

# CRYPTO MAGAZINE



TOTAL INFORMATION SECURITY. FOR THE CLIENTS OF CRYPTO AG, SWITZERLAND.

3 / 0 1

SYSTEMS

INTERVIEW

INSIDE

CRYPTOLOGY

IT SECURITY

NEWS

**EXCLUSIVE INTERVIEW WITH THE  
SWISS AMBASSADOR TO THE UN**

**COMPROMISING EMISSION**

**WHERE IDEAS AND  
VISIONS BECOME PRODUCTS**

**Dear Reader,** Information technology and telecommunications increasingly govern our lives. Whether at the workplace or in the private sphere, the computer is omnipresent. The rapid spread of computers and their interconnectivity in local, regional and world-wide networks has triggered a fundamental change both in Western countries and in Asia and Latin America, which is described by the term “information society”. The dynamics of political, economic and social developments in the information society are defined by the interactive capture, storage, processing, transmission, dissemination and use of information and knowledge. Daniel Bell, one of the early theoreticians of the information society, went to the heart of this when he said: “The crucial point about a post-industrial society is that knowledge and information become the strategic and transforming resources of the society, just as capital and labor have been the strategic and transforming resources of industrial society”.



In the information society, mastery of information and communications technologies and influence over the contents of information increasingly become the sources of political importance, both in a domestic and an international context. This affects diplomatic services in particular. When issues are at stake that involve vital national interests, then information exchanged between embassies and government departments is of extremely great value. Information of this degree of importance thus needs protection at the highest level of security. This security is offered by Crypto AG with its concept of Total Information Security TIS®. We have been exclusively concerned with information security for 50 years. And we will never do anything else.



Giuliano Otth, CEO Crypto AG

**Editorial**

# SCREENS WHISPER – THREATS FROM EAVESDROPPING ATTACKS

**Spies have simple means of detecting monitor contents by picking up emitted signals. Diplomatic missions who share a building with other offices are particularly at risk. But compromising emanations can also be captured outside a building. There is, however, a way of protecting oneself against this: With the Emission Protected Security Workstation by Crypto AG.**

*Dr. Hans Kurmann*

Assessing and reporting events in a foreign country, and analysing the international situation, are among the main tasks of an embassy and can be of the greatest importance for the protection of the cultural, business and economic interests of one’s own country. However, nowadays this information has to be processed electronically somewhere in an embassy, stored, and finally transmitted to the government department. Even if one assumes that an embassy is conscious of the general security risks, that it only transmits news in encrypted form, that it uses a sophisticated key management, and that it employs trustworthy staff, there is still a risk: compromising emanations.

**The risk of an eavesdropping attack**  
Compromising emanations originate in electromagnetic fields which occur wherever electricity is involved: All

electric appliances, as well as cables, printers, modems and cables, send information into the environment with the emitted waves. In this way, a screen discloses the buffer content it displays, cables and modems leak the data which they currently transport. The risk of an eavesdropping attack depends on the type of emission. Be-

## CONTENT

<b>Compromising emission</b>	<b>3</b>	<b>SYSTEMS</b>
Spies have simple means of detecting monitor contents by picking up signal emissions.		
<b>Important messages are only sent in encrypted form</b>	<b>8</b>	<b>INTERVIEW</b>
The Swiss UN-ambassador François Nordmann about communication in the diplomatic service.		
<b>Where ideas and visions are transformed into products</b>	<b>12</b>	<b>INSIDE</b>
At Crypto AG, all security-relevant components for ciphering solutions are produced in-house.		
<b>New Crypto regional office in Oman</b>	<b>16</b>	
Since mid-September, Crypto AG has a presence in the beautiful sultanate.		
<b>The benefit of proprietary cryptographic algorithms</b>	<b>18</b>	<b>CRYPTOLOGY</b>
Correctly used proprietary algorithms make a substantial contribution to a system’s security.		
<b>Hacker glossary (Part II)</b>	<b>20</b>	<b>IT SECURITY</b>
Computer freaks have developed their own, special language.		
<b>Windows-based Crypto solutions</b>	<b>22</b>	<b>NEWS</b>
Crypto AG’s product range includes three Windows-based security solutions. Work is now underway on conversion to Windows XP Professional.		



cause devices are built in different ways, the strength of their emissions varies, with differing radiation profiles. Electromagnetic emissions can contain secret information from an embassy or a company, which spies are able to capture even over fairly long distances if they have the right equipment.

**Anyone can listen in**

Compromising emanations have been known for 40 years. Until now, the main agencies concerned with reception and repulsion have been the armed forces and secret services. Today, emissions represent a rapidly increasing risk of which there is still far too little awareness, and which embassies, too, do not take seriously enough. Not only electromagnetic fields, but also unintentional network signals allow secret data to leak to the outside.

The term compromising is used for all emissions which contain secret information. Data can migrate on the conductors of the cable shields through surface waves, and compromising emanations have been known to occur in power supply systems. There, unintentional signals spread as voltages and currents similar to the signals of the network telephony or a baby alarm. The reach of this effect depends on the type of power supply system.

As a rule, it is possible to receive information inside a building or group of buildings on the linked phase cables. Depending on the equipment used by an attacker, the quality of reception varies. With a directional aerial, it is possible to pick up information outside a building up to a distance of 100 metres. With an investment of just 5000 Swiss francs, spies can get equipment which reproduces the 'stolen information' in



IN CRYPTO'S OWN EMC LABORATORY, OUR EXPERT ANDREAS FOSTER TESTS WHETHER THE EMISSION PROTECTED SECURITY WORKSTATION MEETS THE PRESCRIBED GUIDELINES WITH REGARD TO EMISSIONS.

usable form. If someone wants to decipher alpha-numeric or graphic symbols, they have to spend a bit more. It is therefore high time that embassies devoted the necessary attention to protecting their information systems against attacks. Because the possibilities of infiltrating a network are boundless.

**TEMPEST and COMPREM**

Of course, where such dangers exist, people attempt to eliminate them. The term TEMPEST is normally used in connection with compromising emanations. This term is used in two different definitions:

1 TEMPEST is a NATO standard which aims to reduce the risk from compro-

misising emanations in the vicinity of electronic devices. However, non-NATO members like Switzerland are not authorised to use this standard. It does not contain any recommendation about the measures to be taken to achieve the prescribed limits.

