Online Appendix

1 Data Extraction Form

Table 1: Data type and item extracted from each study and related research questions enclosed in parenthesis

Data Type	ID	Data Item	Description
Qualitative Data	D1	Title	The title of the study.
	D2	Author	The author(s) of the study.
	D3	Venue	Name of the conference or journal where the paper is published.
	D4	Year Published	Publication year of the paper.
	D5	Publisher	The publisher of the paper.
	D6	Summary	A brief summary of the paper along with the major strengths and weaknesses
Context (RQ1)	D7	Security API	The security API that is targeted for misuse detection
	D8	Language	Language of security API under study
Context (RQ2)	D9	Misuses	Misuses of security APIs
	D10	Consequences	Attack types, potential threats or consequences of each misuse type
Context (RQ3)	D11	Technique	Detection techniques including algorithm types and its description
	D12	Modeling Input	Type of data source used for building the detection model
	D13	Testing Input	Type of data source used for testing the detection model
	D14	Output Type	Type of the output generated by detection model
Context (RQ4)	D15	Evaluation Strategy	The method used for evaluation, e.g., manual analysis, user study, or case study
	D16	Evaluation Metrics	The metrics used for evaluating the performance of misuse detection techniques
	D17	Dataset	The dataset(s) used for the evaluation of misuse detection techniques
	D18	Misuses Reported	Misuses identified in the analyzed datasets and their frequency

2 List of Selected Papers

S1 Rahaman S., Xiao Y., Afrose S., Shaon F., Tian K., Frantz M., Kantarcioglu M., Yao D., "Cryptoguard: High precision detection of cryptographic vulnerabilities in massive-sized Java projects", *ACM Conference on Computer and Communications Security (CCS)*, 2019.

S2 Zhang Y., Xiao Y., Kabir M.M.A., Yao D., Meng N., "Example-Based Vulnerability Detection and Repair in Java Code", *IEEE/ACM 30th International Conference on Program Comprehension (ICPC)*, 2022.

S3 Krüger S., Nadi S., Reif M., Ali K., Mezini M., Bodden E., Göpfert F., Günther F., Weinert C., Demmler D., Kamath R., "Cognicrypt: Supporting developers in using cryptography", *IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2017.

S4 Egele M., Brumley D., Fratantonio Y., Kruegel C., "An Empirical Study of Cryptographic Misuse in Android Applications", *ACM SIGSAC Conference on Computer and Communications Security*, 2013.

S5 Nguyen D.C., Wermke D., Acar Y., Backes M., Weir C., Fahl S., "A stitch in time: Supporting Android developers in writing secure code", *ACM Conference on Computer and Communications Security (CCS)*, 2017.

S6 Li Y., Zhang Y., Li J., Gu D., "iCryptoTracer: Dynamic Analysis on Misuse of Cryptography Functions in iOS Applications", *Network and Distributed System Security Symposium (NDSS)*, 2014.

S7 Wang Q., Li J., Zhang Y., Wang H., Hu Y., Li B., Gu D., "NativeSpeaker: Identifying Crypto Misuses in Android Native Code Libraries", *International Conference on Information Security and Cryptology*, 2018.

S8 Tang J., Li J., Li R., Han H., Gu X., Xu Z., "SSLDetecter: Detecting SSL Security Vulnerabilities of Android Applications Based on a Novel Automatic Traversal Method", *Security and Communication Networks*, 2019.

S9 He B., Rastogi V., Cao Y., Chen Y., Venkatakrishnan V.N., Yang R., Zhang Z., "Vetting SSL usage in applications with SSLINT", *IEEE Symposium on Security and Privacy*, 2015.

S10 Piccolboni L., Guglielmo G.D., Carloni L.P., Sethumadhavan S., "CRYLOGGER: Detecting crypto misuses dynamically", *IEEE Symposium on Security and Privacy*, 2021.

S11 Kruger S., Spath J., Ali K., Bodden E., Mezini M., "CrySL: An Extensible Approach to Validating the Correct Usage of Cryptographic APIs", *IEEE Transactions on Software Engineering*, 2019.

