

"Internet und Kommunikation: zuverlässig, sicher, allgegenwärtig?"

Prof. Dr. Dieter Hogrefe, Institut für Informatik, Georg-August-Universität Göttingen

Dienstag, 26.09.06 – Altes Rathaus der Stadt Göttingen, 18:30 Uhr

Wir alle nutzen heute das Internet auf vielfältige Arten und Weisen: Bankgeschäfte, Telefonieren, Kaufen/Verkaufen, Informationen aller Art beschaffen oder Spielen. Inwieweit kann man dem Medium eigentlich trauen, das man da nutzt, wie verlässlich ist es eigentlich im Sinne der Bereitstellung eines Dienstes zu einer bestimmten Zeit an einem bestimmten Ort in der gewünschten Qualität und Sicherheit?

Es ist davon auszugehen und wird sogar von den Nutzern zunehmend erwartet, dass das Internet in der Zukunft allgegenwärtig ist, wir also ständig und überall darauf Zugriff haben, so wie wir heute ständig und überall telefonieren können, wenn wir möchten, ohne auf Telefonzellen und Kleingeld angewiesen zu sein. Wenn man mal kein „Handynetz“ hat, sich z.B. in einem Funkloch befindet, wird das bereits als großer Mangel empfunden: „Wo sind wir denn hier gelandet?“. Was heute für das Telefonieren gilt, wird morgen für den Zugriff auf das Internet mit all seinen Informationsmöglichkeiten gelten. Eigentlich befinden wir uns bereits in diesem Zustand, ohne dass die Gesellschaft das wirklich realisiert. Allerdings hat der ubiquitäre (allgegenwärtige) Internetzugang derzeit noch immer Experimentiercharakter, ist also derzeit eher etwas für eingeweihte Bastler. Das wird sich allerdings ändern. Es ist dabei festzustellen, dass der ubiquitäre Internetzugang eine ökonomische Fragestellung ist, d.h. immer und überall online sein, wird generell teurer sein, als z.B. gelegentlich vom häuslichen DSL-Anschluss das Internet zu nutzen.

In dieser Situation des allgegenwärtigen Internets, stellt sich schnell die berühmte „Big Brother is watching you“-Frage: Wie steht es eigentlich mit Vertraulichkeit, Privatsphäre, und Sicherheit im Allgemeinen?

Es gibt eine Reihe von Sicherheitsinstrumenten wie Verschlüsselung, Authentifizierung, etc., die viele von uns nutzen. Im Allgemeinen soll ein Sicherheits-Mechanismus dazu da sein, gegen böswillige Beteiligte zu schützen. Wenn man das so versteht, dann gibt es aber eine ganze Menge Sicherheitsherausforderungen, denen nicht mit herkömmlichen Instrumenten begegnet werden kann. Traditionelle Instrumente schützen typischerweise Ressourcen vor

böswilligen Nutzern, indem der Zugriff nur den autorisierten Nutzern gewährt wird. Allerdings muss sich der einzelne Benutzer selbst auch oft gegen solche Beteiligte schützen, die böswillige Dienste anbieten. Technisch gesehen geht das in manchen Fällen mit Firewalls, allerdings nur auf sehr niedriger semantischer Ebene. Es geht z.B. dann nicht, wenn wir explizit Dienste in Anspruch nehmen möchten und nicht wissen, ob sie böswillig sind oder nicht. So könnte z.B. ein Informationsanbieter zu seinem eigenen Vorteil absichtlich falsche Informationen anbieten. Dagegen können die traditionellen Sicherheitsmechanismen nicht schützen.

Um diesen Sicherheitsherausforderungen zu begegnen, geraten sog. Vertrauens- und Reputationssysteme [1] immer mehr in den Blickpunkt. Man bezeichnet das neuerdings auch als „Soft-Security“ im Gegensatz zu der herkömmlichen „Hard-Security“.

Reputation ist ein kollektives Maß für Vertrauen im Sinne von Zuverlässigkeit, das auf Bewertungen oder Referenzen von Mitgliedern einer Gemeinschaft basiert. Das subjektive Vertrauensempfinden kann aus der Kombination der Referenzen und eigener Erfahrung abgeleitet werden. Reputation können Individuen oder Gruppen haben. Die Reputation der Gruppe könnte sich aus der durchschnittlichen Reputation der Mitglieder errechnen.

