



CONGRESS HIGHLIGHTS

Ausgabe 7 / November 2003

Sicherheit in Wireless LANs - Technologiefortschritte erfordern Umdenken im Datenschutz

Die Vorteile, die Wireless LANs ihren Nutzern bieten, sind unbestritten. Doch wie hoch ist der Preis der erhöhten Mobilität und Flexibilität? Wie sicher sind kabellose Netzwerke? Durch welche technische, rechtliche und sozioökonomische Maßnahmen kann diese Sicherheit gesteigert werden, und mit welchen Kosten sind diese verbunden? Diesen Fragen widmeten sich am 13. Oktober IT-Experten, Wissenschaft-

ter und Forscher, Wirtschaftsfachleute und Juristen im Rahmen der Tagung Sicherheit in Wireless LANs - Technologiefortschritte erfordern Umdenken im Datenschutz, welche die Europäische Akademie der Wissenschaften und Künste gemeinsam mit der Oesterreichischen Nationalbank veranstaltete. Durch die unterschiedlichen Fachgebiete und Blickwinkel der Konferenzteilnehmer und Referenten war es möglich,



eine Vielzahl unterschiedlicher Aspekte der Sicherheit und Wege, diese zu verbessern, herauszuarbeiten, von der Rolle eines umfassenden Sicherheitsmanagements und -bewußtseins bis zur unbestrittenen Notwendigkeit weiterer Forschung auf diesem Gebiet. ■

Security in Wireless LANs - Technological Progress Necessitates New Approaches in Data Protection

The advantages offered by wireless LANs are clear, but what is the price of greater mobility and flexibility? How safe are wireless networks? By what technical, legal and socioeconomic means can their security be increased, and at what cost? These questions were examined on October 13 by scientists, researcher and experts in the fields of IT, economics and law at the conference Security in Wireless LANs - Technological Progress Necessitates New Ap-

proaches in Data Protection, jointly organized by the European Academy of Sciences and Arts and Oesterreichische Nationalbank. Thanks to the varying fields points of view of the conference participants and speakers, it was possible to include a broad range of issues affecting security and its enhancement in the discussion, ranging from the role of security management and awareness to the undeniable need for additional research in this area. ■

Technologische Sicherheit - Die Rolle von sicheren Identitäten in Wireless LANs

Als erster Redner wies Günther Hruby (Siemens AG) darauf hin, daß erfolgreiche Versuche, Funksignale abzuhören oder in kabellose Netzwerke einzudringen, gezeigt haben, daß bereits implementierte Sicherheitsstandards weiter verbessert werden müssen. Hruby demonstrierte, daß Verschlüsselung in höheren Protokollschichten jedoch nicht genügt; vor allem die lower level security müsse untersucht und verstärkt werden.

Auch Sahin Albayrak (Technische Universität Berlin) verwies auf die speziellen Sicherheitsprobleme, die Wireless LANs mit sich bringen. Die Broadcast Eigenschaft kabelloser Netzwerke ermögliche einen relativ einfachen Zugriff von außen; die Kontrolle des Netzzuganges sei schwierig. Die Integration von Public Key Infrastruktur-Funktionalitäten sei eine wichtige Maßnahme, die die Sicherheit von Wireless LANs erheblich steigern könne.

Heinz Thielmann (Fraunhofer Institute of Secure Telecooperation SIT) verdeutlichte die Notwendigkeit weiterer Forschung auf diesem Gebiet. Real time security auditing, mobile privacy protection und intrusion detection, sowie seamless secure connectivity stellen Forscher vor große Herausforderungen; diese müssen jedoch rasch bewältigt werden, um das Vertrauen in die neue Technologie zu stärken. ■



G. Hruby, J. Avellan, H. Thielmann, H. Broda
(von links nach rechts)

EDITORIAL



The introduction of new technology such as wireless LANs opens up a broad vista of new possibilities, and can lead to great benefits for society as a whole. Progress and innovation, however, often are accompanied by the potential for abuse, and we must ensure that wireless networks and the data therein are adequately protected from such misuse.

Devising and implementing adequate safeguards in wireless LANs is not only a technological question, but must be viewed from legal and social vantage points as well. Additionally, security measures must not undermine the freedom granted by such networks. Finding the right balance between this freedom and the undeniable need for security will present a significant challenge, yet by approaching the subject in an interdisciplinary manner, I am convinced that a solution can be found, and that wireless LANs will become an integral and safe part of our information-based society.