S12 Muslukhov I., Boshmaf Y., Beznosov K., "Source attribution of cryptographic API misuse in Android applications", *Asia Conference on Computer and Communications Security.* 2018.

S13 Li J., Lin Z., Caballero J., Zhang Y., Gu D., "K-Hunt: Pinpointing insecure cryptographic keys from execution traces", *ACM SIGSAC Conference on Computer and Communications Security*, 2018.

S14 Fahl S., Harbach M., Muders T., Baumgärtner L., Freisleben B., Smith M., "Why Eve and Mallory love Android: An analysis of Android SSL (in) security", *ACM Conference on Computer and Communications Security (CCS)*, 2012.

S15 Shuai S., Guowei D., Tao G., Tianchang Y., Chenjie S., "Modelling analysis and auto-detection of cryptographic misuse in Android applications", *International Conference on Dependable, Autonomic and Secure Computing*, 2014.

S16 Ma S., Lo D., Li T., Deng R.H., "CDRep: Automatic repair of cryptographic-misuses in Android applications", *ACM Asia Conference on Computer and Communications Security (ASIA CCS)*, 2016.

S17 Singleton L., Zhao R., Song M., Siy H., "Cryptotutor: Teaching secure coding practices through misuse pattern detection", *Annual Conference on Information Technology Education*, 2020.

S18 Xu Z., Hu X., Tao Y., Qin S., "Analyzing Cryptographic API Usages for Android Applications Using HMM and N-Gram", *International Symposium on Theoretical Aspects of Software Engineering (TASE)*, 2020.

S19 Greenwood D.S.J.S.G., Khan Z.L.L., "SMV-hunter: Large scale, automated detection of SSL/TLS man-in-the-middle vulnerabilities in Android apps", *Network and Distributed System Security Symposium (NDSS)*, 2014.

S20 Wickert A.K., Baumgärtner L., Breitfelder F., Mezini M., "Python Crypto Misuses in the Wild", *ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, 2021.

S21 Gu Z., Wu J., Li, C., Zhou M., Gu M., "SSLDoc: Automatically Diagnosing Incorrect SSL API Usages in C Programs", *International Conference on Software Engineering and Knowledge Engineering (SEKE)*, 2019.

S22 Zhang L., Chen J., Diao W., Guo S., Weng J., Zhang K., "CRYPTOREX: Large-scale Analysis of Cryptographic Misuse in IoT Devices", *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019.

S23 Chatzikonstantinou A., Ntantogian C., Karopoulos G., Xenakis C., "Evaluation of cryptography usage in Android applications", *EAI Endorsed Transactions on Security and Safety*, 2016.

S24 Wang Y., Liu X., Mao W., Wang W., "Dcdroid: Automated detection of SSL/TLS certificate verification vulnerabilities in Android apps", *ACM Turing Celebration Conference-China*, 2019.

S25 Rahaman S., Cai H., Chowdhury O.H., Yao D.D., "From Theory to Code: Identifying Logical Flaws in Cryptographic Implementations in C/C++", *IEEE Transactions on Dependable and Secure Computing*, 2021.

S26 Georgiev M., Iyengar S., Jana S., Anubhai R., Boneh D., Shmatikov V., "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software", *ACM Conference on Computer and Communications Security (CCS)*, 2012.

S27 Gajrani J., Tripathi M., Laxmi V., Gaur M.S., Conti M., Rajarajan M., "sPECTRA: a Precise framEwork for analyzing CrypTographic vulneRabilities in Android apps", *IEEE Annual Consumer Communications and Networking Conference (CCNC)*, 2017.

S28 Feichtner J., Missmann D., Spreitzer R., "Automated Binary Analysis on iOS – A Case Study on Cryptographic Misuse in iOS Apps", *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2018.

S29 Paletov R., Tsankov P., Raychev V., Vechev M., "Inferring Crypto API Rules from Code Changes", *ACM SIGPLAN Notices*, 2018.

