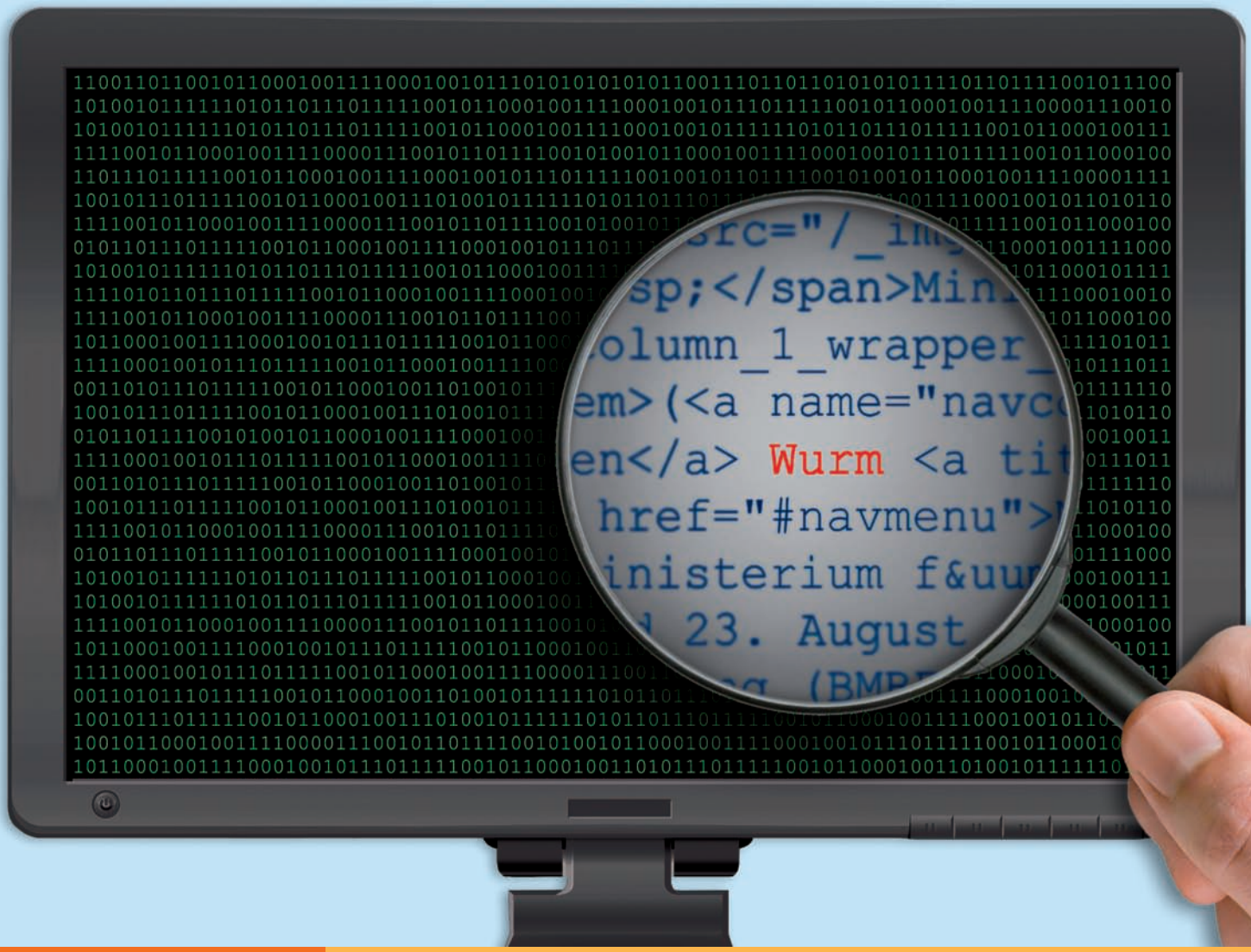
Bundesministerium
für Bildung
und Forschung

Bundesministerium
des Innern

Arbeitsprogramm

IT-Sicherheitsforschung



HIGHTECH-STRATEGIE

Ideen zünden!

Impressum

Herausgeber
Bundesministerium für
Bildung und Forschung (BMBF)
Referat Schlüsseltechnologien; Strategie und Grundsatzfragen
53170 Bonn

Herausgeber
Bundesministerium des Innern (BMI)
Referat IT-Sicherheit
10559 Berlin

Bestellungen
schriftlich an den Herausgeber
Postfach 30 02 35
53182 Bonn
oder per
Tel.: 01805 – 262 302
Fax: 01805 – 262 303
(0,14 Euro/Min. aus dem deutschen Festnetz)
E-Mail: books@bmbf.bund.de
Internet: http://www.bmbf.de

Redaktion
BMBF, Referat Schlüsseltechnologien; Strategie und Grundsatzfragen
BMI, Referat IT-Sicherheit

Gestaltung
FOCON GmbH, Aachen

Bonn, Berlin 2009

Bildnachweis
Fotolia

Bundesministerium
für Bildung
und Forschung

Bundesministerium
des Innern

Arbeitsprogramm

IT-Sicherheitsforschung

Vorwort

Informations- und Kommunikationstechnologien (IKT) sind aus unserem Alltag nicht mehr wegzudenken. Auch ihre wirtschaftliche Bedeutung als Innovationstreiber ist enorm. Quer durch alle Branchen leisten IKT ihren Beitrag, Arbeitsprozesse zu vernetzen und den Ressourceneinsatz effizienter zu gestalten. IKT sind Taktgeber und Rückgrat der Wirtschaft – und damit auch der Garant für neue, zukunftssichere Arbeitsplätze im globalen Wettbewerb.

Allerdings sind Privatpersonen und Unternehmen in zunehmendem Maße von illegalen Zugriffen auf IT-Systeme und Daten betroffen. Sie beeinträchtigen nicht nur die informationelle Selbstbestimmung des Einzelnen, sondern führen auch zu großen wirtschaftlichen Verlusten. Deshalb werden Sicherheit und Datenschutz immer wichtiger. Sie müssen an erster Stelle stehen, wenn wir die Informationsgesellschaft und insbesondere das Internet der Zukunft gestalten.

Das Bundesministerium für Bildung und Forschung (BMBF) hat zusammen mit dem Bundesministerium des Inneren im Rahmen der „Gemeinsamen Erklärung über die Zusammenarbeit auf dem Gebiet der IT-Sicherheitsforschung“ im Oktober 2008 vereinbart, IT-Sicherheit als einen neuen Schwerpunkt der Forschungsförderung zu etablieren. Das vorliegende Arbeitsprogramm IT-Sicherheitsforschung bildet den Kern dieses Förderschwerpunkts. Das BMBF stellt für seine Umsetzung 30 Millionen Euro für eine Laufzeit von fünf Jahren bereit.

IT-Sicherheitsforschung soll helfen, Bürgerinnen und Bürger, Unternehmen und den Staat vor illegalen Zugriffen zu schützen und die Wettbewerbsfähigkeit des Forschungs-, Produktions- und Arbeitsplatzstandortes Deutschland im Bereich IT-Sicherheit zu stärken. Das neue Arbeitsprogramm schafft die besten Voraussetzungen, damit wir unsere sicherheitspolitischen Ziele auf diesem Gebiet schneller und effektiver erreichen können.

