

# Security Issues in Internet Commerce

ICSA White Paper on Internet Commerce

Version 2.0

Stephen Cobb, Director of Special Projects  
National Computer Security Association

This White Paper, which summarizes an ICSA report on Internet commerce that was prepared at the beginning of 1996, highlights key developments which have occurred since then. This paper can be downloaded from our Web site at [www.icsa.net](http://www.icsa.net) (note that ICSA is a registered trademark of National Computer Security Association, Carlisle, PA)

---

- [Introduction](#)
- [Problems](#)
- [Credit Card Transactions](#)
- [Virtual Private Networks](#)
- [Digital Certification](#)
- [General Obstacles](#)
- [The Frontier Problem](#)
- [The Market Problem](#)
- [The Government Problem](#)
- [Current State of Play](#)
- [Credit Cards Orders](#)
- [Virtual Private Networks](#)
- [Digital Certificates](#)
- [The Future of Internet Commerce Security](#)

## Introduction

Information security or infosec is about protecting three things: the confidentiality, integrity, and availability of data. Securing Internet commerce is probably the biggest challenge that infosec professionals have yet faced. Three years ago, Internet commerce did not exist. Today it is attracting enormous financial interest. 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. But what is Internet commerce?

For many companies, Internet commerce means taking credit card orders from customers shopping electronic catalogs on the World Wide Web. For others Internet commerce means dealing electronically with clients and suppliers, as an alternative to private, leased-line electronic document interchange (EDI over Value Added Networks or VANs). 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 companies large and small. As of January, 1996, half of all businesses with more than 1,000 employees had at least one Web site, according to a Yankee Group survey (which also found that nearly two thirds of all companies with web sites had less than 100 employees). The Internet is attractive to smaller companies because it enables them to reach a wide audience/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 (over \$500,000 per company in the 1,000 employee plus category).

## Problems

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

### 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. 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 (non-fabrication),
- \* the sender cannot deny he or she sent it (non-repudiation)

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

If you use the "trace route" command from a Unix workstation that is communicating across the Internet you can see how many different systems the data passes through on the way from client to server. At the beginning and end of the list you will probably see "local providers" or ISPs

(Internet Service Providers). Most of these are considered "easy targets" by hackers, particularly if the ISP has servers on a college campus. In between you will probably see several machines operated by big name communications providers, such as Sprint or MCI. These may be more secure, but illegal penetration of even these systems poses "no problem" to some hackers.

Typically, 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 to 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 which contains the sensitive data. However, encryption incurs performance overhead and requires coordination between legitimate parties to the communication. In commercial terms, such coordination requires widespread standards for secured transactions, which have been slow to emerge.

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 for hackers, largely due to the immaturity of the technology (for details download and read Lincoln Stein's excellent World Wide Web Security FAQ from [www.icsa.net](http://www.icsa.net) [1]). The standard security advice for Web servers is to treat the machine as a sacrificial lamb, i.e. 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 your systems from your 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 [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 electronic data interchange. This differs from credit card and consumer ordering transactions in that the volume of data between the two parties 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.

Despite the potential for greater security, the VPN is still a worrying development from a security perspective. For a start there is the attention that this "increased security" will attract from hackers and cypherpunks [3], possibly leading to embarrassing or even costly cracking of codes. However, even if the encryption techniques employed by the digital tunneling systems currently on the market or under development prove to be very powerful, thus insuring confidentiality and availability of data, this still leaves the third aspect of security, availability.

For the foreseeable future there is huge potential for denial of service attacks on VPNs. There are currently hundreds of retail operations that depend upon just-in-time inventory replacement. The data that triggers the delivery from the manufacturer travels electronically from the store, currently over private lines. If public lines, i.e. the Internet, are used, the potential for intentional disruption is enormous, not to mention the current lack of protection against accidental service outages.