S30 Rahat T.A., Feng Y., Tian Y., "OAUTHLINT: An Empirical Study on OAuth Bugs in Android Applications", *IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2019.

S31 Zhang Y., Kabir M.M.A., Xiao Y., Yao D.D., Meng N., "Automatic Detection of Java Cryptographic API Misuses: Are We There Yet?", *IEEE Transactions on Software Engineering*, 2022.

S32 Afrose S., Xiao Y., Rahaman S., Miller B., Yao D.D., "Evaluation of Static Vulnerability Detection Tools with Java Cryptographic API Benchmarks", *IEEE Transactions on Software Engineering*, 2022.

S33 Alhanahnah M., Yan Q., "Towards Best Secure Coding Practice for Implementing SSL/TLS", *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018.

S34 Ami A.S., Cooper N., Kafle K., Moran K., Poshyvanyk D., Nadkarni A., "Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques", *IEEE Symposium on Security and Privacy*, 2022.

S35 Backes M., Bugiel S., Derr E., "Reliable Third-Party Library Detection in Android and its Security Applications", *ACM Conference on Computer and Communications Security (CCS)*, 2016.

S36 Gao J., Kong P., Li L., Bissyandé T.F., Klein J., "Negative Results on Mining Crypto-API Usage Rules in Android Apps", *International Conference on Mining Software Repositories (MSR)*, 2019.

S37 Bianchi A., Fratantonio Y., Machiry A., Kruegel C., Vigna G., Chung S.P.H., Lee W., "Broken Fingers: On the Usage of the Fingerprint API in Android", *Network and Distributed System Security Symposium (NDSS)*, 2018.

S38 Piskachev G., Petrasch T., Späth J., Bodden E., "AuthCheck: Program-state Analysis for Access-control Vulnerabilities", *International Symposium on Formal Methods*, 2019.

S39 Oltrogge M., Huaman N., Amft S., Acar Y., Backes M., Fahl S, "Why Eve and Mallory Still Love Android: Revisiting TLS(In) Security in Android Applications", *USENIX Security Symposium*, 2021.

S40 Hazhirpasand M., Ghafari M., Nierstrasz O., "Java Cryptography Uses in the Wild", *International Symposium on Empirical Software Engineering and Measurement*, 2020.

S41 Braga A., Dahab R., Antunes N., Laranjeiro N., Vieira M., "Understanding How to Use Static Analysis Tools for Detecting Cryptography Misuse in Software", *IEEE Transactions on Reliability*, 2019.

S42 Tupsamudre H., Sahu M., Vidhani K., Lodha S., "Fixing the Fixes: Assessing the Solutions of SAST Tools for Securing Password Storage", *Financial Cryptography and Data Security*, 2020.

S43 Gao J., Li L., Kong P., Bissyande T. F., Klein J., "Understanding the Evolution of Android App Vulnerabilities", *IEEE Transactions on Reliability*, 2021.

S44 Wei F., Roy S., Ou X., "Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps", *ACM Conference on Computer and Communications Security (CCS)*, 2014.

S45 Fischer F., Bottinger K., Xiao H, Stransky C., Acar Y., Backes M., Fahl S., "Stack Overflow considered harmful? the impact of copy&paste on Android application security", *IEEE Symposium on Security and Privacy (SP)*, 2017.

S46 Ma S., Thung F., Lo D., Sun C., Deng R. H., "VuRLE: Automatic vulnerability detection and repair by learning from examples", *European Symposium on Research in Computer Security*, 2017.

S47 Wang H., Zhang Y., Li J., Liu H., Yang W., Li B., Gu D., "Vulnerability Assessment of OAuth Implementations in Android Applications", *Computer Security Applications Conference*, 2015.

S48 Eric Y. Chen, Pei Y., Chen S., Tian Y., Kotcher R., Tague P., "OAuth Demystified for Mobile Application Developers", *ACM Conference on Computer and Communications Security (CCS)*, 2014.

S49 Li W., Mitchell C.J., "Security issues in OAuth 2.0 SSO implementations", *Information Security Conference*, 2014.