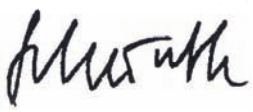
Prof. Dr. Annette Schavan, MdB
Bundesministerin für Bildung und Forschung

Deutschland ist dank seiner wirtschaftlichen Stärke und dem hohen Niveau von Forschung und Technik eine der am höchsten entwickelten Industrienationen der Welt. Unsere Leistungsfähigkeit ist von funktionierender Informationstechnik und sicheren Informationsinfrastrukturen abhängig. Denn eine große Zahl von Prozessen und Aufgaben läuft heute IT-gestützt ab.

Auch professionell organisierte Cyberkriminelle nutzen die Möglichkeiten der Informationstechnik. Damit rückt die Informationssicherheit stärker ins Zentrum unseres Handelns: Für deutsche Unternehmen, die Bürgerinnen und Bürger sowie die staatlichen Institutionen gewinnen Themen wie IT-gestützte Spionage, Bot-Netz-Angriffe und Datenmissbrauch an Bedeutung. Wir müssen davon ausgehen, dass solche Bedrohungen weiter zunehmen werden.

Die durchgängige Verfügbarkeit und Vertraulichkeit von Informations- und Kommunikationstechnologien ist insbesondere bei den kritischen Infrastrukturen unverzichtbar für unsere Sicherheit. Eine gezielte Forschung auf dem Gebiet der IT-Sicherheit ist notwendig, um die IKT-Infrastrukturen vor den derzeitigen und möglichen neuen Bedrohungen zuverlässig zu schützen.

Deshalb haben das Bundesministerium des Innern und das Bundesministerium für Bildung und Forschung gemeinsam das Arbeitsprogramm IT-Sicherheitsforschung erarbeitet. Mit den Forschungsschwerpunkten „Sicherheit in unsicheren Umgebungen“, „Schutz von Internet-Infrastrukturen“, „Eingebaute Sicherheit“ und „Neue Herausforderungen zum Schutz von Informations- und Kommunikationssystemen und Identifikation von Schwachstellen“ unterstützen wir innovative Lösungen zur besseren Absicherung der IKT-Infrastrukturen in unserem Land.



Dr. Wolfgang Schäuble, MdB
Bundesminister des Innern

Inhaltsverzeichnis

Zusammenfassung 2

Ausgangslage und Zielsetzung 3

Schwerpunkte der Förderung 4

Sicherheit in unsicheren Umgebungen 4

Schutz von Internet-Infrastrukturen 6

Eingebaute Sicherheit 9

Neue Herausforderungen zum Schutz von IKT-Systemen und der Identifikation von Schwachstellen 12

Operative Umsetzung 15

Zusammenfassung

Vom richtigen und zuverlässigen Funktionieren der Informations- und Kommunikationstechnologien (IKT) und dem Vertrauen in die Sicherheit der IKT-Systeme hängen inzwischen weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens ab. Gleichzeitig werden die weit vernetzten IKT-Systeme zunehmend auch für kriminelle Zwecke eingesetzt. Dies reicht vom Ausspionieren einzelner Daten von Bürgerinnen und Bürgern mit teils erheblichen Schäden über organisierte Kriminalität bis zu Spionage gegen staatliche Einrichtungen und Unternehmen.

Die Bundesministerin für Bildung und Forschung und der Bundesminister des Innern haben deshalb im Rahmen ihrer Gemeinsamen Erklärung zur Zusammenarbeit auf dem Gebiet der IT-Sicherheitsforschung vom 29. Oktober 2008 vereinbart, IT-Sicherheit als neuen Schwerpunkt der Forschungsförderung im Bereich der IKT zu etablieren, und dafür ein Arbeitsprogramm IT-Sicherheitsforschung vorzulegen. Für eine Laufzeit von 5 Jahren werden vom Bundesministerium für Bildung und Forschung hierfür Fördermittel in Höhe von 30 Mio. Euro bereitgestellt.

Die Förderung im Bereich der IT-Sicherheitsforschung zielt auf die Schaffung der Grundlagen für die Entwicklung überprüfbar und durchgehend sicherer IT-Systeme sowie der Erforschung neuer Ansätze bei der Analyse und Absicherung von IKT-Systemen ab. Darüber hinaus sollen hiervon positive Effekte für die Wettbewerbsfähigkeit des Forschungs-, Produktions- und Arbeitsplatzstandortes Deutschland im Bereich IT-Sicherheit ausgehen, und – sofern es die Sicherheitsinteressen Deutschlands zulassen – eine Verwertbarkeit von Forschungsergebnissen auch außerhalb des sicherheitsrelevanten Bereichs möglich sein.

Das Bundesministerium für Bildung und Forschung und das Bundesministerium des Innern haben gemeinsam die Schwerpunkte der Förderung identifiziert: Da eine Absicherung großer IKT-Umgebungen (z.B. Internet) de-facto nicht möglich ist, soll die Sicherheit von IKT-Systemen, insbesondere mobilen Systemen, auch in unsicheren Umgebungen gewährleistet werden (Schwerpunkt „Sicherheit in unsicheren Umgebungen“). Auch wenn eine vollständige Absicherung von IKT-Systemen gegen Angriffe nicht möglich ist, können die Systeme gegen „Epidemien“ geschützt werden (Schwerpunkt „Schutz von Internet-Infrastrukturen“). Die nachträgliche Absicherung von IKT-Systemen ist extrem aufwendig und vielfach gar nicht möglich. IKT-Systeme sollen deshalb von vornherein so konzipiert und entwickelt werden, dass sie (beweisbar) über ein definiertes IT-Sicherheitsniveau verfügen (Schwerpunkt „Eingebaute Sicherheit“). Um speziellen und zukünftig vielleicht möglichen Angriffen entgegen wirken zu können, sollen zur Absicherung von IKT-Systemen auch neuartige Techniken, Methoden und Ansätze entwickelt werden (Schwerpunkt „Neue Herausforderungen zum Schutz von IT-Systemen und der Identifikation von Schwachstellen“).

Das Arbeitsprogramm IT-Sicherheitsforschung ist als offenes und lernendes Programm angelegt. Das Bundesministerium für Bildung und Forschung und das Bundesministerium des Innern werden zur Fortschreibung und Weiterentwicklung den bereits begonnenen Dialog mit Wissenschaft und Wirtschaft fortsetzen, um auf technologische, wirtschaftliche und gesellschaftliche Entwicklungen abgestimmt und zeitnah reagieren zu können.

Ausgangslage und Zielsetzung

Informations- und Kommunikationstechnologien durchdringen in immer stärkerem Maße alle Bereiche in unserer Gesellschaft. Ob im privaten Umfeld, am Arbeitsplatz oder im öffentlichen Leben: Vom richtigen und zuverlässigen Funktionieren der IKT-Systeme und dem Vertrauen in die Sicherheit dieser Systeme hängen inzwischen weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens ab.