## Digital Certification

This area will continue to grow in importance as companies seek trusted third parties to hold digital certificates that can be used to electronically prove the identities of message senders and receivers, the integrity of documents (e.g. that an invoice has not been changed) and even the validity of digital media, such as sound recordings, photographs, and so on (e.g. if crime scene photographers switch to digital cameras someone will need to verify that the images presented in court are the same as those originally taken at the scene).

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 so on. 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.

## General Obstacles

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

### The Frontier Problem

This can be summed up by saying "Nobody has ever done this before." In other words, this is a new field of knowledge, a genuine electronic frontier. There are some similarities with other areas of experience, such as:

- \* conventional credit and debit card payment/guarantee schemes,
- \* electronic document interchange or EDI systems,
- \* traditional data protection methods,
- \* and everyday infosecurity threat management.

But there are also several significant factors which make commercial transactions on the Internet a "whole new ball game." 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 (and this at a time when many companies are only just realizing that their internal networks have grown incomprehensibly complex),
- \* the big brain factor, the unprecedented amount of brain power 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,
- \* and finally, perhaps most importantly, the inherent insecurity of the Internet, which was not designed with secure transactions in mind, and which has, for many years, been the playground

of hackers.

In the face of massive enthusiasm for this new technology the security professional must stress that "all security is relative" and advise that any practical answer to these problems has to be a compromise between vulnerability and risk (e.g. there are some vulnerabilities which only a handful of people are currently skilled enough to exploit, which implies that the likelihood of the vulnerability materializing as an actual threat is relatively minor). 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. If someone steals credit card information from your site, you had better be able to document your defenses and the basis for deciding that they were adequate. Current technologies for encrypting Web transactions don't necessarily protect customer or company data that sits on the Web server, which is often relatively easy to attack.

Note that liability extends beyond traditional areas. What if your Internet servers are used as a jumping off point for a hacker attack on another company? What if your corporate image is defaced by an attack on your Web content? What if your Web presence creates unexpected responsibilities (as, for example, in the case of Volvo, which found it had a legal obligation to answer all email complaints).

## **The Market Problem**

The limitations of current Internet transaction technology are frustrating because we know that powerful encryption exists with which to insure the confidentiality, integrity, authenticity, and non-repudiation of data. These include private key encryption (e.g. Triple DES, IDEA, Blowfish, RC4, and RC5), plus public key encryption (e.g. RSA, SEEK, PGP, and ECC). 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." [4] Software engineers work for companies that have marketing departments with bottom lines. We will always need to be concerned about quality standards when encryption systems are developed under these circumstances. We have already seen holes in schemes, such as Secure Sockets Layer (SSL), arising not from weaknesses in the underlying encryption technology, but from shortcomings in the implementation.

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 co-operation in an academic/research environment [5].

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 co-operation and consensus. Proposed security measures or operating system enhancements were subject to public scrutiny. Software flaws, including those in production systems, 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 consensus, with business practices sometimes so aggressive that they invite the scrutiny of governments (first IBM, then Microsoft).

In the desktop realm, where the largest number of users now operate, 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 and in several recent cases we have seen the desktop blow new holes in the network [6].

So, 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 [7].

Last year we stated that only an open security architecture, subject to intense testing and scrutiny, free from licensing fees and other vested interests, could serve as the basis for Internet security standards (while noting that there will be plenty of opportunity for competing proprietary implementations and profit-making programs, once safe Internet transaction mechanisms are in place). We are happy to report (see *Current State of Play*) that recently there have been positive moves in this direction.

## **The Government Problem**

Through the International Traffic in Arms Regulations (ITAR), the U.S. government exercises control over the export of "strong" cryptography [8]. While refusing to define "strong" the 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). Among the effects is a large negative financial impact on U.S. software companies who cannot export the same programs that they sell domestically. As William Hugh Murray observes "Since cryptography is heavily used across borders, American vendors of cryptography or software that uses it, operate at a competitive disadvantage because of these controls" [9].

