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. The files for this latex document are in the github repository located at `https://github.com/rodger79/CS6000`.

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.

For my next detailed read I chose a paper called *Causal analysis of attacks against honeypots based on properties of countries* [3]. The following are my raw notes for this paper.

After setting up a honeypot, the authors looks at the demographic, technical, and economic data of the countries the attacks originated from. This could be interesting from a threat perspective, as-in can you use the country of request origination to determine relevant threat levels. They state they are attempting to clarify the relation between the number of attacks and their countries of origin. Set up a "honeynet", collection of 7 honeypots directly on the internet for 1 year. Big assumption that you can actually determine an attacker from their IP address, unclear how they actually determined this other than they say they used databases in 3.3. Oh, the databases weren't for location information they were for exonomic data/demographic data With VPNs and Tor, I seriously question whether any statistical analysis is even valid. A lot of sections on statistics. Seems like they just gathered a bunch of data then tried to write a paper after. Meaning come up with the hypothesis later. I wonder if you could do a second analysis overlaying where Tor is banned to see how that affects the countries of origin. For instance, they claim the Netherlands have an unusual amount of attacks coming from them, do they also have a lot of Tor nodes? I think the idea behind this paper is interesting, but they don't mention once about VPNs. Huge potential problem

Papers that were scanned and trashed are referenced in the bibliography below.

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

[3] M. Zuzk and P. Bujok, "Causal analysis of attacks against honeypots based on properties of countries," *IET Information Security*, vol. 13, no. 5, pp. 435–447(12), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5141

[4] Q. Li, R. Wang, and D. Xu, "Detection of double compression in HEVC videos based on TU size and quantised DCT coefficients," *IET Information Security*, vol. 13, no. 1, pp. 1–6(5), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0555

[5] N. Chakraborty and S. Mondal, "Towards incorporating honeywords in n-session recording attack resilient unaided authentication services," *IET Information Security*, vol. 13, no. 1, pp. 7–18(11), Jan. 2019.

[Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0538

[6] S. A. Musavi and M. R. Hashemi, "HPCgnature: a hardware-based application-level intrusion detection system," *IET Information Security*, vol. 13, no. 1, pp. 19–26(7), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0629

[7] R. Rivera, P. Kotzias, A. Sudhodanan, and J. Caballero, "Costly freeware: a systematic analysis of abuse in download portals," *IET Information Security*, vol. 13, no. 1, pp. 27–35(8), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0585

[8] M. J. Mihaljevi and F. Oggier, "Security evaluation and design elements for a class of randomised encryptions," *IET Information Security*, vol. 13, no. 1, pp. 36–47(11), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0271

[9] Y. Jia, M. Wang, and Y. Wang, "Network intrusion detection algorithm based on deep neural network," *IET Information Security*, vol. 13, no. 1, pp. 48–53(5), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5258

[10] B. Barari, P. K. Sangdeh, and B. Akhbari, "Secure degrees of freedom of two-user X-channel with synergistic alternating channel state information at transmitters," *IET Information Security*, vol. 13, no. 1, pp. 54–60(6), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5239

[11] C. Guo, P. Tian, and C.-C. Chang, "Privacy preserving weighted similarity search scheme for encrypted data," *IET Information Security*, vol. 13, no. 1, pp. 61–69(8), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5187

[12] R. Li and C. Jin, "Meet-in-the-middle attacks on round-reduced tweakable block cipher Deoxys-BC," *IET Information Security*, vol. 13, no. 1, pp. 70–75(5), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5091

[13] H. Lee, C. Pyo, and G. Lee, "Dynamic reencryption of return addresses," *IET Information Security*, vol. 13, no. 1, pp. 76–85(9), Jan. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5142

[14] W. Zhang and V. Rijmen, "Division cryptanalysis of block ciphers with a binary diffusion layer," *IET Information Security*, vol. 13, no. 2, pp. 87–95(8), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5151

[15] S. Jha, S. Sural, V. Atluri, and J. Vaidya, "Security analysis of ABAC under an administrative model," *IET Information Security*, vol. 13, no. 2, pp. 96–103(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5010

[16] H. Qin, R. Tso, and Y. Dai, "Quantum secret sharing by using Fourier transform on orbital angular momentum," *IET Information Security*, vol. 13, no. 2, pp. 104–108(4), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5149

[17] W. Han, J. Xue, and H. Yan, "Detecting anomalous traffic in the controlled network based on cross entropy and support vector machine," *IET Information Security*, vol. 13, no. 2, pp. 109–116(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5186