Für Wirtschaftsunternehmen stellen Angriffe auf deren IKT-Systeme nach derzeitigem Stand die höchste aktuelle und zukünftige Gefährdung dar. Konsequenter Weise steigen daher die aktuellen Budgets für Sicherheitsausgaben in Relation zu den allgemeinen IKT-Ausgaben. Eine leistungsfähige, vertrauenswürdige deutsche IKT-Sicherheitswirtschaft, die Produkte und Dienstleistungen auf technologisch höchstem Stand anbieten kann, muss in diesem Zusammenhang als wichtiger infrastruktureller Standortvorteil gesehen werden.

Um wettbewerbsfähig zu sein und effizient arbeiten zu können, stehen Unternehmen in Deutschland heute insbesondere vor der Herausforderung, immer neuere Informationstechnik einzusetzen. Bereits 2007 wurde angesichts immer neuer Bedrohungsszenarien, mit denen die eingesetzten Systeme konfrontiert werden, der Bedarf nach einem auf Führungsebene der Unternehmen initiierten Sicherheitsprozess thematisiert.

Die weit vernetzten IKT-Systeme werden zunehmend auch für kriminelle Zwecke eingesetzt. Dies reicht vom Ausspionieren einzelner Daten von Bürgerinnen und Bürgern mit erheblichen Schäden, über organisierte Kriminalität bis zu Spionage gegen staatliche Einrichtungen und Unternehmen. Das Auftreten von Schadsoftware (z.B. Viren, Trojaner) ist längst nicht mehr auf den klassischen IT-Bereich (PC und Computernetze) begrenzt. Auch gegen eingebettete Systeme (Embedded Devices) werden Angriffe beobachtet.

Dies wird dadurch begünstigt, dass die heute eingesetzte IT so komplex ist, dass Fehler kaum noch vermeidbar sind. Diese so genannten Sicherheitslücken werden immer wieder von Angreifern ausgenutzt. Außerdem arbeitet Schutzsoftware gegen Angriffe von außen bislang hauptsächlich signaturbasiert, das heißt, ein Virenschutzprogramm erkennt nur bereits bekannte Schadprogramme. Diese Technik ist an ihre Grenzen gestoßen. Es ist daher wichtig, dass neue Schadprogramme auch an ihren Eigenschaften bzw. ihrem Verhalten erkannt werden können.

Ein weiterer Aspekt ist, dass die Informations- und Kommunikationstechnologien sich rasant weiterentwickeln und durch extrem kurze Innovationszyklen geprägt sind. IKT-Systeme, die heute noch als sicher gelten, können durch technologische Entwicklungen morgen bereits unsicher sein. Die heute eingesetzten Sicherheitsmaßnahmen und -systeme sind häufig gegen spezifische Bedrohungen entwickelt worden und werden meist nachträglich in IKT-Systeme integriert. Neben der reaktiven Weiterentwicklung dieser Systeme ist deshalb auch Forschung in Richtung grundsätzlich neuer Systemarchitekturen sowie Sicherheitsmechanismen und -systeme erforderlich.

Mit der Zusammenarbeit auf dem Gebiet der IT-Sicherheitsforschung zielen BMBF und BMI auf folgendes ab:

- **Schaffung der Grundlagen für die Entwicklung überprüfbar und durchgehend sicherer IKT-Systeme**
- **Erforschung neuer Ansätze bei der Analyse und Absicherung von IKT-Systemen**
- **Positive Effekte für die Wettbewerbsfähigkeit des Forschungs-, Produktions- und Arbeitsplatzstandortes Deutschland im Bereich IT-Sicherheit**
- **Verwertbarkeit von Forschungsergebnissen auch außerhalb des sicherheitsrelevanten Bereichs, sofern dies die Sicherheitsinteressen Deutschlands zulassen.**

Schwerpunkte der Förderung

Auf der Basis der Zielsetzung der IT-Sicherheitsforschung (s.o.) haben BMBF und BMI gemeinsam folgende Schwerpunkte der Forschungsförderung identifiziert:

- **Sicherheit in unsicheren Umgebungen: Eine Absicherung großer IKT-Umgebungen (z.B. Internet) ist aufgrund der Komplexität de facto nicht mehr möglich. Die Sicherheit von IKT-Systemen, insbesondere von mobilen Systemen, soll deshalb auch in unsicheren Umgebungen gewährleistet werden.**

- **Schutz von Internet-Infrastrukturen: Eine vollständige Absicherung von IKT-Systemen gegen Angriffe ist nicht möglich, aber die Systeme können gegen „Epidemien" geschützt werden. Dazu müssen Angriffe erkannt, Schadsoftware isoliert, eine Weiterverbreitung verhindert und Dritte rechtzeitig informiert werden.**

- **Eingebaute Sicherheit: Die nachträgliche Absicherung von IKT-Systemen ist extrem aufwendig und vielfach gar nicht möglich. IKT-Systeme sollen deshalb von vornherein so konzipiert und entwickelt werden, dass sie (beweisbar) über ein definiertes IT-Sicherheitsniveau verfügen.**

- **Neue Herausforderungen zum Schutz von IT-Systemen und der Identifikation von Schwachstellen: Um speziellen und zukünftig vielleicht möglichen Angriffen entgegen wirken zu können, müssen zur Absicherung von IKT-Systemen auch neuartige Techniken, Methodiken und Ansätze entwickelt werden.**

FuE-Projekte zu diesen thematischen Schwerpunkten können im Rahmen des Arbeitsprogramms IT-Sicherheitsforschung gefördert werden.

Aufgrund der dynamischen Entwicklung der IKT und der extrem kurzen Innovationszyklen ist das Arbeitsprogramm IT-Sicherheitsforschung als offenes und lernendes Programm ausgelegt. BMBF und BMI werden zur Qualitätssicherung, Fortschreibung und Weiterentwicklung den bereits begonnenen Dialog mit Wissenschaft und Wirtschaft fortsetzen, um auf technologische, wirtschaftliche und gesellschaftliche Entwicklungen abgestimmt und zeitnah reagieren zu können.

Sicherheit in unsicheren Umgebungen

Seit den Anfängen des Internets sind die Zahl der Computer und Anwendungen sowie der Grad der Vernetzung und Mobilität enorm angestiegen. Die Entwicklung zum Internet der Dinge hat für die Zukunft zur Folge, dass auch die Vielfalt der IKT-Systeme drastisch zunehmen wird. Die zunehmende Vernetzung und Mobilität von IKT-Systemen hat dabei nicht nur zu einer wesentlichen Erweiterung der Funktionalität geführt, sondern auch neue Probleme im Bereich der IT-Sicherheit geschaffen. Den Übergängen zwischen dem unsicheren Internet auf der einen und den internen Netzen (oder einzelnen IKT-Systemen) mit hohen Sicherheitsanforderungen auf der anderen Seite kommt dabei eine Schlüsselstellung zu.

Zu den Sicherheitsproblemen aufgrund der drahtlosen Funkanbindung der mobilen Endgeräte kommt erschwerend hinzu, dass diese wegen ihrer begrenzten Leistungsfähigkeit sicherheitstechnisch noch weit hinter den etablierten stationären Rechnersystemen zurück liegen. Den spezifischen Bedrohungen in der mobilen Welt kann also noch nicht mit wirksamen Schutzmechanismen begegnet werden.

