] G. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, April 1965. ftp://download.intel.com/research/silicon/moorespaper.pdf.

[13] K. G. Coffman and A. M. Odlyzko. *Internet growth: Is there a 'Moore's Law' for data traffic*. AT&T Labs – Research, revised version edition, June 2001.

[14] R. D. Silverman. A cost-based security analysis of symmetric and asymmetric key lengths. Technical Report 13, RSA Laboratories, April 2000.

[15] I. Foster and C. Kesselman, editors. *The Grid: Blueprint for a New Computing Infrastructure*, chapter 2: Computational Grids, pages 15–51. Morgan Kaufmann,

San Francisco, 1999.

[16] Liberty Alliance Project — Version 1.2. *Liberty ID-FF Architecture Overview*, 2003. http://www.projectliberty.org/specs/index.html.

[17] Liberty Alliance Project — Version 1.2. *Liberty ID-FF Protocols and Schema Specification*, 2003. http://www.projectliberty.org/specs/index.html.

[18] S. Pearson, B. Balacheff, L. Chen, D. Plaquin, and G. Proudler. *Trusted Computing Platforms — TCPA Technology in Context*. Hewlett-Packard Books, Upper Saddle River, New Jersey, 2003.

[19] Trusted Computing Group. *Trusted Computing Group (TCG) — Main Specification (Version 1.1b)*, February 2003. http://www.trustedcomputing.org/docs/.

[20] Trusted Computing Group. *Trusted Computing Group — Backgrounder*, 2003. https://www.trustedcomputing group.org/downloads/.

[21] M. Abadi and T. Wobber. *A Logical Account of NGSCB*, September 2004.

[22] M. Peinado, Y. Chen, P. England, and J. Manferdelli. *NGSCB: A Trusted Open System*, September 2004.

[23] W3C. *Extensible Markup Language (XML) 1.0*, 2nd edition, October 2000.

[24] International Organization for Standardization, Gen'eve, Switzerland. *ISO 8879:1986(E). Information processing — Text and Office Systems – Standard Generalized Markup Language (SGML)*, 1st edition, October 1986.

[25] L. Mignet, D. Barbosa, and P. Veltri. The XML web: a first study. In *The Twelfth International World Wide Web Conference*. WWW2003, May 2003. http://www.cs.toronto.edu/ mignet/Publications/www2003.pdf.

[26] P. Wilson. Web services security. *Network Security*, 2003(5):14–16, May 2003.

[27] G. Miller. The web services debate—.NET vs. J2EE. *Communications of the ACM*, 46(6):64–67, June 2003.

[28] J. Williams. The web services debate — J2EE vs. .NET. *Communications of the ACM*, 46(6):59–63, June 2003.

[29] P. M. Hallam-Baker and W. Ford. XML Key Management Specification (XKMS). In *The Tenth International World Wide Web Conference*, ISBN 962-85361-3-3. WWW10 Limited, May 2001. http://www10.org/cdrom/posters/1129.pdf.

[30] S. Farrell and M. Zolotarev. XML and PKI — what's the story? *Network Security*, 2001(9):7–10, September 2001.

[31] D. E. Avison and G. Fitzgerald. *Information Systems Development:Methodologies, Techniques and Tools*. McGraw Hill, Maidenhead, 2nd edition, 1995.

[32] P. Jarupunphol. A critical analysis of 3-D Secure. In *Proceedings of the 3rd Electronic Commerce Research and Development (E-COM-03)*, pages 87–94. Gdansk, Poland, October 2003.

[33] A. M. Odlyzko. Economics, psychology, and sociology of security. In J. Camp and R. Wright, editors, *Financial Cryptography: 7th International Conference, FC 2003*, volume 2742 of *Lecture Notes in Computer Science*, pages 182–189. Springer-Verlag, 2003.