[18] Y. Wei, F. Yao, E. Pasalic, and A. Wang, "New second-order threshold implementation of AES," *IET Information Security*, vol. 13, no. 2, pp. 117–124(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5244

[19] Y. Zheng and W. Wu, "On the extension and security of key schedule of GOST," *IET Information Security*, vol. 13, no. 2, pp. 125–132(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5291

[20] A. Bhadane and S. B. Mane, "Detecting lateral spear phishing attacks in organisations," *IET Information Security*, vol. 13, no. 2, pp. 133–140(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5090

[21] J.-Z. Li and J. Guan, "Advanced conditional differential attack on Grain-like stream cipher and application on Grain v1," *IET Information Security*, vol. 13, no. 2, pp. 141–148(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5180

[22] X. Rongrong, Y. Xiaochun, and H. Zhiyu, "Framework for risk assessment in cyber situational awareness," *IET Information Security*, vol. 13, no. 2, pp. 149–156(7), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5189

[23] L. Shen, J. Ma, Y. Miao, and H. Liu, "Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model," *IET Information Security*, vol. 13, no. 3, pp. 167–173(6), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5226

[24] F. Zhang, Z. Ling, and S. Wang, "Unsupervised approach for detecting shilling attacks in collaborative recommender systems based on user rating behaviours," *IET Information Security*, vol. 13, no. 3, pp. 174–187(13), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5131

[25] T. R. Sree and S. M. S. Bhanu, "HAP: detection of HTTP flooding attacks in cloud using diffusion map and affinity propagation clustering," *IET Information Security*, vol. 13, no. 3, pp. 188–200(12), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5382

[26] S. Soltani, S. A. H. Seno, and H. S. Yazdi, "Event reconstruction using temporal pattern of file system modification," *IET Information Security*, vol. 13, no. 3, pp. 201–212(11), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5209

[27] G. A. Abdelmalek, R. Ziani, and R. Mokdad, "Security and fault tolerance evaluation of TMRQDI circuits," *IET Information Security*, vol. 13, no. 3, pp. 213–222(9), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5439

[28] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen, and R. U. Ashraf, "Multi-hop interpersonal trust assessment in vehicular *ad-hoc* networks using three-valued subjective logic," *IET Information Security*, vol. 13, no. 3, pp. 223–230(7), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5336

[29] A. Parihar and S. Nakhate, "Fast Montgomery modular multiplier for RivestShamirAdleman cryptosystem," *IET Information Security*, vol. 13, no. 3, pp. 231–238(7), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5191

[30] M. Uriarte, J. Astorga, E. Jacob, M. Huarte, and O. Lpez, "Impact assessment of policy expressiveness of an optimised access control model for smart sensors," *IET Information Security*, vol. 13, no. 3, pp. 239–248(9), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5204

[31] B. Unlu, "Base for algebraic cryptanalysis based on combined representation of S-box," *IET Information Security*, vol. 13, no. 3, pp. 249–257(8), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5051

[32] A. I. Aysan, F. Sakiz, and S. Sen, "Analysis of dynamic code updating in Android with security perspective," *IET Information Security*, vol. 13, no. 3, pp. 269–277(8), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5316

[33] M. Sheikhi-Garjan, M. Bahramian, and C. Doche, "Threshold verifiable multi-secret sharing based on elliptic curves and Chinese remainder theorem," *IET Information Security*, vol. 13, no. 3, pp. 278–284(6), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5174

[34] M. Yue, Z. Wu, and J. Wang, "Detecting LDoS attack bursts based on queue distribution," *IET Information Security*, vol. 13, no. 3, pp. 285–292(7), May 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5097

[35] M. A. Nia, B. Bahrak, M. Kargahi, and B. Fabian, "Detecting new generations of threats using attribute-based attack graphs," *IET Information Security*, vol. 13, no. 4, pp. 293–303(10), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5409

[36] M. Ouladj, P. Guillot, and F. Mokrane, "Chosen message strategy to improve the correlation power analysis," *IET Information Security*, vol. 13, no. 4, pp. 304–310(6), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5103

[37] S. Bag, M. A. Azad, and F. Hao, "PriVeto: a fully private two-round veto protocol," *IET Information Security*, vol. 13, no. 4, pp. 311–320(9), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5115

[38] J. A. Ruth, H. Sirmathi, and A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks," *IET Information Security*, vol. 13, no. 4, pp. 321–329(8), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5295

[39] X. Zhang, L.-P. Wang, and J. Xu, "Certifying multi-power RSA," *IET Information Security*, vol. 13, no. 4, pp. 330–335(5), Jul. 2019.

[Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5178

[40] M. Noroozi and Z. Eslami, "Public key authenticated encryption with keyword search: revisited," *IET Information Security*, vol. 13, no. 4, pp. 336–342(6), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5315

[41] M. H. Dehkordi and H. Oraei, "How to construct a verifiable multi-secret sharing scheme based on graded encoding schemes," *IET Information Security*, vol. 13, no. 4, pp. 343–351(8), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5306

[42] A. M. Vartouni, M. Teshnehlab, and S. S. Kashi, "Leveraging deep neural networks for anomaly-based web application firewall," *IET Information Security*, vol. 13, no. 4, pp. 352–361(9), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5404

[43] M. C. Pena, R. D. Daz, J.-C. Faugre, L. H. Encinas, and L. Perret, "Non-quantum cryptanalysis of the noisy version of AaronsonChristiano's quantum money scheme," *IET Information Security*, vol. 13, no. 4, pp. 362–366(4), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5307

[44] M. Tang and Q. Qian, "Dynamic API call sequence visualisation for malware classification," *IET Information Security*, vol. 13, no. 4, pp. 367–377(10), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5268

[45] D. Saha, S. Kakarla, and D. R. Chowdhury, "Dinamite: internal differential match-in-the-end attack on eight-round PAEQ," *IET Information Security*, vol. 13, no. 4, pp. 378–388(10), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5033

[46] Y. Zhao, S. Xu, and H. Chi, "Encrypted secure polar coding scheme for general two-way wiretap channel," *IET Information Security*, vol. 13, no. 4, pp. 393–403(10), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5472

[47] M. Baldi, F. Chiaraluce, J. Rosenthal, P. Santini, and D. Schipani, "Security of generalised ReedSolomon code-based cryptosystems," *IET Information Security*, vol. 13, no. 4, pp. 404–410(6), Jul. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5207

[48] L. Jiao, Y. Hao, and Y. Li, "Improved guess-and-determine attack on TRIVIUM," *IET Information Security*, vol. 13, no. 5, pp. 411–419(8), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5357

[49] J.-Y. Wang, S.-H. Lin, W. Cai, and J. Dai, "ESR analysis over ST-MRC multi-input multi-output Nakagami fading channels," *IET Information Security*, vol. 13, no. 5, pp. 420–425(5), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5185

[50] Y. Zhou, B. Yang, Y. Mu, T. Wang, and X. Wang, "Identity-based encryption resilient to continuous key leakage," *IET Information Security*, vol. 13, no. 5, pp. 426–434(8), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5203

[51] H. Arabnezhad-Khanoki, B. Sadeghiyan, and J. Pieprzyk, "S-boxes representation and efficiency of algebraic attack," *IET Information Security*, vol. 13, no. 5, pp. 448–458(10), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5201

[52] P. Rastegari, M. Dakhilalian, M. Berenjkoub, and W. Susilo, "Multi-designated verifiers signature schemes with threshold verifiability: generic pattern and a concrete scheme in the standard model," *IET Information Security*, vol. 13, no. 5, pp. 459–468(9), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5063

[53] H. Yan, X. Lai, L. Wang, Y. Yu, and Y. Xing, "New zero-sum distinguishers on full 24-round Keccak-f using the division property," *IET Information Security*, vol. 13, no. 5, pp. 469–478(9), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5263

[54] L.-C. Li, W.-L. Wu, L. Zhang, and Y.-F. Zheng, "New method to describe the differential distribution table for large S-boxes in MILP and its application," *IET Information Security*, vol. 13, no. 5, pp. 479–485(6), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5284

[55] M. Noferesti and R. Jalili, "Inline high-bandwidth network analysis using a robust stream clustering algorithm," *IET Information Security*, vol. 13, no. 5, pp. 486–495(9), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5287

[56] D. Nuez, I. Agudo, and J. Lopez, "Escrowed decryption protocols for lawful interception of encrypted data," *IET Information Security*, vol. 13, no. 5, pp. 498–507(9), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5082

[57] B. Bagherpour, A. Zaghian, and M. Sajadieh, "Sigma protocol for faster proof of simultaneous homomorphism relations," *IET Information Security*, vol. 13, no. 5, pp. 508–514(6), Sep. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5167

[58] Q. Zhang, J. Qiao, and Q. Meng, "Build a trusted storage system on a mobile phone," *IET Information Security*, vol. 13, no. 2, pp. 157–166(9), Mar. 2019. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2018.5031