**SLAVKO ŠARIĆ**, D.Sc.
**DRAGAN PERAKOVIĆ**, B.Eng.
Fakultet prometnih znanosti
Vukelićeva 4, Zagreb
**DANIJEL BARA**, Eng.

Traffic Safety
Review
U.D.C. 681.188:62-759.8
Accepted: Jan. 19, 1998
Approved: May 6, 1998

# PROBLEM OF INFORMATION SECURITY TRAFFIC ON INTERNET

*SUMMARY*

*Internet information traffic becomes greater and more important. With increasing growth of information importance requirement for its security becomes indispensable. The information security problem especially affect large and small companies whose prosperity is depending on Internet presence. This affecting the three areas of Internet commerce: credit card transactions, virtual private networks and digital certification. To ensure information traffic it is necessary to find a solution, in a proper way, for three major problems: frontier problem, market problem and government problem. While the eventual emergence of security standards for Internet transactions is expected, it will not automatically result in secure Internet transactions. In future, there is a wealth of security issues that will continue to require attention: internal security, continued hacking, social engineering, malicious code, reliability and performance, skills shortages and denial of service attacks.*

## 1. INTRODUCTION

In an age of explosive worldwide growth of electronic data storage and communications, many vital national interests require the effective protection of information.

Information security or infosec is about protecting three things: the confidentiality, integrity, and availability of data. Few years ago, Internet commerce did not exist. Today it attracts enormous financial interest. The investors are enthusiastically backing companies that promise to deliver the hardware and software which Internet commerce requires. Companies are investing in purchases of hardware and software to permit them to engage in Internet commerce.

For many companies, Internet commerce means taking credit card orders from customers shopping electronic catalogues on the World Wide Web. For others Internet commerce means dealing electronically with clients and suppliers, as an alternative to private, leased-line EDI over VAN's (Value Added Networks). This use of the Internet is sometimes called a Virtual Private Network (VPN) or *tunneling*. A third area of Internet commerce, which overlaps both of the others and includes areas largely unexplored, is digital authentication (of anything from contracts and invoices to photographs and sound bites).

The issues involved in Internet commerce affect large and small companies. The Internet is attractive to smaller companies because it enables them to reach a wide audience and market with a presence as impressive as that created by much larger entities. At the same time, most major corporations see enough potential to invest significant dollars.

## 2. AREAS OF INTERNET COMMERCE

The security problems affecting the three areas of Internet commerce are summarized in the following three sections.

### 2.1 Credit card transactions

There is considerable, and justifiable fear that confidential information, such as credit cards and personal details, could be intercepted during transmission over the Internet, for example when submitting an order form on the Web (Figure 1). The challenge is to transmit and receive information over the Internet while insuring that:

- it is inaccessible to anyone but sender and receiver (privacy),
- it has not been changed during transmission (integrity),
- the receiver can be sure it came from the sender (authenticity),
- the sender can be sure the receiver is genuine (nonfabrication),
- the sender cannot deny he or she sent it (nonrepudiation)

Without special software, all Internet traffic travels without protection and so anyone who monitors traffic can read it. This form of attack is relatively easy to intercept using freely available *packet sniffing* software since the Internet has traditionally been a very open network.

Usually, a sniffing attack proceeds by compromising a local ISP at one end of the transmission. No special physical access is required. It is also possible eavesdrop using network diagnostic hardware, if you have physical access to the network cabling. Passwords and credit cards can be distinguished from the rest of the traffic using simple pattern matching algorithms. The defense against this type of attack is to encrypt the traffic, or at least that portion that contains the sensitive data. However, encryption incurs performance overhead and requires coordination between legitimate parties to the communication.

One can note that protecting transactions is only one element of the secure transaction problem. Once confidential information has been received from a client it must be protected on the server. Currently, Web servers are among the softest targets, largely due to the immaturity of the technology.

