Jiangshan Yu (Ph.D Candidate)

CONTACT INFORMATION

Room 125
School of Computer Science
University of Birmingham
Edgbaston
Birmingham
B15 2TT
United Kingdom

Mobile:
+44 7784-692-854
E-mail:
jiangshan.yu@me.com
Home-page:
www.jiangshanyu.com

RESEARCH INTERESTS

His research interests are in **security and privacy**. In particular, the focus of his research has been on secure authentication, public key infrastructure (PKI), key and certificate management, and email security.

APPLICATION AREAS

His research can be applied to the system (e.g. Internet Banking System, Cloud service system) which requires

- secure authentication of users and/or servers;
- secure communication between parties;
- ability of anti-hacking;
- secure data transmission; and
- secure data storage.

EDUCATION

University of Birmingham, Birmingham, West Midlands, UK

Ph.D, Computer Science, Oct.2012-Oct.2015 (Expected)

- Thesis Topic: *Secure the Internet – Cryptographic key management*
- Supervisor: Prof. Mark Ryan
- Area of Study: Computer and Network Security.

University of Wollongong, Wollongong, NSW, Australia

M.Phil, Computer Science and Software Engineering, Jul.2011-Jul.2012

- Thesis Topic: *Remote User Authentication in Distributed Systems and Networks*
- Supervisor: Dr. Guilin Wang, and Prof. Yi Mu
- Area of Study: Cryptography; Computer and Network Security.

M.Sc., Computer Science and Software Engineering, Jul.2010-Jul.2011

- Area of Study: Computer and Network Security; Software Engineering.
- Average Score: 67%.

English for Tertiary Studies, UOW COLLEGE, Feb.2010-Jun.2011

Northeast Agricultural University, Harbin, China

B.Eng., Computer Science and Technology, Sep.2005-Jul.2009

- Thesis Topic: *The Design and Implementation of Secure Internet Forum*
- Area of Study: Computer Science and Technology.
- Average Score: 82.3% (**Top 1** of the school).
- **Best Thesis Award, With Honors in Engineering**

COMPUTER SKILLS

Intermediate: Python, Emacs, LaTeX, OpenSSL, OTR supported tools, SSH, OpenPGP, Tor, etc., and skills for hacking, data encryption, PKI management and secure communication, etc..

Basic: Wireshark, Subversion Control (SVN), git, HTML, Matlab, C, JAVA, Vim, Virtual Machines, etc.

PUBLICATIONS

Journal publications

[1] Guilin Wang, Jiangshan Yu, and Qi Xie, "Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks", *IEEE Transactions on Industrial Informatics* (impact factor = 8.785, h5-index = 46), Vol.9, No.1, pp.294-302, 2013.

[2] Jiangshan Yu, Guilin Wang, Yi Mu, and Wei Gao, "An Efficient and Improved Generic Framework for Three-Factor Authentication with Provably Secure Instantiation', *IEEE Transactions on Information Forensics and Security (TIFS)* (impact factor = 2.065, h5-index = 47), accepted, 2014.

Conference Publications

[3] Jiangshan Yu, Guilin Wang, and Yi Mu, "Provably Secure Sing Sign-on Scheme in Distributed Systems and Networks", *IEEE TrustCom 2012*, pp. 271-278, 2012.

Submitted Papers

[4] Jiangshan Yu, Vincent Cheval, Mark Ryan, "DTKI: A New Formalized PKI with No Trusted Parties", submitted to *Network and Distributed System Security Symposium* (NDSS,2015).

HONORS AND AWARDS

- **First place award**, the Coniston poster competition, University of Birmingham, UK, 2014.
- **Scholarship** from EPSRC, Funding for PhD studies at University of Birmingham, 2012 - 2015.
- **Scholarship** from University of Birmingham, Overseas top up scholarship for PhD studies, 2012 - 2015.
- **Outstanding Graduates of Heilongjiang Province**, Heilongjiang, China, 2009;
- **Outstanding Graduates of Northeast Agricultural University**, Harbin, Heilongjiang, China, 2009;
- **Best Undergraduate Thesis Award**, Northeast Agricultural University, Harbin, Heilongjiang, China, 2009;
- **Outstanding Academic Award**, The Northeast Agricultural University, China, 2008;
- **First class scholarship**, Northeast Agricultural University, Harbin, Heilongjiang, China, 2006, 2007, 2008;
- **First National Prize** of China Contemporary Undergraduate Mathematical Contest in Modeling, China, 2007;

- **Second National Prize** of China Contemporary Undergraduate Mathematical Contest in Modeling, China, 2006;
- **Outstanding Student Award** of The Northeast Agricultural University, China, 2006;
- **Outstanding Student Leadership Award**, The Northeast Agricultural University, China, 2006;

PROFESSIONAL ACTIVITIES

Invited Reviewer (Journal):

- *IEEE Transactions on Information Forensics & Security*;
- *The Computer Journal*;
- *Journal of Information Security and Applications*.

Invited Reviewer (Conference):

- *ACISP 2013*; *ESORICS 2013*; *DPM 2013*; *ACNS 2014*; *SEC 2014*; *FMS 2014*; *WPES 2014* .

OTHER PERSONAL ACTIVITIES

President, Endless Martial Arts Association, Wollongong, NSW, Australia.
Manager, Department of Student Service, Wollongong Chinese Students & Scholars Association, Wollongong, NSW, Australia.