Aber nicht nur bei drahtlosen Kommunikationssystemen stellen sich große Herausforderungen an die Absicherung. Auch bei drahtlosen Sensornetzen, bestehend aus autonomen Sensorknoten, bereiten die drahtlose Kommunikation sowie die eingeschränkten Ressourcen (Energie, Rechenleistung) Probleme bei der Absicherung dieser Systeme.

Eine der zentralen Aufgaben ist es daher, für IKT-Systeme, die in unsicheren Umgebungen eingesetzt werden, Konzepte und Maßnahmen zu entwickeln, die entweder das System selber oder die nähere Umgebung, in der es eingesetzt wird, vor Angriffen von außen absichert.

Prioritärer Handlungsbedarf wird deshalb bei folgenden Themenbereichen gesehen:

- **Sicherheit in der mobilen Welt;**

- **Informationssicherheit in Sensorknoten.**

Sicherheit in der mobilen Welt

Drahtlose Kommunikationssysteme finden bei zunehmender Produktivität eine immer größere Verbreitung. Die Funkanbindung von mobilen Endgeräten an das Telefonnetz, das Internet oder lokale Netze bietet neue Möglichkeiten bei der Nutzung der Netze und deren Dienste. Die große Verbreitung und Beliebtheit mobiler Endgeräte insbesondere auch in der Führungsebene von Wirtschaft und Verwaltung und das damit verbundene hohe Aufkommen an sensiblen und sicherheitskritischen Informationen machen diese Systeme aber auch zu einem attraktiven Angriffsziel.

Angriffsmöglichkeiten ergeben sich über die Mobilfunknetze, über die IP-Anbindung an das Internet sowie durch direkten physikalischen Zugriff auf das mobile Endgerät. Durch die drahtlose Anbindung der mobilen Endgeräte an die Host-Systeme und durch spezifische, architekturbedingte Schwachstellen, die aus Anforderungen der Servicebetreiber resultieren (z.B. Remote-Device-Management) ergeben sich bei mobilen Endgeräten völlig neue Bedrohungen, die bei stationären Systemen in dieser Form nicht bestehen.

Herausforderungen

Die in Mobilfunknetzen standardisierten und implementierten Sicherheitsvorkehrungen sind nicht ausreichend, um qualifizierte Angriffe, die über die Netzinfrastruktur geführt werden, zu verhindern. Darüber hinaus bieten mobile Endgeräte und ihre Betriebssysteme Einfallstore für die Manipulation der Endgeräte und das Einschleusen von Schadsoftware „over-the-air“. Da die von stationären IKT-Systemen bekannten Sicherheitskonzepte und -maßnahmen nicht ohne weiteres auf mobile Endgeräte übertragbar sind, müssen hier neuartige Konzepte entwickelt werden. Die Herausforderung besteht u.a. darin, auch unter der Berücksichtigung beschränkter Ressourcen mobiler Endgeräte sichere, performante und zugleich preiswert realisierbare Sicherheitslösungen für die mobile Welt zu schaffen.

Forschungsthemen

- Neue Ansätze und Konzepte zum Schutz mobiler Kommunikationslösungen vor Angriffen über die Netzinfrastrukturen
- Neuartige Verfahren zur Detektion und Abwehr von Schadsoftware in mobilen Endgeräten
- Grundlagen, Konzepte und neue Verfahren in den Bereichen Mobile Honeypots, Mobile Honeynets und Mobile Sandbox
- Ganzheitliche Sicherheitskonzepte für betreiberunabhängige und netzübergreifende sichere mobile Kommunikationslösungen in heterogenen Mobilfunksystemen, insbesondere neue Forschungsansätze, Prüfverfahren und Werkzeuge
- Umfassende Analyse der Gefährdungen von 4G-Netzen gegen Angriffe auf die Netze selbst, u.a. als Grundlage für betreiberübergreifende Angriffserkennungssysteme und entsprechende Abwehrmaßnahmen.

Informationssicherheit in Sensorknoten

In vielen technischen Anwendungen (z.B. der Steuerung von Industrieanlagen, bei der Entwicklung des Internets der Dinge und zum Ambient Assisted Living) müssen Umgebungsdaten in einem größeren Gebiet erfasst und verarbeitet werden. Klassischerweise geschieht dies mit Hilfe von fest verbauten und verkabelten Sensoren, die Messdaten an einen Zentralrechner übermitteln, wo diese dann ausgewertet werden können.

Drahtlose Sensornetze stellen in vielen Bereichen hierzu eine technologische Alternative mit einem großen Wachstumspotential dar. Ein drahtloses Sensornetz besteht dabei aus einer Menge von Kleinstrechnern (Sensorknoten), die mit Sensoren ausgestattet sind und über einen Funkkanal miteinander kommunizieren können. Diese Sensorknoten verfügen typischerweise über einen einfachen Prozessor, nur wenig Speicher und einen begrenzten Energievorrat (in Form einer Batterie oder eines Akkus). Große Vorteile von drahtlosen Sensornetzen sind die relativ geringen Kosten und die Flexibilität im Einsatz.

Herausforderungen

Durch die Ad-hoc-Vernetzung, die verteilte Verarbeitung der Daten und die funktechnische Kommunikation zwischen den einzelnen Sensorknoten werden besondere Anforderungen an die IT-Sicherheit in Sensornetzen gestellt. Außerdem ist die „Zielsetzung" in herkömmlichen Netzwerken meistens eine andere: Dort geht es im Wesentlichen um eine sichere Ende-zu-Ende Kommunikation. In Sensornetzen hingegen ist eine Datenfusion von der Datenerhebung zur Datensenke gefordert, die mit dem Konzept der Ende-zu-Ende Sicherheit nicht verträglich ist.

Die zur Absicherung herkömmlicher Netzwerke bekannten Konzepte und Maßnahmen können deswegen und wegen der beschränkten Hardware- und Energieressourcen der Sensorknoten zu deren Absicherung de-facto nicht verwendet werden. Hier gilt es neue Sicherheitskonzepte zu entwickeln.

Forschungsthemen

- Grundlagen und Konzepte für ein sicheres Betriebssystem für ressourcenbeschränkte Sensorknoten, insbesondere (verteilter) Mikrokernansatz und Einbeziehung von Kryptoprozessoren, User/Admin-Mode, sicheres Software-Nachladen, sicheres Booten/Wiederaufwachen
- Mechanismen zur Überprüfung von Vertrauenswürdigkeit innerhalb des Betriebssystemkerns

Schutz von Internet-Infrastrukturen

Seit Beginn des Internets (und sogar schon beim „Vorgängernetz") steht die Verfügbarkeit des Netzes an oberster Stelle. Fragen der IT-Sicherheit wurden über lange Zeit hin als nachrangig behandelt, auch weil allein schon der Zugang zum Internet anfangs ausgesprochen schwierig war.

