UNIVERSITÀ DEGLI STUDI DI PADOVA

European Commission

MARIE CURIE ACTIONS

University of Padua - MSc in Cybersecurity

Advanced Topics in Computer and Network Security

Academic Year: 2023/2024

Lecturer: *Mauro Conti*

Topics

You can download the papers automatically from the university if you are connected to eduroam, or from your home by setting up the university proxy.
You can found the guide to install and setup the proxy here (eng) and here (ita).
For any issues, you can contact the teaching assistants.

The topic covers the following macro areas:

- **Android**: security in mobile.
- **Blockchain**: security in blockchain.
- **CPS**: security on Cyber-Physical Systems such as Industrial Control Systems, Vehicular Networks, Internet of Things, and so on.
- **ICN**: security on network paradigms, such as Information-centric networking and Named Data Networking.
- **Malware Detection**: strategies to detect malware.
- **MLS**: Machine Learning for Security.
- **Social Networks**: security and privacy on social networks.
- **Software Security**: security of software and techniques of analysis such as fuzzing or reverse engineering.
- **5G Security**: security of 5G technology and other novel telecomunication systems.
- **MISC**: Other popular cyber-security topics.

Topic 1 (Android): Android Virtualization Technique
Topic 2 (Android): Security and Privacy Vulnerabilities Detection in Android Apps
Topic 3 (Android): Taint Analysis
Topic 4 (Blockchain): Distributed key management systems in blockchains
Topic 5 (Blockchain): Isogeny-based crytography for PKI in blockchains
Topic 6 (Blockchain): Task offloading in mobile blockchains
Topic 7 (Blockchain): Distributed oralce networks truth discovery
Topic 8 (Blockchain): Intergration of Federated learning and Blockchain for data sharing
Topic 9 (CPS): Anomaly Detection in Industrial Systems

Topic 10 (CPS): Industrial Honeypot
Topic 11 (CPS): Air - Ground communication
Topic 12 (CPS): IoT security
Topic 13 (CPS): Identity of Things
Topic 14 (CPS): Cyber-Physical Anomaly Detection
Topic 15 (CPS): Advanced security on Industrial Control System
Topic 16 (CPS): Private Information Retrieval (PIR) for healthcare
Topic 17 (CPS): Privacy for Vehicular Networks - Ride-Hailing Service
Topic 18 (CPS): Privacy for Vehicular Networks - Traffic Monitoring
Topic 19 (CPS): Privacy for Vehicular Networks - Smart Parking
Topic 20 (CPS): Vehicular Security - Automotive Keyless Entry
Topic 21 (CPS): Vehicular Security - Charging-While-Driving
Topic 22 (CPS): Vehicular Security - CAN Security
Topic 23 (CPS): Privacy protection of Electric Vehicles Owners
Topic 24 (CPS): Machine learning techniques for lightweight continuous authentication
Topic 25 (CPS): Vehicular Security - CAN Attacks to error handling
Topic 26 (CPS): Physical side-channel attacks in mobile charging
Topic 27 (CPS): Hyperloop: a cybersecuirty challenge
Topic 28 (CPS): Maritime Security
Topic 29 (ICN): Cache Privacy Attacks
Topic 30 (ICN): Content Popularity Prediction
Topic 31 (ICN): Interest Flooding Attacks
Topic 32 (ICN): Coexistence of TCP/IP and ICN/NDN
Topic 33 (Malware Detection): Malware Analysis and Detection Methods
Topic 34 (Malware Detection): Ransomware Detection using Deception Models
Topic 35 (Malware Detection): Adversarial Machine Learning on Malaware
Topic 36 (Malware Detection): PDF Malware Detection
Topic 37 (MLS): Behavioural Biometrics
Topic 38 (MLS): Deauthentication
Topic 39 (MLS): Security of Machine Learning Implementations
Topic 40 (MLS): Hate Speech Detection on Online Platforms
Topic 41 (MLS): The role of generative models in Cybersecurity
Topic 42 (MLS): Continuous Authentication
Topic 43 (MLS): Evaluation of Adversarial Attacks on Privacy Preserving Machine Learning Models
Topic 44 (MLS): Adversarial Machine Learning: Evasion Attacks
Topic 45 (MLS): GANs for Attack Sample Generation
Topic 46 (MLS): Machine Learning in Intrusion Detection Systems
Topic 47 (Social Networks): Fake Account Detection on Instagram
Topic 48 (Social Networks): Social Network Analysis
Topic 49 (Social Networks): Fake Engagement on Instagram
Topic 50 (Social Networks): Private data inference from Social Networks
Topic 51 (Software Security): Understand humans approach to Reverse Engineering
Topic 52 (Software Security): Find and exploit vulnerabilities
Topic 53 (Software Security): Fuzzing
Topic 54 (5G Security): 5G new radio Handover Security
Topic 55 (5G Security): Open Radio Access Network
Topic 56 (5G Security): Physical layer authentication
Topic 57 (5G Security): Smart Jamming attacks
Topic 58 (MISC): Video forensics
Topic 59 (MISC): Security in Logic-Locking (Logic-Obfuscation)
Topic 60 (MISC): Secure key generation in PUF-based Logic-Locking
Topic 61 (MISC): Misuses in Wearable Devices
Topic 62 (MISC): Cyber-Threat Intelligence
Topic 63 (MISC): Lie Detection
Topic 64 (MISC): Security and Privacy in Online Video Games
Topic 65 (MISC): Securing microservices architectures during SDLC

Topic 66 (MISC): Detecting Wireless Sensors
Topic 67 (MISC): Textual Captchas
Topic 68 (MISC): Covert channel for security and privacy
Topic 69 (MISC): PIN and Password security
Topic 70 (MISC): Security and privacy of keyboard
Topic 71 (MISC): Adversarial attacks on text classification models
Topic 72 (MISC): Document Anonymization
Topic 73 (MISC): Metaverse Security
Topic 74 (MISC): Side-Channel Attacks in PaaS Clouds

Topic 1 (Android): Android Virtualization Technique

Primary:

- Shi, L., Fu, J., Guo, Z., & Ming, J. (2019, June). " Jekyll and Hyde" is Risky: Shared-Everything Threat Mitigation in Dual-Instance Apps. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (pp. 222-235).

Secondary:

- Zhang, L., Yang, Z., He, Y., Li, M., Yang, S., Yang, M., ... & Qian, Z. (2019). App in the middle: Demystify application virtualization in Android and its security threats. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 3(1), 1-24.
- Luo, T., Zheng, C., Xu, Z., & Ouyang, X. (2017). Anti-plugin: Don't let your app play as an Android plugin. Proceedings of Blackhat Asia.
- Dai, D., Li, R., Tang, J., Davanian, A., & Yin, H. (2020, June). Parallel Space Traveling: A Security Analysis of App-Level Virtualization in Android. In Proceedings of the 25th ACM Symposium on Access Control Models and Technologies (pp. 25-32).

Topic 2 (Android): Security and Privacy Vulnerabilities Detection in Android Apps

Primary:

- Nguyen, D. C., Wermke, D., Acar, Y., Backes, M., Weir, C., & Fahl, S. (2017, October). A stitch in time: Supporting android developers in writingsecure code. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1065-1077).

