NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

NATIONALCYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMME (NCR)
CALL FOR PROPOSALS – LETTER OF INTENT (LOI)

All information is treated in confidence. The information is furnished to the National Research Foundation with the understanding that it shall be used or disclosed for evaluation, reference and reporting purposes.

SECTION I:

Proposal ID: NRF2016NCR_NCR001_008 *(generated by RITA)*

Proposal Title: Safety and Privacy of Smart-City Mobile Applications through Model Inference

Budget Requested *(Excluding Indirect Costs)*: **S$ 333,281**

Period of Support: 3 years

Host Institution: Singapore Management University

List of Project Team Members *(Please add/delete rows where necessary)*

Role	***Name***	***Designation***	**School**	**Institution**	**% of time committed on the project**
Lead PI	David Lo	Assistant Professor	School of Information Systems	Singapore Management University	15
Co-PI (1)	Shahar Maoz	Senior Lecturer (equivalent to Assistant Professor)	School of Computer Science	Tel Aviv University	10
Co-PI (2)	Debin Gao	Associate Professor	School of Information Systems	Singapore Management University	10
Co-PI (3)	Eran Tromer	Senior Lecturer	School of Computer Science	Tel Aviv University	5
Co-PI (4)	Eran Toch	Senior Lecturer	Faculty of Engineering	Tel Aviv University	5

SECTION II

Research Objectives

Smart-cities provide new opportunities for organizing and optimizing urban environments, but at the same time they introduce new challenges in securing the city's infrastructure and protecting the safety and privacy of its citizens. As growing number of smart-city operations rely on smartphone mobile applications, the mobile platform becomes a critical point for safety and privacy. Mobile applications can be hacked and compromised. Users' safety and privacy is threatened if applications overreach and mishandle their personal data. Therefore, a basic condition for the success of smart-cities is a trustworthy mobile platform that can empower smart-city operations while providing safety and privacy control for users. With respect to providing a platform for trust, we propose a project, which realizes a system named AppMod*,* with several objectives:

1. *Logging detailed app behaviors*: Designing and evaluating a method to generate rich fine-grained logs capturing app behavior efficiently. Specifically, the method need to track how information flows in an Android app, link related events and their control and data flow dependences, and output them in a succinct log, without sacrificing responsiveness of the app and consuming much energy.
2. *Building and analyzing application process models*: (a) Designing and evaluating a method that infers an expressive model that captures common behaviors of a mobile app. Specifically, the method generates a model that captures control and data flow constraints, which serve as a signature of an app, from rich fine-grained logs of app events. (b) Designing and evaluating a method that efficiently detects violations of an app signature captured in a model. Specifically, the method scans a fine-grained log capturing an app's behavior (in an online or offline fashion) and checks if it deviates from the model by violating some of its control and data flow constraints.
3. *Understanding how users can effectively control their privacy and security in mobile platforms*: Designing and evaluating user interaction models that make use of information flow and program modeling to effectively control access to the data and to foster trust relations with the application. Specifically, we will analyze how different interaction models can help users make informed decisions in an effective way. We will also study how different communities of users, such as power users, senior citizens and children, matching interaction techniques to the digital literacy and cognitive abilities of users.

Approach

The project's approach will be based on developing new techniques for program analysis and usable security, combining theoretical study with empirical analysis of actual applications and user experimentation. To enable the empirical studies, and to provide a practical and meaningful solution, we will focus on the Android OS platform as a testbed for the development, and see how actual smart-city applications can be improved and updated to provide better privacy and to adhere to security standards. We will define new types of cyber security metrics, based on analyzing the differencing factor, how far is the gap between the expected behavior and the actual behavior.

Mobile apps typically perform many highly sensitive operations: interact with end users, manipulate and handle their most private information, perform authentication on their behalf, and access the mobile platform's multitude of sensors and hardware. Apps are thus privileged to perform a wide variety of harmful operations. Many works have sought to define, detect, and prevent harmful or malicious behavior: approaches for dynamic and static information flow analysis (Arzt et al., 2014; Enck et al., 2014) and malware detection (Pandita et al., 2013; Gorla et al. 2014; Avdiienko et al., 2015) have been thoroughly considered. On-device enforcement mechanisms have also been proposed (Jamrozik et al., 2016; Backes et al., 2013), including extending Android to support Information Flow Control (IFC) (Schuster and Tromer, 2016). Some of these mechanisms, such as SEAndroid (Smalley and Craig, 2013), have been successfully integrated into the Android mainline.

Closest to our proposal are on-device enforcement mechanisms (Jamrozik et al., 2016; Backes et al., 2013; Schuster and Tromer, 2016). However, existing work in this area are coarse-grained approaches

that are only based on a set of whitelist APIs (Jamrozik et al., 2016; Backes et al., 2013) or manually specified information flows (Schuster and Tromer, 2016). **Our proposal differentiates itself by introducing a comprehensive model-centric approach that captures fine-grained behavioral properties of an app automatically from typical examples of its executions, along with human-centric user interaction models that allow different communities of users to control their privacy and security needs based on their digital literacy and cognitive abilities.** Our approach, named AppMod, will detect anomalous and potentially harmful behavior and alert the user about it. AppMod will summarize the risk in an informative manner, present it to the users, and give them the opportunity to disallow it, or approve it for current and future runs.

