Xusheng Li

xusheng@vector35.com | https://xusheng.dev | https://github.com/xusheng6 |
https://www.linkedin.com/in/xusheng-li-8819b7329/

ABOUT

I am a software developer at Vector 35 Inc., where I am one of the core developers of Binary Ninja and lead the development of its debugger, including its Time-Travel Debugging (TTD) integration. My research interests span reverse engineering, malware analysis, vulnerability research, and code obfuscation. I am also an independent security researcher with multiple CVEs to my name (CVE-2025-13453, CVE-2025-13454, CVE-2025-13455).

I have spoken at RE//verse (2026) and CODEGATE (2025), guested on the *Behind the Binary* podcast by Google Cloud Security, and have been invited to present on various technical platforms. I have published in peer-reviewed journals including the *Journal of Computer Security* and *IEEE TIFS*, co-authored a book on assembly language and reverse engineering, and created an introductory Binary Ninja course on Open Security Training 2 (OST2). I am a peer reviewer for CCS, ESORICS, DSN, JCS, and other cybersecurity venues. I am a reviewer of *Paged Out!* magazine, and the administrator and reviewer of crackmes.one. I took 1st place in the Grand Reverse Engineering Challenge, completed the Flare-On reverse engineering challenge four consecutive times (2022–2025), and am a member of the Shellphish CTF team. I also contribute to widely-used open-source security tooling, including Google FLARE's capa (120k+ annual downloads) and CodeLLDB (8.4M+ installs).

SKILLS & ABILITIES

Reverse Engineering & Debugging

- Deep understanding of x86/x64 assembly and software reverse engineering. Experienced with binary obfuscation and anti-disassembly techniques
- Extensive debugging experience on Windows and Linux, including anti-debugging and anti-anti-debugging techniques
- Deep understanding of Windows internals
- Familiar with cryptography and networking. Strong in math (B.S. in Mathematics)
- Familiar with a wide spectrum of tools (e.g., Pin, LLVM, PANDA) and can quickly select the most suitable one for a given task

Development

- Proficient in C/C++ and Python, with six years of professional full-time development experience
- Lead developer of Binary Ninja's debugger, including its architecture, cross-platform adapter system, and TTD integration
- Ability to work independently on large-scale projects
- Familiar with software development workflows, e.g., Git and testing

EXPERIENCE

Vector 35 Inc — **Remote/Melbourne, FL**
Software Developer — **May 2020 - Present**

- Development of Debugger
  - Designing, architecting, and developing Binary Ninja's debugger with support for multiple platforms and backends
  - Integrated TTD (Time-Travel Debugging) on Windows via WinDbg/DbgEng and on Linux via rr/GDB RSP

- Created a unified API for the end user use while hiding the differences of the different operating systems
- The repo is open-source at https://github.com/Vector35/debugger

- Development of Binary Ninja. Worked independently on several major features.
  - x86 intrinsic lifting
  - Variable and type cross-references
  - Search enhancement
  - Various bug fixes and workflow improvements that enhance user experience

EDUCATION

Pennsylvania State University — **State College, PA**
Ph.D. in Information Sciences and Technology — **Aug 2017 – Jan 2021**

- Worked with Dr. Peng Liu in Cyber-security lab
- Discontinued due to the pandemic

University of Chinese Academy of Sciences — **Beijing, China**
Master Studies in Mathematics and Systems Science — **Sep 2015 - May 2017**

- Worked on machine learning and intelligent optimization
- Left (without degree) to attend Penn State

Nankai University — **Tianjin, China**
Bachelor Degree in Mathematics — **Sep 2011 – Jun 2015**

- Poling Class of Mathematics (Honorable Program)
- Honors:
  - Microsoft Research Young Fellow Scholarship Award
  - Meritorious Winner of Mathematical Contest in Modeling

