Zhichun Li

Research Interests

I have board research interests in security, system, networking, big-data, and AI related areas. My research has been interdisciplinary. Recently, in NEC Labs, I have combined ingredients from the aforementioned fields to build security solutions to solve difficulty security problems, such as Advanced Persistent Threats (APT) etc.

Education

2004.08 — 2009.12 Northwestern University, Evanston, IL 60201, USA
Ph.D. in Computer Science (Dec 2009)
Dissertation topic: *Router-based Anomaly/Intrusion Detection and Mitigation*
Advisor: Prof. Yan Chen
GPA: 4.0/4.0

2000.09 — 2003.07 Tsinghua University, Beijing, P.R. China
M.S. in Computer Science

1997.09 — 2000.07 Tsinghua University, Beijing, P.R. China
B.S. in Applied Physics
Finished the four-year undergraduate program in three years

Professional Experience

2016.4 — Present Department Head in Computer Security Department in **NEC Research Labs**, Princeton, NJ 08540, USA

- Responsible for the research vision on cyber security in NEC Labs. Provide suggestions on business incubation on security, big-data, and AI solutions
- Manage four million dollar research budget a year. Define the research agenda for the department, lead the team, and work with Business Units on research result technique transfer and funding proposals.
- Manage 10 full-time researchers, and about 8-10 research assistants. Collaborate with six researchers and BU teams in Japan.
- Continue leading the Automated Security Intelligence (ASI) project, which is a flagship large-scale interdisciplinary research project in NEC.
- Based on the ASI commercialization fund directly provided by NEC CEO, work with BU (Business Unit) partners to commercialize ASI as a new security solution for NEC.
- Deliver the ASI prototype with half million lines of code (without counting open-source code) to BU engineering team, together with technology transfer and design knowledge transfer.
- Work with BU engineering team on ASI commercial version enhancement
- Work with BU partners on ASI business development and customer promotion. Promote Lean Enterprise to BU partners to speed up ASI marketization.

2012.5 — 2016.4 Project leader in Autonomic Management Department in **NEC Research Labs**, Princeton, NJ 08540, USA

2015.5 — 2016.4 Senior Research Staff Member in Autonomic Management Department

2012.5 — 2015.5 Research Staff Member in Autonomic Management Department

- Propose, initiate and lead the Automated Security Intelligence (ASI) project, which aims to bring 360

degree visibility to enterprise through ubiquitous endpoint monitoring and big-data processing, to detect unknown attacks and to speed-up incident analysis up to 100 times with AI technologies and advanced algorithms.

- Build full-stack ASI prototype system from agent, data platform, security application to web UI, and produce half million lines of code without counting open-source components. Initialize security research team inside NEC Labs and grow to nine full-time researchers, and collaborate another team of researchers in Tokyo Japan for customer trails (PoC).

2010.8 — 2012.5 Research Staff Member in Autonomic Management Department in **NEC Research Labs,** Princeton, NJ 08540, USA

- Propose and lead the Mobile Application Security project with the goals of designing highly accurate and scalable cloud solutions for filtering the malicious or vulnerable Android apps in different Android markets to improve the security management of smartphone carriers. Design and build DALYSIS a static analysis framework for off-the-shelf Android apps. Furthermore, design and implement a component hijacking vulnerability checker on top of DALYSIS. DALYSIS has been used as an internal developer tool inside NEC.

2004.08 — 2010.08 **Northwestern University**, Evanston, IL 60201, USA

2009.12 — 2010.8 Research Associate for Yan Chen, Department of EECS

2004.08 — 2009.12 Research Assistant for Yan Chen, Department of EECS

I have worked on many different security and networking projects – all motivated by the need to improve security and robustness of network services on the Internet.

- Designed the WebShield system, a secure proxy that prevents JavaScript related attacks.
- Designed the NetShield system which is the first system capable of efficiently matching a large number of vulnerability signatures at high speed.
- Discovered that P2P address misconfiguration is highly prevalent, and further developed the P2PScope system to diagnose the root causes of such misconfiguration.
- Designed LESG, a network-based signature generation algorithm for zero-day polymorphic buffer overflow worms with provable attack resilience.
- Designed Hamsa, a fast content-based signature generator, which has provable attack resilience under reasonable assumptions.
- Designed reversible sketch, a compact streaming data structure, which is able to record hundreds of thousands of flows while recovering the heavy hitters or heavy changes offline even after temporal/spatial linear aggregation.
- Designed a sketch-based DoS resilient high-speed intrusion detection system.

