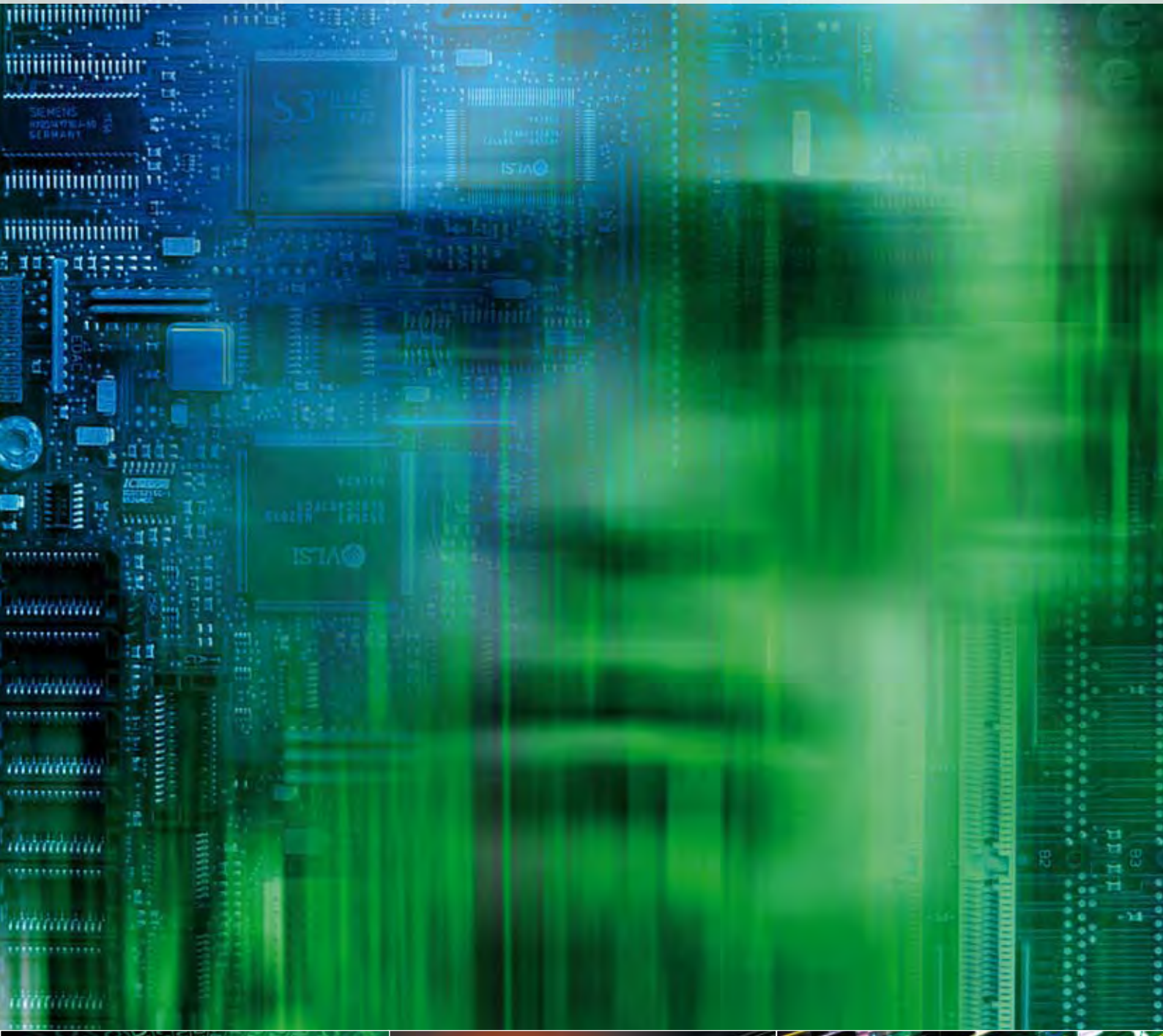
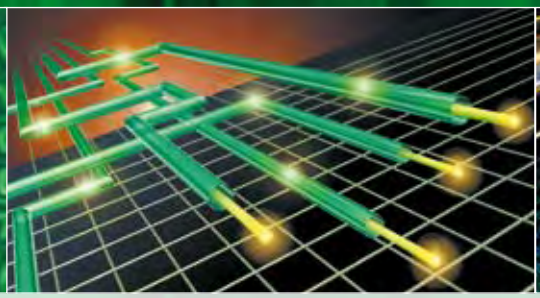
CRYPTOMAGAZINE

HAGELIN-CRYPTOS
CRYPTO AG

For the customers of Crypto AG, Switzerland

1 ▪ 2009





THE WORLD OF CRYPTOGRAPHY

Dear Reader

Cryptography exerts a special fascination on people no matter what the time period involved, past, present or future. People protect their confidential information from prying eyes today, just as they always have. The technology is the only thing that has changed over the years.

There is something in our corporate history to admire every day. We can still be enthusiastic today about the ingenious techniques employed in antiquated products. "Milestones in the Company History of Crypto AG" is a new series of articles that transports us into the past and gives us interesting insights into the history of information security at our company (page 12).

The future has already begun with quantum cryptography. But what significance will this branch of science have for us? Many questions are still unanswered. The significance and benefits of this new field of knowledge are not yet completely clear. Please turn to page 19 to read more.

"Corporate Identity and Corporate Design" is the name of a seminar recently conducted for our employees. It demonstrated again that our corporate values must be practiced and backed by every employee. Security Competency – Innovation – A Commitment to Service. These three principles are more than mere catchwords. They are our contribution to partnerships, now and in the future, that allow us to offer customary values such as security, constancy and anonymity in issues of information security.

I wish you interesting and absorbing reading.

Giuliano Otth

President and Chief Executive Officer

IMPRINT

Published three times a year **Print run** 6000 (German, English, French, Spanish, Russian, Arabic) **Publisher** Crypto AG, P.O. Box 460, 6301 Zug (Switzerland), www.crypto.ch **Editor-in-chief** Gabriela Hofmann, Crypto AG, Tel. +41 41 749 77 81, Fax +41 41 741 22 72, E-mail gabriela.hofmann@crypto.ch **Design/ Typesetting** illugraphic, Sonnhalde 3, 6332 Hagendorn (Switzerland), www.illugraphic.ch **Translation** Apostroph AG, Töpferstrasse 5, P.O. Box, 6000 Lucerne 6 (Switzerland), www.apostroph.ch **Printing** Ennetsee AG, Bösch 35, 6331 Hünenberg (Switzerland) **Reproduction** Free of charge with the consent of the editorial office, courtesy copies requested.

Illustrations Crypto: p. 2, 8, 13, 14, 15 • Fotosearch: cover, p. 4 • Getty: p. 18 • illugraphic: p. 6 • Imagepoint: cover, p. 4, 10, 15, 16, 18, 22 • Kursiv: cover • Roger Casper: p. 11 • Shutterstock: cover, p. 5, 19, 21

DANGERS AND THREATS FOR MODERN COMMUNICATION

FROM SPY TO CYBER HACKER

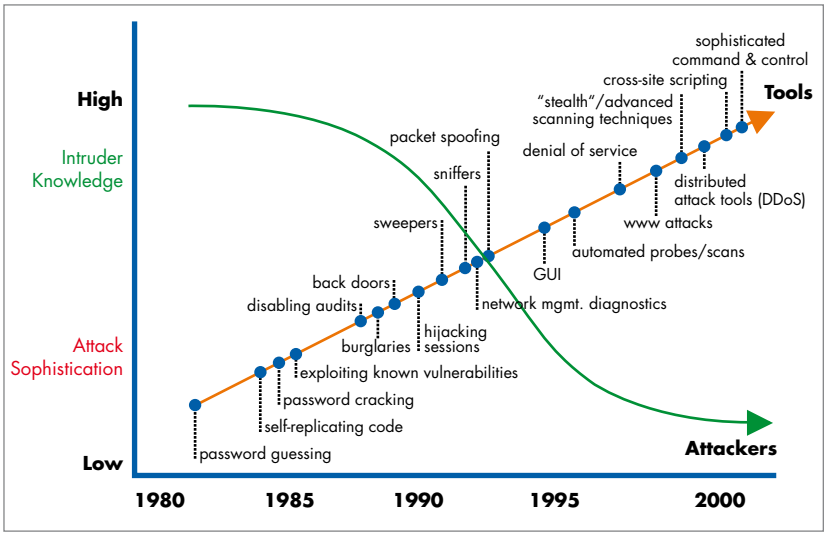
The world of threats and dangers changes so rapidly. Spies are the figures that kept the world in suspense during the Cold War whereas today, the big threats are mainly in modern communications and on the Internet. Our dependencies on means of communication such as satellites, Internet, phone, GSM and the like have grown enormously. It seems business can no longer even function without these tools.

By Philipp Birrer, Marketing Manager

Many economic sectors depend heavily on a well-functioning international global network for the exchange of information. These communication networks are enormously important for governments in particular. After all, they have to monitor disasters, check the availability of resources and patrol national borders. The reliability of these networks is also crucial to tracking hazardous materials and to carrying out surveillance and monitoring at sporting and political events. For instance, precise weather forecasts would be impossible today without satellite communications, computer networks and the Internet. Any inaccuracy could greatly influence and disrupt agriculture, aviation and global logistics. There is no longer any escape for us from this dependency; we are too deeply networked.