Im Fall von Gruppen leitet sich die Reputation eines Gruppenmitglieds a priori aus der Reputation der Gruppe ab. Um Korrelationen und Rekursionen zu vermeiden, dürfen sich Referenzen möglichst nur auf Erfahrungen aus erster Hand beziehen und nicht auf andere Referenzen, um Gerüchten vorzubeugen. Von diesem Prinzip könnte abgewichen werden, wenn die Referenzen normalisiert werden, also z.B. mit der Länge der Referenzkette gewichtet werden.

Es gibt einige wichtige Unterschiede zwischen traditionellen und Online-Umgebungen im Zusammenhang mit Vertrauen und Reputation. Traditionelle, auf physischem Kontakt basierende Wege Vertrauen und Reputation zu erlangen, fehlen in einer Online Umgebung. Information über Vertrauen und Reputation existiert in traditionellen Umgebungen lokal und/oder in sehr begrenzten Gemeinschaften, im Online-Fall dagegen auf einer globalen Skala.

Daraus ergibt sich die Frage, welche Informationselemente es als adäquate Substitute für die traditionellen Hinweise auf Vertrauen und Reputation in einer Online-Umgebung gibt und wie das Internet bzw. die IT allgemein dazu genutzt werden kann, diese Informationen zu sammeln. Dabei sollte Resistenz gegen Attacks und Manipulationsstrategien ebenso berücksichtigt werden wie Effizienz und Benutzerfreundlichkeit. Wie die Benutzer diese Informationen in ihre Entscheidungsprozesse integrieren, welche Rolle solche Systeme im Geschäftsmodell von kommerziellen Akteuren spielen und wie die Systeme die Qualität von Online-Interaktionen und –Handel verbessern können, sind in diesem Zusammenhang weitere interessante Fragestellungen.

Dabei sind die grundlegenden Prinzipien von Reputationssystemen zunächst relativ simpel [3]:

- Entitäten müssen langlebig sein, so dass bei jeder Interaktion die Erwartung an eine zukünftige Interaktion bestehen kann
- Bewertungen über vergangene Interaktionen müssen in Entscheidungen gegenwärtiger Interaktionen einfließen
- Bewertungen über gegenwärtige Interaktionen müssen gesammelt und verteilt werden

Demgegenüber ist der Begriff des Vertrauens sehr vage, so dass das, was ein Vertrauenssystem ausmacht sehr schwer präzise zu beschreiben ist. Auf jeden Fall ist das Transitivitätsprinzip ein natürliches Element eines Vertrauenssystems. Die Idee hinter Transitivität ist, dass wenn Alice Bob vertraut und Bob Claire vertraut und Bob Claire an Alice empfiehlt, dann kann Alice ein gewisses Maß an Vertrauen in Claire ableiten, basierend auf einer Kombination von Bobs Empfehlung und dem eigenen Vertrauen in Bob.

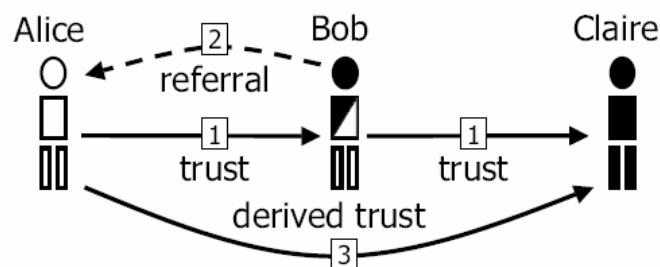


Fig. 1 Transitivitätsprinzip

Es gibt allerdings eine semantische Einschränkung für die Transitivität von Vertrauen, nämlich dass Bob Claire in einem bestimmten Zusammenhang vertrauen muss und Bob Claire an Alice in diesem gleichen Zusammenhang empfehlen muss, damit Alice Claire in diesem Zusammenhang vertrauen kann.

Um die Frage beantworten zu können, ob jemandem, der einen Reputationswert über eine Sache, Person oder Dienstleistung erzeugt, vertraut werden kann, hängen Reputations- und Vertrauenssysteme oftmals eng miteinander zusammen und werden auch kombiniert eingesetzt.

