6

Global digital commerce: Impacts and risks for developments of global information societies

Klaus Brunnstein and Kathrin Schier
Faculty for Informatics, University of Hamburg
Vogt-Koelln-Str. 30, D - 22527 Hamburg-Stellingen
Phone: +49 40 5494 2406, Fax : +49 40 5494 2226
Email: Brunnstein@rz.informatik.uni-hamburg.d400.de,
schier@informatik.uni-hamburg.de

Abstract

Many regard the Internet as a prototype of an information infrastructure on which a global information society may be built. Some enterprises are trying to take advantage of early applications of digital commerce on the Internet. As the Internet is missing essential features of reliability, functionality and confidentiality which are prerequisites for the fair distribution of risks between market participants, current digital commerce services load all the risks on customers and users. This paper discusses some essential requirements for safe and functionally acceptable information services, and it discusses current problems with actual examples from digital payment systems. The paper concludes that public and legal action is required to release customers and users from their overwhelming share of risks.

INTRODUCTION

Concepts of global information societies depend strongly upon the existence and reliable operation of either a unique global (worldwide) information infrastructure or, if several such concepts or structures exist in limited spatial or organizational contexts (dedicated networks such as SWIFT, regional networks, or intranets), on the global acceptance and implementation of a set of standards which, if enforced, guarantee a minimum degree of interoperability of independent information infrastructures. Besides its required global availability, such infrastructures must also support the distribution of and access to information at any of their single

An Ethical Global Information Society J. Berleur & D. Whitehouse (Eds.)

components. In this context, the meaning of information has deliberately been neither specified nor defined *a priori*. Indeed, only the technical implementations of information, as streams of bits transmitted (communication standards: protocols, name services etc.), files of documents stored (databases) and accessed (agents), prescription for processes (executables), structures (relations, directories, dictionaries etc.) of any kind of agglomeration of bits, must be defined to determine the technical details of such infrastructures. This technology-driven approach leaves maximum freedom to its users (at least to those parties dominating information infrastructure usage) to define the purpose, applications and content within such information infrastructures. This implies that social aspects and user concern play a limited role in present developments.

Many people, from technical experts to interested parties of all kinds (not excluding politicians), regard the Internet (which is not a unique information infrastructure but which acts as a cooperation of independently operated networks using a multitude of platforms) as a prototype of a global information infrastructure. If the Internet were indeed such a prototype, then studies of its design and development, experiences with its present usage and services including incidents and malicious usage as well as observations of public discussions about its benefits, should be instructive to discuss likely developments of societies based on related technologies.

Indeed, there is good reason to analyze likely or potential influences of information and communication technologies on updating present societies into future stages wishfully named information societies. It is not the first time in human history that technologies have shaped the developments of societies. Since ancient times, technical abilities and facilities have contributed to shaping societies; one can study such impact in cultural masterpieces such as the Tower of Babylon, the Egyptian pyramids, Greek temples or mediaeval cathedrals with their respective forms of state organization. More recent (and, in several aspects, more relevant) examples may be the impact of Gutenberg's printing machine, as well as the complex set of industrial machines which supported developments in industrial societies. A retrospective analysis of 230 years of industrial history (starting in 1765 with Watts' basic patent of the vapour-driven machine), especially including its false hopes and real dangers (for example, inhumane workplaces and inadequate consumer protection), may be very helpful in understanding the risks and requirements for future developments, and to support forgotten requirements (such as in developing legal systems to protect users).

As the industrial societies differ so visibly and so strongly from those societies valid at their start in their respective domains (nations, areas, organizations etc.), it might be interesting to analyze historical developments against the technical concepts basically built into the dominant industrial techniques. When some achievements (such as the contemporary understanding of concepts such as work or the market) are related to the basic concepts of their constituent technologies, this analysis may also lead to an *a priori* analysis of likely impacts of present information and communication technologies on future information societies.

Following such thoughts, the paper analyses whether and to what degree (if at all) contemporary information technologies fulfil the basic requirements of global digital commerce. Besides, the general implications of technical concepts (part 2), the developments and risks of electronic payment systems are discussed in some

detail (parts 3-4) as one major driving factor of Internet commerce. Finally, some general requirements for improved customer protection in information societies are discussed (part 5).

