Journal of Universal Computer Science, vol. 7, no. 5 (2001), 447-455
submitted: 14/4/01, accepted: 1/5/01, appeared: 28/5/01 *© Springer Pub. Co.*

Will Internet Ever Be Secure ?

Reinhard Posch
(Graz University of Technology, Austria
reinhard.posch@iaik.at)

Abstract:. The users of the Internet in general have not developed a perception of where what security is crucial and beneficial for their applications. At present the average user is provided very few information independent of what is transported over the service and how this is done.
What is needed for a secure Internet, is that security is answered on a system level or on an application level and that an appropriate level of security is reached and still is accepted by the user? These questions are primarily questions on a technical level but have a great dimension of awareness which has to be kept in mind.
However, the main question is not how to secure the Internet in place but how to develop mechanisms and tools for the Internet that can seamlessly improve an ever changing media which opens up new dimensions of security risks with every new protocol system and application. Security will remain a race where comfort is often seen as a competitor.

Keywords: Internet security
Categories: H.0

1 How secure is the Internet in place?

Internet in the private sector has been used mainly as a toy and as an information retrieval media. Transactions that add a further dimension in usability but mainly in security are becoming relevant for masses only recently.

From the point of view of security we have basically three types of threats:

i. Inherent risks through the use and the associated faults of the Internet and the respective applications. These are general deficiencies that will usually be eliminated as soon as they become known and resources to eliminate them can be allocated. Extensive lists of such vulnerabilities are e.g. maintained by [1] and [2].

ii. Risks that result from a malicious exploratory use of the Internet. Viruses could in many cases be classified as such a type [3]. In many cases there is no intention to really damage systems. In some cases these threats are exploited so as to make people aware even if this might be no appropriate method to do so.

iii. Security risks that are introduced so as to result in some commercial "benefit" for the one that is exploiting this risk. Capturing credit card numbers is among the most prominent examples, still other types such as investment fraud show up in Internet fraud complaint trends [4].

Due to the fact that the transactive use of the Internet has not reached volume until recently the third type is not very frequently seen. However, it has to be assumed that in a world where e-commerce and e-government become a common tool and where people start to be depending on such tools, organised crime will activate this field and perhaps is already preparing such activation.

From the practical point of view viruses are basically the only threat the wide public is aware of and ready to undertake limited actions against. But all measures taken are lagging behind the target rather than introduce effective preventing measures. Loveletter to some extent is the perfect example:

i. Loveletter bases on a very simple idea — all damage could have been avoided by sufficiently aware use.

ii. Loveletter exploits features of a system very widely spread.

iii. Loveletter caused damage even in systems that made all and every effort to be protected. Existing protection tools simply were not alerted.

We have not really learned our lessons. An idea that follows a totally different still quite simple scheme would equally cause damage as the general perception is that installing some anti virus tools will yield adequate protection. Antivirus protection is like having a huge property and building a small piece of fence at those points where someone tried to cross the borderline.

Virus protection is just one aspect. We cannot blame manufacturers not to improve security as long as we do not show them that this has an effect on their success on the market. Wide spread systems like OUTLOOK 2000 including previous versions are a perfect example. Such products leave the impression of being adequately secure for applications like e-commerce. Still, having a closer look to such products somewhat show the contrary. Like pointed at in the following figure messages that give the impression of a high security level by digital signature can be spoofed so as to show a security icon on the preview pane. For most users this will be a valid method to recognize security levels.

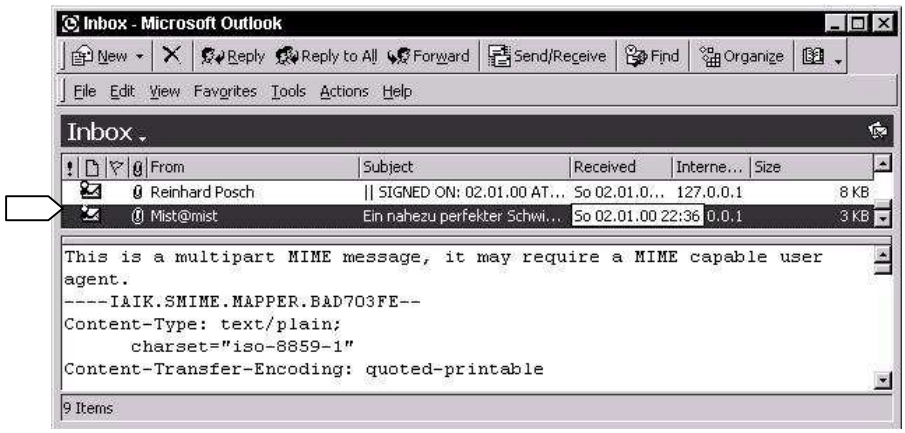

Figure 1: MS-Outlook hides security holes

It is obviously more important to introduce glossy features than to close such security holes.

