

SeMA: A Design Methodology for Building Secure Android Apps

Joydeep Mitra Venkatesh-Prasad Ranganath
Kansas State University, U.S.A
{joydeep,rvprasad}@k-state.edu

Created: February 15, 2019. Revised: September 19, 2019.

Abstract

UX (user experience) designers visually capture the UX of an app via storyboards. This method is also used in Android app development to conceptualize and design apps.

Recently, security has become an integral part of Android app UX because mobile apps are used to perform critical activities such as banking, communication, and health. Therefore, securing user information is imperative in mobile apps.

In this context, storyboarding tools offer limited capabilities to capture and reason about the security requirements of an app. Consequently, security cannot be baked into the app at design time. Hence, vulnerabilities stemming from design flaws can often occur in apps. To address this concern, in this paper, we propose a storyboard based design methodology to enable the specification and verification of security properties of an Android app at design time.

1 Why a new methodology?

Android app development teams use storyboarding as part of their design process [20, 13]. A storyboard is a sequence of images that serves as a specification of the user observed behavior in terms of screens and transitions between screens. Storyboarding helps designers identify different kinds of app users (user profiles), explore possible real world scenarios in which a user will interact with the app, and develop wireframes to capture the scenarios for identified user profiles [13, 9, 11]. Numerous tools such as Xcode [1], Sketch [16], and Android JetPack’s Navigation Component [7] help designers digitally express the storyboard of an app.

Storyboarding is meant to be participatory because it can be used by designers to get feedback from potential users about likely user scenarios, and from developers about the technical challenges of implementing the design. However, in their current form, storyboards do not capture non-functional requirements such as security. Consequently, Android app designers and developers cannot use storyboarding to collaborate and express security requirements at design time. As a result, verification of security requirements is delayed until later stages. This delay increases the cost of app development as vulnerabilities due to flaws detected in later stages increase the cost of development [19].

In this context, to enable reasoning about security at design time, we are exploring two ideas: 1) *extend storyboards to capture non-functional properties* and 2) *develop a methodology that uses storyboards to specify and verify security requirements of apps at design time*.

To understand the reasons for and benefits of these ideas, we need to understand the current landscape of Android app development practices.

Today, developers consider the security requirements of an app while or after implementing the app. Existing research efforts related to Android app security have focused on developing tools and techniques to help detect vulnerabilities in an app’s implementation [18, 8]. Despite such efforts, apps with known vulnerabilities find their way to app stores [15, 4]. This is possibly because existing tools are neither accurate [14] nor scalable [12] in terms of detecting known vulnerabilities. Given this landscape, we believe it is worthwhile to explore the unexplored: *preemptively eliminate vulnerabilities in apps by enabling developers and designers to consider security at design time and thwart the exploits of malicious apps*.

Besides complementing existing techniques, such exploration will help consider the following research questions:

- a) How much effort is required in terms of time and cost to formally reason about Android apps at design time?
- b) In the context of Android app development, is secure-by-design cost-effective?
- c) Is verifying an app based on its storyboard easier than verifying an app based on its code?
- d) In terms of improving security, how will the proposed approach compare to existing curative approaches, i.e., detect vulnerabilities after they occur?

2 What is the methodology?

Motivated by the above reasons, we propose the following methodology, *Securing Mobile Apps (SeMA)*, that borrows heavily from model driven development [3, 5].

- 1) App development begins with the storyboard (model) of an app that captures the screens of the app, the transitions between screens, and the resources used by the app.
- 2) The storyboard is iteratively refined by adding behavioral and security properties.
- 3) As the storyboard is refined, verification techniques are used to check the behavior of the storyboard satisfies the security properties. Once the refined storyboard satisfies the desired requirements, property preserving structural code¹ of the app is automatically generated.
- 4) Business logic is added to the generated code.

2.1 An Illustrative Example

To understand SeMA, consider the development of an app that sends a message to a set of pre-identified contacts at the push of a button.

2.1.1 App Specification

Figure 1 shows the storyboard of this example app along with a brief description of various concepts captured in the storyboard.

