Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

Securing Electronic Business Processes

Highlights of the
Information Security Solutions Europe 2008
Conference

Contents

Preface

Dear Readers,

ENISA is proud to be co-organising the Information Security Solutions Europe Conference 2008 (ISSE) together with eema, TeleTrusT and INTECO. the Spanish National Institute of Communication Technologies, in its tenth year..

The aim of the ISSE has always been to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. ISSE is renowned for its rich content perspective, designed to inform ICT professionals, policy makers and industry leaders on latest developments in technology and best practices. Also ENISA is highly committed to these goals. For this reason we are delighted to support the ISSE again this year. In our work we assist and advise the European Commission, Member States, and business community in the field of network and information security., The security of communication networks and information systems is of increasing concern. In order to face today's complex information security challenges it is clear that working together is the key to generating new strategies to address these problems. It has been an inspiring opportunity to facilitate this collaboration at the ISSE 2008, bringing together the wealth of industry knowledge, information and research that we hold in Europe, as well as across the globe.

The success of this event is based on the unparalled composition of, government, academia and other stakeholders, generating ideas and participating in a frank, lively policy and technical debate in an non commercial context. By sharing different perspectives, experiences and solutions around the complex topics of IT security, the independent and varied nature of the programme guarantees interesting results. This year, we are focusing on highly interesting, cutting edge security and related issues, like costs of ownership, risk management and interoperability, which were all selected by worldwide specialists in the field.

Some of the key topics explored at this year's conference have been chosen as the basis for this book, which serves as an invaluable reference point for anyone involved in the IT security industry.

We hope that you will find it a out of the ordinary, fascinating and motivating read.

Andrea Pirotti, Executive Director, ENISA

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the sixth ISSE book – another mark of the event's success – and with about 40 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ronny Bjones**, Microsoft (Belgium)
- **Gunter Bitz**, SAP (Germany)
- **Lucas Cardholm**, Ernst&Young (Sweden)
- **Roger Dean**, eema (United Kingdom)
- **Ronald De Bruin**, ENISA (Greece)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, NXP Semiconductors (Belgium)
- **Jos Dumortier**, KU Leuven (Belgium)
- **Walter Fumy**, Siemens (Germany)
- **Michael Hange**, BSI (Germany)
- **John Hermans**, KPMG (The Netherlands)
- **Marcos Gómez Hidalgo**, INTECO (Spain)
- **Jeremy Hilton**, Cardiff University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Frank Jorissen**, SafeBoot (Belgium)

- **Matt Landrock**, Cryptomathic (Denmark)
- **Jorge Chinea López**, INTECO (Spain)
- **Madeleine McLaggan-van Roon**, Dutch Data Protection Authority (The Netherlands)
- **Tim Mertens**, ENISA (Greece)
- **Norbert Pohlmann**, University of Applied Sciences Gelsenkirchen, Chairman of the Programme Committee (Germany)
- **Bart Preneel**, KU Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Joachim Rieß**, Daimler (Germany)
- **Paolo Rossini**, TELSY, Telecom Italia Group (Italy)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, CoreStreet (United Kingdom)
- **Robert Temple**, BT (United Kingdom)
- **Arie van Bellen**, ECP.NL (The Netherlands)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

eema (www.eema.org):

For 21 years, eema has been Europe's leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

eema's remit is to educate and inform around over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare and exchange views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through events. All of the information generated by eema and its members is available to other members free of charge.

Examples of papers produced recently are:- Towards Understanding Identity, Spam and e-mail Abuse Management, Role based Access Control – A User Guide, Password Synchronisation, Secure messaging within and between User Organisations. eema members, based on a requirement from the rest of the Membership, contributed all of these papers. Some are the result of many months' work, and form part of a larger project on the subject.

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a Member of eema, and any employee of that organisation is then able to participate in eema activities. Examples of organisations taking advantage of eema membership are Unilever, Volvo, Shell, Hoffman la Roche, KPMG, Magyar Telecom Rt, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

TeleTrusT Deutschland e.V. (www.teletrust.de)

TeleTrusT Deutschland e.V. was founded in 1989 as a non profit association promoting the trustworthiness of information and communication technology in open systems environments. Today, TeleTrusT counts more than 80 institutional members. Within the last 19 years TeleTrusT evolved to a well known and highly regarded competence network for applied cryptography and biometrics.

In the various working groups of TeleTrusT ICT-security experts, users and interested parties meet each other in frequent workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements. TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentification and signature (IAS) schemes in the electronic business and its processes.

TeleTrusT facilitates the information and knowledge exchange between vendors, users and authorities. Subsequently, innovative ICT-security solutions can enter the market more quickly and effectively. TeleTrusT aims on standard compliant solutions in an interoperable scheme.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks the co-operation with European organisations and authorities with similar objectives. Thus, the European Security Conference ISSE is being organised in collaboration with eema, ENISA and INTECO this year.

Contact:
Dr. Günther Welsch
Managing Director of TeleTrusT Deutschland e.V.
guenther.welsch@teletrust.de

Welcome

It is an honour for us to co-organise and host the ISSE 2008 Conference in Madrid (Spain).

Since 2004, the Spanish government, through the Plan Avanza (www.planavanza.es) [an initiative for the development of the Information Society], has worked to promote and to foster the Information Society, the Knowledge Society and Information Technologies, paying special attention to e-government and information security, increasing the security levels of companies, administrations and citizens, and promoting the safety culture and acceptable levels of awareness regarding information security.

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

The penetration of information technologies and the Internet in Spain reaches levels significantly above the average of other similar countries, this year exceeding 22 million internauts and over 80% of companies connected to the Internet. Mechanisms, such as the creation of the digital identity through the Spanish National Electronic Identity Card (DNI-e) – which contains more than 500 services for e-government, e-commerce and e-banking –, or the reactive and preventive attention especially paid to information security incidents in all fields, act as a lever and support for an adequate development of the Information Society.

The inclusion of all sectors in the Information Society is vital to maintain a healthy and competitive economy. The introduction of such a necessary component of information security, allowing a reliable development and a sustainable maintenance, is vital.

ISSE 2008 will serve as an incomparable scenario to deal with the work of the organisations, industry and current and future trends in information security.

We hope that the topics discussed during the event will serve as a reference for the work of the organisations, industry and countries involved and that they will provide a forward-looking perspective that will strengthen the efforts constantly being made in the field of Information Society.

Instituto Nacional de Tecnologías de la Comunicación
(National Institute of Communication Technologies)

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información
(State Secretariat for Telecommunications and the Information Society)

Ministerio de Industria Turismo y Comercio
(Ministry of Industry, Tourism and Trade)

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

Security Management and Economics of Security

The Information Security Framework for Daimler Financial Services and its Implementation

Lenka Fibikova · Roland Müller

Daimler Financial Services AG, ITF Information Security
Epplestraße 225, 70546 Stuttgart
{lenka.fibikova | roland.g.mueller}@daimler.com

Abstract

In 2003, the Board of Management of Daimler Financial Services initiated a 3-year project to establish an information security management system (ISMS) within its organization including all (at that time 43) subsidiaries worldwide. In this article, we describe the setup of the ISMS and demonstrate how this setup allowed extending the scope of the ISMS to entities outside of the financial services market.

1 Legal Requirements for Financial Services Providers

Daimler Financial Services provides financial services in the automotive area in 43 countries on five continents. The portfolio includes financing, leasing, fleet management, insurance brokerage services and structured finance services. These services have to comply with applicable law in all markets and countries. The applicable legal requirements can be structured as follows:

- Risk control legislation,
- Data protection legislation, and
- Legislation fighting organized crime and terrorism.

The following paragraphs will explain what implications each of these legal directives may cause for a corporation especially in the area of information security.

1.1 Risk Control Legislation

Risk Control legislation has always been important for financial institutions, for its primary goal is the protection of customers' money. Almost all countries have regulated the financial market in order to protect customers and avoid bankruptcies caused by poor business execution. However, it gained momentum in the last decade caused by criminal activities in major corporations outside of the financial market. Bankruptcies of large enterprises like Enron and WorldCom led to more rigid legislation to avoid similar misbehaviors. The U.S. Sarbanes-Oxley Act [SOA02] is the most known example resulting from these acts; Basel II [BAS04] is a world-wide accepted and more structured approach for the financial area.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 3-19

Risk control legislation requires companies to sufficiently evaluate any risk it may face and develop adequate strategies to control the identified risks, may they be financial or non-financial. With respect to information security, integrity of financial information and business continuity are major areas to be taken into account.

1.2 Data Protection Legislation

Data protection plays an important role in Europe but becomes also more significant in the U.S. and Asia Pacific. Examples of this kind of legislation are the European directive on Data Protection 96/46/EC [EU96], the various national European privacy acts and the U.S. Gramm-Leach-Bliley Act [GLB99].