Following Web risks can be identified:

1) Private or confidential documents stored in the Web site's document tree falling into the hands of unauthorized individuals.
2) Private or confidential information sent by the remote user to the server (such as credit card information) being intercepted.
3) Information about the Web server's host machine leaking through, giving outsiders access to data that can potentially allow them to break into the host.
4) Bugs that allow outsiders to execute commands on the server's host machine, allowing them to modify and damage the system.

The standard security advice for Web servers is to treat the machine as a sacrificial lambs that is unconnected to any in-house networks and regularly backed up in order to recover from the inevitable attacks. However, many Web applications now in vogue require that the Web server interact with company databases, necessitating a link to internal networks. This link then becomes a pathway into the system from owner's Web site. While firewall technology can help to block this path, it is seldom installed or maintained effectively and does not protect many Web services [1].

### 2.2 Virtual private networks

This is a specialized form of encrypted Internet transaction allowing a secure channel (or tunnel) to be established between two systems for the purposes of EDI. Tunneling allows information to be securely passed between one computer and another over a public network as if the two were connected by a single physical wire. After authenticating the tunnel client and the tunnel server, information is encrypted by its sender, encapsulated into TCP/IP data packets, and sent across the Internet as unreadable and unrecognizable data. Once they reach their final destination, the packets are reconstituted, and decrypted into a readable form.

This differs from credit card and consumer ordering transactions in the volume of data between the two parties. Volume of transactions is greater and the two parties are well known to each other. This means that complex and proprietary encryption and authentication techniques can be used since there is no pretense to offer universal connectivity through this channel.

### 2.3 Digital certification

The importance of this area will continue to grow, as companies seek trusted third parties to hold digital certificates that can be used to electronically prove the identities of message senders and receivers. In addition, it can be proved the integrity of documents and even the validity of digital media, such as sound recordings, photographs and any other field of use.

While the cryptographic basis of these mechanisms is impressive, they leave open several possible areas of exploitation in terms of sharp practice, fraud, extortion and other. It is not fanciful to imagine the value of digital certificates reaching a point where the temptation to betray trust, which rests upon less-than-perfect humans, will be considerable.

## 3. GENERAL OBSTACLES

Apart from the specific problems described above, there are general obstacles to Internet commerce, presented in the following sections.

### 3.1 The frontier problem

This is a new field of knowledge that can be compared with other areas of experience, such as:

- conventional credit and debit card payment and guarantee schemes,
- Electronic Document Interchange or EDI systems,
- traditional data protection methods,
- everyday infosecurity threat management.

In addition, several significant factors make commercial transactions on the Internet completely new base of knowledge. These include:

- the global factor, the need to conduct transactions across international borders, encompassing a wide range of attitudes to commerce and encryption,
- the scale factor, the realization that the Internet is a bigger network than anything else we have encountered, by quantum factors,

- the big brain factor, the unprecedented amount of brain powers that the Internet can focus on any proposed solution. Virtually eliminating the prospect of proprietary solutions, and ensuring that any solution will have to evolve over time,
- the inherent insecurity of the Internet, which was not designed with secure transactions in mind.

In the face of massive enthusiasm for this new technology the security professional must stress that *all security is relative* and advises that any practical answer to these problems have to be a compromise between vulnerability and risk. The assessment of each threat must be weighed against what is at stake, the exposure faced by proceeding with the knowledge that some attacks are possible. This takes system managers into the area of due diligence and liability. Current technologies for encrypting Web transactions do not necessarily protect customer or company data that sits on the Web server, which is often relatively easy to attack.

## 3.2 The market problem

The limitations of current Internet transaction technology are frustrating because we know that powerful encryption that can insure the confidentiality, integrity, authenticity, and non-repudiation of data exists. That includes private key encryption (DES, IDEA, Blowfish, RC4, RC5), plus public key encryption (RSA, SEEK, PGP). However, deployment of this technology is hampered by market forces, which apply immense pressure on companies to release products and create continually shifting alliances between groups of companies hoping to carve up the market.

