Android Security

Code - A1
Android Virtualization Technique

Major paper:

- Shi L, Fu J, Guo Z, Ming J.
  “Jekyll and Hyde” is Risky: Shared-Everything Threat Mitigation in Dual-Instance Apps,
  In Mobisys 2019
  - https://dl.acm.org/doi/pdf/10.1145/3307334.3326072

Minor papers:

- Zhang L, Yang Z, He Y, Li M, Yang S, Yang M, Zhang Y, Qian Z.
  App in the Middle: Demystify Application Virtualization in Android and its Security Threats
  In ACM on Measurement and Analysis of Computing Systems (POMACS) 2019
  - https://dl.acm.org/doi/pdf/10.1145/3322205.3311088
- Tongbo Luo, Cong Zheng, Zhi Xu, Xin Ouyang
  ANTI-PLUGIN: DON’T LET YOUR APP PLAY AS AN ANDROID PLUGIN
  In BlackHat Asia 2017
  - https://www.blackhat.com/docs/asia-17/materials/asia-17-Luo-Anti-Plugin-Don't-Let-Your-App-Play-As-An-Android-Plugin-wp.pdf
- Dai D, Li R, Tang J, Davanian H, Yin H
  Parallel Space Traveling: A Security Analysis of App-Level Virtualization in Android
  In ACM Symposium on Access Control Models and Technologies (SACMAT) 2020
  - https://dl.acm.org/doi/pdf/10.1145/3381991.3395608

Code - A2
Security and Privacy Vulnerabilities Detection in Android Apps

Major paper:

- Duc Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, Sascha Fahl
  A Stitch in Time: Supporting Android Developers in Writing Secure Code
  Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS) 2017
  - https://saschafahl.de/static/paper/fixdroid2017.pdf

Minor papers:

- Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H.
  Paranoid Android: Versatile Protection For Smartphones
  Twenty-Sixth Annual Computer Security Applications Conference, ACSAC 2010
  - http://www.syssec-project.eu/m/page-media/3/paranoid-android-acsac10.pdf

- Qian, C., Luo, X., Le, Y., & Gu, G.
  VULHUNTER: TOWARD DISCOVERING VULNERABILITIES IN ANDROID APPLICATIONS
  IEEE Micro, 2015
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7057600

- Ghafari M, Gadient P, Nierstrasz O.
  Security Smells in Android
  IEEE 17th international working conference on source code analysis and manipulation (SCAM). IEEE, 2017
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8090145

Code - A3
Taint Analysis

Major paper:

- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N.
  TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones
  ACM Transactions on Computer Systems (TOCS), 2014
  - https://www.usenix.org/legacy/event/osdi10/tech/full_papers/Enck.pdf

Minor papers:

- F Wei, S Roy, X Ou
  Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps
  ACM Transactions on Privacy and Security, Vol. 21, No. 3, Article 14. 2018.
  - https://dl.acm.org/doi/pdf/10.1145/3183575

- Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., ... & McDaniel, P.
  Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps
  ACM Sigplan Notices, 2014
  - https://dl.acm.org/doi/pdf/10.1145/2666356.2594299

- Sun, M., Wei, T., & Lui, J. C.
  Taintart: A practical multi-level information-flow tracking system for android runtime
  Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016
  - https://dl.acm.org/doi/pdf/10.1145/2976749.2978343

Blockchain

Code - B1
Distributed key management systems in blockchains

Major paper:

- De Ree, M., Mantas, G., Rodriguez, J., Otung, I. E., & Verikoukis, C.
  DISTANT: DIStributed Trusted Authority-based key managemeNT for beyond 5G wireless mobile small cells
  Computer Communications, 2021
  - https://www.sciencedirect.com/science/article/abs/pii/S014036642100236X

Minor papers:

- Pal, O., Alam, B., Thakur, V., & Singh, S.
  Key management for blockchain technology
  ICT Express, 2021
  - https://www.sciencedirect.com/science/article/pii/S2405959519301894

- Matsumoto, S., & Reischuk, R. M.
  IKP: Turning a PKI around with decentralized automated incentives
  Symposium on Security and Privacy (SP). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/7958590

Code - B2
Isogeny-based crytography for PKI in blockchains

Major paper:

- Fernandez-Carames, Tiago M., and Paula Fraga-Lamas.
  Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks
  IEEE access, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8967098

Minor papers:

- Kock, Bor de, Kristian Gjøsteen, and Mattia Veroni.
  Practical isogeny-based key-exchange with optimal tightness
  International Conference on Selected Areas in Cryptography. Springer, Cham, 2020.
  - https://eprint.iacr.org/2020/1165.pdf

Code - B3
Task offloading in mobile blockchains

Major paper:

- Xiao, K., Gao, Z., Shi, W., Qiu, X., Yang, Y., & Rui, L.
  EdgeABC: An architecture for task offloading and resource allocation in the Internet of Things
  Future Generation Computer Systems, 2020
  - https://www.sciencedirect.com/science/article/abs/pii/S0167739X19323738

Minor papers:

- Dou, W., Tang, W., Liu, B., Xu, X., & Ni, Q.
  Blockchain-based mobility-aware offloading mechanism for fog computing services.
  Computer Communications, 2020
  - https://www.sciencedirect.com/science/article/abs/pii/S0140366420319460

Code - B4
Distributed oracle networks truth discovery

Major paper:

- Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., & Kastania, A.
  Astraea: A decentralized blockchain oracle
  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). IEEE, 2018
  - https://ieeexplore.ieee.org/abstract/document/8726819/

Minor papers:

- Peterson, J., & Krug, J.
  Augur: a decentralized, open-source platform for prediction markets
  arXiv preprint arXiv:1501.01042, 2015, 507.
  - https://res.tuoluocaijing.cn/20180517115326-trzn.pdf

- Nelaturu, K., Adler, J., Merlini, M., Berryhill, R., Veira, N., Poulos, Z., & Veneris, A.
  On public crowdsource-based mechanisms for a decentralized blockchain oracle.
  IEEE Transactions on Engineering Management, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9113449

Code - B5
Integration of Federated learning and Blockchain for data sharing

Major paper:

- Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G.
  Federated learning-based anomaly detection for IoT security attacks.
  IEEE Internet of Things Journal, 2021.
  - https://ieeexplore.ieee.org/iel7/6488907/6702522/09424138.pdf

Minor papers:

- Briggs, C., Fan, Z., & Andras, P.
  A review of privacy-preserving federated learning for the Internet-of-Things.
  Federated Learning Systems, 2021
  - https://arxiv.org/abs/2004.11794

- Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O.
  Federated deep learning for zero-day botnet attack detection in IoT edge devices
  IEEE Internet of Things Journal, 2021.
  - https://ieeexplore.ieee.org/document/9499122?