Dies hat sich auch in den zugrundeliegenden Internet-Protokollen niedergeschlagen: Die grundlegenden Internet-Kommunikationsprotokolle (IPv4) berücksichtigen IT-Sicherheits-erfordernisse nur ansatzweise, einige ihrer Grundfunktionen werden sogar als Werkzeuge für Angriffe auf Computersysteme genutzt. Da praktisch alle großen, heterogenen Netze auf denselben Kommunikationsprotokollen basieren, gilt Entsprechendes auch für diese.

Mit dem enormen Anstieg der Zahl der Computer und Anwendungen sowie des Grades der Vernetzung ist auch die Bedeutung der Sicherheit der Internet-Infrastrukturen angestiegen. Hinzu kommt, dass die Absicherung von internen Netzen und IKT-Systemen gegen das offene Internet deutlich schwieriger ist: Früher gab es nur wenige „Dienste", die eine Firewall überwachen musste, und vielfach wurden Zugriffe nur für sehr wenige definierte IKT-Systeme im internen Netz gestattet. Mit dem Aufkommen einer Vielzahl neuer internetbasierter

Anwendungen, z.B. im Multimedia-Bereich, ist eine „Abschottung“ aber kaum noch sinnvoll möglich. Und damit steigt nicht nur das Datenvolumen extrem an, sondern auch das Sicherheitsrisiko.

Beim neuen Internet-Kommunikationsprotokoll (IPv6-Standard), dessen Verbreitung derzeit allerdings noch eher gering ist, gibt es mittlerweile auch Erweiterungen für Sicherheit und Datenschutz, allerdings nur teilweise und optional. Es ist erkennbar, dass auf absehbare Zeit der Übergang zu IPv6 neue Sicherheitsrisiken durch unvollständige Implementierungen in einer weit größeren Vielfalt von Komponenten hervorruft.

Da das Internet und große, heterogene Netze also prinzipiell nicht umfassend gegen Angriffe gesichert werden können, gilt es vorrangig die Netze sowie die IKT-Systeme gegen „Epidemien“ zu schützen.

Prioritärer Handlungsbedarf wird deshalb bei folgenden Themenbereichen gesehen:

- **Technologien zur Angriffsprävention und Frühwarnung;**
- **Autonome Systeme und Infrastrukturen.**

Technologien zur Angriffsprävention und Frühwarnung

Aktive Netzschutzkomponenten zur Absicherung von Netzen sollen die Sicherheit zukünftiger Dienste gewähren und die Benutzung von mobilen, verteilten und heterogenen Netzen absichern. Entscheidend für eine erfolgreiche Netzabsicherung ist die Angriffserkennung und Prävention. Dynamische Firewalls sowie Firewalls für mobile Systeme benötigen dafür neue selbstlernende Systeme, um durch die automatische Auswahl von Sicherheitsmechanismen geeignete Anpassungen bei sicherheitsrelevanten Vorfällen vornehmen zu können.

Herausforderungen

Die Vielzahl spezialisierter „Security“-Applikationen (von der Netzwerk- bis zur Anwendungsebene) und Quellen für sicherheitsrelevante Informationen stellt ein großes Problem für ein effizientes Frühwarnsystem dar. Die Lösung kann nur in der Integration liegen, d.h. im leistungsfähigen und effektiven Zusammenspiel dieser Applikationen sowie der Bündelung aller relevanten Informationen.

Entscheidend für die Frühwarnung ist die schnelle Erfassung und effiziente Verteilung einer gemeinsamen Lagebildbewertung, um mögliche Überraschungen durch Kaskadeneffekte zu vermeiden. Entsprechende kooperative Szenarien für die Ableitung von gemeinsamen Handlungsempfehlungen, zur Frühwarnung und Ausführung von geeigneten Gegenmaßnahmen sind zu entwickeln.

Neuartige Verfahren zur „Intrusion“- und Anomalie-Detektion, zur Detektion und Abwehr von Schadsoftware oder SPAM können in Verbindung mit geeigneter Frühwarnung sensible IKT-Netze und -Infrastrukturen schützen.

Forschungsthemen

- Grundlagen und Konzepte für aktive Netzschutzkomponenten, insbesondere dynamische Firewalls und Firewalls für mobile Systeme auf Basis selbstlernender Systeme

- Neuartige Verfahren zur „Intrusion-“ und Anomalie-Detektion, insbesondere zur Detektion von Anomalien im Internet bzw. anderen großen, heterogenen Netzwerken und zur Abwehr von Schadsoftware oder SPAM

- „Ganzheitliche“ Sicherheitsanalyse kryptographischer Sicherheitsprotokolle, um die Lücke zwischen komplementären Analysemethoden zu schließen und Empfehlungen für übergeordnete Sicherheitsmechanismen abzuleiten, sowie Entwicklung einer beweistechnischen Unterstützung der Protokollanalyse bis auf Implementierungsebene

- Konzepte für umfassendes Sicherheitsmanagement, d.h. Integration spezialisierter „Security“-Applikationen, Zusammenfassung aller relevanten Informationen und effiziente Verteilung einer gemeinsamen Lagebildbewertung; z.B. Weiterentwicklung der Ansätze SIEM („Security Incident and Event Manager“) und UTM („Unified Threat Management“)

- Entwicklung von Methoden und Werkzeugen für ein umfassendes Sicherheitsmanagement, das für Administrationszwecke ausreichende Flexibilität und für Nutzerbedürfnisse nach vertrauenswürdigen Systemen ausreichende Transparenz aufweist

Autonome Systeme und Infrastrukturen

Eine vollkommene Trennung der für die Gesellschaft wichtigen Netze und Infrastrukturen von den übrigen Infrastrukturen ist selbst im Gefahrenfall nicht möglich. Ausschließlich auf zentralen Komponenten basierende Sicherheitsfunktionen sind hierbei z.B. durch DDoS-Angriffe stark gefährdet, da der zeitweise Ausfall einer zentralen Komponente den Ausfall der entsprechenden Sicherheitsfunktionalität zur Folge hätte.

Herausforderungen

Um diesen Bedrohungen entgegenzuwirken und eine zumindest eingeschränkte Verfügbarkeit auch in Gefahrenlagen zu gewährleisten, müssen Konzepte, Verfahren und Mechanismen entwickelt werden, die auf verteilten und autonomen Hard- und Softwaresystemen beruhen. Im Fokus sollen hier insbesondere Untersuchungen und Erprobungen verteilter Detektions-, Abwehr- und Selbstheilungsmechanismen auf Basis mobiler Softwareagenten und bioanaloger Modelle und Mechanismen, aber auch neue, noch nicht bekannte Ansätze stehen.

Forschungsthemen

- Entwicklung robuster dezentraler identitätsbasierter Authentisierungsverfahren

- Entwicklung eines dezentralen Autokonfigurationssystems für Virtuelle Private Netzwerke mit IPSec unter Berücksichtigung von Vertraulichkeit, Authentizität und Zugriffsschutz

- Konzeption, Entwicklung und Test robuster Verfahren zur Informationsfusion bzw. -klassifikation, um Anomalien sicher zu erkennen, zu klassifizieren und ggf. adäquat reagieren zu können

- Konzeption, Entwicklung und Test (verteilter) Detektions-, Abwehr- und Selbstheilungsmechanismen auf Basis mobiler Softwareagenten und bioanaloger Modelle und Mechanismen

Eingebaute Sicherheit

IT-Sicherheit hat sich in der Praxis dahin entwickelt, in kurzen Abständen neue Sicherheitsupdates für Betriebssysteme, Virenscanner und Firewalls zu suchen und einzuspielen oder darauf zu warten, dass Hersteller von Anwendungssystemen Lösungen zur Entfernung neu bekannt gewordener Sicherheitslücken bereitstellen. Das Auswechseln von – aus Sicht der IT-Sicherheit - mangelhaften Produkten gegen andere bringt allerdings nur begrenzten Zugewinn beim Sicherheitsniveau.