Technically speaking, there is a big difference between an algorithm and its implementation. To quote leading cryptographer Schneier: "The technology is not weak in and of itself, it is just badly implemented." [2].

Another market-related problem has been the lack of broad standards for secure transactions due to the posturing of competing commercial entities. Two technologies, SSL and SHTTP, were headed for broad acceptance over a year ago, until Visa, MasterCard and Microsoft entered the fray (Microsoft pushing PCT or Private Communication Technology). Historically speaking, the Internet was built upon public domain code, free software, and mutual cooperation in an academic and research environment. About 66% of all Web sites use free server software, more than one in eight Web-servers use a free 32-bit multitasking operating system, running on non-proprietary hardware, 386/486/586 clones [3].

Within this open, Unix-based culture, security evolved dialectically, between programmers who openly devised, discussed, and addressed threats and vulnerabilities. Standards tended to emerge through cooperation and consensus. Proposed security measures or operating system enhancements were subject to public scrutiny. Including those in production systems, software flaws were widely broadcast and openly discussed. Today the Internet lies between the land of the mainframe and the realm of the desktop. Both of which have strongly proprietary cultures, with standards tending to emerge through the conflict of the market place, rather than of consensus, with business practices sometimes so aggressive that they invite the scrutiny of governments.

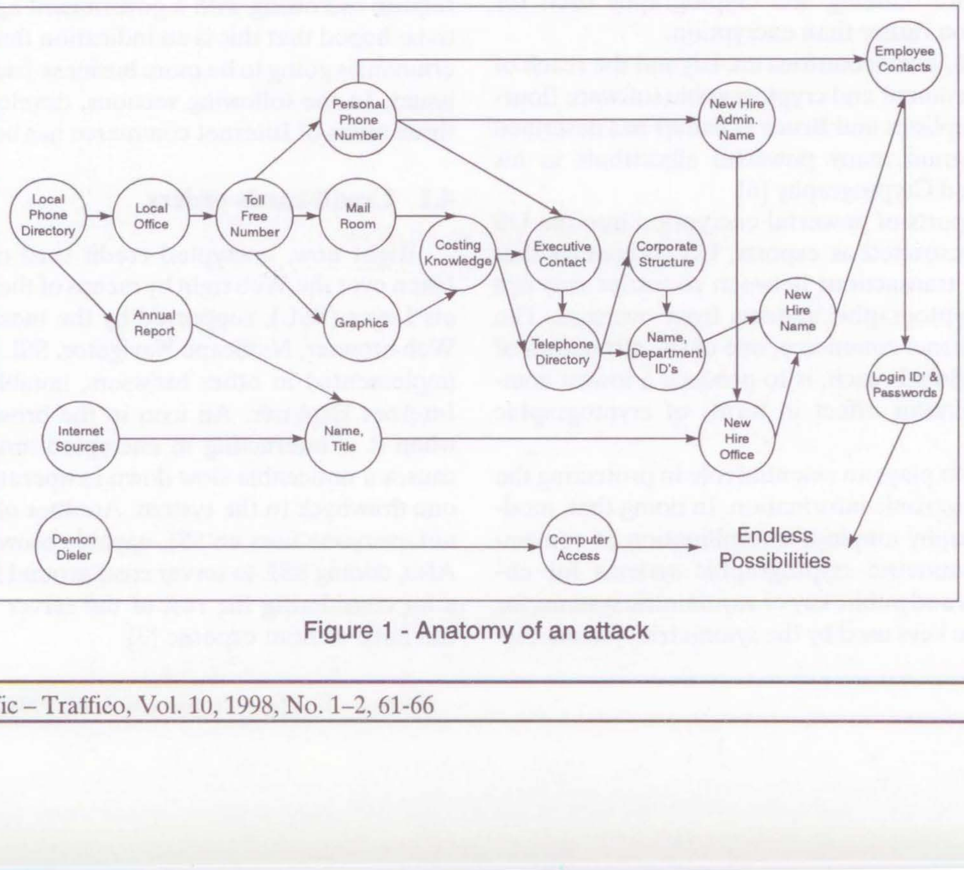

Figure 1 - Anatomy of an attack

In the desktop realm, where the largest number of users now operates, security has largely been ignored. Desktop operating systems are notoriously lacking in security features and most desktop machines are inherently insecure. While the network operating systems, with which PCs are connected, have the ability to implement some sophisticated security measures, the network cannot retrofit security onto the desktop.

