Ph.D. Candidate, School of EECS
Peking University, Beijing 100871, China

Ding Wang

Curriculum Vitae

"Cenius is one percent inspiration and ninety - nine percent perspiration!" - Thomas A. Edison

Research Interests

My research interests include **Password Cryptography** and **Provable Security**.

Academic Achievements

Since 2012, as the first author I have published more than 20 referred research papers at journals like IEEE TDSC and IEEE TIFS, and conferences like ACM CCS'16, ACN AsiaCCS'16, IEEE DSN'16, ESORICS'15, SecureComm 2014, ISC 2013, DBSec 2012, ICICS 2012. My works have 500+ Google Scholar citations. I have served as PC member for 10+ security conferences such as ACM AuthTech'16 and IEEE TrustCom'16, and have been reviewers for 40+ journals/confernces.

Education

2013–Present **Ph.D. Candidate in Information Security** , *School of Electronics Engineering and Computer Science, Peking University*, Beijing 100871, China, Advisor: Prof. Ping Wang.

2010–2013 **Masters of Information Security** , *Harbin Engineering University*, Harbin 150001, China, Advisor: Prof. Chunguang Ma.

2008–2009 **Bachelor of Information Security Engineering**, *Information Engineering University*, Zhengzhou 450001, China.

2004–2008 **Bachelor of Information Security**, *Nankai University*, Tianjing 300071, China.

Masters Thesis

Title *Research on Password-based Remote User Authentication Schemes Using Smart-cards*

Supervisors Professor Chunguan Ma

Description This thesis investigated how to design a two-factor authentication scheme that provides "truly two-factor security" even if the smart cards can be tampered when lost, and solved one important open problem in this area. It has been awarded the **The Excellent Master Thesis Prize of Harbin Engineering University**.

Awards

2016 My paper selected as "ESI Hot Paper" (top 0.1%) by Thomson Reuters

2016 Top-10 Distinguished Academic Fellow Award (first place), EECS of Peking University

2015 Annual Graduate Scholarship of the National Key Laboratory of Information Security (10 Phd. recipients in China);

2015 Annual Innovation Award of Peking University

2015 My paper selected as "ESI Highly Cited Paper" (top 1%) by Thomson Reuters

2014 Graduate Scholarship for Outstanding Academic Innovations of Peking University

(+86) 185 1134 5776 • wangdingg@yeah.net
http://wangdingg.weebly.com/

2013 Outstanding Reviewer Award from Elsevier

2013 Excellent Master Thesis of the University (the only one awarded in our CS college)

2012 Top-Ten Distinguished Graduate Academic Star of Harbin Engineering University

2011 Outstanding graduate cadre of Harbin Engineering University

2009 First prize in "software design competition" of Information Engineering University

2009 Outstanding graduate student of Information Engineering University

2009 Top 50 in the first "Zhong-Ke Cup" National software design contest

2008 First-class National assistant scholarship, Triple-A student

PUBLICATIONS

1. **Ding Wang**, Zijian Zhang, Ping Wang, Jeff Yan, Xinyi Huang. Targeted Online Password Guessing: An Underestimated Threat. *Proc. of the 23nd ACM Conference on Computer and Communications Security (**ACM CCS 2016**)*, pp. 1-13. `http://bit.ly/2b8djJr`

2. **Ding Wang**, Ping Wang. fuzzyPSM: A New Password Strength Meter Using Fuzzy Probabilistic Context-Free Grammars. *Proc. of the 46th IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN 2016**)*, pp. 695-606.

3. **Ding Wang**, Ping Wang. Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound. *IEEE Transactions on Dependable and Secure Computing*, 2016, Minor revision. `http://bit.ly/2aYDrsB`

4. **Ding Wang**, Gaopeng Jian, Xinyi Huang, Ping Wang. Zipf's Law in Passwords. *IEEE Transactions on Information Forensics and Security*, 2016, to appear, `http://bit.ly/2b2DkcT`

5. **Ding Wang**, Qianchen Gu, Haibo Cheng, Ping Wang. The Request for Better Measurement: A Comparative Evaluation of Two-Factor Authentication Schemes. *Proc. of the 11th ACM Asia Conference on Computer and Communications Security (**AISACCS 2016**)*, pp. 475-486.

6. **Ding Wang**, Haibo Cheng, Debiao He, Ping Wang. On the Challenges in Designing Identity-based Privacy-Preserving Authentication Schemes for Mobile Devices. *IEEE Systems Journal*, 2016, Doi: `http://dx.doi.org/10.1109/JSYST.2016.2585681`

7. **Ding Wang**, Ping Wang. The Emperor's New Password Creation Policies. *Proc. of the 20th European Symposium on Research in Computer Security (**ESORICS 2015**)*,LNCS 9237, Springer, pp. 456–477.