The changing face of hackers

Just as threats and dangers have changed over the years so too have the characteristics of the individuals responsible for them. In the early days, Internet hackers were fixated on feeding defective programs into the networks to force their collapse. It was a game for them. The people involved had to have excellent computer expertise. The hackers of the 21st century have rudimentary training and focus mainly on illicitly acquiring sensitive information that promises a commercial gain of some kind. They are little more than modern thieves, to put it somewhat simply.



The types of attacks have changed over the decades. What began as a game of figuring out the password has given way today to the regular "hostile takeover" of an entire network. Even poorly trained individuals can now carry out dangerous attacks with the aid of ultra-modern software tools.[1]

A danger that affects us all

With the increased prevalence of communication over satellites and the Internet, anyone can be the victim of an attack. We have no choice but to address the issue of security in our exchange of information. E-banking, tax returns, payrolls and online purchases are just a few of the applications that affect and occupy individuals, companies and even governments in their daily handling of information. Can a person still feel completely safe without effective protection for sensitive and secret information and the exchange of that information? Danger and threat take on a new dimension in the global information network. You no longer see the attackers physically; the attacks are covert and invisible and can come through any conceivable channel. So, the answer to the above question is a definite "No". All of us have to think about ways of applying adequate means of resistance and/or defence.

Threats from malware – definition and ramifications

Internet use is intensifying and our dependency on it is steadily growing. As everyone can be affected by this danger, malware infection over the Internet is an essential issue. The term malware refers to all types of harmful programs that perform undesirable and harmful functions. In general, a user does not knowingly tolerate any harmful programs, so these damaging functions are usually disguised or the software runs in the background completely unnoticed. Malware distinguishes various types of computer viruses, computer worms, Trojan horses, backdoor attacks, denial of service attacks, spyware, scareware as well as diallers. What all of them

have in common is their intent to influence the system in unwanted ways, e.g. to siphon off information and forward it.

Attacks over the Internet are becoming increasingly sophisticated. A study by F-Secure revealed that as much malware was produced and disseminated in 2007 as over the previous two decades. A single network access to the Internet suffices to make a system vulnerable to attack and in danger of infection. Defective software packages in themselves may pose vulnerability for undesired attacks and are not correctible again until updates (patches) are issued for them. Once a weak flank is found, the hackers exploit it to launch a cyber attack.

These attacks against banks, institutions, organisations and others are aimed at systematically collecting confidential information on corresponding servers. Following a cyber attack in 2007, the Pentagon in Washington had to disconnect 1500 computers from the Internet, including the attacked mail servers. In August 2008, unknown hackers copied all the customer data, including all credit card details, of over eight million people from a database of the Best Western Hotel Group. These stories and attacks are becoming more and more prevalent because companies are using the Internet in increasing numbers. These kinds of threats should be taken seriously. A number of precautions are mandatory on various fronts to meet the challenges of the 21st century. Besides administrative practices and processes, training, and the sensitisation of employees, technical steps also have to be taken to protect sensitive data and avert danger. One thing is clear from the current situation: we cannot do without communications over computer networks today nor will we be able to in the future.

Sources:

[1] Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues; Howard F. Lipson, CERT Coordination Centre; Special Report CMU/SEI-2002-SR-009.

F-Secure Corporation, Helsinki, Finland; www.f-secure.com.

SECURITY FROM A PHILOSOPHICAL PERSPECTIVE

"The only security we have is that nothing is secure. Not even security."
Joachim Ringelnatz (1883 – 1934), German writer, cabaret artist, painter

By Gabriela Hofmann, Corporate Editor, and Dr. Silvan Frik, Head of Marketing Services

Definition of security

Security is a relative concept. It can be seen as the probability of defined potential damage not occurring under defined circumstances.

Or put another way, security is a state free of unreasonable risks that exists for a certain period, in a certain environment or under certain conditions. The term can also refer to an individual, to other forms of life, to non-living real objects or systems (and abstract objects).

Security is a reality as well as a perception. The two may not be exact equivalents, but are extremely closely related in general parlance. Real security is a mathematical variable based on the possibility of different risks and the effectiveness of different countermeasures. Perceived security is based not on possibilities or mathematical calculations but on how people react psychologically to risks and countermeasures.

Various types of security

The security of an individual or an entire group of the population can be subdivided into physical and economic or social security. Physical security means direct physical integrity and freedom from threat. Economic security means stably guaranteeing a livelihood by material and financial means, both of which act as hedges against the future for an individual or a community (collective). Collective security comes to bear especially in conflict situations. This does not mean one side's security is increased at the expense of another's, but rather that joint actions are devised for ensuring the security of both sides. Common sense and experience on the part of individuals and the community are needed to assess situations correctly.

Is there such a thing as absolute security?

Security does not mean that adverse effects are ruled out completely, simply that they are rendered sufficiently improbable. Security concepts must be devised and implemented to minimise final uncertainties yet again and achieve a state of security as close to perfect as possible. Security measures are deemed successful if they help to prevent or render expected or unexpected adverse effects as improbable as possible.

Security in ICT

In technical structures or objects, security refers to a state of operation free from disruption and dangers. A key aspect of security in this sense is how this state is defined or what degree of (un)certainty is acceptable for the use of technical functions. If no danger occurs during a potential disruption, the term reliability is generally used instead of security. The interplay of various mechanisms is required especially for technical security, but a single weak link in the chain is all that is required to allow an internal or external attack to occur.

In everyday operations, risks and security can be addressed with different approaches. In a viable ICT organisation with a performance mandate, resources and competencies, attention is paid to necessary system management, authorisations and password policies. A well-functioning auditing system is equally essential for monitoring and regulating outside attacks on networks and servers as well as the use of network filters.

Meaning of security in cryptology

Cryptographic techniques are integral parts of most security functions

in ICT systems today. They provide the basis for authentication processes and help to ensure the confidentiality and integrity of communications. A major condition for the secure use of these techniques is a high-quality source for random numbers, e.g. for the generation of cryptographic keys. Modern cryptographic processes have been adapted to the way computers work. Instead of dealing with letters, numbers and special characters, they work with individual bits. This increases the number of possible states and allows the processing of non-text data.

As matters stand today, encryption keys generated by electronic means cannot be cracked in a useful time with or without knowledge of the original text even with the greatest conceivable use of computers. According to scientific literature, security is guaranteed with a key 80 bits or longer. 80 bits means 1.2×10^{24} key variations, which corresponds to 1,200,000,000,000,000,000,000,000 variations. Assuming that one computer can conduct 10^9 tests (i.e. one billion) in one second, 1,000 interlinked computers would need more than 19,000 years to find the key. As the key length increases or further elements of the security architecture come into play, this value is increased exponentially into the incalculable range, which means attacks are no longer worthwhile. In this process, it is also important to pay the necessary attention to the architecture of algorithm and key management. Key length is not the only factor that determines the security of an encryption system. ■

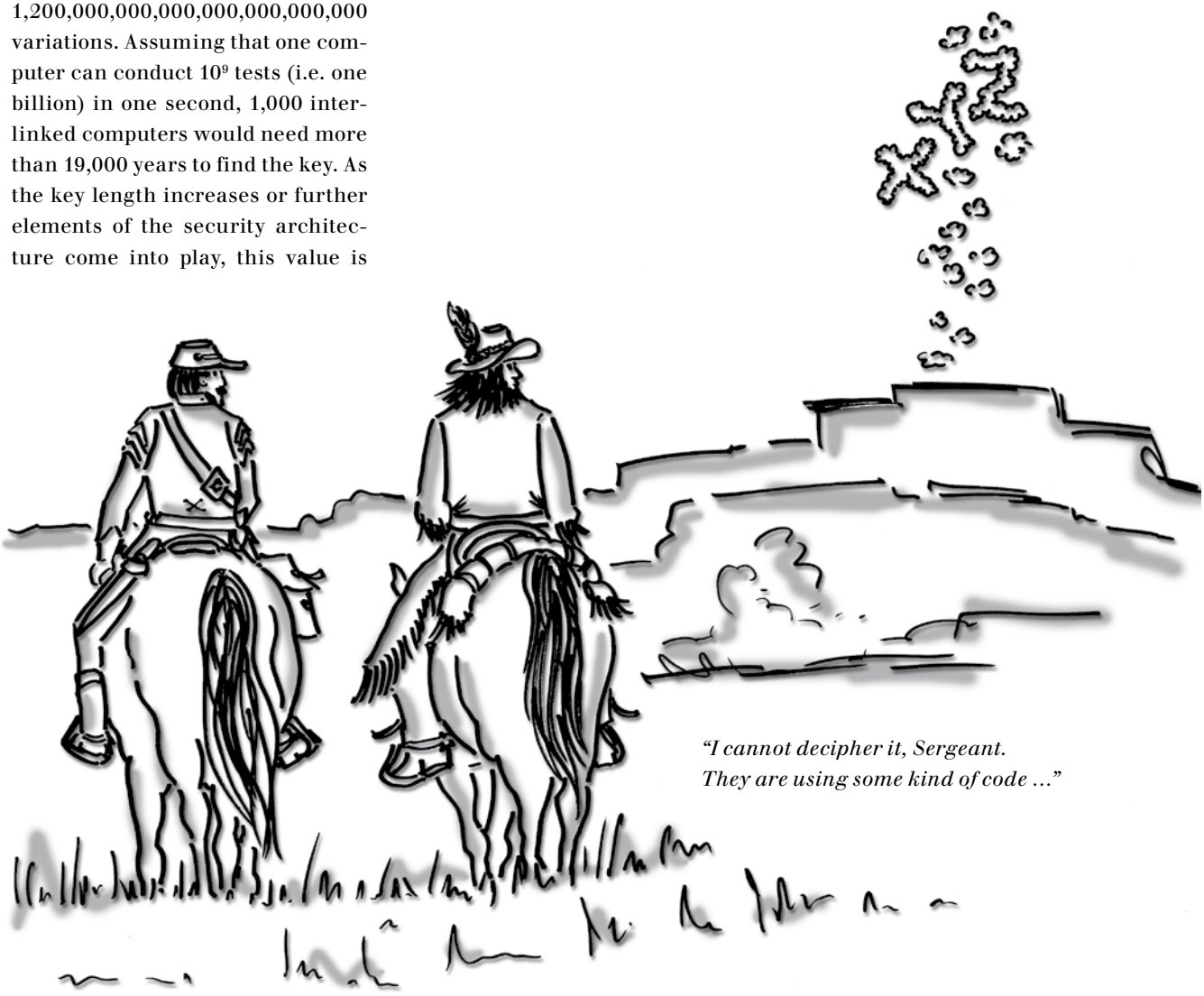
Sources:
10 Thesen zu Risiko und Sicherheit im IT Bereich [10 Theses on Risk and Security in IT], Urs Meile, 2001, www.id.ethz.ch/services/