The intention of this legislation is the protection of personal information processed by companies. For financial services this targets on protecting customer information and avoiding any disclosure or other use without the customers' official consent.

With respect to information security, this legislation requires companies to protect customer data and to provide methods and processes that prohibit misuse and disclosure.

1.3 Legislation Fighting Organized Crime and Terrorism

This legislation, also known as money laundering legislation, can be seen as a contradiction to the data protection legislation for it requires companies to disclose those customers who are assumed to misuse financial transactions for laundering money gained by criminal acts. In light of terrorism, this legislation was amended to include money transfers with terrorist organizations. There are many countries addressing this topic in their legislation; an example of this on the national level is the German Anti-Money-Laundering Law [GWG93]. The United Nations addresses this topic by a program fighting money laundering and countering the financing of terrorism.

For information security, this requires processes to supervise money flow and customer clearance and rating procedures.

2 The Decision to Use an International Standard

Due to the fact that the various entities of Daimler Financial Services had no common understanding of information security nor had they followed any central initiative in the past, the IT management of Daimler Financial Services decided to make use of an internationally accepted approach. Various standards were taken into account:

- NIST Special Publication Series 800 [NIST800],
- German Information Security Agency's Baseline Security Handbook [BSI03],
- ISO/IEC 13335 Guidelines for the management of IT security [ISO13335], and
- ISO/IEC 27002 Code of practice for information security management, at that time known as ISO/IEC 17799 [ISO17799].

2.1 NIST Special Publication Series

The National Institute of Standards and Technology, an institute governed by the U.S. Department of Commerce, provides a lot of guidance material on how to establish information security. However, their primary target is the federal administration of the United States and this restricts the usability of their publications. On the other hand, the material provided is kept up-to date and offers valuable input for various areas of information security. The documents on business continuity, on the installation of an awareness program for employees and technical material on how to protect an infrastructure are a substantial help for any organization dealing with information security.

2.2 German Baseline Security Handbook

The German Baseline Security Handbook follows a similar approach in primarily targeting the German federal administration. Their stronghold is the technical guidance, but they lack management guidance. In addition, due to their concentration on technical issues, they bear the risk of becoming outdated.

2.3 ISO/IEC 13335 Guidelines for the Management of IT Security

The guidelines for the management of IT security published by ISO/IEC during the second half of the last decade are strongly focusing on managerial tasks with respect to information security. Topics like the implementation of an information security organization, responsibilities and awareness are sufficiently well specified to enable an organization in fulfilling its tasks. In addition, risk management is described in a way to establish it without strictly following only one methodology. Finally, guidance is provided how technical issues like those offered in the NIST series or by the German Information Security Agency can be used to complement the series of standards. On the other hand, this standard series becomes less important with the progressing development of the 27000 family of standards.

2.4 ISO/IEC 27002 Code of Practice for Information Security Management

The final candidate was the ISO/IEC 27002, at that time known as ISO/IEC 17799. It was originally derived of the British Standard BS 7799 and tries to cover the technical and the managerial aspects of information security within one document. Although it is not the perfect fit, it offers the best solution for international corporations by its broad orientation. Its areas of control range from policies as the fundament of information security management to compliance with internal regulations and applicable law. Its weaknesses come from excluding risk management from the standard, but it tries to overcome these weaknesses by postulating risk management as a prerequisite. Its specific advantage is that it allows an evaluation of the status of information security on a high level, which executive management prefers.

2.5 Summary

Table 1 summarizes features of the above mentioned information security guidance approaches. Daimler Financial Services decided to focus on ISO/IEC 17799 being aware of the fact that the version from 2000 was to be revised within a few years.

Table 1: Information Security Guidelines

	NIST Special Publications 800-x	BSI Baseline Security Handbook	ISO/IEC 13335 Security Guidelines	ISO/IEC 17799 Code of Practice
Audience	Technical and management	Primarily technical	Management	Management and technical
Content	Technical and management oriented	Primarily technical oriented	Management oriented	Primarily management oriented
Completeness	High	Technically high	Management aspects high	Management aspects high
Software Support	Only few	Quite good	Not	Good
Pros/Cons	Very good quality of information	Good quality, not always up to date	Too extensive and sometimes poor quality	Good quality but requires additional guidance on technical level

3 Initial Information Security Status Evaluation

In order to map the existing status of information security in the organization, the Corporate Information Security Officer initiated an initial information security assessment in all entities of Financial Services. Since it was impossible to visit all 43 entities within a short time, the evaluation was based on a self-assessment conducted at all entities, complemented by on-site assessments, remote penetration testing and on-site technical evaluations at selected entities that helped to verify the plausibility of the results from the self-assessments. The initial status evaluation was conducted within three months.

3.1 Self-assessment

The self-assessment was based on an Excel based questionnaire consisting of more than 200 questions derived out of the ISO/IEC 17799:2000 standard. All ten security control areas of the standard[1] were covered to obtain a comprehensive status of the corporation's information security. Due to the fact that the portfolio of the various entities of the group differed, not each question was relevant for each entity; therefore any question could be answered by one out of four different answers: yes, no, partial, not applicable. The filled-out questionnaires built the basis for the next step – the identification of the appropriate actions on the corporate level as well as locally.

3.2 On-site Assessment

The on-site assessments were intended to verify the results from the self-assessment questionnaire. During the on-site assessment all areas of the questionnaire – the ten security control areas of the ISO standard – were evaluated. This way, information security did not only focus on those topics where IT is mostly involved, but especially on the areas where other departments (e.g., legal department, human resources) were in the lead. During the on-site assessment, all relevant departments were interviewed and each answer was confirmed by evidence. The outcome showed that the entities conducted the self-assessments diligently; deviations were primarily caused by misinterpretations of specific questions. In summary, six entities on three continents were visited and had to undergo an on-site assessment.

1 ISO/IEC 17799 (2000) consisted of 10 control areas; the version of 2005 added incident management as an additional control area.

Privacy, Data Protection and Awareness

Freedom and Security – Responses to the Threat of International Terrorism

Marie-Theres Tinnefeld

University of Applied Sciences Munich
Germany
tinnefeld@cs.hm.edu

Abstract

The September 11 attacs have led to a number of changes in the legislative framework of the EU member states. Governments intended to react quickly, powerfully and with high public visibility reactions in public to justify the power of technology in the interests of national security. The new goal is to search terrorist activity in the ocean of telecommunications data retained by communications providers and accessed by intelligence authorities. EU member states have to put in place a national data retention law by March 2009. In Germany, the most recent problem is the question of the legality of the secret online-surveillance and search of IT-Sytems, especially concerning of individual´s PCs. The German Federal Constitutional Court has held, that the area of governmental authority for intervention must be limited by the constitutional protection of human dignity and fundamental rights like information privacy, telecommunications secrecy and respect for the home. In February 2008 the highest German Court created a new human right of confidentially and integrity of IT-Systems. The decision has to be understood as a reaction to the widespread use of invisible information technology by legal authorities and their secret and comprehensive surveillance of the citizens.

This article highlights the critical question, whether civilization, human rights and democracy can survive at a time, when, after the rise of terrorism the security principle seems to be the primary arbiter of information society. In particular the German Court decisions will serve as convincing evidence on the real strength of balance between freedom and security, both of which are claimed to defend the open information society.

1 Introduction and Background

Since the Enlightenment in the 18th century, the constitutional states of Europe have justified their existence through the protection of fundamental civil and human rights. Their determination was not limited to the proclamation of individual freedoms, especially freedom of thought, conscience and religion, freedom of speech and expression and freedom of the media against power of the state. The greatest gift of the classical and contemporary idea of human rights is the insight, that the core values of the personality are inviolable.

In the most famous essay on privacy ever written, published in the Harvard Law Review in 1890, Samuel D. Warren and Louis D. Brandeis (WaBr 90) wrote that "the common law secures to each individual the right of determing, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." The legal principle that prevented prosecuters from scrutinizing diaries, letters books and private papers was the same principle that, in their view, should prevent gossip columnists from writing about the private lives of citizens. They called that principle the right to an "inviolate personality" as part of the more general "right to be let alone". Alan F, Westin defined in 1967 "information privacy" as "the claim of individuals, groups, or institutions to determine for themselves how, when,

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 93-98

and to what extent information about them is communicated to others (West67). Based on the arguments in the article "The Right to Privacy" written by Warren and Brandeis and the input by Westin the German Federal Constitutional Court postulated information privacy in connection with respect for human dignity in its pathbraking decision "Volkszählungsurteil" in 1983[1] as a "new" human right. It includes basically that:

- Personal data just shall be processed only for a certain purpose
- Individuals have a right to know to what extent their data is processed (requirement for transparency).

