Blockchain-Angriffe

TIS-Workshop 2024

Adrian Schollmeyer

02.02.2024

Gliederung

Time Jacking [3, 2]

- Gezieltes Aushebeln des Konsens über die Uhrzeit im Bitcoin-Netzwerk
- Provokation eines Forks durch Zeitmanipulation
- Opfer zwingen, einen Block zu akzeptieren, der vom restlichen Netzwerk nicht akzeptiert wird
- Endziel: Double Spending

Time Jacking – Ablauf

Phase 1 Fork & Isolate

- Verbindung des Opfers mit vielen Angreiferknoten, die dem Opfer eine falsche Uhrzeit (Uhr geht „nach“) übermitteln
- Opfer lehnt gültige Blöcke ab, die nach seiner Sicht „zu weit“ in der Zukunft liegen
- Isolation des Opfers vom Blockchain-Netzwerk
- Angreifer erzeugt Blöcke für das Opfer mit modifizierter Uhrzeit („Angreifer-Netzwerk“)

Phase 2 Double-Spending

- Angreifer erzeugt Transaktion, die Geld an das Opfer überweist, an das Angreifer-Netzwerk
- Opfer glaubt, Geld erhalten zu haben, und überträgt reale Güter an Angreifer
- Aber: in der global akzeptierten Blockchain hat das Opfer nie Geld erhalten!

Time Jacking – Abwehr

- Nutzung der eigenen Systemzeit statt der Netzwerk-Zeit für die Prüfung von Zeitstempeln
- Toleranzen für akzeptable Zeitabweichungen verkleinern
- Verbindung nur mit „vertrauenswürdigen“ Peers

51 %-Angriff [3, 1]

- Erlangung von $> 50\,\%$ der gesamten Netzwerk-Rechenleistung durch Angreifer
- Volle Kontrolle über die Transaktionen durch den Angreifer
- Endziele: Transaktionen verhindern, Double-Spending

51 %-Angriff – Ablauf

- Angreifer erlangt Rechenleistung, die die gesamte Rechenleistung aller anderen Miner übersteigt
- Angreifer erzeugt eigene Kette, die länger ist als die Kettes des Netzwerks, dabei:
  - Transaktionen, die der Angreifer nicht im Netzwerk haben möchte, werden nicht in die Angreifer-Blöcke aufgenommen
  - Transaktionen vom Angreifer an sich selbst werden in die Angreifer-Blöcke aufgenommen, um sich Mittels Double-Spending Güter u. Ä. zu erschleichen.
- Veröffentlichung der Angreifer-Kette im Netzwerk, um bereits durchgeführte Transaktionen wieder rückgängig machen zu können (die bisher gültige Kette im Netzwerk, in der zu verhindernde Transaktionen enthalten sind, wird vom Netzwerk verworfen und durch die Angreifer-Kette ersetzt)

51 %-Angriff – Abwehr

- Einsatz sehr großer Rechenleistung im Netzwerk, um es Angreifern sehr schwer/teuer zu machen, die nötige Rechenleistung zu erlangen
- Diversifiziertes Netzwerk aus Minern nötig, die nicht in großen Pools zusammenarbeiten, da sonst die Autoritäten im Netzwerk potentiell einen solchen Angriff durchführen könnten.

Spam-Transaktionen [4, 5]

- Flutung des Netzwerks mit „Spam“-Transaktionen
- DoS-Angriff
- Schwer erkennbar
- Hardwareaufwand für Angreifer gering

Spam-Transaktionen – Ablauf

- Angreifer sendet viele Transaktionen (mit wenig oder gar keinen Transaktionsgebühren) ins Netzwerk
- Mempools der Nodes wachsen stark an
- Wachstumsrate der Blockchain wächst stark an
- Warteschlangen unverarbeiteter Transaktionen laufen voll

Spam-Transaktionen – Abwehr

- Unterscheidung zwischen legitimen und Spam-Transaktionen nur schwer umsetzbar
- Spam-Transaktionen auch legitim, daher Verarbeitung durch das Netzwerk korrektes Verhalten
- Priorisierung von Transaktionen nach Transaktionsgebühr hilfreich
- Einführung/Erhöhung einer minimalen Transaktionsgebühr, um die Kosten pro Spam-Transaktion zu erhöhen

Quellen

[1] Boris Koldehofe und Kai-Uwe Sattler. "Transaktionale Informationssysteme". 17. Jan. 2023.

[2] *Time Jacking in Mining Pools - ImmuneBytes*. 29. Aug. 2023. URL: https://www.immunebytes.com/blog/time-jacking-in-mining-pools/.

[3] *Top blockchain attacks, hacks and security issues explained | TechTarget*. Security. URL: https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues.

[4] *Web 3.0 challenges and solutions: Transaction spamming in blockchain | NKN*. 12. Mai 2022. URL: https://nkn.org/community/blog/web-3-0-challenges-and-solutions-transaction-spamming-in-blockchain/.

[5] Jin Yang u. a. "Spam transaction attack detection model based on GRU and WGAN-div". In: *Computer Communications* 161 (1. Sep. 2020), S. 172–182. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2020.07.031. URL: https://www.sciencedirect.com/science/article/pii/S0140366420318430.