Kryptologie-Grundlagen [Basics of Cryptology], www.virtualuniversity.ch

Bruce Schneier; The Psychology of Security, January 21, 2008; Essay-155

Enzyklopädie der Wirtschaftsinformatik [Encyclopaedia of Business Informatics], online encyclopaedia, www.oldenbourg.de

Free University of Berlin, Lutz Suhrbier, Sicherheit mit XML [Security with XML], 2006



"I cannot decipher it, Sergeant. They are using some kind of code …"

THE WORLD OF A SECURITY MANAGER

COMPLEX AT FIRST GLANCE – QUITE EASY AT SECOND

Put simply, information security in the network is what makes the network usable in the first place. Consequently, encryption systems in today's dynamic ICT environment can no longer be static elements. But how is a security manager supposed to keep the administration of complex dynamic networks firmly in hand? The answer: with systematic security management that reduces complex functions to simple procedures. It is all easier than it appears at first glance. That becomes obvious when one approaches the matter didactically.

By Dr. Rudolf Meier, Publicist

Information security systems are increasingly viewed as integral to ICT, even in cases involving applications like radio or satellite that were once subject to special treatment. A major reason is that even different applications can be protected at the same high level with modern encryption technology. The primary factor for availability in daily operations, however, is that the necessary administrative actions in security management (e.g. the formation/changing of cryptographic groups or key changes) are taken free of error and can be implemented as simultaneously as possible in the targeted area of the network.

Security management has a split image traditionally. Although considered enormously important and operationally useful, it involves intervening in the cryptography of a possibly complex security system, which may create headaches for users. Life does not have to be like that. Of course, the necessary care and commitment have to be exercised in management, but in the end, user friendliness is largely what determines the value of a concept.

What characterises an optimum user-friendly security management approach?

The objective of security management is to convey a readily interpretable overview of all encryption functions and operations in the network while providing the right means (i.e. effective actions) of handling all possible incidences.

Complexity has to be reduced to achieve this level of quality. This entails primarily automated procedures that avoid errors, logically traceable links and a logical and understandable user interface. Simplicity is ultimately what determines security and trust in these procedures.

The concept from Crypto AG also keeps in mind the often-cited human factor. Experience shows that available potential is only used if it can be conveyed understandably and lastingly. It is also advantageous if the concept is taught in an efficient and concise manner.

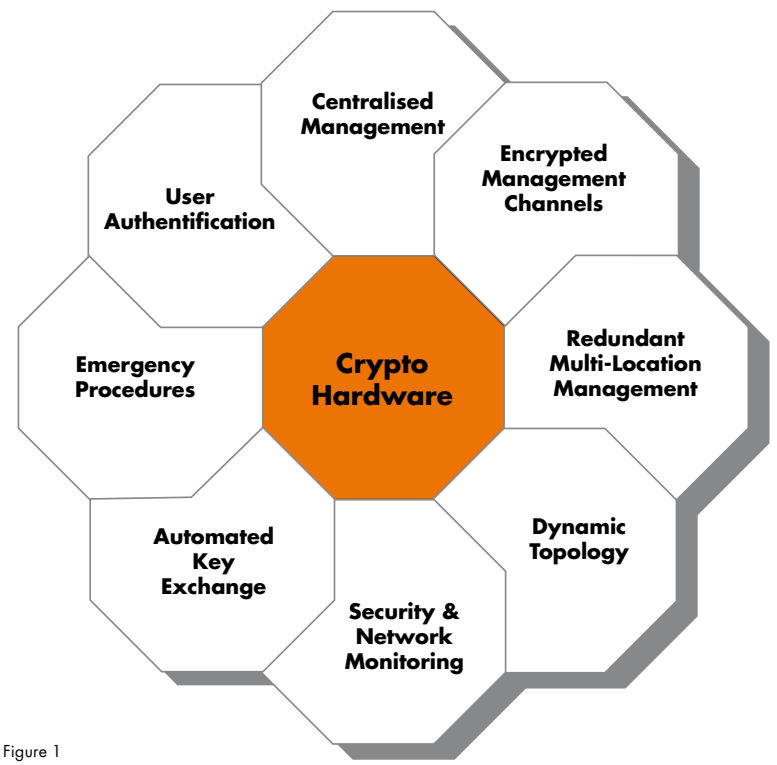


Figure 1

As a series of operational tasks, security management is an issue long before it comes time to configure and operate a system. Even when equipment is purchased,

proof should be given that it is designed with the potential for meeting the user's security policy requirements. As information is required at different levels, Crypto AG uses a three-tier concept for depicting security management potential:

- As an overview, a graphical model to show the core functions (see Figure 1).
- A brief and easy-to-understand description of the core functions in each segment to help comprehend the settings, processes and procedures that can be implemented with it (in various printed and electronic documents).
- In-depth documentation of technical details enabling the individualised use of all functions (data sheets, application notes, white papers, etc.).

The Crypto Academy also conducts customer-specific training and refresher courses for practical training in security management.

Brief description of core functions

Of course, there is not sufficient space in a magazine article to cover the entire potential of security management from Crypto AG. With this brief description of the core functions, we are merely providing an initial overview of the various sub-areas (in-depth information is available from Crypto AG). Except for the Crypto hardware, the central element that lays the technological and mathematical groundwork for all cryptographic processes, all functions can be assigned highly specific uses for individual users to ensure maximum support for the individual security policy.

Crypto hardware

All cryptographic processes are run in a separate hardware security module, from cryptographic processes for payload encryption to procedures carried out in the Security Management Centre (SMC). As each encryption unit has the same security module as the SMC, encrypted data is always exchanged on the same cryptographic basis (with a random-number generator). In this approach, security data (algorithms, keys, access data, etc.) is never accessible in unencrypted form in any of the management procedures.

Centralised management

All encryption units integrated in the network must be involved in the management procedures, regardless of the size or complexity of the network. Logically enough, administration is therefore carried out over a central authority system, the Security Management Centre with backup system. All units can be administered from this centre concurrently. The user's security policy and the ambient conditions (e.g. applications or network size) of the work scenario determine whether the online or offline process is used. The Security Management Centre is a convenient support tool for both concepts (see Figure 2).

Encrypted management channels

Symmetric encryption processes require secure key distribution to the individual encryption units. If you use the same strong basic cryptography as for payload encryption, this procedure can be done online with no security problems at all. No specific operational problems arise and no special procedures are necessary. One individual key per management channel for each encryption unit opens the way to completely individualised administration. In offline mode, the channel comprises SDC Security Data Carriers with data that is likewise encrypted (also refer to Figure 2).

Redundant multi-location management

With multi-location management, larger networks can be divided into flexible sub-networks, which can then be administered independently and more easily. It could be tactically advantageous, for example, to administer front-office areas from nearby or hierarchies independently of each other. Redundancy is increased at the same time. A lost site can be replaced immediately. Intensive round-the-clock operation also allows a better distribution of capacity utilisation. With the shared database, the current status of all units can be retrieved from any site at any time.

Dynamic topology

The assignment of units to groups or hierarchies (i.e. the logical topology) can be flexibly and dynamically adapted to the ambient requirements and tracked from a central point. The security policy can also be changed at any time. In crises, entire networks or parts of them can be given new priorities at short notice with no interruption of operations. This function may even be a mobile one depending on the application.