2008.06 — 2008.09 **Microsoft Research**, Redmond, WA98052, USA

Research Intern mentored by Ming Zhang, Albert Greenberg and Yi-min Wang

- Designed a timing-perturbation based approach to generate the dependency graphs of complex web 2.0 applications.
- Proposed a browser model for identifying performance bottlenecks in complex web 2.0 applications, such as Google Maps, based on their dependency graphs.

2006.06 — 2006.09 **ICSI Center for Internet Research**, **UC Berkeley**, CA94704, USA

Research Intern mentored by Vern Paxson (ICSI & UC Berkeley)

- Investigated the significance of large-scale "botnet probes." Proposed statistical tests for checking the scan strategies used by botmasters and further designed schemes to extrapolate the global properties of botnet events (e.g., total population and target scope) as inferred from the limited local view of a honeynet.

2003.08 — 2004.08 **Tsinghua University**, Beijing P.R. China

Researcher in IP Monitoring and Accounting Group, National Network Center of CERNET[1]

- Analyzed many real-world anomaly/intrusion cases observed on the national backbone of CERNET.
- Designed the high speed MonAgent (Monitoring Agent) based on Intel IXP network processors.

2000.3 — 2003.07 **Tsinghua University**, Beijing P.R. China

Graduate Research Assistant in IP Monitoring and Accounting Group, National Network Center of CERNET

- Designed and implemented Linuxflow, a high-performance passive network measurement facility.
- Designed and implemented the CERNET backbone IP MONitoring system (IPMON) for network monitoring and anomaly detection, which has been used to detect unknown worms and DDoS attacks.

Publications

Book Chapters:

[1] **Zhichun Li**, Anup Goyal and Yan Chen, "Honeynet-based Botnet Scan Traffic Analysis," invited book chapter for "Botnet Detection: Countering the Largest Security Threats," Springer-Verlag, 2007.

Conference and Workshop Papers

[2] Zhang Xu, Zhenyu Wu, **Zhichun Li**, Kangkook Jee, Junghwan Rhee, Xusheng Xiao, Fengyuan Xu, Haining Wang, Guofei Jiang, "High Fidelity Data Reduction for Big Data Security Dependency Analyses, ", in *the proceedings of **ACM CCS 2016***

[3] Bo Zong, Xusheng Xiao, **Zhichun Li**, Zhenyu Wu, Zhiyun Qian, Xifeng Yan, Ambuj K. Singh, and Guofei Jiang, "Behavior Query Discovery in System-Generated Temporal Graphs, " in *the proceedings of **VLDB 2016***

[4] Jianjun Huang, **Zhichun Li**, Xusheng Xiao, Zhenyu Wu, Kangjie Lu, Xiangyu Zhang, Guofei Jiang, "SUPOR: Precise and Scalable Sensitive User Input Detection for Android Apps, " in *the proceedings of **USENIX Security 2015***

[5] Kangjie Lu, **Zhichun Li**, Vasileios Kemerlis, Zhenyu Wu, Long Lu, Cong Zheng, Zhiyun Qian, Wenke Lee, Guofei Jiang, "Checking More and Alerting Less: Detecting Privacy Leakages via Enhanced Data-flow Analysis and Peer Voting, " in *the proceedings of **NDSS 2015***

[6] Yinzhi Cao, Vaibhav Rastogi, Zhichun Li, Yan Chen, Alex Moshchuk,"Redefining Web Browser Principals with a Configurable Origin Policy," In *the proceedings of IEEE/IFIP International Conference on **Dependable Systems and Network (DSN) 2013***.

[7] Long Lu (my intern), **Zhichun Li**, Zhenyu Wu, Wenke Lee, Geoff Jiang, "CHEX: Statically Vetting Android Apps for Component Hijacking Vulnerabilities," in *the Proceedings of ACM **CCS*** 2012 (80/423=18.9%)

[8] Yinzhi Cao, **Zhichun Li**, Vaibhav Rastogi, Xitan Wen and Yan Chen, "Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security," full paper in *the Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (**ASIACCS'12)***, May 2012 (35/159=22.0%)

[9] **Zhichun Li**, Yi Tang, Yinzhi Cao, Vaibhav Rastogi, Yan Chen and Bin Liu, "WebShield: Enabling Various Web Defense Techniques without Client Side Modifications," in *the Proceedings of the Annual Network and Distributed System Security Symposium (**NDSS**)*, 2011 (28/139=20.1%).