PUBLICATIONS

- Luo, Nanqing, **Xusheng Li**, Haizhou Wang, Shuangyi Zhu, Yuan Ma, and Peng Liu. "Detecting Avalanche Effect in Adversarial Settings: Spotting the Encryption Loops in Ransomware." *arXiv preprint arXiv:2604.24131* (2026)
- Zhi Wang, **Xusheng Li**, et al. *Assembly language and reverse engineering technology*. Tsinghua University Press, 2025, ISBN: 978-7-302-68100-7. Sole author of the following chapters:
  - Chapter 9: C language patterns in assembly
  - Chapter 10: Static analysis and reverse engineering
  - Chapter 11: Dynamic analysis and reverse engineering
- Wang, Haizhou, Nanqing Luo, **Xusheng Li**, and Peng LIu. "Unmasking the shadows: Pinpoint the implementations of anti-dynamic analysis techniques in malware using llm." arXiv preprint arXiv:2411.05982 (2024). (Citations: 5)
- **Li, Xusheng**, Zhisheng Hu, Haizhou Wang, Yiwei Fu, Ping Chen, Minghui Zhu, and Peng Liu. "DeepReturn: A deep neural network can learn how to detect previously-unseen ROP payloads without using any heuristics." *Journal of Computer Security* 28, no. 5 (2020): 499-523. (Citations: 18)
- Zhu, Shuangyi, Yuan Ma, **Xusheng Li**, Jing Yang, Jingqiang Lin, and Jiwu Jing. "On the analysis and improvement of min-entropy estimation on time-varying data." *IEEE Transactions on Information Forensics and Security* 15 (2019): 1696-1708. (Citations: 25)

TALKS

- **Xusheng Li.** Invited guest at "Behind the Binary by Google Cloud Security" podcast. May 2026

- **Xusheng Li**. "Breaking Encrypted USB Drives with Time-Travel Debugging." Talk at RE//verse conference, March 2026, Orlando, Florida. Abstract, slides, recording
- **Xusheng Li**. "Introduction to Time-Travel Debugging (TTD)." Invited talk for the Competitive Cyber Security Organization (CCSO), The Pennsylvania State University, November 2025
- **Xusheng Li**. "Leveraging WinDbg in Binary Ninja — TTD and the WinDbg Backend." Invited presentation on Dr Josh Stroschein - The Cyber Yeti, September 2025. Recording
- Kyle Martin, **Xusheng Li**. "Abstractions for Program Analysis." Talk at CODEGATE 2025, July 2025, Seoul, South Korea
- **Xusheng Li**. "Introduction to Working with Time Travel Debugging in Binary Ninja." Invited presentation on Invoke RE with Joshua Reynolds, February 2025. Recording
- **Xusheng Li**. "Inside Windows' Default Browser Protection." Lightning talk at RE//verse conference, March 2025, Orlando, Florida. Article, slides, recording

COURSE DEVELOPMENT

- **Xusheng Li**, Debuggers 1103: Introductory Binary Ninja, Open Security Training 2 (OST2), Online (2025)
  - Created introductory course on Binary Ninja debugger fundamentals which can help cybersecurity professionals, researchers, and students to learn to use the Binary Ninja debugger and enhance practical reverse engineering and debugging skills.

REVIEW SERVICE

- **Peer reviewer for cybersecurity conferences and journals:**
  - Journal of Computer Security (JCS) – 2019, 2025, 2026 (3 manuscripts)
  - ACM Conference on Computer and Communications Security (CCS) – 2018 (2 manuscripts)
  - European Symposium on Research in Computer Security (ESORICS) – 2018, 2019 (4 manuscripts)
  - IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) – 2020 (1 manuscript)
  - IEEE Conference on Communications and Network Security (CNS) – 2018 (1 manuscript)
  - International Conference on Electrical, Computer and Energy Technologies (ICECET) – 2026 (2 manuscript)
- **Reviewer, Paged Out! Magazine**. Reviewed 50+ submitted articles for technical accuracy, clarity, and originality
- **Reviewer, crackmes.one**. Reviewed hundreds of submitted reverse engineering challenges and solutions for technical quality, correctness, and safety