Of course, some countries are beyond the reach of the U.S. government and cryptographic software flourishes in such places. You can buy full 128-bit stream ciphers and 56-bit DES software on the streets of Moscow. You can download Triple-DES encryption programs from sites on the Internet. Several Swiss companies are happy to supply products based on the very powerful, and widely documented, 128-bit IDEA algorithm. Bruce Schneier has described how to program many powerful algorithms in his book, *Applied Cryptography* [10].

Since imports of powerful encryption into the U.S. are not as restricted as exports, U.S. companies that need secure transactions between countries may opt to obtain cryptographic systems from overseas so security professionals in the U.S. thus face a dilemma, either recommend foreign suppliers, because that is best for the client, or risk liability and due diligence claims by recommending "buy American." 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 [11]. This undermines user confidence, although the rate at which current codes are being rendered obsolete by improvements in affordable, computer-based cracking techniques, is hopefully slower than the rate at which Washington is changing its tune on these issues.

## Current State of Play

In terms of government restrictions on cryptography, we have recently seen one company, Trusted Information Systems, the firewall vendor, obtain an export license for encryption which does not require escrowing with a government agency [12]. Hopefully, this is an indication that the government is going to be more business-friendly on these issues. In the following sections I review developments in the three areas of Internet commerce.

### 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, when interacting with NetScape Commerce Server, the secure version of the company's web server software (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 drawback is that not everyone uses an SSL-capable browser or server. Also, adding SSL to a server costs around \$500, which is a lot when the rest of the server software can be had for zero cost [5].

However, the most serious shadows over SSL have been cast by technical problems with the NetScape's implementation of security mechanisms [13]. While these are based on strong public key encryption technology, plus the RC4 private key stream cipher, from RSA (now owned by Security Dynamics), it would appear that, at times, the enormous pressure to bring products to 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. Either explanation is disconcerting for companies taking orders via the Web and consumers already hesitant to transmit their credit card information over the Internet.

Recently, there have been encouraging moves to consolidate, coordinate and publish standards. In April 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 spec). We were particularly pleased that there will be no charge for the reference and object source code versions. At the same time the W3 and CommerceNet consortiums agreed on JEPI (Joint Electronic Payments

Initiative) to cover the specifics of credit card processing.

## **Virtual Private Networks**

We doubt that the Internet is stable and reliable enough yet for companies to bet on this technology. We would hate to see people try it, get disgusted, then desert in droves. 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 companies which now rely on VANs for EDI to promote the Internet as a cheap alternative, forcing improvements in security and reliability (according to SKL Technology, some 64,000 companies were using EDI in 1995 but the number is expected to increase to half a million by the year 2000, with much of that growth coming from Asia and the Pacific Rim).

## **Digital Certificates**

There has been considerable progress on SMIME, Secure Multipurpose Internet Mail Extensions. This will soon be added to products to give you the ability to sign and authenticate anything you 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 events like the recent spoofing of news announcements suggests that we cannot assume any aspect of Internet operation will escape the attention of electronic vandals. There will be attacks on certificate holders and we must prepare for them accordingly.

## **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 are a wealth of security issues that will continue to require attention:

- \* internal security (in all surveys to date, at least 75% of all information security infractions are by insiders and the figure is comparable or higher for credit card and commercial fraud),
- \* 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),
- \* malicious code (this will continue to impose overhead on all open network systems and is likely to prosper in enhanced functionality environments such as Java and OLE, the Microsoft Internet Safe Code Initiative notwithstanding),
- \* reliability and performance (problems with backbones and DNS servers are common at the

moment and most current dial-up PPP 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 the 24x7 up-time requirements of the global Internet),

\* and 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).

In other words, the experience and wisdom of the seasoned InfoSec professional will continue to be of great value, and will have to be heeded if systems are to retain user/consumer confidence. Being able to think like a hacker, while acting like a guardian of the public trust, will always be a requirement for assuring the security of computer-based information. And the need to promote ethical behavior in all aspects of business and personal life will remain a priority if we are not to cripple powerful new technology with ancient human weaknesses.