Secondary:

- Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H. (2010, December). Paranoid android: versatile protection for smartphones. In Proceedings of the 26th annual computer security applications conference (pp. 347-356).
- Qian, C., Luo, X., Le, Y., & Gu, G. (2015). Vulhunter: toward discovering vulnerabilities in android applications. IEEE Micro, 35(1), 44-53.
- Ghafari, M., Gadient, P., & Nierstrasz, O. (2017, September). Security smells in android. In 2017 IEEE 17th international working conference on source code analysis and manipulation (SCAM) (pp. 121-130). IEEE.

Topic 3 (Android): Taint Analysis

Primary:

- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N. (2014). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Transactions on Computer Systems (TOCS), 32(2), 1-29.

Secondary:

- Wei, F., Roy, S., & Ou, X. (2014, November). Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps. In

Proceedings of the 2014 ACM SIGSAC conference on computer and communications security (pp. 1329-1341).
- Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., ... & McDaniel, P. (2014). Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. Acm Sigplan Notices, 49(6), 259-269.
- Sun, M., Wei, T., & Lui, J. C. (2016, October). Taintart: A practical multi-level information-flow tracking system for android runtime. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 331-342).

Topic 4 (Blockchain): Distributed key management systems in blockchains

Primary:
- de Ree, M., Mantas, G., Rodriguez, J., Otung, I. E., & Verikoukis, C. (2021). DISTANT: DIStributed Trusted Authority-based key managemeNT for beyond 5G wireless mobile small cells. Computer Communications.

Secondary:
- Pal, O., Alam, B., Thakur, V., & Singh, S. (2019). Key management for blockchain technology. ICT Express.
- Matsumoto, S., & Reischuk, R. M. (2017, May). IKP: Turning a PKI around with decentralized automated incentives. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 410-426). IEEE.

Topic 5 (Blockchain): Isogeny-based crytography for PKI in blockchains

Primary:
- FernÃ¡ndez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.

Secondary:
- de Kock, B., GjÃ¸steen, K., & Veroni, M. (2020). Practical Isogeny-Based Key-exchange with Optimal Tightness. IACR Cryptol. ePrint Arch., 2020, 1165.

Topic 6 (Blockchain): Task offloading in mobile blockchains

Primary:
- Xiao, K., Gao, Z., Shi, W., Qiu, X., Yang, Y., & Rui, L. (2020). EdgeABC: An architecture for task offloading and resource allocation in the Internet of Things. Future Generation Computer Systems, 107, 498-508.

Secondary:
- Dou, W., Tang, W., Liu, B., Xu, X., & Ni, Q. (2020). Blockchain-based Mobility-aware Offloading mechanism for Fog computing services. Computer Communications, 164, 261-273.

Topic 7 (Blockchain): Distributed oralce networks truth discovery

Primary:
- Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., & Kastania, A. (2018, July). Astraea: A decentralized blockchain oracle. In 2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData) (pp. 1145-1152). IEEE.

Secondary:
- Peterson, J., & Krug, J. (2015). Augur: a decentralized, open-source platform for

prediction markets. arXiv preprint arXiv:1501.01042.
- Nelaturu, K., Adler, J., Merlini, M., Berryhill, R., Veira, N., Poulos, Z., & Veneris, A. (2020). On public crowdsource-based mechanisms for a decentralized blockchain oracle. IEEE Transactions on Engineering Management, 67(4), 1444-1458.

Topic 8 (Blockchain): Intergration of Federated learning and Blockchain for data sharing

Primary:

- Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated Learning-based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal.

Secondary:

- Briggs, C., Fan, Z., & Andras, P. (2021). A review of privacy-preserving federated learning for the Internet-of-Things. Federated Learning Systems, 21-50.
- Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O. (2021). Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT Edge Devices. IEEE Internet of Things Journal.

Topic 9 (CPS): Anomaly Detection in Industrial Systems

Primary:

- Kus, D., Wagner, E., Pennekamp, J., Wolsing, K., Fink, I. B., Dahlmanns, M., ... & Henze, M. (2022, May). A False Sense of Security? Revisiting the State of Machine Learning-Based Industrial Intrusion Detection. In Proceedings of the 8th ACM on Cyber-Physical System Security Workshop (pp. 73-84).

Secondary:

- Wolsing, K., Thiemt, L., Sloun, C. V., Wagner, E., Wehrle, K., & Henze, M. (2022). Can Industrial Intrusion Detection Be SIMPLE?. In European Symposium on Research in Computer Security (pp. 574-594). Springer, Cham.
- Umer, M. A., Ahmed, C. M., Jilani, M. T., & Mathur, A. P. (2021, November). Attack rules: an adversarial approach to generate attacks for Industrial Control Systems using machine learning. In Proceedings of the 2th Workshop on CPS&IoT Security and Privacy (pp. 35-40).
- Castellanos, J. H., Ochoa, M., Cardenas, A. A., Arden, O., & Zhou, J. (2021, October). AttkFinder: Discovering attack vectors in PLC programs using information flow analysis. In 24th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 235-250).

Topic 10 (CPS): Industrial Honeypot

Primary:

- LÃ³pez-Morales, E., Rubio-Medrano, C., DoupÃ©, A., Shoshitaishvili, Y., Wang, R., Bao, T., & Ahn, G. J. (2020, October). HoneyPLC: A next-generation honeypot for industrial control systems. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 279-291).

Secondary:

- Wilhoit, K., & Hilt, S. (2015). The gaspot experiment: Unexamined perils in using.
- Conti, M., Trolese, F., & Turrin, F. (2022, July). ICSpot: A High-Interaction Honeypot for Industrial Control Systems. In 2022 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-4). IEEE.

Topic 11 (CPS): Air - Ground communication

Primary:

- Strohmeier, M., Martinovic, I., & Lenders, V. (2020). Securing the airâ€“ground link in aviation. In The Security of Critical Infrastructures (pp. 131-154). Springer, Cham.

Secondary:

- Smith, M., Strohmeier, M., Lenders, V., & Martinovic, I. (2022). Understanding realistic attacks on airborne collision avoidance systems. Journal of Transportation Security, 15(1), 87-118.
- Strohmeier, M., Smith, M., Lenders, V., & Martinovic, I. (2021). Classi-fly: Inferring aircraft categories from open data. ACM Transactions on Intelligent Systems and Technology (TIST), 12(6), 1-23.
- Baselt, G., Strohmeier, M., Pavur, J., Lenders, V., & Martinovic, I. (2022, May). Security and Privacy Issues of Satellite Communication in the Avlatlon Domain. In 2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon) (Vol. 700, pp. 285-307). IEEE.

Topic 12 (CPS): IoT security

Primary:

- Ambrosin, M., Conti, M., Ibrahim, A., Neven, G., Sadeghi, A. R., & Schunter, M. (2016, October). SANA: Secure and scalable aggregate network attestation. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 731-742).

Secondary:

- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
- Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE.
- Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.

Topic 13 (CPS): Identity of Things

Primary:

- Mahalle, P., Babar, S., Prasad, N. R., & Prasad, R. (2010, July). Identity management framework towards internet of things (IoT): Roadmap and key challenges. In International Conference on Network Security and Applications (pp. 430-439). Springer, Berlin, Heidelberg.