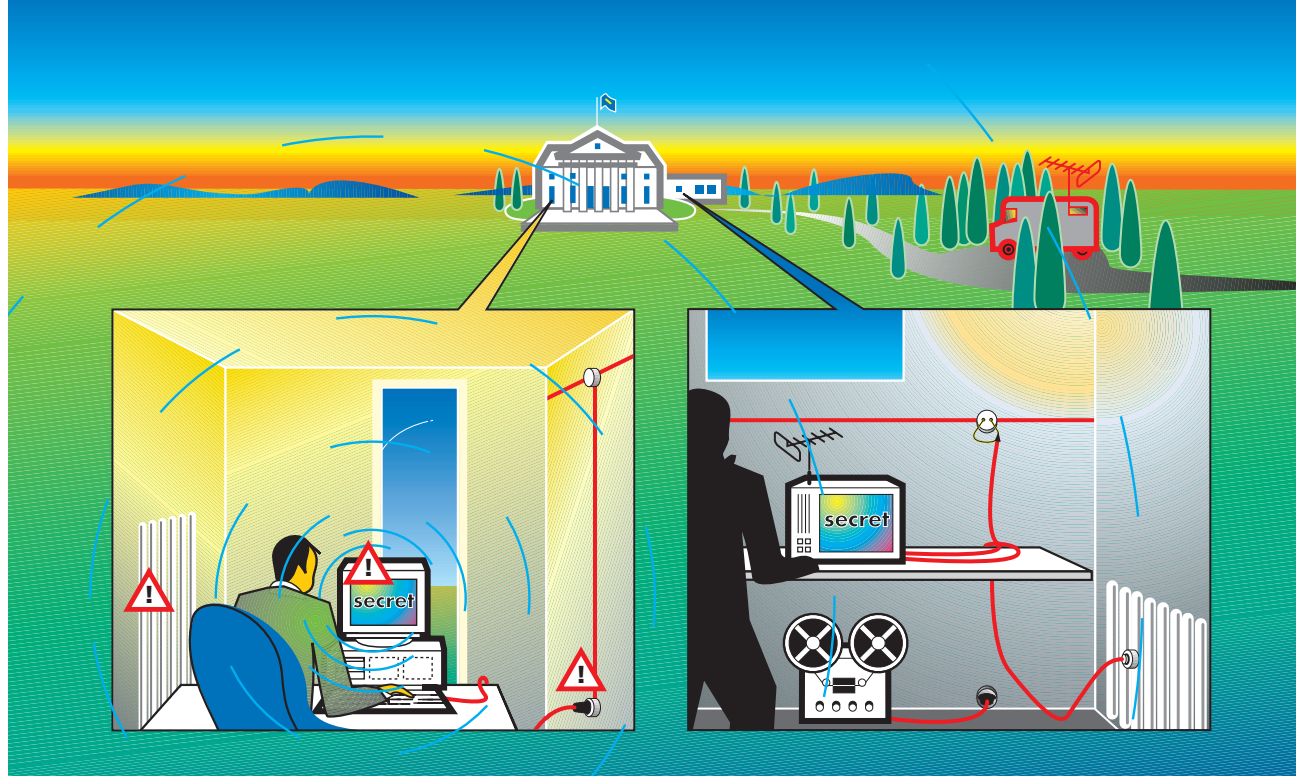
2 TEMPEST is also used as a general term for the science and technology which concerns itself with the

problem and avoidance of compromising emanations.

COMPREM is the Crypto-specific synonym for TEMPEST within the meaning of the second definition. The development of COMPREM technology assumes, on the one hand, knowledge about the mechanisms that lead to the creation of this problem, and on the

other hand, the know-how required to be able to take the appropriate counter-measures at the early stage of the product design process. People talk about the so-called red-black separation, the filtering of signals and cables, the protection or insulation of critical components, etc. Finally, COMPREM includes the verification of the counter-measures taken. Based on





COMPROMISING EMISSION ENABLES INFORMATION TO BE CAPTURED BOTH FROM CABLES AND VIA THE AIR.

the EMC-Guidelines, the appropriate measurements are performed at Crypto's own EMC laboratory by a team of experts.

The HC-6950 Emission Protected Security Workstation by Crypto AG (see box) meets all these guidelines

and guarantees protection against the undesired emission of compromising information.



Further information:  
hans.kurmann@crypto.ch

### HC-6950 Emission Protected Security Workstation

Guarantees full protection against the emanation of compromising information. The system provides full protection for stored and transmitted data. It consists of a COMPREM PC and a comprehensive security package and may be integrated into any IT system.

#### The Main Features:

- Emission protection by sliding front door covering: Removable hard disk drive, CD drive, Crypto card reader

- Full protection of the 17" monitor
- Specially designed keyboard without traditional screening
- Switches off monitor, mouse and keyboard, when opening front door

#### The Security Features:

- Access protection
- Fully transparent disk encryption for extended hard disk and floppy disk
- File encryption for file storage or transmission over e-mail system

- Access to encrypted disks and to file decryption is locked during Internet network access
- Using IP security standard (IPSec) for VPN encryption
- ESP (Encapsulating Security Payload) tunnel mode protocol
- Each secure tunnel has an individual communication key



THE HC-6950 EMISSION PROTECTED SECURITY WORKSTATION BY CRYPTO AG OFFERS COMPREHENSIVE PROTECTION AGAINST UNINTENTIONAL EMISSION OF COMPROMISING INFORMATION.

Press review

### Data are at risk outside the corporate network

The times when a company's network was also simultaneously representative of its workplace are long gone. Employees are constantly on the move and need rapid access to their company data and information from different Internet sources. Today, laptops and mobile microcomputers are part of many employees' basic equipment. But smartphones, communicators, personal digital assistants (PDA), or whatever these micro-computers are called, are not immune from security risks.

