Sicherheit in einer digitalen Welt

Unsere Welt wird „digital“ und das Internet wird zur ihrer wichtigsten und kritischsten Infrastruktur. Sicherheit ist Grundvoraussetzung für die Entwicklung der digitalen Welt. Besonders die Absicherung des Internets auf allen Ebenen ist eine immense Herausforderung für Forschung und Entwicklung. Darmstadt ist ein international anerkanntes Zentrum für IT-Sicherheitsforschung. Dieses Heft gibt einen Einblick in zentrale Sicherheitsthemen für die digitale Welt, an denen die vorgestellten Autorinnen und Autoren in Darmstadt arbeiten.

Security in a Digital World

As our world becomes more digitalized, the internet is becoming the world’s most important and critical infrastructure. For this development security is essential. Ensuring security, especially on the internet and its various levels, is a substantial challenge for research and development. Darmstadt is an internationally renowned center for IT security research. This magazine gives an impression of central security topics researched by the authors of this issue.

Johannes Buchmann • Die Informations- und Kommunikationstechnologie (IKT) und besonders das Internet sind eine Erfolgsgeschichte der letzten Dekaden. Das Internet durchdringt und verändert alle Aspekte unserer Wirtschaft und Gesellschaft, führt zu völlig neuen Formen der Kommunikation und Kooperation. Es unterstützt Kreativität, Innovation und wirtschaftliches Wachstum in ungeahnter Weise. Schon heute hat das Internet über 1,6 Milliarden Nutzer, mehr als 4 Milliarden Mobiltelefone sind in Betrieb.

Blick in das Internet der Zukunft

Im zukünftigen Internet werden nahezu alle Dinge und alle Menschen digital präsent und miteinander verbunden sein: Billionen von kleinsten Computern sind in die Dinge des alltäglichen Lebens (Fahrzeuge, Geräte, Kleidung, usw.) eingebettet und verbinden sich in einem „Internet der Dinge“. Große Sensornetze erfassen den Zustand der Welt. Intelligente digitale Assistenten vertreten die Interessen der Menschen. Gigantische Großrechner führen Berechnungen durch, die heute noch undenkbar sind und speichern Unmengen an Daten. Auch in der Wirtschaft finden viele Prozesse weitgehend im Internet statt. Softwarekomponenten repräsentieren Hersteller, Anbieter und Kunden im Internet der Dienste. Software steuert alle Geschäftsprozesse, zum Beispiel Produktion, Angebote, Verhandlungen, Kauf, Verkauf und Vertrieb. Die IKT-Ressourcen sind virtualisiert in der sogenannten Cloud. Rechenleistung und Speicherplatz werden genutzt, ohne dass die Anwender

Johannes Buchmann

wissen, wo die entsprechenden Computer und Speichermedien stehen und wer sie kontrolliert.
Das zukünftige Internet bringt Intelligenz in Straßen und Fahrzeuge. Es trägt dazu bei, Unfälle und Kosten, z. B. durch Verkehrsstaus zu vermeiden. In einer digitalen Welt wird Gesundheitsversorgung im häuslichen Umfeld auf hohem Niveau möglich. Gleichzeitig werden ihre Kosten gesenkt. Intelligente Produktionssysteme erlauben es besonders kleinen und mittleren

Unternehmen, gemeinsam Produkte und Dienstleistungen zu entwickeln und weltweit zu vermarkten. Solche Kooperationen finden im Internet statt und eröffnen ungeahnte neue Geschäftsmöglichkeiten.
Eine weitere, zentrale Aufgabe des heutigen und zukünftigen Internets ist der reibungslose Betrieb und Schutz unserer kritischen Infrastrukturen. Dazu gehören Energieversorgung, Kommunikation, Verkehr und Transport. In Katastrophensituationen ermöglicht das Internet schnelle und effektive Hilfe.

Sicherheit und Privatsphäre als Herausforderung
Die „digitale" Welt wird sich nur entwickeln können und das Internet wird sein Potenzial nur dann voll entfalten können, wenn Sicherheit und Privatsphäre der Beteiligten gewährleistet sind. In Artikel 8 der Charta der Grundrechte der EU heißt es unter der Überschrift: Schutz personenbezogener Daten *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.*
Sicherheit in dieser Form zu gewährleisten ist eine immense Herausforderung für Forschung und Entwicklung.

