XIANG CAI

Contact Information

29 Millbrook Drive
Stony Brook, NY 11790, USA

Mobile: (631)680-8544
Email: xcai@cs.stonybrook.edu

Education

- **Stony Brook University** — Stony Brook, NY
  Ph.D. *candidate in Computer Science(GPA:3.93/4)* ***Expected May 2014***
  - Research focuse on **System Security, Network Security** and **Privacy.**
- **University of Sciences & Technology of China(USTC)** — Hefei, Anhui, China
  B.E. *in Computer Science(GPA:3.83/4.3)* ***July 2007***

Technical Skills

- Programming Languages: **C/C++** (proficient, 3+ years of experience), **Java** (intermediate), **python, ruby, PHP** (beginner)
- Development Tools: **gdb**, **git**, **Netbeans**
- Operating Systems: **Linux (Ubuntu)** (4+ years of experience)

Working Experience

- **Hewlett-Packard Labs** — Princeton, NJ
  Research Associate Internship ***June 2012 – August 2012***
  - Conduct large scale data analysis on passive DNS traffic to find malicious command-and-control servers.

Research Projects

- **Website fingerprinting defenses. Aug. 2012. [C++/ruby/python/MYSQL]**

  Developed bounds on the trade-off between security and bandwidth overhead that any fingerprinting defense scheme can achieve, which enables us to compare schemes with different security/overhead trade-offs by comparing how close they are to the lower bound.

  Refine, implement, and evaluate the Congestion-Sensitive BuFLO scheme, which attracted the attention of the Tor developers. Experiments find that Congestion- Sensitive BuFLO has high overhead (around 2.3-2.8x) but can get 6x closer to the bandwidth/security trade-off lower bound than Tor or plain SSH.
- **Website fingerprinting attacks on Tor. May. 2011. [C++/Java/ruby/MYSQL]**

  Proposed and implemented two new website fingerprinting attacks on the Tor anonymity system. Our web page classifier was novel in that, unlike all previous classifiers, it completely ignored packet sizes. Despite its simplicity, our attack outperformed recently-published fingerprinting attacks on Tor. Source code: **git@github.com:xiang-cai/fingerprinting_attack_code.git**

- **A novel machine registration procedure. Dec. 2010. [PHP/MYSQL]**

  Designed a novel online machine registration system. Users can register their computers to certain service providers (e.g. Banks, SNS websites) by visiting the registration website and then following specific instructions. This new process is as simple as most existing machine registration procedures yet more secure. Phishing and MITM attacks against the system are almost impossible.

- **A C library for serializable file-system accessing. Feb. 2010. [C/C++/Shell]**

  Proposed and implemented an easy-to-use, portable, provably-secure system for accessing UNIX file-systems without race conditions and that supported arbitrary sequences of operations within each pseudo-transaction and which had negligible overhead on a mail-server benchmark. Source code: **git@github.com:xiang-cai/trace.git**

- **Race attack on Unix File-Systems. Oct. 2008. [C/Shell]**

  Defeated two proposed Unix file-system race condition defense mechanisms. We argued that all kernel-based dynamic race detectors must have a model of the programs they protect or provide imperfect protection. Source code: **git@github.com:xiang-cai/race_attack.git**

Talks

- **Touching From a Distance: Website Fingerprinting Attacks and Defenses.**

  Invited talk to Symantec Research Labs. September 25th, 2012. Conference presentation at ACM CCS, Raleigh, NC, October 2012.

- **Exploiting Unix File-System Races via Algorithmic Complexity Attacks.**

  Conference presentation at IEEE Symposium on Security and Privacy, Oakland, CA, May 2009.

Academic Activities

- **Security and Communication Networks 2013,** Invited journal reviewer.

Publications

- New Approaches to Website Fingerprinting Defenses. **Xiang Cai**, Rishab Nithyanand and Rob Johnson. Submitted to *IEEE Symposium on Security and Privacy, Oakland, CA, 2014.*
- Touching From a Distance: Website Fingerprinting Attacks and Defenses. **Xiang Cai**, Xincheng Zhang and Rob Johnson. *ACM Conference on Computer and Communications Security, Raleigh, NC, October 2012.* (Acceptance rate: 19%, 81/426)
- Fixing Races For Good: Serializable File-System Access for UNIX. **Xiang Cai**, Rucha Lale, Xincheng Zhang and Rob Johnson. Recommended for publication. *ACM Transactions on Storage, 2012.*
- Exploiting Unix File-System Races via Algorithmic Complexity Attacks. **Xiang Cai**, Yuwei Gui, and Rob Johnson. *IEEE Symposium on Security and Privacy, Oakland, CA, May 2009.* (Acceptance rate: 10.2%, 26/254)