SECURITY RESEARCH

- **Encrypted USB Drives:**
  - Discovered multiple severe vulnerabilities across 10+ devices from multiple vendors including Lenovo, Lexar, and Netac
  - Findings included unencrypted data storage, cleartext password exposure, and authentication bypasses
  - Lenovo published a security advisory and released fixes; Lexar implemented fixes for affected products
  - Assigned CVE-2025-13453, CVE-2025-13454, CVE-2025-13455
  - Research accepted as a talk at RE//verse 2026
- **Enterprise Encrypted USB:**

- Identified security weaknesses in an enterprise-grade encrypted USB drive from a Fortune 500 storage vendor
- Findings included unauthorized metadata modification and bypass of enforced read-only access policies
- Subsequently contracted by the vendor to verify the effectiveness of their remediation

- **BYOTC (Bring Your Own Trusted Client):**
  - Discovered a novel vulnerability class affecting Windows kernel-mode drivers with privileged user-mode components — a variant of the well-known BYOVD attack
  - Responsibly disclosed to System Informer, a widely-used Windows security tool, leading to the implementation of a fix
  - The vulnerability pattern affects a broader class of privileged driver implementations beyond a single product
- **Microsoft User Choice Protection Driver (UCPD):**
  - Reverse engineered undocumented Windows kernel-level mechanisms used to prevent third-party browsers from setting themselves as the default
  - Documented the technical cat-and-mouse dynamics between browser vendors attempting bypasses and Microsoft's countermeasures
  - Presented as a lightning talk at RE//verse 2025; published as a technical article on the Binary Ninja blog

OPEN-SOURCE CONTRIBUTIONS

- **capa (Google FLARE):**
  - Implemented a Binary Ninja-based feature extractor for capa, a widely adopted open-source malware capability detection tool with 120,000+ annual downloads
  - Contributed performance improvements, bug fixes, and architectural enhancements
- **LLVM/LLDB:**
  - Fixed a bug in LLDB preventing proper communication with gdbserver, restoring remote debugging functionality used by tools including VMware, QEMU, and Qiling
  - Fix resolved downstream issues in CodeLLDB (8.4M+ installs) and Binary Ninja's debugger
- **Msoffcrypto-tool:**
  - Enhanced encrypted Microsoft Office document handling, improving analysis capabilities for malware analysts and incident responders

AWARDS/RECOGNITIONS/CERTIFICATIONS

- Flare-on challenge: solved all challenges in 2022, 2023, 2024, and 2025. My write-ups for year 2023, 2024
- Completed NSA Coderbreaker challenge in 2019 (No.12 to finish)
- Took 1st place in the Grand Reverse Engineering Challenge. My writeup is here
- Administrator and maintainer of crackmes.one (since March 2025)
- Organizer of crackmes.one RE CTF
- Member of Shellphish CTF team
- GREM (GIAC Reverse Engineering Malware) certification
- Member of GIAC advisory board

ONLINE PUBLICATIONS (SELECTED)

- **Company Blogs/Technical Reports:**

- Li, Xusheng. “Defeating Anti-Reverse Engineering: A Deep Dive into the 'Trouble' Binary.” Binary Ninja. January 23, 2026. https://binary.ninja/2026/01/23/reversing-linux-anti-re.html
- Li, Xusheng. “Working with Global Pointers in Binary Ninja.” Binary Ninja. August 7, 2025. https://binary.ninja/2025/08/07/working-with-global-pointers.html
- Li, Xusheng. “Inside Windows' Default Browser Protection.” Binary Ninja. March 29, 2025. https://binary.ninja/2025/03/25/default-browser-upcd.html
- Li, Xusheng. “Having Fun with Flare-on Using Time-Travel Debugging (TTD).” Binary Ninja. December 16, 2024. https://binary.ninja/2024/12/16/flareon-ttd.html
- Li, Xusheng. “Analyzing Obfuscated Code with Binary Ninja -- a Flare-on Journey.” Binary Ninja, November 13, 2023. https://binary.ninja/2023/11/13/obfuscation-flare-on.html
- Li, Xusheng. “Reverse Engineering a Cobalt Strike Dropper with Binary Ninja.” Binary Ninja, July 22, 2022. https://binary.ninja/2022/07/22/reverse-engineering-cobalt-strike.html
- Li, Xusheng. “Winning the Grand Reverse Engineering Challenge with Binary Ninja.” Binary Ninja, September 2, 2021. https://binary.ninja/2021/09/02/winning-the-grand-re-challenge.html. (Citations: 1)
- Li, Xusheng. “Solving an Obfuscated Crackme with Binary Ninja and Triton.” Binary Ninja, July 14, 2020. https://binary.ninja/2020/07/14/solving-an-obfuscated-crackme-with-binaryninja-and-triton.html.

