Xinlei He | CV

xinlei.he@cispa.de • www.xinlei.info

last update: December 16, 2021

Education

CISPA Helmholtz Center for Information Security — **Saarbrücken, Germany**
Ph.D. in Computer Science — *February 2020 –*
Advisor: Dr. Yang Zhang

Fudan University — **Shanghai, China**
Master in Computer Science — *September 2017 – January 2020*
Advisor: Prof. Yang Chen

Fudan University — **Shanghai, China**
Bachelor in Computer Science — *September 2013 – June 2017*
Advisor: Prof. Yang Chen

Research Interests

Trustworthy Machine Learning

Service

- PC member
  - 2021: ESORICS (Poster Session)
  - 2020: SocInfo
- External reviewer
  - 2021: USENIX Security, CCS, NDSS, Euro S&P, ICLR, WWW, ICWSM, CHI, AAAI, AISACCS, PETS
  - 2020: Usenix Security, CCS, CSCW, ESORICS, PETS

Publication

Conference

[1] Yun Shen*, **Xinlei He***, Yufei Han, and Yang Zhang. Model Stealing Attacks Against Inductive Graph Neural Networks. In *IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2022 (* Equal contribution).

[2] Yugeng Liu, Rui Wen, **Xinlei He**, Ahmed Salem, Zhikun Zhang, Michael Backes, Emiliano De Cristofaro, Mario Fritz, and Yang Zhang. ML-Doctor: Holistic Risk Assessment of Inference Attacks Against Machine Learning Models. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2022.

[3] **Xinlei He**, Jinyuan Jia, Michael Backes, Neil Zhenqiang Gong, and Yang Zhang. Stealing

Links from Graph Neural Networks. In *USENIX Security Symposium (USENIX Security)*. USENIX, 2021.

[4] **Xinlei He** and Yang Zhang. Quantifying and Mitigating Privacy Risks of Contrastive Learning. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*. ACM, 2021.

Preprint

[5] **Xinlei He**, Rui Wen, Yixin Wu, Michael Backes, Yun Shen, and Yang Zhang. Node-Level Membership Inference Attacks Against Graph Neural Networks. *CoRR abs/2102.05429*, 2021.

Teaching

Lectures

Teaching Assistant **Advanced Lecture: Privacy Enhancing Technologies**
May 2020 - September 2020, Saarland University

Teaching Assistant **Seminar: Data-driven Approaches on Understanding Disinformation**
May 2020 - September 2020, Saarland University