Why hackers have to work hard

Description

A 4 digit mechanical combination lock is designed so that a person trying to break into your locker (a padlock *hacker*) would have to try on average 5,000 combinations ($10^4/2$). Thatâ??s about 2-5 hours work, which is a big investment in time, and before the hacker exhausts all iterations he or she may well be caught in the act.

Computers perform millions of meaningful mathematical operations a second. But some sequences of operations still take a long time, measured in minutes, hours, days or even years. A computer trying to guess an 8 character password or sequence of passwords by brute force could take several hours. (In any case the security software would detect that someone is trying lots of combinations and shut them out.)

One of the ways to foil hackers is to ensure that the effort in working through combinations to break into a system is just not worth it. CPU processing costs time and resources. You need the hardware, network connectivity, power, and time to do the hack before being detected, and hackers may need to work on many accounts or passwords at once.

A common hacking target is to break into a digital ledger of transactions and place fake transactions that funnel money to the hackerâ??s own account. If a legal account holder tries to adjust transactions in their own account thatâ??s also hacking. Banks and other custodians of financial ledgers have increasingly sophisticated systems to prevent such doctoring of transactions.

Shared ledgers

In the case of cryptocurrencies (e.g. bitcoin) thereâ??s no centralised data management. The entire ledger gets distributed to everyone in the network, with names and other details encrypted so that you can only really read details of your own transactions.

The problem with a shared ledger is that anyone (a hacker, attacker or even a regular customer) could plant bogus transactions. The method for avoiding this is to make it hard to hack, i.e. the hacker would have to expend so much CPU resource that itâ??s either impossible or just not worth the effort.

One of the means of making it difficult to make changes to a database (e.g. a ledger) is to set up an arbitrary computational puzzle for anyone involved in adding legitimate transactions to the ledger. A hacker would have to expend even more CPU effort than legitimate users to make alterations. The challenge that draws on CPU time and energy gets coded into the ledger. As the ledger grows it gets densely packed with difficulty â?? the further back in time you go. Older transactions are â??immutable,â?• i.e. virtually impossible to change. See previous posts: Immutable data and Wasting time in the bit economy.

Iâ??ll attempt to explain the anti-hack puzzle in the next post.

Reference

- Nakamoto, S. (2008), â??Bitcoin: A Peer-to-Peer Electronic Cash Systemâ??. *Bitcoin*. Available online: https://bitcoin.org/bitcoin.pdf (accessed 19 June 2017).

Note

- For an interesting explanation and application of cryptocurrency technology see: Maxwell, Deborah, Chris Speed, and Larissa Pschetz. 2017. Story Blocks: Reimagining narrative through the blockchain. *Convergence: The International Journal of Research into New Media Technologies*, (23) 1, 79-97.

Category

1. Economics

Tags

1. bitcoin
2. blockchain
3. ciphercity
4. cryptocurrency
5. hacking
6. hash
7. security

Date Created
August 5, 2017
Author

rcoyne99