Mobile Security

Projektleiter
Prof. Dr.-Ing. Evren Eren

Forschungsschwerpunkt
Mobile Business
Mobile Systems

Kontakt
Prof. Dr.-Ing. Evren Eren
Fachbereich Informatik
Fachhochschule Dortmund
Emil-Figge-Straße 42
44227 Dortmund
Tel.: (0231) 755-6776
E-Mail: eren@fh-dortmund.de

Forschungsschwerpunkt „Mobile Security“
Im Rahmen des Forschungs- und Entwicklungsschwerpunktes „Mobile Business & Mobile Systems“ hat sich Prof. Eren mit dem Themenspektrum „Mobile Security“, d.h. mit den Sicherheitsaspekten der Mobilkommunikation, von mobilen Anwendungen und Diensten sowie Infrastrukturen auseinandergesetzt. Das breite Themenspektrum umfasst u.a. die Sicherheit von Wireless LAN (WLAN), Bluetooth, WiMAX, GSM/GPRS/EGDE, UMTS, mobilem Voice-over-IP, Mobile IP.

Hintergrund „Mobile Security“
Immer mehr innovative und moderne Unternehmen optimieren ihre Geschäftsprozesse durch nahtlose Erweiterung Ihrer IT-Infrastruktur, um dem steigenden Bedarf an Flexibilität und Mobilität nachzukommen. Mitarbeiter werden zusehends mit mobilen Geräten ausgestattet, damit sie auf Unternehmens-, Kunden- sowie andere prozessspezifische Daten unabhängig von Ort und Zeit zugreifen können. Wesentlicher Gewinn dabei ist die Optimierung der Koordination von Geschäftsprozessen und Workflows im Hinblick auf Produktivitäts- und Qualitätssteigerung.

Dieser Trend und damit der Grad der Nutzung von mobilen Anwendungen sowie der Datenaustausch über mobile Kommunikationsnetze werden in den nächsten Jahren stark zunehmen. Fest-, Mobil- und Funknetze verschmelzen zu einer Kommunikationseinheit. Einher mit dem steigenden Nutzungsgrad gehen erhöhte Anforderungen an die Sicherheit, die denen jedoch nicht zufriedenstellend begegnet wird. Gefordert werden nahtlose und durchgängige Sicherheitsmechanismen von der Anwendung im mobilen Endgerät bis zur Gegenstelle; d.h. Verschlüsselung, Autorisierung und Authentifizierung über komplexe Prozessketten wie z.B. „Mobiles Endgerät -› Mobiler Übertragungskanal (Luftschnittstelle) -› Netzwerkverbindung und Netzwerkübergang -› Internet oder Intranet -› Backendsysteme wie Server und Anwendungen bzw. Services. Während bei Mobilkommunikationsstandards wie GSM, GPRS und UMTS eine Verschlüsselung der Daten erfolgt, so lange sie über die Funkschnittstelle übertragen werden, liegen nach Verlassen dieser Netze die Daten offen. Für eine Ende-zu-Ende-Sicherheit muss demnach zusätzlich gesorgt werden.

Obgleich das Thema IT-Sicherheit bereits seit Jahren eine hohe Sensibilisierung bei Unternehmen unterschiedlichster Größenordnung erfahren hat, sind Entscheider verhalten, wenn es um den Einsatz von Mobiler Sicherheit geht. Dieser Sachverhalt verwundert, da im klassischen IT-Sicherheitsbereich mittlerweile ausreichend Erfahrungen vorliegen sollten, um ähnliche Fehler und zögerliche Haltung zu wiederholen. Viele Beispiele verdeutlichen dies im Einsatz von mobilen Endgeräten wie Handys, Smartphones, Organisern, PocketPCs oder PDAs im geschäftlichen Bereich. Ungesicherte WLAN- und Bluetooth-Verbindungen bzw. Konfigurationen öffnen Türen und Tore für Angreifer und kompromittieren die Integrität von geschäftlich signifikanten Daten.

Mobile Endgeräte werden in unsicheren Umgebungen betrieben und sind damit einem höheren Angriffspotenzial ausgesetzt als Computer in Büroumgebungen. Sie sind mit immer mehr Schnittstellen für die drahtlose Kommunikation wie WLAN, Bluetooth, IrDA ausgestattet. Unkontrollierte private Nutzung der mobilen Geräte (z.B. Downloads, Emails) sowie der Verzicht auf die notwendigen Sicherheitsvorkehrungen verwandeln mobile Geräte einfach und schnell zur gefährlichen Hintertür in sonst gewissenhaft geschützten IT-Umgebungen. Sicherheitstechnisch weisen PDAs und Mobiltelefone den Stand der ersten vernetzten Systeme in den 80er Jahren auf.

Die Verbreitung von Sicherheitsrisiken und Angriffspotentialen (wie z.B. Viren, Trojaner, Würmer, Spyware und Bluejacking) löst selten ausreichende Besorgnis und entsprechendes Handeln in Unternehmen und Organisationen aus. Man kann festhalten, dass der Grad der Sensibilisierung für das Thema „Mobile Sicherheit“ de facto nicht ausreichend vorhanden ist und bei den wenigen, die dieses thematisieren, sind strategische und technische Maßnahmen zur Eliminierung bzw. Reduktion von mobilen Sicherheitsrisiken nicht nachhaltig erkennbar. Wesentliche Hemmfaktoren für viele Unternehmen, insbesondere kleine und mittelständische (KMU), sind finanzielle Gründe, Unsicherheit oder fehlendes Wissen. Es wird sogar die Meinung vertreten, dass mobile Sicherheit durch allgemeine IT-Sicherheitslösungen automatisch mit abgebildet wird.

