Kontrolle ist gut, Vertrauen ist besser

Transparentere Sicherheit – von persönlicher Interaktion bis zum globalen Internet

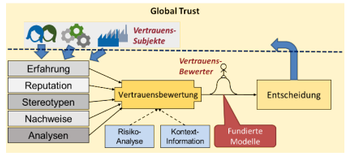
CROSSING Projekt S1: Scalable Trust Infrastructures / Skalierbare Vertrauens-Infrastrukturen

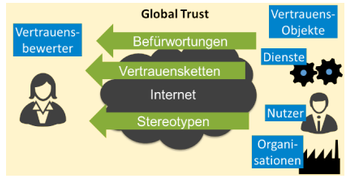
Prof. Matthias Hollick betreut den Teilbereich „Local Trust“ im Projekt S1 „Scalable Trust Infrastructures“ des Sonderforschungsbereichs CROSSING und ist Leiter des Fachgebiets SEEMOO (Secure Mobile Networking) an der TU Darmstadt.

Prof. Max Mühlhäuser betreut den Teilbereich „Global Trust“ im Projekt S1 „Scalable Trust Infrastructures“ des Sonderforschungsbereichs CROSSING und ist Leiter des Fachgebiets Telekooperation an der TU Darmstadt

Wer im Internet seine Kreditkarteninformationen oder andere sensible Daten eingibt, sollte vorher immer einen Blick auf die Adresszeile seines Browsers werfen: Signalisiert dort ein grünes Schloss, dass die Verbindung gesichert ist und der Server sich mit einem Zertifikat ausgewiesen hat? Doch die Aussagekraft dieses grünen Schlosses trügt, denn sie gaukelt vollkommene Sicherheit vor, warnt Professor Max Mühlhäuser, Principal Investigator im CROSSING-Projekt S1. „Das ist wie die Frage: Ist Deine Wohnung einbruchssicher? Jeder weiß, dass die Sicherheit einer Wohnung relativ ist: je mehr und je klüger man investiert, desto mehr Sicherheit bekommt man.“ Genauso müsse man die Sicherheit online differenzierter bewerten: „Eine mehrstufige Farbcodierung könnte ein erster Schritt sein, um das Maß der Sicherheit zu signalisieren“, sagt Mühlhäuser. Doch wie bestimmt man dieses Maß? Das sei extrem schwierig, so der CROSSING-Forscher, denn es gebe viele Schwachstellen: ein mithörender „Keyboard Logger“, ein Virus im eigenen Betriebssystem oder Browser, unsichere Protokoll-Versionen, Schlamperei der Programmierer oder IT-Kräfte auf der Server-Seite, und vieles mehr – nicht zuletzt die Vertrauenswürdigkeit jener Zertifizierungsstellen, die die Echtheit des Zertifikats sicherstellen sollen, mit dem ein Server sich ausweist.

„Das heutige Zertifikatssystem ist nicht sicher genug“, ergänzt Professor Matthias Hollick, ebenfalls Principal Investigator im CROSSING Projekt S1. Eine einzige Schwachstelle, ein sogenannter „single point of failure“, genügt – und die Gesamtsicherheit kann nicht mehr garantiert werden. Die Zertifizierungsbehörden könnten beispielsweise über einen unzuverlässigen Mitarbeiter einer Manipulation zum Opfer fallen. Wie in der Wohnung eine schlecht gesicherte Haustür, ist auch in der Online-Situation die größte Schwachstelle eine wichtige Größe für die Gesamtsicherheit. Die Bewertung der Vertrauenswürdigkeit ist aber nicht nur bei Webseiten und E-Mails wichtig. In Zukunft könne man diese auch für die digitale Identität von Personen, ein intelligentes Türschloss oder einen mit diversen Sensoren vernetzten Insulin-Dosimeter benötigen, erläutert Hollick weitere praktische Beispiele.





Ziel des Projekts „Skalierbare Vertrauens-Infrastrukturen“ ist es, neue Vertrauensbewertungskonzepte für die Sicherheit von beliebigen Nutzungsszenarien vernetzter Computer zu erforschen. Beliebig bedeutet dabei auch, dass eine größtmögliche Heterogenität an Geräten unterstützt werden soll. Bei der Lösung dieser Herausforderung gilt es, zwei Dimensionen zu beachten: „Local Trust“ und „Global Trust“.

Local Trust: Vertrauen in den Cyberspace bringen

Matthias Hollick betreut den Teilbereich „Local Trust“, dessen Ziel es ist, das Vertrauen aus der physischen Welt in den Cyberspace zu überführen. Im Moment bauen Prof. Hollick und seine Mitarbeiter an einem Prototyp für ein Experiment: über ein Smartphone wird erhoben, wie häufig die Testpersonen elektronisch miteinander kommunizieren und wie oft sie in der Nähe der anderen Testpersonen sind. Über diese Messungen kann dann die Intensität von Beziehungen durch die Erkennung von Mustern bestimmt werden. Vertrauen kann aber auch über vorgegebene, externe Grundannahmen etabliert werden, zum Beispiel bei Arbeitskollegen über die Zugehörigkeit zur gleichen Organisation.
Die Vertrauensbewertung soll aber nicht komplett automatisiert werden, sondern der Nutzer beim Verwalten und Klassifizieren seiner Vertrauensbeziehungen unterstützt werden. Hat man sich mit einem engen Freund zerstritten, sollte die Vertrauensbeziehung zu ihm auch im Cyberspace zunächst zurückgestuft werden, nennt Hollick ein Beispiel. Der Vorteil für die Nutzer: Sie können das Vertrauen aus der physischen Welt in die digitale überführen. Dafür müssen allerdings viele Daten gesammelt und ausgewertet werden – und das muss natürlich privatheitsschützend geschehen. Dabei hilft ein weiteres CROSSING-Forschungsprojekt, „Private Set Intersection“ (Projekt E3), das sich mit dem sicheren Teilen von Datenschnittmengen beschäftigt. „Mit dieser Technik können Gemeinsamkeiten gefunden werden, ohne zu viel preiszugeben“, erklärt Hollick.