Last year, 387000 laptops were reported stolen, and American projections forecast the loss of 250000 mobile phones this year - at US airports alone. The damage is not limited to the expensive hardware in these cases. Data are also lost, to which unauthorised persons could gain access. Confidential information on laptops, but also on smartphones or PDAs, is usually only protected against unauthorised access through simple passwords, and its encryption is usually weaker than that provided in the system. If the removable memory cards are taken out, then these can in most cases be read in with a compatible device. The first incidents with viruses and Trojan horses have shown that it is possible to write viruses capable of causing damage on pocket computers and mobile phones. These can very quickly spread in the wireless environment, too. Despite all these dangers it should be said that properly protected devices are considerably more secure than the conventional paper notebooks. Only digital data can be protected through encryption, and in the event of a loss, the user can take recourse to his backup copy on the server at home or in the office.

Source: Neue Zürcher Zeitung

INTERVIEW WITH THE UN AMBASSADOR NORDMANN:

# “ONE ALWAYS HAS TO ASSUME THAT SOMEONE IS LISTENING IN”

**The Swiss UN-ambassador in Geneva, François Nordmann, has had an exemplary career in the diplomatic service. In this interview, he talks about the stages in his career, the relationship between Switzerland and the United Nations, and the handling of secret information.**

*Your Excellency, you have been head of the permanent mission of Switzerland to the International Organisations in Geneva since December 1999. In the*

*past, you were ambassador in Central America and in England, and also held various functions at UNESCO in Paris and the United Nations in New York. Can you tell us something about the specific tasks and challenges of each of these positions?*

**François Nordmann:** I had the good fortune in my career of getting to know both the bilateral and the multilateral aspects, and to be able to switch between the two.

While there is also the model of specialisation, which many of my colleagues have chosen, I think that by pursuing my particular path, I was able to gain a lot of experience. It allowed me to get to know all the different facets of the profession over a period of 30 years. Moreover, I had the opportunity to work both in Switzerland and abroad. In Bern, for example, I worked in the office of the chief secretary to the ministry. In such a position, which is so to speak ‘on the roof of the world’, one gains an overview of

the topical issues, both in the Ministry and in the Federal Council as a whole.

*You were then appointed embassy councillor at the permanent observer mission in New York.*

**François Nordmann:** Yes, I worked in the political sphere of the UN, particularly during the time of the Falklands war. That was under Secretary General Perez de Cuellar, who was very kindly disposed towards our country and still is.

*You were then appointed ambassador to Guatemala, Costa Rica, Honduras, Nicaragua, El Salvador and Panama. What did you find there?*

**François Nordmann:** I was in

Central America between 1984 and 1987, when the spotlight of international politics was focused on the war of the Sandinistas and on the efforts to bring peace to the region. It was an exciting time, because these peace efforts required a neutral mediator. I had contact with the guerrillas, and participated in the negotiations. It was also the first time that Switzerland sent an election observer, in this case to the presidential elections in March 1984. The ambassador on the spot was chosen for this role. I left there just before the UN started its activities to achieve a final peace agreement.

*After that, you were again posted to an international organisation, at UNESCO in Paris.*

**François Nordmann:** The situation here was quite different than in the present position with the UN, because I was head of a delegation in an organisation of which we were a member. We were able to exert a certain amount of influence here, in the areas of the budget, general policies, education policy etc., at a time of reorganisation at UNESCO – when there was a need to

reestablish confidence in this organisation. The USA had withdrawn, and still has no presence today, while Great Britain has meanwhile rejoined. For Switzerland, which was not (and is not) represented in the actual political or-

ganisations of the UN, membership of UNESCO is doubly important, particularly in order to be able to play a part in solving general social problems.

*What was your task as head of the Directorate for international organisations in the Bern Foreign Ministry headquarters?*

**François Nordmann:** One of the highlights were the negotiations about the headquarters of the WTO, the seat of this organisation in Geneva. Here, we were confronted with a completely new situation, because for the first time, we had serious competition from

other cities for the location of an important organisation, based on practical-commercial grounds. It was a new political environment: the cold war was over, and so the single deciding factor was who made the best offer. Consequently, we reviewed all our operations and considerably enhanced our general provisions for the organisations and diplomats in Geneva. In the end, we were chosen.

After that, I was in London, where I was mainly responsible for three im-

portant areas. For one, there was a new government after 18 years. It was necessary to create a new network of contacts with new personalities who had come to power and did not always have a good opinion of Swit-

erland. The second area I was concerned with was the presidency of the European Union, which was held by Great Britain. It was an important time in the bilateral negotiations between Switzerland and the EU. The task was to make the British government aware of the issues at stake. The third matter was purely bilateral: It concerned the reappraisal of Switzerland’s role during the second world war, and the corresponding attitude of the British government and public.

*And what is your present task in Geneva?*

**François Nordmann:** In one respect, it is concerned with protecting Swiss interests at the diplomatic level in all the organisations of which we are

a member. In addition, I concentrate on the fields of human rights and humanitarian issues among other things, which are the direct responsibility of the Federal Ministry of Foreign Affairs. Finally, there is also a whole range of organisational tasks, such as receiving national delegations, looking after the foreign missions here in Geneva, which also touches on problems of a structural nature like the housing shortage, questions of security, etc.

*Of course, at the moment the question of whether Switzerland should join the UN is very topical.*

*There will soon be a referendum about this. What advantages do you see, from your experience, in closer cooperation between Switzerland and the UN?*

**François Nordmann:** Our present situation at the po-





litical level is very unsatisfactory. Firstly, while we can state our point of view to various UN committees, for example in the field of human rights, we are excluded from all decision-making processes. In other words: We carry little weight. Secondly, important and responsible ranks are allocated in the United Nations. These posts are distributed among the member states on the basis of negotiation and consultation. Switzerland cannot participate in this 'give and take'. And thirdly: My view is that the General Assembly, of which we are not a member, is something like the cockpit of the organisation. This is where important decisions are taken, where the general direction of the organisation is established, for example in the discussion about globalisation, which is of fundamental im-

portance for our economy. Here, too, we have no influence. Although Switzerland has survived the last 50 years without being a UN member, it is really strange. We are the twentieth largest economy in the world, but we are completely absent from the political debate.