Examples of anomalies that AppMod would highlight include: when an error dialog with a given message is shown in a state where it was not supposed to be (according to the original model), when some parts of an app is invoked in a state where it was not supposed to be, when a permission is used in a state where it was not supposed to be, when a location/contact/file is shared in a state where it was not supposed to be, etc. Once an anomaly is recognized, it can be used in a couple of ways:

1. *In real time, to help the user assess the situation*: We will provide an informative alert about the anomaly, e.g., that the error dialog is different from normal, or this time the app is sending the user's contact list to a different URL.
2. *Sent to a sysadmin/guardian of the user for later review*: Concretely, parents are often extremely concerned with their children's exposure to the virtual world. One use case would be enabling a parent of a 7-year old to learn about anomalous usages of an app's functions, summarized via a series of screenshots the parent can scrutinize at the end of the day. But once a function becomes part of the norm (i.e., part of the inferred model of normal behavior), parents may not want to be bothered with it repeatedly. Notably, since this is not necessarily "malicious or buggy" behavior that parents (or sysadmins) are concerned about, none of the mentioned previous endeavors to improve mobile security have defined and handled such scenarios.

Our implementation will rely on coupling and extending of our model inference and differencing technology, developed in Singapore Management University and Tel Aviv University (Le et al., 2015; Le and Lo, 2015; Fahland et al., 2013; Lo and Maoz, 2012; Lo et al., 2012a; Lo et al., 2012b; Kumar et al., 2012; Maoz et al., 2011a; Maoz et al., 2011b), with Android dynamic analysis capabilities developed in Tel Aviv University (Schuster and Tromer, 2016). We will: (1) Instrument Android OS to output logs of low-level events apps, e.g., Android component life cycle events, inter-component communication (ICC) events, invoking sensitive API; (2) Construct a model of what the app does using model inference; (3) Using model differential analysis, we will identify anomalous behavior that violates previously inferred models; (4) Provide suitable alerts.

The approach of using the user's decisions in mitigating the risk in app behavior is novel, and is applicable to all mobile platforms (our initial focus will be on Android, due to its popularity and availability of open source code). Moreover, it presents challenges that this team of researchers is in a unique position to tackle, given their proven technical and empirical tools.

Program Plan

To carry out the project, we plan 3 overlapping Work Packages (WPs) as listed below. Each WP would be for 3 years. The phases for each WP follow the deliverables that are described later in the proposal. The manpower on the SMU side would include a research fellow (i.e., post-doc) for 35 months, in addition to Lo and Gao. The manpower on the TAU side would include 3 PhD students/research fellows (funded through TAU-ICRC), in addition to Maoz (coordinator), Tromer, and Toch.

Work Package 1: Generation of rich fine-grained logs and stateful model inference

Efficient Logging: We would design and implement an efficient monitoring technique that captures information about application behaviors. Two variants of the technique would be designed and

implemented: a highly efficient variant that builds on top of an emulator, and an on-device monitoring variant that builds on top of an app-specific sandbox. The former is designed to capture app behaviors when AppMod is run on a set of test cases to create an initial model, while the latter is needed to capture app behaviors live when it is used by end users. For either variant, we follow the following process: (1) An app would first be statically analysed to identify a minimal set of locations where instrumentation code need to be injected to capture app behaviors; (2) Next, data and control flow dependencies among events would be identified statically (as much as possible) and dynamically; (3) Finally, a succinct log file would be created when the instrumentation code are executed. An encoding strategy would be designed and implemented such that only a minimal amount of data is written to file.

Model Inference: We would run an existing regression test suite of a target app in an emulator. If the regression test suite is not available or is not comprehensive enough, additional test cases are generated by running an automated test case generation technique specialized for mobile apps, e.g., Monkey (Android, 2016), Dynodroid (Machiry et al., 2013), Puma (Hao et al., 2014), etc. We would generate detailed yet clean logs following CopperDroid which can generate high-level events from low-level ones which are invoked by both Android and native code (Tam et al., NDSS15). These logs would then be analysed to capture data and control flow invariants governing the signature of how the APIs are used in the normal context. We employ a combination of models to capture these invariants. We build upon our previous experience of building behavioural model inference algorithms that mine models in various formats (Le et al., 2015; Le and Lo, 2015; Fahland et al., 2013; Lo and Maoz, 2012; Lo et al., 2012a; Lo et al., 2012b; Kumar et al., 2012). We would integrate these algorithms so as to optimize its performance and reduce redundancies among inferred models. We would also enhance the expressiveness of some of the mined models so as to capture pertinent properties important for detecting anomalous app behaviors.

Work Package 2: Differencing analysis and anomaly detection
Our approach to differencing will build on and extend Maoz et al. recent work on semantic model differencing (Maoz et al. 2011a, Maoz and Ringert 2015), which aims at computing and presenting the semantic differences between two or more models in an efficient and succinct way. While the models themselves may be large and complex, the differences in our context are expected to be small. Thus, it is important that the complexity of computing the differences and presenting them will depend more on the size of the difference than on the size of the models involved. Differences need to be identified and then filtered and selected for presentation, e.g., by presenting only representatives from equivalence classes.

Rather than dealing only with Boolean differences, such as identifying shortest sequences of events that are not possible in the original mined model but happen in the app as it is executed by the end user, we will extend the model differencing techniques to consider quantitative and statistical properties, such as identifying sequences of events that were very rare in the original mined model but are rather frequent in the app as it is executed by the user. This will require incorporating statistical techniques for computing distances between distributions into the model differencing approach. Furthermore, to assist in prioritizing and reducing information overload, the differences found will be accompanied with statistical confidence measures, building on our recent experience in extending model inference with statistical guarantees (Busany and Maoz, 2016).

Work Package 3: Model-based user interaction
The differencing model will serve as the basis for designing and evaluating new types of interaction models. To tackle the cognitive overload of managing large number of privacy decisions, this package will focus on creating new user interfaces to let end-users specify acceptable behavior of their private data based on anomaly definition and context (e.g. no location recording when I am at home), and easily understand the tradeoffs involved (e.g. turning off location data for this app means that the map

functionality will no longer work). This work represents new kind of functionality that has not been previously explored.