CPS

Code - C1
Anomaly Detection in Industrial Systems

Major paper:

- Ahmed, M., Mahmood, A. N., & Hu, J.
  A survey of network anomaly detection techniques
  Journal of Network and Computer Applications, 2016
  - https://www.sciencedirect.com/science/article/pii/S1084804515002891

Minor papers:

- Bernieri, G., Conti, M., & Turrin, F
  Evaluation of machine learning algorithms for anomaly detection in industrial networks.
  IEEE International Symposium on Measurements & Networking (M&N). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8805036

- Ditzler, G., Roveri, M., Alippi, C., & Polikar, R.
  Learning in nonstationary environments: A survey
  IEEE Computational Intelligence Magazine, 2015
  - https://ieeexplore.ieee.org/abstract/document/7296710

Code - C2
Industrial Control Systems Security

Major paper:

- Adepu, S., Kang, E., & Mathur, A. P.
  Challenges in Secure Engineering of Critical Infrastructure Systems.
  34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8967443

Minor papers:

- Hemsley, K., & Fisher, R.
  A history of cyber incidents and threats involving industrial control systems.
  International Conference on Critical Infrastructure Protection. Springer, Cham, 2018
  - https://link.springer.com/chapter/10.1007/978-3-030-04537-1_12

- Adepu, S., Kang, E., & Mathur, A. P.
  Challenges in Secure Engineering of Critical Infrastructure Systems
  34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8967443

Code - C3
Industrial Honeypot

Major paper:

- López-Morales, E., Rubio-Medrano, C., Doupé, A., Shoshitaishvili, Y., Wang, R., Bao, T., & Ahn, G. J.
  HoneyPLC: A next-generation honeypot for industrial control systems.
  Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020
  - https://dl.acm.org/doi/abs/10.1145/3372297.3423356

Minor papers:

- Wilhoit K, Hilt S.
  The GasPot Experiment: Unexamined Perils in Using.
  A TrendLabs Research Paper
  - https://documents.trendmicro.com/assets/wp/wp_the_gaspot_experiment.pdf

- You, J., Lv, S., Sun, Y., Wen, H., & Sun, L.
  HoneyVP: A Cost-Effective Hybrid Honeypot Architecture for Industrial Control Systems.
  /ICC 2021-IEEE International Conference on Communications. IEEE, 2021
  - https://ieeexplore.ieee.org/abstract/document/9500567

Code - C4
Air - Ground communication

Major paper:

- Strohmeier, M., Martinovic, I., & Lenders, V.
  Securing the air–ground link in aviation.
  The Security of Critical Infrastructures. Springer, Cham, 2020
  - https://link.springer.com/chapter/10.1007/978-3-030-41826-7_9

Minor papers:

- Olive, X., Tanner, A., Strohmeier, M., Schäfer, M., Feridun, M., Tart, A., ... & Lenders, V.
  OpenSky Report 2020: Analysing in-flight emergencies using big data.
  AIAA/IEEE 39th Digital Avionics Systems Conference (DASC). IEEE, 2020
  - http://www.cs.ox.ac.uk/files/12039/OpenSky%20Report%202020.pdf

- Darabseh, A., AlKhzaimi, H., & Pöpper, C.
  MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors.
  Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2020

- https://dl.acm.org/doi/abs/10.1145/3395351.3399361

- Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R.
  Detecting ADS-B spoofing attacks using deep neural networks
  IEEE conference on communications and network security (CNS). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8802732

Code - C5
NFC Security - SDR receiver-transmitter

Major paper:

- Gummeson, J. J., Priyantha, B., Ganesan, D., Thrasher, D., & Zhang, P. |
  EnGarde: Protecting the mobile phone from malicious NFC interactions.
  Proceeding of the 11th annual international conference on Mobile systems, applications, and services. 2013
  - https://dl.acm.org/doi/abs/10.1145/2462456.2464455

Minor papers:

- Le Roy, F., Quiniou, T., Mansour, A., Lababidi, R., & Le Jeune, D.
  RFID Eavesdropping Using SDR Platforms
  International Conference on Applications in Electronics Pervading Industry, Environment and Society. Springer, Cham, 2016
  - https://link.springer.com/chapter/10.1007/978-3-319-55071-8_27

- Erb, M., Steger, C., Troyer, M., & Preishuber-Pfluegl, J.
  Towards fully interoperable NFC devices
  IEEE International Conference on RFID (RFID). IEEE, 2020
  - https://ieeexplore.ieee.org/document/9244914

- Zhang, L., Xu, H., Dai, Y., & Min, H.
  An NFC system with high sensitivity based on SDR
  IEEE 10th International Conference on ASIC. IEEE, 2013
  - https://ieeexplore.ieee.org/abstract/document/6812011/

Code - C6
IoT security

Major paper:

- Ambrosin, M., Conti, M., Ibrahim, A., Neven, G., Sadeghi, A. R., & Schunter, M.
  SANA: Secure and scalable aggregate network attestation.
  Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016
  - https://dl.acm.org/doi/abs/10.1145/2976749.2978335

Minor papers:

- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P.
  Blockchain for IoT security and privacy: The case study of a smart home
  IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/7917634

- Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I.
  Internet of things (IoT) security: Current status, challenges and prospective measures
  10th international conference for internet technology and secured transactions (ICITST). IEEE, 2015
  - https://ieeexplore.ieee.org/abstract/document/7412116

- Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D.
  IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?
  IEEE Signal Processing Magazine, 2018
  - https://ieeexplore.ieee.org/abstract/document/8454402

Code - C7
Identity of Things

Major paper:

- Mahalle, P., Babar, S., Prasad, N. R., & Prasad, R.
  Identity management framework towards internet of things (IoT): Roadmap and key challenges.
  International Conference on Network Security and Applications. Springer, Berlin, Heidelberg, 2010
  - https://link.springer.com/chapter/10.1007/978-3-642-14478-3_43

Minor papers:

- Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., & Kayssi, A.
  Identity-based authentication scheme for the Internet of Things
  IEEE Symposium on Computers and Communication (ISCC). IEEE, 2016
  - https://ieeexplore.ieee.org/abstract/document/7543884

- Lam K Y, Chi C H.
  Identity in the Internet-of-Things (IoT): New challenges and opportunities
  International Conference on Information and Communications Security. Springer, Cham, 2016
  - https://link.springer.com/chapter/10.1007/978-3-319-50011-9_2

- Zhu X, Badr Y.
  Identity management systems for the internet of things: a survey towards blockchain solutions
  Sensors, 2018
  - https://www.mdpi.com/1424-8220/18/12/4215

Code - C8
Cyber-Physical Anomaly Detection

Major paper:

- Marchetti M, Stabili D.
  Anomaly detection of CAN bus messages through analysis of ID sequences
  IEEE Intelligent Vehicles Symposium (IV). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/7995934

Minor papers:

- Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D.
  Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities
  ACM Computing Surveys (CSUR), 2021
  - https://dl.acm.org/doi/pdf/10.1145/3453155

- Xu, Q., Ali, S., & Yue, T.
  Digital twin-based anomaly detection in cyber-physical systems
  14th IEEE Conference on Software Testing, Verification and Validation (ICST). IEEE, 2021
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9438560