8. **Ding Wang**, Nan Wang, Ping Wang, Sihan Qing. Preserving Privacy for Free: Efficient and Provably Secure Two-Factor Authentication Scheme with User Anonymity. *Information Sciences*, 2015, volume 321, pp.162–178. Doi: `http://dx.doi.org/10.1016/j.ins.2015.03.070`

9. **Ding Wang**, Ping Wang. On the Anonymity of Two-Factor Authentication Schemes for Wireless Sensor Networks: Attacks, Principle and Solutions. *Computer Networks*, 2014(73): 41–57. Doi: `http://dx.doi.org/10.1016/j.comnet.2014.07.010`

10. **Ding Wang**, Ping Wang. On the Usability of Two-Factor Authentication. *Proceedings of 10th International Conference on Security and Privacy in Communication Networks (**SecureComm 2014**)*, September 24–26, 2014, Beijing, China.

11. **Ding Wang**, Ping Wang. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Ad Hoc Networks* (2014), `http://dx.doi.org/10.1016/j.adhoc.2014.03.003`

12. **Ding Wang**, Ping Wang, Jing Liu. Improved Privacy-Preserving Authentication Scheme for Roaming Service in Mobile Networks. *Proceedings of 15th IEEE Wireless Communications and Networking Conference (WCNC 2014)*, 2014, pp.3178–3183, IEEE. (Regular paper)

13. Debiao He, **Ding Wang**. Robust biometric-based user authentication scheme multi-server environment. *IEEE Systems Journal*, 2014, Doi: `http://dx.doi.org/10.1109/JSYST.2014.2301517`

14. **Ding Wang**, Ping Wang. Offline Dictionary Attack on Password Authentication Schemes using Smart Cards. *Proc. 16th Information Security Conference (**ISC 2013**)*, November 13-15, Dallas, Texas, USA. Lecture Notes in Computer Science, pp. 1–16, Springer-Verlag. Full version `http://eprint.iacr.org/2014/208.pdf` (Regular paper, acceptance rate 16/70=22.8%)

15. **Ding Wang**, Chunguang Ma. Cryptanalysis of a Remote User Authentication Scheme for Mobile Client-Server Environment With Provable Security based on ECC. *Information Fusion*, 2013, 41(4):498–503. Doi: `http://dx.doi.org/10.1016/j.inffus.2012.12.002`

16. Debiao He, **Ding Wang**, Shuhua Wu. Cryptanalysis and Improvement of a password-based remote user authentication scheme without smart cards. *Information Technology and Control*, 2013, 42(4):170–177. Doi: `http://dx.doi.org/10.5755/j01.itc.42.2.2554`

17. **Ding Wang**, Chunguang Ma. Cryptanalysis and security enhancement of a remote user authentication scheme. *Elsevier Journal of China Universities of Posts and Telecommunications*, 2012, 19(5): 104–114, Doi: `http://dx.doi.org/10.1016/S1005-8885(11)60307-5`

18. **Ding Wang**, Chunguang Ma, Qiming Zhang, Songdong Zhao. Secure Password-based Remote User Authentication Scheme against Smart Cards Loss attack. *Journal of Networks*, 2013, 8(1):148–155.

19. **Ding Wang**, Chunguang Ma, Sendong Zhao, Changli Zhou. Breaking a Robust Remote User-Authentication Scheme using Smart Cards. *Proceedings of the 9th IFIP International Conference on Network and Parallel Computing (IFIP NPC 2012)*, Gwangju, Korea, Sep 6-8, Lecture Notes in Computer Science, vol.7351, pp. 110–118. Berlin: Springer-Verlag, 2012. (Regular paper, acceptance rate: 38/136=27.7%)

20. **Ding Wang**, Chunguang Ma, Deli Gu, Zhenshan Cui. Cryptanalysis of Two Dynamic ID-based Remote User Authentication Schemes for Multi-Server Architecture. *Proceedings of the 6th International Conference on Network and System Security (NSS 2012)*, Wuyishan, China, Nov 21-23, Lecture Notes in Computer Science, Vol.7645, pp. 462–475. Berlin: Springer-Verlag, 2012. (acceptance rate: 39/173=22.5%, full paper)

21. **Ding Wang**, Chunguang Ma, Peng Wu. Secure password-based remote user authentication scheme with non-tamper resistant smart cards. *Proceedings of the 26th Annual IFIP Conference on Data and Applications Security and Privacy (IFIP **DBSec 2012**)*, Paris, France, July 13-16, Lecture Notes in Computer Science, vol.7371, pp.114–121. Berlin: Springer-Verlag, 2012 (Short paper, acceptance rate: 23/49=46.9%)