Secondary:

- Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., & Kayssi, A. (2016, June). Identity-based authentication scheme for the Internet of Things. In 2016 IEEE Symposium on Computers and Communication (ISCC) (pp. 1109-1111). IEEE.
- Lam, K. Y., & Chi, C. H. (2016, November). Identity in the Internet-of-Things (IoT): New challenges and opportunities. In International Conference on Information and Communications Security (pp. 18-26). Springer, Cham.
- Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors, 18(12), 4215.

Topic 14 (CPS): Cyber-Physical Anomaly Detection

Primary:

- Marchetti, M., & Stabili, D. (2017, June). Anomaly detection of CAN bus messages through analysis of ID sequences. In 2017 IEEE Intelligent Vehicles Symposium (IV) (pp. 1577-1583). IEEE.

Secondary:

- Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR), 54(5), 1-36.
- Xu, Q., Ali, S., & Yue, T. (2021, April). Digital Twin-based Anomaly Detection in Cyber-physical Systems. In 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST) (pp. 205-216). IEEE.

Topic 15 (CPS): Advanced security on Industrial Control System

Primary:

- Tychalas, D., Benkraouda, H., & Maniatakos, M. (2021). ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in {ICS} Control Applications. In 30th {USENIX} Security Symposium ({USENIX} Security 21).

Secondary:

- Sarkar, E., Benkraouda, H., & Maniatakos, M. (2020, October). I came, I saw, I hacked: Automated Generation of Process-independent Attacks for Industrial Control Systems. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (pp. 744-758).
- Wang, X., Konstantinou, C., Maniatakos, M., Karri, R., Lee, S., Robison, P., ... & Kim, S. (2016). Malicious firmware detection with hardware performance counters. IEEE Transactions on Multi-Scale Computing Systems, 2(3), 160-173.

Topic 16 (CPS): Private Information Retrieval (PIR) for healthcare

Primary:

- Lai, J., Mu, Y., Guo, F., Jiang, P., & Susilo, W. (2018). Privacy-enhanced attribute-based private information retrieval. Information sciences, 454, 275-291.

Secondary:

- Domingo-Ferrer, J., Bras-AmorÃ³s, M., Wu, Q., & ManjÃ³n, J. (2009). User-private information retrieval based on a peer-to-peer community. Data & Knowledge Engineering, 68(11), 1237-1252.

Topic 17 (CPS): Privacy for Vehicular Networks - Ride-Hailing Service

Primary:

- Pham, A., Dacosta, I., Endignoux, G., Pastoriza, J. R. T., Huguenin, K., & Hubaux, J. P. (2017). ORide: A privacy-preserving yet accountable ride-hailing service. In 26th {USENIX} Security Symposium ({USENIX} Security 17) (pp. 1235-1252).

Secondary:

- Luo, Y., Jia, X., Fu, S., & Xu, M. (2018). pRide: Privacy-preserving ride matching over road networks for online ride-hailing service. IEEE Transactions on Information Forensics and Security, 14(7), 1791-1802.
- Xie, H., Guo, Y., & Jia, X. (2021). A Privacy-Preserving Online Ride-Hailing System Without Involving a Third Trusted Server. IEEE Transactions on Information Forensics and Security, 16, 3068-3081.

Topic 18 (CPS): Privacy for Vehicular Networks - Traffic Monitoring

Primary:

- Hoh, B., Gruteser, M., Herring, R., Ban, J., Work, D., Herrera, J. C., ... & Jacobson, Q. (2008, June). Virtual trip lines for distributed privacy-preserving traffic monitoring. In Proceedings of the 6th international conference on Mobile systems, applications, and services (pp. 15-28).

Secondary:

- Li, M., Zhu, L., & Lin, X. (2019). Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing. IEEE Transactions on Services Computing.
- Li, M., Zhu, L., & Lin, X. (2019). Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing. IEEE Transactions on Services Computing.

Topic 19 (CPS): Privacy for Vehicular Networks - Smart Parking

Primary:

- Lu, R., Lin, X., Zhu, H., & Shen, X. (2009, April). SPARK: A new VANET-based smart parking scheme for large parking lots. In IEEE INFOCOM 2009 (pp. 1413-1421). IEEE.

Secondary:

- Zhu, L., Li, M., Zhang, Z., & Qin, Z. (2018). ASAP: An anonymous smart-parking and payment scheme in vehicular networks. IEEE Transactions on Dependable and Secure Computing, 17(4), 703-715.
- Ni, J., Lin, X., & Shen, X. (2019). Toward privacy-preserving valet parking in autonomous driving era. IEEE Transactions on Vehicular Technology, 68(3), 2893-2905.

Topic 20 (CPS): Vehicular Security - Automotive Keyless Entry

Primary:

- Garcia, F. D., Oswald, D., Kasper, T., & PavlidÃ¨s, P. (2016). Lock it and still lose itâ€”on the (in) security of automotive remote keyless entry systems. In 25th {USENIX} Security Symposium ({USENIX} Security 16).

Secondary:

- Benadjila, R., Renard, M., Lopes-Esteves, J., & Kasmi, C. (2017). One car, two frames: attacks on hitag-2 remote keyless entry systems revisited. In 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17).
- Glocker, T., Mantere, T., & Elmusrati, M. (2017, April). A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography. In 2017 8th International Conference on Information and Communication Systems (ICICS) (pp. 310-315). IEEE.
- Wouters, L., Gierlichs, B., & Preneel, B. (2021). My other car is your car: compromising the Tesla Model X keyless entry system. IACR Transactions on Cryptographic Hardware and Embedded Systems, 149-172.

Topic 21 (CPS): Vehicular Security - Charging-While-Driving

Primary:

- Roman, L. F., & Gondim, P. R. (2020). Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment. Ad Hoc Networks, 97, 102004.

Secondary:

- Li, H., DÃ¡n, G., & Nahrstedt, K. (2013, October). FADEC: Fast authentication for dynamic electric vehicle charging. In 2013 IEEE Conference on Communications and

Network Security (CNS) (pp. 369-370). IEEE.

- Li, H., DÃ¡n, G., & Nahrstedt, K. (2016). Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging. IEEE Transactions on Smart Grid, 8(5), 2305-2313.

Topic 22 (CPS): Vehicular Security - CAN Security

Primary:

- Groza, B., Popa, L., Murvay, P. S., Elovici, Y., & Shabtai, A. (2021). {CANARY}-a reactive defense mechanism for Controller Area Networks based on Active RelaYs. In 30th {USENIX} Security Symposium ({USENIX} Security 21).

Secondary:

- Humayed, A., & Luo, B. (2017, April). Using ID-hopping to defend against targeted DoS on CAN. In Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles (pp. 19-26).
- Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive experimental analyses of automotive attack surfaces. In USENIX Security Symposium (Vol. 4, No. 447-462, p. 2021).
- Islam, R., & Refat, R. U. D. (2020). Improving CAN bus security by assigning dynamic arbitration IDs. Journal of Transportation Security, 13(1), 19-31.

Topic 23 (CPS): Privacy protection of Electric Vehicles Owners

Primary:

- Brighente, A., Conti, M., Donadel, D., & Turrin, F. (2021). EVScout2. 0: Electric Vehicle Profiling Through Charging Profile. arXiv preprint arXiv:2106.16016.