Even the professional world gets steadily puzzled. PGP as an open source product has been assumed as a most transparent and thus secure solution. With the changing situation that NAI is exploiting this in a much more commercial way and with the integration into the Windows platform, open source is no longer true in the original sense. Moreover is the fact that Phil Zimmermann—the creator of PGP—has turned towards hushmail at least irritating.

The general flexibility of the Internet adds various degrees of freedom which result in various security concerns. It is not in the mindset of the average user that email senders are not secured it is also not generally known that proxies introduce a further level of possible manipulation of content.

2 Do we need a more secure Internet?

It has already been mentioned that security is not a major concern of manufacturers that their products are secure. This is not really changing their business cases. On the other hand companies tend to shift responsibility to the consumer.

Such a shift of responsibilities does not come without good reason. There is a substantial increase of security needs. Visa International said in 1999 that “half of all credit-card disputes are about Internet transactions. - That is despite online transactions making up just 2% of Visa's overall business” [5].

The most severe threat however is in the area of industrial and professional espionage. There seems to be the highest “benefit” for the attacker. This field has to be observed with scrutiny, as the units producing the largest amount of intellectual property—the SMEs—do not have awareness and potential of securing themselves against such threat. If this is not addressed by infrastructure, it will not be addressed at all. Such danger is extremely relevant in small countries with an economy largely based on SMEs.

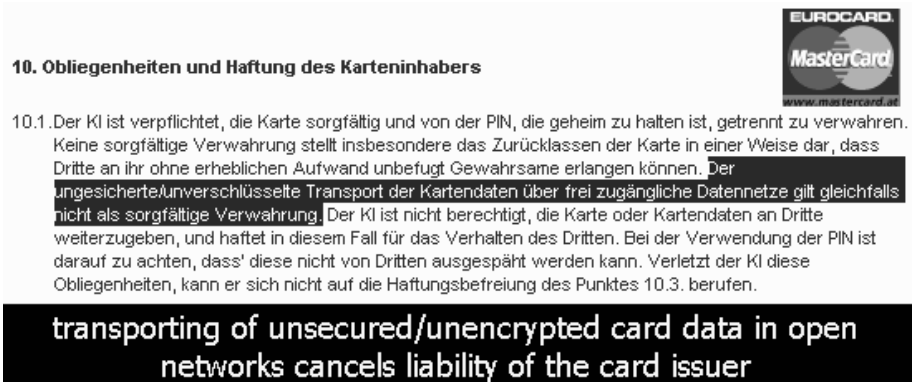

Figure 2: MasterCard shifts the burden of security to the consumer.

Internet has mechanisms that allow acceptable levels of security, such as IPSEC [6] or secure socket layer (SSL) [7] and transport layer security (TLS) [8]. For a series of reasons these mechanisms are quite isolated. The "banned" status of cryptography classified as dual use is just one of these reasons. There is an emerging need not to have isolated exploited mechanisms to be replaced by infrastructures. Infrastructures are needed in both the field of confidentiality and electronic signature and authentication.

3 What are the services secure Internet has to provide?

The present approach to Internet security yields the need of substantial changes. As these practical situations need improved mechanisms. The following enumeration is not deemed to be complete, but shows a variety of fields concerned:

i. Contracts over the Internet

It is frequently blamed that e-commerce as B2C is not growing fast enough. One of the reasons for this is that both customers and businesses have a feeling of insecurity in their background. The practically limited liability is a fact. As 8% of the contracts initiated just do not terminate normally, as a study of the European Union shows, this is not a unjustified feeling. There might be some hope that e-Government which has a higher need of security might improve the overall situation.

ii. Configuration of systems and downloads

The general approach by the vendors and by industry like Microsoft is to generate an overall perception of being reasonably secure. As known from the press recently even the internal security of companies like

Microsoft is doubtful. Certificates as infrastructure for a trusted download basis have been compromised [9]. It therefore has to be assumed that even the configuration of systems is in danger.

iii. Defending industrial espionage

Small and medium enterprises can or will not afford security that does not come with the system. Facing a tough business model these companies cut expenses on security as this is the least visible, still very risky area. This makes it very important that security services including confidentiality are provided. Recent developments in the area of export of cryptographic devices could make this more viable [10].

iv. Watermarking for proof of origin

This area is of prime importance for the entertainment industry. As this is a huge industry sector, it can be expected that there will be many efforts in this area by this industry to protect their assets.

v. Payment for online procedures

Unfortunately payment especially of small amounts is not yet satisfactory. There is not yet a model that allows for the small margins needed to boost online payment.

