



Internet der Zukunft

1. Koordinator der Vorschläge

Prof. Dr. Hannes Federrath, Universität Hamburg, Fachbereich Informatik, Vogt-Kölln-Str. 30, 22527 Hamburg

2. Titel der Grand Challenge

Internet der Zukunft – sicher, schnell, vertrauenswürdig

3. Allgemein verständliche Kurzfassung der Grand Challenge

In den 40 Jahren des Bestehens des Internets lässt sich eine zunehmende Diskrepanz zwischen seiner immensen gesellschaftlichen, wirtschaftlichen und politischen Bedeutung und der nur zaghaften Weiterentwicklung seiner technischen Basisprotokolle erkennen. Ursprünglich waren die Protokolle des Internets aus Sicherheitssicht bestenfalls auf hohe Verfügbarkeit ausgerichtet. Vertraulichkeit und Authentizität spielten keine große Rolle. Für seine heutige Rolle wurde das Internet nicht konzipiert. Seine Weiterentwicklung zu einem sicheren, vertrauenswürdigen und störungsfrei nutzbaren Netz der Zukunft ist eine dringende und herausfordernde Aufgabe für die Informatik.

4. Beschreibung der Grand Challenge

Das Netz der Zukunft muss als Kommunikations- und Informationsinfrastruktur wie das bisherige Internet die Bedürfnisse der Wirtschaft und die individuellen Kommunikationsbedürfnisse befriedigen, darf dabei aber die Defizite des derzeitigen Internets nicht aufweisen:

1. Ein Grundproblem ist der Konflikt zwischen Privatsphäre und Eindeutigkeit im Internet. Privatsphäre erfordert Vertraulichkeit und Anonymität. Eindeutigkeit erfordert Authentizität und Autorisierung.

- Daten dürfen grundsätzlich nicht ausgespäht oder unbefugt modifiziert werden. Jeder Internetnutzer soll seine Identität geheim halten können. Der Absender von Nachrichten muss aber auf Wunsch eindeutig vom Empfänger identifizierbar sein. Entsprechendes gilt für den Urheber von Aktivitäten. Nur die wirklich berechtigten Personen dürfen entsprechende Aktionen durchführen. Diesen Zielkonflikt adressiert die sog. mehrseitige Sicherheit. Die Herausforderung an die Informatik besteht in der Bereitstellung von Verfahren, die eine mehrseitige Sicherheit bieten.
- Zweckgebundene sensitive oder persönliche Daten dürfen nur für den angegebenen Zweck verwendet werden können. Diese Zweckbestimmung muss auch durchsetzbar sein. Die Herausforderung an die Informatik ist also, Verfahren zu entwickeln, mit denen sensitive persönliche Daten für einen konkreten und benannten Zweck bereitgestellt werden können. Da digitale Daten beliebig vervielfältigt werden können, ist



Internet der Zukunft

es technisch kaum möglich, einen Missbrauch zu verhindern. Mindestens muss aber erkennbar sein, dass Daten entgegen dem ursprünglichen Zweck verwendet werden.

2. Kriminelle Handlungen müssen möglichst verhindert oder wenigstens geahndet werden können (z.B. kollektives Mobbing, Verabredung zu terroristischen Anschlägen), insbesondere solche, die erst durch das Netz möglich werden und solche, die das Netz betreffen (z.B. distributed denial of service). Spam soll nicht durch erst den Empfänger (teilweise automatisch) erkannt werden, sondern darf nicht die Infrastruktur erheblich belasten. Dasselbe gilt im noch verstärkten Maße für Malware.

3. Jeder Nutzer soll ein Bewusstsein für den Vertraulichkeitsstatus seiner Daten und Nachrichten besitzen bzw. für die Verlässlichkeit der über das Internet erhältlichen Informationen. Dies erfordert einerseits grundsätzlich eine Stärkung der Medienkompetenz, andererseits aber auch eine entsprechende Darstellung in den Benutzungsschnittstellen.

Zur Realisierung dieser Anforderungen werden neue Mechanismen, Protokolle und Verfahren benötigt.