Security and network monitoring

Monitoring gives the security manager a complete overview of all network states with respect to security parameters and network settings of the encryption units, so he can respond immediately and correctly to any problems. He can request information of possible value for maintenance or audits from the unit logs on past processes. Depending

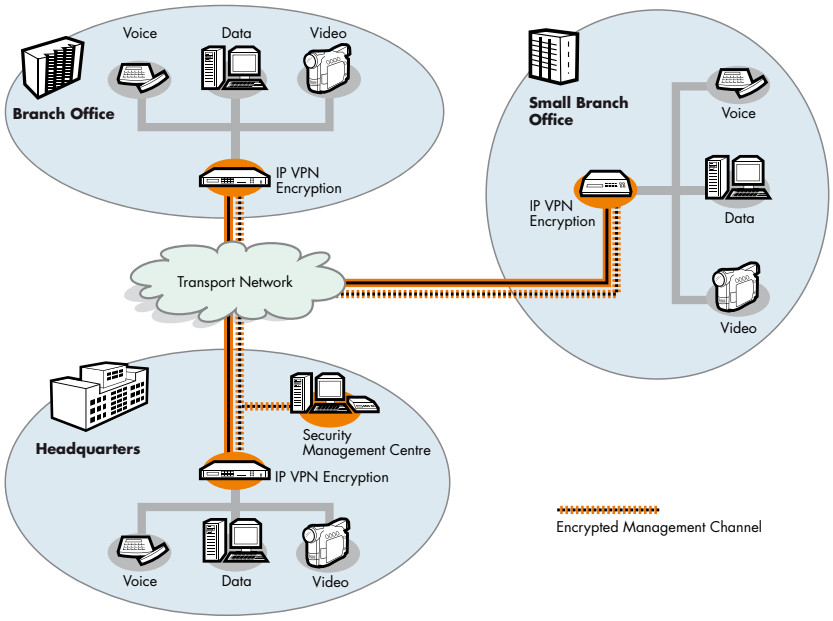


Figure 2

In online security data distribution, separate encrypted management channels are set up by the network from the SMC to all units, complete with keys of the same strength as for payload encryption. The encryption output of the units is not impaired.

on the security policy in force, the roles of security management and network management (as regards the encryption units) can be performed separately or jointly. This flexibility may be advantageous, for example, if a network provider operates an encryption solution for its customers.

Automated key exchange

The best practice quasi-standard requires a periodic replacement of the unit keys/master unit keys (new session keys are generated each time anyway). This key change is simple and automated and is accomplished without interrupting operations. Programmability enables optimum timing for the use of load/network presence. The multi-key process automatically reconciles any time differences in key installation, even in offline mode with its larger time shifts. All procedures are automatically logged, allowing subsequent verification of who took what action.

Emergency procedures

A threatened or already compromised encryption device can pose a serious risk to the user. These problems can be greatly mitigated by having procedures that are as simple as possible. Emergency procedures, for example, allow the user to delete all cryptographic data immediately at the simple press of a button (even without a power supply) or to exclude a certain unit instantly from the cryptography of a network with an online command. Secure operations can be resumed quickly thanks to a central recovery procedure.

User authentication

Authentication can be based on persons or roles at each unit and individually set via the SMC, in offline or online mode. This feature reliably excludes unauthorised parties. Identity-based procedures can be recorded with logs and evaluated for audits. With the block function, each unit can be shut down securely for a shorter or longer period, for example for interim storage or for transport.

Security as an entity

Encryption systems are always operated in a user's own specific scenario, so the associated security management has to support the individual security policy. It is therefore preferable to implement security in an ICT environment individually as a project entity. An experienced supplier can include the aspect of security management early on in a project, with a focus on its benefits. This inclusion substantially increases efficiency for project realisation and trust in security.

SECURITY INFORMATION AND EVENT MANAGEMENT

INCREASING AVAILABILITY AND SECURITY WITH INTELLIGENT CENTRALISED LOG MANAGEMENT

By Gabriela Hofmann, Corporate Editor

In the realm of ICT, companies are faced with increasingly diverse networked challenges. Not only is it necessary to ward off external attacks from hackers and phishing, but internal security violations also need to be tracked. A company's infrastructures are also subject to a constant challenge from statutory regulations on data protection. These tasks need to be managed in less and less time, with shrinking budgets and a minimum of staff resources.

In view of the increasingly complex network and server structures, smooth operation of ICT is becoming ever more demanding. Each device in a company generates hundreds of pieces of log information daily which need to be gathered and evaluated. A log message is created for e.g. each log-on, each PC crash and each attempt to access unauthorised data. The real challenge for those responsible for ICT now consists of filtering out the operational information of importance for security from the huge amount of data in the ICT systems, database servers, firewalls and web servers, interpreting it correctly and, if necessary, implementing the relevant measures.

INTERVIEW WITH ROGER CASPAR, INFOGUARD AG

What can companies do in order to cope with the constantly increasing flood of information in ICT?

The messages, in other words the log data of the individual ICT and software components, play a crucial role in the smooth operation of ICT systems both in the operational and security fields. They supply important information about the status of the infrastructure and help in making sustained improvements to the availability and also the reliability and security of ICT systems. The flood of data can be processed more efficiently with an intelligent log management system.

What does intelligent log management mean to you?

All or at least the important systems in a company, such as routers, server and proxy systems, and systems which are crucial for security, such as firewalls, IDS and anti-virus systems, need to send their log information to a central database. These messages will be gathered, analysed and evaluated there using an appropriate system. The data gathered centrally needs to be linked and displayed with the risk assessment from the relevant systems, so that a meaningful evaluation can take place. It is important that as many systems as possible are supported by the selected log management system, with particular attention given to a company's critical systems. As a minimum, servers, network components and security components such as gateways should be integrated in and supported by a log management system.

What purpose does a log management system serve for a company from an operational viewpoint?

The benefit of a centralised log management system in the operational field consists of the fact that faults can be recognised in good time, reaction times are short and so system failures can be prevented or minimised. In addition, there are also benefits in relation to security.

About the interviewee

Roger Caspar is Senior Security Consultant at InfoGuard AG and for his own company appsphere GmbH. As a graduate in computer science and Master of Advanced Studies in Software Engineering, he can look back on over 15 years of international experience in the information technology field. He worked for eight years as an IT security officer for Bluewin/Swisscom Fixnet, the largest Swiss Internet service provider. His specialist areas are the development of security concepts, definition of application architectures, design of security information and event management systems and integration of security solutions, and the implementation of security audits in web applications.

A company's most common compliance requirements can be supported. In addition, many solutions offer report models for evaluation of events at the level of company management.

What might happen if a company does not have a centralised log management system?

If log data is not gathered centrally, it is harder for those responsible for ICT to monitor critical messages in the enormous flood of data. In addition, it is not possible to correlate the messages from different systems with one another. Resources are then often not allocated to the critical messages from important systems. This results in important information from critical systems being noticed too late. A log management system reports performance or resource bottlenecks in the system which might lead to breakdowns at some future point. This is even more important if there are service level agreements, in other words a contractual service arrangement with an external company. Network and system problems and breakdowns could present a breach of contract and quickly lead to high costs.

How important is the preparation for the evaluation of a log management system?

Correct preparation is immensely important. The company's needs must be clarified before the evaluation so that the best solution can be found.

If the following six points are defined, the result is a system where the benefits will far exceed the costs, even for smaller businesses. These are:

- What aim do you want to achieve with the log management system? Does this relate more to the operational realm or the security realm?
- Are there compliance requirements which have to be fulfilled?
- Which event sources need to be integrated and are all relevant systems included?
- How long should data be stored?
- How is the log data to be analysed and evaluated, e.g. should this be done in real time or only used for reports?
- Are the necessary resources, skills and processes available?

What do you perceive as the limits of this kind of system?

There are limits in two areas. First, despite a central system, there is still a need for personnel and organisational resources to evaluate the events. Although support is provided for evaluating the entries, there is still manual processing required. Second, a log management system reaches its limits if very specific systems and applications, e.g. SAP, CRM, are to be integrated. A log management system is more appropriate for systems and networks. In these cases solutions specific to the applications may be better suited for this task in certain circumstances.

Thank you very much for your comments.

MILESTONES IN THE HISTORY OF THE COMPANY PART 1: THE 1950S

ENCRYPTION USING MECHANICAL "CALCULATORS"

Long before Boris Hagelin founded his Crypto AG in Switzerland in 1952 he had already built mechanical cipher devices in Sweden. These functioned like mechanical calculators in principle, only that they deliberately calculated "wrong" – meaning that they swapped letters in a defined irregular pattern. The first article in our series on the milestones in company history investigates how Boris Hagelin further developed his encryption idea – in particular the ingenious "C calculating drum" – ensuring Crypto AG pioneer status over decades.