[10] Hongyu Gao, Jun Hu, Christo Wilson, **Zhichun Li**, Yan Chen, and Ben Y. Zhao, "Detecting and Characterizing Social Spam Campaigns", in *the Proceedings of ACM SIGCOMM **IMC*** 2010 (47/211=22.3%). (featured in The Wall Street Journal Online, MIT Technology Review and ACM Tech News)

[1] CERNET (China Education and Research Network)

[11] **Zhichun Li**, Gao Xia, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Junchen Jiang and Yuezhou Lv, "NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense," In *the Proceedings of ACM **SIGCOMM*** 2010, August 2010 (33/276=12%). (Cisco has been interested in this project, and has shared us the Cisco IPS ruleset).

[12] **Zhichun Li**, Ming Zhang, Zhaosheng Zhu, Yan Chen, Albert Greenberg and Yi-Min Wang, "WebProphet: Automating Performance Prediction for Web Services," in *the Proceedings of USENIX Symposium on Networked Systems Design and Implementation (**NSDI**),* April 2010 (29/175=17%).

[13] **Zhichun Li**, Anup Goyal, Yan Chen and Aleksandar Kuzmanovic, "Measurement and Diagnosis of Address Misconfigured P2P Traffic," in *the Proceedings of IEEE **INFOCOM** 2010*, March 2010 (276/1575=18%)

[14] **Zhichun Li**, Anup Goyal, Yan Chen and Vern Paxson, "Automating Analysis of Large-Scale Botnet Probing Events," in *the Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (**ASIACCS'09**)*, March 2009 (33/147=22%).

[15] **Zhichun Li**, Lanjia Wang, Yan Chen and Judy Fu, "Network-based and Attack-resilient Length Signature Generation for Zero-day Polymorphic Worms," in *the Proceedings of the IEEE **ICNP** 2007*, October 2007 (32/220=14%).

[16] **Zhichun Li**, Manan Sanghi, Yan Chen, Ming-Yang Kao and Brian Chavez, "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience," full paper in *the Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**)*, May 2006 (23/251=9%).

[17] **Zhichun Li**, Yan Chen and Aaron Beach, "Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing," in *the Proceedings of ACM SIGCOMM Workshop on Large-Scale Attack Defense (**LSAD**)*, September 2006 (11/33=33%).

[18] Yan Gao, **Zhichun Li** and Yan Chen, "A DoS Resilient Flow-level Intrusion Detection Approach for High-speed Networks," in *the Proceedings of the 26th International Conference on Distributed Computing Systems (**ICDCS**)*, July 2006 (75/536=14%).

[19] Robert Schweller, **Zhichun Li**, Yan Chen, Yan Gao, Ashish Gupta, Yin Zhang, Peter Dinda, Ming-Yang Kao and Gokhan Memik, "Reverse Hashing for High-speed Network Monitoring: Algorithms, Evaluation, and Applications," in *the Proceedings of IEEE **INFOCOM** 2006*, April 2006 (252/1400=18%).

[20] Pin Ren, Yan Gao, **Zhichun Li**, Yan Chen and Ben Watson, "IDGraphs: Intrusion Detection and Analysis Using Histographs," in *the Proceedings of the IEEE Workshop on Visualization for Computer Security (**VizSEC**), in conjunction with Visualization 2005 and InfoVis 2005 conferences*.

[21] **Zhichun Li**, Hui Zhang, Yue You and Tao He "Linuxflow: A High Speed Backbone Measurement Facility," in *the Proceedings of Passive and Active Measurement Workshop 2003 (**PAM2003**)*, April 2003.

[22] Tao He, Xing Li, Jian Qiu, Hui Zhang and **Zhichun Li**, "Statistical Characteristics of Multicast Traffic on a Nationwide Backbone Network," in *the Proceedings of Asia-Pasific Advanced Network*, August 2003.

[23] Tao He, Hui Zhang, Xing Li and **Zhichun Li**, "A Methodology for Analyzing Backbone Network Traffic at Stream-Level," in *the Proceedings of IEEE International Conference on Communication Technology (ICCT2003)*, April 2003.

Journal Papers

[24] **Zhichun Li**, Anup Goyal, Yan Chen and Aleksandar Kuzmanovic, "Measurement and Diagnosis of Address Misconfigured P2P Traffic," in ***IEEE Network Magazine**,* Volume. 25, no. 3, May 2011.

[25] **Zhichun Li**, Anup Goyal, Yan Chen and Vern Paxson, "Towards Situational Awareness of Large-scale Botnet Probing Events," in *IEEE **Transactions on Information Forensics and Security,*** volume 6, Issue 1, March 2011.