These three cultures, UNIX, Mainframe and Desktop, are converging on the Internet at a time when security of transactions and data is higher than ever before in the consciousness of users. In other words, users are now demanding greater security than ever before, in more places than ever before. History suggests that open, non-proprietary standards are the key to future growth of the Internet. Tending to confirm this is the dismal track record of the largest player in the proprietary, PC-based world [4].

Few years earlier it was stated that only open security architecture, subject to intense testing and scrutiny, free from licensing fees and other personal stakes, could serve as the basis for Internet security standards. Once safe Internet transaction mechanisms are in place.

### 3.3 The government problem

Through the International Traffic in Arms Regulations (ITAR), the US government exercises control over the export of "strong" cryptography. Violation of ITAR still carries a maximum penalty of $1 million and 10 years in prison for criminal violation, or $500,000 and a 3-year export ban for civil violation [5].

While refusing to define "strong", the US government regularly denies export licenses to products, such as database software, that use encryption. Some exceptions are banking and cryptography used for authentication rather than encryption.

Of course, some countries are beyond the reach of the US government and cryptographic software flourishes in such places and Bruce Schneier has described how to program many powerful algorithms in his book, Applied Cryptography [6].

Since imports of powerful encryption into the US are not as restricted as exports, US companies that need secure transactions between countries may opt to obtain cryptographic systems from overseas. The effect on Internet commerce, one of the attractions of which is its global reach, is to produce a lowest common denominator effect in terms of cryptographic strength.

Encryption plays an essential role in protecting the privacy of electronic information. In doing that, modern cryptography employs a combination of conventional or symmetric cryptographic systems for encrypting data and public key or asymmetric systems for managing the keys used by the symmetric systems. Assessing the strength required of the symmetric cryptographic systems is therefore an essential step in employing cryptography for computer and communication security.

Technology readily available today makes brute-force attacks against cryptographic systems considered adequate for the past several years, both fast and cheap. General-purpose computers can be used, but a much more efficient approach is to employ commercially available Field Programmable Gate Array (FPGA) technology. For attackers prepared to make a higher initial investment, custom-made, special-purpose chips make such calculations much faster and significantly lower the amortized cost per solution.

Consequently, cryptosystems with 40-bit keys offer virtually no protection against brute-force attacks. Even the US Data Encryption Standard with 56-bit keys is increasingly inadequate.

Fortunately, the cost of very strong encryption is as greater as than that of weak encryption. Therefore, to provide adequate protection against the most serious threats (well-funded commercial enterprises or government intelligence agencies) keys used to protect data today should be at least 75 bits long. To protect information adequately for the next 20 years, in the face of expected advances in computing power, keys in newly deployed systems should be at least 90 bits long [7].

## 4. PRESENT CONDITION

In terms of government restrictions on cryptography, there have been recently seen one company, Trusted Information Systems - the firewall vendor, obtained an export license for encryption that does not require escrowing with a government agency [8]. It is to be hoped that this is an indication that the US government is going to be more business-friendly on these issues. In the following sections, development in the three areas of Internet commerce has been reviewed.