*And what about our independence?*

**François Nordmann:** All other countries are members, even the smallest island in the Pacific. It has always been the case so far that countries which gained their independence, either after a war or a peaceful transition, immediately strove to join the United Nations. Joining the UN was something like a confirmation of independence. And certain voices in our country assert the opposite.

*To change the subject: Diplomacy means cultivating relations between states – particularly through negotia-*

*tions – and is a peaceful tool of foreign policy. In this, information and the edge in information play a key role. What are the sources for your information?*

**François Nordmann:** The work of the diplomat today no longer simply consists of informing his government about events, irrespective of whether it is an earthquake, a new president or a coup d'état. One can assume that the news agencies or the television pursue this task around the clock. Fundamentally, these sources are also useful for us, but what counts is the reliability of the information. Because journalists – a respectable profession – also sometimes make mistakes. But we have to be completely certain that things are presented in the way in which they happened. Then there is also information that is ignored by the press but is nevertheless important. Finally, we have a task of explaining to do. Events have to be analysed, put into context, and possible repercussions, particularly on our country, pointed out.



*Diplomacy also needs secure information in two respects. On the one hand, the information has to be accurate, and on the other hand, it also has to be protected against unauthorised access. What protective measures does an embassy or a diplomat have available?*

**François Nordmann:** As a rule, embassies have various types of communication equipment which is secure. For important messages, a fax machine is normally used which encrypts the message. Another element is of course the diplomatic courier,

through whom important information reaches the central government in Bern safely and quickly. But it cannot be assumed that we have secure telephones, for example.

*Does this mean that you are very cautious when it comes to information by telephone?*

**François Nordmann:** There are certainly messages that one can convey by telephone without secret information being discussed.

*Today, the fax is increasingly superseded by e-mail. Is this the case with you?*

**François Nordmann:** We, too, constantly send and receive e-mails. I regularly correspond via our Intranet

with my colleagues about current business, as for example questions concerning buildings. We constantly provide buildings and premises for the international organisations in Geneva. So there are always issues about construction, maintenance, or the purchase of buildings to be dealt with. But when we deal with important and sensitive information, we continue to use encrypted fax messages.

*Cue: Interception of information. What is your assessment of the current threat to Swiss business from spying and the interception of information?*

**François Nordmann:** I don't want to get carried away with speculations here... I have of course read such news articles, but I am not an expert in this field. But if you look around here, and see all these antennae on

the roofs... They are certainly not just there to get the BBC. Geneva has become an important centre for information, including in the economic sphere. It is the headquarters of the World Trade Organisation (WTO). Important decisions are made here. So if there is economic espionage, which one must assume, then Geneva is undoubtedly a lucrative target, alongside other business centres. As I have said, that is why we are very careful, particularly about what we discuss on the telephone. There should always be the assumption that someone is listening in.

*Your Excellency, many thanks for the interview.*



Press review

### **Billions worth of losses through online spying**

According to estimates of those interviewed, European companies have lost around 3.6 billion Euro in the last two years as a result of industrial crime. Average financial losses amount to roughly 15 million Euro just among the large companies with more than 5000 employees. This is the conclusion of a topical study conducted by PricewaterhouseCoopers, for which 3400 companies, organisations and administrations in 15 European countries were questioned about fraud cases in the last two years. Throughout Europe, the risk of white-collar crime rises in line with the growing size of a company. Ever more complex structures make central control of internal processes and transactions with outside parties more difficult. Weak identification of the staff with their companies, and thus a lower level of resistance, is another danger. In more than 60 per cent of cases, the crimes are committed by people within the company. The public mostly associates white-collar crime with corruption, money laundering or blackmail. As the study by PWC shows, the greatest problem is embezzlement of money or property by staff: 63 per cent of the companies affected are cheated by their own staff. In second place comes breach of confidence by the management. A quarter of all fraud cases are due to abuse of management authority, such as falsification of the books or misappropriation of assets. Added to this traditional white-collar crime are new dangers arising from modern technologies and e-business. But cybercrime is still underestimated. While only 6 per cent of those questioned currently see a danger in computer viruses, hackers or Internet fraud, 13 per cent of companies are actually already the victims of such attacks. In future – and here 43 per cent of those interviewed agree – cybercrime will become one of the highest risks, alongside embezzlement.





## WHERE IDEAS AND VISIONS BECOME PRODUCTS

**Total information security is a matter for the absolute specialist. One who can directly provide all the security services. Crypto AG is one of the few providers who, for this reason, develops and manufactures all security-relevant components for its encryption solutions in-house – this eliminates the risk of weak points remaining undetected.**

*Michael Zimmermann*

Saturday morning in Steinhausen near Zug. While the machines have stopped running in most Swiss manufacturing plants – as is commonly the case at the weekend – the lights are on in the production halls of Crypto AG. A special shift is being worked to ensure that all orders can be delivered on time. The visitor first sees the impressive, 19 metre long assembly line on which up to 40000 components can be manufactured per hour. But for Crypto AG, the key asset in the production division is not the machinery, but the roughly 70

employees who operate it. Their commitment and flexibility make it possible to deal with significant peaks in orders to meet customer specifications and deadlines.

The production division of Crypto AG – called the T division – brings together all the disciplines that ensure that the device functions defined in the design departments are translated into solid products. The advantages of this close dovetailing of all production processes and the entire in-house production of

all security-relevant components are obvious:

- **Security:** All production processes, from the procurement of individual components via the implementation of security-relevant parameters in the device, to its delivery to the customer, take place through channels and on premises that meet the high security requirements of our customers.
- **Quality:** The close collaboration of all the departments involved in the pro-





PROGRAMMING OF THE FULLY AUTOMATED EQUIPMENT WITH WHICH UP TO 40 000 ELECTRONIC COMPONENTS PER HOUR CAN BE INSERTED ON PRINTED CIRCUIT BOARDS.

efficient production and testing are developed, implemented and finally verified. This product development process is geared both to the customer's requirements and to the production process.