We will also explore the notion of communities of users, relying on two observations that are becoming central to human-computer interaction. First, that different groups of users have different needs (e.g., senior citizens vs. teens or power users vs. novice users). The second, that users turn to others in understanding and tackling difficult interaction tasks. We will explore new UIs that engage different groups of users with different models of interactions, and develop new interaction models that allow users to aid others, or to get help, when prompted with privacy decisions. Specifically, we will look at new types of UIs that build on small computities, such as family circles, allowing users to "sponsor" their kids or their parents when making privacy decisions.

Technical Risks and Their Mitigation

Efficient logging: In the event the cost of our logging solution remains prohibitive for it to be deployed live, we plan to reduce the number of events and ask security experts to filter some of the instrumentation points that cover less critical part of an app.

Model inference and anomaly detection: In the event where not all work items can be fully automated with high accuracy, we will design a semi-automated approach that allows for domain experts to provide additional inputs either in the beginning of the process (e.g., by providing a partial model), or during the process (e.g., by designing an active learning methodology that allows security experts and end users to be more involved in the mining and anomaly detection process by providing simple feedback to well-defined questions or tasks). Lo and Maoz have prior experience in designing behavioural model inference approaches that allow users to provide partial answers (Lo and Maoz, 2008), and in designing various active learning approaches (Wang et al., 2014; Lucia et al., 2012; Gong et al., 2012).

User interaction: This stage heavily relies on the previous ones for input, this work package will start by simulating simulate several types of anomalies. Thus, we can start designing and testing the framework without totally relying on previous steps. To mitigate the risk of unusable and unuseful interaction models, we will carry qualitative initial studies with relevant users, understanding how users make similar decisions using today's UIs.

Role of Team Members

Work package 1 would be assigned to Eran Tromer (TAU) and David Lo (SMU) in collaboration with Shahar Maoz (TAU). Tromer would focus on the generation of rich fine-grained logs capturing information flow in apps, while Lo would focus on the inference of expressive and stateful models from a set of logs. Tromer has much experience in instrumenting and generating logs from Android apps (Schuster and Tromer, 2016) while Lo and Maoz has much experience in inferring models from logs (Le et al., 2015; Le and Lo, 2015; Fahland et al., 2013; Lo and Maoz, 2012; Lo et al., 2012a).

Work package 2 would be assigned to Shahar Maoz (TAU) and David Lo (SMU). Maoz has much experience in differencing models (Maoz et al., 2011a; Maoz et al., 2011b) and Lo has worked before on anomaly detection (Milea et al., 2011). Maoz and Lo have collaborated on many past projects (Fahland et al., 2013; Lo and Maoz, 2012).

Work package 3 would be assigned to Debin Gao (SMU) and Eran Toch (TAU) in collaboration with David Lo (SMU). Both Gao, Toch, and Lo have worked on usable security and have conducted user studies evaluating security mechanisms with end users (Tey et al., 2013; Gupta et al., 2012; Gupta and Gao, 2010; Toch and Levi, 2015). Gao, Toch, and Lo would work on the conceptualization, implementation, and experimentation design together. Gao and Lo would conduct user studies in Singapore while Toch would perform similar studies in Israel.

.Outcomes and Deliverables

Work Package 1: Generation of rich fine-grained logs and stateful model inference

Year 1:

- Initial logging prototype that can generate logs of a number of events along with control and data flow relationships between them.
- Initial model inference prototype that can generate simple models that capture control flow relationships among events.

Year 2:

- Improved logging prototype that can generate logs of a comprehensive set of events with control and data flow relationships between them.
- Improved model inference prototype that can generate comprehensive models that capture control and data flow relationships among events.
- An initial academic paper describing the research.

Year 3:

- Advanced logging prototype that can generate rich logs succinctly while incurring minimal overhead in terms of responsiveness and energy consumption.
- Advanced model inference algorithm that can not only generate but also efficiently and correctly *update* comprehensive behavioral models when new examples become available.
- Large scale accuracy and efficiency studies.
- Academic papers describing the research.

Work Package 2: Differencing analysis and anomaly detection

Year 1:

- Initial model differencing framework applied to several kinds of inferred models, finite-state machines, temporal invariants, scenarios etc.
- Prototype implementation of differencing tool, experiments with synthetic data.

Year 2:

- Improved prototype implementation of differencing tool, experiments with real data.
- Extension of differencing to include quantitative and statistical properties.

Year 3:

- Improved prototype implementation to support quantitative and statistical properties.
- Differences selection and prioritization.
- Academic papers describing the research.

Work Package 3: Model-based user interaction

Year 1:

- Initial prototype for *offline* analysis of mobile app anomalies (with rudimentary event set, inference and HCI)

Year 2:

- Improved prototype for *offline* analysis of mobile app anomalies (additional events, improved inference and HCI)
- Initial prototype for *online* analysis of mobile app anomalies (with rudimentary event set, inference and HCI)

Year 3:

- Improved prototype for *online* analysis of mobile app anomalies (additional events, improved inference and HCI)
- Usability studies in the context of smart cities
- Academic papers describing the research

SECTION III: Proposed Budget

Please provide an estimated budget and a brief narrative in the "Description" column. This should not exceed 1 page.

