

## Improvements in Internet Security Case Study – Deutsche Bank AG

a report by

**Professor Clemens Jochum and Bernhard Esslinger**

*Chief Information Officer, Private Clients & Asset Management –  
Global Technology and Corporate Head, IT Security, Deutsche Bank AG*

Professor Clemens Jochum is the Chief Information Officer (CIO) of Private Clients & Asset Management – Global Technology, at Deutsche Bank AG, a position he assumed in February 2001, prior to which he was CIO of Consumer Banking Applications – Global Technology and Services Division. He was in charge of a worldwide joint venture of the Beilstein Institute and the Thyssen Bornemisza Group from 1994 to 1998 and, afterwards, was appointed to the Gesellschaft für Finanzmarketing (GEFM), a subsidiary of Deutsche Bank AG. Since 1993, he has also been Honorary Professor at the University of Darmstadt. In 1984, he became Head of the Information Technology (IT) department of the Beilstein Institute, where he was appointed member of the board in 1985. After working as the Head of Laboratory of Chemometrics at the University of Washington/Seattle from 1980 to 1982, he commenced his professional career, co-founding the software company Softron.

Bernhard Esslinger is Corporate Head of IT Security at Deutsche Bank AG, having previously served as Chief Security Officer of SAP AG until March 1998. Since January 2000, he has been responsible for global co-ordination and deployment of Deutsche Bank AG's public key infrastructure (PKI). Under his direction, an Identrus infrastructure for the Bank was created and he was appointed Bank Program Manager at Identrus for Deutsche Bank AG. Mr Esslinger started the Bridge-CA initiative and is a member of the Board of Bridge-CA. He provides consulting for all e-commerce projects of Deutsche Bank AG and is actively involved in public relations concerning Deutsche Bank AG PKI activities.

Security in data networks has been a hot topic for several years. Though security incidents such as the 'I Love You' virus are still not the exception, developments in recent years have produced considerable results. It is becoming increasingly clear that security cannot be achieved simply by installing a firewall or introducing encryption. Holistic concepts, based on risk management, are needed and user acceptance is essential.

Many computer users have unpleasant memories of May 2000, when the now legendary 'I Love You' virus inflicted damage that ran into billions of dollars worldwide. The more recent 'Naked Wife' e-mail 'worm' looks feeble by comparison. However, there is no denying that security in computer networks is more topical than ever. This is proven, not only by many hacked websites, (including that of the Central Intelligence Agency (CIA)), but also by more serious breaks into corporate networks. In October 2000, for example, people were shocked by the news that hackers had penetrated the Microsoft® Corporation's network totally unnoticed.

All of these events look relatively harmless compared with the activities of the National Security Agency (NSA), a US secret service. An EU Commission estimate indicates that this organisation employs no fewer than 68,000 people simply to eavesdrop on and evaluate the global exchange of information. The NSA listening system, Echolon, has meanwhile come to be the epitome of secret surveillance.

Given such events and threats, it is no surprise that information security has been riding high for several years. A study by US analysts puts annual sales in this area in 2001 at US\$17.4 billion, with annual growth of 61%.

The emergence of the 'I Love You' virus, etc., has in some cases led to the belief that the battle against the unsafe Internet was lost long ago. "Not at all," says Hermann-Josef Lamberti, member of the Board of Managing Directors of Deutsche Bank AG. "Looking back over the last five years, I can only say

that enormous progress has been made in data security." Lamberti can remember clearly that, at the beginning of the boom midway through the 1990s, the Internet was a wide-open door. As the Internet pioneers had left aside the subject of encryption, unsolicited listeners, such as the NSA, had an easy time. Firewalls to prevent hackers from breaking in were just as rare in those pioneering days as a well-designed authorisation management or chip card-based access control. Under those conditions, online banking and other security-critical activities in the Internet were almost inconceivable.

Half a decade later, the Internet is almost unrecognisable – even for security experts. Firewalls have long since become a bulk product and, today, protect even small corporate networks. Encryption is supported by any of the more sophisticated e-mail applications and by all popular Web browsers. In many security-critical systems, safe chip card solutions have replaced password entry.

