Jiangshan Yu (BE, MSc, MPhil, PhD 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

My research interests are in **cyber security and user privacy**. In particular, the focus of my research has been on applied crypto, protocol design and verification, secure authentication, key management, public key certificate security, email security, and secure cloud storage. I'm also interested in the IoT security.

EDUCATION

University of Birmingham, Birmingham, West Midlands, UK

Ph.D, Computer Science, Oct.2012-March.2016 (Expected)

- Thesis Topic: *Protection against private key compromise*
- Supervisor: Prof. Mark Ryan
- Area of Study: Computer and Network Security.
- Short summary: Available on page 5.

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.
- Short summary: Available on page 6.

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 out of 82** of the school).
- **Best Thesis Award, With Honors in Engineering**

POSITIONS

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

Director, CloudTomo Limited, UK. (2014-present)
(A technology company producing IT security solutions.)

My work so far mainly includes seeking and applying for grants, analysing markets, finding and interviewing programmers, leading projects, developing operating plans and business plans, and meeting and negotiating with sponsors and potential cooperators.

Manager, Jin Xin Tong Trust and Investment Corporation Ltd, UK. (2014-2015)
(A Chinese investment company.)

My work is to discover green-tech academic inventions for the company to invest. This involves meeting and networking with people, and discussing the potential cooperation. We are setting up the fourth round of a negotiation on a project concerning seawater purification.

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

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

President, Guild of Students, Northeast Agricultural University. (2007-2009)

PROFESSIONAL ACTIVITIES:

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

Project manager. *Innovate UK project on user-friendly security and privacy to increase confidence in cloud-based systems*, UK.June - September, 2015.

Invited Reviewer (Journal):

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

Invited Reviewer (Conference):

- *ACISP 2013*; *ESORICS 2013*; *DPM 2013*; *ACNS 2014*; *SEC 2014*; *FMS 2014*; *WPES 2014*; *POST (ETAPS) 2015*; *ASIACCS 2015*; *IFIP SEC 2015*; *IEEE Euro S&P 2016*.

PATENTS

Key Usage Detection (Patent pending)

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

AWARDS

Grant:

- "Technology inspired feasibility study (ICT)", GBP33,000 from Technology Strategy Board (Innovate UK), 2015.

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.

Other:

- **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.

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), Vol.9, No.12 , pp. 2302-2313, Dec. 2014. DOI: 10.1109/TIFS.2014.2362979.

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.

[4] Jiangshan Yu and Mark Ryan, "Device attacker models: fact and fiction", Security Protocols XXIII, pp. 158–167, 2015.

Other drafts

[5] Jiangshan Yu, Vincent Cheval, Mark Ryan, “DTKI: a new formalized PKI with verifiable trusted parties”. (Under 2nd round review by The Computer Journal).

[6] Jiangshan Yu, Mark Ryan, and Cas Cremers. ”How to detect unauthorised usage of a key”. IACR Cryptology ePrint Archive 2015: 486, 2015.

[7] Jiangshan Yu and Mark Ryan. ”Evaluating web PKIs”.. (Submitted to “Software Architecture for Big Data and the Cloud” as a book chapter.)

[8] Jiangshan Yu, Guilin Wang, and Yi Mu. ”Efficient and provably secure single sign-on schemes in distributed systems and networks”. (To be submitted.)

[9] Jiangshan Yu, Mark Ryan, and Liqun Chen. “Security in periodically compromised cloud storage”. (Work in progress.)

[10] Jiangshan Yu, Mihai Ordean, Mark Ryan. “A practical gossip protocol”. (Work in progress.)

TALKS

- A Generic Framework for Three-Factor Authentication, Security Seminar, University of Birmingham, Birmingham, March, 2013.
- DTKI: Distributed Transparent Key Infrastructure
  - Google Certificate Transparency Hack Day, Google, London, August, 2013.
  - Foundations of Security Analysis and Design (FOSAD), Italy, September, 2013.
  - The 3rd International CryptoForma workshop at ESORICS, London, September 2013.
  - Cloud Technologies and Trust Domains (CTTD) 2013, HP Labs Bristol, UK;
  - HotSpot Workshop at ETAPS2014, Grenoble, France.
- Device attacker models: fact and fiction
  - Security Seminar, University of Birmingham, Birmingham, Oct, 2014.
  - Twenty-third International Workshop on Security Protocols, Cambridge, UK, April, 2015.
- Key usage detection
  - Security Seminar, University of Birmingham, Birmingham, March, 2015.
- Security in periodically compromised cloud storage
  - CryptoForma, University of Strathclyde, Glasgow, UK, Oct. 2015..