Budget Category	Description	Budget(S$)
A. Expenditure on Manpower (EOM)	The cost would cover the salary of the research fellow for 35 months. The research fellow would be the main person who work on the work items in Singapore. During the first month of the project, the PI and co-PIs would first finalize the detailed plan of the project. Thus the research fellow would only be hired from the second month onwards.	**S$303,781**
B. Expenditure on New Equipment	This cost would cover the purchase of one laptop for the research fellow (S$3,000). The laptop is needed for day-to-day activities of the research fellow. SMU does not provide computing equipment for this project and existing ones have been utilized for other projects/purposes.	**S$3,000**
C. Other Operating Expenses (OOE)	The OOE includes 2 conference travels: once at year 2 and another at year 3. The conference travels are needed to disseminate research results. In the area of security and software engineering, conferences are one of the major means to disseminate research results. The OOE also includes 3 trips by the PI to visit Israel for one week. One trip is planned for each year. The cost for each of such trips is estimated to be 5,300 SGD.	**S$26,500**
Total Direct Costs (S$):		**S$333,281**
Please indicate other in-kind contribution, including post-graduates funded by other sources, involved in the project.		

References

(Busany and Maoz, 2016) Nimrod Busany, Shahar Maoz, Behavioral Log Analysis with Statistical Guarantees, in Proc. of ACM/IEEE Int. Conf. on Software Engineering (ICSE 2016)

(Maoz and Ringert, 2015) Shahar Maoz, Jan Oliver Ringert, A Framework for relating semantic and syntactic differences, in Proc. of ACM/IEEE Int. Conf. on Model Driven Engineering Languages and Systems (MODELS 2015)

(Schuster and Tromer, 2016) Roei Schuster, Eran Tromer, DroidDisintegrator: Intra-Application Information Flow Control in Android Apps, Proceedings of ACM Asia Conference on Computer and Communications Security (ASIACCS 2016)

(Smalley and Craig, 2013) Stephen Smalley, Robert Craig: Security Enhanced (SE) Android: Bringing Flexible MAC to Android. Proceedings of 20th Annual Network and Distributed System Security Symposium (NDSS 2013)

(Arzt et al., 2014) Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Octeau,Patrick McDaniel: FlowDroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps. Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2014): 29

(Enck et al., 2014) William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, Anmol N. Sheth: TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. ACM Transactions on Computing Systems 32(2): 5:1-5:29 (2014)

(Avdiienko et al., 2015) Vitalii Avdiienko, Konstantin Kuznetsov, Alessandra Gorla, Andreas Zeller, Steven Arzt, Siegfried Rasthofer, Eric Bodden: Mining Apps for Abnormal Usage of Sensitive Data. ICSE (1) 2015: 426-436

(Pandita et al., 2013) Rahul Pandita, Xusheng Xiao, Wei Yang, William Enck, Tao Xie: WHYPER: Towards Automating Risk Assessment of Mobile Applications. Proceedings of the 22nd USENIX Security Symposium (Usenix Security 2013): 527-542

(Gorla et al., 2014) Alessandra Gorla, Ilaria Tavecchia, Florian Gross, Andreas Zeller: Checking app behavior against app descriptions. Proceedings of the 36th ACM/IEEE International Conference on Software Engineering (ICSE 2014): 1025-1035

(Jamrozik et al., 2016) Konrad Jamrozik, Philipp von Styp-Rekowsky, and Andreas Zeller: Mining Sandboxes. Proceedings of the 38th ACM/IEEE International Conference on Software Engineering (ICSE 2016): 37-48

(Backes et al., 2013) Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, Philipp von Styp-Rekowsky: AppGuard - Enforcing User Requirements on Android Apps. Proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013): 543-548

(Le et al., 2015) Tien-Duy B. Le, Xuan-Bach D. Le, David Lo, Ivan Beschastnikh: Synergizing Specification Miners through Model Fissions and Fusions. Proceedings of the 30th IEEE/ACM International Conference on Automated Software Engineering (ASE 2015): 115-125

(Le and Lo, 2015) Tien-Duy B. Le, David Lo: Beyond support and confidence: Exploring interestingness measures for rule-based specification mining. Proceedings of the 22nd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2015): 331-340

(Fahland et al., 2013) Dirk Fahland, David Lo, Shahar Maoz: Mining branching-time scenarios. Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE 2013): 443-453

(Lo and Moaz, 2012) David Lo, Shahar Maoz: Scenario-based and value-based specification mining: better together. Automated Software Engineering 19(4): 423-458 (2012)

(Lo et al., 2012a) David Lo, Leonardo Mariani, Mauro Santoro: Learning extended FSA from software: An empirical assessment. Journal of Systems and Software 85(9): 2063-2076 (2012)