Code - C9
Advanced security on Industrial Control System

Major paper:

- Tychalas, D., Benkraouda, H., & Maniatakos, M.
  ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in ICS Control Applications
  30th USENIX Security Symposium (USENIX Security 21). 2021
  - https://www.usenix.org/system/files/sec21-tychalas.pdf

Minor papers:

- Sarkar E, Benkraouda H, Maniatakos M.
  I came, I saw, I hacked: Automated Generation of Process-independent Attacks for Industrial Control Systems
  Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020
  - https://dl.acm.org/doi/abs/10.1145/3320269.3384730

- Wang, X., Konstantinou, C., Maniatakos, M., Karri, R., Lee, S., Robison, P., ... & Kim, S.
  Malicious firmware detection with hardware performance counters
  IEEE Transactions on Multi-Scale Computing Systems, 2016
  - https://ieeexplore.ieee.org/abstract/document/7470546

Code - C10
Private Information Retrieval (PIR) for healthcare

Major paper:

- Lai, J., Mu, Y., Guo, F., Jiang, P., & Susilo, W.
  Privacy-enhanced attribute-based private information retrieval
  Information sciences, 2018
  - https://www.sciencedirect.com/science/article/abs/pii/S0020025518303530

Minor papers:

- Domingo-Ferrer, J., Bras-Amorós, M., Wu, Q., & Manjón, J.
  User-private information retrieval based on a peer-to-peer community
  Data & Knowledge Engineering, 2009
  - https://www.sciencedirect.com/science/article/abs/pii/S0169023X09000937

Code - C11
Privacy for Vehicular Networks - Ride-Hailing Service

Major paper:

- Pham, A., Dacosta, I., Endignoux, G., Pastoriza, J. R. T., Huguenin, K., & Hubaux, J. P.
  ORide: A Privacy-Preserving yet Accountable Ride-Hailing Service
  26th USENIX Security Symposium (USENIX Security 17). 2017
  - https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/pham

Minor papers:

- Luo, Y., Jia, X., Fu, S., & Xu, M.
  pRide: Privacy-preserving ride matching over road networks for online ride-hailing service
  IEEE Transactions on Information Forensics and Security, 2018
  - https://ieeexplore.ieee.org/document/8565927

- Xie H, Guo Y, Jia X.
  A privacy-preserving online ride-hailing system without involving a third trusted server
  IEEE Transactions on Information Forensics and Security, 2021
  - https://ieeexplore.ieee.org/document/9376938/

Code - C12
Privacy for Vehicular Networks - Traffic Monitoring

Major paper:

- Hoh, B., Gruteser, M., Herring, R., Ban, J., Work, D., Herrera, J. C., ... & Jacobson, Q.
  Virtual trip lines for distributed privacy-preserving traffic monitoring.
  Proceedings of the 6th international conference on Mobile systems, applications, and services. 2008
  - https://dl.acm.org/doi/10.1145/1378600.1378604

Minor papers:

- Li, M., Zhu, L., & Lin, X.
  Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing
  IEEE Transactions on Services Computing, 2019.
  - https://ieeexplore.ieee.org/document/8658122

- Wang, Y., Ding, Y., Wu, Q., Wei, Y., Qin, B., & Wang, H.
  Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs
  IEEE Transactions on Information Forensics and Security, 2018
  - https://ieeexplore.ieee.org/document/8566002/

Code - C13
Privacy for Vehicular Networks - Smart Parking

Major paper:

- Lu, R., Lin, X., Zhu, H., & Shen, X.
  SPARK: A new VANET-based smart parking scheme for large parking lots
  IEEE INFOCOM 2009. IEEE, 2009
  - https://ieeexplore.ieee.org/document/5062057

Minor papers:

- Zhu, L., Li, M., Zhang, Z., & Qin, Z.
  ASAP: An anonymous smart-parking and payment scheme in vehicular networks
  IEEE Transactions on Dependable and Secure Computing, 2018
  - https://ieeexplore.ieee.org/document/8396301/

- Ni J, Lin X, Shen X.
  Toward privacy-preserving valet parking in autonomous driving era
  IEEE Transactions on Vehicular Technology, 2019
  - https://ieeexplore.ieee.org/document/8624339/

Code - C14
Vehicular Security - Automotive Keyless Entry

Major paper:

- Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P.
  Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems
  25th USENIX Security Symposium (USENIX Security 16). 2016.
  - https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

Minor papers:

- Benadjila, R., Renard, M., Lopes-Esteves, J., & Kasmi, C.
  One car, two frames: attacks on hitag-2 remote keyless entry systems revisited
  11th USENIX Workshop on Offensive Technologies (WOOT 17). 2017
  - https://www.usenix.org/conference/woot17/workshop-program/presentation/benadjila

- Glocker, T., Mantere, T., & Elmusrati, M.
  A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography
  8th International Conference on Information and Communication Systems (ICICS). IEEE, 2017
  - https://www.researchgate.net/publication/311430666

- Wouters, L., Gierlichs, B., & Preneel, B.
  My other car is your car: compromising the Tesla Model X keyless entry system
  IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021
  - https://www.youtube.com/watch?v=36AvYW48JtQ
  - https://pdfs.semanticscholar.org/9aeb/ca93875ed86ef5914a0c9e595efd3ee9fd47.pdf
  - My other car is your car: compromising the Tesla Model X keyless entry system - Lennert Wouters
    https://www.youtube.com/watch?v=36AvYW48JtQ

Code - C15
Vehicular Security - Charging-While-Driving

Major paper:

- Roman, L. F., & Gondim, P. R.
  Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment
  Ad Hoc Networks, 2020
  - https://www.sciencedirect.com/science/article/abs/pii/S1570870519303609

Minor papers:

- Li, H., Dán, G., & Nahrstedt, K.
  FADEC: Fast authentication for dynamic electric vehicle charging
  IEEE Conference on Communications and Network Security (CNS). IEEE, 2013
  - https://ieeexplore.ieee.org/document/6682732

- Li, H., Dán, G., & Nahrstedt, K.
  Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging
  IEEE Transactions on Smart Grid, 2016
  - https://experts.illinois.edu/en/publications/portunes-privacy-preserving-fast-authentication-for-dynamic-elect-2

Code - C16
Vehicular Security - CAN Security

Major paper:

- Groza, B., Popa, L., Murvay, P. S., Elovici, Y., & Shabtai, A.
  CANARY - a reactive defense mechanism for Controller Area Networks based on Active RelaYs
  30th USENIX Security Symposium (USENIX Security 21). 2021
  - https://www.usenix.org/conference/usenixsecurity21/presentation/groza

Minor papers:

- Humayed, A., & Luo, B.
  Using ID-hopping to defend against targeted DoS on CAN
  Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles. 2017
  - https://dl.acm.org/doi/abs/10.1145/3055378.3055382

- Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T.
  Comprehensive experimental analyses of automotive attack surfaces
  20th USENIX Security Symposium (USENIX Security 11). 2011
  - https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces

- Islam R, Refat R U D.
  Improving CAN bus security by assigning dynamic arbitration IDs
  Journal of Transportation Security, 2020
  - https://link.springer.com/article/10.1007/s12198-020-00208-0

Code - C17
Privacy protection of Electric Vehicles Owners

Major paper:

- Alessandro Brighente, Mauro Conti, Denis Donadel, Federico Turrin
  EVScout2.0: Electric Vehicle Profiling Through Charging Profile
  arXiv preprint arXiv:2106.16016, 2021
  - https://arxiv.org/abs/2106.16016

Minor papers:

- Leukam Lako F, Lajoie-Mazenc P, Laurent M.
  Privacy-Preserving Publication of Time-Series Data in Smart Grid
  Security and Communication Networks, 2021
  - https://www.hindawi.com/journals/scn/2021/6643566/

- Saxena, N., Grijalva, S., Chukwuka, V., & Vasilakos, A. V.
  Network security and privacy challenges in smart vehicle-to-grid
  IEEE Wireless Communications, 2017
  - https://ieeexplore.ieee.org/document/7880513

Code - C18
Machine learning techniques for lightweight continuous authentication

Major paper:

- Hou, W., Wang, X., Chouinard, J. Y., & Refaey, A.
  Physical layer authentication for mobile systems with time-varying carrier frequency offsets
  IEEE Transactions on Communications, 2014
  - https://ieeexplore.ieee.org/abstract/document/6804410

Minor papers:

- Brighente, A., Formaggio, F., Di Nunzio, G. M., & Tomasin, S.
  Machine learning for in-region location verification in wireless networks
  IEEE Journal on Selected Areas in Communications, 2019
  - https://ieeexplore.ieee.org/abstract/document/8798661

- Ihsan U, Malaney R, Yan S.
  Machine learning and location verification in vehicular networks
  IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8855920

Code - C19
Vehicular Security - CAN Attacks to error handling

Major paper:

- Serag, K., Bhatia, R., Kumar, V., Celik, Z. B., & Xu, D.
  Exposing New Vulnerabilities of Error Handling Mechanism in CAN
  30th USENIX Security Symposium (USENIX Security 21). 2021
  - https://www.usenix.org/system/files/sec21-serag.pdf

Minor papers:

- Cho K T, Shin K G.
  Error handling of in-vehicle networks makes them vulnerable
  Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016
  - https://dl.acm.org/doi/10.1145/2976749.2978302

- Kulandaivel, Sekar, Jain, Shalabh, Guarajardo, Jorge, and Sekar, Vyas
  CANnon: Reliable and Stealthy Remote Shutdown Attacks via Unaltered Automotive Microcontrollers
  In IEEE Sympoosium on Security and Privacy 2021
  - https://users.ece.cmu.edu/~vsekar/assets/pdf/oakland21_cannon.pdf (URL may be broken)

ICN

Code - D1
Cache Privacy Attacks

Major paper:

- Acs, G., Conti, M., Gasti, P., Ghali, C., Tsudik, G., & Wood, C. A.
  Privacy-aware caching in information-centric networking
  IEEE Transactions on Dependable and Secure Computing, 2017
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7874168

Minor papers:

- Mohaisen, A., Mekky, H., Zhang, X., Xie, H., & Kim, Y.
  Timing attacks on access privacy in information centric networks and countermeasures
  IEEE Transactions on Dependable and Secure Computing, 2014
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6990508

- Acs, G., Conti, M., Gasti, P., Ghali, C., & Tsudik, G.
  Cache privacy in named-data networking
  33rd International Conference on Distributed Computing Systems. IEEE, 2013
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6681574

- Compagno, A., Conti, M., Losiouk, E., Tsudik, G., & Valle, S.
  A proactive cache privacy attack on ndn
  NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9110318

Code - D2
Content Popularity Prediction

Major paper:

- Yao, L., Zeng, Y., Wang, X., Chen, A., & Wu, G.
  Detection and defense of cache pollution based on popularity prediction in named data networking
  IEEE Transactions on Dependable and Secure Computing, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8962195

Minor papers:

- Li, J., Wu, H., Liu, B., Lu, J., Wang, Y., Wang, X., ... & Dong, L
  Popularity-driven coordinated caching in named data networking
  ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS). IEEE, 2012
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7846694

- Cho, K., Lee, M., Park, K., Kwon, T. T., Choi, Y., & Pack, S.
  WAVE: Popularity-based and collaborative in-network caching for content-oriented networks
  2012 Proceedings IEEE INFOCOM Workshops. IEEE, 2012
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6193512

- Zhang, R., Liu, J., Huang, T., & Xie, R.
  Popularity based probabilistic caching strategy design for named data networking
  2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2017
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8116423

Code - D3
Interest Flooding Attacks

Major paper:

- Compagno, A., Conti, M., Gasti, P., & Tsudik, G.
  Poseidon: Mitigating interest flooding DDoS attacks in named data networking
  38th annual IEEE conference on local computer networks. IEEE, 2013
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6761300

Minor papers:

- Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., & Zhang, L.
  Interest flooding attack and countermeasures in named data networking
  IFIP Networking Conference. IEEE, 2013
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6663516

- Salah, H., Wulfheide, J., & Strufe, T.
  Coordination supports security: A new defence mechanism against interest flooding in NDN
  IEEE 40th conference on local computer networks (LCN). IEEE, 2015
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7366285

- Benarfa, A., Hassan, M., Compagno, A., Losiouk, E., Yagoubi, M. B., & Conti, M.
  Chokifa: A new detection and mitigation approach against interest flooding attacks in ndn
  International Conference on Wired/Wireless Internet Communication. Springer, Cham, 2019
  - https://link.springer.com/chapter/10.1007/978-3-030-30523-9_5

Code - D4
Coexistence of TCP/IP and ICN/NDN

Major paper:

- Conti, M., Gangwal, A., Hassan, M., Lal, C., & Losiouk, E.
  The road ahead for networking: A survey on icn-ip coexistence solutions
  IEEE Communications Surveys & Tutorials, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9094202

Minor papers:

- Rahman, A., Trossen, D., Kutscher, D., & Ravindran, R.
  Deployment considerations for information-centric networking
  ICNRG draft, 2018
  - https://tools.ietf.org/id/draft-irtf-icnrg-deployment-guidelines-01.html

Malware Detection

Code - E1
Malware Analysis and Detection Methods

Major paper:

- Alazab, M., Alazab, M., Shalaginov, A., Mesleh, A., & Awajan, A.
  Intelligent mobile malware detection using permission requests and API calls
  Future Generation Computer Systems, 2020
  - https://www.sciencedirect.com/science/article/pii/S0167739X19321223

Minor papers:

- Zhao, Y., Li, L., Wang, H., Cai, H., Bissyandé, T. F., Klein, J., & Grundy, J.
  On the impact of sample duplication in machine-learning-based android malware detection
  ACM Transactions on Software Engineering and Methodology (TOSEM), 2021
  - https://dl.acm.org/doi/abs/10.1145/3446905

- Roopak, S., Thomas, T., & Emmanuel, S. (2020).
  A TAN based hybrid model for android malware detection
  Journal of Information Security and Applications, 2020
  - https://www.sciencedirect.com/science/article/pii/S2214212618308263

Code - E2
Ransomware Detection using Deception Models

Major paper:

- Davies, S. R., Macfarlane, R., & Buchanan, W. J.
  Differential area analysis for ransomware attack detection within mixed file datasets
  Computers & Security, 2021
  - https://www.sciencedirect.com/science/article/pii/S0167404821002017

Minor papers:

- Moussaileb, R., Cuppens, N., Lanet, J. L., & Bouder, H. L.
  A survey on windows-based ransomware taxonomy and detection mechanisms
  ACM Computing Surveys (CSUR), 2021
  - https://dl.acm.org/doi/pdf/10.1145/3453153

- Min, D., Ko, Y., Walker, R., Lee, J., & Kim, Y.
  A Content-based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense
  IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9493745

- Faghihi F, Zulkernine M.
  RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware
  Computer Networks, 2021
  - https://www.sciencedirect.com/science/article/pii/S1389128621001250

Code - E3
Adversarial Machine Learning on Malaware

Major paper:

- Maiorca, D., Demontis, A., Biggio, B., Roli, F., & Giacinto, G.
  Adversarial detection of flash malware: Limitations and open issues
  Computers & Security, 2020
  - https://www.sciencedirect.com/science/article/pii/S0167404820301760

Minor papers:

- Demetrio, L., Coull, S. E., Biggio, B., Lagorio, G., Armando, A., & Roli, F.
  Adversarial exemples: a survey and experimental evaluation of practical attacks on machine learning for windows malware detection
  ACM Transactions on Privacy and Security (TOPS), 2021
  - https://arxiv.org/abs/2008.07125

- Demetrio L, Biggio B.
  Secml-malware: Pentesting Windows malware classifiers with adversarial EXEmples in Python
  arXiv preprint arXiv:2104.12848, 2021
  - https://arxiv.org/pdf/2104.12848

Miscellanea

Code - F1
Security in Logic-Locking (Logic-Obfuscation)

Major paper:

- Yasin M, Sinanoglu O.
  Evolution of logic locking
  IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC). IEEE, 2017
  - https://ieeexplore.ieee.org/document/8203496

Minor papers:

- Yasin, M., Sengupta, A., Nabeel, M. T., Ashraf, M., Rajendran, J., & Sinanoglu, O.
  Provably-secure logic locking: From theory to practice
  Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017
  - https://dl.acm.org/doi/10.1145/3133956.3133985

- Xie Y, Srivastava A.
  Anti-SAT: Mitigating SAT attack on logic locking
  IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018
  - https://ieeexplore.ieee.org/document/8279462

Code - F2
Secure key generation in PUF-based Logic-Locking

Major paper:

- Enamul Quadir M S, Chandy J A.
  Key generation for hardware obfuscation using strong PUFs
  Cryptography, 2019
  - https://www.mdpi.com/2410-387X/3/3/17

Minor papers:

- Suh G E, Devadas S.
  Physical unclonable functions for device authentication and secret key generation
  44th ACM/IEEE Design Automation Conference. IEEE, 2007
  - https://ieeexplore.ieee.org/document/4261134

- Kareem H, Dunaev D.
  Physical Unclonable Functions based Hardware Obfuscation Techniques: A State of the Art
  16th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2021
  - https://ieeexplore.ieee.org/abstract/document/9476669

Code - F3
Misuses in Wearable Devices

Major paper:

- Naveed, M., Zhou, X. Y., Demetriou, S., Wang, X., & Gunter, C. A.
  Inside Job: Understanding and Mitigating the Threat of External Device Mis-Binding on Android
  NDSS. 2014
  - https://www.ndss-symposium.org/wp-content/uploads/2017/09/03_5_0.pdf

Minor papers:

- Fereidooni, H., Frassetto, T., Miettinen, M., Sadeghi, A. R., & Conti, M.
  Fitness trackers: fit for health but unfit for security and privacy
  IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2017
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8010569

- Rahman M, Carbunar B, Topkara U.
  Secure management of low power fitness trackers
  IEEE Transactions on Mobile Computing, 2015
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7078927

- Classen, J., Wegemer, D., Patras, P., Spink, T., & Hollick, M.
  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, 2018
  - https://dl.acm.org/doi/pdf/10.1145/3191737

Code - F4
Cyber-Threat Intelligence

Major paper:

- Barbieri, G., Conti, M., Tippenhauer, N. O., & Turrin, F.
  Assessing the Use of Insecure ICS Protocols via IXP Network Traffic Analysis
  International Conference on Computer Communications and Networks (ICCCN). IEEE, 2021
  - https://ieeexplore.ieee.org/abstract/document/9522219

Minor papers:

- Cabana, O., Youssef, A. M., Debbabi, M., Lebel, B., Kassouf, M., Atallah, R., & Agba, B. L.
  Threat Intelligence Generation Using Network Telescope Data for Industrial Control Systems
  IEEE Transactions on Information Forensics and Security, 2021
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9425553

- Torabi, S., Bou-Harb, E., Assi, C., Karbab, E. B., Boukhtouta, A., & Debbabi, M.
  Inferring and investigating IoT-generated scanning campaigns targeting a large network telescope
  IEEE Transactions on Dependable and Secure Computing, 2020
  - https://ieeexplore.ieee.org/abstract/document/9027816

Code - F5
Lie Detection

Major paper:

- Monaro, M., Galante, C., Spolaor, R., Li, Q. Q., Gamberini, L., Conti, M., & Sartori, G.
  Covert lie detection using keyboard dynamics
  Scientific reports, 2018
  - https://www.nature.com/articles/s41598-018-20462-6

Minor papers:

- Jia, Shan, Shuo Wang, Chuanbo Hu, Paula Webster, and Xin Li.
  "Detection of Genuine and Posed Facial Expressions of Emotion: A Review."
  arXiv preprint arXiv:2008.11353 (2020).