With larger amounts credit cards are frequently used but as mentioned earlier this is not a way that can continue. Secure electronic transaction (SET) [11] has been developed to secure this sector but in the private area it is not yet deployed.

vi. Confidentiality and data protection

For historical reasons this is a field which is not well developed. First there was and is the problem of crypto export and additionally the law enforcement issues yield de facto obstacles in many countries.

vii. Protecting the content

Malicious content is an aspect that is well recognized in the public. However, so far there is no good tool that does not in turn limit the comfort of use of the Internet and thus is not well accepted. This aspect asks mainly for an adequate education on how to use the Internet in education premises and homes.

When resolving issues as mentioned above it has to be assured that this does not yield a societal digital divide. On a practical basis, this means that security must become much easier to handle and to understand by a large public.

4 What are the tools to be used to yield acceptably secure Internet

Internet is dominated by the use of open standards and protocols. Security likewise has to follow open standards. The assumptions are nonetheless different with security. Whereas it is assumed with the proposal and application of standards that a process will start that sorts out less acceptable ones automatically, as these do not perform, this situation is very different with security: Security usually is invisible to the normal user. Appropriate performance and absence of risks cannot be differentiated. A normal user will not get exposed to risks deliberately to get informed about the readiness of his IT-security measures. Therefore, some intermediate judge is needed and too often this intermediate judge is the vendor which makes the judgment biased and thus less valuable.

Configuration policy: A first tool which is not yet there on the market in a satisfactory manner is the configuration policy for a computer. Usually a workstation or a laptop will be sold in the store with most questionable security environments. The average user will be satisfied when he/she brings the computer to function, but will not consider security implications when installing. Moreover this happens at a point in time where the user has the probably lowest level of experience on the specific machine. A secure configuration tool would have to start with the installation according to a security policy. Such policy can base on questions asked to the user in a way that he/she can understand. Setting system parameters by the user is generally an insecure approach.

Secure Download: For many vendors we observe signed code as a method of having a trusted download. However, this is a single level of trust and we face situations of where we need different levels of trust according to environments and applications. There is usually no choice of the user whom to trust and in practical situations the user does not even know the units he has to trust. In a practical situation this is even more complicated: We have practically no choice and need to use systems and software that is on the market. Moreover even institutions like Microsoft suffer from insufficient security as recent compromise of certificates has shown [9].

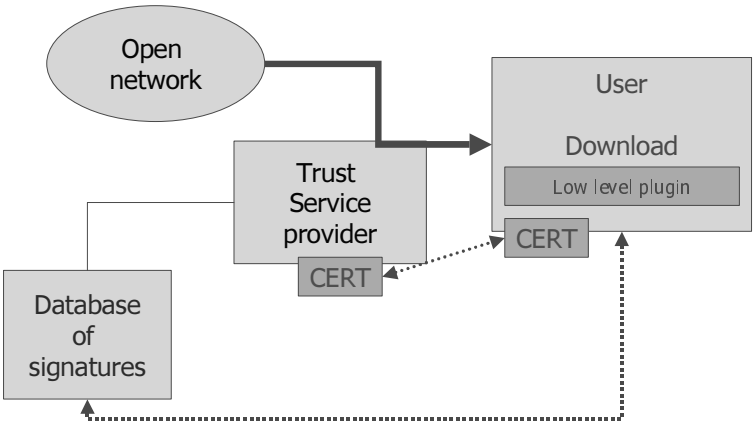

Figure 3: Trusted download using independent signatures

In the real world there is no need that the trusted party is the same institution that provides software. As shown in the previous figure the manufacturer of software need not even to know about the party the user trusts. Very simple additions in conjunction with an independent archive of signatures related to software downloaded from the open network can increase trust and at the same time control system environments that are highly reliable. Basically, an appropriate proxy will manage this task independent of the actual system the user is running.

Watermarking: In several cases proof of origin is needed and the information should not be changed without the intension of the information provider. Digital watermarking goes in this direction. For the proof of origin and the integrity of the information, digital signatures can do the job. It is however fairly impossible to prevent copies in the general case of the Internet. Watermarking with known features which is needed for being able to proof the watermark and resistant enough so that a similarly usable information cannot be produced is rather impossible. This is shown with a simple text. If such text is converted to plain ASCII and then reformatted for the Internet, a watermark will disappear. Watermarking will have a high level of importance with streaming data. Audio and video through the Internet can gain a certain level of security with such enhancement.