Felix Unger
President of the European Academy of Sciences and Arts

Technological Security - The Role of Secure Identity in Wireless LANs

The day's first speaker, Günther Hruby (Siemens AG), pointed out that successful attempts to eavesdrop on wireless signals or to penetrate wireless networks have shown that existing security standards must still be improved upon. Hruby noted that encryption in higher protocol levels is not sufficient; above all, lower level security must be analyzed and strengthened.

Sahin Albayrak (Technische Universität Berlin) also focused on the specific secu-

rity problems of wireless LANs. The broadcast characteristic of wireless networks makes it relatively easy to gain access from outside; controlling network access is difficult. The integration of public key infrastructure functionalities is an important step toward enhancing the security of wireless LANs.

Heinz Thielmann (Fraunhofer Institute of Secure Telecooperation SIT) stressed the need for further research in this field. Real time security auditing, mobile privacy protection and intrusion detection,

"Critical business applications and privacy problems require urgent security solutions. Otherwise, growth of all mobile applications (WLANs, UMTS, etc.) could rapidly downturn into a longterm resistance of users. International policies and guidelines for mobile security may help to avoid such risks."

Heinz Thielmann
(Fraunhofer Institute of Secure Telecooperation SIT)

and seamless secure connectivity pose great challenges for researchers; these, however, must be mastered swiftly in order to heighten trust in this new technology. ■

Sicherheitsmanagement - Sicherheit ist ein kontinuierlicher Prozeß und beruht nicht nur auf Produkten

Die Sicherung von Identitäten sei das wichtigste Element in der Beziehung zu Kunden, betonte Hellmuth Broda (Sun Microsystems). Identitätsmanagement sei essentiell, um Vertrauen aufzubauen und werde künftig ein nichtwegzudenkender, allgegenwärtiger Bestandteil unseres Umgangs mit Datennetzwerken sein. Erworbenes Vertrauen könne aber nicht allein durch konsequente Sicherheitsmaßnahmen erhalten und gehegt werden; klare, verständliche Sicherheitspolitik, die einem regelmäßigem Auditing unterzogen wird, und gezieltes Trust Management seien ebenso unerlässlich.

Ingrid Schaumüller-Bichl (IT-Sicherheitsberatung) bezeichnete Sicherheitsmanagement als kontinuierlichen Prozeß, der methodisches Vorgehen verlangt mit der Zielsetzung, ein angemessenes Sicherheitsniveau im Unternehmen zu etablieren. Nicht nur Risikoanalyse und daraus resultierende organisationsweite Sicherheitsmaßnahmen seien unumgänglich, um ein angemessenes Sicherheitsniveau zu erreichen und aufrecht erhalten zu können, sondern auch

Risikomanagement und gezielte Nachfolgeaktivitäten.

Im Bereich des Sicherheitsmanagements sei es wichtig, erklärte Gerhard Donner (Moore Stephens Austria Consulting GmbH) in seiner Präsentation, die optimale Balance zwischen Nutzen, Kosten und Risiko zu finden. Vertrauensverluste als Folge von Sicherheitslücken können für Unternehmen ebenso schwerwiegende Folgen haben wie finanzielle

„Die bisher ergriffenen, meist sehr technisch orientierten Maßnahmen reichen allein nicht für eine wirklich wirksame Sicherung und Kontrolle aus - es bedarf auch und vor allem der Berücksichtigung sozialer, psychologischer, rechtlicher und ökonomischer Aspekte.“

Gerhard Donner
(Moore Stephens Austria Consulting GmbH)

Einbußen; vor allem durch gesteigerte Bewußtseinsbildung sei es möglich, viele dieser Lücken zu schließen. ■



H. Broda, I. Schaumüller-Bichl, G. Donner, (von links nach rechts)

Security Management - Security is a Constant Process and does not only Stem from Products

Hellmuth Broda (Sun Microsystems) stressed that securing identities is the most important element of the relationship to customers. In order to build trust, identity management is essential, and will become an integral omnipresent part of our use of data networks. Acquired trust must, however, be retained and nurtured not only by means of security measures, but through clear policies and focused trust management.

Ingrid Schaumüller-Bichl (IT-Sicherheitsberatung) characterized security management as an ongoing process that must be approached in a methodical manner. Not only risk analysis and resulting organizationwide security measures are indispensable, but also risk management and targeted follow-up activities.