Kryptographie als Basis für IT-Sicherheitslösungen
Basis für jede IT-Sicherheitslösung sind kryptographische Verfahren, zum Beispiel Verschlüsselung. Verschlüsselung ermöglicht Vertraulichkeit. Die Erfahrung zeigt aber, dass Verschlüsselungsverfahren nach spätestens dreißig Jahren gebrochen werden können, zum Beispiel durch Quantencomputer, die heute diskutiert werden. Für langfristige Vertraulichkeit, die für viele Informationen im zukünftigen Internet erforderlich ist, zum Beispiel für medizinische Daten, reicht das nicht. Abhilfe kann hier nur mathematisch anspruchsvolle kryptographische Forschung oder vielleicht sogar die Quantenkryptographie schaffen. Ihre Sicherheit beruht auf der bedeutendsten Entdeckung der Physik des zwanzigsten Jahrhunderts, der Quantenmechanik. Viel Forschung wird aber noch nötig sein, bevor die Quantenkryptographie praktisch einsetzbar wird.
Die Entwicklung sicherer Kryptographie ist eine große Aufgabe und doch nur ein kleiner Schritt in Richtung eines sicheren Internets. Die komplexen Infrastrukturen des Internets mit den unzähligen Computern und Netzen wollen abgesichert werden und Sicherheitslösungen für die vielen Aufgaben des Internets müssen gefunden und implementiert werden.
So wird zum Beispiel in Zukunft der gesamte Lebenszyklus von Produkten von der Herstellung über Verkauf, Auslieferung, Wartung und Entsorgung im Internet gesteuert und überwacht. Dadurch wächst die Herausforderung, Produktfälschungen zu verhindern. Solche Herausforderungen führen zu komplexen Lösungen. Alle Sicherheit ist verloren, wenn bei der Implementierung der besten Sicherheitslösungen neue Sicherheitslücken eingebaut werden. So wird die Implementierung mit Sicherheitsgarantien zu einer weiteren wichtigen Disziplin.

Wie viel Sicherheit ist notwendig?
Sicherheit für das Internet ist eine conditio sine qua non – aber auch sehr teuer. Zu teuer? Darf es auch ein bisschen weniger Sicherheit sein? Die Beantwortung dieser Frage ist Aufgabe für viele nichttechnische Disziplinen. Welche Sicherheit ist unabdingbar? Was verlangen die Gesetze, und welche neuen Gesetze sind erforderlich? Welche Sicherheit wünschen sich die Bürger? Welche Sicherheit ist ökonomisch geboten und vertretbar?
Dieser Jahrhundertherausforderung, Sicherheit für die zukünftige „digitale" Welt und besonders das Internet der Gegenwart und Zukunft zu ermöglichen, widmet sich die interdisziplinäre Forschung und

Johannes Buchmann ist seit 1996 Professor am Fachbereich Informatik der TU Darmstadt. Er leitet das Fachgebiet Theoretische Informatik und ist Direktor des LOEWE-Zentrums CASED.

Entwicklung in Darmstadt seit vielen Jahren in all ihren Dimensionen.
Mit dem Center for Advanced Security Research Darmstadt (CASED) ist Darmstadt inzwischen zum größten europäischen Forschungs- und Ausbildungszentrum für Internet- und IT-Sicherheit geworden. Ermöglicht wurde dies durch die hessische Landes-Offensive zur Entwicklung wissenschaftlich-ökonomischer Exzellenz (LOEWE). Die drei führenden Darmstädter Institutionen für IT-Sicherheit, die TU Darmstadt, das Fraunhofer Institut für Sichere Informationstechnologie SIT und die Hochschule Darmstadt, haben sich im LOEWE-Exzellenzwettbewerb behauptet und konnten im Juli 2008 CASED als eines von fünf LOEWE-Zentren gründen.

IT-Sicherheitsstandort Darmstadt

In weniger als zwei Jahren wurden für CASED fünf neue international renommierte Professoren berufen, mehr als sechzig Wissenschaftlerinnen und Wissenschaftler für die Mitarbeit gewonnen und ein neuer Master-Studiengang IT-Sicherheit an der TU Darmstadt etabliert. Große Unternehmen wie die Darmstädter Software AG und die SAP AG sind Partner von CASED. Aber auch viele mittelständische Firmen, die sich auf IT-Sicherheit spezialisiert haben wie Kobil Systems und die USD AG. Die CASED-Exzellenz hat sich in weiteren Wettbewerben bewiesen: CASED vertritt im BMBF-Spitzencluster „Softwareinnovationen für das digitale Unternehmen“ schwerpunktmäßig die IT-Sicherheitsforschung und ist Sitz seiner Koordinierungsstelle. Auf internationaler Ebene beteiligt sich CASED an der europäischen Exzellenzinitiative European Institute of Innovation and Technology (EIT).
Die Artikel dieses Heftes geben einen Eindruck von der Spannbreite der Darmstädter IT-Sicherheitsforschung und -Entwicklung.

Fachgebiet Theoretische Informatik – Kryptographie und Computeralgebra
Prof. Dr. Johannes A. Buchmann
Tel. 06151/16-3416
E-Mail: buchmann@cdc.informatik.tu-darmstadt.de
www.cdc.informatik.tu-darmstadt.de

ANZEIGE