Auch Software, die nach hohen Standards entwickelt wurde, wird manipulierbar, wenn sie auf Computern und in Softwareumgebungen eingesetzt wird, die Sicherheitslücken aufweisen.

Maximale Sicherheit ist nur zu erreichen, wenn es gelingt, ein konkretes IKT-System formal so zu entwerfen und zu konstruieren, dass seine korrekte Funktionsweise verifizierbar ist. Die Sicherheit wird also von vornherein in das IKT-System eingebaut. Theoretische und praktische Grundlagen für den Nachweis der formalen Korrektheit von Hardware und Software wurden bereits geschaffen. Das Problem bleibt jedoch bestehen, dass weder eine Verifikation der großen Vielfalt von nützlicher Software zu leisten ist, noch die Möglichkeit besteht, ein definiert sicheres Verhalten von IT-Systemen – also ein umfassendes System Health Monitoring – zu erkennen und zu überwachen.

Prioritärer Handlungsbedarf wird deshalb bei folgenden Themenbereichen gesehen:

- **Innovative Sicherheitsmechanismen für heterogene Plattformen;**
- **Sicherheitsaspekte bei FPGA und deren Einbettung;**
- **Hostbasierte Anomalieerkennung auf Rechnersystemen.**

Innovative Sicherheitsmechanismen für heterogene Plattformen

Auch für heterogene Plattformen gibt es mittlerweile erste Ansätze zur Begrenzung bedeutender Sicherheitslücken. Diese zielen ab auf die Sicherheit von Betriebssystemen (z.B. durch spezielle Kernel oder durch Virtualisierung), die Weiterentwicklung von Trusted-Computing-Ansätzen sowie die Anwendung beider Konzepte für eingebettete Systeme.

Kryptografische Verfahren stellen dabei eine Querschnittstechnologie dar, da sie einerseits ein grundlegendes Element der notwendigen Sicherheitsmechanismen darstellen, und andererseits in vielen anderen Bereichen der IT-Sicherheit zum Einsatz kommen können. Kryptografische Verfahren sind für die genannten Problembereiche auf verschiedenen Wegen weiter zu entwickeln.

Herausforderungen

Trotz erfolgversprechender Ansätze zur Begrenzung bedeutender Sicherheitslücken fehlt es immer noch an wesentlichen Elementen, um bei herkömmlichen PC oder eingebetteten Systemen ein System- und Security-Monitoring im laufenden Betrieb zu ermöglichen, Sicherheitsmechanismen über verschiedene Plattformen hinweg zu realisieren und Aussagen über den Sicherheitszustand eines komplexen Gesamtsystems treffen zu können.

Forschungsthemen

- Entwicklung von Schlüsseltechnologien (unterschiedlicher Komplexität) für verifizierbar sichere IKT-Systeme und ein umfassendes System Health Monitoring
- Grundlagen und Konzepte für den korrekten, vertraulichen und sicheren Betrieb durch die Nutzung von Trusted Computing (oder ähnlichen Funktionalitäten) bei Betriebssystemen und anderer systemnaher Software
- Entwicklungen für vertrauenswürdige ressourcenbeschränkte Komponenten (z.B. für RFID-Nachfolgetechnologie, eingebettete und mobile Systeme) und deren Integration in ein umfassendes Sicherheitsmanagement

Sicherheitsaspekte bei FPGA und deren Einbettung

Standard Chips haben aus Sicherheitssicht den Nachteil, dass die konkrete technologische Ausgestaltung, wie auch Änderungen des Herstellungsprozesses vom Anwender kaum beeinflusst werden können. Wird eine technologienahe Eigenschaft einer Hardware (z.B. physikalisches Rauschen als Quelle für einen physikalischen Zufallszahlengenerator) von einer Sicherheitsfunktion ausgenutzt und die zugrundeliegende Technologie geändert, so kann sich, ohne dass die Sicherheitsfunktionalität selbst geändert wurde, eine Schwachstelle ergeben.

Eine wichtige Technologie, die Flexibilität bei hoher Leistungsfähigkeit ermöglicht, sind FPGA (Field Programmable Gateway Arrays). Die applikationsspezifisch programmierbaren FPGA bieten dabei Freiheitsgrade, die jene von Standard Prozessoren übersteigen. Nicht nur, dass sich auf dem programmierbaren Teil Prozessoren einbetten lassen – teilweise enthalten FPGA sogar schon hardwaretechnisch eingebettete Prozessoren. Somit wird der Gedanke des „System on a Chip" sogar in der programmierbaren Variante auf einem Quasistandard-Hardwarebaustein zunehmend Realität.

Herausforderungen

Damit einher geht insbesondere auch im Hochsicherheitsbereich die Notwendigkeit, sowohl Sicherheitsfunktionen sicher, dauerhaft und nachweisbar separiert implementieren zu können, als auch Komponenten, die auf physikalischen Effekten (z.B. Rauschen) beruhen, nachweisbar sicher implementieren zu können. Technische Eigenschaften (z.B. hohe Verlustleistung) können dazu führen, dass die Sicherheitsfunktionen auf mehrere Bauelemente aufgeteilt werden müssen. Dadurch entstehen Bauelemente-externe Schnittstellen, die von einem Angreifer leichter zugänglich sind, als Chip-interne Schnittstellen.

Forschungsthemen

- Grundlagen und Konzepte der Nutzung technischer FPGA-Eigenschaften für Sicherheitsfunktionen sowie Entwicklung von Prüfmethoden zur Feststellung der Aufrechterhaltung der technischen Eigenschaften bei der Geräteherstellung und bei Seriengeräten im Feld
- Grundlagen und Konzepte für die Integrität von Sicherheitsfunktionen, insbesondere zur Separation von Sicherheitsfunktionen auf einem Chip und der Vermeidung der Aufteilung auf mehrere Chips (z.B. Verlustleistungsabfuhr und -minimierung) sowie Absicherung von auf mehrere Chips verteilte Sicherheitsfunktionen
- Test- und Evaluierbarkeit von hochintegrierten Sicherheitsfunktionen und Absicherung für solche im Seriengerät verbleibende Schnittstellen

Hostbasierte Anomalieerkennung auf Rechnersystemen

Der Ansatz, vertrauenswürdige Systeme durch eine möglichst kleine, mit beweisbarer Sicherheit implementierte sog. Trusted Computing Base (TCB) zu realisieren, wird seit mehreren Jahrzehnten verfolgt und hat bisher noch keine, für eine breite Nutzung taugliche Plattform hervorgebracht. Dem relativ starren Ansatz einer minimalen TCB widerspricht zudem die Tendenz zu immer schnelleren Innovationszyklen im Bereich von kommerziellen Rechnerplattformen (Hardware und Betriebssysteme) und Anwendungen.