In the field of security management, finding the correct balance between benefits, costs and risks is essential, as

"Today's acceptance of web-based services is hampered by the lack of consumers' trust in the system. They are not sure who is 'on the other side,' who they are talking to, and who does what with their data and personal information."

Hellmuth Broda
(Sun Microsystems)

Gerhard Donner's (Moore Stephens Austria Consulting GmbH) presentation showed. Loss of trust resulting from security leaks can be just as detrimental as financial losses; by heightening awareness, however, many of these leaks may be closed. ■

Rechtliche Sicherheit - Wie rasch finden sich technologische Entwicklungen in gesetzlichen Regelungen wieder?

Georg Lechner (Österreichische Datenschutzkommission) analysierte die derzeit in Österreich geltenden Rechtsgrundlagen, die Datenschutz in technologischen Umgebungen sichern sollen, und stellte fest, daß einige Fragen, vor allem im Bereich der Haftung, noch nicht restlos geklärt seien. Einige Änderungen, zum Beispiel die besondere Berücksichtigung von kleinen Auftraggebern, die nicht über IT-Abteilungen verfügen, seien denkbar.

Karl Anton Fröschl (ec3) mahnte zur Vorsicht bei der Erschaffung neuer Gesetze, um auf neu entstandene Technologien zu reagieren. Der Gesetzgeber müsse nicht nur die Frage stellen, ob bereits vorhandene Regelungen ausreichen, um Datenschutz und die Rechte aller Teilnehmer zu gewährleisten, sondern eben-

so hinterfragen, ob neue rechtliche Maßnahmen angesichts der neuen technischen Möglichkeiten auch durchgesetzt werden können.

Auch Andreas Wiebe (Wirtschaftsuniversität Wien) forderte eine vorsichtige Analyse der Folgen der Anwendung einer neuen Technik für rechtlich geschützte Güter und Werte vor der Einführung neuer Gesetze. Stärkere Datensicherheit müsse außerdem ein gemeinsames Interesse aller Beteiligten sein. Vor allem eine technische Standardisierung auf hohem Niveau sowie ein erhöhtes Risikobewußtsein von sowohl Nutzern als auch Anbietern können dazu beitragen, die Sicherheit von Wireless LANs zu erhöhen.

Vor allem Unklarheiten in bestehenden Gesetzen müssen beseitigt werden, erklärte Juan Avellan (Wisekey). Eine Vielzahl von Fragen seien noch ungeklärt, die



G. Lechner, K. Fröschl, A. Wiebe, S. Albayrak
(von links nach rechts)

von der Legalität, Netzwerke zu suchen bis hin zur Verantwortung von Hard- und Softwareherstellern reichen. Die potentiellen Auswirkungen der neuen Technologie müssen noch aus einer Vielzahl von Perspektiven analysiert werden, um Bereiche, wo Reformen notwendig sind, zu identifizieren, und vor unangenehmen Überraschungen zu schützen. ■

Legal Security - How Quick are Technological Developments Reflected in Legal Regulations?

Georg Lechner (Österreichische Datenschutzkommission) analyzed the current legal framework designed to ensure data protection in technological environments in Austria, and noted that several questions, particularly involving liability, are not yet fully clarified. Several changes, for instance giving special consideration to small principals without separate IT divisions, are conceivable.

Karl Anton Fröschl (ec3) advised caution when creating new laws as a reaction to new technologies. Lawmakers must not only ask whether already existing regulations are a sufficient means of guaranteeing data protection and the rights of all parties, but also question whether new

legal measures can be enforced in light of new technical possibilities.

Andreas Wiebe (Vienna University of Economics and Business Administration) also called for a cautious analysis of the implications of the use of a new technology on legally protected goods and values before introducing new laws. Increased data security must also be a common interest of all involved parties. Above all, technical standardization at a high level and increased risk awareness of both users and providers can contribute to improved security in wireless LANs.

Above all, declared Juan Avellan (Wisekey), lack of clarity in existing laws must be dealt with. A multitude of questions still need clarification, ranging from

the legality of detecting networks to the responsibilities of hardware and software manufacturers. The potential repercussions of new technology must still be analyzed from a variety of perspectives in order to identify areas in need of reform and to protect against unforeseen negative effects. ■

"The legal aspects of Wifi are quite diverse and can be complex. Upon analyzing Wifi from different legal perspectives, many issues arise, from the regulatory aspects of radio spectrum licensing, privacy, data protection and service legal provision to cybercrime, employment law, and sector-specific legal compliance issues."