(Lo et al., 2012b) David Lo, G. Ramalingam, Venkatesh Prasad Ranganath, Kapil Vaswani: Mining quantified temporal rules: Formalism, algorithms, and evaluation. Science of Computer Programming 77(6): 743-759 (2012)
(Kumar et al., 2012) Sandeep Kumar, Siau-Cheng Khoo, Abhik Roychoudhury, David Lo: Inferring class level specifications for distributed systems. Proceedings of the 34th ACM/IEEE International Conference on Software Engienering (ICSE 2012): 914-924
(Maoz et al., 2011a) Shahar Maoz, Jan Oliver Ringert, Bernhard Rumpe: ADDiff: semantic differencing for activity diagrams. Proceedings of the 8th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/SIGSOFT FSE 2011): 179-189
(Maoz et al., 2011b) Shahar Maoz, Jan Oliver Ringert, Bernhard Rumpe: CDDiff: Semantic Differencing for Class Diagrams. Proceedings of the 25th European Conference on Object Oriented Programming (ECOOP 2011): 230-254
(Milea et al., 2011) Narcisa Andreea Milea, Siau-Cheng Khoo, David Lo, Cristian Pop: NORT: Runtime Anomaly-Based Monitoring of Malicious Behavior for Windows. Proceedings of the 2nd International Conference on Runtime Verification (RV 2011): 115-130
(Gupta and Gao, 2010) Payas Gupta, Debin Gao: Fighting Coercion Attacks in Key Generation using Skin Conductance. Proceedings of the 19th USENIX Security Symposium (USENIX Security 2010)
(Gupta et al., 2012) Payas Gupta, Tan Kiat Wee, Narayan Ramasubbu, David Lo, Debin Gao, Rajesh Krishna Balan: HuMan: Creating memorable fingerprints of mobile users. Proceedings of the 10th IEEE International Conference on Pervasive Computing Workshops (PerCom Workshops 2012)
(Tey et al., 2013) Chee Meng Tey, Payas Gupta, Debin Gao: I can be You: Questioning the use of Keystroke Dynamics as Biometrics. Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS 2013)
(Toch and Levi, 2013) Eran Toch, Inbal Levi: Locality and privacy in people-nearby applications. Proceedings of the ACM Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2013): 539-548
(Android, 2016) Android: UI/Application Exerciser Monkey. Available online at: http://developer.android.com/tools/help/monkey.html
(Machiry et al., 2013) Aravind Machiry, Rohan Tahiliani, Mayur Naik: Dynodroid: an input generation system for Android apps. Proceedings of the 9th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/SIGSOFT FSE 2013): 224-234
(Hao et al., 2014) Shuai Hao, Bin Liu, Suman Nath, William G. J. Halfond, Ramesh Govindan: PUMA: programmable UI-automation for large-scale dynamic analysis of mobile apps. Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2014): 204-217
(Tam et al., 2015) Kimberly Tam, Salahuddin J. Khan, Aristide Fattori, Lorenzo Cavallaro: CopperDroid: Automatic Reconstruction of Android Malware Behaviors. Proceedings of the 22nd Annual Network and Distributed System Security Symposium (NDSS 2015)
(Lo and Maoz, 2008) David Lo, Shahar Maoz: Mining Scenario-Based Triggers and Effects. Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering (ASE 2008)
(Wang et al., 2014) Shaowei Wang, David Lo, Lingxiao Jiang: Active code search: incorporating user feedback to improve code search relevance. Proceedings of the 29th IEEE/ACM International Conference on Automated Software Engineering (ASE 2014): 677-682
(Lucia et al., 2012) Lucia, David Lo, Lingxiao Jiang, Aditya Budi: Active refinement of clone anomaly reports. Proceedings of the 34th ACM/IEEE International Conference on Software Engineering (ICSE 2012): 397-407
(Gong et al., 2012) Liang Gong, David Lo, Lingxiao Jiang, Hongyu Zhang: Interactive fault localization leveraging simple user feedback. Proceedings of the 28th IEEE International Conference on Software Maintenance (ICSM 2012): 67-76

SECTION IV: Curricula Vitae

David LO (PI)
NRIC#: S8373352G; Email: davidlo@smu.edu.sg; Tel: 6828-0599; HP: 9842-1014
Mailing Address: School of Information Systems (SIS), Singapore Management University (SMU), 80 Stamford Road, Singapore 178902

Current Position and Employment History

Time	Employment
01/2009 to present	Assistant Professor of Information Systems, SIS, SMU
07/2014 to 09/2014	Visiting Researcher, Microsoft Research, USA
05/2008 to 12/2008	Lecturer of Information Systems, SIS, SMU
02/2008 to 04/2008	Research Intern, Microsoft Research India
10/2004 to 03/2006	Research Assistant, School of Computing, National University of Singapore

Academic Qualifications

- Ph.D. in Computer Science, National University of Singapore, Singapore, 2008
- B.Eng. in Computer Engineering, Nanyang Technological University, Singapore, 2004

Professional Awards (including Major Nominations)

- Most Influential Paper Award Nominee at the 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER), 2016. The nomination is for a paper published in 2006 entitled "QUARK: Empirical Assessment of Automaton-based Specification Miners" which lays the foundation on how to compare the effectiveness of behavioral model inference algorithms.
- Outstanding Reviewer Award, Information and Software Technology journal, 2016
- Most Active Reviewer Award, Empirical Software Engineering journal, 2015
- ACM SIGSOFT Distinguished Paper Award at the 10th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on Foundations of Software Engineering (ESEC-FSE), 2015
- Distinguished Reviewer Award at the 22nd IEEE International Conference on Software Analysis, Evolution, and Reengineering, 2015
- Best Student Paper Award at the 19th International Conference on Engineering of Complex Computer Systems (ICECCS), 2014
- Most Promising Idea Award at the 22nd International Conference on Program Comprehension (ICPC), 2014
- Distinguished Reviewer Award at the 20th Working Conference on Software Engineering (WCRE), 2013
- Nominated for Best Paper Awards (2 Papers), 29th IEEE International Conference on Software Maintenance (ICSM), September 2013. Both papers were invited and accepted by a special issue of ICSM best papers published in the Empirical Software Engineering journal.
- ACM SIGSOFT Distinguished Paper Award at the 27th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2012
- SMU Most Promising Teacher Award 2012 Nominee (1 of the 7 nominees)
- SMU Most Promising Teacher Award 2011 Nominee (1 of the 7 nominees)
- Lee Foundation's Fellow of Research Excellence, 2009-2010

Research Interests

Automated software engineering; Software security; Software reliability; Software maintenance; Data mining and big data analysis; Social network mining

Five Most Important Publications Most Relevant to This Grant Application (Last 5 Years)