5. Warum ist das Problem schwierig?

Zur Verbesserung des Internets gab es schon Dutzende Vorschläge, insbesondere aus der Informatikforschung. Bislang hatte die Informatik aber bei der Gestaltung, dem Wachstum und der Verwendung des Internets eher die Rolle des Beobachters als die des Gestalters. Teil der großen Herausforderung, und vielleicht schwieriger als inhaltliche Aspekte, ist die Fragestellung, wie die Informatik (als integrierende Wissenschaft, wenn auch mit Unterstützung benachbarter Wissenschaften) bei der Weitergestaltung und Erneuerung des Internets die maßgebliche gestaltende Rolle erhält, die ihr vernünftigerweise zusteht. Nur die Informatik als Disziplin verfügt über entsprechende Kompetenzen und inhaltliche Breite, dies insbesondere weil in der Informatik technische Aspekte, Aspekte der Sicherheit, aber auch gesellschaftliche und ethische Aspekte diskutiert werden. Nur in diesem Zusammenspiel ist eine vernünftige Herangehensweise möglich.

Ein sicheres, schnelles und vertrauenswürdiges Netz der Zukunft kann nur entstehen, wenn zunächst viele schwierige Einzelprobleme gelöst sind und anschließend auch ein entsprechendes Gesamtsystem entsteht, das nachweislich den Anforderungen entspricht. Allein der scheinbare Widerspruch zwischen Offenheit des Internets und notwendiger Kontrolle zur Schadenabwehr ist ein solches Einzelproblem. Noch schwieriger scheint aber das Zusammenspiel der verschiedenen Aspekte zu sein.

6. In welchem Zeithorizont erwarten Sie eine Lösung?

In 5 bis 15 Jahren kann eine Lösung erreicht werden, durch schrittweise Veränderung des existierenden Internets oder durch ein gänzlich neues Netz.



Internet der Zukunft

7. Welche Anstrengungen wurden bereits in die Lösung investiert und welche Disziplinen müssten zusammenarbeiten?

Es gibt vielfältige singuläre Lösungsansätze, aber unseres Wissens keine konzertierte Aktion der gesamten Informatik, die im Rahmen einer „Grand Challenge“ möglich und auch nötig wäre. Innerhalb der Informatik sind in jedem Fall zu beteiligen: alle Fachrichtungen der Informatik, Forschungsgruppen und Experten an Hochschulen, in der Industrie und der Verwaltung, Normengremien (ISO, W3C), außerdem mindestens die Gebiete Elektrotechnik, Wirtschaftswissenschaften, Psychologie und Rechtswissenschaften.

Lösungen können auf dem existierenden Internet basieren oder dieses grundlegend erneuern. Sie können aber auch ein internationales, nationales oder europäisches neues Netz sein mit Schnittstellen zum weiterhin existierenden Internet. Zudem könnte es zukünftig ganz andere Geschäftsmodelle geben, zum Beispiel kostenpflichtige Dienste mit garantierten Eigenschaften. Derlei Fragestellungen sind nur interdisziplinär zu beantworten.

8. Bitte beschreiben Sie die mögliche Lösung der Grand Challenge in einem leicht verständlichen Ziel-Szenario.

Ein Netz der Zukunft ist offen gestaltet. Dienste können ohne Beschränkungen für beliebige Kommunikationsformen (Text, Sprache, Bilder, Video etc.), den Austausch von Daten und (digitalen) Gütern verwendet werden. Alle Dienste sind mit einem mobilen, vertrauenswürdigen Endgerät in der Hand des Endnutzers verwendbar. Dieses Gerät enthält sicheren Speicher für persönliche Daten des Nutzers und sicheren Speicher für Daten von Diensten. Die Speicherbereiche sind definiert voneinander abgegrenzt.

Auch Sensoren werden als offene Systeme innerhalb dieses Netzes sicher angebunden.

Die Kommunikation zwischen allen Geräten findet stets verschlüsselt und authentifiziert statt. Pseudonyme (zum Schutz der Identität) ermöglichen den authentifizierten Datenaustausch bei gleichzeitiger Ermöglichung von Privatheit.

Ein Netz der Zukunft verzichtet weitgehend auf Medienbrüche, es sei denn sie sind vom Nutzer gewünscht oder rechtlich (oder aus anderen nicht-technischen Gründen) notwendig. Mit dem persönlichen mobilen Endgerät des Nutzers werden sehr viele verschiedene Nutzungsarten ermöglicht, z.B. die (bargeldlose und anonyme) Bezahlung in Geschäften, in Verkehrssystemen und im Internet oder auch die Vorlage eines (digitalen) Ausweises bei Sicherheitsbehörden, an der Grenze und im Internet.