- Monaro M, Gamberini L, Sartori G.
  The detection of faked identity using unexpected questions and mouse dynamics
  PloS one, 2017
  - https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0177851

Code - F6
Security and Privacy in Online Video Games

Major paper:

- Conti M, Tricomi P P.
  PvP: Profiling Versus Player! Exploiting Gaming Data for Player Recognition
  International Conference on Information Security. Springer, Cham, 2020
  - https://link.springer.com/chapter/10.1007/978-3-030-62974-8_22

Minor papers:

- Martinovic, D., Ralevich, V., McDougall, J., & Perklin, M.
  “You are what you play”: Breaching privacy and identifying users in online gaming
  Twelfth Annual International Conference on Privacy, Security and Trust. IEEE, 2014
  - https://ieeexplore.ieee.org/document/6890921

- Moon S, Reidenberg J R, Russell N C.
  Privacy in Gaming and Virtual Reality Technologies: Review of Academic Literature[J]. 2017.
  - https://www.fordham.edu/download/downloads/id/10331/privacy_in_gaming_and_virtual_reality_technologies_review_of_academic_literature_2012-2017.pdf

Code - F7
5G new radio Handover Security

Major paper:

- Giordani, M., Polese, M., Roy, A., Castor, D., & Zorzi, M.
  A tutorial on beam management for 3GPP NR at mmWave frequencies
  IEEE Communications Surveys & Tutorials, 2018
  - https://ieeexplore.ieee.org/abstract/document/8458146

Minor papers:

- Zhao, D., Yan, Z., Wang, M., Zhang, P., & Song, B
  Is 5G handover secure and private? A survey
  IEEE Internet of Things Journal, 2021
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9385385

- Peltonen A, Sasse R, Basin D.
  A comprehensive formal analysis of 5G handover
  Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2021
  - https://people.inf.ethz.ch/rsasse/pub/5G-handover-WISEC21.pdf

Code - F8
Securing microservices architectures during SDLC

Major paper:

- Nehme, A., Jesus, V., Mahbub, K., & Abdallah, A.
  Securing microservices
  IT Professional, 2019
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8657392

Minor papers:

- Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S.
  Exploring software security approaches in software development lifecycle: A systematic mapping study
  Computer Standards & Interfaces, 2017
  - https://www.sciencedirect.com/science/article/abs/pii/S0920548916301155

- Combe T, Martin A, Di Pietro R.
  To docker or not to docker: A security perspective
  IEEE Cloud Computing, 2016
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7742298

Code - F9
Detecting Wireless Sensors

Major paper:

- Singh, A. D., Garcia, L., Noor, J., & Srivastava, M.
  I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors
  30th USENIX Security Symposium (USENIX Security 21). 2021
  - https://www.usenix.org/system/files/sec21-singh.pdf

Minor papers:

- Wu K, Lagesse B.
  Do you see what i see?< subtitle> detecting hidden streaming cameras through similarity of simultaneous observation
  IEEE International Conference on Pervasive Computing and Communications (PerCom. IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8767411

- Cheng, Y., Ji, X., Lu, T., & Xu, W.
  Dewicam: Detecting hidden wireless cameras via smartphones
  Proceedings of the 2018 on Asia Conference on Computer and Communications Security. 2018
  - https://dl.acm.org/doi/abs/10.1145/3196494.3196509

Code - F10
Textual Captchas

Major paper:

- Ahn, L. V., Blum, M., Hopper, N. J., & Langford, J.
  CAPTCHA: Using hard AI problems for security
  International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2003
  - https://link.springer.com/chapter/10.1007/3-540-39200-9_18

Minor papers:

- Bursztein, E., Aigrain, J., Moscicki, A., & Mitchell, J. C.
  The End is Nigh: Generic Solving of Text-based CAPTCHAs
  8th USENIX Workshop on Offensive Technologies (WOOT 14). 2014
  - https://www.usenix.org/conference/woot14/workshop-program/presentation/bursztein

- Chellapilla, K., Larson, K., Simard, P. Y., & Czerwinski, M.
  Computers beat Humans at Single Character Recognition in Reading based Human Interaction Proofs (HIPs)
  CEAS. 2005.
  - https://www.microsoft.com/en-us/research/publication/computers-beat-humans-at-single-character-recognition-in-reading-based-human-interaction-proofs-hips/

Code - F11
Covert channel for security and privacy

Major paper:

- Zander S, Armitage G, Branch P.
  A survey of covert channels and countermeasures in computer network protocols
  IEEE Communications Surveys & Tutorials, 2007
  - https://ieeexplore.ieee.org/abstract/document/4317620

Minor papers:

- Ying, X., Bernieri, G., Conti, M., & Poovendran, R.
  TACAN: Transmitter authentication through covert channels in controller area networks
  Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems. 2019
  - https://dl.acm.org/doi/abs/10.1145/3302509.3313783

- Taylor J M, Sharif H R.
  Enhancing integrity of modbus TCP through covert channels
  11th International Conference on Signal Processing and Communication Systems (ICSPCS). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/8270454

Code - F12
PIN and Password security

Major paper:

- Cardaioli, M., Conti, M., Balagani, K., & Gasti, P.
  Your pin sounds good! augmentation of pin guessing strategies via audio leakage
  European Symposium on Research in Computer Security. Springer, Cham, 2020
  - https://link.springer.com/chapter/10.1007/978-3-030-58951-6_35

Minor papers:

- Balagani, K., Cardaioli, M., Conti, M., Gasti, P., Georgiev, M., Gurtler, T., ... & Wu, L.
  Pilot: Password and pin information leakage from obfuscated typing videos
  Journal of Computer Security, 2019
  - https://content.iospress.com/articles/journal-of-computer-security/jcs191289

- Kim H, Huh J H.
  PIN selection policies: Are they really effective?
  computers & security, 2012
  - https://www.sciencedirect.com/science/article/pii/S0167404812000363

Code - F13
Security and privacy of keyboard

Major paper:

- Monaco J V.
  Sok: Keylogging side channels
  IEEE Symposium on Security and Privacy (SP). IEEE, 2018
  - https://ieeexplore.ieee.org/abstract/document/8418605

Minor papers:

- Cecconello, S., Compagno, A., Conti, M., Lain, D., & Tsudik, G.
  Skype & type: Keyboard eavesdropping in voice-over-IP
  ACM Transactions on Privacy and Security (TOPS), 2019
  - https://dl.acm.org/doi/abs/10.1145/3365366

- Anand S A, Saxena N.
  Keyboard emanations in remote voice calls: Password leakage and noise (less) masking defenses
  Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018
  - https://dl.acm.org/doi/abs/10.1145/3176258.3176341

Code - F14
Fake news detection

Major paper:

Peng Qi, Juan Cao, Xirong Li, Huan Liu, Qiang Sheng, Xiaoyue Mi, Qin He, Yongbiao Lv, Chenyang Guo, and Yingchao Yu.
Improving Fake News Detection by Using an Entity-enhanced Framework to Fuse Diverse Multimodal Clues.
Proceedings of the 29th ACM International Conference on Multimedia. 2021
https://doi.org/10.1145/3474085.3481548

Minor papers:

Jing Ma, Wei Gao, Prasenjit Mitra, Sejeong Kwon, Bernard J. Jansen, Kam-Fai Wong, and Meeyoung Cha. 2016.
Detecting rumors from microblogs with recurrent neural networks.
In Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence (IJCAI'16).