1. “Synergizing Specification Miners through Model Fissions and Fusions”, by Tien-Duy B. LE, Xuan-Bach D. LE, David LO, and Ivan BESCHASTNIKH, 2015, Proceedings of the 30th IEEE/ACM International Conference on Automated Software Engineering (ASE)
2. “Mining Branching-Time Scenarios”, by Dirk FAHLAND, David LO, and Shahar MAOZ, 2013, Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE)
3. "Inferring Class Level Specifications for Distributed Systems", by Sandeep KUMAR, Siau-Cheng KHOO, Abhik ROYCHOUDHURY, and David LO, 06/2012, Proceedings of the 34th ACM/IEEE International Conference on Software Engineering (ICSE)
4. "Mining Quantified Temporal Rules: Formalism, Algorithms, and Evaluation", by David LO, Ganesan RAMALINGAM, Venkatesh Prasad RANGANATH, and Kapil VASWANI, 2012, Science of Computer Programming
5. "Scenario-Based and Value-Based Specification Mining: Better Together", by David LO and Shahar MAOZ, 2012, Automated Software Engineering Journal

Patents

1. “Abstracting Events for Data Mining” by David LO, Ganesan RAMALINGAM, Venkatesh-Prasad RANGANATH, and Kapil VASWANI, US 20110087700 A1, 2011.

Research Grants (as PI and co-PI)

- “Improving Clone Detection for Systems Software” (01/2013 – 12/2014), Ambassade de France à Singapour and SMU, Singapore PI. Outcome: The grant has resulted in a number of publications including the following:

    1. "An Empirical Assessment of Bellon's Clone Benchmark", by Alan CHARPENTIER, Jean-Rémy FALLERI, David LO, and Laurent REVEILLERE, 2015, Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering (EASE).
    2. "Understanding the Genetic Makeup of Linux Device Drivers", by Peter Senna TSCHUDIN, Laurent REVEILLERE, Lingxiao JIANG, David LO, and Julia LAWALL, 2013, Proceedings of the Seventh Workshop on Programming Languages and Operating Systems (PLOS).

- "Improving System Maintainability and Reliability: A Data Mining Approach” (04/2009-03/2010), Lee Foundation, PI. Outcome: The grant has resulted in a number of publications including the following:

    1. "Mining Hierarchical Scenario-Based Specifications", by David LO, and Shahar MAOZ, 2009, Proceedings of the 24th IEEE/ACM International Conference on Automated Software Engineering (ASE)
    2. "Automatic Steering of Behavioral Model Inference", by David LO, Leonardo MARIANI, and Mauro PEZZE, 2009, Proceedings of the Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE).

- "User-Centric Mobile Authentication Mechanisms" (09/2009-12/2010), SMU, Co-PI. Outcome: The grant has resulted in the following publication:

    1. "HuMan: Creating Memorable Fingerprints of Mobile Users", by Gupta PAYAS, Kiat Wee TAN, Narayanasamy RAMSUBBU, David LO, Deibn GAO, and Rajesh Krishna BALAN, 2012, Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (Percom Workshops).

Shahar MAOZ (Co-PI)
Email: maoz@cs.tau.ac.il
Mailing Address: School of Computer Science, Tel Aviv University (TAU), Tel Aviv 69978

Current Position and Employment History

Time	Employment
10/2012 to present	Senior Lecturer, School of Computer Science, Tel Aviv University
01/2010 to 09/2012	Postdoc Research Fellow, RWTH Aachen University, Germany

Academic Qualifications

- **Ph.D. in Computer Science, The Weizmann Institute, Israel, 2009**
- M.B.A., Management of Technology Program, University of California at Berkeley, 2004
- **M.Sc. in Computer Science, Tel Aviv University, Israel, 2000**
- B.Mus., Music Composition, Tel Aviv University, Israel, 2000
- B.A., General Humanities, The Open University, Israel, 1999
- **B.Sc. in Mathematics, Tel Aviv University, Israel, 1996**

Professional Awards

- Distinguished Reviewer Award, ACM/IEEE ASE Conference, 2015
- Best Foundations Paper Award, ACM/IEEE MODELS Conference, 2015
- Best Paper Award, ACM/IEEE MODELS Conference, 2011
- Postdoctoral Wolfgang Gentner excellence award from the Minerva Foundation

Research Interests

Modeling and Formal Methods in Software Engineering, Software Engineering Tools

Five Most Important Publications Most Relevant to This Grant Application (Last 5 Years)

1. “Behavioral Log Analysis with Statistical Guarantees”, Nimrod Busany and Shahar Maoz, ACM/IEEE Int. Conf. on Software Engineering (ICSE), 2016
2. “Have We Seen Enough Traces?”, Hila Cohen and Shahar Maoz, ACM/IEEE Int. Conf. on Automated Software Engineering (ASE), 2015
3. “A framework for relating syntactic and semantic model differences”, Shahar Maoz and Jan Oliver Ringert, ACM/IEEE Int. Conf. on Model Driven Engineering Languages and Systems (MODELS), 2015
4. “Mining Branching-Time Scenarios”, by Dirk Fahland, David Lo, and Shahar Maoz, 2013, Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE)
5. "Scenario-Based and Value-Based Specification Mining: Better Together", by David Lo and Shahar Maoz, 2012, Automated Software Engineering Journal

Research Grants (as PI and co-PI)

- SYNTECH: Synthesis Technologies for Reactive Systems Software Engineers, sole PI, **ERC Starting Grant** (2015-2020)
- Crosscutting Structural Views for Component and Connector Models, sole Israeli PI joint with one German PI, **German Israeli Foundation for Scientific Research and Development (GIF)** (2015-2017)

Debin Gao (Co-PI)
NRIC#: S7776468B; Email: dbgao@smu.edu.sg; Tel: 6828-0969
Mailing Address: School of Information Systems (SIS), Singapore Management University (SMU), 80 Stamford Road, Singapore 178902