RISKS CAUSED BY BASIC TECHNICAL PARADIGMS AND CONCEPTS OF THE INTERNET

To measure and predict the side-effects, in both wishful and beneficial but also in possibly hazardous and undesirable directions, of actual information and communication technologies, the following frame of reference is suggested:

In order that any information technology can be regarded as a globally accepted basis for commercial activities, services derived from such technologies must fulfil a set of requirements (R1-4) from the beginning:

R1) Services must be well-defined, reproduced and controlled.
R2) Services must be available when needed, and must work reliably.
R3) Misuse or unauthorized use of services must be excluded.
R4) Proper means must guarantee that customers can trust services even if they do not understand how they work.

It is interesting to analyze whether and to what degree the Internet supports such services on any acceptable level of functionality, safety, and security. The facts may be shocking:

The Internet's basic built-in concepts of communication, especially packet-driven data exchange built on TCP/IP protocols and naming conventions are technically well-defined but in a way that misuse is easy to manage and hard to detect. The following experiences (for example, reports of Computer Emergency Response Teams (CERTs)) are ubiquitous:

- *Spoofing*: it is easy to misuse electronic addresses;
- *Sniffing*: inherent in demands for performance monitoring, it is easy to monitor and store foreign electronic traffic;
- *Hijacking*: it is easy to steal or misuse data streams;
- *Manual or Automated Hacking*: it is easy to access or misuse services or information which should be solely accessible or used from its owner; there are multiple sites on the Internet which offer introductory or assistant material on hacking techniques;
- *Malicious Agents*: it is easy to design malicious software exploiting features or weaknesses of Internet services; such malicious software may even distribute itself through the network, and it will be difficult (if not impossible) to control activities or consequences of such agents;
- *Malicious Documents*: even documents regarded as non-malicious for long times can import unforeseeable malicious side-effects into a single local Internet station.

As the Internet does not fulfil any of the above-mentioned requirements (R1-R4) even on a minimum level of service, the Internet cannot be regarded as a relevant prototype of a global information infrastructure, at least from the point of view of customer protection. Otherwise, an information infrastructure based on contemporary insecure and unsafe technologies will provide such serious risks to digital commerce that related applications can at best work only with severe

restrictions. The following examples of digital commerce, namely Internet-based payment systems, show how some services may be conceived to reduce risks somewhat but that there are side-effects, for example, on user privacy that develop even from security mechanisms.

EXAMPLE: INTERNET-BASED PAYMENT SYSTEMS: RISKS AND IMPACTS FOR THE GLOBAL SOCIETY

Information technology provides an important support to many different financial services like various payment mechanisms and remote banking. Industrial developments push the use of electronic payment mechanisms. A huge amount of information technology is already in use or in pilot projects to support Internet-based financial services. People are beginning to use the Internet for widespread applications. Transferring money on a chipcard, buying goods over the net, booking and paying travels via the net, or using remote banking will become more and more common.

The new network technology changes people's everyday life very quickly. In the past, and still somewhere in the present, people had to go outside of their home to work, shop, or manage their banking. These activities were often combined with important social and personal contacts. Especially old and lonely people used the daily walks to the bank or to the shops to get some personal talks and contacts with other people.

Nowadays, and in some foreseeable future, properly equipped people can arrange their daily shopping, banking, and even working, directly from their home. Information technologies like international networks make it possible and viable. The Internet seems to satisfy all commercial needs: it supports the mechanisms to buy goods, information and services and to do remote banking over the net. Today, several different types of electronic payment systems are more or less available and usable.

Internet banking started with the transmission of credit card numbers over the net for paying ordered goods and services; this mode is obviously rather insecure. Now, there are concepts for digital money, digital credit cards, digital cheques and digital coupons at least in test phases which seem to fulfil some security requirements.

Digital payment systems can be seen as the electronic representation of conventional payment schemes. Therefore, all characteristics of conventional schemes have to be implemented in their digital analogies. Indeed, Internet banking overcomes some of the disadvantages of traditional money: digital money can be easily accessed (if an access service is available), stored and transmitted to any remote location, and its exchange into any other currency is done just-in-time (as multiplication with a suitable currency factor). In the following four world-renowned pilot projects, payment mechanisms will be discussed briefly.

Digital Money: Mondex

The concept of digital money proposed by Mondex International [Mondex 96] especially provides the property of transferability of money between private

persons. The money is stored on a chipcard; it is more than an Internet payment system because it can also be used in ordinary (not networked) shops. The money on the card can be stored in five different currencies. With an additional device, money can be transferred from one card to another. Both cards have to authenticate each other. A personal identification number can be used to lock the card but no authentication will happen if the card is 'open'. While transferring money, identification data can be stored to prevent unauthorized use. Payment profiles should help to block a card suspected of misuse but, at the same time, risks of misuse of personal data are evident. Pilot projects started in Swindon in Britain and with major banks in Australia.