In 2004, in its decision on the „Great Eavesdropping Offensive" (*Großer Lauschangriff*)[2] concerning laws regulating wiretapping and visual surveillance, the German Court emphasized the fundamental nature of an individual´s right to be informed that he or she has been placed under (telecommunications) surveillance, even in times of terrorism. Part of this decision rests on the importance of:

- The role that one´s home and its physical space plays in insuring the "right to be let alone".
- Information privacy as a basic right is necessary for the free development of personality and for a liberal democracy.

The countries of the European Union confidently argued in the same way for the adoption of a general data protection directive in 1995 (Directive 95/46/EC). Accordingly, security technology has to support the understanding of information privacy, which views privacy as a right to control the use of one´s personal data.

As a result, security technology must guarantee:

- Transparency (the use of security technology has to be apparent to the data subject, Article 12 and Art. 17 Data Protection Directive.)
- Openness (Requirement for truthful information about the pros and cons of security technology in special contexts)
- Careful Treatment (In cases where the identification of a specific individual is not necessary for security purposes, it must be avoided.)
- Respect for legal requirement (Security technology has to comply with legal requirements. For example, security technology must support the person´s rights of recification, erasure or blokking of data, Article 12 lit. b and Article 17 Data Protection Directive.)

In response to the deadly attacks of 9/11 the situation has changed. The increasing use for security technologies jeopardizes the freedom of the citizen. Since the attacks, the U.S. have inacted more "predictive offense". Law enforcement authorities have moved towards preventive or "anticipatory" surveillance in the fight against terrorism. This development produced a number of counterterrorism laws and techniques – like, for instance, data mining searches (LeSch05), which have a significant negative impact on civil liberties. More specially, one could find leading examples of advanced technology control in George Orwell´s Telescreen from 1984, Jeremy Bentham´s Panopticon from 1791, in movies such as Minority Report from 2002 (Tinn08).

The following paper will first give a brief outline on the most significant changes in techniques and laws:

- Preventive Telecommunications Surveillance
- Data Mining Searches

1 BVerfGE 65, 1.

2 1 BvR 2378, 288-318, available at://www.bverg.de/entscheidungen/rs2004_1bvr237898.

- The Data Retention Directive 2006/24 EC.

Secondly, the developments will analysed in the light of the jurisdiction of the highest German Court, especially concerning the secret online-surveillance and search of IT-Sytems.

The final part identifies key issues of privacy principles and and other fundamental values of an open, democratic society, and might serve as a reponse to the threat of international terrorrism.

2 Terrorism Information Awareness

2.1 Preventive Telecommunications Surveillance

The U.S. and European Countries´ law enforcement authorities are engaged in anticipatory strategies, especially in preventive telecommunications surveillance. Preventive wiretapping is different from the traditionel repressive surveillance (Abro3):

- Repressive wiretapping investigates a specific criminal offense, which requires proof that a crime has taken place or is likely to occur.
- Preventive wiretapping starts without a reasonable suspicion of a specific person or a specific offence. This means that there is a great danger of intruding into the privacy of innocent persons.

In its decision on the *"Große Lauschangriff"* in 2004, the German Constitutional Court emphasized that the constitutional protection of human dignity extends broadley to situation, in which an individual "communicates with others".

2.2 Data Mining Searches

Data mining refers to techniques which are used by intelligence authorities to extract intelligence from vaste stores of digital informations (LeSchw05). Based on the premise that the planning of terrorist leave their mark, they investigate "in the ocean of transaction data created in the course of daily life" (DeFl04). There is a big difference beween behavioural- and subject-based searches:

- Subject-based searches start from the basis of reasonable suspicion.
- Behaviour-based searches trust in the predictive power of behavioural patterns for the identification of terrorists.

The international well-known security specialist Bruce Schneier views data mining on behaviour-based searches as a sort of enlarging the proverbial haystack where you look for a needle, or a terrorist (Schn05). James X. Dempsey and Lara D. Flint point out, that the behaviour-based data mining is in conflict "with the constitutional presumption of innocence and the Fourth Amendment principle that the government must have individual suspicion before it can conduct a search" (DeFl05). This result corresponds with the preliminary judgement of the German Constitutional Court in March 2008 concerning the German Data Retention law adopted in January 2008. The judges held that under Art. 10´s explicit constitutional protection of telecommunications secrecy the use of telecommunications data is only permitted for the prosecution cases of serious crimes. The surveillance should capture evidence of the crime. An unlimited control of communications data strays into "communication behaviour" and damages the rights of an innocent person.

2.3 The Europeans Union Data Retention Directive

Initially, the supranational institutions of the EU were divided on the issue of retention of telecommunications data. But in 2006, problems with the "prevention, detection and investigation of crime and terrorism" led to the adoption of the Data Retention Directive 2006/24/EC (Watn07). By March 2009, all EU member states must provide for the retention of subscribe, traffic and location data generated through the sending of e-mails, and fax transmission, fixed-line and mobile phone calls and internet usage by communication service providers. Law enforcement agencies will have access to this data for public security purposes. Under German law implementing the directive which was adopted in January 2008, communications providers must save communications data for a period of six months. As described above, the Constitutional Court´s decision of March 2008 restricts the intelligence services´use of that data to the purpose of preventing, detecting and prosecuting serious crimes.

The European directive is limited to the surveillance of telecommunications data including, among other things, the telephone numbers dialed, e-mail address from which and to which a message is sent and subscriber details such as bank account numbers, that are transmitted with the use of the phone. The directive is not concerned with the content of those communications including the words spoken in a conversation or the words, pictures and sounds found in the message part of an e-mail or text message.

With the storage of communications data the state can track people´s online activities. Law enforcement agencies and intelligence services can develop comprehensive internet profiles of those persons.

In Germany, communications service providers may already store communications data for their own business purposes, for example billing purposes for as long as the data are required for those purposes. Under the EC´s Directive, Germany´s providers, like those of all member states, must now store those data for the purposes of the intelligent services. The 6-months retention period under the directive is likely to extend that which would have been permitted for billing purposes. Moreover, the directive actually permits the member states to adopt laws which allow the mandatory retention for up to 24 months. Many member states have indicated that they will require the retention for the maximum period.

This raises the spectre of the inconspicuous, if unlawful, use of those additional data by the communication service providers for their own purposes. This fear has been confirmed by the well-publicised "Telekom-Scandal" uncovered in Germany recently. Over a number of years the German Telecom AG systematically collected communications data relating to fixe-line and mobile telephone calls between employees of the company und journalists that were made via its network. The intention was to identify employees who may have disclosed confidential information about the company to journalists. Via which interfaces did the Telekom spies access the communications data? Did they access the data collected by the Telekom's billing and accounts department, or did they use the infrastructure put in place on behalf of German law enforcement authorities? Was there a logging of this accesses? According to new information the company is even said to have created individual profiles, collected banking data and cross-referenced location data relating to the peaple whose communications it monitored[3].

It becomes clear, therefore that adequate technological safeguards must be in place to ensure that access to such data is only possible only when it is necessary and where it is required by those with legal authority. Under the circumstances, the only „tidy" solution for data retention is likely to be the establishment of two separate databases:

3 http://www.heise.de/newsticker/Wissenschaftler-analysieren-individuelle-Bewegungsprofile-von-Handynutzern--/meldung/109012

- One for data already being legally stored for billing purposes
- Another one for „communications data, intended to be accessed solely by law enforcement authorities.
- However, who is to implement security and logging functions? Can the industry be trusted to implement a government-only communications data database with no backdoors? Where access is reserved exclusively to law enforcement authorities?

3 The secret online-surveillance and search of IT-Systems

The Internet´s technical qualities and the widespread use of information technology are linked to the secret online-surveillance and search of IT-Systems by intelligence agencies, especially of individuals' PC and portable devices. On these devices one can find diaries, love letters, health data, accounts data, mailing-lists and business reports: files that are a key to the privacy and intimate sphere of a person. On 27 February 2008, the German Constitutional Court has addressed this problem. The Court created a new human right of the "confidentiality and integrity of IT-Systems" as a constitutional safeguard under Article 2 (1) and Article 1 (2) of the German Constitution (*Grundgesetz*)[4].

In asserting this new human right that could protect citizens against the secret infiltration and search of IT-Systems the German Court says: "The right of informational self-determination does not sufficiently take account of the dangers of a violation of an individual's personality right resulting from the fact, that individuals depend on the use of information technology systems for the development of their personality and therefore entrust to those systems, are even forced to populate those systems, with personal data. A third party with access to such a system, is able to procure a substantial amount of crucial data and will no longer need to rely on further data retrieving or data processing measures. The impact of such access on the individual's personality exceeds by far that of specific data collection which the right to informational self-determination protects[5]."

The decision is part of the Court´s evolving case law on personality rights. As noted above, the core of privacy information is the individual´s right to determine " to what extent she or he will communicate his thoughts, sentiments, and emotions to others". This new fundamental right goes further. It protects the citizens against an invisible data access by the state, for example by "spyware". Protected are, for instance, recording processes in the background of an IT-System.

