CS 5158/6058 Data Security and Privacy, Spring 2018
Final Project

Instructor: Dr. Boyang Wang

Final Paper Due Date: 04/23/2018 (Monday), 11:59pm.
Format: Please submit a pdf of your summary in Blackboard.
Total Points: 20 points
Note: This is a **group project**. You can form a group of 2 or 3.

1 Project Description

In this final project, you will study several research papers related to the area of data security and privacy and write a summary describing the technical problems addressed by each paper that you select. This is a group project, and you will need to form a group of 2 or 3.

- If you form a group of 2, then you need to select at least 2 papers, and your summary (including references) should be at least **3** pages;
- If you form a group of 3, then you need to select at least 3 papers, and your summary (including references) should be at least **5** pages.

A list of research papers are listed at the end of this project description.

Format: You should write your summary with LaTeX [1] using the latest ACM conference template. The ACM template can be found at [2]. Specifically, you should follow the template example in

```
./sample-sigconf.tex
./sample-sigconf.pdf
```

and use the following document class in your LaTeX file

```
\documentclass[sigconf]{acmart}
```

A ready-to-use package of this ACM template will be provided in Blackboard. In addition, you can also use Overleaf [3], which is a great online LaTeX editor for group projects. For the submission of your summary, each member should submit a copy of your summary with the names of all the members on it. This will help the instructor and the TA to record your grade of your final paper easily.

In addition to this summary, your group will also need to give a presentation based on **one** of the papers you select. The presentation will be about 10 to 15 minutes depending on the total number of groups (I will confirm this after the spring break). You can choose to present as a team together or select one of your members to present.

In order to finalize the schedule of your presentations, please submit a pdf with the names of your group members. The deadline to submit this pdf is 03/09/2018, Friday, 11:59pm. If you could not find a teammate yourself, please submit a pdf with your name on it and indicate you need a teammate. I will help you find a teammate.

Note: For online graduate students from Northrop Grumman, there will be no oral presentations, please submit a copy of your slides with your summary together in Blackboard (due date: 04/23/2018 Monday, 11:59pm).

2 Project Details

Your summary/presentation should include the following aspects:

- An introduction that describes the technical problem addressed in a paper
- System model
- Main technique approach in a paper and how the paper solves the technical problem
- Evaluation and experiment results
- A discussion on the importance of the problem, the adequacy of the proposed solution, and potential future research directions.

3 Evaluation

You final project will be evaluated based on your summary (**60%**) and presentation (**40%**). For online students from Northrop Grumman, the final project will be evaluated based on your summary (**60%**) and slides (**40%**)

4 A List of Papers

A set of suggested papers is listed below. Besides selecting the papers listed below, you can also select other papers in the area of data security and privacy from top conferences, such as ACM CCS, IEEE S&P, NDSS, USENIX Security, PETS (now called PoPETs), ACM ASIACCS, ACM CODASPY. Normally, pdfs of those papers can be obtained through UC library or Google Scholar.

Searchable Encryption

1. Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. "All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption." In USENIX Security. pp.707–720. 2016.
2. Dawn Song, David Wagner, and Adrian Perrig. "Practical Techniques for Searches on Encrypted Data." In Proc. of IEEE S&P'00, 2000.
3. Raluca Ada Popa, Catherine M.S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. "CryptDB: Protecting Confidentiality with Encrypted Query Processing." In Proc. of ACM SOSP'11, 2011
4. Raluca Ada Popa, Frank H. Li, and Nickolai Zeldovich. "An Ideal-Security Protocol for Order-Preserving Encoding." In Proc. of IEEE S&P'13, 2013.
5. M. Naveed, S. Kamara, and C. V. Wright. "Inference Attacks on Property-Preserving Encrypted Databases." In Proc. of ACM CCS'15, 2015
6. Mohammad Saiful Islam, Mehmet Kuzu, and Murat Kantarcioglu. "Access Pattern Disclosure on Searchable Encryption: Ramification, Attack and Mitigation." In Proc. of NDSS'12, 2012
7. Florian Kerschbaum. "Frequency-Hiding Order-Preserving Encryption." In Proc. of ACM CCS'15, 2015