Secondary:

- Leukam Lako, F., Lajoie-Mazenc, P., & Laurent, M. (2021). Privacy-Preserving Publication of Time-Series Data in Smart Grid. Security and Communication Networks, 2021.
- Saxena, N., Grijalva, S., Chukwuka, V., & Vasilakos, A. V. (2017). Network security and privacy challenges in smart vehicle-to-grid. IEEE Wireless Communications, 24(4), 88-98.

Topic 24 (CPS): Machine learning techniques for lightweight continuous authentication

Primary:

- Hou, W., Wang, X., Chouinard, J. Y., & Refaey, A. (2014). Physical layer authentication for mobile systems with time-varying carrier frequency offsets. IEEE Transactions on Communications, 62(5), 1658-1667.

Secondary:

- Brighente, A., Formaggio, F., Di Nunzio, G. M., & Tomasin, S. (2019). Machine learning for in-region location verification in wireless networks. IEEE Journal on Selected Areas in Communications, 37(11), 2490-2502.
- Ihsan, U., Malaney, R., & Yan, S. (2019, August). Machine learning and location verification in vehicular networks. In 2019 IEEE/CIC International Conference on Communications in China (ICCC) (pp. 91-95). IEEE.

Topic 25 (CPS): Vehicular Security - CAN Attacks to error handling

Primary:

- Serag, K., Bhatia, R., Kumar, V., Celik, Z. B., & Xu, D. (2021). Exposing New Vulnerabilities of Error Handling Mechanism in {CAN}. In 30th {USENIX} Security

Symposium ({USENIX} Security 21).

Secondary:

- Cho, K. T., & Shin, K. G. (2016, October). Error handling of in-vehicle networks makes them vulnerable. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1044-1055).
- Kulandaivel, S., Jain, S., Guajardo, J., & Sekar, V. (2021, May). CANNON: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 195-210). IEEE.

Topic 26 (CPS): Physical side-channel attacks in mobile charging

Primary:

- Wang, Y., Guo, H., & Yan, Q. (2022). GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line. arXiv preprint arXiv:2202.02585.

Secondary:

- Wang, K., Mitev, R., Yan, C., Ji, X., Sadeghi, A. R., & Xu, W. (2022). GhostTouch: Targeted Attacks on Touchscreens without Physical Touch. In 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA. https://www. usenix. org/conference/usenixsecurity22/presentation/wang-kai.
- Spolaor, R., Abudahi, L., Moonsamy, V., Conti, M., & Poovendran, R. (2017, July). No free charge theorem: A covert channel via usb charging cable on mobile devices. In International Conference on Applied Cryptography and Network Security (pp. 83-102). Springer, Cham.
- Liu, J., Zou, X., Zhao, L., Tao, Y., Hu, S., Han, J., & Ren, K. (2022). Privacy Leakage in Wireless Charging. IEEE Transactions on Dependable and Secure Computing.

Topic 27 (CPS): Hyperloop: a cybersecuirty challenge

Primary:

- Brighente, A., Conti, M., Donadel, D., & Turrin, F. (2022). Hyperloop: A Cybersecurity Perspective. arXiv preprint arXiv:2209.03095.

Secondary:

- Tavsanoglu, A., Briso, C., Carmena-Cabanillas, D., & Arancibia, R. B. (2021). Concepts of Hyperloop Wireless Communication at 1200 km/h: 5G, Wi-Fi, Propagation, Doppler and Handover. Energies, 14(4), 983.
- Zhang, J., Liu, L., Han, B., Li, Z., Zhou, T., Wang, K., ... & Ai, B. (2020). Concepts on train-to-ground wireless communication system for hyperloop: Channel, network architecture, and resource management. Energies, 13(17), 4309.
- Hedhly, W., Amin, O., Shihada, B., & Alouini, M. S. (2021). Hyperloop Communications: Challenges, Advances, and Approaches. IEEE Open Journal of the Communications Society, 2, 2413-2435.

Topic 28 (CPS): Maritime Security

Primary:

- Amro, A., & Gkioulos, V. (2022). From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. In European Symposium on Research in Computer Security (pp. 535-553). Springer, Cham.

Secondary:

- Wolsing, K., Saillard, A., Bauer, J., Wagner, E., van Sloun, C., Fink, I. B., ... & Henze, M. (2022, September). Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset. In 2022 IEEE 47th Conference on Local Computer Networks (LCN) (pp. 114-122). IEEE.

- Tam, K., & Jones, K. (2019, June). Factors affecting cyber risk in maritime. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-8). IEEE.

Topic 29 (ICN): Cache Privacy Attacks

Primary:

- Acs, G., Conti, M., Gasti, P., Ghali, C., Tsudik, G., & Wood, C. A. (2017). Privacy-aware caching in information-centric networking. IEEE Transactions on Dependable and Secure Computing, 16(2), 313-328.

Secondary:

- Mohaisen, A., Mekky, H., Zhang, X., Xie, H., & Kim, Y. (2014). Timing attacks on access privacy in information centric networks and countermeasures. IEEE Transactions on Dependable and Secure Computing, 12(6), 675-687.
- Acs, G., Conti, M., Gasti, P., Ghali, C., & Tsudik, G. (2013, July). Cache privacy in named-data networking. In 2013 IEEE 33rd International Conference on Distributed Computing Systems (pp. 41-51). IEEE.
- Compagno, A., Conti, M., Losiouk, E., Tsudik, G., & Valle, S. (2020, April). A proactive cache privacy attack on ndn. In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium (pp. 1-7). IEEE.

Topic 30 (ICN): Content Popularity Prediction

Primary:

- Yao, L., Zeng, Y., Wang, X., Chen, A., & Wu, G. (2020). Detection and Defense of Cache Pollution Based on Popularity Prediction in Named Data Networking. IEEE Transactions on Dependable and Secure Computing.

Secondary:

- Li, J., Wu, H., Liu, B., Lu, J., Wang, Y., Wang, X., ... & Dong, L. (2012, October). Popularity-driven coordinated caching in named data networking. In 2012 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS) (pp. 15-26). IEEE.
- Cho, K., Lee, M., Park, K., Kwon, T. T., Choi, Y., & Pack, S. (2012, March). WAVE: Popularity-based and collaborative in-network caching for content-oriented networks. In 2012 Proceedings IEEE INFOCOM Workshops (pp. 316-321). IEEE.
- Zhang, R., Liu, J., Huang, T., & Xie, R. (2017, May). Popularity based probabilistic caching strategy design for named data networking. In 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 476-481). IEEE.

Topic 31 (ICN): Interest Flooding Attacks

Primary:

- Compagno, A., Conti, M., Gasti, P., & Tsudik, G. (2013, October). Poseidon: Mitigating interest flooding DDoS attacks in named data networking. In 38th annual IEEE conference on local computer networks (pp. 630-638). IEEE.

Secondary:

- Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., & Zhang, L. (2013, May). Interest flooding attack and countermeasures in named data networking. In 2013 IFIP Networking Conference (pp. 1-9). IEEE.
- Salah, H., Wulfheide, J., & Strufe, T. (2015, October). Coordination supports security: A new defence mechanism against interest flooding in NDN. In 2015 IEEE 40th Conference on Local Computer Networks (LCN) (pp. 73-81). IEEE.
- Benarfa, A., Hassan, M., Compagno, A., Losiouk, E., Yagoubi, M. B., & Conti, M. (2019, June). Chokifa: A new detection and mitigation approach against interest flooding

attacks in ndn. In International Conference on Wired/Wireless Internet Communication (pp. 53-65). Springer, Cham.