As Tomas Petri (Petr08) notes, the online search and surveillance intervention goes much further than a continuing telecommunication surveillance, from which the right to telecommunications secrecy provides protection. In its continuing case law, the Constitutional court has repeatedly pointed out that the state, when carrying out secret surveillance operations, must respect a core area within which the individual can make decisions about his private life[6]. In practice, it is of course not very easy for the law enforcement agencies to assess the limits of that core area before they start collecting the data. Consequently, security technolgy must be embedded in good privacy practice.

4 BvR 370/07 and 1 BvR 595/07, available under: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
5 Id. Part 200
6 See BVerfGE 6, 32, 41; vgl. z. B. BVerfGE 109, 279, 313.

Trusted Computing and Biometrics

Trusted Storage: Putting Security and Data Together

Michael Willett · Dave Anderson

Seagate Technology and
the Trusted Computing Group
{michael.willett | david.b.anderson}@seagate.com

Abstract

State and Federal breach notification legislation mandates that the affected parties be notified in case of a breach of sensitive personal data, unless the data was provably encrypted. Self-encrypting hard drives provide the superior solution for encrypting data-at-rest when compared to software-based solutions. Self-encrypting hard drives, from the laptop to the data center, have been standardized across the hard drive industry by the Trusted Computing Group. Advantages include: simplified management (including keys), no performance impact, quick data erasure and drive re-purposing, no interference with end-to-end data integrity metrics, always encrypting, no cipher-text exposure, and scalability in large data centers.

1 Introduction

Is there no end to reports of data breaches? Every week headlines tell of yet more incidents. Data encryption has been recognized by law in 42 states and more widely as good practice by security experts to be an effective measure for protecting sensitive information against data breaches. Moreover, those laws state that the use of encryption eliminates the requirement for public notification of the breach.

Laptops and tapes are not the only potential risks. Every day, thousands of TB of data leak out of data centers as old systems are retired or replaced, often with little thought given to *properly* erasing the data they contain on their hard-drives. But what if those hard drives had all been quietly encrypting all of that data, transparently & automatically, such that only the true owner were able to access real data?

Until now, however, encryption has been hard to use, and in some cases discouraged users from incorporating it into their security strategy. Instead many users simply hope the data breach bug will not bite them. Embedding the encryption function within the storage device (often called Full Disk Encryption, or FDE) improves this, and makes it easier to choose protection over hoping. FDE offers several benefits over other approaches to encryption:

- Makes deploying and managing encryption easier, and doing so with no impact to system performance
- Makes the confidentiality that encryption affords even stronger
- Integrates better with other functions of enterprise storage architectures

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 131-138

This paper will explain these benefits in greater depth. It assumes a basic understanding of FDE operation. For information on FDE operations, see "Self-Encrypting Hard Disk Drives in the Data Center" on the Seagate web site: www.seagate.com or consult the Storage section of the Trusted Computing Group: www.trustedcomputinggroup.org) .

2 Definitions

- Array Controller: The hardware/software combination that abstracts and exposes for host access the logical blocks of the hard drives attached to it. For the purposes of Hard Drive-based security services, like FDE, the Array Controller is the only device that communicates directly with the Hard Drives. Consequently, it is responsible for directing how the security will be configured and arranging for the drives to be unlocked for use.
- FDE: Full disk encryption. A disk drive (see below) which includes within it the ability to encrypt all data stored on it.
- Hard Drive: A disk drive. In a data center the hard drive is usually attached to the Array Controller that will be responsible for managing it.
- IPSec. Internet Protocol Security. A method for providing confidentiality and authentication on Internet communications.
- Keys: Secrets used to protect the confidentiality of stored data and Hard Drives. This paper describes at least three types of keys:
  - Authentication Key. A credential used to lock and unlock an FDE drive.
  - Data Encryption Key, or Encryption Key: A symmetric key generated by the Hard Drive used to encrypt/decrypt data.
  - Session Key. An encryption key used to provide confidentiality of transmitted data. See IPSec and TLS.
- Entropy. A measure of randomness or unpredictability
- Storage System: See Array Controller.
- Re-encryption: The process whereby the data encrypted with one key is read from storage, decrypted, encrypted again with a new key and written back to storage.
- TLS. Transport Layer Security. A data transmission protocol designed to preserve the confidentiality of transmitted information.

3 Self-encrypting disk drives, simplifying management

3.1 FDE: Requires no changes to OS, applications, or networks

An advantage that first stands out when users learn of FDE is that it is isolated from most of the other system elements. The Operating Systems, applications, and network infrastructure do not have to change to accommodate FDE. Isolating the impact of introducing encryption to the storage system and its management minimizes who needs to be educated on FDE, and simplifies the adaptation of existing processes.

3.2 FDE: A model for completeness

Since FDE always encrypts everything written to the drive, there is no need to worry about data classification. Identifying all the instances of personally identifiable information can be a nightmare for an IT department, especially when such information can so easily be extracted from a protected database into an unprotected destination. An authorized user could paste social security numbers from a strictly controlled database into a spreadsheet, where tracking its existence is almost impossible. Since FDE makes it so simple to just encrypt everything, the entire problem of data classification (and the attendant management challenges that start once data is classified) is avoided.

3.3 One secret to manage

When managing encryption, there are typically two sets of secrets to keep track of and protect. The first are the data encryption keys. These are the values used to encrypt and decrypt the user data as it is written to or read from the drive. It is obvious that care must be taken to prevent the compromise of the encryption keys; the data is only as secure as these keys are safe. The other set of secrets are the authentication keys. These are the credentials that must be supplied to authorize the drive to commence operation. In some systems these are passwords, pass phrases, biometric scans or smartcard protected values. These often represent the authorization users have to make changes to the encryption function. For instance, an administrator may be authorized (know the authentication key necessary) to remove some storage from the data center for replacement. Should that administrator leave, security policy will likely call for that key to change. This would only be good practice.

The distinct advantage FDE brings to this situation is that the encryption key is in the drive, never leaves the drive, and never needs to be managed outside the drive. This lessens the problem of secrets management associated with the encryption function. As we will see later, in addition to simplifying key management, isolating the encryption key in the drive will make for a superior data destruction model. For key management, though, since no auditing, tracking, or external exposure of the encryption key is necessary with FDE, it is less likely that re-encryption will be called for than with any other encryption technology.

Although some approaches to encryption use only a single set of secrets, it should be pretty clear why there must be two sets of secrets, and why they must be kept separate. If the administrator who left knew the encryption key, it would have to change – and all the data protected by that key would have to be read and re-encrypted. In a large data center this could be traumatic. By separating the authentication keys from the encryption keys, a change in personnel would only require a change in authentication key and leave the encryption key unaffected. FDE embodies this, adding the benefit of eliminating the separate management of the encryption key.

3.4 An open interface and multiple sources

The FDE drive is intended to be a component in a larger security system. To this end, it exposes an interface, based on industry standards activity in the Trusted Computing Group (TCG) that enables exercising the various processes associated with key management. This makes it relatively straightforward for an array controller in a storage system to incorporate controlling the encryption function along with the other drive responsibilities it assumes.

Web 2.0 Security and Large Scale Public Applications

Development and Implementation of an Encryption Strategy for a global Enterprise

Guido von der Heidt

Siemens AG
Corporate Information Technology, CIT G ISEC
guido.von_der_heidt@siemens.com

Abstract

Encryption is a main instrument of Information Security Management to ensure confidentiality of electronic information and communications.

Following an information centric security approach based on risk management and information classification we develop an encryption strategy for a global enterprise and describe the implementation of this strategy in a case study on Siemens Corporation.

1 Introduction

Encryption controls are main elements of an Information Security Management Program to ensure confidentiality and with restrictions integrity of data and communications. Industrial espionage, (targeted) attacks against IT-enabled business processes, data privacy protection requirements, etc. increase the need for deploying encryption technologies and a variety of encryption products and solutions are available on the market. However, encryption technologies often are still not widely adopted or used in isolated scenarios only.

In this presentation we describe the development and implementation of an encryption strategy for a global enterprise based on a case study on Siemens Corporation.

Following an universal information centric security approach based on risk management, information classification and specific influencing factors – in particular the technical environment the dare processed in – we derive at first a generic Encryption Framework defining and prioritizing the demand for encryption.

In the second part of the presentation we discuss encryption technologies and business/IT-related requirements for encryption solutions. The identified encryption solutions are mapped to the Encryption Framework and a general Encryption Technology Deployment Strategy is developed.

In the last section we present the implementation of the described encryption strategy at Siemens, measure the current implementation degree and discuss open issues. As specific aspect for global enterprises we allude to the deployment of encryption technology in face of international regulations for import, export and use of encryption products.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 197-207

2 Definition of an Encryption Framework

Confidentiality, Integrity, Availability and Liability are considered as core principles of Information Security. Thereby, confidentiality is defined as "preventing disclosure of information to unauthorized individuals or systems".