The next interface between development and production is the Order Processing department, which produces the sets of documents necessary for a qualitatively perfect production process: technical drawings, parts lists and operational plans. This also involves the practical implementation of a customer's requirements that may diverge from standard versions. Precise device models with suitable versions and add-ons have to be specified from a broad description of a market product. While the technical drawings and parts lists clearly define a product, the operational plans lay down a sensible production process. Order volumes and individual deadlines have to be coordinated and checked as to their feasibility.

#### ...to delivery

The staff of the Procurement department are the third pillar of the T division in the development of new market products. They clarify which components have to be procured in line with our requirements – Procurement processed more than 6000 orders last year – and they agree the terms with the suppliers. The three departments do the necessary preliminary work that ensures that the actual manufacturing process can be triggered on behalf of the Sales department.

The staff of the Mechanic Production department know how to produce very precise housings, base plates, front and back panels from various raw materials. They get the very best value from the high-quality materials and the latest technologies.

duction process, from the development to the final testing and inspection, allows constant improvements and, if necessary, corrections to be made to the product. Moreover, the production process is constantly being developed so that it is capable of using state-of-the-art technologies.

- Reliability: Because all production staff are employed directly by Crypto AG, a high degree of reliability is guaranteed at the human level, too.

#### From design engineering...

At the beginning of the production chain is the Production Engineering department. That is where the device design is decided, in close collaboration with the design engineers. Measures for the protection of users, aspects of fault-free operation, but also the technical prerequisites for

In the Sub-Assembly Production department, the printed boards are fitted with the electronic and electromechanical components. Most of the printed boards consist of a highly complex network of thousands of connections. Component groups with more than 6000 soldering joints have to be processed. A single mistake would result in a whole device being discarded. The increasing miniaturisation, as well as the huge diversity of the component groups and components, places additional new challenges on the staff in this department on a daily basis.

ing product variety, as well as the broad range of technology – new alongside 'old' – forces the people in Final-Assembly&Test to process each order individually in the third stage, the final device test.

Our customers' special requirements regarding security and conduct demand a lot of empathy, understanding, willingness to perform special services, and discretion from the staff.



THE MAIN BUILDING OF CRYPTO AG WITH ADJACENT BUILDINGS WHICH HOUSE THE PRODUCTION AREA WITH 70 STAFF.

Final-Assembly&Test checks the produced and procured goods at the first stage. Next, the individual modules are assembled into a complete device or system. Each customer receives devices with customised parameters and settings. The result-

Stores & Dispatches is the real logistics centre in the manufacturing process of Crypto AG. Here, our products have to be packed suitable for transport, and 'taken to the customer'. The chauffeur service for our customers is also part of this department.

Press review

#### Internet: PCs as open as barn gates

Half of all PCs connected to the Internet via wideband networks are not protected. As research carried out in the USA showed, many users of fast Internet links are not aware that hackers can gain unhindered access to their computers. They do not protect their data either with firewalls or anti-virus software despite the fact that some of the PCs are permanently online. The greatest danger is no longer data theft, according to Alan Paller, head of the System Administration Networking and Security Institute (SANS). Instead, many open computers are used to start DDoS attacks (Distributed Denial of Service). Up to 3000 network scanners are searching daily for PCs suited for such attacks. There is also an increasing risk of hackers controlling the computers via Trojan Horses which they introduce through mail attachments. Experts anticipate that wideband access in the USA alone will rise from 8.3 million this year to nearly 40 million in 2005. The risks on the Internet will rise correspondingly, according to Paller.

Source: Computerworld



# NEW CRYPTO REGIONAL OFFICE IN OMAN – THE GATEWAY TO THE EAST

Since mid-September, Crypto AG has been represented in Oman with a new regional office, to enable us to offer our customers in the region even closer commercial and technical support. The beautiful Sultanate has a lot to offer: sights bearing witness to a long history, ancient traditions, as well as a rich diversity of landscapes with wildly rugged mountains, lush green oasis, magnificent desert regions and miles of sandy beaches. A visit to Aladdin's wonderland.

Walter Hediger

Oman certainly lives up to its reputation as an 'enchanted kingdom': From the shadows of the Al Hajar Mountains in the east via the lush green regions in the south, where the monsoon reigns from June to the end of September, to the 'Wahiba Sands', one of the most perfect deserts of the world which has remained untouched by time.

The desert landscape of the Arabian peninsula, which is as beautiful as it is hostile to life, has marked its inhabitants. Hospitality was a vital ingredient of everyday life, in which the nomads provided other travellers with water, food, and shelter for the night. The Bedouin tribes were the precursors of the settled life of their descendants in the towns. Today, only a few nomads still travel through the land with their camels, sheep and goats.

Visitors to their country are kept at a friendly distance. An unusual experi-

ence for many new arrivals is the completely different cultural system from which the country originates. Women have almost no presence in the city. They can be seen shrouded in dark 'abayas'. The black cloaks cover their hair and usually also the face. Oman is considered to be a progressive country on the Arabian peninsula. Nowadays, girls can study and then take a job. Whether as a teacher, doctor or market stallholder – women in Oman are conquering the world of work, thanks to Sultan Qaboos Bin Said Al Said.

Anyone participating in a traditional Arab banquet gains an insight into the inner workings of oriental culture. He will experience the hospitality of the East and enjoy the aroma and taste of the delicious, exquisitely prepared food. The custom of eating while sitting on valuable carpets and hand-woven, embroidered cushions goes back to the Bedouins. It is a special honour for the foreign visitor to be invited by an Omani to a traditional meal in his house. Such companionship is reserved for the male members of the host family. Having taken off one's shoes and sat down, the food is served in numerous bowls and plates placed in a circle: Lamb, goat, beef and chicken, fish and shellfish,

grilled or boiled, prepared in a sauce made with various vegetables. This is accompanied by marinated cauliflower, asparagus and pumpkin, white turnips and fennel.

