Gustav LINDSTROM

Information Technology Security in the 21st Century: Implications for the EU

5 March 2004, EU Institute for Security Studies, Paris

Background

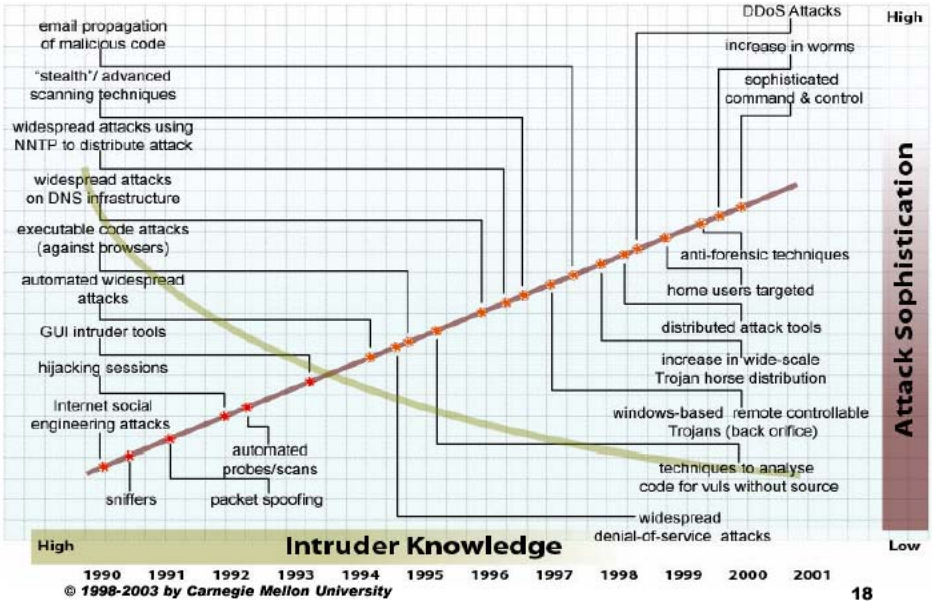
The purpose of this seminar was threefold. First, to highlight the potential security and safety risks to information technology (IT) infrastructures. Second, to explore and highlight the link between information technologies and the critical infrastructures that rely on them either directly or indirectly. Third, to reunite a group of analysts from across Europe with a wide variety of backgrounds and expertise in IT related issues to bring attention to the issue of IT security.

While threats are numerous, no catastrophic event has yet occurred

The initial sessions discussed potential threats to IT structures as well as the link between IT and critical infrastructures. A practical demonstration session showed how unauthorised individuals could compromise computers using a combination of viruses, worms, sniffing programs, etc. Weaknesses in word processing programs, email programs, and web browsers were similarly highlighted.

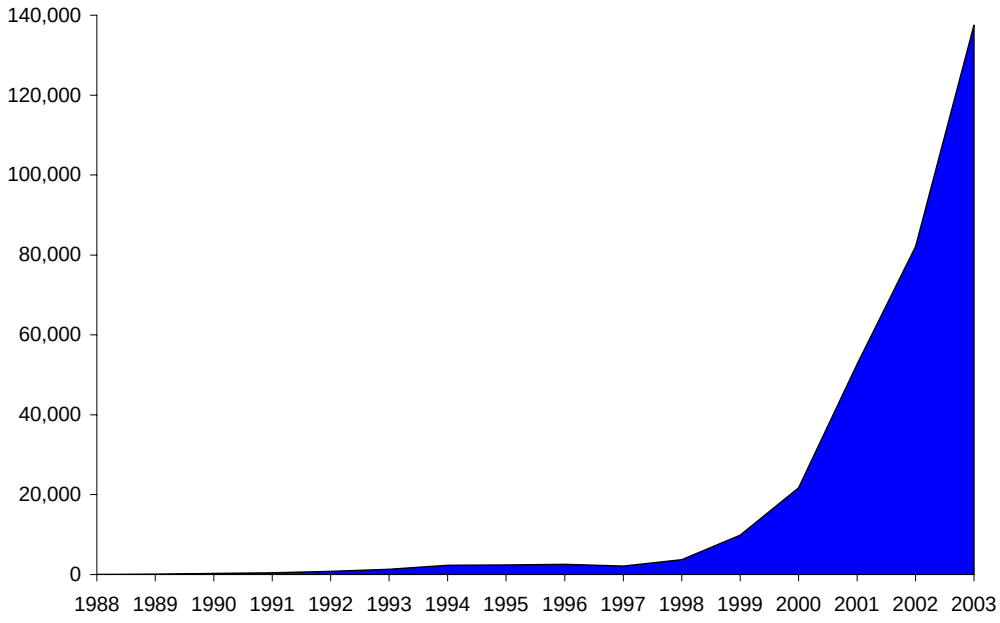
Concerning the threat, two trends are worth noting. First, while the sophistication of computer attacks are increasing, the knowledge required to carry them out is decreasing over time. Today, individuals and groups can free ride on previous knowledge and semi-automated programs to enhance the effectiveness of their attacks (see Figure 1).