In order to determine appropriate confidentiality protection measures for a certain information asset an information centric security approach based on the classification of the information and an individual risk management is pursued, cf. the NIST Risk Management Framework [NIST02].

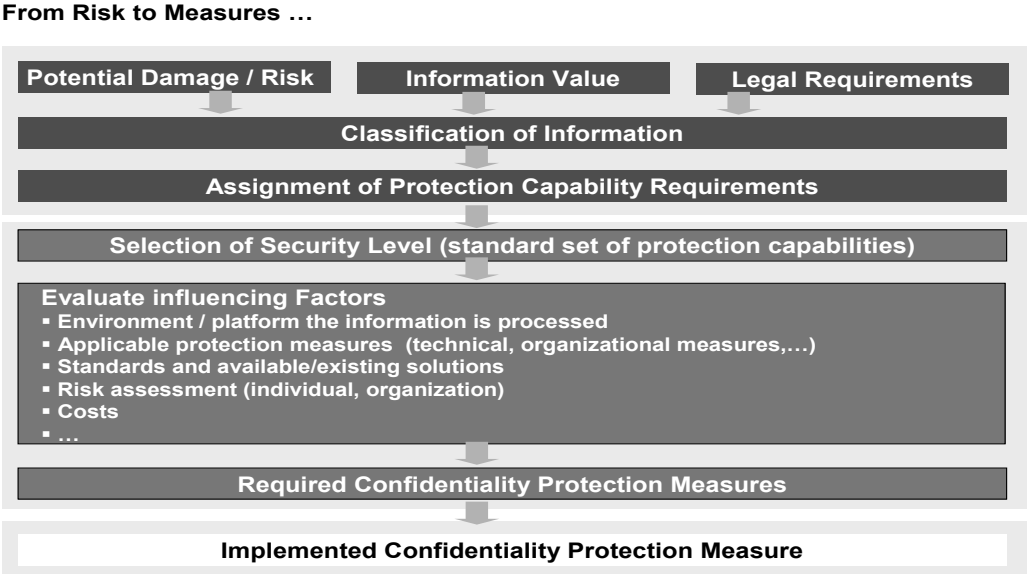

Figure 1: Information centric Security Approach to determine Confidentiality Protection Measures

2.1 Classification and Assignment of Security Levels

Information classification is a well-established practice in many companies and organizations. Classification means the categorization of (proprietary) information in classes with similar damage potential in case of unwanted disclosure of the information. Main factors for the classification of an information asset are:

- Damage / business impact of unwanted disclosure of the information
- Value of the information
- Legal and regulatory requirements (e. g. data protection laws)
- For this paper we assume a classification scheme consisting of 4 information classes:
- "Public"
- "Internal"
- "Confidential"
- "Strictly Confidential"

For each of these classes we define basic conditions for accessing information of the respective class and an required quality level for controlling the access. The access control and it's enforcement must comply with the confidentiality requirements of the respective class, i.e. the higher the confidentiality class the higher the required quality of the access control. In order to determine the quality levels we define a standard set of protection capabilities which must be met for each class:

- Access control enforcement capabilities
- Capabilities for proof of identity
- Authorization capabilities

These sets of protection capabilities form default security levels which are assigned to the information class. The following Tables give a generic definition of the 4 information classes and the assigned security levels.

Table 1: Information Classes

Classification	Definition	Access Conditions
Public	Public information	No requirements
Internal	Proprietary information with potential damaging consequences in case of unwanted disclosure	All employees / members of an organization can have access to the information. The information is not intended for outsiders but defined external partners can have access (e. g. in course of a contractual relationship). No further specification of authorization rules by the information owner
Confidential	Proprietary information with high business impact. Unwanted disclosure can bring substantial (financial) damage.	Only a defined group of users (.e . g. based on roles) is authorized to have access. The group of authorized users is defined by the information owner.
Strictly Confidential	Proprietary information with very high business impact. Unwanted disclosure can bring severe (financial) damage.	Only a explicitly named group of users is authorized to have access. The group of authorized users is defined by the information owner.

Table 2: Security Levels

Classification	Security Level	
	Access Control Enforcement	Proof of Identity / Authorization
Public	No requirements	No requirements
Internal	Authorization rules (if available) are applied to "standard" users Privileged users (e. g. IT administrators) exist, authorization rules are not under control of the information owner	Simple proof of identity required, e. g. by possession of a device All users with sufficient access rights can define authorizations
Confidential	Authorization rules are applied to all users (if possible) Privileged users may exist, access by privileged users is restricted and controllable Fail-secure access Negative access decisions and access by privileged users are traceable	Explicit proof of identity required, the digital identity must be explicitly assignable to a person, team, etc. Explicit authorization rules required Only a group of users defined by the information owner can define authorization rules
Strictly Confidential	Authorization rules are applied consequently to all users No privileged users Fail-secure access All access control decisions are traceable	Non-repudiation of proof of identity required, the digital identity must be explicitly assignable to a person Explicit authorization rules required Only the information owner defines authorization rules

2.2 Scenarios and Risk Assessment

The definition of protection measures to realize a selected security level is significantly impacted by influencing factors such as:

- Environment and technical platform the information is processed or stored
- Applicable protection measures
  - Technical measures
  - Organization measures
  - Process measures
- Standards
- Available/existing products and solutions
- Specific business risks
- Individual risk assessment
- Costs

In particular the environment and the technical platform electronic information are processed is essential.

Finding appropriate protection measures for an individual information asset which comply with the selected security class is a complex process. In order to manage this process we define standard scenarios for the environment data are processed, perform a risk assessment for this scenarios and define an encryption framework based upon this scenarios.

We differentiate the following environments/platforms:

Networks

- Internal Networks – Networks exclusively managed for the company/organization by an internal service provider or IT department, e. g. LANs
- Outsourced Networks – Networks operated by an external service provider and leased or managed for the company/organization, e. g. WANs
- Public Networks – Public available/accessible networks, e. g. Internet, public telecommunication networks or wireless networks

Systems

- Internal systems – Systems or applications in the intranet managed exclusively for the company/organization by an internal service provider or IT department
- Outsourced systems – Systems or applications in the Intranet managed for the company/organization by an external service provider, e. g. application service providing
- Extranet Systems – Systems accessible from external/public networks
- Mobile Systems – Mobile devices and removable media, e. g. notebooks, PDAs, USB sticks etc.

The networks and systems are listed with increasing exposure to unwanted disclosure of information. Public systems are not considered since we assume here that storage/processing of classified data on public system is not allowed at all.

Fraud Detection, Prevention and Critical Infrastructures

OTP and Challenge/Response algorithms for financial and e-government identity assurance: current landscape and trends

Philip Hoyer

Senior Architect – Office of CTO, ActivIdentity (UK)
117 Waterloo Road, London SE1 8UL
Philip.Hoyer@actividentity.com

Abstract

This paper will analyse the current landscape of One Time Password (OTP) and Challenge-Response algorithms. It will detail the technical and security differences between algorithms such as the OATH algorithms (HOTP, OCRA, HOTP time based), EMV CAP and the proprietary algorithms from ActivIdentity. The paper describes the most common use cases and applicability as important tools for identity assurance in the financial and e-government industry sectors. It also outlines observed trends in current usage and future trends providing the audience with the valuable information to make a more informed choice in their identity assurance challenges.

1 Anatomy of OTP algorithms

Before delving into the history and differences between the various OTP algorithms lets start with the basics. This will allow the understanding of where the differences lie between algorithms and how they impact security and usability.

1.1 What is a one time password (OTP)

A code that changes after every use, can only be used once, hence is a one-time-password, or OTP.