No wonder that our Crypto staff member Beat Meyer, who manages the regional office in Muscat, is very happy

in Oman. For Crypto AG, which has regional offices throughout the world, it is very important to be able to be constantly and quickly available to its customers, enabling it to provide the required support. Particularly in view of the time difference in the working day between Switzerland and Oman, a presence there is of great importance.

wilayats (districts) is administered by a wali (governor) who is responsible to the Ministry of Interior. The head of state is His Majesty Sultan Qaboos Bin Said Al Said. Part of the government administration system are the Diwan of the Royal Court, the office of his Majesty, the cabinet as the highest executive organ, the governorate of

Muscat and the state consultative council. The cabinet receives instructions directly from the Sultan and is collectively responsible to him.

During its long and varied history, Oman has always remained an independent country. The Persians and Portuguese tried in vain to dominate it. The intruders only succeeded temporarily in establishing small settlements along the coast before they were finally driven out. The currents of history and civilisation have left the sultanate with a proud heritage. More than 500 fortresses, some originating from the 14th century, are scattered throughout the country. Some of these architectural miracles are recognised by UNESCO as symbols of the world's architectural heritage. Islam was adopted even during the lifetime of the Prophet Mohammed, and remains the country's religion.

## Oman

*Political leadership: Head of State  
Head of government and Foreign  
Minister: Sultan Qaboos  
Bin Said Al Said  
Political system: Sultanate  
(absolute monarchy) since 1744  
Area: 309 500 km<sup>2</sup>  
Population: 2'348 000 = 7,6 per km<sup>2</sup>  
Capital: Masqat (Muscat)  
350 000 inhabitants  
State structure: 59 provinces  
Official language: Arabic  
GDP: \$ 9266  
Currency: 1 Rial Omani (R.O.)  
= 1000 Baizas  
National Holiday: 18 November  
(Sultan's birthday)*

*Sultanate of Oman  
Crypto AG Representative Office  
P.O. Box 2911  
Postal Code 111  
Seeb  
Sultanate of Oman  
Phone +968 504 966  
Fax +968 504 929*



CRYPTO AG: THE CENTRAL OPERATIONS IN SWITZERLAND...

...A BASE IN OMAN.

After Saudi Arabia, the Sultanate of Oman is the second-largest country on the Arabian Peninsula. The Sultanate's 1700 kilometre long coast stretches from the Strait of Hormuz in the north to the Arabian Sea in the south. In the west, Oman borders on the United Arab Emirates, the Kingdom of Saudi Arabia and the Republic of Yemen. The Sultanate divides into 8 geographic regions. Each of the 59



# THE BENEFIT OF PROPRIETARY CRYPTOGRAPHIC ALGORITHMS

**Cryptographic algorithms are used to transform plain text into encrypted text and vice versa. The issue of whether the algorithms should be proprietary or standardised seems to be a question of faith. This article demonstrates that this is not the case. Correctly used proprietary algorithms significantly contribute to a system's security.**

*Jürg Eiholzer*

The history of modern cryptography begins in the last century: Ingenious algorithms (mathematical formulae), mostly developed by mathematicians in government service, are at the origin of this booming science. Since these algorithms were normally the property of the organisation that developed them, and were also exclusively used by it, they were all proprietary algorithms.

The first standard for a cryptographic algorithm was developed in the 1970s: The national standardisation agency in the USA at that time, the National Bureau of Standards (NBS), published the FIPS 46 standard with the 'Data Encryption System' algorithm, or DES. This standard then went on a triumphant march around the world and was used above all by banks to protect financial transactions. The reason for its success was that a standard enables the required interoperability between two products of different origin. It was not the strength of the DES that led to its widespread use, but rather its standardisation! Interestingly, the weakness of the DES – the too short key of 56 bits – which was obvious from the

start, did not inhibit its widespread use in the banking sector.

Alongside the few standardised algorithms, there are a large number of publicly known but non-standardised and thus proprietary algorithms. They are often subject to private exploitation rights, that is the user has to acquire them under a licence. Comparing such published, proprietary algorithms to the standard algorithms may be interesting in terms of interoperability or even 'multi-vendor systems'. But when security is at issue, other criteria are important.

The correct comparison in terms of security is: Secret algorithm as opposed to publicly known algorithm. And it is precisely at this point where the other aspect of the proprietary algorithm comes into play, namely the secret algorithm: Only a proprietary algorithm can also be a secret algorithm!

Keeping the algorithm secret is important because it significantly helps to increase the security of a system. It is thus good practice to build a cryptographic system on the principle of 'multiple lines of defence': A system with a secret algorithm that is only known to the respective user offers a certain degree of security even if, for some reason, a secret key has been compromised. Moreover, the user can decide to split the knowledge about the algorithm and that about the keys used in such a way that simultaneous exposure is very unlikely or even impossible ('secrecy splitting'). Furthermore, a great number of attacks can be made much more difficult, or even impos-

sible, with the use of a secret algorithm. A 'brute force attack' on the key used, for example, becomes a priori impossible without knowing the algorithm.

The customers of Crypto AG are not the only ones who require a cryptographic system with secret algorithms. As soon as a government's sensitive information is at stake, or indeed the protection of information relating to national security, all the major countries throughout the world work with secret algorithms known only to them. To give just one example: the DES successor, AES (Advanced Encryption Standard) can only be used in the USA to protect information that is categorised at the lowest level of protection, as 'classified'. To protect more highly classified information, a secret – and thus proprietary – algorithm has to be used. Crypto AG enables its customers to do precisely this: to guarantee the protection, with secret algorithms which are known exclusively to the respective customer, of his most sensitive information at the highest level.





Computer specialists have developed their own language when it comes to information security and attacks on IT systems. In this mini-series – part 1 appeared in the August issue – we aim to explain some of the most frequently used hacker terms.

## HACKER GLOSSARY PART 2

**DoS – Denial of Service** DoS is the name for an exploit which prevents the use of a service on an attacked system by crashing or blocking programmes or entire systems. There are different types of DoS:

**System Flooding** a system receives huge data volumes so that the normal data no longer *'get through'*.

**Service Flooding** services like IRC are flooded with so much data that they cannot process them.

**TCP/IP Crashing** by sending incorrect TCP/IP packets, the operating system routines are *'confused'* or the entire system traffic is disrupted. An example is the well-known Ping of Death.