Zhou, X., Wu, J., Zafarani, R. (2020).
SAFE: Similarity-Aware Multi-modal Fake News Detection. Advances in Knowledge Discovery and Data Mining.
PAKDD 2020.
https://doi.org/10.1007/978-3-030-47436-2_27

Code - F15
Differential privacy

Major paper:

- Zeyu Ding, Yuxin Wang, Guanhong Wang, Danfeng Zhang, and Daniel Kifer. 2018.
  Detecting Violations of Differential Privacy.
  In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18).
  https://doi.org/10.1145/3243734.3243818

Minor papers:

- Q. Ye, H. Hu, X. Meng and H. Zheng,
  PrivKV: Key-Value Data Collection with Local Differential Privacy,
  2019 IEEE Symposium on Security and Privacy (SP), 2019,
  doi: 10.1109/SP.2019.00018.

M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu and S. Jana,
Certified Robustness to Adversarial Examples with Differential Privacy,
2019 IEEE Symposium on Security and Privacy (SP), 2019,
doi: 10.1109/SP.2019.00044.

MLS

Code - G1
Behavioural Biometrics

Major paper:

- Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I
  Evaluating behavioral biometrics for continuous authentication: Challenges and metrics
  Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. 2017
  - https://dl.acm.org/doi/abs/10.1145/3052973.3053032

Minor papers:

- Bhatt S, Santhanam T.
  Keystroke dynamics for biometric authentication—A survey
  2013 international conference on pattern recognition, informatics and mobile engineering. IEEE, 2013
  - https://ieeexplore.ieee.org/abstract/document/6496441

- Alzubaidi A, Kalita J.
  Authentication of smartphone users using behavioral biometrics
  IEEE Communications Surveys & Tutorials, 2016
  - https://ieeexplore.ieee.org/abstract/document/7423666

Code - G2
Deauthentication

Major paper:

- Kaczmarek T, Ozturk E, Tsudik G.
  Assentication: user de-authentication and lunchtime attack mitigation with seated posture biometric
  International Conference on Applied Cryptography and Network Security. Springer, Cham, 2018
  - https://arxiv.org/abs/1708.03978

Minor papers:

- Conti, M., Lovisotto, G., Martinovic, I., & Tsudik, G.
  Fadewich: fast deauthentication over the wireless channel
  IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/7980185

- Mare, S., Markham, A. M., Cornelius, C., Peterson, R., & Kotz, D.
  Zebra: Zero-effort bilateral recurring authentication
  IEEE Symposium on Security and Privacy. IEEE, 2014
  - https://ieeexplore.ieee.org/document/6956596

Code - G3
Security of Machine Learning Implementations

Major paper:

- Xiao, Q., Chen, Y., Shen, C., Chen, Y., & Li, K.
  Seeing is not believing: Camouflage attacks on image scaling algorithms
  28th USENIX Security Symposium (USENIX Security 19). 2019
  - https://www.usenix.org/system/files/sec19-xiao.pdf
  - https://www.usenix.org/conference/usenixsecurity19/presentation/xiao

Minor papers:

- Pajola L, Conti M.
  Fall of Giants: How popular text-based MLaaS fall against a simple evasion attack
  IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2021
  - https://arxiv.org/abs/2104.05996

Code - G4
Hate Speech Detection on Online Platforms

Major paper:

- Gröndahl, T., Pajola, L., Juuti, M., Conti, M., & Asokan, N.
  All you need is" love" evading hate speech detection
  Proceedings of the 11th ACM workshop on artificial intelligence and security. 2018
  - https://dl.acm.org/doi/abs/10.1145/3270101.3270103

Minor papers:

- Kiela, D., Firooz, H., Mohan, A., Goswami, V., Singh, A., Ringshia, P., & Testuggine, D.
  The hateful memes challenge: Detecting hate speech in multimodal memes
  Advances in Neural Information Processing Systems, 2020
  - https://arxiv.org/abs/2005.04790

- Schmidt A, Wiegand M.
  A survey on hate speech detection using natural language processing
  Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media, April 3, 2017, Valencia, Spain. Association for Computational Linguistics, 2019
  - https://aclanthology.org/W17-1101.pdf

Code - G5
The role of generative models in Cybersecurity

Major paper:

- Yinka-Banjo C, Ugot O A.
  A review of generative adversarial networks and its application in cybersecurity
  Artificial Intelligence Review, 2020
  - https://link.springer.com/article/10.1007/s10462-019-09717-4

Minor papers:

- Zhang X, Karaman S, Chang S F.
  Detecting and simulating artifacts in gan fake images
  IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2019
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9035107

- Ye, G., Tang, Z., Fang, D., Zhu, Z., Feng, Y., Xu, P., ... & Wang, Z.
  Yet another text captcha solver: A generative adversarial network based approach
  Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018
  - https://dl.acm.org/doi/abs/10.1145/3243734.3243754

Code - G6
Continuous Authentication

Major paper:

- Feng H, Fawaz K, Shin K G.
  Continuous authentication for voice assistants
  Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. 2017
  - https://dl.acm.org/doi/pdf/10.1145/3117811.3117823

Minor papers:

- Camara, C., Peris-Lopez, P., Gonzalez-Manzano, L., & Tapiador, J.
  Real-time electrocardiogram streams for continuous authentication
  Applied Soft Computing, 2018
  - https://www.sciencedirect.com/science/article/pii/S156849461730443X

- Liang, Y., Samtani, S., Guo, B., & Yu, Z.
  Behavioral biometrics for continuous authentication in the Internet-of-Things era: An artificial intelligence perspective
  IEEE Internet of Things Journal, 2020
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9121981

Code - G7
Evaluation of Adversarial Attacks on Privacy Preserving Machine Learning Models

Major paper:

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

- https://dl.acm.org/doi/pdf/10.1145/3437880.3460403

Minor papers:

- Liu, X., Li, H., Xu, G., Chen, Z., Huang, X., & Lu, R.
  Privacy-enhanced federated learning against poisoning adversaries
  IEEE Transactions on Information Forensics and Security, 2021
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9524709

- Costa, G., Pinelli, F., Soderi, S., & Tolomei, G
  Covert Channel Attack to Federated Learning Systems
  arXiv preprint arXiv:2104.10561, 2021.
  - https://arxiv.org/pdf/2104.10561

Code - G8
Adversarial Machine Learning: Evasion Attacks

Major paper:

- Biggio, B., Corona, I., Maiorca, D., Nelson, B., Šrndić, N., Laskov, P., and Roli, F.
  Evasion attacks against machine learning at test time
  Joint European conference on machine learning and knowledge discovery in databases. Springer, Berlin, Heidelberg, 2013
  - https://link.springer.com/chapter/10.1007/978-3-642-40994-3_25

Minor papers:

- Su J, Vargas D V, Sakurai K.
  One pixel attack for fooling deep neural networks
  IEEE Transactions on Evolutionary Computation, 2019
  - https://ieeexplore.ieee.org/abstract/document/8601309

