Virtual money and user's identity

25 November 2014

Bitcoin is the new money: minted and exchanged on the Internet. Faster and cheaper than a bank, the service is attracting attention from all over the world. But a big question remains: are the transactions really anonymous?

Several research groups worldwide have shown that it is possible to find out which transactions belong together, even if the client uses different pseudonyms. However it was not clear if it is also possible to reveal the IP address behind each transaction. This has changed: researchers at the University of Luxembourg have now demonstrated how this is feasible with only a few computers and about €1500.

"It's hard to predict the future, but some people think that Bitcoin could do to finance what the Internet did to communications", says Prof. Alex Biryukov, who leads digital currency research at the University. "So I think especially for Luxembourg it is important to watch what happens with Bitcoin".

The Bitcoin system is not managed by a central authority, but relies on a peer-to-peer network on the Internet. Anyone can join the network as a user or provide computing capacity to process the transactions. In the network, the user's identity is hidden behind a cryptographic pseudonym, which can be changed as often as is wanted. Transactions are signed with this pseudonym and broadcast to the public network to verify their authenticity and attribute the Bitcoins to the new owner.

In their new study, researchers at the Laboratory of Algorithmics, Cryptology and Security of the University of Luxembourg have shown that Bitcoin does not protect user's IP address and that it can be linked to the user's transactions in real-time. To find this out, a hacker would need only a few computers and about €1500 per month for server and traffic costs. Moreover, the popular anonymization network "Tor" can do little to guarantee Bitcoin user's anonymity, since it can be blocked easily.

The basic idea behind these findings is that Bitcoin entry nodes, to which the user's computer connects in order to make a transaction, form a unique identifier for the duration of user's session. This unique pattern can be linked to a user's IP address. Moreover, transactions made during one session, even those made via unrelated pseudonyms, can be linked together. With this method, hackers can reveal up to 60 percent of the IP addresses behind the transactions made over the Bitcoin network.

"This Bitcoin network analysis combined with previous research on transaction flows shows that the level of anonymity in the Bitcoin network is quite low", explains Dr. Alex Biryukov. In the paper recently presented at the ACM Conference on Computer and Communications Security the team also described how to prevent such an attack on user's privacy. Software patches written by the researchers are currently under discussion with the Bitcoin core developers.

More information: Deanonymisation of clients in Bitcoin P2P network.
orbilu.uni.lu/handle/10993/18679

Provided by University of Luxembourg