An OTP is based on a cryptographic algorithm using a key K a cryptogram is generated

$$\text{Cryptogram} = f(K)$$

Computing the cryptogram with other, moving factors makes the output random and one time:

- Counter – increased with each usage (also called event) and/or
- Time – number of time intervals (e.g. seconds)

$$\text{Cryptogram} = f(K,C,T)$$

A truncation function makes it short and human readable:

$$\text{OTP} = \text{Truncate}\,(f(K,C,T))$$

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 281-290

1.1.1 OTP moving factor analysis

The moving factors used to make the password one-time have implications both for the usage and the security of the overall OTP algorithm:

1.1.1.1 Time only based algorithms

- the OTP changes based on time-interval (e.g. every 30 seconds)
- the OTP has a time to live (e.g. can be used within next 2 minutes)
- the OTP is harder to phish because it must be used within the time to live
- it is not possible to generate a new OTP within the same time interval (e.g. user needs to wait for next interval -> up to 30 seconds)
- needs replay protection on the server since a simple algorithm would successfully validate attempts with the same OTP within the same time interval

1.1.1.2 Event only based algorithms

- the OTP can be requested at any time (no need to wait for time interval to pass)
- the OTP can be used at any time after being produced = no time to live
- easier to phish since phisher does not need to use the OTP within a time to live but can harvest the passwords and use them later
- Replay protection is simply based on forward moving counter only

1.1.1.3 Time and Event algorithms (combines best of above)

- the OTP has a time to live (e.g. can be used within next 2 minutes)
- the OTP can be requested at any time (no need to wait for time interval to pass)
- the OTP is harder to phish because it must be used within the time to live
- Replay protection is simply based on forward moving counter only
- Needs more complex auto-resync (2 moving factors instead of 1 that could go out of sync between the server and the device)

1.1.2 OTP algorithm analysis

Let's look more closely at what cryptographic algorithms can be used to generate OTPs:

1.1.2.1 OTP algorithms using asymmetric cryptography

Because of the nature of asymmetric keys the verifier will need the complete signature to be able to validate it. The length of PKI signatures depend on the length of the key used so for example:

RSA 1024 = 1024 bits long = 128 bytes long = not easy to type

This makes the use of asymmetric algorithms less suitable for OTP algorithms, they could be used in situations where there is no human involved when transcribing the OTP for transmission to the validation server, for example in an OTP device that is connected via the USB port to a laptop.

1.1.2.2 OTP algorithms using symmetric cryptography

The nature of symmetric key cryptography means that the same Cryptogram can be regenerated by the verifying party and only part of the cryptogram (the truncated bit) can be compared. This means that an arbitrary length of the cryptogram can be used as the OTP making it short and easy to type.

Historically all well known OTP algorithms are based on symmetric key cryptography.

1.1.3 OTP authenticaion – how it works

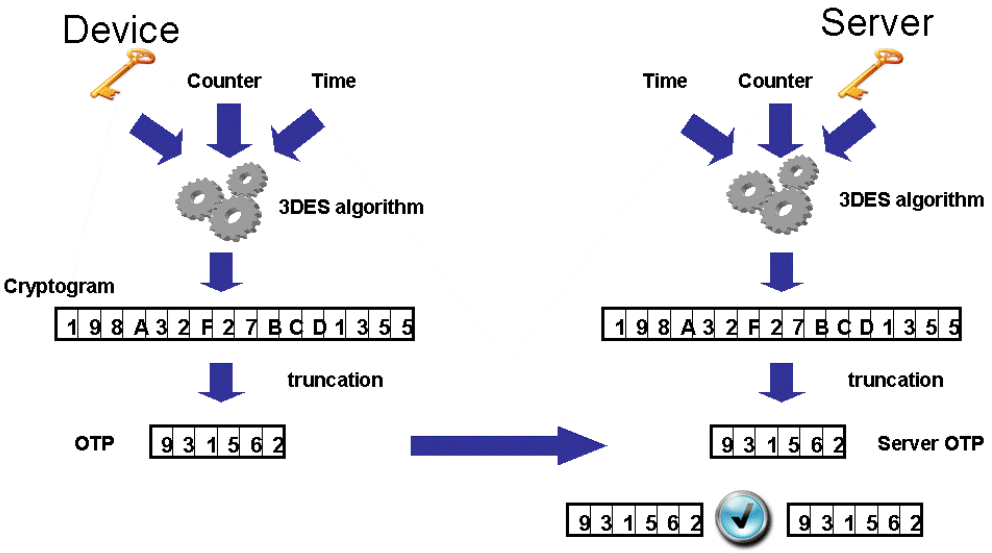

Figure 1: OTP algorithm in action

2 History and evolution of OTP algorithms

2.1.1 Traditionally – proprietary

Traditionally strong authentication algorithms using OTP were invented by private companies and their use immediately protected via patents.

One of the best known such algorithms is SecurID, invented in the U.S.A. by the company Security Dynamics, then acquired by RSA, now part of EMC. Initially these technologies were used to protect the network as part of authenticating a user strongly for access to the enterprise.

The same problem was solved independently on the old continent by companies such as ActivCard (now re-branded to ActivIdentity) out of France, now headquartered in Fremont California and later by Vasco (Belgium) now headquartered in Zurich.

With the emergence of internet based financial services, the need to protect those services became crucial and the same algorithms and technologies were used. Furthermore the requirement to protect specific transaction brought the emergence of challenge/response and Symmetric Key Signature (MAC over several parameter) algorithms.

2.1.2 Emerging – based on Industry standard (Financial Services)

The Europay MasterCard Visa Chip Authentication Program (EMV/CAP) is a set of specifications that detail the use of existing device technology [Mas04] (EMV compliant smartcard with unattached reader) for the use of consumer authentication for cardholder not present services e.g. internet based.

The specifications detail:

- A one time password algorithm
- A handheld reader
- A validation service

In 2003 MasterCard CAP was harmonized with an equivalent standard from the UK's Association of Payment and Clearing Services (APACS). APACS is currently developing a new specification which refines the user interface model for a handheld reader. This specification makes no proposed changes to the algorithm or validation service.

The EMV CAP specification seeks to leverage the extensive deployments of EMV chip based debit and credit cards, by expanding their use to include strong authentication and simple transaction signatures.

MasterCard CAP can also be used for transaction verification, either through forcing a re-authentication or more effectively through a Challenge/Response mechanism.

To use EMV for authentication requires the use of a Hand Held Device (HHD) that generates a One Time Password from the EMV card application (after correct PIN entry);

The resulting Cryptogram can be used for authentication to access and manage accounts held by the cardholder or during "cardholder not present" payments. As with other OTP technologies the model is suitable for use over the internet or other channels such as a call-centre.

Another benefit of the EMV CAP model is that the PIN used to activate the card is typically the same as the PIN that is already used with the card, for example to access ATM based services. This has the advantage that the customer is not required to remember an additional secret, and the infrastructure for PIN issuance and reset is already in place.

Visa, aside from a few minor changes to the standard, have adopted the MasterCard CAP specification, thus enabling re-use of CAP readers for Visa members. In Visa terminology, CAP is referred to as Dynamic Passcode Authentication – DPA.

The focus of this paper will hence treat the two as common under EMV CAP.

Currently EMV CAP is being deployed by major financial services institutions in the UK, Netherlands and France as an authentication mechanism for their retail customer base.

2.1.3 Recently – Open and Royalty free (OATH)

The Initiative for open authentication [OATH] is an industry consortium launched in 2004 and now grown to almost 100 members. OATH was formed after analysis of the existing algorithms for one time passwords suitable for a strong authentication ecosystem showed that they were all proprietary and from competing companies. OATH therefore endeavoured to create a royalty and patent free algorithm based on HMAC. This algorithm was submitted as a draft to IETF and has now become an RFC [RFC4226].

Security for VoIP, Mobility and Web

Evaluating Measures and Countermeasures for SPAM over Internet Telephony

Andreas U. Schmidt[1] · Nicolai Kuntze[1] · Rachid El Khayari[2]

[1]Fraunhofer Institute SIT
{andreas.schmidt | nicolai.kuntze}@sit.fraunhofer.de

[2]Technical University Darmstadt
rachid.el.khayari@googlemail.com

Abstract

Nowadays telephony has developed to an omnipresent service. Furthermore the Internet has emerged to an important communication medium. These facts and the raising availability of broadband internet access have led to the fusion of these two services. VoIP is the keyword that describes this combination.

Furthermore it is undeniable that one of the most annoying facets of the Internet nowadays is email spam, which is considered to be 80 to 90 percent of the email traffic produced.

The threat of so called voice spam or Spam over Internet Telephony is even more fatal than the threat that arose with email spam, for the annoyance and disturbance factor is much higher. From the providers point of view both email spam and voice spam produce unwanted traffic and loss of trust of customers into the service.

In this paper we discuss how SPIT attacks can be put into practice, than we point out advantages and disadvantages of state of the art anti voice spam solutions. With the knowledge provided in this paper and with our SPIT producing attack tool, it is possible for an administrator, to find out weak points of VoIP systems and for developers to rethink SPIT blocking techniques.

1 What is SPAM over Internet Telephony?

In order to know how to deal with SPIT, we must at first know what SPIT is and we will find that SPIT is described very similar in different publications and the descriptions can be summarized as 'unwanted', 'bulk' or 'unsolicited' calls. In [2] e.g. SPIT is defined as 'unsolicited advertising calls', which is of course already a special form of SPIT (namely advertising calls). In [3] SPIT is defined as 'transmission of bulk unsolicited messages and calls' which is a more general definition than the first one, as it doesn't characterize the content and includes also messages. Nevertheless the most precise definition is found in [1] where 'Call SPAM' (as the authors call it) is defined as 'a bulk unsolicited set of session initiation attempts (e.g., INVITE requests), attempting to establish a voice, video, instant messaging, or other type of communications session'. The authors of [1] go even one step further and classify that 'if the user should answer, the spammer proceeds to relay their message over the real-time media.' and state that this 'is the classic telemarketer spam, applied to SIP[1]'. We can easily see that the presented definitions so far are very similar, but differ in their deepness.