- **Paged Out! Institute Magazine Articles:**

- Li, Xusheng. “The x86 Read Watchpoint That Doesn’t Exist.” Paged Out! No. 8, Feb 19, 2026. https://pagedout.institute/download/PagedOut_008.pdf.
- Li, Xusheng. “How Does Your Browser Pause Downloads?.” Paged Out! No. 8, Feb 19, 2026. https://pagedout.institute/download/PagedOut_008.pdf.
- Li, Xusheng. “Reviving an Excel 2000 Easter Egg.” Paged Out! No. 6, March 29, 2025. https://pagedout.institute/download/PagedOut_006.pdf.
- Li, Xusheng. “Examining USB Copy Protection.” Paged Out! No. 5, November 19, 2024. https://pagedout.institute/download/PagedOut_005.pdf.
- Li, Xusheng. “Brotli Zip Archive.” Paged Out! No. 4, June 2, 2024. https://pagedout.institute/download/PagedOut_004_beta1.pdf.
- Li, Xusheng. “Solving a Snake Challenge with Hamiltonian Cycle.” Paged Out! No. 3, December 18, 2023. https://pagedout.institute/download/PagedOut_003_beta1.pdf.

- **Crackmes.one Blogs:**

- Li, Xusheng. “Crackmes.one RE CTF 2026 - A Recap.” Crackmes.one blog, February 21, 2026. https://blog.crackmes.one/2026/02/21/crackmes-one-ctf-2026-recap.html

- **Personal Blogs:**

- Li, Xusheng. “Solving a VM Challenge Using Binaryninja.” Xusheng’s blog, April 18, 2021. https://xusheng.dev/posts/reversing/kata_vm/readme/
- Li, Xusheng. “Solving Two Ocaml Crackmes without Knowing Much about OCaml.” Xusheng’s blog, December 13, 2020. https://xusheng.dev/posts/reversing/ocaml_crackmes/readme/
- Li, Xusheng. “Deciphering a Windows Anti-Debugging Challenge.” Xusheng’s blog, November 29, 2020. https://xusheng.dev/posts/reversing/reverseme3/readme/
- Li, Xusheng. “Dealing with Manipulated Elf Binary and Manually Resolving Import Functions.” Xusheng’s blog, August 30, 2020. https://xusheng.dev/posts/reversing/elf_format/readme/
- Li, Xusheng. “Making and Solving a Reversing Challenge Based-on X86 Isa Encoding.” Xusheng’s blog, August 2, 2020. https://xusheng.dev/posts/reversing/x86/readme/

- Li, Xusheng. “Solving a Recursive Crackme by Automating GDB.” Xusheng’s blog, July 27, 2020. https://xusheng.dev/posts/reversing/automating-gdb/readme/
- Li, Xusheng. “Solving an Arm Challenge with Z3.” Xusheng’s blog, June 18, 2020. https://xusheng.dev/posts/reversing/armageddon/solve/
- Li, Xusheng. “Debugging and Solving an Android Challenge.” Xusheng’s blog, May 30, 2020. https://xusheng.dev/posts/reversing/quarkslab_android_crackme/main/
- Li, Xusheng. “Solving a Reversing Challenge with Mitmproxy and OCR.” Xusheng’s blog, April 27, 2020. https://xusheng.dev/posts/reversing/client_houseplant_ctf_2020/solve/

ADDITIONAL INFORMATION

Languages: English (fluent), Chinese (native)