Figure 1: Relationship between intruder knowledge and attack sophistication



Second, the number of computer attacks is growing exponentially if we look at the reported data spanning the last few years. As more and more computers are connected to the Internet (roughly 170 million), it is of little surprise that the number of attacks is growing (Figure 2).

Figure 2: Computer Incident reports 1988-2003



Source: CERT/CC Statistics online @ http://www.cert.org/stats/

The reliance on IT goes beyond individuals, corporations, and the public sector. Speakers noted that a number of critical infrastructures increasingly rely on IT to provide their services. Examples of such sectors include: telecommunications, finance, water, food, energy, transport, health services, and emergency services. Should the Internet be brought

down temporarily, the consequences on these critical infrastructures could be severe. Practical examples range from a loss of energy service to paralysed telephone networks. A cascading effect could eventually mire other sectors outlined above.

Given the relative ease of carrying out an attack – and the potential for significant ensuing damages – the question "why have we not seen anything yet?" was posed. Explanations ranged from the profile of attackers (youth trying to show their technical skills as opposed to terrorists with malicious intent) to the high impact visibility of bombs compared to IT attacks. Limited media interest in the potential consequences of an IT attack was also identified as a factor.

Speakers also covered the potential threats to IT stemming from monoculture and proprietary standards. It was noted that monoculture raises the risk level for information technology systems. In an industry characterised by a high degree of monoculture, an attack on the system's weaknesses can result in substantial impacts for a large number of end-users. From a different perspective, the possibility to affect a large number of users may entice attackers to look for specific vulnerabilities in systems that benefit from a large proportion of the market share.

Managing IT threats requires a multipronged approach

Speakers noted that a managing the threats to IT infrastructures requires various strategies. Examples range from obtaining a better understanding of the threat and its consequences to harmonising legislation.

Concerning the risks associated with IT attacks, a speaker noted that more quantitative studies are needed to attain a better understanding of the risks and effects of an IT structure attack. Such studies would allow IT users to be more strategic when deciding on the level of resources required to effectively manage the risks. For example, costs arising from computer viruses tend to be estimated on an ad-hoc basis using a number of different methodologies, making it difficult to obtain comparable estimates. Furthermore, many such estimates may fail to acknowledge substantial non-quantifiable costs (e.g. negative externalities).

Vis-à-vis legislation, the global nature of the risk requires that countries work together to harmonise their laws to minimise the number of loopholes available to eventual attackers. Recent initiatives include the Council of Europe's convention on cybercrime (to be ratified), the OECD's guidelines for the security of information systems and networks, the United Nation's resolutions on cybersecurity, and the G-8's Groupe de Lyon.

Related to the measures above is the need to increase awareness at all levels. Speakers underlined that individuals increasingly need to obtain proper training and awareness—from an early age on forward—to minimise the risks to users worldwide. The same goes for companies and government agencies and their staff. Speakers highlighted a number of practical measures such as:

- Ensuring security as an integral part of any training and education program concerned with IT
- Defining and agreeing on a role for the media
- Developing new analytical methods and tools to raise awareness (e.g. through the use of exercises)

- Strengthening international cooperation regimes and standards

With respect to the commercial sector, a speaker noted that most European companies have devoted few resources to boost IT security levels. Among the more telling statistics from 2002 are:

- 75% of European companies had no security strategy
- IT security investments in Europe touched 5 billion dollars (up 25% from 2001), i.e. only 1.8% of the overall IT investments

Balancing national and EU policies

Information security policies exist both at the national and EU level. Speakers noted that while national information security policies tend to trace their origins to their historical heritage and needs, EU level policies are driven by efficiency, competitiveness, and coordination requirements. This discrepancy in starting points makes it difficult to find a balance between national and EU policies. Moreover, a comparison of national level measures shows substantial intra-European differences. For example, agencies responsible for information security within EU member states usually differ in terms of organisation, staff size, ministerial links, and association levels with other national institutions handling similar issues.

