CSE 707: Seminar on Wireless Networks Security – Principles and Practices

Presentation Schedule – Fall 2023

Last Name, First Name	Username	Group No.	Presentation Date	Topic
Jain, Sarthak	sjain34	6	10/4/2023	A.6
Putta, Sai Saran	vputta	6	10/4/2023	A.6
Karkera, Shrishti Lakshmesh	karkera	6	10/4/2023	A.6
Kajol, .	kajol	1	10/4/2023	B.10
Mehta, Aishwarya	amehta9	1	10/4/2023	B.10
Kondepati, Sai Abhilash	skondepa	10	10/11/2023	B.20
Nallamothu, Pavithra	pnallamo	10	10/11/2023	B.20
Lingabathina, Anurag	anuragli	9	10/11/2023	B.12
Nimbalkar, Rahul Pundalik	rahulpun	9	10/11/2023	B.12
Balusamy, Dhayaneshwar	dhayanes	7	10/18/2023	C.6
Murugiah, Sowmiya	sowmiyam	7	10/18/2023	C.6
Pachhipulusu, Ramya	ramyapac	4	10/18/2023	B.18
Srivastava, Shubhi	shubhisr	4	10/18/2023	B.18
Angeri, Jaswanth Reddy	jangeri	3	10/25/2023	D.2
Polamreddy, Gayeethri	gayeethr	3	10/25/2023	D.2
Banerjee, Namrata	banerje3	5	10/25/2023	B.9
Mondal, Sagnik	sagnikmo	5	10/25/2023	B.9
Arumalla, Sai Vineeth	sarumall	8	11/1/2023	C.1
Kulkarni, Rahul	rahulkul	8	11/1/2023	C.1
Penumuru, Pavithra	ppenumur	2	11/1/2023	B.1
Valavala, Nikhil	nvalaval	2	11/1/2023	B.1
Aggarwal, Rishab	rishabag	13	11/8/2023	B.17
Mittal, Mehul	mehulmit	13	11/8/2023	B.17
Basireddy, Ithihas Reddy	ithihasr	11	11/8/2023	A.7
Gandham, Jayadhar	jayadhar	11	11/8/2023	A.7
Kassyap Subramanian, Naren	nkassyap	12	11/15/2023	B.16
Rama Krishna Reddy, Yashwanth	ramakri4	12	11/15/2023	B.16

10/23/2023

Topics and Papers

(Already selected papers are highlighted)

A. Vehicular Networks Security and Machine Learning

1) Tamal Biswas, Ameya Sanzgiri and Shambhu Upadhyaya, "Building Long Term Trust in Vehicular Networks", *IEEE 83rd Vehicular Technology Conference (VTC)*, Nanjing, China, May 2016.
2) Felipe Boeira, Mikael Asplund, Marinho P. Barcellos, Mitigating Position Falsification Attacks in Vehicular Platooning, *2018 IEEE Vehicular Networking Conference (VNC)*, December 5–7, 2018, Taipei, Taiwan.
3) Ahmad, F., Franqueira, V.N.L., Adnane, A., TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks. *IEEE Access* 2018.
4) F. Ahmad, A. Adnane, V. N.L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," *Sensors*, vol. 18, no. 11, 2018.
5) Sharma, P., Austin, D., & Liu, H., (2019), Attacks on Machine Learning: Adversarial Examples in Connected and Autonomous Vehicles, *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1-7.
6) Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors J.*, vol. 20, no. 22, pp. 13752–13767, Nov. 2020.
7) A. Kumar and D. Das, "IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV)," *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Helsinki, Finland, 2022, pp. 1-5, doi: 10.1109/VTC2022-Spring54318.2022.9860946.
8) E. A. Da Rocha Pires, I. L. P. Pires and L. C. P. Albini, "Supporting Confidentiality and Integrity on V2V Communications," *2022 International Conference on Connected Vehicle and Expo (ICCVE)*, Lakeland, FL, USA, 2022, pp. 1-6, doi: 10.1109/ICCVE52871.2022.9742867.
9) L. G. Jaimes *et al*., "A Generative Adversarial Approach for Sybil Attacks Recognition for Vehicular Crowdsensing," *2022 International Conference on Connected Vehicle and Expo (ICCVE)*, Lakeland, FL, USA, 2022, pp. 1-7, doi: 10.1109/ICCVE52871.2022.9743106.
10) L. Wei, J. Cui, H. Zhong, Y. Xu and L. Liu, "Proven Secure Tree-Based Authenticated Key Agreement for Securing V2V and V2I Communications in VANETs," in *IEEE Transactions on Mobile Computing*, vol. 21, no. 9, pp. 3280-3297, 1 Sept. 2022, doi: 10.1109/TMC.2021.3056712.