**Service Crashing** the sending of unexpected data causes a system to crash or fail.

**DDoS – Distributed Denial of Service** DDoS is a type of DoS attack in which systems are synchronised in such a way that they simultaneously attack a single system and cause it to crash. This is used particularly in flooding attacks, where the accumulated total of the limited bandwidths of individual attackers exceeds the bandwidth available to

the victim and thus overloads the system.

**Dropper** Droppers are programmes which, particularly in the context of viruses and Trojan horses, smuggle malware into a system and install it there. They are usually disguised as meaningful and useful programmes to attract attention and lower resistance to their use.

**Exploit** In this context, it is used generally for the exploitation of programming or configuration errors in systems in order to gain access to them. Exploits subdivide into several major categories: Buffer Overflow, Directory Climbing, Defaults, Denial of Service.

**Hijacking** An attack where an attacker takes over one end of an authenticated network connection and may first *'nuke'* the other party. Since authentication usually only takes place at the start of a connection, the attacker can impersonate the original communication partner without any further security questions.

**Hacker** The term hacker is used in computer circles for someone who is so familiar with the *'insides'* of computers, information systems or

generally with certain technologies that he can manipulate processes according to his own wishes. A hacker is thus not always an *'intruder into computer systems'*, and not necessarily malicious. Malicious hackers are sometimes called crackers, while others use the term only for people who decode encrypted data or have specialised in breaking the copy-protection of programmes.

**Island Hopping** A process in which a system which has already been broken into is used as a basis (island) for attacking other systems.

**Keystroke Logging** Keystroke loggers are programmes which run in the background, unnoticed by the victim, and log the user's keyboard strokes. These records are then transmitted to the hacker who searches them for passwords or similar secret information.

**Malware** General term for any type of *'malignant'* software such as viruses, Trojan attacks, logic bombs etc.

**Man-in-the-Middle-Attack** A type of attack in which the attacker (for example in a network connection), inserts himself between the two parties in such a way that both think they are communicating with the desired partner – but in reality both sides are communicating with the man in the middle, who intercepts

and evaluates the captured data and possibly passes them on (unnnoticed) in altered form.

**Network Meltdown** Describes the crashing, or the state, of a network resulting from excessive data volumes. The cause is often an out-of-control Broadcast Storm. This can also occur if the bandwidth was too narrow for the data volume to be expected, and the required network connections are already overloading the infrastructure.

**Nuke** This term is used as a synonym for DoS in this context.

**Packet Filter** Packet Filters are programmes which scan data packets (usually TCP/IP packets) according to their origin (IP address, TCP port), their destination (target IP address, TCP port) and various data fields in the packet headers and discard them if their transmission or receipt is not wanted. Normally, these types of packet filter are part of a firewall infrastructure.

**Phreaking** Phreaking is the term used for all attacks on telecommunications systems.

**Sniffing** A sniffer is a programme that *'taps'* a data connection and spies on the data traffic on this connection in order to detect secret data such as passwords. This passive mode of attack requires direct access to the transmission medium

between the two parties to be spied on. This is relatively simple in LANs, since all computers are normally connected to an Ethernet or TokenRing cable.

**Social Engineering** This is an efficient, but often underestimated type of attack in which it is not so much a victim's computer, but rather their thoughts, characteristics and social environment that are exploited. It happens, for example, by guessing someone's password through trying out names in the victim's circle (friend, husband...). Since the same password is often used in different settings, one can often get easy access to many transactions. Social Engineering also includes the category where someone uses the victim's computer which was left *'open'* without password protection and prior logging off (lunch break or getting a cup of coffee are favoured situations).

**Spoofing** The name for a situation where someone pretends to be someone else or assumes their identity. Specifically in the network environment, this usually involves falsifying the sender's IP address in order to lead the recipient to believe that the sender is genuine. Spoofing is therefore usually associated with *'masqueraded clients'*. The reverse case – where a server pretends to be a different one and offers, for example, infected malware for downloading to unsuspecting clients instead

of the expected software – is just as worrying.

**Time Bomb** An expression for malware which activates its damaging function only after a certain period, or at a pre-set time.

**Trojan** A Trojan is a type of malware which hides a damaging function in a genuine-looking package (often in a useful programme). Its aim is to induce the victim to transfer the malware to their own computer and to start the *'useful'* programme.



Source: *'Internetworld'*



## WINDOWS-BASED CRYPTO SOLUTIONS: ALWAYS AT THE CUTTING EDGE



MATTHIAS HÄUSLER (LEFT) AND ADRIAN FUCHS TEST WINDOWS XP PROFESSIONAL FOR COMPATIBILITY WITH OUR SECURITY SOLUTIONS.

**Crypto AG has three Windows-based security solutions in its product range: VPN Encryption, PC Security and the combined solution PC Security and VPN Encryption. Great importance is attached to ensuring that the products always use state-of-the-art technology. After the Windows NT 4.0 and Windows 2000 versions, work is already underway on conversion to Windows XP Professional.**

Matthias Häusler


Windows XP was formally launched on the market on 25 October. With this

operability. However, Windows XP Professional also offers new functions, as for example remote support and remote desktop. Improvements in the support of these functions enable further cutting of administrative costs. In addition, Windows XP also has some improved features that allow increased productivity and offer user-friendly functions.

The new operating system was under discussion at Crypto AG long before its market launch. With Crypto solutions based on NT 4.0 and Windows 2000 already available, the change to Windows XP Professional is now being made, though the 'older' versions will continue to be available. Beta versions of Windows XP Professional were subjected to extensive tests at Crypto AG some time ago, and checked as to their compatibility with our security philosophy. Windows XP Professional-based encryption solutions by Crypto AG will thus be available on the market in a few months time. We are convinced that Windows XP Professional, with its well-functioning platform, is the operating system of the future and, particularly from the security aspect, forms the ideal base for our encryption solutions – for the benefit of our customers.

Windows XP Professional is used in altogether three Crypto solutions: PC Security, VPN Encryption and the security package PC Security and VPN Encryption. PC Security is the comprehensive, hardware-based security solution for Windows-based PCs. It offers confidentiality and integrity for local data and data stored on network servers. The same applies for e-mail or data transmission programmes.