Mobile Sicherheit ist für ein breites Spektrum an Anwendungen und Infrastrukturen von Bedeutung. Diese sind u.a. Mobile Commerce und Business, Location Based Services, Mobile Payment, Mobile Gaming, Mobile Brokerage, Drathlose Internet Service Provider, Notebook University, RFID, Gesundheitskarte, Maut, digitaler Personalausweis, viele mehr. Ziel der zukünftigen „Mobilen

Sicherheit“ ist der Einsatz von Cross-Network und Cross-Device, d.h. Anwendungsorientierter Sicherheit – unabhängig vom Anwendungsumfeld.

Forschungsarbeiten und erzielte Ergebnisse
Flankiert durch diverse Bachelor und Diplomarbeiten wurden typische mobile IT-Anwendungen sowie mobile Kommunikation systematisch untersucht und vor dem Hintergrund der Sicherheit analysiert und bewertet. Anhand zahlreicher Beispielimplementierungen wurde aufgezeigt, wie sich diese Risiken mit geeigneten Konzepten, Strategien und Lösungen beseitigen lassen. Darauf basierend wurden zahlreiche Strategieempfehlungen, Planungshilfen und Implementierungsanleitungen erarbeitet.

Ein Auszug der relevanten Bachelor und Masterarbeiten wird im Folgenden gegeben:
- „GPS-Empfänger-API“, Asseng-Atouba, 2007
- „Voice-over-IP-Sicherheit“, Billerbeck und Stock, 2007
- „Voice-over-IP-Sicherheit“, Safak und Malkoc, 2006
- „Mobile IP und mobile Sicherheit“, Konzag, 2005
- „WiMAX-Sicherheit“, Pugliese, 2007

Das Gesamtergebnis wurde schließlich als Fachbuch unter „Mobile Security - Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit“ beim Hanser Verlag im Jahre 2006 veröffentlicht:

- Evren Eren, Kai-Oliver Detken: Mobile Security – Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit. Carl Hanser Verlag. ISBN 3-446-40458-9; München Wien 2006

Des Weiteren wurde im Jahre 2007 ein Fachbuch zum Thema VoIP-Sicherheit veröffentlicht, das sich u.a. den mobilen Einsatz von VoIP behandelt:
- Evren Eren, Kai-Oliver Detken: VoIP-Security - Konzepte und Lösungen für sichere VoIP-Anwendungen. Carl Hanser Verlag. ISBN-10: 3-446-41086-4; München Wien 2007

Neben den o.g. Fachbüchern sind aus den Themenbereichen wie WLAN-, Bluetooth sowie WiMAX-Sicherheit weitere Publikationen entstanden:
- E. Eren: „Die Sicherheit von IEEE 802.16“: Rheinlandtreffen 23.-24. Oktober 2007 – Gemeinsame Veranstaltung von Fachgruppen der HP User Society DECUS München e.V. und der Gesellschaft für Informatik e.V. (GI)
- E. Eren: „WiMAX Security Architecture“: 4th IEEE Workshop on - Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications – IDAACS 2007, 06. - 08.09.2007, Dortmund
- Evren Eren: „Absicherung von WLANs – Kurzer Vergleich und Bewertung einiger Verfahren“: IT-Symposium 2007 - HP User Society DECUS – Nürnberg, 19. April 2007
- Kai Detken, Evren Eren: Evaluation of current security mechanisms and lacks in wireless and Bluetooth networks: INTERWORKING 2006 – Eighth International Symposium on Interworking, Santiago, Chile, January 2007
- E. Eren, K. Detken: „ Bluetooth-Sicherheit – Schwachstellen und potenzielle Angriffe“: D-A-CH Mobility 2006, 17. - 18.10.2006, München, 10/06
- E. Eren: „Robust Secure Networks – WLAN-Sicherheit mit 802.11i“: Wireless Communication and Information, 13.10.2006, Berlin
- E. Eren, K. Detken: „WLAN-Sicherheit von WEP bis CCMP“: D-A-CH Security 2006, syssec, 28. - 29.03.2006, Düsseldorf, 03/06
- E. Eren, F. Pugliese: „Die Sicherheitselemente und Schwachstellen von IEEE 802.16“: NET (Zeitschrift für Kommunikationsmanagement), 03/07

Publikationen

[1] Evren Eren, Kai-Oliver Detken: „WiMAX-Security – Assessment of the Security Mechanisms in IEEE 802.16d/e“, The 12th World Multi-Conference on Systemics, Cybernetics, and Informatics; Proceedings (Volume III - ISBN10: 1-934272-32-7); Published by International Institute of Informatics and Systemics; 29th June bis 2nd July; Orlando (Florida); USA 2008

[2] Evren Eren, Kai-Oliver Detken: „VoIP Security regarding the Open Source Software Asterisk”; International Multi-Conference on Engineering and Technological Innovation (IMETI) 2008; Proceedings (Volume I - ISBN10: 1-934272-46-9); 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA); Published by International Institute of Informatics and Systemics; 29th June bis 2nd July; Orlando (Florida); USA 2008