Digital Money: Ecash

Ecash [Digicash 96] is designed for secure payments from any personal computer to any other workstation over Internet or email. Ecash is one-sided anonymous. When paying with Ecash, the identity of the customer is not revealed automatically. During the payment he/she can identify him/herself, but only when he/she chooses. When clearing a transaction, the merchant is identified by the bank. Before Ecash can be used to purchase products, it must first be withdrawn from the bank. The withdrawal uses a blind signature to prevent the bank from recognizing the coins as having come from a particular account. Customers create the coins at random, hide them in a digital envelope and send them off to the bank. The bank withdraws them from the customer's account and makes them valid using an embossed stamp on the envelope before returning them to the customer's computer. Now, the money can be spent in a shop or between private persons. When merchants receives the money, they automatically send it to the bank and wait for the acceptance before sending the goods to the customer along with a receipt.

Digital Credit Cards: Secure Electronic Transaction (SET)

VISA and MASTERCARD have jointly developed the Secure Electronic Transaction (SET) Protocol as a method for bank-card transactions over open networks [SET 96]. The SET protocol provides a payment gateway, an institution which organizes the transfer of money from the consumer's bank to the merchant's bank. The protocol is divided into two phases, the purchase request and the payment authorization. In the purchase request, the first phase handles the initiation request and response, followed by the second phase where the purchase request and response take place between the consumer and the merchant. The payment authorization will be done by authorization request and response, and it will capture the request and response via the payment gateway. This procedure enforces a certification process producing certificates binding the user's identity to the person's public encryption key. SET uses cryptographic methods to provide confidentiality of information, payment integrity and authentication of consumers and merchants. Here, there are problems with the strength of cryptosystems as well as the legality of their usage.

Digital Coupons: Millicent

In December 1995, the System Research Centre of Digital Equipment Corporation presented the Millicent Protocol for Inexpensive Electronic Commerce [Millicent 96]. It is designed for very small amounts of money, so it should not require high security standards. The idea of this protocol is based on a new currency named *Scrip*. Scrip is comparable with tickets or coupons, therefore it depends on the product and its merchant. The protocol contains three different types concerning security, complexity and secrecy. On the lowest level, one finds Scrip in the clear which is very easy and efficient, and uses no cryptography at all. The Private and Secure type uses encryption and digital signatures to ensure privacy and integrity of the user and the transaction. While using public key algorithms, it is quite slow. A compromise is the Secure without encryption type, which renounces privacy while only using digital signatures.

These four new digital payment systems offer several new payment mechanisms but also introduce huge possibilities for misuse. The Internet is completely insecure and unreliable, and it is not acceptable to provide these financial services without reflecting on the impacts for society and without caring for the security and privacy needs of individual customers. Some concepts have built-in security features. Presently, means of encryption and digital signatures are used to secure electronic transactions over the Internet. It is quite established to use a symmetric algorithm (like Data Encryption Standard (DES)) for quick encryption as well as asymmetric algorithms (like Rivest, Shamir, Adleman (RSA)) for creating digital signatures. One still unresolved problem is the establishment of an international solution for key exchange and certification authorities. Some national or regional suggestions exist to solve this problem but global concepts are missing. The situation is especially complex as relevant national laws and regulations start from different assumptions and are somewhat contradictory.

Another problem is concerned with suggestions for key escrow and regulations for export licenses for symmetric and asymmetric algorithms. Limitations of the key length decrease the security of the algorithms and will not be of any help in detecting criminal actions over the net. A law for depositing a part of the used key will not hinder criminally-oriented people from hiding information in other ways. Several methods, summarized as steganography, allow the hiding of information in texts and pictures, etc. Everyone who has seen pictures treated with steganography knows that it is impossible to detect whether a picture contains any secret information or not. For an example, look at the two pictures of Shakespeare presented on a special webpage: one is hiding information, the other is not [Stegano 96].

Besides these more technical problems, other problems are concerned with legal and social implications. In several countries with a constitutional or regulatory basis of privacy, the fact that data protection cannot be guaranteed when user data are collected during transmission is of major importance. With broader usage of financial services, new threats develop especially when user profiles are collected without proper customer protection.

SPECIAL REQUIREMENTS FOR PROTECTING USERS OF FINANCIAL INTERNET SERVICES

New technical and organizational institutions for trusted key management and new trusted services have to be installed to decide what kind of information or services conforms with the responsible organization's policy. The price for such improved security may be high, as this leads to growingly complex technologies providing a little bit more security within the intrinsically insecure technology of the Internet. In this way, easy handling of these systems is lost, and people need to become experts to ensure a correct and secure usage.