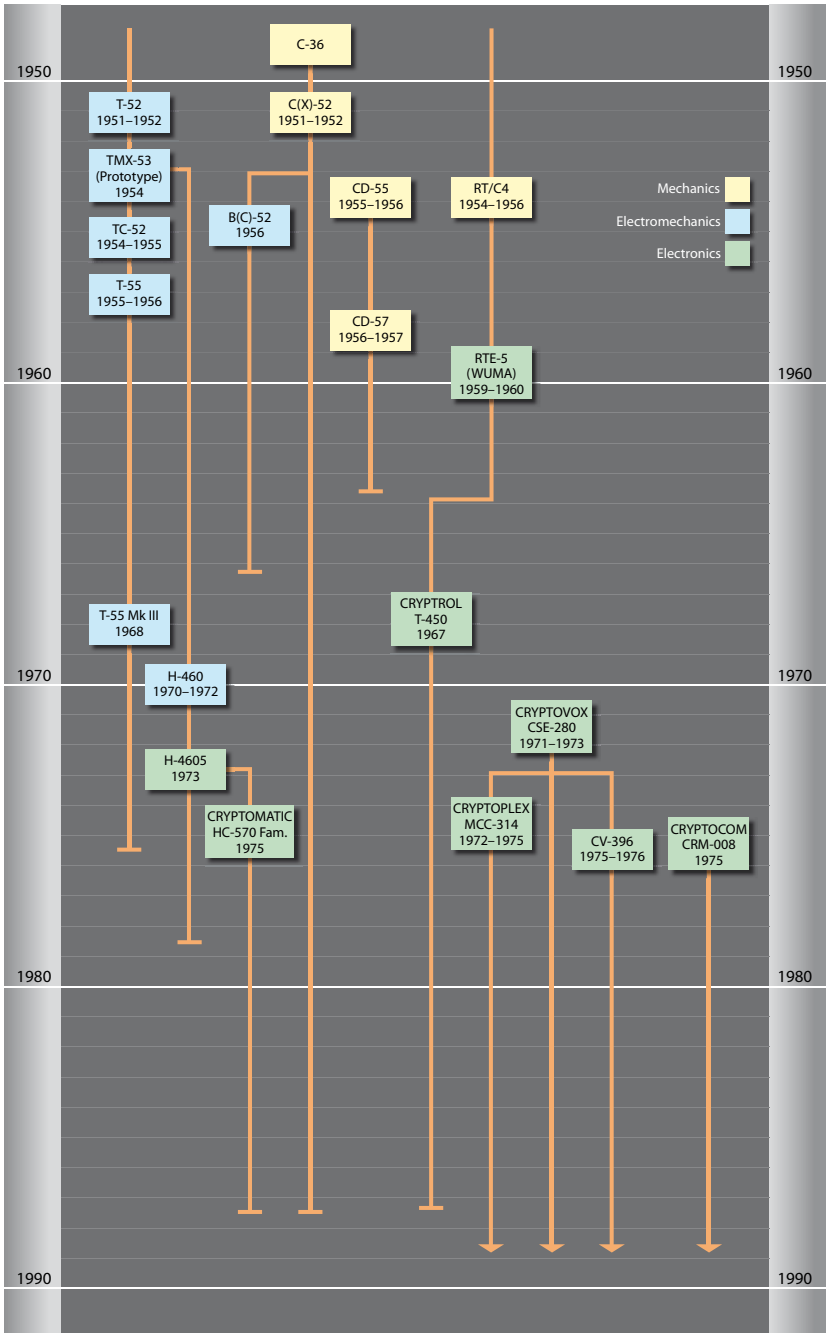
By Dr. Rudolf Meier, Publicist

At the beginning of the 1950s, Boris Hagelin came to Switzerland from Sweden and resumed his occupation as a designer of cipher devices. The first device produced in Switzerland was the C-52 which sold very successfully (in accordance with tradition, he always chose the year of construction as the type designation). It was a further development of his C-36 which he had sold to numerous countries before the war and under licence (type M 209) to the US armed forces. During the fifties, numerous additional models arose from the structural components of the C-36 at Crypto AG. It is therefore worthwhile taking a quick look at the basic principle of the mechanical encryption of that era.

Mechanical encryption is based on what is known as the Caesar cipher: the individual letters in the letter sequence are exchanged consecutively, i.e. replaced by other letters according to a particular key. The sender and receiver of a message encrypted in this way both use the same number as the key (symmetrical encryption).

Because a short key which remains unchanged could easily be derived from the ciphertext (there were refined methods for doing this even early on, especially frequency statistics), a key needs to be long and must not display any regularities. The aim was therefore to achieve long keys (also known as key

Products – Crypto AG's family tree



periods) by means of a mechanical calculator.

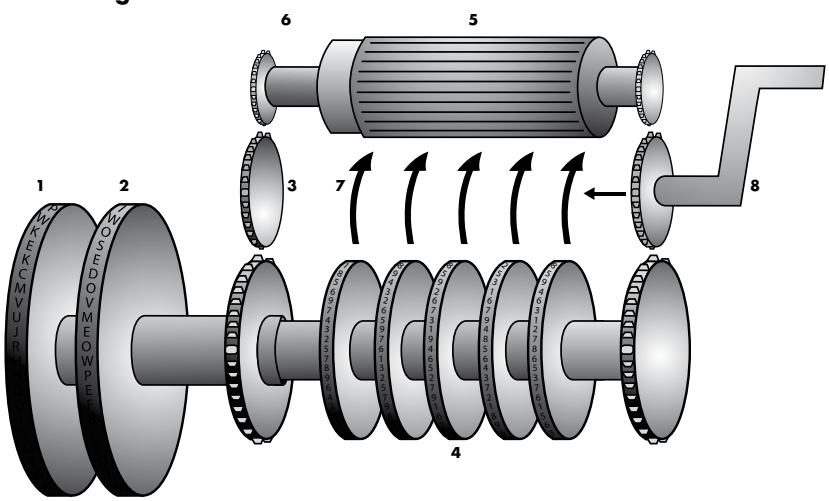
The mechanisms used by Boris Hagelin were extremely complicated, so we shall only look at the most important principles. Looked at as a black box, a device of this kind has two alphabet wheels or type wheels for input and output of text. The two type wheels sit directly next to one another, secured on the internal axle and the hollow axle. The cleartext is set on the first type wheel (input). For each cleartext letter, the calculation or encryption mechanism now "automatically" twists the second type wheel by the appropriate number of steps in accordance with the correct key sequence and displays the encrypted value. If the "output type wheel" is made as a daisy wheel, the result is obtained on a printing strip, which is obviously very useful for deciphering. If the sequence of type on the wheels is not arranged alphabetically but randomly or this is changed from time to time, the ciphering quality is increased.

The photographs of the C-36 show the most important elements of the cipher device: key wheels with letters for setting the key word (4) for the start of the key periods (the key wheels possess adjustable movable pins which operate the calculation drum by rotation via the control lever), gear elements (8) and the "C calculation drum" (5) behind. The latter is what is ingenious about this device because it transforms the control impulses of the key wheels into variable step switch impulses by means of the axial rods and riders directly and transfers them to the output wheel on the concentric axle (all in a single mechanical process). The C-36 already had a built-in strip printer.

Operation of the device is very simple. The basic key (starting position) must be set on the five key wheels – that is, a particular sequence of five letters. Then the first letters to be encrypted are set on the type wheel, the handle is turned once and the first encrypted letters appear on the output wheel. Then the next letters are set on the type wheel, the handle turned again and so on.*

The C-52 manufactured in Switzerland by Crypto AG displayed numerous small improvements in comparison with the C-36 (e.g. six key wheels) and served as a platform for the continual functional expansion of new models. A big step forwards was made in particular by the development of a base for the keys and an electrical drive system (BC-52). The C-52 could be placed on this and was therefore much more convenient to operate and the speed of encryption was increased. However, the BC-52 was definitely no longer a pocket device. The inclusion of two "parallel" strip printers, one each for the input and output text, was also of great importance in practice.

Block diagram



1 Cleartext type wheel

2 Ciphertext type wheel on hollow axle

3 Adjusting mechanism for ciphertext type wheel

4 Key wheels with position transfer

5 Calculation drum

6 Result output (wheel rotation)

7 Control of calculation pins by key wheels

8 Crank handle for encryption process

Transfer mechanism (gear wheels) only schematic representation

Because the C devices had been intended for tactical use, Boris Hagelin looked for the opportunity of incorporating even more irregularity and therefore more variability/security into the key periods. This was achieved with the devices in the CX type series, in which the key wheel feed runs irregularly. At first a mathematical principle got in his way here, in that the C mechanism sometimes randomly and unintentionally produced period lengths which were too short, in other words which began from the beginning again too soon. However, with a great deal of technical effort he succeeded in guaranteeing minimal period lengths. Later on, the CX devices were given additional key wheels and a correspondingly enlarged calculation drum. The various CX types were sold successfully all over the world.

The new dimension of telex encryption

In the 1950s the need for telex encryption arose. This required the cipher device to be inserted between the telex and the line so that the person writing only needed to write cleartext but the transmission down the line occurred encrypted. This only worked using electrical circuits (relays) and (in some cases) with punch tape systems. Types T-52 and T-55 were made in Zug, Switzerland, using the well-known C drum and key wheels. The T-52 still had to be converted from send to receive manually while the T-55 already operated without intermediate storage of the key symbols but directly connected the sender and receiver whose encryption units ran synchronously and could therefore be switched over automatically. The T types were able to operate along with telex devices from various manufacturers.

The One-Time Pad system

If punch tape is used for the input, the very secure One-Time Pad concept can be used in which each message uses its own new key sequence consisting of random numbers. This was of great interest to clients with high security requirements.

In this case the punch tape drives the C drum directly, without any key wheels. However, the random sequences had to be really random, for which Crypto AG developed its own high-quality random-number generators in accordance with the principle of the lottery number machines with "falling balls" which are familiar nowadays. These generators stamped the numbers produced directly onto punch tape, with the sender and receiver naturally having to use the same (duplicated) tape.


