ACM CCS Sample Template 2019

Rahul Chatterjee
UW–Madison

ABSTRACT

Abstractly this is an ACM CCS Template. Keep it short and simple, highlight the main problem and give your punch line contributions. For example,

Setting up the ACM CCS template is non-trivial. This is a document to help you get started with ACM CCS template over Overleaf quickly. I also provide some macros in the `defs.tex` file, that can be helpful for new writers.

1 INTRODUCTION

Introduction to your project. Start from some common knowledge that most of the reader (in computer security) would have and then narrow down to the details of your project. Speak about why the project is important, and why the reader should care about it. Finally talk briefly about what are you have done (for final project), what you are planning to do (for proposal). Reader should get a good chunk of understanding about your project from this introduction section (Section 1). It's good to finish introduction section with a quick list of contributions.

1.1 For project proposal.

The sections mentioned here is just for reference. You are free to change them as you find suitable. In particular for proposal, some of the sections such as Section 4 might not make much sense. You can skip that.

2 BACKGROUND AND RELATED WORK

In Section 1 you talked about the project at a very high-level. This is the section from where you will start giving details. First with things that are already done, and familiarize the reader with background information they will need to understand you work.

Threat model. Often this section you will discuss the threat-model, but there is no strict consensus on that.

Here is how you cite papers. For example, we read papers in the class [3, 5]. And here is some random citation [1, 2, 6–8]

2.1 Overview of the design

And then just to showoff some LaTeXskills, here is a Tikz plot.

You refer to a figure in the following way. In Figure 1 we show some thing that is relevant for the Multisketch paper by Chatterjee et al. [4]. Add your bibliography to the bib.bib file. You can copy the Bibtex format citation from Google Scholar.

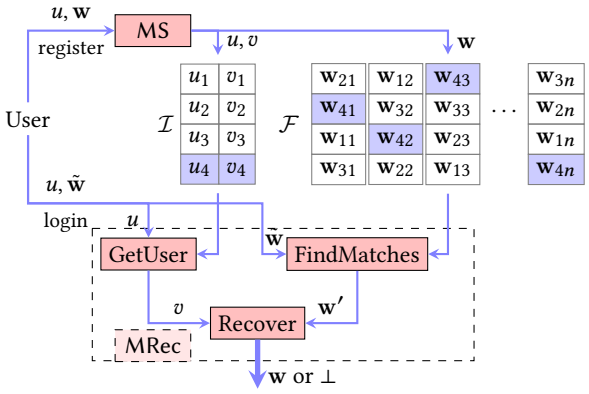

Figure 1: Diagram of multisketch as a part of an authentication service.

3 METHODOLOGY/DESIGN

Use this section describe the main contribution of your paper. If you are building something, describe the design of the system you built. If you are measuring something (like the world!) then include the measurement pipeline.

This is typically the largest section in your paper. (In case of measurement the result section might be bigger.)

Make sure you give enough details so that the reader is able to reproduce your work.

4 EVALUATION

The results section should have the results of your experiments and measurements. Evaluation is the most important part of the research. Sometime you might want to split it into more than one section depending on the type of the project.

Again make sure you give enough details so that the reader can reproduce your evaluation. Your GitHub code is not a replacement of the details, GitHub will perish, your paper will remain in this world for centuries to come. Of course, you need strike a balance between mundane details vs what makes your evaluation unique.

5 CONCLUSION

What is the big take away from your research. Include any limitations or future work here.

REFERENCES

[1] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. 2009. Format-preserving encryption. In *Selected Areas in Cryptography*. Springer Berlin Heidelberg, 295–312.

[2] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh. 2010. Kamouflage: Loss-resistant password management. In *ESORICS*. 286–302. http://dl.acm.org/citation.cfm?id=1888881.1888904

[3] Rahul Chatterjee, Anish Athalye, Devdatta Akhawe, Ari Juels, and Thomas Ristenpart. 2016. pASSWORD tYPOS and How to Correct Them Securely. *IEEE*

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Symposium on Security and Privacy (may 2016). Full version of the paper can be found at the authors' website.

[4] Rahul Chatterjee, M Sadegh Riazi, Tanmoy Chowdhury, Emanuela Marasco, Farinaz Koushanfar, and Ari Juels. 2019. Multisketches: Practical Secure Sketches Using Off-the-Shelf Biometric Matching Algorithms. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1171–1186.

[5] Y. Dodis, L. Reyzin, and A. Smith. 2004. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Eurocrypt 2004*, C. Cachin and J. Camenisch (Eds.). Springer-Verlag, 523–540. LNCS no. 3027.

[6] Adam Everspaugh, Rahul Chatterjee, Samuel Scott, Ari Juels, Thomas Ristenpart, and Cornell Tech. 2015. The Pythia PRF service. In *Proceedings of the 24th USENIX Conference on Security Symposium*. USENIX Association, 547–562.

[7] A. Juels. 2014. A bodyguard of lies: the use of honey objects in information security. In *SACMAT*. 1–4.

[8] S. Schechter, C. Herley, and M. Mitzenmacher. 2010. Popularity is everything: a new approach to protecting passwords from statistical-guessing attacks. In *USENIX HotSec*. 1–8. http://dl.acm.org/citation.cfm?id=1924931.1924935

A OVERFLOW FORM OTHER SECTIONS

Sometime you ware super excited about some details that does not quite fit with the rest of the paper goes here. For example, some details about how you instrumented the Android Linux kernel should go to appendix, and for really curious reader to read. Remember it's appendix, so the reader is not required to read, and you should not put critical information in appendix that is crucial for understanding the rest of the paper.