Virtuelles Geld: Benutzeridentität lässt sich viel leichter ermitteln als bisher angenommen

Virtuelles Geld: Benutzeridentität lässt sich viel leichter ermitteln als bisher angenommen
"Die Zukunft lässt sich schwer vorhersagen, doch manche meinen, Bitcoin könnte den Geldverkehr so verändern, wie das Internet die Kommunikation", so Prof. Alex Biryukov, Leiter der Forschungseinheit, die sich an der Universität Luxemburg mit digitaler Währung befasst. "Daher glaube ich, dass es speziell für Luxemburg wichtig ist, die Entwicklung von Bitcoin im Auge zu behalten."
Das Bitcoin-System wird nicht von einer zentralen Instanz verwaltet, sondern von einem Peer-to-Peer-Netzwerk im Internet getragen. Jeder kann sich dem Netzwerk als Benutzer anschließen oder Rechnerkapazitäten zur Abwicklung der Transaktionen zur Verfügung stellen. Im Netzwerk ist die Identität des Benutzers hinter einem verschlüsselten Pseudonym verborgen, das nach Belieben geändert werden kann. Transaktionen werden mit diesem Pseudonym signiert und dem öffentlichen Netzwerk mitgeteilt, wo ihre Authentizität verifiziert wird und die Bitcoins dem neuen Besitzer gutgeschrieben werden.
In ihrer neuen Studie haben Forscher an dem Laboratory of Algorithmics, Cryptology and Security der Universität Luxemburg gezeigt, dass Bitcoin die IP-Adresse des Benutzers nicht schützt und dass sie sich in Echtzeit den Transaktionen des Benutzers zuordnen lässt. Um diese zu ermitteln, würde ein Hacker nur ein paar Computer und etwa ?1500 im Monat für Server- und Traffic-Kosten benötigen. Außerdem kann das beliebte Anonymisierungsnetzwerk "Tor" wenig tun, um die Anonymität des Bitcoin-Verkehrs zu gewährleisten, da es sich mühelos blockieren lässt.
Dieser Befund bezieht sich auf die Grundidee, dass die Eingangsknoten von Bitcoin, in die sich der Computer des Benutzers einwählt, um die Transaktion durchzuführen, während der Sitzung des Benutzers einen unverwechselbaren Identifikator bilden. Dieses unverwechselbare Muster lässt sich der IP-Adresse eines Benutzers zuordnen. Zudem können Transaktionen, die während einer Sitzung getätigt wurden, selbst jene, die über nicht verwandte Pseudonyme erfolgen, einander zugeordnet werden. Mit dieser Methode können Hacker bis zu 60 Prozent der IP-Adressen ermitteln, die sich hinter den über das Bitcoin-Netzwerk getätigten Transaktionen verbergen.
"Im Verbund mit früherer Forschung über Transaktionsströme zeigt diese Analyse, dass das Anonymitätsniveau im Bitcoin-Netzwerk recht niedrig ist", erklärt Prof. Alex Biryukov. In dem Beitrag, der kürzlich anlässlich der ACM Conference on Computer and Communications Security vorgelegt wurde, beschreibt das Team auch, wie sich ein solcher Angriff auf die Privatsphäre des Benutzers verhindern lässt. Software-Patches, die von den Forschern geschrieben wurden, werden derzeit mit den Bitcoin-Hauptentwicklern diskutiert.
Die im Jahr 2003 gegründete Universität Luxemburg ist eine mehrsprachige, internationale Forschungsuniversität mit 6200 Studierenden und Mitarbeitern aus der ganzen Welt. Forschungschwerpunkte sind Informatik, Recht und Europarecht, Finanzwissenschaften, Erziehungswissenschaften sowie fachübergreifende Forschung durch das "Interdisciplinary Centre for Security, Reliability and Trust" (SnT) in Informations- und Kommunikationstechnologie und das "Luxembourg Centre for Systems Biomedicine" (LCSB) in System-Biomedizin.
Hinweis an die Redaktion
Der vollständige wissenschaftliche Artikel "Deanonymisation of clients in Bitcoin P2P network", wie in "Proceedings of the ACM Conference on Computer and Communications Security" veröffentlicht, kann hier: http://orbilu.uni.lu/handle/10993/18679 eingesehen werden. DOI: 10.1145/2660267.2660379

Universität Luxemburg - Université du Luxembourg
162a, Avenue de la Faïencerie
L-1511 Luxembourg
Telefon: + 352 46 66 44 6563
Telefax: + 352 46 66 44 6561
Mail: communication@uni.lu
URL: http://wwwde.uni.lu
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=582236" width="1" height="1">

Pressekontakt

Universität Luxemburg - Université du Luxembourg

L-1511 Luxembourg

wwwde.uni.lu
communication@uni.lu

Firmenkontakt

Universität Luxemburg - Université du Luxembourg

L-1511 Luxembourg

wwwde.uni.lu
communication@uni.lu

Weitere Informationen finden sich auf unserer Homepage