Computer scientists improve the privacy of the Internet currency Bitcoin

January 22 2015

It is traded on special stock exchanges and is accepted not only by various online shops, but also by thousands of brick-and-mortar stores across the globe: the virtual currency Bitcoin. The users benefit from its advantages: Since it does not require a central bank, the transactions can be concluded more quickly and with reduced charges. Moreover, many Bitcoin users appreciate more anonymity while paying. Nevertheless, its popularity is also resulting in thefts with increasing frequency. Computer scientists in Saarbrücken have now presented an approach that enhances anonymity and can be applied without long waits.

"Within the research community, it is well-known that the anonymity of Bitcoin can be broken", explains Aniket Kate of Saarland University, who leads the independent research group "Cryptographic Systems" at the Cluster of Excellence "Multimodal Computing and Interaction". Experts like him associate two ideas with the term "Bitcoin": Firstly, there is the online payment system. It consists of people using special computer programs, so-called Bitcoin clients. As a whole, they form a network in which every transaction is registered and recorded. In this manner, neither a central banking institution nor restrictions due to national borders are necessary. Secondly, there is the currency. In the last few years, Bitcoin not only attracted media attention, but also increased unprecedentedly in value. At present, one Bitcoin, abbreviated as BTC, is worth over 200 US-dollars. The anticipated anonymity of this virtual currency relies on the so-called Bitcoin addresses. "They are pseudonyms through which users perform and publicly record transactions. If those pseudonyms can be tracked back to the real

initiators, the anonymity of Bitcoin is broken", explains Aniket Kate. In collaboration with his PhD students Tim Ruffing and Pedro Moreno-Sanchez, the computer scientist has now developed a method that protects the user's anonymity, prevents fraud and can be easily incorporated into current Bitcoin programs.

So far, users are dependent on so-called "mixing services". In theory, they should accept the Bitcoin transfers of various users as a sort of digital mediator and forward them to each of the provided addresses, but of course without revealing the client. In practice, the process is not as honorable: Sometimes the providers of mixing services steal the digital money, plus the identities of their clients are also not safe, because mixing services are able to relate the clients to the addressees.

Kate and his colleagues have now advanced the idea behind this system. With their novel approach, the users are no longer dependent on the secrecy provided by their intermediaries. Similar to the network "Tor", which allows anonymous access of the Internet, several Bitcoin users form a sort of sworn community in advance. To hide the source of their transactions, each one of them conforms to a certain pre-determined succession of actions – the so-called CoinShuffle protocol, which was developed by Kate and his team. Every participant decodes the list of recipient addresses he has received, adds his own to it and forwards the encrypted list to the next participant. This process is repeated with every participant. In this way they shuffle the order of the addresses and hence the traces to the recipient, similar to shuffling a deck of cards.

"The result is a list of addresses, which does not contain any indication of the initial client. To prevent abuse, everyone subsequently checks the released list", says Aniket Kate. What is special about this approach is that if something appears to be suspicious or some participants try to defraud the others, the offenders can be easily exposed. To test their approach in practice, the Saarbrücken computer scientists implemented

it in the programming language Python. In this way, they could prove that the additional time costs for mixing do not create any problems. The researchers explain that with twenty participants, their method completes in less than 20 seconds. At the same time, one transaction with Bitcoin takes several minutes in any case. "To the best of our knowledge, CoinShuffle is the first solution worldwide that is immediately usable and provides anonymity without an intermediary", explains Tim Ruffing. He has already spread the word within the Bitcoin community. "Currently, several developers are reprogramming our approach to incorporate it into their Bitcoin clients", says Ruffing.

More information: "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin." Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate, 19th European Symposium on Research in Computer Security (ESORICS 14)

Provided by Saarland University