Masterthesis im Bereich Secure Software Engineering

Wir suchen engagierte Studierende, die Interesse an der Erforschung von Sicherheitslücken haben und dabei die modernsten Technologien nutzen möchten. Diese Masterarbeit bewegt sich an der Schnittstelle zwischen KI und Softwaresicherheit.

Klassische Schwachstellenscanner sind sehr gut darin, mögliche Sicherheitslücken in Binärcode zu identifizieren. Dabei können jedoch sowohl falsch-positive als auch irrelevante Ergebnisse auftreten. Letztere sind zwar prinzipiell korrekt, lassen sich jedoch nicht für einen echten Angriff ausnutzen, z.B. weil die entsprechende Schwachstelle Vorbedingungen erfordert, die nie eintreten können. Die große Anzahl an Scanner-Ergebnissen manuell zu prüfen, skaliert insbesondere in großer und komplizierter Software schlecht.

Um dieses Problem zu lösen, möchten wir in dieser Arbeit KI nutzen, um Schwachstellen zu verifizieren. Dabei greifen wir auf die detaillierten Daten eines hochwertigen statischen Scanners zurück und nutzen die Fähigkeit großer generativer KI-Modelle, neue Antworten einschließlich (Exploit-)Code zu generieren. Gelingt es, die Schwachstelle auszunutzen, gilt sie als verifiziert und muss vom Entwickler priorisiert behoben werden. Kann sie nicht verifiziert werden, wollen wir mittels interaktiver Prompting-Techniken versuchen, das LLM mit weiteren Informationen zu versorgen, um entweder doch noch einen Exploit zu erhalten oder eine hinreichende Konfidenz in die Nichtausnutzbarkeit der Schwachstelle zu erlangen.
Als KI-Modelle sollen neben GPT-4 auch diverse Open Source-Modelle genutzt werden. Wir stellen dabei die Ressourcen für Experimente mit großen OSS-LLMs bereit. Als Schwachstellenscanner steht unser hauseigener Scanner VUSC zur Verfügung.

Was Du bei uns tust

- Entwicklung einer Methode zur Verifikation von Sicherheitslücken mittels KI auf Basis von Ergebnissen des Schwachstellenscanners
- Durchführung von Experimenten und Evaluierung der Ergebnisse

Was Du mitbringst

- Studierende im Bereich Informatik, IT-Sicherheit oder einem ähnlichen Fachgebiet
- Kenntnisse in der Softwaresicherheit, Kenntnis klassischer Schwachstellen (SQL Injection, XSS, Crypto API Misuse, etc.)
- Erfahrung im Umgang mit KI-Modellen (insbesondere GPT) und KI-Frameworks (insbesondere DeepSpeed) sind von Vorteil
- Erfahrung mit statischer Codeanalyse ist von Vorteil

Was Du erwarten kannst

- Selbstständige Arbeitszeiteinteilung
- Einblicke in das Schnittfeld von akademischer Forschung und industrieller Anwendung

Wir wertschätzen und fördern die Vielfalt der Kompetenzen unserer Mitarbeitenden und begrüßen daher alle Bewerbungen – unabhängig von Alter, Geschlecht, Nationalität, ethnischer und sozialer Herkunft, Religion, Weltanschauung, Behinderung sowie sexueller Orientierung und Identität. Schwerbehinderte Menschen werden bei gleicher Eignung bevorzugt eingestellt.
Haben wir Dein Interesse geweckt? Dann bewirb Dich jetzt online mit Deinen aussagekräftigen Bewerbungsunterlagen. Wir freuen uns darauf, Dich kennenzulernen!

Kennziffer: 72741