1 The whole discussion is based on the Session Initiation Protocol (SIP, RFC 3261)

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 329-340

1.1 SPIT is not SPAM!

Although SPIT contains the phrase 'SPAM' and has some parallels with email spam, it also has major differences. The similarity of email spam and SPIT is that in both cases senders (or callers) use the Internet to target recipients (or callees) or a group of users, in order to place bulk unsolicited calls [3]. The main difference between email spam and SPIT is that an email arrives at the email server before it is accessed by the user. This means that structure and content of an email can be analyzed at the server before it arrives at the recipient and so SPAM can be detected before it disturbs the recipient. As in VoIP scenarios delays of call establishment are not wished, session establishment messages are forwarded immediately to the recipients. Besides this fact the content of a VoIP call is exchanged not until the session is already established. In other words if the phone rings it is too late for SPIT prevention and the phone rings immediately after session initiation, while an email can be delayed and even, if it is not delayed, the recipient can decide if he wants to read the email immediately or not. In addition to these aspects another main difference between email spam and SPIT is the fact, that the single email itself contains information that can be used for spam detection. The header fields contain information about sender, subject and content of the message. A single SPIT call in contradiction is technically indistinguishable from a call in general. A SPIT call is initiated and answered with the same set of SIP messages as any other call.

1.2 How does a SPIT producing tool work?

The next questions that have to be considered are, how attackers behave and what techniques are used in order to generate SPIT. We can split the SPIT process into three steps:

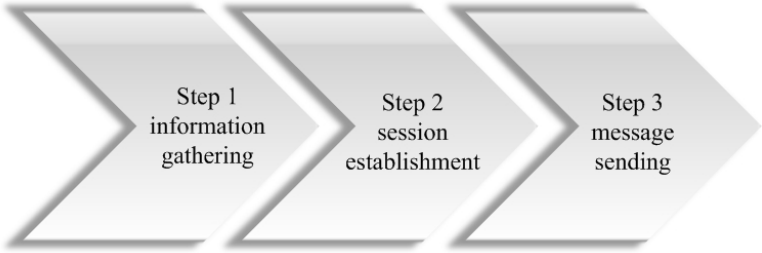

Figure 1: Three steps of SPIT

These three steps can be viewed as fundamental and are fulfilled by any attacker in a systematic manner. The first step the 'Information gathering' is used in order to find out targets for possible future attacks. The second step the 'session establishment' leads to the establishment of a communication session wit the victims. In the last step of SPIT the 'message sending' media is exchanged between attacker and victim.

1.2.1 SIP XML Scenario Maker

Now what we need is a tool that implements the presented SPIT process. Therefore we developed SIP XML Scenario Maker (SXSM), a tool with which it is possible to scan systematically for targets, establish sessions to these targets and exchange pre recorded media. SXSM is based on SIPp [12] developed by HP and expands SIPp with a graphical user interface that allows us to fulfill the requirements stated above. SXSM can be used in order to create any kind of SIP messages, put them into a sequence as XML scenarios, execute created scenarios and evaluate the result of the execution.

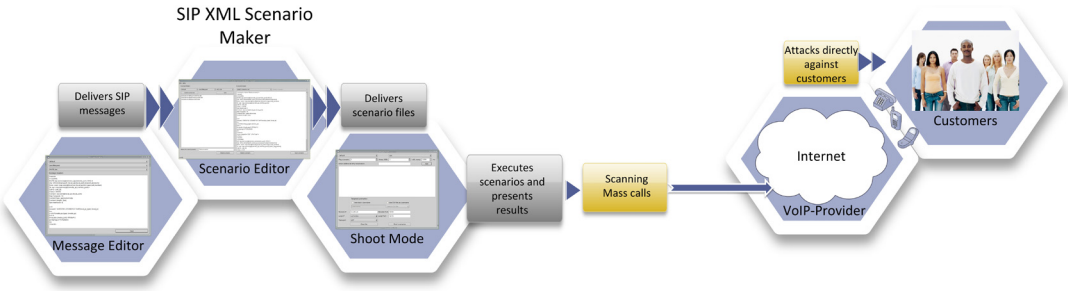

Figure 2: SXSM Workflow

We will now take a look on how SXSM works. First SXSM consists of the following three modes.

1.2.1.1 Message Editor

The message editor can be used to organize and create custom SIP messages that can later be used in the scenario editor. The power of this mode lies within the possibility to create any kind of SIP message and manipulate SIP header fields in any way. SXSM is pre configured with a complete set of standard compliant SIP messages.

1.2.1.2 Scenario Editor

The scenario editor is the core element of SXSM. In this mode the user can create SIP scenarios based on the message bricks created in the message editor mode. Additionally the created scenarios can be organized in different sets.

In order to create a new scenario the user simply needs to select the messages that should be contained in the scenario in the preferred order and then let SXSM create an XML scenario file automatically. The XML file can then be viewed in detail and tweaked manually (if wished).

1.2.1.3 Shoot Mode

Within the shoot mode the user puts the previously generated scenarios into a batch and execute them one after the other. The results of the execution are presented within the process output window. Before execution the user can specify scenario specific settings, such as e.g. how often and in which time intervals the scenario should be executed. Additionally he can adjust and set global parameters such as information about target (targeted username, remote IP, remote port) and about himself (local IP, local Port).

The scenarios are then played with the specified settings and the result is presented as a success rate. If e.g. 5 out of 10 selected scenarios were finished successfully the success rate would be fifty percent. Additionally the user can consult log files that are presented in case of unsuccessful execution.

1.2.2 How can we use SXSM as attack tool?

The goal that we wanted to reach was the creation of a tool with which it is possible to implement a SPIT attack in its fundamental three steps.

With SXSM we can now create scenarios for each of the three steps and execute them against any target. At first we can create a scenario for information gathering which we can call a scan attack scenario. The scan attack scenario can be implemented as follows. As SXSM contains the possibility of injecting values from CSV (Comma Separated Values) files, we would create a CSV file containing all usernames that we want to scan for. Then we would create a scenario with standard SIP messages that works e.g. as follows:

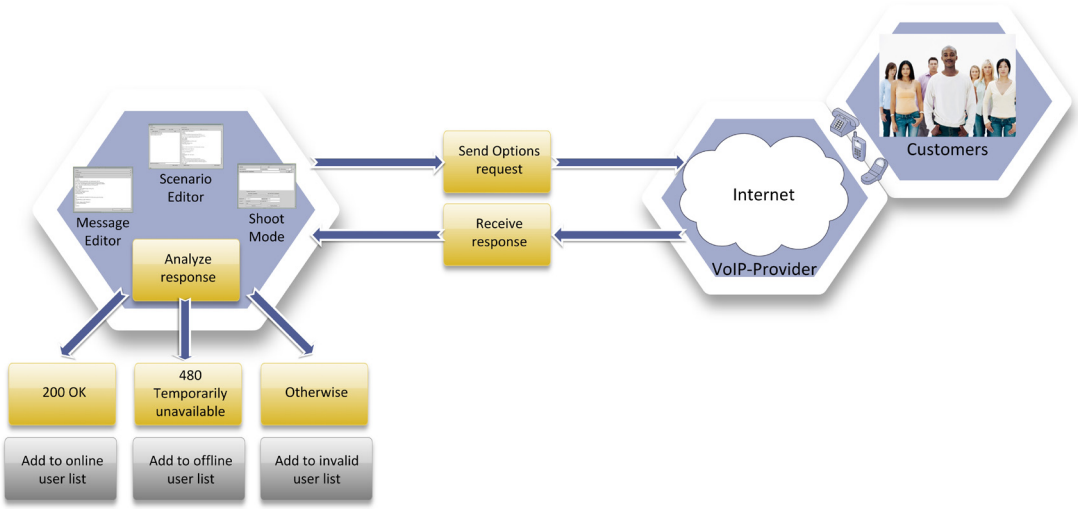

Figure 3: SXSM Scan Attack

With a scenario file that corresponds to the presented sequence of messages and logging methods, an attacker can populate lists of targets for future attacks.

The next steps would be session establishment and media exchange. With SXSM we could create a second scenario that establishes sessions to the targets collected in the first step.