Topic 32 (ICN): Coexistence of TCP/IP and ICN/NDN

Primary:

- Conti, M., Gangwal, A., Hassan, M., Lal, C., & Losiouk, E. (2020). The road ahead for networking: A survey on icn-ip coexistence solutions. IEEE Communications Surveys & Tutorials, 22(3), 2104-2129.

Secondary:

- Rahman, A., Trossen, D., Kutscher, D., & Ravindran, R. (2018). Deployment considerations for information-centric networking (ICN). Internet Engineering Task Force, Internet-Draft draft-irtf-icnrg-deployment-guidelines-03.

Topic 33 (Malware Detection): Malware Analysis and Detection Methods

Primary:

- Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A. (2020). Intelligent mobile malware detection using permission requests and API calls. Future Generation Computer Systems, 107, 509-521.

Secondary:

- Zhao, Y., Li, L., Wang, H., Cai, H., BissyandÃ©, T. F., Klein, J., & Grundy, J. (2021). On the Impact of Sample Duplication in Machine-Learning-Based Android Malware Detection. ACM Transactions on Software Engineering and Methodology (TOSEM), 30(3), 1-38.
- Surendran, R., Thomas, T., & Emmanuel, S. (2020). A TAN based hybrid model for android malware detection. Journal of Information Security and Applications, 54, 102483.

Topic 34 (Malware Detection): Ransomware Detection using Deception Models

Primary:

- Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2021). Differential Area Analysis for Ransomware Attack Detection within Mixed File Datasets. Computers & Security, 102377.

Secondary:

- Moussaileb, R., Cuppens, N., Lanet, J. L., & Bouder, H. L. (2021). A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms. ACM Computing Surveys (CSUR), 54(6), 1-36.
- Min, D., Ko, Y., Walker, R., Lee, J., & Kim, Y. (2021). A Content-based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.
- Faghihi, F., & Zulkernine, M. (2021). RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware. Computer Networks, 191, 108011.

Topic 35 (Malware Detection): Adversarial Machine Learning on Malaware

Primary:

- Maiorca, D., Demontis, A., Biggio, B., Roli, F., & Giacinto, G. (2020). Adversarial detection of flash malware: Limitations and open issues. Computers & Security, 96, 101901.

Secondary:

- Demetrio, L., Coull, S. E., Biggio, B., Lagorio, G., Armando, A., & Roli, F. (2020).

Adversarial EXEmples: A survey and experimental evaluation of practical attacks on machine learning for windows malware detection. arXiv preprint arXiv:2008.07125.
- Demetrio, L., & Biggio, B. (2021). Secml-malware: A Python library for adversarial robustness evaluation of windows malware classifiers. arXiv preprint arXiv:2104.12848.

Topic 36 (Malware Detection): PDF Malware Detection

Primary:

- Maiorca, D., Biggio, B., & Giacinto, G. (2019). Towards adversarial malware detection: Lessons learned from PDF-based attacks. ACM Computing Surveys (CSUR), 52(4), 1-36.

Secondary:

- Corum, A., Jenkins, D., & Zheng, J. (2019, June). Robust PDF malware detection with image visualization and processing techniques. In 2019 2nd International Conference on Data Intelligence and Security (ICDIS) (pp. 108-114). IEEE.
- Jordan, A., Gauthier, F., Hassanshahi, B., & Zhao, D. (2019, November). Unacceptable behavior: Robust pdf malware detection using abstract interpretation. In Proceedings of the 14th ACM SIGSAC Workshop on Programming Languages and Analysis for Security (pp. 19-30).

Topic 37 (MLS): Behavioural Biometrics

Primary:

- Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017, April). Evaluating behavioral biometrics for continuous authentication: Challenges and metrics. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 386-399).

Secondary:

- Bhatt, S., & Santhanam, T. (2013, February). Keystroke dynamics for biometric authenticationâ€”A survey. In 2013 international conference on pattern recognition, informatics and mobile engineering (pp. 17-23). IEEE.
- Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998-2026.

Topic 38 (MLS): Deauthentication

Primary:

- Kaczmarek, T., Ozturk, E., & Tsudik, G. (2018, July). Assentication: user de-authentication and lunchtime attack mitigation with seated posture biometric. In International Conference on Applied Cryptography and Network Security (pp. 616-633). Springer, Cham.

Secondary:

- Conti, M., Lovisotto, G., Martinovic, I., & Tsudik, G. (2017, June). Fadewich: fast deauthentication over the wireless channel. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 2294-2301). IEEE.
- Mare, S., Markham, A. M., Cornelius, C., Peterson, R., & Kotz, D. (2014, May). Zebra: Zero-effort bilateral recurring authentication. In 2014 IEEE Symposium on Security and Privacy (pp. 705-720). IEEE.

Topic 39 (MLS): Security of Machine Learning Implementations

Primary:

- Xiao, Q., Chen, Y., Shen, C., Chen, Y., & Li, K. (2019). Seeing is not believing: Camouflage attacks on image scaling algorithms. In 28th {USENIX} Security Symposium

({USENIX} Security 19) (pp. 443-460).

Secondary:

- Xiao, Q., Chen, Y., Shen, C., Chen, Y., & Li, K. (2019). Seeing is not believing: Camouflage attacks on image scaling algorithms. In 28th {USENIX} Security Symposium ({USENIX} Security 19) (pp. 443-460).
- Pajola, L., & Conti, M. (2021). Fall of Giants: How popular text-based MLaaS fall against a simple evasion attack. arXiv preprint arXiv:2104.05996.

Topic 40 (MLS): Hate Speech Detection on Online Platforms

Primary:

- GrÃ¶ndahl, T., Pajola, L., Juuti, M., Conti, M., & Asokan, N. (2018, January). All you need is" love" evading hate speech detection. In Proceedings of the 11th ACM workshop on artificial intelligence and security (pp. 2-12).

Secondary:

- Kiela, D., Firooz, H., Mohan, A., Goswami, V., Singh, A., Ringshia, P., & Testuggine, D. (2020). The hateful memes challenge: Detecting hate speech in multimodal memes. arXiv preprint arXiv:2005.04790.
- Schmidt, A., & Wiegand, M. (2017, April). A survey on hate speech detection using natural language processing. In Proceedings of the fifth international workshop on natural language processing for social media (pp. 1-10).

Topic 41 (MLS): The role of generative models in Cybersecurity

Primary:

- Yinka-Banjo, C., & Ugot, O. A. (2020). A review of generative adversarial networks and its application in cybersecurity. Artificial Intelligence Review, 53(3), 1721-1736.

Secondary:

- Zhang, X., Karaman, S., & Chang, S. F. (2019, December). Detecting and simulating artifacts in gan fake images. In 2019 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.
- Ye, G., Tang, Z., Fang, D., Zhu, Z., Feng, Y., Xu, P., ... & Wang, Z. (2018, October). Yet another text captcha solver: A generative adversarial network based approach. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 332-348).

Topic 42 (MLS): Continuous Authentication

Primary:

- Feng, H., Fawaz, K., & Shin, K. G. (2017, October). Continuous authentication for voice assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (pp. 343-355).

