Dr. Jiangshan Yu (B.Eng, MSc, MPhil, PhD)

Contact Information

E02 0245-280,
Maison du Nombre,
University of Luxembourg,
6, Avenue de la Fonte
L-4364, Esch-sur-Alzette,
Luxembourg.

E-mail:
j.yu.research@gmail.com

Home-page:
www.jiangshanyu.com

Education

Ph.D in Cyber Security (2012-2016). **University of Birmingham**, UK.
Thesis: *Mitigating private key compromise*.

M.Phil in Cryptography (2011-2012). **University of Wollongong**, Australia.
Thesis: *Remote User Authentication in Distributed Systems and Networks*.

M.Sc. in Information Security (2010-2011). **University of Wollongong**, Australia.

B.Eng. in Computer Science and Technology (2005-2009), **Northeast Agricultural University**, Harbin, China. (**Top 1 out of 82, Best Thesis Award**).

Positions

Research fellow, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg. (2016-Present)

Honorary research fellow, University of Birmingham, UK. (2016-Present)

Director, CloudTomo Limited, UK. (2014-Present)

Tech consultant, Jin Xin Tong Trust and Investment Corporation Ltd, UK. (2014-2015)

President, Endless Martial Arts Association, Wollongong, Australia. (2011-2012)

Manager, Department of Student Service, Wollongong Chinese Students & Scholars Association, Wollongong, NSW, Australia.(2010-2012)

Selected projects:

Co-leader. *Huawei SoC Secure Boot Solution*, UK, 2016. (Funded by Huawei Ltd.)

Project leader. *Technological aspects of the Internet of Things.*, UK, 2016. (Funded by Law School, University of Birmingham.)

Project leader. *Innovate UK project on user-friendly security and privacy to increase confidence in cloud-based systems*, UK, 2015. (Funded by Innovate UK.)

Grant:

“Investigating scalable blockchains”, 10,000 (Euro) from The University of Luxembourg, 2016.
“Technology inspired feasibility study for secure email and cloud storage”, 33,000 (GBP) from Technology Strategy Board (Innovate UK), 2015.

Professional Activities:

(Finalist) RAEng Enterprise Fellowship, Royal Academy of Engineering, UK. 2015.

Chair, *The future of digital currency and block chain technology workshop*, Birmingham, UK. September, 2015.

PC member, *Software Architecture for Big Data and the Cloud*, 2016.

PATENTS

Key Usage Detection (Patent pending)

- UK Patent Application GB 1416188.9
- US Patent Application US 14/852,342

AWARDS

Honor:

- **Chinese Government Award For Outstanding PhD Scholar Abroad**, 2016. (Success rate: 1% worldwide.)
- **First place award**, the Coniston poster competition, University of Birmingham, UK, 2014.
- **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 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.

Scholarships:

- Universitas 21 scholarship from the University of Birmingham, 2015.
- EPSRC project funding for PhD studies at University of Birmingham, 2012 - 2015.
- Overseas top-up scholarship from the University of Birmingham for PhD studies, 2012 - 2015.
- First class scholarship, Northeast Agricultural University, Harbin, Heilongjiang, China, 2006, 2007, and 2008.

Publications

Book Chapter

[1] Jiangshan Yu and Mark Ryan. “Evaluating web PKIs”, *Software Architecture for Big Data and the Cloud*, 1st Edition, Chapter 7, 2016.

Journal publications

[2] Jiangshan Yu, Mark Ryan, and Cas Cremers. “DECIM: Detecting Endpoint Compromise In Messaging’, *IEEE Transactions on Information Forensics and Security (IEEE TIFS)*, 2017. (To appear)

[3] Jiangshan Yu, Vincent Cheval, and Mark Ryan. “DTKI: a new formalized PKI with verifiable trusted parties ”, *The Computer Journal*, Vol. 59 No. 11, pp. 1695-1713, 2016.

[4] 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)*, Vol.9, No.12, pp. 2302-2313, 2014.

[5] Guilin Wang, Jiangshan Yu, and Qi Xie, “Security analysis of a single sign-on mechanism for distributed computer networks”, *IEEE Transactions on Industrial Informatics (IEEE TII)*, Vol.9, No.1, pp.294-302, 2013.

Conference Publications

[6] Kevin Milner, Cas Cremers, Jiangshan Yu, Mark Ryan. ”Automatically Detecting the Misuse of Secrets: Foundations, Design Principles, and Applications”. *IEEE Computer Security Foundations Symposium (IEEE CSF)*, 2017. (To appear)

[7] Jiangshan Yu, Mark Ryan and Liqun Chen. “Authenticating compromisable storage systems”, *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE Trustcom)*, 2017. (To appear)

[8] Marcus Vlp, Francisco Rocha, Jrmie Decouchant, Jiangshan Yu and Paulo Verissimo. “Permanent Reencryption: How to Survive Generations of Cryptanalysts to Come”. *Security Protocols XXV*, 2017. (To appear)

[9] Jiangshan Yu and Mark Ryan. “Device attacker models: fact and fiction”, *Security Protocols XXIII*, pp. 158-167, 2015, Cambridge, UK.

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