At the EU level, information security policies are largely anchored to growth and efficiency programmes such as the Lisbon strategy and the Europe programme. The European Commission is currently managing a €70 million budget to enhance the security of information infrastructures. Present priorities include the enhancement of security standards/certification mechanisms, improvement of security practices, protection of networks, and increased resources for security RTD. Looming around the corner is the establishment of the European Network and Security Agency (ENISA). ENISA will ensure a high and effective level of network and information security and develop a culture of network and information security.

List of Participants

Information Technology Security in the 21st century:
Implications for the EU

EU Institute for Security Studies, Paris 5 March 2004

Carlos **BRAVO BALMORI –** Attaché, Ambassade du Royaume d'Espagne, Paris

Laurent **CABIROL** – Project Officer, DG Information Society "Security Research", European Commission, Brussels

Martin **DAVIS** – Outreach Team, National Infrastructure Co-ordination Centre, London

Gilles **DE LABAREYRE** – Security Business Manager, BV Public Safety, EADS Telecom, St. Quentin Yvelines

Edgar **DE LANGE –** Senior Policy Advisor Security, Ministry of Economic Affairs, The Hague

Malin **FYLKNER –** Researcher, Project Manager, Division of Defence Analysis, FOI, Stockholm

Gebhard **GEIGER –** Research Fellow, Stiftung Wissenschaft und Politik, Berlin

Nicole **GNESOTTO –** Directeur, Institut d'Etudes de Sécurité de l'Union européenne, Paris

Jaime **GOTOR** – Deputy Director Assistant, Centro Cryptológico Nacional, Ministry of Defence, Madrid

Reinhard **HUTTER** – Senior Vice President, IndustrieAnlagen-BetriebsGesellschaft mbH, Ottobrunn

Gustav **LINDSTROM –** Research Fellow, European Union Institute for Security Studies, Paris

Eric **LUIIJF –** Principal Consultant INFOSEC & CIP, TNO Physics and Electronics Laboratory, The Hague

Bartolomeo **MANENTI –** Head of Division INFOSEC, Secretariat General of the Council of the European Union, Brussels

Antonio **MISSIROLI** – Chargé de recherche, Institut d'Etudes de Sécurité de l'Union européenne, Paris

Xavier **PASCO –** Maître de recherche, Fondation pour la Recherche Stratégique, Paris

Jean-Pierre **QUEMARD –** Chief Security Officer, EADS Telecom, St. Quentin Yvelines

Hanno **RANCK** – Head of IT Department, European Union Institute for Security Studies, Paris

Burkard **SCHMITT –** Assistant Director, European Union Institute for Security Studies, Paris

Isabelle **WIGERT –** Researcher CIIP Project, Center for Security Studies, Swiss Federal Institute of Technology, Zurich

Richard **YOUNG –** EU Desk Officer, CESG International Relations, Communications-Electronics Security Group, Cheltenham

There were also a number of participants from the SGDN.

Observers

*Timo **BEHR*** – German Intern, EU Institute for Security Studies, Paris

*Elisabeth **DIETL*** – German Research Award Holder, EU Institute for Security Studies, Paris

*Rem **KORTEWEG*** – Dutch Research Award Holder, EU Institute for Security Studies, Paris

*Lada **PARIZKOVA*** – Czech Research Award Holder, EU Institute for Security Studies, Paris

*Laura **SALICH*** – Italian Intern, EU Institute for Security Studies, Paris

Seminar on Information Technology Security in the 21st century: Implications for the EU

5 March 2004

First session: Why should we care about IT security?
Chair: Nicole **GNESOTTO**
IT infrastructures as platforms for attacks
Participant from SGDN
Potential spill over effects (critical infrastructure)
Martin Davis, Outreach Team, National Infrastructure Co-ordination Centre (NISCC)

Second Session: Information security (Infosec) vulnerabilities
Chair: Burkard Schmitt
Threats to the IT backbone
Gustav Lindström, Research Fellow, EUISS
Risks posed by "monoculture" and proprietary standards
Jean Pierre Quemard, Chief Executive Officer, EADS Telecom

Third Session: Managing threats to IT infrastructures
Chair: Gustav Lindström
Criteria and strategies for an effective IT-security risk management
Gebhard Geiger, Research Fellow, Technische Universität München & SWP
Legal measures
Participant from SGDN
Public awareness measures
Reinhard Hutter, Senior Vice President InfoCom, Industrieanlagen-Betriebsgesellschaft mbH (IABG)

Fourth Session: IT security in Europe - current and future steps
Chair: Gustav Lindström
National and EU level policies to counter IT threats
Participant from SGDN
Implications for CFSP/ESDP
Bartolomeo Manenti, Head of Division Infosec, Secretariat General of the Council of the European Union
Towards an effective EU policy
Laurent Cabirol, Project Officer, DG Information Society, European Commission

End of seminar