Secondary:

- Camara, C., Peris-Lopez, P., Gonzalez-Manzano, L., & Tapiador, J. (2018). Real-time electrocardiogram streams for continuous authentication. Applied Soft Computing, 68, 784-794.
- Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2020). Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal, 7(9), 9128-9143.

Topic 43 (MLS): Evaluation of Adversarial Attacks on Privacy Preserving Machine

Learning Models

Primary:

- Zhao, C., Wen, Y., Li, S., Liu, F., & Meng, D. (2021, June). FederatedReverse: A Detection and Defense Method Against Backdoor Attacks in Federated Learning. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (pp. 51-62).

Secondary:

- Liu, X., Li, H., Xu, G., Chen, Z., Huang, X., & Lu, R. (2021). Privacy-Enhanced Federated Learning against Poisoning Adversaries. IEEE Transactions on Information Forensics and Security.
- Costa, G., Pinelli, F., Soderi, S., & Tolomei, G. (2021). Covert Channel Attack to Federated Learning Systems. arXiv preprint arXiv:2104.10561.

Topic 44 (MLS): Adversarial Machine Learning: Evasion Attacks

Primary:

- Biggio, B., Corona, I., Maiorca, D., Nelson, B., Å rndiÄ‡, N., Laskov, P., ... & Roli, F. (2013, September). Evasion attacks against machine learning at test time. In Joint European conference on machine learning and knowledge discovery in databases (pp. 387-402). Springer, Berlin, Heidelberg.

Secondary:

- Su, J., Vargas, D. V., & Sakurai, K. (2019). One pixel attack for fooling deep neural networks. IEEE Transactions on Evolutionary Computation, 23(5), 828-841.
- Gao, J., Lanchantin, J., Soffa, M. L., & Qi, Y. (2018, May). Black-box generation of adversarial text sequences to evade deep learning classifiers. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 50-56). IEEE.
- Demontis, A., Melis, M., Pintor, M., Jagielski, M., Biggio, B., Oprea, A., ... & Roli, F. (2019). Why do adversarial attacks transfer? explaining transferability of evasion and poisoning attacks. In 28th {USENIX} Security Symposium ({USENIX} Security 19) (pp. 321-338).

Topic 45 (MLS): GANs for Attack Sample Generation

Primary:

- Trehan, H., & Troia, F. D. (2021, December). Fake Malware Generation Using HMM and GAN. In Silicon Valley Cybersecurity Conference (pp. 3-21). Springer, Cham.

Secondary:

- Andresini, G., Appice, A., De Rose, L., & Malerba, D. (2021). GAN augmentation to deal with imbalance in imaging-based intrusion detection. Future Generation Computer Systems, 123, 108-127.
- Lu, D., Fei, J., Liu, L., & Li, Z. (2022, June). A GAN-based Method for Generating SQL Injection Attack Samples. In 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) (Vol. 10, pp. 1827-1833). IEEE.

Topic 46 (MLS): Machine Learning in Intrusion Detection Systems

Primary:

- Parkar, P., & Bilimoria, A. (2021, May). A survey on cyber security IDS using ML methods. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 352-360). IEEE.

Secondary:

- Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber

security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840.
- Pooja, T. S., & Shrinivasacharya, P. (2021). Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security. Global Transitions Proceedings, 2(2), 448-454.

Topic 47 (Social Networks): Fake Account Detection on Instagram

Primary:
- Sheikhi, S. (2020). An Efficient Method for Detection of Fake Accounts on the Instagram Platform. Rev. d'Intelligence Artif., 34(4), 429-436.

Secondary:
- Akyon, F. C., & Kalfaoglu, M. E. (2019). Instagram fake and automated account detection. In 2019 Innovations in Intelligent Systems and Applications Conference (ASYU) (pp. 1-7). IEEE.
- Purba, K. R., Asirvatham, D., & Murugesan, R. K. (2020). Classification of instagram fake users using supervised machine learning algorithms. International Journal of Electrical and Computer Engineering, 10(3), 2763.

Topic 48 (Social Networks): Social Network Analysis

Primary:
- Rout, D., Bontcheva, K., PreoÅ£iuc-Pietro, D., & Cohn, T. (2013, May). Where's@ wally? a classification approach to geolocating users based on their social ties. In Proceedings of the 24th ACM Conference on Hypertext and Social Media (pp. 11-20).

Secondary:
- Can, U., & Alatas, B. (2019). A new direction in social network analysis: Online social network analysis problems and applications. Physica A: Statistical Mechanics and its Applications, 535, 122372.
- Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. Expert Systems with Applications, 67, 49-58.
- Vosecky, J., Hong, D., & Shen, V. Y. (2009, July). User identification across multiple social networks. In 2009 first international conference on networked digital technologies (pp. 360-365). IEEE.

Topic 49 (Social Networks): Fake Engagement on Instagram

Primary:
- Thejas, G. S., Soni, J., Chandna, K., Iyengar, S. S., Sunitha, N. R., & Prabakar, N. (2019, April). Learning-based model to fight against fake like clicks on instagram posts. In 2019 SoutheastCon (pp. 1-8). IEEE.

Secondary:
- Zarei, K., Farahbakhsh, R., & Crespi, N. (2020, June). How impersonators exploit Instagram to generate fake engagement?. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

Topic 50 (Social Networks): Private data inference from Social Networks

Primary:
- Fang, Q., Sang, J., Xu, C., & Hossain, M. S. (2015). Relational user attribute inference in social media. IEEE Transactions on Multimedia, 17(7), 1031-1044.

Secondary:

Han, X., Huang, H., & Wang, L. (2019). F-PAD: Private attribute disclosure risk estimation in online social networks. IEEE Transactions on Dependable and Secure Computing, 16(6), 1054-1069.
- Mao, J., Tian, W., Yang, Y., & Liu, J. (2019). An efficient social attribute inference scheme based on social links and attribute relevance. IEEE Access, 7, 153074-153085.

Topic 51 (Software Security): Understand humans approach to Reverse Engineering

Primary:
- Mantovani, A., Aonzo, S., Fratantonio, Y., & Balzarotti, D. (2022). {RE-Mind}: a First Look Inside the Mind of a Reverse Engineer. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 2727-2745).

Secondary:
- Votipka, D., Rabin, S., Micinski, K., Foster, J. S., & Mazurek, M. L. (2020). An Observational Investigation of Reverse {Engineersâ€™} Processes. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 1875-1892).
- Burk, K., Pagani, F., Kruegel, C., & Vigna, G. (2022). Decomperson: How Humans Decompile and What We Can Learn From It. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 2765-2782).

Topic 52 (Software Security): Find and exploit vulnerabilities

Primary:
- Shoshitaishvili, Y., Wang, R., Salls, C., Stephens, N., Polino, M., Dutcher, A., ... & Vigna, G. (2016, May). Sok:(state of) the art of war: Offensive techniques in binary analysis. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 138-157). IEEE.

Secondary:
- One, A. (1996). Smashing the stack for fun and profit. Phrack magazine, 7(49), 14-16.
- Bao, T., Wang, R., Shoshitaishvili, Y., & Brumley, D. (2017, May). Your exploit is mine: Automatic shellcode transplant for remote exploits. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 824-839). IEEE.
- Shoshitaishvili, Y., Bianchi, A., Borgolte, K., Cama, A., Corbetta, J., Disperati, F., ... & Vigna, G. (2018). Mechanical phish: Resilient autonomous hacking. IEEE Security & Privacy, 16(2), 12-22.

