idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Universität des Saarlandes
Thorsten Mohr

12/18/2014
http://idw-online.de/en/news618743

Research results, Scientific Publications
Economics / business administration, Information technology
transregional, national

Informatiker der Universität des Saarlandes verbessern die Internet-Währung Bitcoin

Gehandelt an speziellen Börsen, wird die virtuelle Währung Bitcoin nicht nur von diversen Online-Händlern, sondern auch von tausenden Geschäften weltweit akzeptiert. Die Anwender schätzen die Vorteile: Da keine zentrale Bank existiert, lassen sich Überweisungen schneller und mit geringeren Gebühren abwickeln. Zudem versprechen sich viele Bitcoin-Anwender mehr Anonymität beim Bezahlen. Doch diese Beliebtheit zieht auch immer öfter Diebstähle nach sich. Saarbrücker Informatiker haben nun ein Verfahren vorgestellt, das die Anonymität erhöht und sich ohne erhebliche Wartezeiten einsetzen lässt.

„In der wissenschaftlichen Gemeinde ist es bekannt, dass sich die Anonymität von Bitcoin aushebeln lässt“, erklärt Aniket Kate von der Universität des Saarlandes. Kate leitet dort am Exzellenzcluster „Multimodal Computing and Interaction“ die Gruppe „Kryptografische Systeme“. Unter dem Begriff „Bitcoin“ verstehen Experten wie er zwei Aspekte. Erstens, das Zahlungssystem im Internet: Es besteht aus Personen, die spezielle Computerprogramme, die sogenannten Bitcoin-Clients, verwenden. Zusammen bilden sie ein Netzwerk, in dem jede Transaktion aufgezeichnet und protokolliert wird. Auf diese Weise ist weder ein zentrales Bankinstitut noch eine Beschränkung auf Ländergrenzen notwendig. Zweitens, die Währung: In den vergangenen Jahren hat sie nicht nur an medialer Aufmerksamkeit, sondern auch an Wert gewonnen. Derzeit entspricht ein Bitcoin, abgekürzt BTC, rund 290 Euro. Die erhoffte Anonymität dieser virtuellen Währung hängt von den sogenannten Bitcoin-Adressen ab. „Sie sind Decknamen, unter denen die Anwender öffentlich einsehbar ihre Transaktionen durchführen und dokumentieren. Lassen sich diese Decknamen auf die realen Personen dahinter zurückführen, ist die Anonymität von Bitcoin gebrochen“, erläutert Aniket Kate. Der Informatiker hat nun zusammen mit seinen Doktoranden Tim Ruffing und Pedro Moreno-Sanchez ein Verfahren entwickelt, das die Anonymität schützt, Missbrauch verhindert und sich einfach in die aktuellen Bitcoin-Programme der Anwender einarbeiten lässt.

Bisher sind die Anwender auf sogenannte „Mixe“ angewiesen. In der Theorie sollen sie die Bitcoin-Überweisungen diverser Anwender wie eine Art digitaler Strohmann annehmen und sie an die jeweils angegebene Adresse weiterleiten, natürlich ohne den Auftraggeber zu verraten. Die Praxis ist jedoch nicht so edelmütig: Manchmal stehlen die Betreiber der Mixe das digitale Geld, und auch die Identität ihrer Auftraggeber ist bei ihnen nicht sicher. Denn die Mixe sind in der Lage, Auftraggeber und Empfänger miteinander in Verbindung zu bringen. Kate und seine Kollegen haben die Idee dieses Systems erweitert. Anwender müssen sich bei ihrem neuen Ansatz nicht mehr auf die Verschwiegenheit eines Mittelsmanns verlassen. Ähnlich wie bei dem Netzwerk „Tor“, das anonymes Surfen im Internet ermöglicht, bilden mehrere Bitcoin-Nutzer ad hoc eine Art verschworene Gemeinschaft. Um die Herkunft ihrer Überweisungen zu vertuschen, hält sich jeder von ihnen an eine vorab festgelegte Abfolge, dem von Kate und seinem Team entworfenen CoinShuffle-Protokoll. Jeder Teilnehmer entschlüsselt die ihm zugesandte Liste mit Empfänger-Adressen, fügt seine eigene ein und schickt die Liste verschlüsselt an den nächsten weiter. Dieser Vorgang wiederholt sich bei jedem Teilnehmer. Auf diese Weise mischen sie die Reihenfolge der Adressen ähnlich wie Spielkarten.

„Das Ergebnis ist eine Liste von Adressen, die keine Hinweise auf die Auftraggeber dahinter gibt. Um Missbrauch auszuschließen, überprüft jeder die nun veröffentlichte Liste“, sagt Aniket Kate. Das Besondere an diesem Ansatz: Ist etwas suspekt oder versuchen sogar einige Teilnehmer, die anderen zu betrügen, können die Übeltäter entlarvt werden. Um ihren Ansatz auch in der Praxis zu testen, haben die Saarbrücker Informatiker ihn in der Sprache Python programmiert. Auf diese Weise konnten sie nachweisen, dass der zusätzliche Zeitaufwand für das Mischen kein Problem darstellt. Bei 20 Teilnehmern bleibe er unter 60 Sekunden, sagen die Forscher. Dabei dauert eine Transaktion ohnehin bereits mehrere Minuten. „So weit wir wissen, ist CoinShuffle damit weltweit die erste sofort einsetzbare Lösung, die Anonymität bietet, ohne sich auf einen Mittelsmann verlassen zu müssen“, erklärt Tim Ruffing. Er hat die Kunde davon bereits in die Bitcoin-Gemeinde getragen. „Momentan programmieren mehrere Entwickler unseren Ansatz nach, um diesen in ihre Bitcoin-Clients zu integrieren“, so Ruffing.

Quelle: CoinShuffle: Practical Decrentralized Coin Mixing for Bitcoin; Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate; 19th European Symposium on Research in Computer Security (ESORICS 14)

Fragen beantworten:

Tim Ruffing
Cryptographic Systems Research Group
Cluster of Excellence „Multimodal Computing and Interaction“
Tel.: 0681 302 70786
E-Mail: tim.ruffing@mmci.uni-saarland.de

Pedro Moreno-Sanchez
Cryptographic Systems Research Group
Cluster of Excellence „Multimodal Computing and Interaction“
Tel.: 0681 302 70758
E-Mail: pedro@mmci.uni-saarland.de

Aniket Kate
Head of Cryptographic Systems Research Group
Cluster of Excellence „Multimodal Computing and Interaction“
E-Mail: aniket@mmci.uni-saarland.de

Redaktion:
Gordon Bolduan
Wissenschaftskommunikation
Kompetenzzentrum Informatik Saarland
Tel: 0681 302-70741
E-Mail: bolduan@mmci.uni-saarland.de

URL for press release: http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/

Aniket Kate und seine Kollegen stellen sicher, dass das Bezahlen mit der virtuellen Währung Bitcoin anonym bleibt.
Foto: Manuela Meyer