VIENNA DECLARATION

On Wireless Local Area Networks (WLANs)

Conference on Security in Wireless Local Area Networks

European Academy of Sciences and Arts (EASA), Mönchsberg 2, A-5020 Salzburg, Tel: +43/662/ 84 13 45, Fax: +43/662/ 84 13 43

*office@european-academy.at; presidential.office@european-academy.at;
http://www.european-academy.at/de/index.html*

Abstract: In October 2003 the European Academy, together with Österreichische Nationalbank, held a conference on Security in Wireless Local Area Networks (WLANs). During this conference, speakers, members of the audience and organisers agreed upon recommendations regarding WLAN usage and implementation. In light of the rapidly increasing acceptance and use of WLANs, the European Academy of Sciences and Arts seeks to ensure that security risks arising from these open networks and the lack of security standards do not increase accordingly. The areas concerned are: technological security, security management, legal security and privacy awareness.

Key words: legal security, open networks, privacy, security risks, technological security, wireless

INTRODUCTION

In October 2003 the European Academy, together with Österreichische Nationalbank, held a conference on Security in Wireless Local Area Networks, chaired by Dr. Hellmuth Broda, EASA/Sun Microsystems. During this conference, speakers, members of the audience and organisers agreed upon the following recommendations regarding WLAN usage and implementation. In light of the rapidly increasing acceptance and use of Wireless Local Area Networks (WLANs), the European Academy of Sciences and Arts seeks to ensure that security risks arising from these open networks and the lack of security standards do not increase accordingly (for details on individual presentations see the « Downloads » link at <http://www.europeanacademy.at>).

TECHNOLOGICAL SECURITY

- a) New security standards will have to be defined by the industry (see standards set by personal area networks such as Bluetooth).
- b) Before a wireless network is implemented, its necessity should be questioned in the light of today's security issues. Upon its implementation, accurate event log files are vital to security and for tracing security gaps.
- c) For the user, seamless connectivity irrespective of the connection protocol (e.g. WLAN and UMTS) is desirable.
- d) Ease of use: researchers and developers are called upon to make their products as easily accessible and understandable for their users as possible, without sacrificing security.
- e) Users should be encouraged to acquire a certain degree of technical competence and knowledge of the underlying physics (e.g. optimal positioning of antennae) in order to be able to make informed security decisions. A European Security Certificate for users would be worth considering.

SECURITY MANAGEMENT

- a) Security is achieved through products: security is a continuous management process. The entire communication/data path needs to be made secure; the security of a system is determined by its weakest link.
- b) Trust management builds upon security management. Both need to be seen as ongoing, continuous processes, and approached in a methodical,

inclusive way. Transparent policies on data protection and handling will add to users' trust. Audits and quality seals can play an important role in this process.

- c) The awareness of both users and providers regarding security concerns must be heightened, and a sustained framework for quality created.
- d) Management concepts must be inclusive, taking behavioural, legal, social, organisational, technical and economic aspects into account.

LEGAL SECURITY

- a) A comprehensive analysis of the legal aspects and implications of WiFi based on requirements (e.g. Basel II) regarding IT infrastructure is urged.
- b) Legislative reforms should not be made without careful consideration. Should they be necessary at all, new regulations should be created in a minimalist fashion.
- c) Laws concerning network and data security must be clarified and interpreted, and should converge on a European level.

PRIVACY AND AWARENESS

- a) Management of authentication and confidentiality should be seen as key factors for overall security. In order to more effectively protect privacy and confidentiality, further research with the goal of heightening security must be encouraged and supported by the private and public sector (e.g. by the European Commission).
- b) Education in security know-how and awareness should be incorporated into school and university curricula.
- c) Widespread acceptance of WLANs depends in part on the cost structure for usage, which today is often prohibitive.
- d) Ethical behaviour should be promoted and integrated into everyday use. Legal stopgaps and regulations are not sufficient.

COMPREHENSIVE, INTERDISCIPLINARY APPROACH

The conference agreed that only a comprehensive approach and ongoing interdisciplinary co-operation will enable us to build trust and confidence in wireless network technology.