XIN HU

IBM T.J. Watson Research Center, Yorktown Heights, NY
734-717-5947 • huxin@us.ibm.com

RESEARCH INTERESTS

My research interests lie primarily in the general area of cybersecurity, with an emphasis on network security and application of data mining and machine learning techniques on large-scale network traffic and malware data for predictive analytics, anomaly detection and reputation systems. Other research interests include botnet detection, malware analysis, signature generation, sensor network, routing protocol security.

EDUCATION

Ph.D. in Computer Science and Engineering 09/2007 – 08/2011
University of Michigan, Ann Arbor
Dissertation: Large scale malware analysis, detection and signature generation
Advisor: Professor Kang G. Shin

Master of Science in Computer Science and Engineering 09/2005 – 05/2007
University of Michigan, Ann Arbor
GPA: 8.529/9.0 (8.0 = A, 9.0 = A^+)

Bachelor of Engineering in Computer Science and Engineering 09/2001 – 06/2005
Zhejiang University, Zhejiang, China
GPA: 3.94/4.0 (91.56/100); GPA for Major Courses: 4.0/4.0 (93.25/100)

PUBLICATIONS

1. **Can Open WiFi Networks Be Lethal Weapons for Botnets?**
   Matthew Knysz, Xin Hu, Yuanyuan Zeng and Kang G. Shin
   Proceedings of 31th IEEE International Conference on Computer Communications, Mini-Conference (IEEE INFOCOM 2012), Shanghai, China, April 2012
2. **Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets**
   Yuanyuan Zeng, Kang G. Shin and Xin Hu
   Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks, (ACM WiSec' 12), 2012
3. **Privacy Protection for Users of Location-Based Services**
   Kang G. Shin, Xiaoen Ju, Zhigang Chen, and Xin Hu
   IEEE Wireless Communications Magazine, Volume 19, Issue 1, Pages: 30-39, February, 2012
4. **Measurement and Analysis of Global IP-Usage Patterns of Fast-Flux Botnets**
   Xin Hu, Matthew Knysz, Kang G. shin
   Proceedings of 30th IEEE International Conference on Computer Communications (IEEE

INFOCOM 2011), Shanghai, China, April 2011 (Acceptance ratio: 15.96% = 291/1823)

5. **Good Guys vs. Bot Guise: Mimicry Attacks Against Fast-Flux Detection Systems**
   Matthew Knysz, Xin Hu, Kang G. shin
   Proceedings of 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), Shanghai, China, April 2011 (Acceptance ratio: 15.96% = 291/1823)

6. **Secure Cooperative Sensing in IEEE 802.22 WRANs using Shadow Fading Correlation**
   Alexander W. Min, Kang G. Shin and Xin Hu,
   IEEE Transactions on Mobile Computing (TMC), Volume 10, Issue 10, Pages 1434-1447, 2011

7. **Detection of Botnets Using Combined Host- and Network-Level Information**
   Yuanyuan Zeng, Xin Hu, Kang G. Shin
   Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (IEEE/IEIF DSN 2010), June 2010 (Acceptance ratio: 23.2% = 39/168)

8. **A Study on Latent Vulnerabilities**
   Beng Heng Ng, Xin Hu, Atul Prakash
   1st International Workshop on Resilience Assessment of COmplex Systems (RACOS 2010), Delhi, India, November 2010

9. **Large-Scale Malware Indexing Using Function-Call Graphs**
   Xin Hu, Tzi-cker Chiueh, Kang G. Shin
   Proceedings of the 16th ACM Conference on Computer and Communications Security (ACM CCS 2009), Chicago, IL, November 2009 (Acceptance ratio: 18.4% = 58/315) **2nd Place AT&T Award for Best Applied Security Research Paper**

10. **RB-Seeker: Automatic Detection of Redirection Botnets**
    Xin Hu, Matthew Knysz, Kang G. Shin
    Proceedings of the 16th Annual Network and Distributed System Security Symposium (NDSS 2009), San Diego, CA, February 2009 (Acceptance ratio:11.7% = 20/171)

11. **Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks**
    Alexander W. Min, Kang G. Shin and Xin Hu
    Proceedings of the 17th IEEE International Conference on Network Protocols (IEEE ICNP 2009), Princeton, NJ, October 2009 (Acceptance ratio: 18.3% = 36/197)