Juan Avellan
(Wisekey)

Freier Zugang für alle? - Modelle zur Berechnung der Kosten von sicherem Zugang zu Wireless LANs

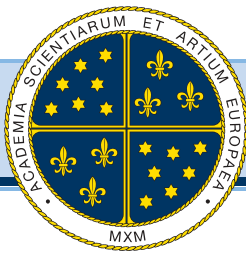
Anwendungen von Wireless LANs seien zwar in einigen Bereichen bereits erfolgreich realisiert, und die Voraussetzungen für weitere, visionäre Services seien gegeben, erklärte Matthias Rudowicz (UTA Telekom AG). Damit diese jedoch erfolgreich realisiert werden können müssen allerdings nicht nur technische Sicherheitsrisiken beseitigt werden, sondern ebenso kommerzielle.

Sicherheitsrisiken stellen zweifellos eine Hürde für eine breite Akzeptanz

der Technologie dar, sagte Hannes Stiebitzhofer (metronet copperoptics gesmbH), andererseits werden gerade durch das gesteigerte Sicherheitsbewußtsein der Benutzer erhöhte Sicherheitsmaßnahmen eingefordert. Diese Maßnahmen müssen jedoch einfach handhabbar sein, ohne große technische Anforderungen an den einzelnen User zu stellen.

Den vollständigen Text des Vienna Memorandums, welches aus der Diskussion von Konferenzteilnehmern und Referenten entstanden ist und Empfehl-

ungen für eine weitere Erhöhung der Sicherheit in kabellosen Netzwerken enthält, finden Sie auf der letzten Seite dieser Congress Highlights sowie als Download auf der Homepage der Europäischen Akademie unter <<http://www.european-academy.at/client/download.html?lang=de>>. Auf dieser Web Site finden Sie ebenso sämtliche Präsentationen dieser Tagung als Downloads. ■



Free Access for All? - Models for Calculating the Costs of Secure Access to Wireless LANs

Wireless LAN applications have already been realized successfully in several areas, and the conditions for additional visionary services are in place, said Matthias Rudowicz (UTA Telekom AG). For these to be successfully realized, however, not only technical, but also commercial security risks must be eliminated.

Security risks are undoubtedly an obstacle blocking a broad acceptance of the technology, said Hannes Stiebitzhofer (metronet copperoptics gesmbH); on the other hand, users' increased security

awareness leads to greater demand for heightened security measures. These measures must, however, be easy to use, without great technical demands on individual users.

The complete text of the Vienna Memorandum, created through discussions between conference participants and speakers and comprised of recommendations for further enhancing the security in wireless networks, is included on the final page of these Congress Highlights and can also be downloaded at the homepage of the European Academy under <<http://www.european-academy.at/client/download.html?lang=de>>. This web site also contains all presentations from this conference in a downloadable format.

www.european-academy.at/client/download.html?lang=de>. This web site also contains all presentations from this conference in a downloadable format.



H. Broda, M. Rudowicz, H. Stiebitzhofer, H. Schindler
(von links nach rechts)

Vienna Memorandum on "Security in Wireless Local Area Networks (WLAN, WiFi)"

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. For details on individual presentations from the Conference Security in Wireless LANs (Oesterreichische Nationalbank, October 13, 2003) during which this Memorandum was composed, see the "Downloads" link at www.european-academy.at.

1. Technological Security

- i. New security standards will have to be defined by the industry (see standards set by personal area networks such as Bluetooth).
- ii. Before a wireless network is implemented, its necessity should be questioned due to today's security issues. Upon its implementation, accurate event log files are vital to security and for tracing security gaps.
- iii. For the user, seamless connectivity irrespective of the connection protocol (e.g. WLAN and UMTS) is desirable.
- iv. 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.
- v. 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.

2. Security Management

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

3. Legal Security

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

4. Privacy and Awareness

- i. 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).
- ii. Education in security know-how and awareness should be incorporated into school and university curricula.
- iii. Widespread acceptance of WLANs depends in part on the cost structure for usage, which today is often prohibitive.
- iv. Ethical behaviour should be promoted and integrated into everyday use. Legal stopgaps and regulations are not sufficient.

Only a comprehensive approach and ongoing interdisciplinary co-operation will enable us to build trust and confidence in wireless network technology. Vienna, October 13th 2003

For additional information, please contact the chairman of the conference:
Dr. Hellmuth Broda
Sun Microsystems Inc.
Elisabethenanlage 11
4051 Basel, Switzerland
Hellmuth.Broda@Sun.Com