- Gao, J., Lanchantin, J., Soffa, M. L., & Qi, Y.
  Black-box generation of adversarial text sequences to evade deep learning classifiers
  IEEE Security and Privacy Workshops (SPW). IEEE, 2018
  - https://ieeexplore.ieee.org/abstract/document/8424632

- Demontis, A., Melis, M., Pintor, M., Jagielski, M., Biggio, B., Oprea, A., ... & Roli, F.
  Why do adversarial attacks transfer? explaining transferability of evasion and poisoning attacks
  28th USENIX security symposium (USENIX security 19). 2019
  - https://www.usenix.org/conference/usenixsecurity19/presentation/demontis

Multimedia Forensics

Code - H1
Adversarial Multimedia Forensics

Major paper:

- Barni, M., Costanzo, A., Nowroozi, E., & Tondi, B.
  CNN-based detection of generic contrast adjustment with JPEG post-processing
  25th IEEE International Conference on Image Processing (ICIP). IEEE, 2018
  - https://ieeexplore.ieee.org/abstract/document/8451698

Minor papers:

- Nowroozi, E., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R.
  A survey of machine learning techniques in adversarial image forensics
  Computers & Security, 2021
  - https://www.sciencedirect.com/science/article/pii/S0167404820303655

- Barni M, Nowroozi E, Tondi B.
  Higher-order, adversary-aware, double jpeg-detection via selected training on attacked samples
  25th European signal processing conference (EUSIPCO). IEEE, 2017
  - https://ieeexplore.ieee.org/abstract/document/8081213

Code - H2
Adversarial Multimedia Forensics - Security

Major paper:

- Barni M, Nowroozi E, Tondi B.
  Detection of adaptive histogram equalization robust against JPEG compression
  International Workshop on Biometrics and Forensics (IWBF). IEEE, 2018
  - https://ieeexplore.ieee.org/abstract/document/8401564

Minor papers:

- Barni, M., Nowroozi, E., Tondi, B., & Zhang, B.
  Effectiveness of random deep feature selection for securing image manipulation detectors against adversarial examples
  ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2020
  - https://ieeexplore.ieee.org/abstract/document/9053318

- Barni M, Nowroozi E, Tondi B.
  Improving the security of image manipulation detection through one-and-a-half-class multiple classification
  Multimedia Tools and Applications, 2020
  - https://link.springer.com/article/10.1007/s11042-019-08425-z

Code - H3
Video forensics

Major paper:

- Lukas J, Fridrich J, Goljan M.
  Digital camera identification from sensor pattern noise
  IEEE Transactions on Information Forensics and Security, 2006
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1634362

Minor papers:

- Chen, M., Fridrich, J., Goljan, M., & Lukás, J.
  Determining image origin and integrity using sensor noise
  IEEE Transactions on information forensics and security, 2008
  - https://ieeexplore.ieee.org/document/4451084

- Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., & Tubaro, S.
  An overview on video forensics
  APSIPA Transactions on Signal and Information Processing, 2012
  - https://www.cambridge.org/core/services/aop-cambridge-core/content/view/585CF8F1CAB9400D215A7C8266A7FB22/S2048770312000029a.pdf

- Ling, C., Balcı, U., Blackburn, J., & Stringhini, G.
  A first look at zoombombing
  IEEE Symposium on Security and Privacy (SP). IEEE, 2021
  - https://arxiv.org/abs/2009.03822

Code - H4
DeepFake Detection

Major paper:

- Alamayreh O, Barni M.
  Detection of GAN-synthesized street videos
  29th European Signal Processing Conference (EUSIPCO). IEEE, 2021
  - https://arxiv.org/abs/2109.04991

Minor papers:

- Barni, M., Kallas, K., Nowroozi, E., & Tondi, B.
  CNN detection of GAN-generated face images based on cross-band co-occurrences analysis
  IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2020
  - https://ieeexplore.ieee.org/abstract/document/9360905

- Ferreira A, Nowroozi E, Barni M.
  VIPPrint: Validating synthetic image detection and source linking methods on a large scale dataset of printed documents
  Journal of Imaging, 2021
  - https://www.mdpi.com/2313-433X/7/3/50

Social Networks

Code - I1
Fake Account Detection on Instagram

Major paper:

- Sheikhi S.
  An Efficient Method for Detection of Fake Accounts on the Instagram Platform
  Rev. d'Intelligence Artif., 2020
  - https://www.iieta.org/journals/ria/paper/10.18280/ria.340407

Minor papers:

- Akyon F C, Kalfaoglu M E.
  Instagram fake and automated account detection
  Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/8946437

- Purba K R, Asirvatham D, Murugesan R K.
  Classification of instagram fake users using supervised machine learning algorithms
  International Journal of Electrical and Computer Engineering, 2020
  - https://pdfs.semanticscholar.org/14f1/b5ab561f3a26d48ca2a46fcebe4c172e37b3.pdf

Code - I2
Social Network Analysis

Major paper:

- Rout, D., Bontcheva, K., Preoţiuc-Pietro, D., & Cohn, T.
  Where's@ wally? a classification approach to geolocating users based on their social ties
  Proceedings of the 24th ACM Conference on Hypertext and Social Media. 2013
  - https://dl.acm.org/doi/abs/10.1145/2481492.2481494

Minor papers:

- Can U, Alatas B.
  A new direction in social network analysis: Online social network analysis problems and applications
  Physica A: Statistical Mechanics and its Applications, 2019
  - https://www.sciencedirect.com/science/article/pii/S0378437119313597

- Colladon A F, Remondi E.
  Using social network analysis to prevent money laundering
  Expert Systems with Applications, 2017
  - https://www.sciencedirect.com/science/article/pii/S0957417416305139

- Vosecky J, Hong D, Shen V Y.
  User identification across multiple social networks
  first international conference on networked digital technologies. IEEE, 2009
  - https://ieeexplore.ieee.org/abstract/document/5272173

Code - I3
Fake Engagement on Instagram

Major paper:

- Thejas, G. S., Soni, J., Chandna, K., Iyengar, S. S., Sunitha, N. R., & Prabakar, N.
  Learning-based model to fight against fake like clicks on instagram posts
  SoutheastCon. IEEE, 2019
  - https://ieeexplore.ieee.org/abstract/document/9020533

Minor papers:

- Zarei K, Farahbakhsh R, Crespi N.
  How impersonators exploit Instagram to generate fake engagement?
  ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020
  - https://ieeexplore.ieee.org/abstract/document/9149431

Code - I4
Private data inference from Social Networks

Major paper:

- Fang, Q., Sang, J., Xu, C., & Hossain, M. S.
  Relational user attribute inference in social media
  IEEE Transactions on Multimedia, 2015
  - https://ieeexplore.ieee.org/abstract/document/7103313

Minor papers:

- Han X, Huang H, Wang L.
  F-PAD: Private attribute disclosure risk estimation in online social networks
  IEEE Transactions on Dependable and Secure Computing, 2019
  - https://ieeexplore.ieee.org/abstract/document/8895669