KI und Sicherheit

Einladung zur Herbsttagung

Mittwoch, 4. September 2024, 13:00 bis 17:00 Uhr

Gleisarena FFHS, Zollstrasse 17, Zürich

Die Teilnahme ist kostenlos
Anmeldung bis Freitag, 16. August 2024
www.cnlab.ch/herbsttagung

cnlab

Information. Technology. Research_

WORUM GEHT'S?

KI und Sicherheit

Wir betrachten Künstliche Intelligenz und Machine Learning durch die Sicherheitsbrille: Wie funktioniert das? Was geht? Was geht nicht?

4. SEPTEMBER

13:00–17:00

ab 13:00

Eintreffen der Gäste

13:30

Grundlagen

Wie funktioniert KI?

- KI und Machine Learning
- Regression
- Classification
- Neural Networks
- Clustering

Martin Kaufmann

14:00

Anwendungen

Wozu wird KI eingesetzt?

- Data Mining
- Erkennung (Bilder, Objekte)
- Klassifizierung (Threats, Fraud)
- Generierung (Text, Bilder, Musik, Software)
- Gesetzliche Schranken

Stephan Verbücheln

14:30

Software-Entwicklung mit KI

Ein Praxis-Beispiel

- Methoden
- Anwendungsbereiche
- Hits und Flops
- Software-Qualität
- Urheberrecht
- Vertraulichkeit

Daniel Zimmermann

cnlab
Information. Technology. Research_

Gleisarena FFHS, Zollstrasse 17, Zürich

cnlab.ch/herbsttagung

15:00

Kaffee-Pause

15:20

KI und Sicherheit Teil 1

Angriffe gegen KI

- Poisoning
- Evasion
- Adversarial Examples
- Privacy
- Abuse

Zuzana Trubini

15:50

KI und Sicherheit Teil 2

Angriffe mit KI

- Gamechanger
- … oder nur Enabler?
- Angriffstechniken
- Kann KI AES brechen?

Urs Wagner

16:20

Fazit

Was heisst das jetzt?

Thomas Lüthi

16:30

Demos und Apéro

- KI selber betreiben
- öffentliche KI-Dienste
- Prompting

cnlab

REFERENTEN

Stephan Verbücheln
cnlab security AG. Diplom-Informatiker. Aktuelle Schwerpunkte: Technische Sicherheitsexpertisen in Kryptographie und Security-Reviews von IT-Infrastrukturen und Applikationen.

Zuzana Trubini
cnlab security AG. Dipl. Math ETH. Promotion ETH in theoretischer Informatik (Dr. Sc.). Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten Konzepten, sicheres Onboarding, sichere Aktivierung und Authentisierung.

Urs Wagner
cnlab security AG. M. Sc. Math UZH. Promotion UZH (Dr. Sc. Nat.) im Bereich Kryptologie. Mehrjährige Erfahrung in der Beurteilung von kryptologischen Schutzfunktionen. Aktuelle Schwerpunkte: Analyse von sicherheitsrelevanten IT-Konzepten in der Finanzindustrie.

Stefan Kunz
cnlab security AG. M. Sc. in Informatik. Aktuelle Schwerpunkte: Technische Sicherheits-Expertisen und Security-Reviews von IT-Infrastrukturen und verteilten Anwendungen mit Fokus auf die Bereiche Web, Mobile und Kubernetes.

Martin Kaufmann
cnlab security AG. M. Sc. in Robotics, System & Control, ETH Zürich. Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten IT-Konzepten, sichere Authentisierung und Autorisierung.

Thomas Lüthi
cnlab security AG. Dipl. El. Ing. HTL. Technische Expertisen und Security-Reviews von Netzwerken und verteilten Applikationen, Cloud-Integrationen, Netzwerk-Design, Design und Konfigurationen von Firewall-Systemen und Umsetzung von Sicherheitsmassnahmen in verteilten Systemen.

Daniel Zimmermann
cnlab software AG. Diplom-Informatiker. Full Stack Software Engineer mit mehrjähriger Erfahrung. Aktuelle Schwerpunkte: Web-Backend, Desktop- und Mobile-Frontend.

Raphael Juchli
cnlab software AG. Diplom-Informatiker HSR (B. Sc.). Software Engineer, mehrjährige Erfahrung in der Entwicklung von Backend- & Desktop-Anwendungen. Erfahrung mit allen modernen Programmiersprachen und Technologien.

Pasqualino Casciano
cnlab security AG. B. Sc. Informatik, CISSP. Über 20 Jahre Erfahrung in der Software-Entwicklung und in der IT-Architektur (vorwiegend im Finanzsektor). Aktuelle Schwerpunkte: Analyse und Design von sicherheitsrelevanten IT-Konzepten.

Julian Koch
cnlab security AG. B. Sc. in Computer Science. Langjährige Erfahrung in der Software-Entwicklung. Aktuelle Schwerpunkte: Security-Reviews von Infrastruktur und Applikationen.

Simran Tinani
cnlab security AG. M. Sc. Math UZH. Promotion UZH (Dr. Sc. Nat.). Aktuelle Schwerpunkte: Sicherheitsexpertisen in der Kryptographie. Analyse von sicherheitsrelevanten IT-Konzepten in der Finanzindustrie.