T-52


T-55

The CD-57 pocket machine

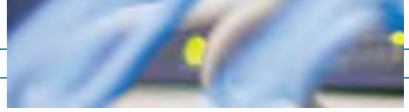
Because the C types had become increasingly large, the desire for a "real" pocket version emerged amongst clients in the diplomatic service. This request was able to be fulfilled by making a miniature version of the rotor technology. The CD-57 could be operated single-handed using the thumb while the other hand remained free for making a note of the ciphertext or

deciphered text. However, the device had no printer and was not compatible with the CX machines already developed. Shortly before the beginning of miniaturisation due to electronics, this was another master stroke which met with great market success.

However, the emerging trend towards electronics could now be clearly seen, a trend which would influence the development of cryptography in the 1960s in a decisive way.

* For those interested in mathematics, the C-36 key wheels exhibit different divisions (operating positions) which do not possess any common factors: 17, 19, 21, 23, 25. This gives rise to a key period of 3,900,225 operations until the wheels return to the initial position – a unique degree of variability for those times! Added to this was that the axial pins which operate the calculation drum by means of the control lever could be set randomly for each key wheel, giving a further theoretical variability of 10^{29} possibilities. In later devices, up to 12 key wheels with higher divisions (25 to 47) came into use, which once more increased the key periods enormously.

CD-57



SERIES ON CRYPTO SERVICES (III)

ICT SECURITY REQUIRES COMPETENT PARTNERS FOR IMPLEMENTATION

The requirement for security systems to be implemented within a defined budget, on schedule and with full functionality is obvious. Implementation of the security aspect and therefore the security management system must be paid a great deal of attention in this process. Crypto AG gives security top priority when implementing projects in cooperation with our clients.

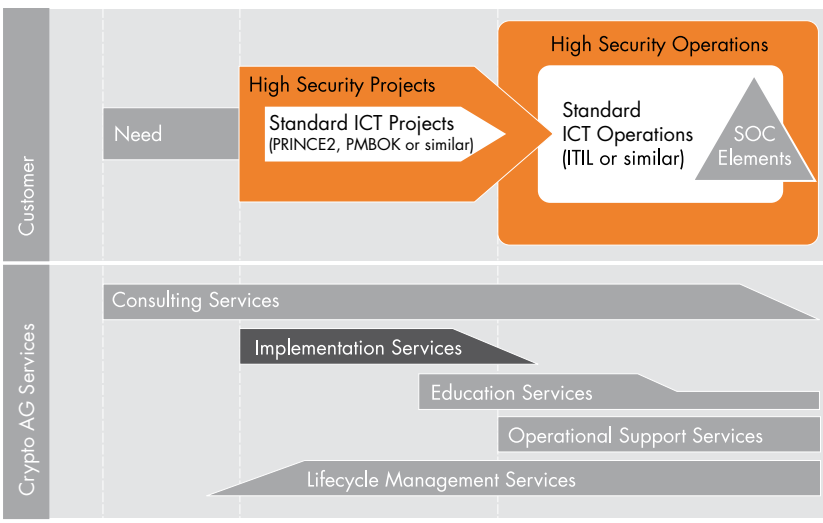
By Christof Eberle, Head of Customer Projects

In previous articles in this series it has already been mentioned that implementation of ICT systems is normally carried out according to standards applicable throughout the world (PRINCE2, PMBOX or similar). These standards are important and necessary but are not focused enough on the high security requirements of Crypto AG's clients.

Using our expertise and many years of experience in high-security projects, we have extended these "state-of-the-art" methodologies with tasks and procedures required for security and adapted them to differing client requirements.

Crypto AG has been implementing security solutions in the most varied client environments and scenarios for decades. This has led to the collection and further development of a large amount of knowledge and experience in this field.

To begin with encryption systems were offline, meaning that these did not need to be integrated in an infrastructure. Since the 1980s security systems increasingly came into use in which the security solutions were integrated into an existing communications system or one which still had to be developed.



Our competency covers the implementation and integration of comprehensive security systems for applications for military and civil authorities:

- secure radio systems in HF and VHF ranges
- secure network systems for line, fibre and directional radio applications
- secure messaging systems for radio, line, satellite and Internet applications

The design, preparation, installation and commissioning are all done from one source. The systems can be maintained for years to come if desired.

The key criteria

The technological challenge for these kinds of systems is to combine security, the connection to a wide range of communication channels, functional security and good operability, and easy management all under one roof. But the qualification of operating and maintenance personnel and their security-related workflows are also frequently key criteria for the successful implementation of a larger infrastructure project.

The "technology/people/processes" criteria differ in importance depending on each application.

Security should be given the highest priority when choosing partners for implementation. However, the other priorities of functionality, cost and implementation time should not be neglected (Figure 1).

Project implementation

The following sequence has emerged and proved itself as the best in practice. For more complex projects it is possible to repeat the sequence several times (see Figure 2).

SOC Element	Large IT Nets	MoFA Applications	Military Solutions
People/Processes	▪ Central management ▪ System operation and maintenance ▪ Maintaining operating personnel expertise throughout the period of operation	Training of periodically changing embassy personnel	For joint forces: ▪ Various, partially incompatible regulations and processes ▪ Many different interests of the individual member countries
Technology	▪ Networked, existing infrastructures and components undergoing rapid change (life cycle aspect) ▪ Network complexity	▪ Embassies distributed throughout the world result in challenges for dispatch, installation and maintenance due to time differences ▪ Highest security classification	▪ Differing proprietary, often incompatible infrastructures and systems already in existence ▪ Many non-uniform proprietary company standards ▪ Product and solution longevity ▪ Highest security classification

Figure 1

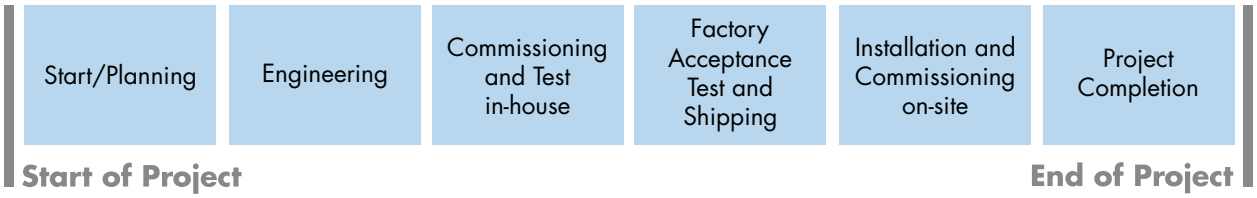


Figure 2

Start / planning
The client is familiar with the project aims, the bi-directional communication and the project organisation.
During the first phase of the project the project leader and all additional personnel from both sides are decided on. After this it is important to sort out the project aims and communication. At a kick-off meeting the project is planned and the project timetable with its milestones developed.

Engineering
The client is informed about the technical solution to the project and about the acceptance tests.
During the engineering phase the detailed design and acceptance procedure for the solution are developed and the project design review carried out with the client. The client gives his agreement to implement and accept the solution as described. After this the engineering of the solution can be started and the project defined in detail. The operational concepts are also developed during this phase. At the end of the engineering phase a security review is carried out in order to verify that all agreements and instructions related to security have been complied with.

Commissioning & test in-house
The client has the guarantee that the system has been developed and comprehensively tested.
The material for the solution is procured, partly assembled by Crypto AG, commissioned and comprehensively tested. This test system enables the first version of the system documentation to be produced and initial client training on the system to be carried out.

Factory acceptance and shipping
The client has tested whether the solution fulfils his requirements for security and functionality.
The client personally carries out a "Factory Acceptance Test" at Crypto AG. After this acceptance the material can be shipped.

Installation and commissioning
The client has the guarantee that the system was installed in such a way as to fulfil his security requirements and he will be capable of guaranteeing the operation of the solution.
The material supplied is installed and commissioned. A "Site Acceptance Test" is carried out at each installation site and the certificate for this signed. After all sites have been accepted, the operating handbook (as built documentation) can be produced. Training on the system and advice for operating the solution can now take place. Finally, a security review is carried out on the entire installed system. This verifies the correct implementation of all security targets.

The project leader – a success factor for successful project implementation
At the start of every project a project leader for the client and one for the supplier are named. These two are responsible for the smooth running of the project. The project must fulfil the agreed security and defined functionality in the required time and to the agreed costs. The two project leaders are the primary contacts in each of the organisations. They are each in charge of a project team which produces the required services in accordance with the agreed schedule and is made up of various specialists.

CORRECT RISK ASSESSMENT AT THE START OF THE PROJECT

The importance of the initial phases of putting a project into practice are often underestimated. In a representative study, the University of St. Gallen discovered that the greatest risk of project failure occurs due to mistakes at the start of the project.

The most important risk factors in IT projects are

- No defined project aims
- Imprecise specification of the IT solution
- No allocation or wrong personnel for project tasks
- Superficial project planning
- Unrealistic resource planning
- Badly defined responsibilities
- Inadequate communication

Source:
OPPORTUNITIES INSTEAD OF RISKS
Learning from mistakes and weaknesses for the sustained success of IT projects in public administration

Prof. Dr. Kuno Schedler and Alexandra Collm

University of St. Gallen, Switzerland, http://www.idt.unisg.ch

Project completion

The client has received the desired system and all his requirements – especially for security – have been met.