22. **Ding Wang**, Ying Mei, Chunguang Ma, Zhenshan Cui. Comments on an Advanced Dynamic ID-based Authentication Scheme for Cloud Computing. *Proceedings of International Conference on Web Information Systems and Mining (WISM 2012)*, Chengdu, China, Oct 26ÍC28, Lecture Notes in Computer Science, vol.7529, pp.246–253. Berlin: Springer-Verlag, 2012. (Regualr paper, acceptance rate: 87/418=20.8%)

23. **Ding Wang**, Chunguang Ma, Lan Shi, Yu-Heng Wang. On the Security of an Improved Password Authentication Scheme Based on ECC. *Proceedings of the Third International Conference Information Computing and Applications (ICICA 2012)*, Chende, China, Lecture Notes in

Computer Science, vol.7473, pp. 181–188. Berlin: Springer-Verlag, 2012. (Regualr paper, 100/1089=9.1%)

24. Chunguang Ma, **Ding Wang**, Sen-Dong Zhao. Security flaws in two improved remote user authentication schemes using smart cards. *International Journal of Communication Systems*, 2012, Doi: `http://dx.doi.org/10.1002/dac.2468`

25. Sendong Zhao, **Ding Wang**, Sicheng Zhao, et al.. Cookie-Proxy: A Solution to Prevent SSLStrip Attack. *The 14th International Conference on Information and Communications Security (ICICS 2012)*, Hongkong,China, Lecture Notes in Computer Science, vol. 7618, pp. 365–372. Berlin:Springer-Verlag, 2012. (Short paper, acceptance rate: 49/101=48.5%)

26. Chun-guang Ma, **Ding Wang**, Ping Zhao, et al.. A new dynamic ID-based remote user authentication scheme with forward secrecy. *Proceedings of the 14th Asia-Pacific Web Conference (APWeb 2012 Workshops)*, Kunming, China, April 11-13, Lecture Notes in Computer Science, vol. 7234, pp. 199–211. Berlin: Springer-Verlag, 2012. (Regualr paper, acceptance rate: 28/68=41.1%)

27. Chun-guang Ma, **Ding Wang**, Qi-ming Zhang. Cryptanalysis and Improvement of Sood et al.'s Dynamic ID-based Authentication Scheme. *Proceedings of the 8th International Conference on Distributed Computing andInternet Technology (ICDCIT 2012)*, Bhubaneswar, India, February 2-4, Lecture Notes in Computer Science, vol. 7154, pp. 141–152. Berlin: Springer-Verlag, 2012. (Regualr paper, acceptance rate: 17/89=19.1%)

Other papers in Chinese:

1. **Ding Wang**, Ping Wang, Ming Lei. Cryptanalysis and Improvement of Gateway-Oriented Password Authenticated Key Exchange Protocol based on RSA. Chinese Journal of Electronics, Accepted, 2014. Online version: `http://bit.ly/2bnsgYM`

2. **Ding Wang**, Ping Wang, Zengpeng Li, Chun-guang Ma. Provably secure RSA-based remote user authentication protocol using passwords. Chinese Journal of Systems Engineering–Theory & Practice, Accepted, 2014. Online version: `http://bit.ly/2bceeZw`

3. **Ding Wang**, Chun-guang Ma, Chen Wen, Chunfu Jia. Cryptanalysis and Improvement of a Remote User Authentication Scheme for Resource-limited Environment. Chinese Journal of Electronics & Information Technology, 2012, 34(10): 2520–2526. Online: `http://bit.ly/2b2DMaO`

4. **Ding Wang**, Feng Xue, Liping Wang, Chunguang Ma.Improved password-based key agreement scheme with perfect forward secrecy. Journal of Shandong University (Natural Science), 2012, 47(9): 19–25. Online version: `http://bit.ly/2b3AZjW`

5. **Ding Wang**, Chunguang Ma, Chen Wen, Chunfu Jia. Research of man-in-the-middle attack in robust security network. Chinese Journal of Computer Applications, 2012, 32(1): 42–45. Online version: `http://wangdingg.weebly.com/uploads/2/0/3/6/20366987/cjca2012.pdf`

6. **Ding Wang**, Chunguang Ma, Qi Zhang, Deli Gu. Attacks and Improvements on a Strong Password Authentication Scheme. Chinese Journal of Computer Science, 2012, 39(6): 72–76. Online version: `http://wangdingg.weebly.com/uploads/2/0/3/6/20366987/cjcs2012.pdf`