Digital signature: This is probably the most important tool that will secure applications through the Internet, in particular as the legal admissibility has been established such as by the European Directive on electronic signatures [12]. Fraud increases with volume as this increases also the potential of anonymity for those acting fraudulently. Digital signature separates the class of users that act with identity from those acting anonymously. Above a certain level of value of the data or the transaction it cannot be justified not to operate in the class of identified use. At present security is often based on confidentiality which serves one purpose but confidentiality will not be sufficient without introducing identities.

Encrypting the content: There are several standards for content encryption over the Internet. IPSEC, PGP, SSL, TLS all these serve for adequate security, if used with keys that are cryptographically strong and generated and handled in a secure manner. Content encryption is well placed in the context of privacy. It is much less used in the field of espionage prevention and small and medium enterprises suffer from this attitude most. There is also the inherent problem that existing browser technologies do not easily show the quality of encryption. In addition there is usually no method to define a policy which leads to the fact that basically all installations are operated with standard settings and thus quite insecure. SMEs that have to build on off the shelf products suffer from such situation most. Internet will need customized system configuration tools to create trusted environments for the various applications.

e-payment: Many approaches have been tried so far but we still lack acceptable standards. This is mainly because of the different goals electronic payment might have. Some of the approaches are too complex and too monopolistic. E-Cash is such an example. Still development of fraud and false claims show that there is a big need. It has to be expected that signature-based mechanisms like SET will enhance security and offer an accepted solution. This does however not solve the problem of micro payments which is an important factor for Internet applications and it does equally not solve the problem of anonymity yet.

Content security: Different aspect are addressed when speaking about Internet security. Content security as the field of prevention of criminal content is frequently discussed as this is easily understood as a problem. In the context discussed so far, this has limited relevance in terms of security. However, this will influence the use of the Internet in a professional manner to quite an extent. As this aspect is totally different, it is not stressed in here.

5 Final remarks

It seems that security is an increasingly important field and that infrastructures provide more and more support for security. Especially for the private sector and for SMEs this is a crucial fact. In this context we will definitely face a more secure Internet.

However, there remain at least two questions in the field open:

(a) Will security become more important than glossy and fancy programs and applications.

(b) Will the increase of security be faster than the increase of risk. Up to now there seems to be limited hope that this will be the case. Perhaps we need a few more loveletters, another series of credit card attacks and lots of cases of industrial espionage before this will happen.

Certainly we will face lots of further threats with the emerging technologies and as we are going miniature we will experience the need to minimize resources and will have to reinvent the wheel security-wise.

For quite a while resources that are needed to secure communications have been an important argument. This is no more the case for PCs and workstations. Comfort and flexibility is still the biggest security threat. With UMTS and other new technologies we are back a few steps again.

Bright ideas and building new applications and unawareness of manufactures and users still seems to dominate the development. It is mainly due to lack of awareness that interest in secure solutions is quite limited.

References

[1] Mitre Corporation, Common Vulnerabilities and Exposures – CVE, online resource http://www.mitre.org, 2001.

[2] Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team Coordination Center, CERT® CC, online resource http://www.cert.org, 2001.

[3] L.M. Bridwell, P. Tippett, ICSA Labs 6th Annual Computer Virus Prevalence Survey, ICSA Labs, 2000.

[4] Internet Fraud Complaint Center, Six-Month Data Trend Report May-November 2000, National White Collar Crime Center and Federal Bureau of Investigation, 2000.

[5] NUA Internet Survey, Visa: Net Transactions Cause Credit Card Disputes, online resource http://www.nua.ie/surveys, article id 905356338, 1999.
[6] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, 1998.
[7] Frier, P. Karlton, and P. Kocher, The SSL 3.0 Protocol, Netscape Communications Corp., 1996.
[8] T. Dierks, C. Allen, The TLS Protocol Version 1.0, RFC 2246, 1999.
[9] National Infrastructure Protection Center, Warning Not To Accept VeriSign Microsoft Digital Certificates dated January 29-30 2001, NIPC advisory 01-006, 2001.
[10] Bureau of Export Administrations, Revisions to Encryption Items, US Department of Commerce, Federal Register Volume 65, Number 203, Page 62600-62610. Online resource http://www.bxa.doc.gov/Encryption, 2000.
[11] Mastercard, Visa: SET Secure Electronic Transaction Specification, Book 1 – Book 3, Version 1.0, 1997
[12] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, 1999.