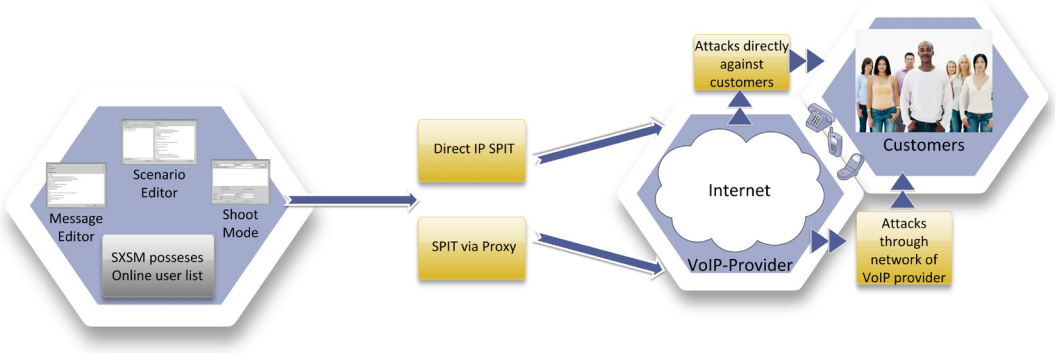

Figure 4: SXSM Session establishment

In Figure 4 we can see, that session establishment can be reached via two ways. SPIT via Proxy uses a valid account from targeted VoIP provider and the provider's network (Proxy, Registrar) in order to establish a session. In Direct IP SPIT context the targeted endpoint (telephone) is contacted directly via his IP and Port.

German Workshop: European Citizen Cards

Deployment of German Electronic Citizen Cards in Banking: Opportunities and Challenges

Matthias Büger

Group Technology & Operations
Deutsche Bank AG
matthias.bueger@db.com

Abstract

The German federal government plans to issue an electronic citizen card (eID) in 2009, replacing the current identity card (Personalausweis). Since the eID should be good for identification in E-government as well as E-business applications, it is aimed to be used in the banking environment. One application would be opening a bank account in the internet. If this was possible, the process would be much easier than today. However, German law still requires a physical ID card. We will discuss the opportunities and the challenges of possible usage of eID in banking.

1 Introduction: authentication & banking

From an IT perspective, a financial transaction consists of receiving data from a customer, processing data and finally giving some notice back. This is the structure of a money transfer, a brokerage order or any other standard transaction in online banking. Hence, the most efficient way to deal with such transactions is to exchange the data electronically.

The challenge is, however, that the data transferred is highly sensitive: Information must not be presented to any unauthorized person. This applies in particular to account information. Data received must be proven authentic before the bank can process a transaction. In case of a legal claim, the bank has to give evidence that the transaction was initiated by the customer. Unfortunately, the Internet itself does not come along with a security layer. There is an old (well known) cartoon, which shows what lies at the heart of the problem.

Figure 1: Lack of authentication in the Internet

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2008), 393-397

1.1 The PIN-TAN-system

This question of authentication is not new to banks. Ever since banks started online banking, authentication had to be guaranteed. In the 1990s a system named PIN-TAN (personal identification number – transaction number) was established in Germany. Every customer obtains letters with a PIN and a list of TANs. The PIN is needed to log-in to the system, while every transaction is authorized by a TAN. Today, Deutsche Bank (like many other German banks) uses indexed TANs (iTAN), where each TAN in the list has an index and the bank asks to enter a special TAN. This results in a higher level of security. Standard phishing attacks, where an attacker spies out TANs and tries to use them later, do not work with iTAN. There are also other flavours of the PIN-TAN-system. For example, a TAN might be sent on demand as a SMS (sometimes called mobile TAN or mTAN). Overall, PIN-TAN-systems work more or less alike: the user authorises a transaction using a knowledge he had received from the bank before.

Despite academic discussions, in practice the PIN-TAN-system has been working successfully for many years. User acceptance is high: In Germany, there are more than 10 million online banking accounts, and nearly all of them are based on some flavour of the PIN-TAN-system.

There are many reasons for the success of the PIN-TAN-system. The most prominent are: The system is low cost and easy to use. The customer needs only Internet access; neither extra hardware nor software needs to be installed.

1.2 The quest for a nation-wide authentication infrastructure

Though the PIN-TAN-system works successfully, it requires an initial contact when the account is opened. Thus, a nation-wide authentication infrastructure would be helpful. Therefore, most German banks joined the German Signature Alliance (see [Büger, Esslinger, Koy]) founded in 2003 and discussed how a nation-wide authentication infrastructure could be implemented. Such an infrastructure should be based on public key cryptography and work under the legal frame of the European Signature Directive.

Deutsche Bank was one of the fore-runners in the alliance and offered a signature card “dbSignaturCard” in October 2003, which could be used for online banking as well as other applications or securing Emails.

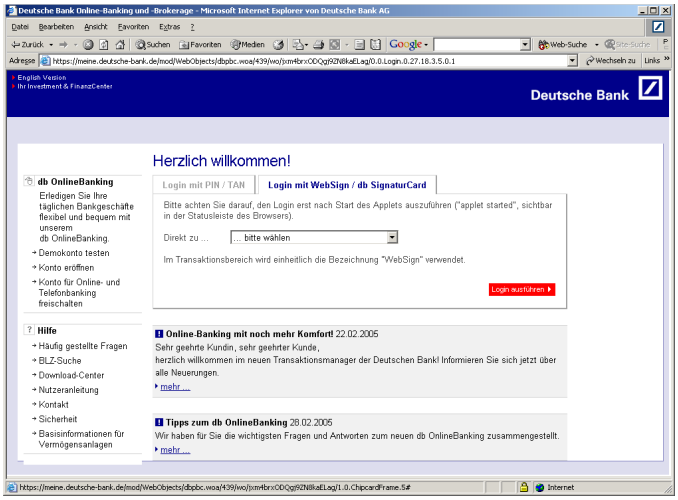

Figure 2: Usage of dbSignaturCard in online banking

The dbSignaturCard has successfully proved evidence that it is possible to combine bank cards, public key cryptography and online banking. The demand for signature cards, however, is still small. This was not unexpected: There was no killer application for signature cards. Usage of electronic signatures required new hardware (card reader). In online banking, existing systems (PIN-TAN) work quite well. In E-government, the number of use cases is still small. A key finding of the Signature Alliance was to emphasize the importance of the business case. When a document is signed electronically, German signature law states the recipient of a document has the right to ask for the status of the underlying certificate at no cost. In addition, the provider has to store and deliver this information for many years (in some cases up to 30 years). This raises the cost for the provider, which he will charge to the cardholder when issuing the card. The benefit, however, is with the application provider (who can streamline his processes), while the cardholder stays with the cost. No wonder that the demand for signature cards stayed small.

In this situation the introduction of the German electronic citizen card is promising: The card will be issued by the federal government and is mandatory to all citizens. Some questions, however, remain open: How many years will it take before a significant number of citizens are equipped with the new eID? Will there be inexpensive contactless card-readers? Will the identification function of the eID be sufficient to fulfil the legal requirements to open a bank account? If a qualified signature is still needed, how difficult and costly will it be to upgrade the eID?

2 Possible usage of eID in online banking

There are two scenarios in which electronic citizen cards can be used: First, a new customer can be identified with the eID when the account is opened. Today, opening an account online is a difficult and expensive process. The second scenario is to use the eID as an alternative to PIN/TAN in online banking (like the dbSignaturCard). We will have a closer look at both cases:

2.1 Opening an account with an eID

From a bank's perspective, opening an account in the Internet is one of the most interesting use cases for an electronic citizen card. German law[1] states that the bank has to identify the person when opening an account. The money laundering law[2] describes the way the bank has to identify its customers: The identification may either be based on the (physical) ID card, the passport or a qualified electronic signature. For an online account, identification based on a physical ID card or passport is a complicated and expensive process: In this case, banks use the Postident[3] scheme, which means that the customer is identified at the local post office or by the postman. As long as the customer has not shown-up at the post office, the bank is not allowed to open the account. The cost (about 5-8 EUR per identification due to company information[4]) is charged to the bank. In the context of the Internet, this identification scheme is a kind of workaround which is necessary since there is no online authentication.

1 [AO] § 154 AO (2) Niemand darf auf einen falschen oder erdichteten Namen für sich oder einen Dritten ein Konto errichten oder Buchungen vornehmen lassen, Wertsachen (Geld, Wertpapiere, Kostbarkeiten) in Verwahrung geben oder verpfänden oder sich ein Schließfach geben lassen.

2 [GwG] § 1 Abs. 5 GwG Identifizieren im Sinne dieses Gesetzes ist das Feststellen des Namens aufgrund eines gültigen Personalausweises oder Reisepasses sowie des Geburtsdatums, des Geburtsortes, der Staatsangehörigkeit und der Anschrift, soweit sie darin enthalten sind, und das Feststellen von Art, Nummer und ausstellender Behörde des amtlichen Ausweises. Die Identifizierung kann auch anhand einer qualifizierten elektronischen Signatur im Sinne von § 2 Nr. 3 des Signaturgesetzes erfolgen.

3 Postident-Verfahren: Identification either at the post office or by the postman when the post is delivered.

4 Based on company data Deutsche Post AG, July 2008