Current Position and Employment History

Time	Employment
07/2015 to present	Associate Professor of Information Systems, SIS, SMU
07/2007 to 06/2015	Assistant Professor of Information Systems, SIS, SMU
01/2007 to 05/2007	Software systems engineer, CyLab, Carnegie Mellon University
05/2005 to 08/2005	Research Intern, Microsoft Research Redmond USA
06/2001 to 05/2002	Teaching Assistant, School of Computing, National University of Singapore

Academic Qualifications

- Ph.D. in Electrical and Computer Engineering, Carnegie Mellon University, 2006
- M.Sci. in Electrical and Computer Engineering, Carnegie Mellon University, 2004
- B.Eng. in Electrical and Electronic Engineering, Nanyang Technological University, Singapore, 2001

Professional Awards (including Major Nominations)

- Distinguished paper award in the 20th Annual Network & Distributed System Security Symposium (NDSS 2013)

Research Interests

Systems security, intrusion detection, mobile security, software security, human factors in computer security

Five Most Important Publications Most Relevant to This Grant Application (Last 5 Years)

1. "Stack Layout Randomization with Minimal Rewriting of Android Binaries", by Yu Liang, Xinjie Ma, Daoyuan Wu, Xiaoxiao Tang, Debin Gao, Guojun Peng, Chunfu Jia and Huanguo Zhang, 2015, In Proceedings of the 18th annual International Conference on Information Security and Cryptology (ICISC 2015)
2. "RopSteg: Program Steganography with Return Oriented Programming", by Kangjie Lu, Siyang Xiong and Debin Gao, 2014, In Proceedings of the 4th ACM Conference on Data and Application Security and Privacy (CODASPY 2014)
3. "Comparing Mobile Privacy Protection through Cross-Platform Applications", by Jin Han, Qiang Yan, Debin Gao, Jianying Zhou and Robert Deng, 2013, In Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS 2013)
4. "Launching generic attacks on iOS with approved third-party applications", by Jin Han, Mon Kywe Su, Qiang Yan, Feng Bao, Huijie Robert Deng, Debin Gao, Yingjiu Li, and Jianying Zhou, 2013, In Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS2013)
5. "Gray-Box Extraction of Execution Graphs for Anomaly Detection", by Debin Gao, Michael K. Reiter and Dawn Song, 2004, In Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004)

Patents Filed

1. "Obfuscation of code using ROP", Singapore, 2014.
2. "Defense against ROP on ARM via instruction randomization", Singapore, 2014.

Research Grants (as PI and co-PI)

- “Secure mobile center” (02/2015 – 02/2019), NRF Singapore, Co-PI
- “Advanced ROP execution and defences on Android” (06/2015 – 06/2016), Huawei Co. Ltd., PI
- “Analyzing and defending against ROP-embedded mobile application” (12/2013 – 12/2014), Huawei Co. Ltd., PI
- “A study of the usability of keystroke biometrics in exceptional conditions” (02/2013 – 02/2014), SMU, PI
- “Binary difference analysis” (01/2012 – 12/2012), SafeNet Inc., PI
- "User-Centric Mobile Authentication Mechanisms" (09/2009-12/2010), SMU, Co-PI
- “Malware analysis” (01/2009 – 12/2010), DSTA/MINDEF Singapore, PI

Eran Tromer (co-PI)
tromer@cs.tau.ac.il; Tel: +972-54-4754756
Mailing Address: School of Computer Science, Tel Aviv University, Tel Aviv 6997801, Israel

Current Position and Employment History

Time	Employment
01/2011 to present	Senior Lecturer, School of Computer Science, Tel Aviv University
06/2015 to 08/2015	Visiting Scientist, Simons Institute for for Theory of Computing, UC Berkeley
09/2010 to 12/2010	Visiting Researcher, Microsoft Research New England
02/2007 to 08/2010	Postdoctoral Associate, Massachusetts Institute of Technology
09/1998 to 01/2000	Consultant, Virtue Ltd.
08/1995 to 08/1998	Intelligence Corps, Israeli Defense Forces
05/1995 – 08/1998	Senior developer, Shells Interactive Film-Art

Academic Qualifications

- Ph.D. in Computer Science, Weizmann Institute of Science, Israel, 2006
- B.A. in Computer Science, Technion, Israel, 2000

Professional Awards (including Major Nominations)

- Paper “Acoustic Cryptanalysis” in CRYPTO’14 selected as one of the 3 top papers and invited to the top-papers issue in Journal of Cryptology
- Paper “Get your hands off my laptop: physical side-channel key-extraction attacks on PCs” selected as one of the 3 top papers and invited to the top-papers issue in Journal of Cryptographic Engineering
- Black Hat 2014 Pwnie Award for Most Innovative Research, 2014
- Tel Aviv University’s Sackler Prize for Young Faculty, 2013
- Rothschild Fellowship for Postdoctoral Studies, 2006
- Weizmann Institute’s John F. Kennedy Award (top Ph.D. distinction), 2006
- Israeli Defense Forces’s Director of Military Intelligence’s Uzi Yairi Award for Innovation, 1998

Research Interests

Information security, cryptography, privacy, resilient systems and networks, efficient algorithms.