### 4.1 Credit cards orders

Right now, encrypted credit card orders can be taken over the Web right by means of the Secure Sockets Layer (SSL), supported by the most widely used Web browser, NetScape Navigator. SSL has also been implemented in other browsers, notably Microsoft's Internet Explorer. An icon in the browser indicates when it is interacting in encrypted mode. This also causes a noticeable slow down in operations, which is one drawback to the system. Another obstacle is that not everyone uses an SSL-capable browser or server. Also, adding SSL to server costs around $500, which is a lot considering the rest of the server software one can have without expense [3].

However, the most serious shadows over SSL have been cast by technical problems with the NetScape's implementation of security mechanisms. While these are based on strong public key encryption technology, plus the RC4 private key stream cipher from RSA, it would appear that at times, the enormous pressure to bring products to the market has triumphed over quality control. The only other explanation for some of the holes found in NetScape (such as the weak seeding of the random number generator) is that the software engineers themselves did not fully understand what they were doing. All these explanations are disconcerting for companies taking orders via the Web and consumers already hesitant to transmit their credit card information over the Internet.

Recently, encouraging moves have been taken to consolidate, coordinate and publish the standards. Microsoft and NetScape agreed to place their respective encryption specifications in the public domain and combine SSL 3.0 with PCT 2.0 into STLP (Secure Transport Layer Protocol) which also includes the European Secure Shell Remote Login. At the same time the WWW and CommerceNet consortiums agreed on JEPI (Joint Electronic Payments Initiative) to cover the specifics of credit card processing.

### 4.2 Virtual private networks

There has been serious doubt that the Internet is stable and reliable enough for companies to bet on this technology. This could turn the Internet into a short-lived, proof-of-concept entity, side-lined by purely commercial, aggressively marketed systems that capitalize upon a proven demand for secure, high-bandwidth, broad-access, computer-enabled communications. On the other hand, the constant pressure on the bottom line may lead the companies that now rely on VANs for EDI to promote the Internet as a cheap alternative, forcing improvements in security and reliability.

### 4.3 Digital certificates

There has been considerable progress on SMIME - Secure Multipurpose Internet Mail Extensions. This will soon be added to the products to give the ability to sign and authenticate anything send via email. At the same time, PGP is expanding its scope by enabling the use of trusted third parties for key holding, a more commercially attractive solution than the original web-of-trust approach.

At the same time, malicious event suggests that is difficult to escape the attention of electronic vandals in any aspect of Internet operation. There will be attacks on certificate holders and one have to be prepared for them accordingly.

## 5. THE FUTURE OF INTERNET COMMERCE SECURITY

While the eventual emergence of security standards for Internet transactions is expected, it will not automatically result in secure Internet transactions. Even if governments relent and allow strong encryption, even if marketing departments listen to engineering and permit masterful implementations, there is a wealth of security issues that will continue to require attention (Figure 1):

- internal security (in all surveys to date great deal of all information security infractions are made by insiders and the figure is comparable or higher for credit card and commercial fraud) [9],
- continued hacking (systems will need to evolve as hacking eats away at current technology - the process is iterative and never-ending),
- social engineering (without proper security awareness training, organizations will continue to be susceptible to costly social engineering attacks). Social engineering is the term computer user's associates with the process of using social interactions to obtain information about a victim's computer system.
- malicious code (this will continue to impose overhead on all open network systems and is likely to prosper in enhanced functionality environments),
- reliability and performance (problems with backbones and DNS servers are common at the moment and most current dial-up connections are notoriously unreliable and slow, which will probably not improve until there is widespread use of ISDN),
- skills shortages (there are not enough people who know enough about how this technology works, a problem only made worse by requirements of the global Internet),
- denial of service attacks (using brute force with malice or extortion as the motive, hardware and software independent and possibly encouraged by improvements in confidentiality and integrity mechanisms).

## 6. CONCLUSION

In today's world, there are varieties of barriers to the wide spread acceptance of electronic commerce. Many of the greatest advantages of banking and shopping in electronic space hold potential pitfalls that need to be addressed.