Crypto Currency

1. Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system." www.bitcoin.org. 2008
2. M. Jakobsson and A. Juels. "Proofs of Work and Bread Pudding Protocols." In Communications and Multimedia Security (CMS). pp.258–272. 1999.
3. G. Dagher, B. Bunz, J. Bonneau, J. Clark, and D. Boneh, "Provisions: Privacy-preserving Proofs of Solvency for Bitcoin Exchanges," in ACM CCS'15, 2015.
4. Y. Kwon, D. Kim, Y. Son, E. Vasserman, Y. Kim, "Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin,", in ACM CCS'17, 2017.
5. M. Green and I. Miers, "Bolt: Anonymous Payment Channels for Decentralized Currencies," in ACM CCS'17, 2017.
6. F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. van Renesse. "REM: Resource-Efficient Mining for Blockchains." USENIX Security, 2017.
7. F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi. "Town Crier: An Authenticated Data Feed for Smart Contracts." ACM CCS, pp. 270-282, 2016.

8. I. Eyal, A. E. Gencer, E. G. Sirer, R. V. Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol." USENIX NSDI'16, 2016.

Differential Privacy

1. U. Erlingsson, V. Pihur, A. Korolova, "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response,", ACM CCS'14, 2014
2. Tianhao Wang, Jeremiah Blocki, Ninghui Li, Somesh Jha, "Locally Differentially Private Protocols for Frequency Estimation," USENIX Security, 2017

Provable Data Possession

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598610.
2. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in the Proceedings of ACM CCS 2009, 2009, pp. 213–222.
3. E. Stefanov, M. van Dijk, A. Oprea, and A. Juels. Iris: A Scalable Cloud File System with Efficient Integrity Checks. Annual Computer Security Applications Conference (ACSAC), pp. 229-238, 2012.
4. M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos. Hourglass Schemes: How to Prove That Cloud Files Are Encrypted. ACM Computer and Communications Security (ACM CCS), pp. 265-280, 2012.

Other Topics

1. H. Corrigan-Gibbs, D. Boneh, and D. Mazires, "Riposte: An Anonymous Messaging System Handling Millions of Users." IEEE Symposium on Security and Privacy 2015, pp. 321-338.
2. V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft. "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records." in Proceedings of IEEE Symposium on Security and Privacy 2013, pp. 334-348.
3. S. Heuser, B. Reaves, P. Kumar Pendyala, H. Carter, A. Dmitrienko, W. Enck, N. Kiyavash, A. Sadeghi, and P. Traynor. "Phonion: Practical Protection of Metadata in Telephony Networks," Proceedings on Privacy Enhancing Technologies (PoPETs), 2017.
4. N. Scaife, H. Carter, P. Traynor and K. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," In IEEE International Conference on Distributed Computing Systems (ICDCS), 2016.
5. C. Garman, M. Green, G. Kaptchuk, I. Miers, M. Rushanan. "Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage," In Usenix Security 2016.
6. M. Green, W. B. Ladd, I. Miers. "A Protocol for Privately Reporting Ad Impressions at Scale." In ACM CCS 2016.
7. D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thom, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Bguelin, P. Zimmermann. "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice." In ACM CCS 2015. 2015
8. Emil Stefanov, Marten van Dijk, Elaine Shi, Christopher Fletcher, Ling Ren, Xiangyao Yu, and Srinivas Devadas. "Path ORAM: An Extremely Simple Oblivious RAM Protocol." In Proc. of ACM CCS'13. pp.299–310, 2013.
9. R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. IEEE Symposium on Security and Privacy (S&P), pp. 481-498, 2015.
10. Z. Huang, E. Ayday, J.-P. Hubaux, J. Fellay, and A. Juels. "GenoGuard: Protecting Genomic Data against Brute-Force Attacks." IEEE Symposium on Security and Privacy (S&P), pp. 447-462, 2015.
11. Anh Pham, Italo Dacosta, Guillaume Endignoux, Juan Ramon Troncoso-Pastoriza, Kevin Huguenin, Jean-Pierre Hubaux, "ORide: A Privacy-Preserving yet Accountable Ride-Hailing Service," USENIX Security, 2017
12. Steven Englehardt, Jeffrey Han and Arvind Narayanan, "I never signed up for this! Privacy implications of email tracking," Proceedings on Privacy Enhancing Technologies (PoPETs), 2018.
13. Jesse Victors, Ming Li, and Xinwen Fu, "The Onion Name System: Tor-powered Decentralized DNS for Tor Onion Services," Proceedings on Privacy Enhancing Technologies (PoPETs), 2017.

References

1. `https://www.latex-project.org/`
2. `https://www.acm.org/publications/proceedings-template`
3. `https://www.overleaf.com/`