B. Cell Phone Security, Mobile Devices Security, Bluetooth Security, IoT Security, RFID Security and Social Networks Security

1) Aaron Beach, Mike Gartrell, and Richard Han, Solutions to Security and Privacy Issues in Mobile Social Networking, in *International Conference on Computational Science and Engineering* 2009.
2) Ahren Studer and Adrian Perrig. 2010, Mobile user location-specific encryption (MULE): using your office as your password. In *Proceedings of the third ACM conference on Wireless network security (WiSec '10)*. ACM, New York, NY, USA, 151-162.

3) Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*. ACM, New York, NY, USA, 551-562.
4) René Hummen, Jan H. Ziegeldorf, Hossein Shafagh, Shahid Raza, and Klaus Wehrle. 2013. Towards viable certificate-based authentication for the internet of things. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy (HotWiSec '13)*. ACM, New York, NY, USA, 37-42.
5) Zhi-Kai Zhang, Michael Cheng Yi Cho, and Shiuhpyng Shieh, "Emerging Security Threats and Countermeasures in IoT*", Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15)*. ACM, New York, NY, USA, 2015, 1-6.
6) Quang Do, Ben Martini, and Kim-Kwang Raymond Choo, "A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers*", IEEE Transactions on Information Forensics And Security*, Vol. 11, No. 10, October 2016.
7) Bing Zhou, Jay Lohokare, Ruipeng Gao, Fan Ye, EchoPrint: Two-factor Authentication using Vision and Acoustics on Smartphones, *Mobicom 2018*, October 29 – Nov. 2, 2018, New Delhi, India.
8) Devkishen Sisodia, Samuel Mergendahl, Jun Li and Hasan Cam, Securing the Smart Home via a Two-Mode Security Framework, SecureComm 2018 - *14th EAI International Conference on Security and Privacy in Communication Networks,* August 8-10, 2018, Singapore, Singapore.
9) Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh, Security Vulnerabilities in Bluetooth Technology as Used in IoT*, Journal of Sensor and Actuator Networks*, 2018.
10) A. I. Newaz, A. K. Sikder, M. A. Rahman and A. S. Uluagac, "HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems," *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, Granada, Spain, 2019, pp. 389-396, doi: 10.1109/SNAMS.2019.8931716.
11) Huangxun Chen, Wei Wang, Jin Zhang, Qian Zhang, EchoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication, *IEEE Internet of Things Journal*, December 2019.
12) Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, Christian Becker, "I don't see why I would ever want to use it": Analyzing the Usability of Popular Smartphone Password Managers, *ACM CCS* 2019.
13) Youqian Zhang, Kasper Rasmussen, "Detection of Electromagnetic Interference Attacks on Sensor Systems", *41st IEEE Symposium on Security and Privacy*, Oakland, CA, May 2020.
14) Marco Cominelli, Francesco Gringoli, Margus Lind, Paul Patras, Guevara Noubir, "Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices", *41st IEEE Symposium on Security and Privacy*, Oakland, CA, May 2020.
15) X. Xu, J. Yu, Y. Chen, Q. Hua, Y. Zhu, Y. Chen, M. Li, "TouchPass: Towards Behavior-irrelevant on-touch User Authentication on Smartphones Leveraging Vibrations", *Mobicom* 2020.
16) Sunwoo Lee, Wonsuk Choi, and Dong Hoon Lee. 2021. Usable User Authentication on a Smartwatch using Vibration. In Proceedings of the *2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21)*, November 15–19, 2021.
17) Kaifa Zhao, Hao Zhou, Yulin Zhu, Xian Zhan, Kai Zhou, Jianfeng Li, Le Yu, Wei Yuan, and Xiapu Luo. 2021. Structural Attack against Graph Based Android Malware Detection. In *Proceedings of the 2021*

ACM SIGSAC Conference on Computer and Communications Security (CCS '21), November 15–19, 2021.

