netidee

STIPENDIEN

Automated Verification of Game-Theoretic Security Properties for Decentralized Protocols

Zwischenbericht | Call 17 | Stipendium ID 6321

Inhalt

1 Einleitung

In meinem Dissertationsprojekt Automated Verification of Game-Theoretic Security Properties for Decentralized Protocols habe ich es mir zum Ziel gesetzt ein automatisiertes Framework zu entwickeln, das es ermöglicht Blockchain Protokolle auf deren spieltheoretische Sicherheit zu untersuchen. Dadruch wird sichergestellt, dass sich niemand zu unrecht bereichern kann und dass ehrlichen Nutzern kein Schaden entstehen kann.

Im vorliegenden Zwischenbericht erläutere ich die Fortschritte von November 2022 bis Juni 2023. Weiters gehe ich darauf ein inwiefern ich vom ursprünglichen Planungsdokument abgewichen bin und warum. Außerdem gebe ich einen Überblick über den verbleibenden Förderungszeitraums.

2 Status

2.1 Meilenstein 1 – Publikation zum Prototyp

Der Prototyp beinhaltet insbesondere die Definition von spieltheoretischer Sicherheit und verwendet den SMT Solver Z3 wie geplant, um Sicherheitsanalysen von Blockchain Protokollen zu erhalten. Der Prototyp, namens CheckMate, bekommt ein Spiel als Input und gibt die Ergebnisse der Sicherheitsanalyse zurück. Das heißt, der wichtige und komplexe Arbeitsschritt der Modellierung eines Protokolls als Spiel ist noch nicht automatisiert.

Die Haupttätigkeiten dieses Meilensteins waren einerseits die Definition von Sicherheit als logische Formeln, deren Implementierung in Python und die mathematischen Beweise der Korrektheit unseres Konzepts und andererseits das Verfassen eines wissenschaftlichen Papers. Der Prototyp liefert vielversprechende Ergebnisse und wir werden die gewählte Vorgangsweise weiter verfolgen.
Die Ergebnisse des Meilensteins sind sowohl der Prototyp selbst, auf github verfügbar (im Planungsdokument verlinkt), sowie das Paper. Leider wurden wir bei der Konferenz abgelehnt, mit dem Argument, dass gewisse Nuancen bei CheckMate noch fehlen. Auf die dahingehende Erweiterung von CheckMate gehe ich in Meilenstein 3 noch weiter ein.
Durch die Ablehnung des Papers und die Anforderung der Ergänzungen hat sich der Zeitplan so geändert, dass vor der Erstellung des Zwischenberichts nochmal eine Automatisierungsphase eingeschoben wurde.

2.2 Meilenstein 2 – Spieltheoretische Modellierung

Wie in Meilenstein 1 erwähnt, kann CheckMate momentan keine Protokolle als Spiele modellieren. Daher ist die spieltheoretische Modellierung ein essenzieller Teil meines Projekts. Erstens werden die Spiele als Benchmarks für CheckMate gebraucht und zweitens erhält man duch das manuelle Modellieren wichtige Einsichten in gewisse Muster und sich wiederholende Ansätze, die eine Automatisierung in der Zukunft erleichtern.
Die Haupttätigkeiten waren das detaillierte Verständnis der modellierten Protokolle, manuelles Modellieren der groben Züge und schließlich das Schreiben eines Codes zur Erstellung aller Abweichungen im Modell.
Die wichtigste Erkenntnis war, dass es mit hoher Expertise möglich ist ein Spiel generieren zu lassen. Eine gute Beschreibung des Zustandes aller Spieler im Modell ist dafür entscheident.
Wir haben zwei Blockchain Protokolle erfolgreich modelliert, eines davon wurde wie gesagt zum Teil durch Code generiert. Die Dateien und der Code, der für die Generierung verwendet wurde, sind ebenfalls auf github zu finden.
Es gab keine besonderen Erfolge oder Probleme. Aufgrund der Planadaptierung von Meilenstein 1 und des Interesse eines Partners aus der Wirtschaft, wird es von Oktober bis November nochmals eine Modellierungsphase geben.

2.3 Meilenstein 3 – Erweiterung der Automatisierung

Wie schon in Meilenstein 1 erklärt, wurde die Einfügung eines zweiten Automatisierungsmeilensteins notwendig. Die Reviewer bemängelten zu Recht, dass gewisse Aspekte des Tools noch unvollständig vorhanden waren. In Meilenstein 3 wurden diese Mängel behoben.
Die Haupttätigkeiten waren die Verfeinerung der logischen Formeln einer Sicherheitseigenschaft, die Erstellung von Gegenbeispielen (=Attack Vectors) für nicht sichere Protokolle und die mathematischen Beweise dessen Korrektheit. Wir haben CheckMate mit dieser Erweiterung wieder bei einer Fachkonferenz eingereicht. Die ersten Reviews waren gut, ein engülltiges Ergebnis steht erst Mitte Juli fest. Dann wird das Paper ebenfalls Open Source auf arxiv veröffentlicht.
Die Adaptierungen erweitern nicht nur die Features von CheckMate, sie haben auch zu einem Speed Up des Tools geführt.

3 Zusammenfassung Planaktualisierung

Zusammenfassend wurde das Planungsdokument wie folgt aktualisiert. Der Meilenstein 3 Erweiterung der Automatisierung wurde wegen Ablehnung des Papers zum Prototypen CheckMate eingefügt. Dadurch verkürzte sich der Zeitrahmen für die spieltheoretische Modellierung (Meilenstein 2).

Dies, sowie das Interesse eines industrial Partners an einer spieltheoretischen Modellierung ihres Protokolls, machte es notwendig einen zweiten Modellierungsmeilenstein (Meilenstein 6) hinzuzufügen.

Darüberhinaus hat sich ein vielversprechender Ansatz ergeben: Ein Spiel in mehrere Teilspiele zu zerlegen und die Sicherheitsanalyse auf den Teilspielen durchzuführen, um das Resultat auf das gesamte Spiel zu propagieren. Ich habe daher noch einen weiteren Meilenstein im Planungsdokument ergänzt (Meilenstein 5 Compositionality).

Die oben genannten Änderungen führen dazu, dass für den vorletzen Meilenstein zur Synthetisierung von Modellen weniger Zeit bleibt. Ich bin allerdings davon überzeugt, dass die eingefügten Meilensteine 5 und 6 einen wesentlichen Beitrag zur Synthetisierung von Modellen führen, da sie wichtige Einsicht in den Modellierungs- und Analysevorgang gewähren.