TRAINING

1. Midlands Graduate School: Mathematical Foundations of Computing Science(MGS2013), one week coursework, Leicester, UK. 2013.
2. 13th International School on Foundations of Security Analysis and Design (FOSAD2013), University Residential Center of Bertinoro, Italy, 2013.
3. Leading Academic, University of Birmingham, Birmingham, UK. 2013.

4. Intensive Programme on Information & Communication Security, Lesvos island, Greece, 2014;
5. Commercialisation Training (by EPSRC, Strategy in motion, and BizzInn), Birmingham, UK. 2015.
6. How to commercialise Your Own Research and Develop Economic Impact, Birmingham, UK. 2015
7. Partnerships for Success: Human Security and Research Impact Conference, organised by The Partnership for Conflict, Crime and Security Research (PaCCS), London, UK. 2015.
8. Pitch training, organised by Innovate UK, London, UK. 2015.
9. International Summer School on Information Security, Bilbao, Spain. 2015
10. 15th International School on Foundations of Security Analysisand Design (FOSAD2015), University Residential Center of Bertinoro, Italy, 2015.

COMPUTER SKILLS

Intermediate: Python, Emacs, LaTeX, OpenSSL, 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, etc.

SUMMARY OF THESIS

PhD Thesis

Security systems relies on the assumption that the computer end-points can securely store and use cryptographic keys. Yet, this assumption is rather hard to justify in practice. New software vulnerabilities are discovered every day, and malware is pervasive on mobile devices and desktop PCs.

This thesis provides research on how to secure a system even when secret keys are compromised by attackers, in three different cases. The first case considers compromised signing keys of certificate authorities in public key infrastructure. To address this problem, this thesis first provides a critical analysis on existing prominent certificate management systems, then proposes a new system called “Distributed and Transparent Key Infrastructure (DTKI)”, based on Google’s certificate transparency project, to make all certificate issuance and revocation transparent. DTKI prevents attacks that use fake certificates, provides a way to manage certificate revocation, verifies the behaviour of trusted parties, and is secure even if all service providers collude together. A formalisation of the system, and formal machine-checked verification of its core security property using the Tamarin prover are also provided.

The second case considers the key compromise in secure communications. If a device is compromised by exploiting software vulnerabilities, and is then made secure again, the attacker remains in possession of secrets (such as keys) he obtained during the compromise. Since victims do not know when compromises take place, they are not motivated to revoke their keys. In practice, it is impractical to ask users to revoke their keys and distribute new ones after every security update. We develop messaging protocols that allow users to detect if their long-term keys have been compromised and are being used by an attacker. Our proposal not only detects situations in which the adversary has copied a key and uses it, but also situations in which he has access to a key but is not able to copy it (for example, if it is protected in a TPM). We also provided a formal machine-checked verification to prove its core security property.

The third case considers the key compromise in secret sharing with applications in secure cloud storage. Secret sharing schemes allow a user to split a secret into shares, so that each share is held by a server. Then, when the user wants to retrieve the secret, the servers can combine their shares to recover the data. Unfortunately, if the servers become compromised (say by malware) one by one over a long period, an attacker could accumulate all the shares and hence reconstruct the secret. We develop a provably secure secret sharing scheme by using Bilinear parings. It works even if all the servers are compromised during the storage of the secret. We assume that the server owners periodically detect compromises and patch the servers to make them secure after such an incident. Thus, in different time periods, different subsets of the servers will be compromised. We prove that our protocol satisfies the following property: if in every time period the number of compromised servers is less than a threshold number servers, then the secret remains secure.

MPhil Thesis

This thesis provides efficient and secure authentication protocols for distributed systems and networks. In particular, this thesis presents my research on both single sign-on (SSO) systems and three-factor authentication systems. The thesis first provides a security analysis with two attacks on a supposed secure SSO scheme (proposed in 2012). In the first attack, a malicious service provider who has communicated with a user twice can recover the users credential. The other attack may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services. The thesis then formalises the security model, and proposes two provably secure SSO systems based on verifiable encryption of RSA signature (RSA-VES), and on Schnorr identification scheme, respectively. The last work presented in the thesis is an efficient generic framework for generating a secure three-factor authentication scheme from any secure two-factor authentication scheme, with a provably secure instantiation.