Dennoch gibt es Unterschiede zwischen Vertrauens- und Reputationssystemen. Vertrauenssysteme produzieren einen Wert, der für einen Vertrauenden die subjektive Vertrauenswürdigkeit einer Entität widerspiegelt. Reputationssysteme hingegen produzieren einen (öffentlich zugänglichen) Reputationswert einer Entität, wie er von der gesamten Gemeinschaft gesehen wird. Die Annahme ist, dass alle Nutzer den gleichen „Geschmack“ haben, zumindest bei negativen Reputationsaussagen. Ziel ist es schlechte Dienste, etc. zu „bestrafen“. Der Geschmack kann in Form von sog. „Colaborative Filtering“ Systemen mit berücksichtigt werden, in denen der Reputationswert dann auch noch mit dem Geschmack des Bewerter gewichtet wird. Dazu müssen Informationen über den Geschmack der Nutzer eingeholt und gespeichert werden, was wiederum gewisse Datenschutzaspekte anschließt, denn diese Information kann auch genutzt werden, um gezielt für Produkte zu werben.

Reputationssysteme können zentral oder dezentral aufgebaut sein. In einem zentralen System sammelt ein „Reputation Centre“ die Reputationswerte, von wo sie dann wieder abgefragt werden können.

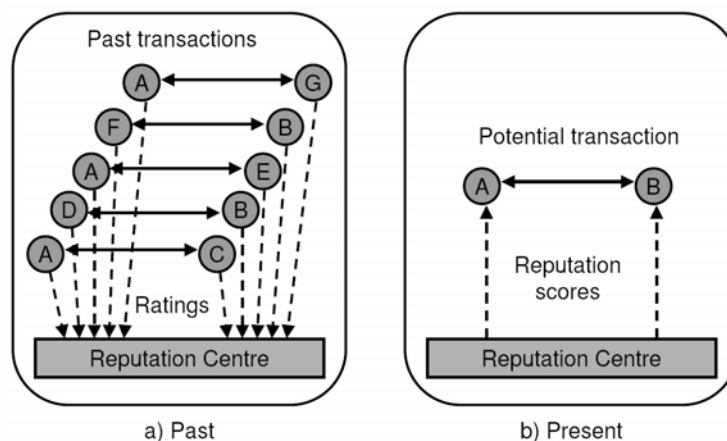


Fig. 2 Zentralisiertes Reputationssystem

In manchen Fällen kann es sinnvoll sein, das Reputationssystem nicht zu zentralisieren, sondern die Reputationswerte verteilt zu halten. Es werden dann keine zentralen Funktionen benötigt. Ein Reputationswert bleibt in diesem Fall stets bei dem Urheber des Wertes und wird nur nach Bedarf von einem Teilnehmer abgerufen. Ein Interessent sucht sich also bei

Bedarf nach einem bestimmten Schema (dazu könnte es natürlich auch wieder ein zentrales Directory geben) die einzelnen Reputationswerte zusammen und berechnet daraus einen individuellen Wert, der dann auch abhängig von bestimmten persönlichen Erfahrungen sein. P2P-Netze sind eine ideale Umgebung, in der so etwas funktioniert, weil dort jeder Netzknoten gleichzeitig Client und Server ist, also Mechanismen existieren, die eigenen Ressourcen zur Verfügung zu stellen.

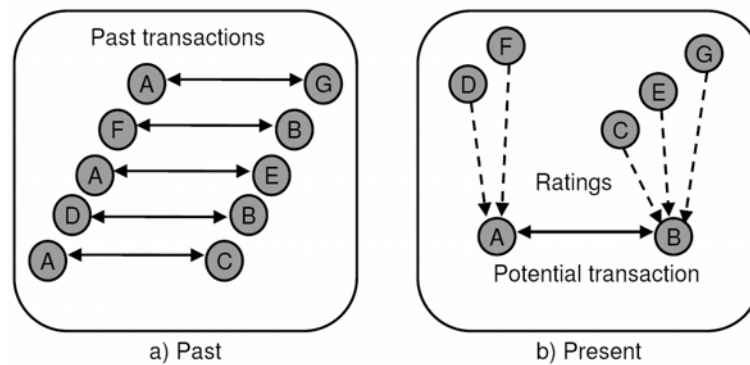


Fig. 3 Dezentrales Reputationssystem

Vertrauenssysteme sind in der Regel in Form von Vertrauensnetzen organisiert. Dazu wird zunächst auf ein einfaches bewährtes zwischenmenschliches Funktionsprinzip zurückgegriffen: ich vertraue jedem, dem jemandem vertraut, dem ich vertraue. Und umgekehrt: jeder, der jemandem vertraut, der mir vertraut, vertraut auch mir.