Neben dem Datenschutz muss auch die Administration des Vertrauensbewertungs-Systems als weiterer praktischer Aspekt bei der Umsetzung beachtet werden: Diese könne weder Staaten noch großen Technologiekonzernen anvertraut werden, denn letztendlich seien diese auf lange Sicht nicht vertrauenswürdig, sagt Hollick. Wenn eine kritische Masse von Nutzern erreicht sei, könne das System auch per „Crowdsourcing“ entstehen, stellt er eine Alternative vor.

Global Trust: Vertrauensketten im Internet

Max Mühlhäuser betreut den Teilbereich „Global Trust“, der den wissenschaftlich neuen Ansatz verfolgt, Vertrauensketten für Szenarien der vernetzten IT-Sicherheit zu bewerten. Ein OnlineSzenario mit vielen Komponenten, die Kettenglieder, wird dabei als Vertrauenskette modelliert. Durch die Verzahnung mit den Vertrauensbewertungen aus dem „Local Trust“ wird es möglich, das Vertrauen zwischen Menschen und gegenüber Organisationen zu berücksichtigen, die mit den Kettengliedern in Beziehung stehen. Aus der Vertrauenswürdigkeit der einzelnen Kettenglieder kann dann mit mathematisch fundierten Methoden auf das Gesamtvertrauen geschlossen werden. Dabei spielen auch so genannte Stereotypen eine Rolle, die man sich zunächst wie Vorurteile vorstellen kann. Stereotypen seien nicht grundsätzlich schlecht, auch menschliche Lebenserfahrung falle in diese Kategorie, erklärt Mühlhäuser. „Wenn jemand bestimmte Merkmale vorzeigen kann, bekommt er eine Art Vertrauensvorschuss, den wir Anfangsvertrauen nennen: wer in der Bank an einem Mitarbeiter-Arbeitsplatz sitzt, dem geben wir vertrauliche Kontoinformationen, als Autofahrer folgen wir den Anweisungen einer Person in Polizeiuniform.“ Reicht die Vertrauenskette lückenlos vom Dienstanbieter zum Nutzer, kann das Gesamtvertrauen als sehr hoch bewertet werden.

Eigentlich kennt man das Prinzip der Vertrauensbewertung im Internet seit Jahren, zum Beispiel von Produktbewertungen bei Onlinehändlern wie Amazon und eBay oder auf Hotelbuchungs-Portalen. Dort gibt es aber keine Vertrauensketten, wie Mühlhäusers Team sie erforscht. „Diese Verfahren sind auch recht ‚hemdsärmelig‘, weil weder fälschungssicher noch im mathematischen Sinn korrekt – beides mit erheblichen Nebenwirkungen für den Nutzer. Dafür sind sie in der Praxis akzeptiert.“, sagt Mühlhäuser. Die Forscher haben daher den Ehrgeiz, auch für ihre komplizierten und mathematisch fundierten Modelle zu beweisen, dass sie in der Praxis funktionieren.

„Ist man heute mit dem Smartphone unterwegs, erhält man oft lokale und kontextabhängige Dienstangebote, zum Beispiel Onlineshopping-Angebote oder Empfehlungen für Läden, und natürlich für ‚freie‘ WLAN-Netze“, nennt Max Mühlhäuser ein Beispiel aus dem Alltag. Können diese digitalen und physischen Dienste in Zukunft über durchgehende Vertrauensketten bewertet werden, dann kann sich der Nutzer im „Internet of Things and Services“ sicherer bewegen und Dienstleistungen ohne Furcht vor ungewollten juristischen oder finanziellen Konsequenzen in Anspruch nehmen.

CROSSING

Mehr als 65 Wissenschaftler aus den Forschungsbereichen Kryptographie, Quantenphysik, Systemsicherheit und Softwaretechnik an der TU Darmstadt in CROSSING zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Das Ziel von CROSSING ist es, Kryptographie-basierte Sicherheitslösungen zu entwickeln, um auch in der Zukunft sichere und vertrauenswürdige Rechenumgebungen zu schaffen. Neben hohen Ansprüchen an die Effizienz und Sicherheit der entwickelten Lösungen, spielt auch die Usability, also die Benutzbarkeit, eine große Rolle: Software-Entwickler, Administratoren und sogar Endanwender sollen in der Lage sein, die Lösungen zu verwenden, auch wenn sie keine Kryptographie-Experten sind.

CROSSING wird seit Oktober 2014 als Sonderforschungsbereich der Deutschen Forschungsgemeinschaft (DFG) mit 8 Millionen Euro gefördert. Das Programm ist auf bis zu zwölf Jahre ausgelegt.

Ann-Kathrin Braun
Wissenschaftskommunikation
akbraun@cysec.tu-darmstadt.de
06151 / 16-22662