Immer mehr sicherheitskritische Prozesse und Anwendungen sowohl im Bereich Sicherheit als auch im Bereich Zuverlässigkeit werden mit Hilfe von konventionellen, handelsüblichen Rechnerplattformen, Betriebssystemen und Anwendungsprogrammen abgewickelt. Die Praxis hat gezeigt, dass nur bei ganz besonders sicherheitskritischen Anwendungen, z.B. im Bereich der Flugsicherheit, eine langwierige, tiefgreifende und systematische Analyse von Systemplattformen wirtschaftlich vertretbar ist. Durch die Zunahme diverser gegenseitiger Abhängigkeiten zwischen den verschiedensten Bereichen (z.B. globales Finanzwesen) können Störungen und Schäden an einem System katastrophale Auswirkungen auf andere Systeme haben.

Herausforderungen

Neben dem klassischen, aber in der Praxis nur eingeschränkt verwendbaren Ansatz der sicheren TCB, müssen neue Methoden erforscht werden, die es erlauben, handelsübliche Rechnersysteme engmaschig zu überwachen. Fehlfunktionen in Folge von Systemfehlern oder von Angriffen müssen frühzeitig erkannt werden, damit das System anschließend wieder in einen definierten Ausgangszustand überführt wird und das Ereignis nachgewiesen werden kann. Diese Ansätze müssen den technologischen Innovationen auf dem IT-Sektor schnell folgen können und flexibel an die Gegebenheiten der jeweiligen Anwendungen adaptiert werden können.

Die Aufgabe besteht vor allem darin, das Risiko für sicherheitskritische Anwendungen auch beim Einsatz per se nicht vertrauenswürdiger und nicht eingehend geprüfter Rechnerplattformen entscheidend zu minimieren. Zugleich sollen die erforschten Methoden flexibel und anpassungsfähig sein, um den rasanten Innovationen auf dem IT-Sektor folgen zu können.

Forschungsthemen

- Entwicklung eines neuen Ansatzes zur Anomalieerkennung auf handelsüblichen Rechnerplattformen und Betriebssystemen mit Fokus auf Hypervisor, Agentensystem und Softwaresensoren
- Analyse eines typischen Anwendungssystems und Entwicklung eines wirksamen Sicherheitszustandsmodells, basierend auf obigem Ansatz
- Spezifikation und prototypische Implementierung eines aussagefähigen Agenten-/Softwaresensorennetzwerkes auf einem Produktiv-System
- Penetration eines Produktiv-Systems (gemäß Stand der Technik) unter realistischen Umgebungs- und Einsatzbedingungen sowie Analyse des Reaktionsverhaltens des Hypervisor-/Softwaresensornetzwerks

Neue Herausforderungen zum Schutz von IKT-Systemen und der Identifikation von Schwachstellen

Die Angriffe auf IKT-Systeme werden zunehmend gezielter und reichen von organisierter Kriminalität über Wirtschaftsspionage bis hin zu Angriffen auf die Infrastruktur ganzer Staaten. Dies bedeutet, dass die IT-Systeme auch gegen sehr spezielle Angriffe abgesichert werden müssen, und es nicht ausreicht, sich auf die gängigen, derzeit bekannten Angriffe zu konzentrieren. Insbesondere werden Werkzeuge zum Nachweis gezielter Angriffe benötigt.

Der Schutz der IT-Systeme der Zukunft kann auf verschiedenen Wegen sichergestellt werden. Im Hinblick auf weitere Technologieentwicklungen der Zukunft muss aber in Betracht gezogen werden, dass heute als sicher angesehene Kryptographie durch spezielle Systeme der Zukunft (z.B. Quantencomputer) möglicherweise problemlos entschlüsselt werden kann. In diesem Zusammenhang gilt es, völlig neue Verfahren zu entwickeln, um auch die Daten der Zukunft vor unberechtigtem Zugriff zu sichern.

Ein weiterer, heute noch nicht ausreichend untersuchter Aspekt ist, Schutzmaßnahmen gegen indirekt ausgeführte Angriffe – so genannte Seitenkanalangriffe – zu finden. Hierbei kann einerseits bei der Entwicklung der Systeme darauf geachtet werden, dass das Design sicherer konzipiert wird, andererseits ist aber auch die Kenntnis der Angriffsmöglichkeiten gerade auf spezielle Funktionen oder Bausteine in IKT-Systemen wichtig, um Abwehrmaßnahmen entwickeln zu können.

Prioritärer Handlungsbedarf wird daher bei folgenden Themenbereichen gesehen:

- **Neue Analyseansätze bei Seitenkanalangriffen;**
- **Entwicklung analytischer und forensischer Werkzeuge;**
- **Quanteninformatik.**

Neue Analyseansätze bei Seitenkanalangriffen

Seitenkanalangriffe stellen eine reale Gefahr für sicherheitskritische IKT-Systeme dar, weil mit ihrer Hilfe Implementierungen grundsätzlich starker kryptographischer Algorithmen angegriffen und gebrochen werden können. Vor allem die Halbleiterhersteller besitzen auf diesem Gebiet hohe Expertise, und die Resistenz gegen Seitenkanalangriffe ist ein zentrales Designkriterium für Chipkarten.

Vereinfacht gesagt, zerfallen Seitenkanalangriffe in zwei Phasen. In Phase 1 werden Messungen am Zielobjekt (und ggf. an typgleichen „Trainingsobjekten“) durchgeführt, etwa einer Chipkarte oder einem PC. Diese Messreihen beinhalten üblicherweise Laufzeiten von kryptographischen Operationen oder deren Stromverbrauch. Ziel der Phase 2 ist es, aus den vorhandenen Messreihen die schlüsselabhängige (Nutz-)Information zu extrahieren. Ein erfolgreicher Angriff liefert dann den gesuchten Schlüssel. Phase 1 erfordert normalerweise ingenieurmäßige Expertise bzw. ein sehr gutes Verständnis von Rechnern und Betriebssystemen, während Phase 2 im Wesentlichen mathematische Probleme aufwirft.

Herausforderungen

In der Vergangenheit konnten viele Angriffe durch bessere mathematische Methoden in Phase 2 deutlich effizienter gestaltet werden, und zuweilen wurden neue Angriffe erst auf diese Weise möglich. Obwohl es bereits gemeinsame Projekte zwischen Mathematikern und Ingenieuren bzw. Mathematikern und Informatikern auf diesem Gebiet gab und gibt, ist eine langfristige Kooperationen erstrebenswert.

Seit einigen Jahren hat sich die Forschung auch verstärkt Seitenkanalangriffen gegen Softwareimplementierungen für PC oder Server zugewendet. Seitenkanalangriffe gegen FPGA und eingebettete Systeme wurden bislang jedoch noch nicht systematisch untersucht und sollen deshalb einen Schwerpunkt bilden.