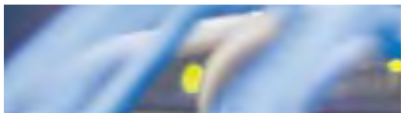
To complete the project, the final documentation is handed over to the client. After signing the "Final Acceptance Certificate" a project review is carried out with the client and Crypto AG.

System solution continuity

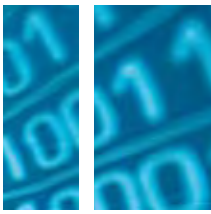
The processes described in this article ensure that the client is able to guarantee the operation of the security solution which has been implemented. The employees are capable of commissioning the solution, of guaranteeing operation and of ensuring maintenance.

Competent partners for ICT security

Security must be granted the highest priority during the implementation of a high-security project. Only during the next phase is attention given to the remaining standard project disciplines. In order to guarantee continuity in the project, planning, supply, installation and commissioning should all take place from a one-stop source. The partner selected for carrying out the project must have not only the theoretical knowledge but also practical experience in the implementation of high-security projects. The qualification of the operating and maintenance personnel and their security-related workflows must also be given attention as these are often key criteria for the successful implementation of a larger infrastructure project and for its sustainability.



QUANTUM CRYPTOGRAPHY: NO REVOLUTION IN SIGHT



"Good news" about the implementation of projects in quantum cryptography appears regularly in the media. Mostly also accompanied by negative statements about modern mathematical cryptography. What is to be made of this? Quantum physics is definitely an interesting field but in relation to practical security solutions, theory and practice still lie far apart – and are very unlikely to converge.

By Dr. Rudolf Meier, Publicist

Quantum physics is a scientific field which can attract a lot of research money nowadays. This is because it is assumed that this field of physics might one day put many technical processes on a new basis. Research groups mainly in the USA, Switzerland and Austria have been involved for several years with applying the principles of quantum physics to a new approach to encryption. The message given out primarily by these research circles is that quantum cryptography is the only physical and/or mathematical unbreakable encryption method.

Naturally, practice-oriented cryptographers and mathematicians are always interested in following all the relevant developments. But when it is claimed that all normal encryption algorithms can be broken with high-performance computers, something like unfair competition sets in because this statement is only valid when the necessary data processing capacity and time requirement are simply ignored! Laymen may be impressed by this, but not the experts.

Just a quick comment about the real situation: even a key with a length of 128 bits can supply 10^{38} key variations. This is a number with 38 zeros. What does this mean in terms of security? For example, if all computers in existence today were connected together and used only for the task of breaking a key of this kind, it would require millions of years to try all the variations one after another. If this seems unbelievable, the proof for it is to be found in all the better mathematical textbooks.

In an expert report from 29 February 2008, Gartner Inc. also clearly advised: *"Don't be distracted by rumours that all current cryptography-based security will be rendered useless anytime soon by commercially available quantum computers. Continue to secure sensitive assets using current, proven technologies, methods and solutions."* [1]

Security is not an isolated value in itself

Information security can also be guaranteed very reliably in a "conventional" way. Up until now, however, only "security in itself" was considered. But what is meant by this in practice?

What is typically meant here is to be able to exchange large quantities of data flexibly between many participants in complex networks and in such a way that no unauthorised person can access data at any point in the network and can read or alter it. Application-oriented encryption should therefore be regarded as part of information and communication technology (ICT). Each encryption solution must be implemented seamlessly into the ICT and be able to be administered simply and reliably. If encryption is to be beneficial it must be able to function perfectly within the context of these requirements. And quantum cryptography must be able to be put into the same context if it is to fulfil the requirement of being able to protect business or organisational processes reliably, simply and efficiently.

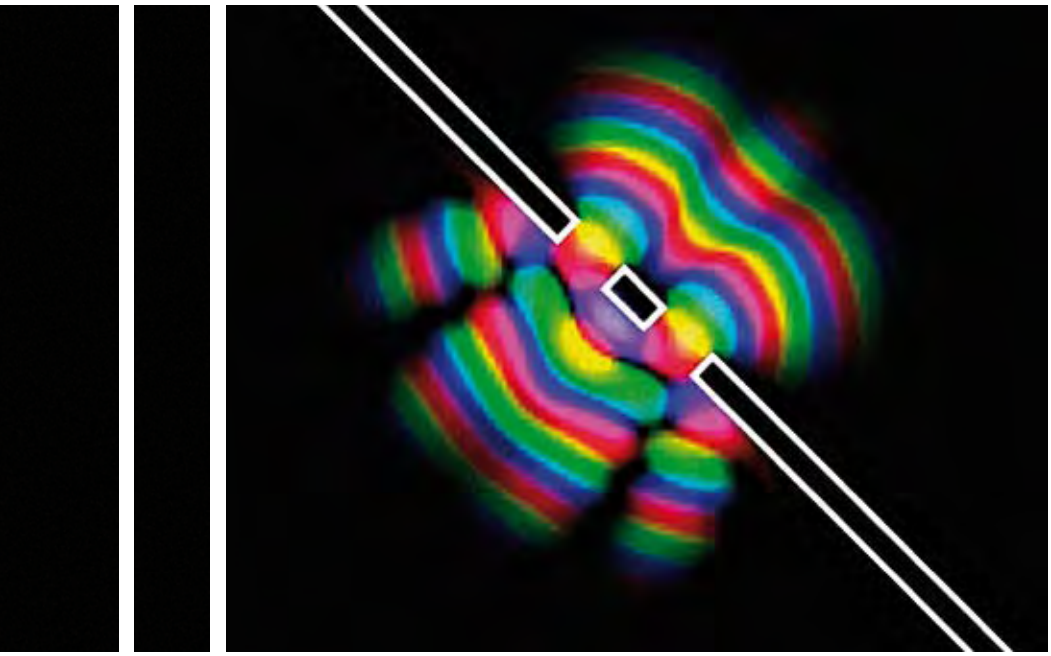
Let us look at the features which it could offer a potential user.

Theory is not the same as practice

Quantum cryptography is based on sending photons, that is, particles of light. A characteristic of these particles is that when moving through space they oscillate – however not randomly or chaotically, but always through a plane which is constant for each particle. This oscillation plane is known as polarisation of the particle. As photons can oscillate in all directions (meaning a 360° circle) they need to be filtered in order to be of use for cryptography (polarisation filter). By filtering, particular entanglement states can be defined, such as 90° or 45° towards the theoretical plane. The resulting entangled photons sent from sender to receiver (mostly via glass fibre) can – using complicated processes – be used for the transmission of binary values.

In conclusion, it is possible to have direct encrypted data transmission from a point A to a second point B. If a photon is "touched" en route by some action, it changes its entanglement or is lost. This means that the attack is noticed and – what is important in practice – the connection is no longer usable.

This description is naturally greatly simplified – however there is



In the realm of quantum mechanics, light has both a wave character (energy) and a particle character (material). This can be demonstrated by electron particles which are sent through a narrow double slit. After passing through this slit, an interference pattern is formed from the overlapping of the two beams of electrons similar to a diffracted superimposed beam of light. The particles therefore behave like waves here (movement). Due to this double character, each individual particle can be used to transmit a piece of information.[3]

extensive literature on the topic (see appendix). The most important consequences for the task of "practice-oriented information security" can nevertheless be demonstrated with this:

- Quantum cryptography can only be carried out point to point by the exchange of light particles (photons) along a seamless glass fibre. The range is limited physically.
- If individual routes are to be linked up, quantum cryptography has to be "set up again" and so, at each junction, there is a cleartext risk: in principle, the unprotected data can be accessed at this point. And no network in the public domain can be permanently protected from someone attempting an attack at some node or other.
- In addition, this "non continuity" makes quantum cryptography unusable for direct routing, meaning that no real network with branches can be developed to connect several participants in the same network on a continuous protocol level.
- Real end-to-end security is likewise not possible – a photon signal cannot be fed and relayed via a LAN and a server to a WAN.
- Authentication of the sender or receiver is not possible directly using photon communication – additional processes need to be used for this. As expected, these are based on an additional "secure" connection with which the authenticity of the participants can be confirmed. Again, this can only be done with traditional cryptography.
- The performance of quantum cryptography is not very high. The usable bandwidth is hardly of practical value for present day applications – a speech signal would be the most that could be achieved. Suggestions are often made about using quantum cryptography primarily for the secure exchange of keys for symmetrical encryption because in this process both sides need to use the same key. In practical terms this means exchanging a secret key using quantum polarisation – e.g. a 256-bit AES key – then switching off the photon link and establishing a conventional link (e.g. Ethernet). This Ethernet link is then used for conventional encryption! The operating security level therefore corresponds to every other AES encryption. In addition, a key change during operation – as is best practice in traditional link encryption – would not be possible.