Initially, the app designer specifies the required screens and the transitions between the screens as shown in the sub-diagram in the top left corner of the figure (labeled A). The initial snapshot is similar to how storyboards are used in designing apps today. Besides the graphical description of screens of the app, this snapshot captures the navigational possibilities in the app: 1) user will see the *Messenger* screen up on launching the app, 2) the user can transition to either *Contacts* or *MsgStatus* screens from the *Messenger* screen, and 3) the user can transition to *SaveStatus* screen from the *Contacts* screen.

Next, the app designer refines the initial snapshot with constraints based on user actions (marked in red in the main diagram). For example, when the user clicks the *Add* button in the *Messenger* screen, the app transitions to the *Contacts* screen.

As the next refinement, the app developer (in collaboration with the app designer) adds more behavioral constraints to the storyboard. For example, a constraint based on the state of the app (marked in blue) is added to the transition from the *Contacts* screen. Other transitions in the app are enriched with constraints in subsequent refinements.

Many constraints rely on operations involving the resources in the device. While such resources are pre-defined, apps can specify views of resources that they will use.

The *resource view* of the app (shown in Figure 1) describes the view of the resources used in the example app as follows.

- *EXT.STORE* denotes the external storage on Android devices that can be accessed by all apps installed on the device. The app uses the following two capabilities of this resource: `write(f,p)` writes the value `p` into file `f` and `read(f)` reads a value from file `f` and returns it.

¹Structural code is traditional skeletal code along with some non-trivial logic to enforce properties.