Just how great the change has been can be seen, for example, in the use of encryption in the World Wide Web. In 1995, World Wide Web pioneer Netscape had to urge the foundation of a Certification Agency, to be able to equip their own browser with digital certificates. Today, any Netscape user can choose between a dozen certificates supplied by his/her browser.

The pioneers in this phase of development towards a safe Internet were undoubtedly the banks. Deutsche Bank AG, for example, founded its Information Security Department in 1996 and, since then, has regarded this subject as a strategic target. The banks were also the first to provide secure customer access using the Internet. With online banking common to all banks today, insurance companies, public departments, logistics companies and other suppliers meanwhile offer secured Internet portals as well.

In the fields of encryption and digital signatures, there are currently a number of interesting banking innovations, one of which is the international public key infrastructure (PKI), Identrus.<sup>1</sup> Under the

1. <http://www.identrus.com>

framework of Identrus, a global security infrastructure is currently being set up by more than 40 financial institutions that enable trust for business-to-business transactions. The objective is to set up a legal and contractual framework and equip corporate customers with digital certificates to be used for encryption and digital signatures when conducting e-business.

An additional track initiated by Deutsche Bank AG and Deutsche Telekom in Europe is Bridge-CA.<sup>2</sup> Its goal is to connect various, already-existing PKIs in companies and public authorities with one another. In contrast to Identrus, the PKI operators do not necessarily have to be banks. Bridge-CA's focus is on interoperability, investment protection and its high degree of integration of different approaches in high security – both software and hardware-based certificates, as well as certificates, conforming and non-conforming, to electronic signature law. Its pragmatic approach has led to the system's success since its foundation in October 2000. It managed, for example, to enable interoperable secure e-mail between major companies and government authorities.

time to enter the latest security patches. Hacked websites and uninvited guests in corporate networks are due less, in the opinion of security experts, to the genius of hackers than to the negligence of operators.

However, appeals to operators does not mean that the battle has been won. A new mindset is needed with respect to the solution of security problems. Security must not be treated like goods that can be bought and installed. Security is a permanent process to which all components of a system contribute. The weakest link in the chain is always the most important one, which is often the user. The user who sticks a piece of paper containing a password on his/her monitor is still a relatively harmless case compared with that experienced in practice. Tests carried out by security experts show time and again that users readily communicate their passwords over the telephone if they are skillfully asked to do so. It is also common practice to transmit sensitive data unencrypted, even if encryption is available. It is obvious that even the best security system can be thwarted by such irresponsibility. This area in particular is seen as a core

*... security cannot be achieved simply by installing a firewall or introducing encryption. Holistic concepts, based on risk management, are needed and user acceptance is essential.*

The bank has assumed technological and conceptual leadership in PKIs in two ways – not only has it actively established two PKIs early (for software and hardware certificates according to requirements), but has pushed for these corporate PKIs to be inter-operational in international and intercompany structures. The bank is both an active member of Identrus and a co-initiator of the European Bridge-CA.

Since progress in the field of security could not prevent either 'I Love You' or 'Naked Wife', the question remains about how the remaining security gaps can be filled. First of all, we must make people more security-sensitive. Many operators of networked computer systems still try, for cost reasons, to get by without urgently needed security facilities. They were the ones who also suffered most from these threats, while network operators who invested wisely in security were quickly back to business as usual. Investment here does not mean primarily the acquisition of technology and licences, but investment in highly qualified and motivated employees undergoing permanent training, and who have the

focus for the future. If we can get final users to be more aware, then we have taken a big step forward. The 'I Love You' virus is a good example – cautious e-mail recipients did not even open infected mails, and so prevented further damage.

A computer emergency response team within Deutsche Bank AG deals with any computer emergency incidents in a rapid and effective manner, minimising the effects on the bank. This team also alerts the relevant personnel of potential incidents and takes the actions required to prevent them from occurring. All of this demonstrates that Deutsche Bank AG understands that the integrity, availability and confidentiality of its data and information systems are vital to its continued success. The bank assures its customers that its information is secure. A comprehensive security framework consisting of policies, standards, tools and services covers all aspects of information usage in the Bank. This framework provides tight security but is flexible enough to accommodate the pursuit of current and future business objectives. ■

2. <http://www.bridge-ca.org>