Topic 53 (Software Security): Fuzzing

Primary:
- Fioraldi, A., Maier, D., EiÃŸfeldt, H., & Heuse, M. (2020). {AFL++}: Combining Incremental Steps of Fuzzing Research. In 14th USENIX Workshop on Offensive Technologies (WOOT 20).

Secondary:
- Zhang, Z., Patterson, Z., Hicks, M., & Wei, S. (2022). {FIXREVERTER}: A Realistic Bug Injection Methodology for Benchmarking Fuzz Testing. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 3699-3715).
- Hernandez, G., Muench, M., Maier, D., Milburn, A., Park, S., Scharnowski, T., ... & Butler, K. R. (2022, January). FIRMWIRE: Transparent Dynamic Analysis for Cellular Baseband Firmware. In 29th Annual Network and Distributed System Security Symposium, NDSS.

Topic 54 (5G Security): 5G new radio Handover Security

Primary:

- Giordani, M., Polese, M., Roy, A., Castor, D., & Zorzi, M. (2018). A tutorial on beam management for 3GPP NR at mmWave frequencies. IEEE Communications Surveys & Tutorials, 21(1), 173-196.

Secondary:

- Zhao, D., Yan, Z., Wang, M., Zhang, P., & Song, B. (2021). Is 5G Handover Secure and Private? A Survey. IEEE Internet of Things Journal.
- Peltonen, A., Sasse, R., & Basin, D. (2021, May). A Comprehensive Formal Analysis of 5G Handover. In 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM.

Topic 55 (5G Security): Open Radio Access Network

Primary:

- Mimran, D., Bitton, R., Kfir, Y., Klevansky, E., Brodt, O., Lehmann, H., ... & Shabtai, A. (2022). Security of Open Radio Access Networks. Computers & Security, 122, 102890.

Secondary:

- Mimran, D., Bitton, R., Kfir, Y., Klevansky, E., Brodt, O., Lehmann, H., ... & Shabtai, A. (2022). Evaluating the Security of Open Radio Access Networks. arXiv preprint arXiv:2201.06080.
- Abdalla, A. S., Upadhyaya, P. S., Shah, V. K., & Marojevic, V. (2022). Toward Next Generation Open Radio Access Networks--What O-RAN Can and Cannot Do!. IEEE Network.
- Polese, M., Bonati, L., D'Oro, S., Basagni, S., & Melodia, T. (2022). Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. arXiv preprint arXiv:2202.01032.

Topic 56 (5G Security): Physical layer authentication

Primary:

- Tomasin, S., Zhang, H., Chorti, A., & Poor, H. V. (2022). Challenge-Response Physical Layer Authentication Over Partially Controllable Channels.

Secondary:

- Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., & Srivastava, M. (2015, October). Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 1004-1015).
- Chorti, A., Barreto, A. N., KÃ¶psell, S., Zoli, M., Chafii, M., Sehier, P., ... & Poor, H. V. (2022). Context-aware security for 6G wireless: the role of physical layer security. IEEE Communications Standards Magazine, 6(1), 102-108.

Topic 57 (5G Security): Smart Jamming attacks

Primary:

- Bout, E., Brighente, A., Conti, M., & Loscri, V. (2022, August). FOLPETTI: A Novel Multi-Armed Bandit Smart Attack for Wireless Networks. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-10).

Secondary:

- Yin, W., Hu, P., Zhou, H., Xing, G., & Wen, J. (2022). Jamming attacks and defenses for fast association in IEEE 802.11 ah networks. Computer Networks, 208, 108890.
- Pirayesh, H., & Zeng, H. (2022). Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials.

Topic 58 (MISC): Video forensics

Primary:

- Lukas, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security, 1(2), 205-214.

Secondary:

- Chen, M., Fridrich, J., Goljan, M., & LukÃ¡s, J. (2008). Determining image origin and integrity using sensor noise. IEEE Transactions on information forensics and security, 3(1), 74-90.
- Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., & Tubaro, S. (2012). An overview on video forensics. APSIPA Transactions on Signal and Information Processing, 1.
- Ling, C., BalcÄ±, U., Blackburn, J., & Stringhini, G. (2021, May). A first look at zoombombing. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1452-1467). IEEE.

Topic 59 (MISC): Security in Logic-Locking (Logic-Obfuscation)

Primary:

- Yasin, M., & Sinanoglu, O. (2017, October). Evolution of logic locking. In 2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) (pp. 1-6). IEEE.

Secondary:

- Yasin, M., Sengupta, A., Nabeel, M. T., Ashraf, M., Rajendran, J., & Sinanoglu, O. (2017, October). Provably-secure logic locking: From theory to practice. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1601-1618).
- Xie, Y., & Srivastava, A. (2018). Anti-sat: Mitigating sat attack on logic locking. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 38(2), 199-207.

Topic 60 (MISC): Secure key generation in PUF-based Logic-Locking

Primary:

- Enamul Quadir, M. S., & Chandy, J. A. (2019). Key generation for hardware obfuscation using strong PUFs. Cryptography, 3(3), 17.

Secondary:

- Suh, G. E., & Devadas, S. (2007, June). Physical unclonable functions for device authentication and secret key generation. In 2007 44th ACM/IEEE Design Automation Conference (pp. 9-14). IEEE.
- Kareem, H., & Dunaev, D. (2021, June). Physical Unclonable Functions based Hardware Obfuscation Techniques: A State of the Art. In 2021 16th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

Topic 61 (MISC): Misuses in Wearable Devices

Primary:

- Naveed, M., Zhou, X. Y., Demetriou, S., Wang, X., & Gunter, C. A. (2014, February). Inside Job: Understanding and Mitigating the Threat of External Device Mis-Binding on Android. In NDSS.

Secondary:

- Fereidooni, H., Frassetto, T., Miettinen, M., Sadeghi, A. R., & Conti, M. (2017, July). Fitness trackers: fit for health but unfit for security and privacy. In 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering

Technologies (CHASE) (pp. 19-24). IEEE.

- Rahman, M., Carbunar, B., & Topkara, U. (2015). Secure management of low power fitness trackers. IEEE Transactions on Mobile Computing, 15(2), 447-459.
- Classen, J., Wegemer, D., Patras, P., Spink, T., & Hollick, M. (2018). Anatomy of a vulnerable fitness tracking system: Dissecting the fitbit cloud, app, and firmware. Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies, 2(1), 1-24.

Topic 62 (MISC): Cyber-Threat Intelligence

Primary:

- Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. Computers & Security, 112, 102511.

Secondary:

- Cabana, O., Youssef, A. M., Debbabi, M., Lebel, B., Kassouf, M., Atallah, R., & Agba, B. L. (2021). Threat intelligence generation using network telescope data for industrial control systems. IEEE Transactions on Information Forensics and Security, 16, 3355-3370.
- Barbieri, G., Conti, M., Tippenhauer, N. O., & Turrin, F. (2021, July). Assessing the Use of Insecure ICS Protocols via IXP Network Traffic Analysis. In 2021 International Conference on Computer Communications and Networks (ICCCN) (pp. 1-9). IEEE.