First, recent growth in Internet usage has prompted worldwide attention to a glaring problem — privacy. There have been no real safeguards to ensure that the messages have not been intercepted, read, or even altered by unknown interloper since no one person really runs or controls the Internet.

Second, in the emerging realm of cyberspace, the potential for fraud and deception is far greater. The ability to tap into information around the clock, from just about anywhere in the world is perceived by many as a benefit of the Internet. However, it does pose some practical drawbacks.

Therefore, it is necessary to ensure proper education for the following generations as well as this one, in exigency of information security, privacy and confidence.

| | |
|---|---|
| DES | Data Encryption Standard |
| DNS | Domain Name System (or Service) |
| EDI | Electronic Data Interchange |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| ITAR | International Traffic in Arms Regulations |
| JEPI | Joint Electronic Payments Initiative |
| NCSA | National Computer Security Association |
| OLE | Object Linking and Embedding |
| PCT | Private Communication Technology |
| PGP | Pretty Good Privacy |
| RSA | Rivest Shamir Adleman |
| SHTTP | Secure HyperText Transfer Protocol |
| SMIME | Secure Multipurpose Internet Mail Extensions |
| SSL | Secure Sockets Layer |
| STLP | Secure Transport Layer Protocol |
| TCP/IP | Transport Control Protocol/Internet Protocol |
| VAN | Value Added Networks |
| VPN | Virtual Private Network |

## *SAŽETAK*

### *PROBLEM SIGURNOSTI PROMETA INFORMACIJA INTERNETOM*

*Promet informacija Internetom postaje sve važniji i sve veći, a potreba za njihovom sigurnošću eksponencijalno raste s važnošću i kvalitetom informacija. Problem sigurnosti prometa informacija posebno pogađa tvrtke koje svoj prosperitet vide u prisustvu na Internetu. Ovo se posebno odnosi na tri interesantna područja poslovanja: transakcije s kreditnim karticama, virtualne privatne mreže i digitalnu provjeru autentičnosti. Kako bi se povećala sigurnost protoka informacija potrebno je na odgovarajući način riješiti tri glavna problema: problem državnih granica (transakcije preko Interneta ne ovise o međudržavnim granicama), problem otvorenosti tržišta (postoje snažni kriptografski algoritmi, međutim tvrtke ih ne primjenjuju na adekvatne načine, već konkuriraju na tržištu s nekvalitetnim, ali jeftinim proizvodima) problem vlade (američka vlada ne dozvoljava izvoz tehnologija za kriptiranje, jer ih svrstava u teško naoružanje). Iako se očekuju određena poboljšanja sigurnosnih standarda u transakcijama Internetom to neće automatski rezultirati potpunom sigurnošću pri razmjeni informacija. U budućnosti će posebno trebati obratiti pažnju na: internu mrežnu sigurnost, obranu od nedozvoljenih upada u osjetljive informacijske sustave (kako izvana tako i iznutra), socijalni inženjering, greške u programiranju, pouzdanost i performanse te nedostatak obučenih ljudi, sposobnih za rad s novim tehnologijama.*

## LITERATURE:

[1] NCSA Firewall Policy Guide, www.ncsa.com.

[2] Infosecurity News, Jan/Feb 1996, v7 n1, p.24.

[3] *Network Wizards*, Internet Domain Survey, July 1995, http://www.nw.com/.

[4] **Steve Higgins**, PC Week, Feb 8, 1993, v10 n5, p1.

[5] For extensive libraries on ITAR see: http://www.cygnus.com/~gnu/export.html, http://www.eff.org/crypto plus http://epic.org, ftp://ftp.cygnus.com/pub/export/itar.in.full.

[6] **Bruce Schneier**, *Applied Cryptography*, 2nd edition, John Wiley & Sons, 1995.

[7] **Matt Blaze, Whitfield, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, Michael Wiener**, *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996, ftp://ftp.research.att.com/dist/mab/keylength.ps.

[8] NCSA NEWS, March, 1996.

[9] http://www.trouble.org/survey