12. **Automatic Generation of String Signatures for Malware Detection**
    Kent Griffin, Scott Schneider, Xin Hu, Tzi-cker Chiueh
    Proceedings of the 12th Symposium on Recent Advances in Intrusion Detection (RAID 2009), Brittany, France, September 2009 (Acceptance ratio: 28.8% = 17/59)

13. **Behavioral Detection of Malware on Mobile Handsets**
    Abhijit Bose, Xin Hu, Kang G. Shin,Taejoon Park
    Proceedings of the 6th Annual International Conference on Mobile Systems (ACM/Usenix Mobisys 2008), Breckenridge, CO, June 2008 (Acceptance ratio: 17.9% = 22/123)

14. **Attack-Tolerant Time-Synchronization in Wireless Sensor Networks**
    Xin Hu, Taejoon Park, Kang G. Shin

Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM 2008), Phoenix, AZ, April 2008 (Acceptance ratio: 20.5% = 236/1152)

15. **Wide-Area IP Network Mobility**
    Xin Hu, Li Li, Z. Morley Mao, Yang Richard Yang
    Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM 2008), Phoenix, AZ, April 2008 (Acceptance ratio: 20.5% = 236/1152)

16. **Containment of Network Worms by Per-Process Rate-Limiting**
    Yuanyuan Zeng, Xin Hu, Abhijit Bose, Haixiong Wang, Kang G. Shin
    Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SecureCom 2008), İstanbul, Turkey, September, 2008 (Acceptance ratio: 21.1% = 26/123)

17. **Accurate Real-time Identification of IP Prefix Hijacking**
    Xin Hu and Z. Morley Mao
    Proceedings of IEEE Symposium on Security and Privacy (IEEE Oakland 2007), Oakland, CA, May 2007 (full paper, Acceptance ratio: 8.1% = 20/246)

HONORS AND AWARDS

- **IBM Appreciation Award** 2012
  For "tremendous help with Cyber Security Assets"
- **2nd place, AT&T Award for Best Applied Security Research Paper** 2010
- **Winner of Yahoo! Key Scientific Challenges Program** 2010
  One of 23 exceptional Ph.D. students nationwide to receive the award with 5K research funding
- **Symantec Research Labs Graduate Fellowship** 2010
  One of the two winners of the fellowship, which covers full tuition and stipend
- **Travel Grant to Google GRAD CS Forum** 2010
- **2nd place, CSE Graduate Honor Competition, University of Michigan**
  For the best research and presentations among graduate students in the CSE Department
- **ACM CCS Travel Grant Award** 2009
- **2nd place in Symantec Research/Project Showcase Competition** 2008
  Awarded to top research work among all interns in Symantec Research Labs
- **Mobisys 2008 Travel Grant Award** 2008
- **IEEE Security and Privacy Student Travel Grant** 2007
- **1st place winner in Windows CE Shared Source Contest** 2006
  1st place winner in the national contest sponsored by Microsoft and WindowsForDevices.com
- **Rackham Graduate Fellowship, University of Michigan**
  To selected incoming students with outstanding academic records

PATENTS

Issued Patents:

- Tzi-cker Chiueh, Kent Griffen, Scott Schneider, Xin Hu, "**Selecting Malware Signatures Based on Malware Diversity**", US Patent No. 8,321,942, Issued on Nov. 27, 2012
- Taejoon Park, Kang Geun Shin, Xin Hu, Abhijit Bose, "**Apparatus and Method For Detection of Malicious Program Using Program Behavior**", US Patent No. 8,245,295, Issued on Aug. 14, 2012
- Kent Griffin, Tzicker Chiueh, Scott Schneider, Xin Hu, "**Selecting Malware Signatures to Reduce False-Positive Detections",** US Patent No. 8,239,948, Issued on Aug 7th, 2012

Patent Applications:

- Andrew White, Mihai Christodorescu, Marc Stoecklin, Xin Hu, Ting Wang, Reiner Sailer, Douglas Schales, **"Method and Apparatus for the Identification and Classification of Web Traffic Inside Encrypted Network Tunnels"**, Patent Disclosure No. YOR820120996, by IBM Corp., 2013
- Douglas Schales, Reiner Sailer, Marc Stoecklin, Ting Wang, Xin Hu, Mihai Christodorescu, **"Apparatus and Method for Highly Scalable Distributed Feature Collection Engine for Cyber Security Analytics",** Patent Disclosure No. YOR820120857, by IBM Corp., 2012
- Xin Hu, Sandeep Bhatkar and Kent Griffin, "**Method for Encoding Machine Code Instructions for Static Feature based Malware Clustering**", US Patent Application No. 13/014,552 by Symantec Corp. 2010
- Kent Griffen, Xin Hu, Tzi-cker Chiueh,and Scott Schneider, "**Systems and Methods for Library Function Identification in Automatic Malware Signature Generation**", US Patent Application, Applied by Symantec Corp., 2009
- Abhijit Bose, Xin Hu, Kang G. Shin and Taejoon Park, "**Method and Apparatus For Repairing Computer System Infected By Malware**", US Patent Application No. 20090031162, Applied by Samsung Electronics, 2007
- Abhijit Bose, Xin Hu, Kang G. Shin and Taejoon Park, "**Method and Apparatus for Modeling Computer Program Behaviour for Behaviorial Detection of Malicious Program**", US Patent Application No. 20090019546, Applied by Samsung Electronics, 2007

PROFESSIONAL SERVICES

- Program Committee and reviewers for 1st IEEE SECON 2012 Workshop on Vehicular Communications, Sensing and Computing
- Reviewer for Journals:
  - IEEE/ACM Transactions on Networking
  - IEEE Transactions on Parallel and Distributed Systems
  - IEEE Transactions on Dependable and Secure Computing

- IEEE Transactions on Vehicular Technology
- The International Journal of Sensor Networks
- The International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)
- The International Journal for the Computer and Telecommunications Industry
- ACM Transactions on Information and System Security

- Reviewer of best paper award of CSAW (CyberSecurity Awareness Week) 2012
- External reviewer for IEEE INFOCOM'09, ACM MobiCom'08.

EXPERIENCE

10/2011 – present **IBM T.J Watson Research Center** Yorktown Heights, NY
Research Scientist

- Develop innovative methods for Predictive HTTP analytics based on URL requests, responses and web content
- Work with teammembers to
- Create new methods for evaluating reputation and risks of internal systems for IBM North data
- Implement cybersecurity assets monitoring and detection systems in Streams 2 platform and transfer it to Haifa research Lab
- Lead the design of innovative methods for mobile devices identification and risk evaluation

05/2006 – 09/2011 **RTCL Lab, University of Michigan** Ann Arbor, MI
Research Assistant

- Initiated and led the RB-Seeker project, designing and developing an automatic detection system for redirection botnets by correlating a variety of data sources
- Build a global DNS monitoring system and analyze botnet's IP-usage patterns
- Created a behavioral malware detection system on mobile handsets
- Investigated the effectiveness of using per-process rate limiting in containing various Internet worms
- Implemented a smart camera system for conference rooms. The project won the Windows CE Programming Contest
- Enhanced the security of time synchronization protocols of sensor networks by adding attack-tolerant features into the protocols
- Analyzed the IP prefix hijacking attack and developed a real-time detection system for it

05/2010 - 08/2010 **Symantec Research Lab, Symantec Corporation** Los Angeles, CA
Research Intern

- Designed a scalable framework for automatic malware clustering and label generation, which helps backend analysis teams more efficiently process new malware and significantly reduces the number of unlabeled samples

05/2008 - 12/2008 **Symantec Research Lab, Symantec Corporation** Los Angeles, CA
Research Intern

- Participated in the Hancock project, designing algorithms for reverse-engineering malware and automatic generating string signatures
- Leveraged instruction-level information to considerably reduce false positive rate in the automatically generated anti-virus signatures
- Led the SMIT project and developed efficient algorithms for indexing very large malware database based on call graphs

REFERENCES

Prof. Kang G. Shin
University of Michigan, Ann Arbor
EECS Computer Science Division
2260 Hayward St.
Ann Arbor, MI 48109-2121
(734) 763-0391 (voice)
(734) 763-8094 (fax)
kgshin@eecs.umich.edu

Prof. Tzi-cker Chiueh
Stony Brook University
Computer Science Department
1419 Computer Science
Stony Brook, NY 11794-4400
(631) 632-8449 (voice)
(631) 632-8334 (fax)
tcchiueh@gmail.com

Dr. Kent Griffin
Director, Symantec Research Labs
Symantec Corporation
900 Corporate Pointe
Culver City, CA 90230
(424) 750-7493 (Office)
(424) 750-7001 (Fax)
Kent_Griffin@symantec.com

Dr. Reiner Sailer
RSM and Manager
IBM T.J Watson Research Lab
1101 Kitchawan Rd
Yorktown Heights, NY 10598
(914)784-6280
sailer@us.ibm.com