Topic 63 (MISC): Lie Detection

Primary:

- Monaro, M., Galante, C., Spolaor, R., Li, Q. Q., Gamberini, L., Conti, M., & Sartori, G. (2018). Covert lie detection using keyboard dynamics. Scientific reports, 8(1), 1-10.

Secondary:

- Monaro, M., Gamberini, L., & Sartori, G. (2017). The detection of faked identity using unexpected questions and mouse dynamics. PloS one, 12(5), e0177851.
-

Topic 64 (MISC): Security and Privacy in Online Video Games

Primary:

- Conti, M., & Tricomi, P. P. (2020, December). PvP: Profiling Versus Player! Exploiting Gaming Data for Player Recognition. In International Conference on Information Security (pp. 393-408). Springer, Cham.

Secondary:

- Martinovic, D., Ralevich, V., McDougall, J., & Perklin, M. (2014, July). â€œYou are what you playâ€Â : Breaching privacy and identifying users in online gaming. In 2014 Twelfth Annual International Conference on Privacy, Security and Trust (pp. 31-39). IEEE.
- Moon, S., Reidenberg, J. R., & Russell, N. C. (2017). Privacy in Gaming and Virtual Reality Technologies: Review of Academic Literature.

Topic 65 (MISC): Securing microservices architectures during SDLC

Primary:

- Nehme, A., Jesus, V., Mahbub, K., & Abdallah, A. (2019). Securing microservices. IT Professional, 21(1), 42-49.

Secondary:

Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S. (2017). Exploring software security approaches in software development lifecycle: A systematic mapping study. Computer Standards & Interfaces, 50, 107-115.
- Combe, T., Martin, A., & Di Pietro, R. (2016). To docker or not to docker: A security perspective. IEEE Cloud Computing, 3(5), 54-62.

Topic 66 (MISC): Detecting Wireless Sensors

Primary:
- Singh, A. D., Garcia, L., Noor, J., & Srivastava, M. (2021). I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors. In 30th {USENIX} Security Symposium ({USENIX} Security 21).

Secondary:
- Wu, K., & Lagesse, B. (2019, March). Do you see what i see?< subtitle> detecting hidden streaming cameras through similarity of simultaneous observation. In 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom (pp. 1-10). IEEE.
- Cheng, Y., Ji, X., Lu, T., & Xu, W. (2018, May). Dewicam: Detecting hidden wireless cameras via smartphones. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security (pp. 1-13).

Topic 67 (MISC): Textual Captchas

Primary:
- Von Ahn, L., Blum, M., Hopper, N. J., & Langford, J. (2003, May). CAPTCHA: Using hard AI problems for security. In International conference on the theory and applications of cryptographic techniques (pp. 294-311). Springer, Berlin, Heidelberg.

Secondary:
- Bursztein, E., Aigrain, J., Moscicki, A., & Mitchell, J. C. (2014). The end is nigh: Generic solving of text-based CAPTCHAs. In 8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14).
- Chellapilla, K., Larson, K., Simard, P. Y., & Czerwinski, M. (2005, July). Computers beat Humans at Single Character Recognition in Reading based Human Interaction Proofs (HIPs). In CEAS.

Topic 68 (MISC): Covert channel for security and privacy

Primary:
- Zander, S., Armitage, G., & Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials, 9(3), 44-57.

Secondary:
- Ying, X., Bernieri, G., Conti, M., & Poovendran, R. (2019, April). TACAN: Transmitter authentication through covert channels in controller area networks. In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems (pp. 23-34).
- Taylor, J. M., & Sharif, H. R. (2017, December). Enhancing integrity of modbus TCP through covert channels. In 2017 11th International Conference on Signal Processing and Communication Systems (ICSPCS) (pp. 1-6). IEEE.

Topic 69 (MISC): PIN and Password security

Primary:
- Cardaioli, M., Conti, M., Balagani, K., & Gasti, P. (2020, September). Your PIN Sounds

Good! Augmentation of PIN Guessing Strategies via Audio Leakage. In European Symposium on Research in Computer Security (pp. 720-735). Springer, Cham.

Secondary:

- Balagani, K., Cardaioli, M., Conti, M., Gasti, P., Georgiev, M., Gurtler, T., ... & Wu, L. (2019). Pilot: Password and pin information leakage from obfuscated typing videos. Journal of Computer Security, 27(4), 405-425.
- Kim, H., & Huh, J. H. (2012). PIN selection policies: Are they really effective?. computers & security, 31(4), 484-496.

Topic 70 (MISC): Security and privacy of keyboard

Primary:

- Monaco, J. V. (2018, May). Sok: Keylogging side channels. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 211-228). IEEE.

Secondary:

- Cecconello, S., Compagno, A., Conti, M., Lain, D., & Tsudik, G. (2019). Skype & type: Keyboard eavesdropping in voice-over-IP. ACM Transactions on Privacy and Security (TOPS), 22(4), 1-34.
- Anand, S. A., & Saxena, N. (2018, March). Keyboard emanations in remote voice calls: Password leakage and noise (less) masking defenses. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (pp. 103-110).

Topic 71 (MISC): Adversarial attacks on text classification models

Primary:

- Xu, J., & Du, Q. (2020). Texttricker: Loss-based and gradient-based adversarial attacks on text classification models. Engineering Applications of Artificial Intelligence, 92, 103641.

Secondary:

- Xu, J., & Du, Q. (2020). Adversarial attacks on text classification models using layerâ€Â wise relevance propagation. International Journal of Intelligent Systems, 35(9), 1397-1415.

Topic 72 (MISC): Document Anonymization

Primary:

- Han, Q., Molinaro, C., Picariello, A., Sperli, G., Subrahmanian, V. S., & Xiong, Y. (2021). Generating fake documents using probabilistic logic graphs. IEEE Transactions on Dependable and Secure Computing.

Secondary:

- Hassan, F., Sanchez, D., & Domingo-Ferrer, J. (2021). Utility-preserving privacy protection of textual documents via word embeddings. IEEE transactions on knowledge and data engineering.

Topic 73 (MISC): Metaverse Security

Primary:

- Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials.

Secondary:

- Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. Journal of Financial Crime, (ahead-of-print).

- Yarramreddy, A., Gromkowski, P., & Baggili, I. (2018, May). Forensic analysis of immersive virtual reality social applications: a primary account. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 186-196). IEEE.
- Valluripally, S., Gulhane, A., Hoque, K. A., & Calyam, P. (2021). Modeling and defense of social virtual reality attacks inducing cybersickness. IEEE Transactions on Dependable and Secure Computing.

Topic 74 (MISC): Side-Channel Attacks in PaaS Clouds

Primary:

- Zhang, Y., Juels, A., Reiter, M. K., & Ristenpart, T. (2014, November). Cross-tenant side-channel attacks in PaaS clouds. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 990-1003).

Secondary:

- Van't Hof, A., & Nieh, J. (2022). {BlackBox}: A Container Security Monitor for Protecting Containers on Untrusted Operating Systems. In 16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22) (pp. 683-700).
- Fang, C., Wang, H., Nazari, N., Omidi, B., Sasan, A., Khasawneh, K. N., ... & Homayoun, H. (2021). Repttack: Exploiting Cloud Schedulers to Guide Co-Location Attacks. arXiv preprint arXiv:2110.00846.

Last update: 2023-10-02