**CS 4920/5920 Research Paper List (22 papers)**

1. Genkin et al., Physical key extraction attacks on PCs, ACM CACM 2016
http://delivery.acm.org/10.1145/2860000/2851486/p70-genkin.pdf?ip=128.198.169.175&id=2851486&acc=ACTIVE%20SERVICE&key=B63ACEF81C6334F5%2EBE54B6F0117A5174%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=736744438&CFTOKEN=15511619&__acm__=1489027754_725a098a59e9c49cb3b9c69791d54ba9

2. Egele et al., An empirical study of cryptographic misuse in Android applications, ACM CCS 2013
https://cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

3. Chandron et al., Position based cryptography, CRYPTO 2009
http://web.cs.ucla.edu/~rafail/PUBLIC/102.pdf

4. Fischlin et al., Key confirmation in key exchange: a formal treatment and implications for TLS 1.3, IEEE S&P 2016
http://ieeexplore.ieee.org/document/7546517/

5. Kim et al., Lightweight source authentication and path validation, ACM Sigcomm 2014
https://www.scion-architecture.net/pdf/2014-OPT.pdf

6. Fett et al., A comprehensive formal security analysis of OAuth 2.0, ACM CCS 2016
https://infsec.uni-trier.de/people/publications/paper/FettKuestersSchmitz-CCS-2016.pdf

7. Dorre and Klebanov, Practical detection of entropy loss in pseudo-random number generators, ACM CCS 2016
https://formal.iti.kit.edu/~klebanov/pubs/ccs2016.pdf

8. Garrison et al., On the practicality of cryptographically enforcing dynamic access control policies in the cloud, IEEE S&P 2016
https://arxiv.org/pdf/1602.09069.pdf

9. Schneier et al., Surreptitiously Weakening Cryptographic Systems, *Cryptology ePrint Archive*, Report 2015
https://eprint.iacr.org/2015/097.pdf

10. Raj et al., fTPM: A Software-only Implementation of a TPM Chip, USENIX Security 2016
https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_raj.pdf

11. Svenda et al., The Million-Key Question – Investigating the Origins of RSA Public Keys, USENIX Security 2016
https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_svenda.pdf

12. Bojinov et al., Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks, USENIX Security 2012
https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final25.pdf

13. Heninger et al., Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, USENIX Security 2012
https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf

14. Kammerstetter et al., Efficient High-Speed WPA2 Brute Force Attacks using Scalable Low-Cost FPGA Clustering, CHES 2016
https://eprint.iacr.org/2016/547.pdf

15. Dimur et al., Memory-Efficient Algorithms for Finding Needles in Haystacks, CRYPTO 2016
https://eprint.iacr.org/2016/560.pdf

16. Derbez and Fouque, Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks, CRYPTO 2016
https://eprint.iacr.org/2016/579.pdf

17. Atwater and Hengartner, Shatter: Using Threshold Cryptography to Protect Single Users with Multiple Devices, ACM WiSec 2016
http://dl.acm.org/citation.cfm?id=2939932

18. Braga et al., Practical Evaluation of Static Analysis Tools for Cryptography: Benchmarking Method and Case Study, IEEE ISSRE 2017
https://www.computer.org/csdl/proceedings/issre/2017/0941/00/0941a170.pdf

19. Acar et al., Comparing the Usability of Cryptographic APIs, IEEE S&P 2017
https://saschafahl.de/papers/cryptoapis2017.pdf

20. Matsumoto and Reischuk, IKP: Turning a PKI Around with Decentralized Automated Incentives, IEEE S&P'17
https://www.ieee-security.org/TC/SP2017/papers/290.pdf

21. Nemec et al., The Return of Coopersmith's Attack: Practical Factorization of Widely Used RSA Moduli, ACM CCS 2017
https://acmccs.github.io/papers/p1631-nemecA.pdf

22. Kogan et al., T/Key: Second-Factor Authentication From Secure Hash Chains, ACM CCS 2017
https://arxiv.org/pdf/1708.08424.pdf