Das finale Ziel ist das sichere Design von IT-Systemen. Viele Angriffe geben jedoch nur indirekt Informationen über die Ursachen bzw. die Schwachstellen, die den Angriff ermöglicht haben. Bereits 2005 wurde ein stochastischer Ansatz eingeführt und später weitergehend untersucht, der die Angriffsursachen quantifiziert, was wiederum ein Re-Design konstruktiv unterstützt. Dieser Ansatz sollte weiter verfolgt und vertieft werden, und ggf. sollten weitere Ansätze dieser Art entwickelt werden, um das Zusammenwirken von Sicherheitsanalyse und Design zu verbessern.

Forschungsthemen

- Untersuchung von Analogien und der Adaptionsfähigkeit von Seitenkanalangriffen gegen Chipkarten, FPGA und Sicherheitssoftware
- Untersuchung der Seitenkanalresistenz von eingebetteten Systemen mit sicherheitskritischen Anwendungen
- Verbindung ingenieurmäßiger Ansätze bei Seitenkanalangriffen mit mathematischen Methoden und Einbettung in eine mathematische Theorie, u.a. um das tatsächliche Risikopotential von Angriffen zuverlässig abschätzen zu können
- Gezielte Nutzung von abgeleiteten Informationen aus Angriffen zum konstruktiven Re-Design und zur Konzeption unterstützender Werkzeuge zu diesem Zweck

Entwicklung analytischer und forensischer Werkzeuge

Derzeit gibt es keine Untersuchungen über Werkzeuge zur systematischen Analyse von Schwachstellen in Software, mit der Administratoren und Softwareanbieter den Sicherheitsstandard ihrer Produkte testen können. Es fehlen etablierte Werkzeuge zur praxistauglichen Analyse von Anomalien in IT-Systemen.

Weiterhin fehlt eine offen nutzbare Datenbank mit korrekten Signaturen von Standardsoftware, um die Integrität einer Systemkonfiguration zu testen. Während Angreifer „Seitenkanalangriffe“ nutzen, um Schwachstellen beispielsweise bei Verschlüsselungsverfahren, auszunutzen, bleibt deren Potential zur systematischen Verbesserung der Systemsicherheit ungenutzt.

Herausforderungen

Zentrale Aufgabe ist die Stärkung der forensischen IT durch die Entwicklung innovativer Werkzeuge. Insbesondere gilt es Anreize zu geben, IT-Sicherheitsprobleme zu identifizieren und zu beseitigen, und dieses Wissen in die Praxis zu transferieren, geeignete komplexe analytische und forensische Werkzeuge zu entwickeln, sowie analytische Werkzeuge zu systematisieren und für Entwicklungen zur Verbesserung der IT-Sicherheit zu optimieren.

Forschungsthemen

- Weiterentwicklung forensischer Werkzeuge (einschließlich revisionssicherer Verfahren) zur besseren Nutzbarkeit für einen größeren Kreis von Anwendern
- Verbesserung der Leistungsfähigkeit forensischer Werkzeuge, insbesondere für die Analyse im laufenden Betrieb, bei großen Datenmengen, zur Binärcodeanalyse sowie bei der Analyse von Schadcode und kryptierter Daten
- Weiterentwicklung von Analysetechniken und -methoden auf formaler und praktischer Ebene, insbesondere von formalen Methoden zum Nachweis von Systemeigenschaften und zur theoretischen und praktischen Evaluation von Systemen

Quanteninformatik

In den vergangenen Jahren hat es erhebliche Fortschritte in der Grundlagenarbeit zur Realisierbarkeit von Quantencomputern gegeben. Falls Quantencomputer in einer bestimmten Größenordnung technisch realisiert werden, können sie bestimmte Aufgaben um Größenordnungen effizienter erledigen als herkömmliche Computer und viele der zur Zeit gängigen kryptographischen Algorithmen faktisch brechen.

Kurz- und mittelfristig stellen Quantencomputer zwar noch keine Gefahr für die gängigen kryptographischen Algorithmen dar. Allerdings gibt es Daten, die langfristig geheim gehalten werden müssen. Daher ist es notwendig, bereits heute über Alternativen nachzudenken und diese in absehbarer Zeit auch bereitzustellen.

Herausforderungen

Benötigt werden kryptographische Algorithmen, die Quantencomputern widerstehen, gleichzeitig aber auch durch „klassische“ kryptanalytische Angriffe nicht überwunden werden können. In der Forschung werden verschiedene Alternativen diskutiert. Allerdings ist die Effizienz dieser Verfahren (Speicherplatzbedarf, Laufzeit) um Größenordnungen geringer als die der heute üblichen (prinzipiell durch Quantencomputer gefährdeten) kryptographischen Algorithmen und Protokolle.

Einige dieser Algorithmen überfordern insbesondere die Ressourcen der heute gängigen Chipkarten. Der Entwicklung effizienter und effizient implementierbarer kryptographischer Algorithmen und Protokolle, die gegen Quantencomputer und gegen klassische Kryptanalyse resistent sind, kommt deshalb eine besondere Bedeutung zu. Ebenso ist die Sicherheit ihrer Implementierung (z.B. in Chipkarten) von großer Bedeutung. Diese muss z.B. Seitenkanalangriffen und Fault Attacks widerstehen. In dieser Hinsicht unterscheiden sich „klassische“ kryptographische Algorithmen nicht von quantencomputerresistenten Algorithmen.

Forschungsthemen

- Identifizierung kritischer Anwendungen mittels Risikoanalyse
- Entwicklung effizient implementierbarer kryptographischer Algorithmen und Protokolle, die gegen Quantencomputer (und gegen klassische Kryptanalyse) resistent sind
- Chipkarten-basierte Sicherheitsimplementierung von quantencomputerresistenten Kryptoverfahren und deren Integration in sicherheitskritische Applikationen

Operative Umsetzung

Die Umsetzung des vorliegenden Arbeitsprogramms erfolgt unter dem Dach des BMBF-Programms „IKT 2020 – Forschung für Innovationen“ gemeinsam durch BMBF und BMI. Grundlage für die Förderung im Bereich IT-Sicherheitsforschung im Rahmen der direkten Projektförderung ist der in Kapitel 3 abgesteckte thematische Rahmen. Für eine Laufzeit von 5 Jahren werden vom BMBF hierfür Fördermittel in Höhe von 30 Mio. Euro bereitgestellt.

Sowohl Unternehmen der gewerblichen Wirtschaft (mit Sitz und überwiegender Ergebnisverwertung in Deutschland) als auch Hochschulen, Forschungseinrichtungen und andere FuE-Institutionen sowie Behörden können sich an diesem Programm beteiligen. Einschränkungen sind möglich, sofern dies die Sicherheitsinteressen Deutschlands erfordern. Die Beteiligung kleiner und mittlerer Unternehmen wird ausdrücklich begrüßt.

Aktuelle Bekanntmachungen zu den Förderschwerpunkten werden gemeinsam durch BMBF und BMI erarbeitet, im Bundesanzeiger veröffentlicht und über die Internetseiten der Förderinstitutionen verbreitet. Mit diesen werden die Fördermodalitäten und -regularien verbindlich festgelegt.

Bundesministerium
für Bildung
und Forschung

Bundesministerium
des Innern