The simple installation, configuration and administration mean very low support costs during integration and operation. VPN Encryption: With a Secure Virtual Private Network, you can communicate without fear via any public or private telecommunications network. World-wide, uncomplicated and completely secure. Whether you want to use an internationally accessible Wide Area Network (WAN) or develop a Local Area Network (LAN) for work groups within your organisation, the hardware-based Secure VPN System solution by Crypto AG

ensures the complete security of all your data communications. Encryption also guarantees the authentication of the communication, which means that nobody can enter the network by stealth. The PC Security and VPN Encryption package combines both solutions in one product. 

*If you have any questions regarding Windows XP Professional or our Windows-based encryption solutions, please contact our specialist: matthias.haeusler@crypto.ch*

Recommended

### 'Angewandte Kryptographie'

by Wolfgang Ertel

*Experts estimate that in Germany alone, losses to industry resulting from Internet espionage amount to at least DM 30 billion. But the German informatics expert, Professor Wolfgang Ertel, believes that by now, losses are quite likely to have reached the three-digit billion range.*

*'Awareness about data security simply does not exist yet', says Ertel and points to a scenario that ought to surprise both experts and lay people. After all, the European Parliament came to the unambiguous conclusion in July, after long and difficult investigations, that there can no longer be any doubt about the 'existence of a global spy network' which involves, in addition to the United States, also Great Britain, Canada, Australia and New Zealand. But the issue is not only the threat coming from Echelon, the surveillance system controlled by the National Security Agency and used successfully by the US technical secret service for industrial espionage.*

*According to STOA (Scientific and Technical Options Assessment of the European Union) major international*

*companies have also acquired a taste for spying and are busy copying the American model. For all these reasons, Wolfgang Ertel believes that there is a need for more action. The informatics professor, who has been giving lectures on the subject of data security since 1996, has now written a book which can be used by non-specialists in information technology to learn how to effectively encrypt their personal data with relative ease. In 'Angewandte Kryptographie', Ertel provides basic information about algorithms and protocols, and also deals thoroughly with cryptographic applications. Rather than being confronted with lots of mathematics, readers are given numerous examples and exercises. In addition, the author presents a wide range of current developments – as for example the Advanced Encryption Standard (AES) launched in summer 2001- and also deals with the headline-grabbing attacks on the Public Key System PGP and the crypto chip cards. Finally, in the three short chapters on 'Cryptography and eavesdropping attack', 'US export legislation' and 'sig-*

*nature law', Ertel looks at the current state of the political environment.*

*The disruptive actions referred to above have at least shown that security on the Internet is as rare as it is in real life. But that is not what matters to Ertel. His proposals cannot prevent industrial espionage and private attacks in every case, but they should at least help to make it as difficult as possible for the 'thief'. Ertel is convinced that 'by using appropriate encryption programmes, the effort becomes so great that an attack is no longer worth it.'*

*Wolfgang Ertel's book 'Angewandte Kryptographie' (ISBN 3-446-21549-2) is published by Hanser, 186 pages, and costs DM 39.80. (only German edition)*



## Trade Fairs/Exhibitions

Crypto AG will take part in the following trade fairs:

**CeBIT/Cefis Hannover 2002**  
**Hannover, from 13 – 20 March 2002**

**Defence Services Asia – DSA 2002**  
**Kuala Lumpur, from 8 – 11 April 2002**

Press review

### **Digital signature could be effective against e-mail viruses**

e-mail worms are currently causing huge damage and cost valuable working hours. According to a study, viruses have swallowed up resources world-wide worth 17.1 billion dollar in the year 2000 alone. But companies could protect themselves against viruses if they were to change to the digital signature, suggest management consultants Mummert + Partner. Worms often capture the address book in the mail-client in order to automatically spread to all those listed in it. 'By installing an electronic certificate on the work station, the e-mail systems can be configured in such a way that an electronic signature has to be used to send an e-mail', says Wilhelm Alms, chairman of the board of Mummert + Partner management consultants. It is a simple but effective protection against e-mail worms which unfortunately very few companies are using as yet. Large corporate networks, in particular, are affected, because viruses spread like wildfire via local e-mail programmes. Almost 99 per cent of e-mail worms are transmitted between staff members. One method of protection is to institute an electronic signature, without which no mail can be sent. Except for Netscape, all the commonly used e-mail clients support the use of the electronic signature. While e-mail worms can still intrude from outside, a stop is put on the automatic distribution of hundreds of copies of a hacker programme.

#### **Crypto AG, Head office**

Crypto AG  
P.O. Box 460  
CH-6301 Zug/Switzerland  
Phone +41 41/749 77 22  
Fax +41 41/741 22 72  
e-mail [crypto@crypto.ch](mailto:crypto@crypto.ch)  
[www.crypto.ch](http://www.crypto.ch)

#### **Crypto AG, Regional offices**

##### **Abidjan**

Crypto AG  
01 B.P. 5852  
Abidjan 01  
République de Côte d'Ivoire  
Phone +225/22 43 40 84  
Fax +225/22 43 32 75

##### **Abu Dhabi**

Crypto AG  
Regional Office Middle East  
P.O. Box 41076  
Abu Dhabi/UAE  
Phone +971 2/44 55 737  
Fax +971 2/44 55 151

##### **Buenos Aires**

Crypto AG  
Maipu 1256 PB "A"  
1006 Buenos Aires/Argentina  
Phone +54 11/4312 1812  
Fax +54 11/4312 1812

##### **Kuala Lumpur**

Crypto AG  
Regional Office Pacific Asia  
No. 2 Jalan SS7/11 Kelana Jaya  
47301 Petaling Jaya/Malaysia  
Phone +60 3/7872 2150  
Fax +60 3/7872 2140

##### **Riyadh**

Crypto AG Representative Office  
P.O. Box 59701  
Riyadh 11535  
Kingdom of Saudi Arabia  
Phone +966 1/454 1011  
Fax +966 1/454 9030

##### **Sultanate of Oman**

Crypto AG Representative Office  
P.O. Box 2911  
Postal Code 111  
Seeb  
Sultanate of Oman  
Phone +968 504 966  
Fax +968 504 929