Bei Unterstützung von (digitalen) Pseudonymen werden auch (digitale) Nachweise von Eigenschaften (z.B. Volljährigkeit) ohne Offenlegung identifizierender Informationen möglich



Internet der Zukunft

und damit sogar Anwendungen, die heute in der physischen Welt nicht ohne Weiteres realisierbar sind.

9. Bitte benennen Sie eine Ziellinie, anhand derer die Herausforderung als gelöst betrachtet werden kann.

Die Grand Challenge, die wir in einem sicheren Netz der Zukunft sehen, kann nur schrittweise realisiert werden. Daher ist es kaum möglich, eine Ziellinie zu benennen. Einen Zeithorizont als Ziellinie haben wir bereits genannt.

10. Welche sozialen / gesellschaftlichen / ökonomischen Probleme lassen sich mit der Grand Challenge adressieren?

Insbesondere nach dem Bekanntwerden der Überwachungsmöglichkeiten durch die NSA ist klar, dass ein sicheres Netz der Zukunft notwendig ist. Es wäre mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar, wenn sich beim normalen Internetnutzer die Meinung festigt, eine (abhör)-sichere Kommunikationsinfrastruktur könne es nicht geben. Ebenso schlecht wäre es, wenn urheberrechtlich geschützte und/oder strafrechtlich relevante Inhalte technisch schrankenlos im Internet verbreitet werden könnten. Praktisch tragfähige Lösungen für derartige Probleme existieren nicht. Zudem gibt es noch einen erheblichen Forschungsbedarf, sowohl innerhalb der oben genannten Teildisziplinen der Informatik als auch übergreifend und interdisziplinär.

Die in diesem Vorschlag genannte Herausforderung muss nicht öffentlich beworben werden, sie ist bereits in der öffentlichen Diskussion präsent. Allerdings wird weder die Fragestellung noch die Kompetenz für Lösungen unmittelbar mit dem Fach Informatik assoziiert, geschweige denn mit der Gesellschaft für Informatik.

11. Weiterführende Literatur (wenn nötig oder gewünscht)

Forderungen nach einem „neuen Internet“ findet man seit geraumer Zeit in der Presse. Die aktuellen politischen Entwicklungen lassen sogar einen entsprechenden Hype erkennen, der von öffentlichen Rundfunkanstalten bis zur Boulevard-Presse reicht. Beispiele:

- DIE ZEIT vom 12.09.2011: *Baut ein neues Internet!*
- DIE ZEIT vom 31. August 2012: *Das neue Internet*. Zitiert wird: Michel Bauwens, Gründer der Stiftung P2P und ehemals Analyst der United States Information Agency
- Technology Review vom 28.08.2013: *Was wir brauchen, ist ein neues Internet*. Zitiert wird: Daniel Suarez, „Star-Autor des Silicon Valley“ (früher IT-Berater)
- ADMIN IT-Praxis & Strategie 11/2013: *Ein neues Internet*. Zitiert wird der Krypto-Experte Bruce Schneier.
- WDR 5 (04.01.2014): „Computerexperten fordern neues Internet - Ein Netz ohne NSA“. Bezieht sich auf: Chaos Computer Club („Das Internet müsse neu erfunden



Internet der Zukunft

werden, so die Forderung“). Weiter werden indirekt zitiert: US-Medientheoretiker Douglas Rushkoff, „zahlreiche Programmierer“, Faroo-Mitgründer Wolf Garbe, Gründer von Diaspora.

Es geht hier also nicht darum, die Öffentlichkeit von der Dringlichkeit einer Grand Challenge zu überzeugen, sondern deutlich zu machen, dass es sich um *unsere* Grand Challenge handelt.

12. Unterstützende GI-Gliederungen (Fachbereiche, Fachgruppen), Mitautoren

Prof. Dr. Jörg Desel, Sprecher des GI-Fachbereichs IAD, Fernuniversität Hagen, Universitätsstraße 1, 58097 Hagen

Prof. Dr. Albert Endres, Iselerstr.1, 71067 Sindelfingen

Dr. rer. pol. Dipl.-Inf. Patrick Stoll, Schwabstrasse 1, 72574 Bad Urach