Week 2 Journal

Rodger Byrd

I. Process

For this Journal, I used Zotero to track all of my bibliography entries and notes. It was significantly faster and easier than what I did in Journal 1. For the "top" journal I chose IET Information Security [1]. It had 5 issues in 2019 with 10-12 articles per issue. My filed of study is related to both Compute Science and Computer Security so I thought this would include relevant papers for me to read. My process included 3 phases. First, quickly browse each paper using my phone as a stopwatch to determine if I wanted to scan or trash the paper with a note about why. Secondly, I did a 5-10 minute scan of the papers chosen in phase 1 to determine if I wanted to critically and creatively read them. Lastly, I chose the best 2 papers and read them tracking my notes. The notes are included in the next section.

II. Raw Notes

For my first detailed read I chose a paper called *Re-definable access control over outsourced data in cloud storage systems* [2].

The following are my raw notes for this paper. Authors propose RDAC as approach to secure outsourced data and allow access control. Interesting idea to take encrypted data and somehow conver that to another type of encrypted data that could be decrypted by authorized users based on different criteria than original encryptor. How does the IBE (identity based encryption) actually convert to ABE (attribute based encryption). Seems non-trivial. I can see how a company would use ABE or IBE/PKI, curious to see how they propose to convert from one to the other. conversion keys? Multiple pages on how great ABE and IBE are, but they are proposing RDAC (re-difinable access control). Use a bunch of set theory to define who should get access to what. Looks like a proxy server will decide whether to decrypt data out of IBE for approved users Even more detail on IBE and ABE in section 5.3. 6.1 Basic idea, just restate everying already talked about in detail, waste of a section. Looking back at the system architecture, it doesn't show hot the Trusted Authority would authorize the proxy do do the "re-encryption"? They are finally talking about a master secret key (msk). finally, section 6.2.4 File conversion. Still claiming that it doesn't need to be decrypted, just converted to another encryption, i'm not convinced, hopefully they built some actual system. Experimental section 8.2 included more information about performance of different encryption then the conversion process. I think this is more of a toy example. I'd like to see something more comphrensive then a few small tests on a mobile device and PC. Overall, dissapointed in this paper, although I can see how the concept is very relevant with so many companies outsourcing to the cloud. They could have done a better job explaining the implementation and doing performance testing.

The next paper I read in detail was

References

[1] "IET Information Security." [Online]. Available: https://digital-library.theiet.org/content/journals/iet-ifs

[2] Z. Zhang, C. Chang, Z. Guo, and P. Han, "Re-definable access control over outsourced data in cloud storage systems," *IET Information Security*, vol. 13, no. 3, pp. 258–268(10), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5365