Five Most Important Publications Most Relevant to This Grant Application (Last 5 Years)

1. “DroidDisintegrator: intra-application information flow control in Android apps”, by Roei SCHUSTER and Eran TROMER, ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS) 2016
2. “Secure association for the Internet of Things”,Almog BENIN, Sivan TOLEDO and Eran TROMER, Proc. International Workshop on Secure Internet of Things (SIoT) 2015, 25–34, IEEE, 2015
3. “Zerocash: decentralized anonymous payments from Bitcoin”, by Eli BEN-SASSON, Alessadro CHIESA, Christina GARMAN, Matthew GREEN, Ian MIERS, Eran TROMER and Madars VIRZA, Proc. IEEE Symposium on Security & Privacy (Oakland) 2014, 459–474, IEEE, 2014
4. “Analyzing unique-bid auction sites for fun and profit” by Ori SAMORODINTZKY, Eran TROMER, and Avishai WOOL, Proc. Annual Network and Distributed System Security Symposium (NDSS) 2013
5. “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption”, by Adriana LOPEZ-ALT, Eran TROMER, and Vinod VAIKUNTANATHAN, Proc. ACM Symposium on Theory of Computing (STOC) 2012, 1219–1234, ACM, 2012

Research Grants (as PI and co-PI)

- Securing Servers and Endpoints using Software Guard Extensions, Blavatnik Interdisciplinary Cyber Research Center, 2015—2017. PIs: Shay Gueron, Sivan Toledo, E. Tromer
- Proving Image AuthenticityBroadcom Foundation and Tel Aviv University Authentication Initiative, 2014—2016
- Leona M. and Harry B. Helmsley Advanced Communications Technology Project, The Leona M. & Harry B. Helmsley Charitable Trust, 2013—2016. PIs: E. Socher and E. Tromer,
- Secure Implementation of Post-Quantum Cryptography, NATO Science for Peace and Security Programme, 2013—2016. PIs: V. Fischer, O. Grosek, R. Steinwandt, E. Tromer.
- Cyber-Secure Computer Systems: Refactoring Computer Systems for the Cyber Era, Israeli Ministry of Science and Technology, Infrastructure grant, 2013--2015. PIs: Y. Etzion, A. Schuster, E. Tromer, D. Tzafrir, E. Yahav
- Security of Remotely Controlled DevicesIsraeli Ministry of Science and Technology, Infrastructure grant, 2013--2015.PIs: S. Toledo, E. Tromer
- Towards Secure Storage and Computing in the Cloud, Israeli Ministry of Science and Technology, Infrastructure grant, 2012--2015. PIs: B. Applebaum, A. Herzberg, B. Pinkas, E. Tromer
- Check Point Institute for Information Security, Check Point Ltd., 2008--2017. Role: codirector (2011--present) and principal investigator

Eran Toch (Co-PI)
Email: erant@post.tau.ac.il
Mailing Address: Department of Industrial Engineering, Tel Aviv University (TAU), Tel Aviv 69978

Current Position and Employment History

Time	Employment
10/2010 to present	Senior Lecturer, Department of Industrial Engineering, Tel Aviv University
09/2008 to 09/2010	Postdoc Research Fellow, School of Computer Science, Carnegie Mellon University

Academic Qualifications

- Ph.D. in Information Systems, The Technion – Israel Institute of Technology, 2008
- B.Sc. in Computer Science and B.A. Honors Program in Humanities, Haifa University, 2001

Professional Awards

- Best paper award, ACM CASEMANS '11, 2011.
- Dean's teaching award, 2014-2015.
- 2007/2008 – Levi Eshkol scholarship for scientific achievement
- Postdoctoral excellence fellowship from Carnegie Mellon University

Research Interests

Usable security and privacy, human-comptuer interaction, data mining

Five Most Important Publications Most Relevant to This Grant Application (Last 5 Years)

1. Omer Barak, Gabriella Cohen, and Eran Toch. **Anonymizing Mobility Data using Semantic Cloaking**, Pervasive and Mobile Computing, 2015.
2. Ron Hirschprung, Eran Toch and Oded Maimon, **Simplifying Data Disclosure Configurations in a Cloud Computing Environment**, ACM Transactions on Intelligent Systems and Technology, vol 6, no. 3, article 32, 2015.
3. Eran Toch, **Crowdsourcing Privacy Preferences in Context-Aware Applications**, Personal and Ubiquitous Computing, vol 18, no 1, pp. 129-141, 2014.
4. Oshrat Rave-Ayalon and Eran Toch. **Retrospective Privacy: Managing Longitudinal Privacy in Online Social Networks**, In Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS'13). ACM, New York, NY.
5. Eran Toch, Yang Wang, and Lorrie Faith Cranor, **Personalization and Privacy.** User Modeling and User-Adapted Interaction (UMUAI), vol 22, no 1-2, pp. 203-220, 2012.

Research Grants (as PI and co-PI)

Research Topics	Funding Agency	Years	Total grant
Mobility Patterns Analysis	Israel Ministry of Science	2012-2015	1,265,281 NIS
Analyzing user behaviors in cyber security	Israel Cyber Security Bureau and Israel Ministry of Science	2012-2015	868,883 NIS
Privacy by Design – Identifying Gaps and in the Intersection of Law and Engineering	ISF	2012-2015	650,000 NIS
Analyzing application purpose for analyzing and enhancing privacy in mobile operating systems	DARPA	2016-2020	$1.9 Mil
Cyber Security and privacy in Smart Cities	ICRC – Blavatnik Interdisciplinary Cyber Research Center	2015-2018	500,000 NIS
Privacy & Us: reason, design and develop novel solutions to questions related to the protection of citizens' privacy	Horizon 2020, Marie Sklodowska Curie Innovative Training Networks	2015-2019	€3.362 Million
Privacy-Aware Cybersecurity	Israel Ministry of Science Italy-Israel Collaborative Fund	2016-2018	900,000 NIS
Design and operation of a crowd-sourced package delivery system	Israel Ministry of Science	2016-2019	1,150,920 NIS