### **Notes:**

[1] Not only does this FAQ contains some detailed code fixes and suggestions, it sheds a lot of light on the security issues that professionals coming to the Web from other fields sometimes find hard to appreciate. For example, why do so many Web sites use free server software? Because you get the source code, typically not available with commercial packages, and traditional Unix folks seldom trust any program the source code of which is not published.

There is a link to the WWW Security FAQ at [www.icsa.net](http://www.icsa.net). Here are the main Web risks that Stein identifies:

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/or damage the system. This includes "denial of service" attacks, in which the attackers pummel the machine with so many requests that it is rendered effectively useless.

And here are three truths to live by: 1. Buggy software opens security holes 2. Complex programs always contain bugs 3. Web servers are complex programs.

[2] See the ICSA Firewall Policy Guide, which can be downloaded from [www.icsa.net](http://www.icsa.net).

[3] For more about Cypherpunks, see Stephen Levy in *Wired*, April, 1996 and Stephen Cobb in *Internetwork*, May, 1996: "The first thing to know about cypherpunks is that they like to crack codes....although they have no formal organization and most are not in it for the money....Cypherpunks are a whole new dimension in code-breaking. They are part of an Internet

phenomenon that I call the "big brain factor" -- the unprecedented amount of human brain power that the Internet can focus on any given subject." Cobb describes cypherpunks act as "a cutting edge quality control mechanism...for pioneering Internet merchants."

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

[5] About 66% of all Web sites use free server software, more than one in eight Web-servers use a free 32-bit multi-tasking operating system, running on non-proprietary hardware, 386/486/586 clones. Network Wizards, *Internet Domain Survey*, July 1995, <http://www.nw.com/>.

[6] The Microsoft Windows File Sharing bug and the Microsoft Windows Password List Security Issue have been extensively reported and "fixes" are posted on the Microsoft Web site: [www.microsoft.com](http://www.microsoft.com).

[7] See "Microsoft InfoSec Stall of Shame: the MISS Top Ten" in *Security Insider Report*, Jan 1995, v5 n1.

[8] "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." Steve Higgins, *PC Week*, Feb 8, 1993, v10 n5, p1. Note that ITAR was passed in 1943, during time of war and without public debate. Also note that the prison term is served in a very uncomfortable federal facility.

[9] William Hugh Murray, *Communications of the ACM*, July, 1992, v35 n7, p.13.

[10] Bruce Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, 1995. While the book is freely exportable, a disk containing the source code listings from the book is not, which suggests that the National Security Agency believes foreigners can read but not type. See: <http://www.qualcomm.com/people/pkarn/export/index.html>.

For extensive libraries on ITAR see: <http://www.cygnum.com/~gnu/export.html>

and <http://www.eff.org/crypto> plus <http://epic.org>.

[11] In 1995, French researcher and cypherpunk, Damien Doligez, used 120 workstations and two super computers to crack a single session encrypted with the 40 bit export version of RC4 in 8 days (see Ryan O. Tabibian, *PC Magazine*, Oct 24, 1995, v14, n18, p.29 and Stephan Somogyi, *Digital Media*, Sept 11, 1995, v5 n4, p.29). Since then several others have accomplished the task with a variety of hardware. In fact, this weakness was predicted by NetScape, which faces and is fighting, the same government restrictions on strong encryption encountered by all other American software companies. Bear in mind that the difficulty of cracking this particular algorithm increases exponentially with each additional bit of key length. So a 41 bit key would theoretically take twice as long to crack as a 40 bit key, and so on. The U.S. government discourages the export of this sort of encryption software if the key length is greater than 40. By comparison, retail domestic versions of the NetScape browser are free to use a 128 bit key (the versions you download for free are limited to 40 bits).

[12] See *ICSA NEWS*, March, 1996.

[13] Note that these "holes" are different from the "weakness" in RSA's RC4 stream cipher

algorithm, employed by NetScape, demonstrated by Damien Doligez (see [11] above).