18) Classen, J., Heinrich, A., Reith, R., Hollick, M.: Evil never sleeps: when wireless malware stays on after turning off iphones, Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 146–156, *WiSec '22*, Association for Computing Machinery, New York, NY, USA (2022).
19) Muslum Ozgur Ozmen, Ruoyu Song, Habiba Farrukh, and Z. Berkay Celik, Evasion Attacks on Smart Home Physical Event Verification and Defenses, *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2023.
20) H. Farrukh, M. O. Ozmen, F. Kerem Ors and Z. B. Celik, "One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices," *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2023, pp. 3026-3042, doi: 10.1109/SP46215.2023.10179369.

C. Attacks in Wireless Networks

1) Nidal Nasser and Yunfeng Chen, "Secure Multipath Routing Protocol for Wireless Sensor Networks", *ICDCSW'07*.
2) Oscar Punal, Ismet Akta, Caj-Julian Schnelke, Gloria Abidin, Klaus Wehrle and James Gross, "Machine Learning-based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation*", IEEE Conference on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2014.
3) Q. Duan, M. Virendra, S. Upadhyaya and A. Sanzgiri, "Minimum Cost Blocking Problem in Multi-path Wireless Routing Protocols", *IEEE Transactions on Computers*, Vol. 63, No. 7, pp. 1765-1777, July 2014.
4) Vanhoef, Mathy, and Piessens, Frank. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2." *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017)*, 2017, pp. 1313–1328.
5) Zendehdel, Ghazale Amel, Ratinder Kaur, Inderpreet Chopra, Natalia Stakhanova and Erik J. Scheme, "Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices," *ACM Transactions on Internet Technology (TOIT)* 22 (2021): 1 - 31.
6) Blumbergs, B., Dobelis, Ē., Paikens, P., Nesenbergs, K., Solovjovs, K. and Rušiņš, A., 2023, January, WearSec: Towards Automated Security Evaluation of Wireless Wearable Devices, Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30–December 2, 2022, *Proceedings (pp. 311-325). Cham: Springer International Publishing*.

D. Insider Attack Detection

1) Fang Liu; Xiuzhen Cheng; Dechang Chen, "Insider Attacker Detection in Wireless Sensor Networks," INFOCOM 2007. *26th IEEE International Conference on Computer Communications*. IEEE, vol., no., pp. 1937, 1945, 6-12 May 2007.
2) Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov, "Know your enemy: the risk of unauthorized access in smartphones by insiders", In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13)*, 2013.
3) Mihai Bâce, Alia Saad, Mohamed Khamis, Stefan Schneegass, and Andreas Bulling, 2022, PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices, In *Proc. on Privacy Enhancing Technologies (PETs)*, Sciendo.

E. Smart Grid Security

1) S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, “SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures”, *IEEE Transactions on Smart Grid*, vol. 3, no. 4, December 2012, pp. 1790-1799.
2) Seung-Hyun Seo, Xiaoyu Ding and Elisa Bertino, “Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures”, *Proceedings of the IEEE international conference on smart grid communications (SmartGridComm)*; 21−24 Oct. 2013. p. 498−503.
3) Bertino, Elisa, and Murat Kantarcioglu. "A cyber-provenance infrastructure for sensor-based data-intensive applications." *2017 IEEE International Conference on Information Reuse and Integration (IRI). IEEE*, 2017.
4) Yan, Lili, Yan Chang, and Shibin Zhang. "A lightweight authentication and key agreement scheme for smart grid." *International Journal of Distributed Sensor Networks* 13.2 (2017): 1550147717694173.
5) Chehri, A.; Fofana, I.; Yang, X. Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability* 2021, 13, 3196.

F. Student Selected Additions