S50 Sun S.T., Beznosov K., "The devil is in the (implementation) details: an empirical analysis of oauth SSO systems", *ACM Conference on Computer and Communications Security (CCS)*, 2012.

S51 Yang R., Li G., Lau W.C., Zhang K., Hu P., "Model-based Security Testing: an Empirical Study on OAuth 2.0 Implementations", *ACM on Asia Conference on Computer and Communications Security (Asia CCS)*, 2016.

S52 Shernan E., Carter H., Tian D., Traynor P., Butler K., "More guidelines than rules: CSRF vulnerabilities from noncompliant OAuth 2.0 implementations", *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2015.

S53 Calzavara S., Focardi R., Maffei M., Schneidewind C., Squarcina M., Tempesta M., "WPSE: Fortifying Web Protocols via Browser-Side Security Monitoring", *USENIX Security Symposium*, 2018.

S54 Sharif A., Carbone R., Sciarretta G., Ranise S., "Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients", *Journal of Information Security and Applications*, 2022.

S55 Bonifácio R., Krüger S., Narasimhan K., Bodden E., Mezini M., "Dealing with Variability in API Misuse Specification", *European Conference on Object-Oriented Programming*, 2021.

S56 Mitchell D., Kinder J., "A formal model for checking cryptographic API usage in Javascript", *European Symposium on Research in Computer Security*, 2019.

S57 CİBALIK K.E., Koçak C.E.M.A.L., "Detection of SSL/TLS Implementation Errors in Android Applications", *Gazi University Journal of Science Part C: Design and Technology*, 2021.

S58 Wickert A.K., Baumgärtner L., Narasimhan K., Schlichtig M., Mezini M., "To Fix or Not to Fix: A Critical Study of Crypto-misuses in the Wild", *International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021.

S59 Gorski P.L., Iacono L.L., Wermke D., Stransky C., Möller S., Acar Y., Fahl, S., "Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic API Misuse", *Symposium on Usable Privacy and Security*, 2018.

S60 Acar Y., Backes M., Fahl S., Garfinkel S., Kim D., Mazurek M.L., Stransky C., "Comparing the Usability of Cryptographic APIs", *IEEE Symposium on Security and Privacy (SP)*, 2017.

S61 Tony C., Ferreyra N.E.D., Scandariato R., "GitHub Considered Harmful? Analyzing Open-Source Projects for the Automatic Generation of Cryptographic API Call Sequences", *Software Quality, Reliability, and Security*, 2022.

S62 Li W., Jia S., Liu L., Zheng F., Ma Y., Lin J., "CryptoGo: Automatic Detection of Go Cryptographic API Misuses", *Computer Security Applications Conference*, 2022.

S63 Zhao R., Siy H., Pack C., Soh L.K., Song M., "An Intelligent Tutoring System for API Misuse Correction by Instant Quality Feedback", *Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022.

S64 Braga A., Dahab A., "Mining cryptography misuse in online forums", *Software Quality, Reliability, and Security*, 2016.

S65 Rodrigues G.E.D.P., Braga A.M., Dahab R., "Using Graph Embeddings and Machine Learning to Detect Cryptography Misuse in Source Code", *IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2020.

S66 Chen M., Fischer F., Meng N., Wang X., Grossklags J., "How reliable is the crowdsourced knowledge of security implementation", *International Conference on Software Engineering (ICSE)*, 2019.

S67 Wang Y., Xu G., Liu X., Mao W., Si C., Pedrycz W., Wang W., "Identifying vulnerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis", *Journal of Systems and Software*, 2020.

S68 Hue M.H., Debnath J., Leung K.M., Li L., Minaei M., Mazhar M.H., Xian K., Hoque E., Chowdhury O., Chau S.Y., "All your Credentials are Belong to Us: On Insecure WPA2-Enterprise Configurations", *ACM SIGSAC Conference on Computer and Communications Security*, 2021.

S69 Ibrahim M., Imran A., Bianchi A., "SafetyNOT: On the usage of the SafetyNet attestation API in Android", *Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2021.