[26] **Zhichun Li**, Yan Gao and Yan Chen, "HiFIND: a High-speed Flow-level Intrusion Detection Approach with DoS Resiliency," in ***Journal of Computer Networks***, Volume 54, Issue 8, June 2010 (Interested by Cisco, which wants to implement this into their switch security framework)

[27] Lanjia Wang, **Zhichun Li**, Yan Chen and Judy Fu, "Thwarting Zero-Day Polymorphic Worms with Network-Level Length-Based Signature Generation," in *IEEE/ACM **Transactions on Networking***, Volume 18, Issue 1, 2010.

[28] Robert Schweller, **Zhichun Li**, Yan Chen, Yan Gao, Ashish Gupta, Yin Zhang, Peter Dinda, Ming-Yang Kao and Gokhan Memik, "Reversible Sketches: Enabling Monitoring and Analysis over High-speed Data Streams," in *IEEE/ACM **Transactions on Networking***, Volume 15, Issue 5, Oct. 2007.

[29] Pin Ren, Yan Gao, **Zhichun Li**, Yan Chen and Benjamin Watson, "IDGraphs: Intrusion Detection and Analysis Using Stream Compositing," in *IEEE **Computer Graphics and Applications***, vol. 26, no. 2, pp. 28-39, Mar/Apr, 2006.

[30] **Zhichun Li**, Hui Zhang, Yue You and Zimu Li, "Design and Implementation of A High Speed Backbone Measurement System" (in Chinese), in *Journal of Computer Engineering* (Chinese), Vol.29, pp.53-56, 2002.

Software (Released prior joining NEC Labs)

NetShield. A software prototype of the NetShield vulnerability-signature based intrusion detection system. We intend to build the software prototype of NetShield as a better alternative to the popular open source tool Snort.
(http://www.nshield.org)

Hamsa. A C++ implementation of the Hamsa polymorphic worm signature generator that includes a fast token extraction library and the Hamsa core engine. When given suspicious traffic as input and normal traffic as reference, Hamsa generates the token conjunction signatures for possible worms in the suspicious traffic. Upon the requests from various institutions such as Columbia Univ., UT Austin, Purdue Univ., Georgia Tech and UC Davis, I released the Hamsa system and its related testing polymorphic worms in 2006.
(http://www.zhichunli.org/software/download.php?file=CHamsa-1.0.tar.gz)

RevSketch. A C++ implementation of the *k*-ary reversible sketch data structure and its heavy key recovery algorithm. RevSketch is capable of recording a large number of flows. It has APIs to combine multiple reversible sketches linearly and then to recover the heavy keys.
(http://www.zhichunli.org /software/download.php?file=RevSketch-1.0.tar.gz)

Linuxflow. A passive network measurement facility which is faster than the standard AF_PACKET in the Linux kernel. It includes a set of Linux kernel modules designed for high-speed networks such as gigabit networks. It provides APIs for users to write packet-filter code and to manipulate packets in Linux kernel space, and also provides capability to send packet information to user-space applications by a socket interface. This tool has been used in the IP Accounting System of CERNET (China Education and Research Network), and has stably run for more than five years.
(http://www.zhichunli.org/linuxflow)

Teaching Experience

- **Co-Instructor** of EECS 450 – Internet Security (*Northwestern University*)
  Developed the syllabus, gave lectures to the class, mentored individual class projects, and led the class discussion.
- **Guest Lectures** in EECS 340 – Introduction to Computer Networking (*Northwestern University*)
  Gave guest lectures on the topics of network security.
- **Teaching Assistant** of CS 395/495 – Introduction to Computer Security (*Northwestern University*)
  Developed all the course projects including encryption, intrusion detection and network penetration. Led the quiz reviews and Q&A sessions.

- **Teaching Assistant** of EECS 328 – Numerical Methods for Engineers (*Northwestern University*)
  Taught Matlab recitation sessions for 55 students. Answered students' questions, graded programming assignments, and led quiz reviews.
- **Teaching Assistant Training**
  Participated in the one-year teaching assistant training program for international students (I- Scholar program). Worked with undergraduate teaching partners. Taught them computer science and various other topics for two hours every week. This helped improve my teaching skills based on their feedback.