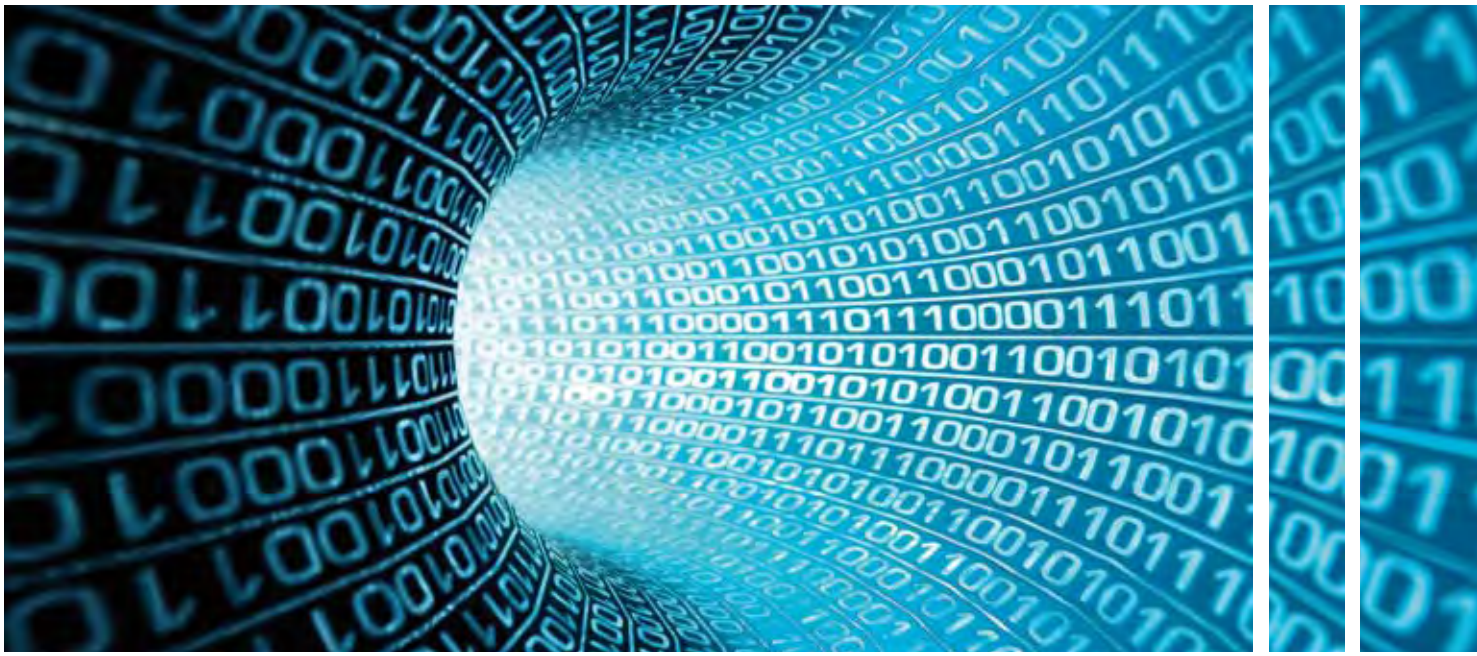
It should be added that, in the case of hardware-based traditional encryption, the problem of secure key exchange never actually existed. This is primarily because a new secret short-term connection key is generated for each connection in a complex process (by means of random numbers) and the secret cryptographic parameters which are stored encrypted in the individual devices serve as a basis for this process.

The user lacks control and autonomy

Quantum cryptography is a very complex matter. In practice hardly any users would be in a position to configure and operate equipment of this kind on their own. And a large amount of physics equipment would be necessary for real tests. *What* was *really* happening with encryption using photons would not be visible to the user.

For the user, however, this means that the critical aspects of a sensible security architecture are missing, in other words the essential comprehensive control over the encryption processes (transparency) and autonomy in relation to supporting your own security policy. A user is therefore always obliged to work with a third party who will inevitably know part of the user's security arrangements.

These disadvantages can be reliably avoided with mathematical cryptography. If the user sets up his own secret algorithm basis and undertakes his own key management (i.e. the whole security management), he possesses complete transparency in all processes. Flexibility of this kind would be unimaginable in quantum cryptography.



The famous cryptography expert Bruce Schneier summarises the situation aptly: *"Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. The real problems are elsewhere: computer security, network security, user interfaces and so on."*[2]

Quantum physics: interesting, but...

Quantum physics is and remains a very interesting discipline. The hope that results from quantum physics research will one day play a role in particular areas of our lives is justified. Obvious examples could be measurement technology, sensor technology, production techniques (nano technology) or bionics. The day of quantum physics will therefore definitely come – even if this is more likely to be in completely new areas where it will be able to bring real progress to the economy and society. Bruce Schneier shares this opinion: *"I'm always in favor of security research, and I have enjoyed following the developments in quantum cryptography. But as a product, it has no future. It's not that quantum cryptography might be insecure; it's that cryptography is already sufficiently secure."*[2]

Source:

[1] Quantum Cryptography: Too Early Even for Early Adopters. Publication Gartner Inc., 29 February 2008

[2] Crypto-Gram, Bruce Schneier, Chief Security Officer. November 15, 2008: www.schneier.com

[3] Picture: University of Graz, Austria, www.kfunigraz.ac.at

PASSWORDS – BETTER PROTECTION AGAINST DATA THEFT

Information security is not only a technical discipline but has a great deal to do with people because it depends on the conscious thinking and actions of the user. So what is a practical and safe way to deal with information and IT equipment? Crypto Magazine looks at the different topic areas, from the Internet to passwords, giving useful tips for everyday life. This fourth article in the series looks at the secure use of passwords.

*By Franco Cerminara, Head of Consulting and Education, InfoGuard AG**

We cannot imagine being without passwords as an important part of IT security in our electronic daily life. We have a password for our computer or an application, a PIN code for credit cards, another for e-banking transactions – the list can be extended as much as you like. Risks arise in the many areas where specific combinations of letters and numbers are required. Passwords and PIN numbers are some of the things most frequently attacked by hackers and criminals. Once the password is known, everything a user can access in an application or on a computer system is exposed to a very high risk. A password not only serves to protect a system of this kind; it is also a protection of the person concerned. Or would you give your cash dispenser PIN to a stranger?

It is possible to have reliable protection against unauthorised theft, but what does a perfect password look like?

Tips for creating a good password

Both your computer and various online services require you to enter a password. Passwords which are badly chosen or too short – in other words weak passwords – present a considerable safety risk. When choosing a password, keep the following principles in mind:

- A password should be at least eight characters in length and consist of both letters, numbers and special symbols (e.g. ! ? “ ” * + -) .
- Find a sentence which consists of at least eight words, numbers and punctuation marks so that the password has the required length: I was at the golf club for 8 hours yesterday! -> IwatGCf8hy!; information security is more than a firewall! -> ISi>a1F!.
- Create passwords from words without vowels in combination with numbers and special characters: Donald has 3 nephews! -> Dnldhs3Nphws!; my shares fell by 9 percent -> Mshrsfllb9%.
- Do not use any generally known facts about yourself in your password, for example names, nicknames, initials or birthdays.
- Avoid trivial passwords (e.g. “guest”, “qwertyui” or “12345678”). Also avoid words which appear in dictionaries.

Passwords must be changed at regular intervals, at the latest when you suspect a password might be known to a third party. Basically each application should have a different password.

Remember your word combinations but on no account write them down. Also make sure that you are not being watched when you enter your password.

Your password is your personal ID – do not pass it on to anyone!

* InfoGuard AG, a company affiliated to Crypto AG and a member of the Crypto Group, specialises in comprehensive information security. Its fields of expertise include advice, training and awareness-raising as well as the development and implementation of technical security solutions.

HAGELIN-CRYPTOS
CRYPTO AG

TRADE FAIRS

DSEi, 8 to 11 September 2009
London, Great Britain

SEMINARS by InfoGuard AG

For Information Security Professionals

ISC09/1	20 – 24 April 2009
ISC09/2	15 – 19 June 2009
ISC09/3	28 September – 02 October 2009
ISC09/4	09 – 13 November 2009

Contemporary Cryptography

CCC09/1	27 April – 01 May 2009
CCC09/2	22 – 26 June 2009
CCC09/3	16 – 20 November 2009

Ethical Hacking and Cyber Crime

EHC09/1	08 – 12 June 2009
EHC09/2	05 – 09 October 2009
EHC09/3	23 – 27 November 2009

Further information at www.infoguard.ch/crypto

PRESS REVIEW

Study confirms fears about personal data on the Internet

To mark the third European data protection day on 28 January in Berlin, Privatim, the association of Swiss data protection registrars, commissioned a survey. Around 1,600 people were interviewed throughout Switzerland and the results showed that Swiss inhabitants see data protection as being important.

Nine out of ten interviewed consider it important (22 percent) to very important (69 percent) that companies and administrative authorities protect personal data. More than four in five interviewees trust public authorities such as the police, hospitals or residents' registry offices to handle data carefully.
Industry did not come off well in the survey. 44 percent mistrust their credit card company when it comes to data protection: the proportion is even worse (54 percent) for telecommunication suppliers. In general, just 18 percent of those interviewed consider protection to be inadequate; 15 percent even claim to have been affected by data abuse at lease once already.

Sources: www.werbewoche.ch and heise online, news from 27 January 2009

CRYPTO AG – TO REMAIN SOVEREIGN

Crypto AG, Headquarters

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, Regional Offices

Abidjan
Crypto AG
01 B.P. 5852
Abidjan 01
Ivory Coast
Tel. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi
Crypto AG – Abu Dhabi
P.O. Box 41076
Abu Dhabi
United Arab Emirates
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires
Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentina
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat
Crypto AG
Regional Office
P.O. Box 2911
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group