Besides the technical requirements for secure electronic payment systems, a lot of organizational or even social aspects have to be required and specified to support proper implementation. The use of asymmetric cryptographic algorithms enforces a structure for key management. The keys have to be created, issued and administrated by a trusted third party (TTP). This party or another trustworthy organization signs the public keys and gives out certifications of validity and any expiring information. Additional tasks can include consulting and teaching about security issues and how to use security in an effective way. Trusted third parties should also built up trust in new payment systems or should at least inform the users about trustbuilding activities. To realize an effective work of trusted third parties, acceptance studies are necessary to find out what the users really need. Nowadays almost all acceptance studies are product-oriented and not, as they should be, user-oriented. A new approach to the area of acceptance studies is necessary. The general question behind such concepts is : if trusted third parties are at least initially trustworthy, can customers safely assume that they remain trustworthy under any future conditions (for example, after unfriendly take-overs by other parties)? At least, legal prescriptions (which are presently being discussed in several countries including Germany) should allow users to get legal assistance in cases of TTP frauds.

Following traditional security requirements, an essential requirement is that all relevant financial transactions are logged and audited. Audit data can help to detect unauthorized use of systems or even to prevent misuse. As usual, auditing of logfiles is the weakest point, because the logfiles contain very interesting information about the financial behaviour of people. If logfiles are audited in an unauthorized way, the information can be misused for advertising or marketing purposes. It depends on the point of view if this is wanted or not. From the privacy viewpoint, it is very delicate to create profiles about financial behaviour and to sell them to commercial companies. So there has to be a strict regulation of the purposes of auditing and using audit data. The users have to be informed about the use of the information being collected about them. For that reason (and even for others), it is necessary to provide anonymous payment systems for daily use. The electronic form of ordinary payment systems must have at least the same properties as the ordinary ones have. Especially the form of coins has the property of being anonymous. So it has to be required that there is free choice of using anonymous payment systems whenever they are wanted, independent of whether they are in an electronic form or not.

GENERAL REQUIREMENTS FOR PROTECTION OF CUSTOMER INTERESTS AND RIGHTS

The cases given are just very obvious examples of what happens, usually at the expense of customers and users, with the introduction of so-called information infrastructures. Less obvious are other changes, for example, in controlling the growth of the (formerly national, now worldwide) monetary system as well as its misuse in such issues as how to detect and hinder the laundering of digital money. From discussions of other risks, one reaches the following general conclusions:

- *If Internet-like techniques are used, huge risks arise, most of which materialize at the expense of the weakest parties in the game: customers and users!*
- *If present trends in information economies continue, the winners will be the suppliers of those technologies which today determine all the features but which guarantee nothing, thus rendering users, customers and those affected by the technologies with no chance of influencing features essentially structuring such information societies!*

To avoid such perspectives, control of developments must be broadened from supply-side control to include all participants, especially users, customers and those indirectly affected by such developments. This approach may be compared to Ralph Nader's contribution to customer protection in the 1950s. As cars *were* unsafe at any speed in those times, Nader began to fight a long but eventually successful battle to develop customer-friendly legislation, mainly at the expense of car manufacturers. Presently, the situation is similar to the missing qualities of cars in the 1950s: customers have no support when information technology services fail, and the Internet is unsafe at any speed. In order to develop guarantees for the quality of IT products and services, developers and vendors must be forced, for example, by legal action (possibly initiated by customer protest) to change their design, implementation and services accordingly.

One basic prerequisite for such a development will be that politicians and bureaucrats stop painting insecure and unsafe techniques in inadequately beautiful colours. It must become common knowledge that present computer and network techniques (including PCs, the various UNIX systems, Internet and intranets) are not reliable and not functional enough to make future economies and human lives dependent on them. Such insight (though difficult without hands-on experience with crashing personal computers and failing Internet email) may become a starting point for a Ralph Cyber-Nader to fight for customer protection against the disadvantages of digital commerce.

REFERENCES

[Digicash 96]Product information, Digicash (http://www.digicash.nl)
[Millicent 96] Information about Millicent (http://www.research.digital.com/SRC/millicent/)
[Mondex 96] Information about Mondex (http://www.mondex.com/mondex/)
[SET 96] SET specification, Visa and Mastercard 1996,
(http://www.visa.com/cgi-bin/vee/sf/set/intro.html)
[Stegano 96] Information about Stegano, 1996,
(http://patriot.net/-johnson/html/neil/stegdoc/sec101.html)