Honors

- ASI project led by me won CEATEC 2016 Award
- NEC Excellent Invention Award 2016
- Our SUPOR paper in USENIX Security 2015 has been selected as top 10 finalists of CSAW Best Paper Award
- NEC Labs Spot Recognition Award 2012
- Terminal Year Smith Fellowship, Northwestern University, 2008-2009
- Nominee for Microsoft Research Fellowship, EECS Dept, Northwestern University, 2007
- IEEE Symposium on Security and Privacy (Oakland) travel grant, 2006, 2008 and 2009
- ACM SIGCOMM 2007 travel grant, 2007
- IEEE ICNP 2007 travel grant, 2007
- First prize of National Physics Olympics, China, 1996

Professional Activities

- **Conference and Workshop Organization:**

2017	Program Committee, ACM Conference on Computer and Communication Security (CCS)
2015	Program Committee, Network & Distributed System Security Symposium (NDSS)
2015	Program Committee, IEEE INFOCOM
2014	Program Committee, ACM Conference on Computer and Communication Security (CCS)
2014	Program Committee, IEEE CNS (IEEE Conference on Communications and Network Security)
2014	Program Committee, IEEE INFOCOM
2014	Program Committee, ACM Symposium on Information, Computer Communications Security (ASIACCS)
2014	Program Committee, MoST (Mobile Security Technologies Workshop)
2013	Program Committee, International ICST Conference on Security and Privacy in Communication Networks (SecureComm)
2013	Program Committee, IEEE/ACM International Symposium on Quality of Service (IWQoS)
2013	Program Committee, ACM Symposium on Information, Computer & Communications Security (ASIACCS)
2013	Program Committee, Network & Distributed System Security Symposium (NDSS)

2013 Program Committee, IEEE INFOCOM

2012 Program Committee, International Conference on Availability, Reliability and Security (AReS)

2012 Program Committee, ACM Symposium on Information, Computer & Communications Security (ASIACCS)

2012 Program Committee, International World Wide Web Conference (WWW), the Security, Privacy, Trust and Abuse track

2012 Program Committee, IEEE INFOCOM

2012 Program Committee, IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium (ICNC-CLD)

2011 Web Chair, ACM Conference on Computer and Communication Security (CCS)

2011 Program Committee, ACM Conference on Computer and Communication Security (CCS) Poster & Demo Session

2011 Program Committee, IEEE GLOBECOM Next-Generation Networking (NGN) Symposium

2011 Program Committee, IEEE International Workshop on Security in Computers, Networking and Communications (SCNC)

2011 Program Committee, IEEE ICC Next-Generation Networking and Internet Symposium (ICC NGNI)

2010 Program Committee, IEEE International Workshop on Quality of Service (IWQoS)

2010 Program Committee, IEEE GLOBECOM Next-Generation Networking (NGN) Symposium

2010 Program Committee, IEEE Vehicular Technology Conference: VTC2010-Fall

2009 Program Committee, International ICST Conference on Security and Privacy in Communication Networks (SecureComm)

- **External Reviewer**:
    - IEEE Transactions on Dependable and Secure Computing
    - IEEE Transactions on Information Forensics & Security
    - IEEE/ACM Transactions on Networking
    - IEEE Transactions on Parallel and Distributed Systems
    - IEEE Transactions on Network and Service Management
    - IEEE Transactions on Computers
    - ACM Transactions on Internet Technology
    - IEEE Network Magazine
    - ACM Computing Surveys
    - Journal on Selected Areas in Communications (JSAC)
    - Journal of Computer Networks
    - Journal of Computer Communications
    - Security and Communication Networks
    - International Journal of Network Security
    - Network & Distributed System Security symposium (NDSS) (2010,2009)

- IEEE/IFIP International Conference on Dependable System and Networks (DSN) 2010
- IEEE INFOCOM (2010—2007)
- IEEE ICNP (2009—2007)
- International ICST Conference on Security and Privacy in Communication Networks (SecureComm) (2010, 2008)
- IEEE ICDCS (2008,2007)
- ACM Mobicom 2007
- IFIP/IEEE International Symposium on Integrated Management (IM) 2007
- IEEE International Workshop on Quality of Service (IWQoS) (2007,2006).

- **Previous Grant Proposal Contributions**:
  "Router-Based Signature Generation for Zero-Day Polymorphic Worms," NSF Cyber Trust Program, Award CNS-0627751 (my paper [16] and the early draft of my paper [15] serve the basis for this proposal)

  "High-Speed Network Defense with Massive and Diverse Vulnerability Signatures," NSF Cyber Trust Program, Award CNS-0831508 (the early draft of my paper [11] serves the basis for this proposal)

  "HPNAIDM: The High-Performance Network Anomaly/Intrusion Detection and Mitigation System," DoE (Department of Energy), Early CAREER Award DE-FG02-05ER25692//A001 (the early drafts of my paper [17][18][19] serves the basis for this proposal)

  "Intrusion Detection and Forensics for Self-defending Wireless Networks," DoD (Air Force Office of Scientific Research), Young Investigator Award FA9550-07-1-0074 (the early draft of my paper [13][14] has contributed to this proposal)