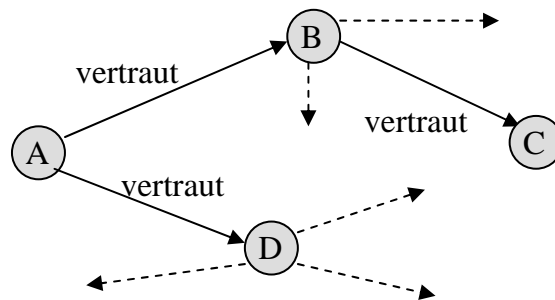


Fig. 4 Vertrauensnetz

Da einem i.d.R. die Bewerter, die Urteile über eine Sache, Person, Dienstleistung fällen, nicht bekannt sind, ist ein Vertrauensnetz hilfreich, deren Glaubwürdigkeit einzuschätzen. Vertrauen ist niemals etwas Absolutes sondern etwas graduelles. Um nun feststellen zu können, wie sehr man einer fremden Entität trauen kann, kann man einfache und intuitive Regeln in dem Vertrauensnetz anwenden, z.B. die folgenden.

In einem Vertrauensnetz ergeben sich Vertrauenspfade. Je kürzer der Vertrauenspfad ist, desto höher das Vertrauen. Je mehr Vertrauenspfade es zu einem Knoten gibt, desto höher das Vertrauen.

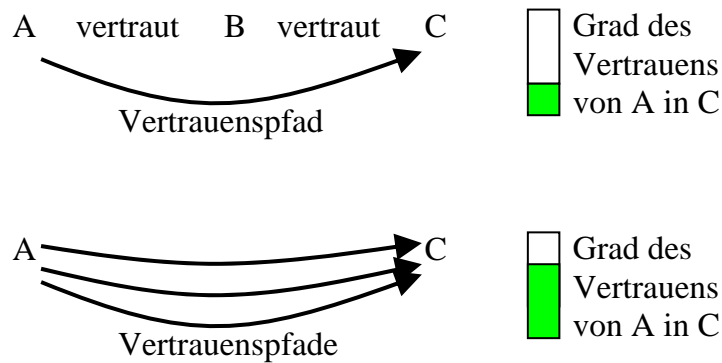


Fig. 5 Vertrauenspfade in einem Vertrauensnetz

Guha, et.al. [2] haben sich 2004 mit der Frage auseinandergesetzt, ob es ein Vorteil ist, wenn ein Vertrauenssystem neben Vertrauensbeziehungen auch Misstrauensbeziehungen beinhaltet, und ob es Algorithmen gibt, die dann Vertrauensbeziehungen berechnen können. Ausgangsüberlegung dabei: ein Vertrauenswert von 0 muss nicht gleichbedeutend mit Misstrauen sein, sondern kann bedeuten, dass man keine Aussage über den Grad des Vertrauens machen kann. Misstrauen ist also eher als negatives Vertrauen zu interpretieren. Guha, et.al. haben ein formales Schema entwickelt, wie Vertrauen und Misstrauen in ein Vertrauensnetz eingebracht und verarbeitet werden können. Sie konnten empirisch mit Hilfe des Epinions-Systems (www.epinions.com) zeigen, dass eine kleine Anzahl Vertrauens- und Misstrauensbeziehungen für jedes Individuum reichen, um Vertrauen zwischen zwei beliebigen Individuen vorauszusagen, besser als ohne Misstrauensbeziehungen.

Zusammenfassend kann gesagt werden, dass herkömmliche Vorstellungen von Sicherheit und Zuverlässigkeit für Transaktionen im Internet nicht ausreichen und „Soft-Security“ als Ergänzung zunehmend wichtiger wird. Darüber hinaus stellt sich zukünftig die Frage, ob „Soft-security“ auch für automatisierte Informationsdienste (Temperaturmessungen, etc.) verwendet werden könnte und ob Vertrauen in das korrekte Funktionieren von Geräten auf diese Weise bestimmt werden kann.

Literatur:

- [1] A. Jøsang, R. Ismail, C. Boyd: A Survey of Trust and Reputation Systems for Online Service Provision, Decision Support Systems, July 2005.
- [2] R. Guha, et al.: Propagation of trust and distrust, Proceedings of the 13th international conference on World Wide Web, 2004.
- [3] P. Resnick, R. Zeckhauser, R. Friedman, and K. Kuwabara. Reputation Systems. Communications of the ACM, 43(12):45-48, December 2000.