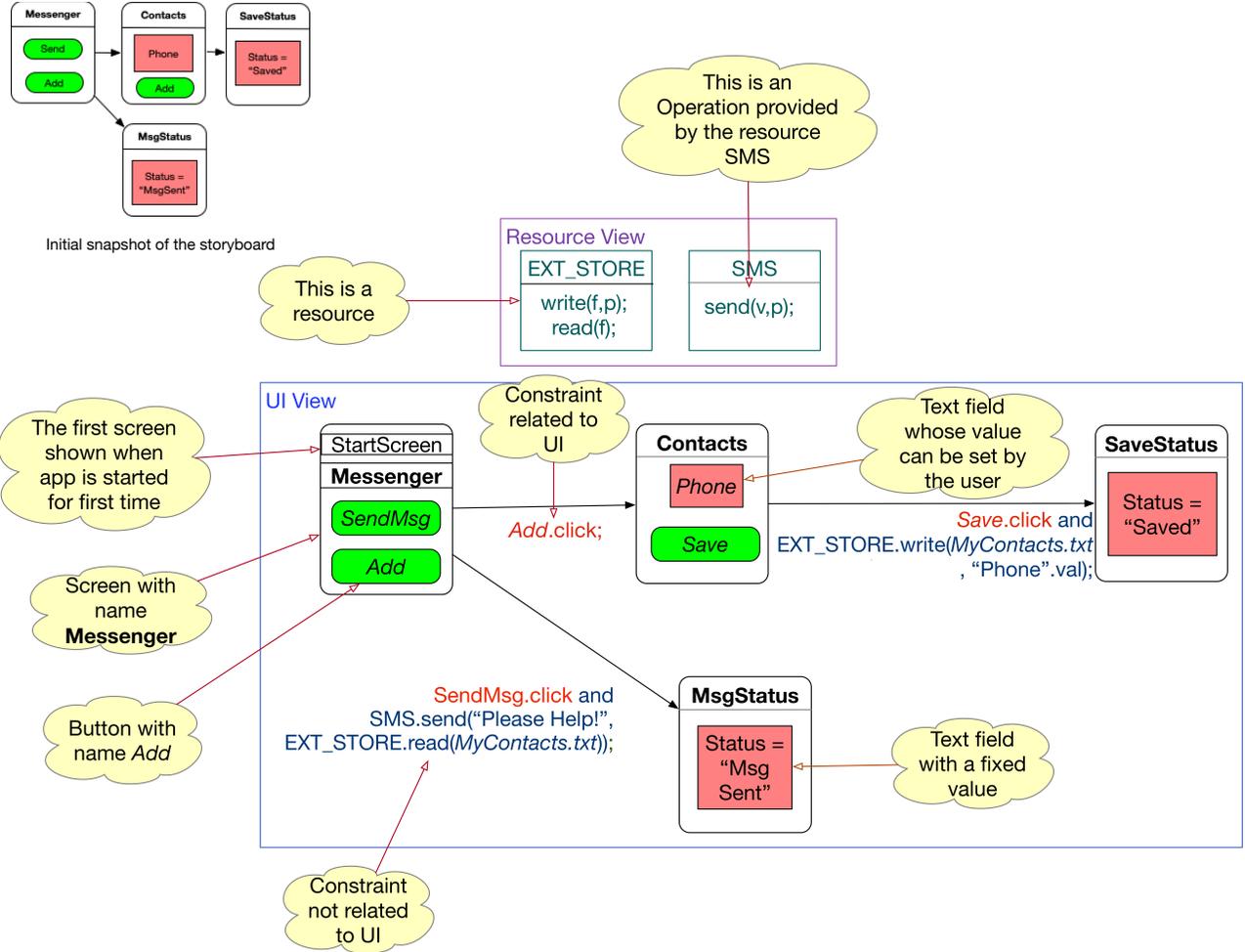


Figure 1: Storyboard of the Emergency App. The clouds are not part of the storyboard; they provide information about the different graphical elements in the figure.

- *SMS* denotes a pre-defined service available on Android devices that the app uses to send a SMS message m to a list of phone number p via `send(m,p)` operation.

The final storyboard with all the behavior and resource operations specified will look like Figure 1.

To give an example of how the constraints in a transition are interpreted, the transition from the *Messenger* screen to the *MsgStatus* screen is taken when 1) the *SendMsg* button is pressed and 2) an SMS message is successfully sent to the phone numbers in the file named *MyContacts.txt*.

2.1.2 Analysis

In this example, suppose we are interested in the violation of this property: *malicious input should not influence data flow in the app*.

Based on the semantics of *EXT_STORE*, all apps can access data in *EXT_STORE*. Hence, *EXT_STORE* can possibly contain malicious inputs as malicious apps can modify the contacts stored by the example app. Since the phone numbers from *EXT_STORE* is used in `SMS.send(...)`, a violation of the property is detected by analyzing the data flow through the storyboard in accordance with the semantics of resources used by the app.

This vulnerability can be fixed by storing the phone numbers in a more secure way. For example, *MyContacts.txt* file can be stored in the app's internal storage that is accessible only by the app. This fix

can be suggested by tooling support, expressed by the developer in the storyboard by using appropriate resources, and enforced via code generation.

3 Realizing the methodology

To validate the feasibility of this methodology, we are currently developing the design language, its formal syntax and semantics, and the analysis engine required to reason about the design. In addition, we are exploring the following few design choices.

3.1 Leverage existing mobile app design frameworks

Android JetPack Navigation (AJN) [7] is a suite of libraries that helps Android developers design their apps' navigation. Navigation refers to the interactions that allow users to move between screens with simple button clicks and other more complex patterns. Since AJN is open source, is already supported in Android Studio, and can easily be extended, we chose to extend AJN with functionality to enable the specification and analysis of an app's design as described in Section 2.1.1. The modified library currently allows users to do the following:

1. Initialize the widgets of a screen with data.
2. Annotate transitions between screens with constraints.
3. Pass data as arguments on a transition into a screen.

3.2 Support pre-defined security properties

We do not want to burden app developers or designers with specifying the security properties required for verification because specifying such properties may initially be a non-trivial burden for the average app developer or designer. Moreover, requiring app developers or designers to specify such properties will unnecessarily complicate the existing design process. Therefore, we envision SeMA will initially support the checking of pre-defined security properties that are based on classes of common vulnerabilities [10] e.g., listed in Section 4.

3.3 Leverage existing tooling framework

Android Lint [6] is a static code analysis tool that helps analyze Android project source files. We have extended Android Lint with customized checks on navigation graphs. Currently, our extension to Android Lint can check the following properties:

1. Data accepted as input via an exported screen² is used to perform a sensitive operation in the app.
2. Data from an untrusted source (e.g., app's external storage) is used to perform a sensitive operation in the apps.

To check these properties, we rely on Android Lint to identify data sources and sinks. Then, our Lint extension tracks the data flow between data sources and data sinks. A violation is flagged when data flows from a potential malicious data source into a data sink associated with sensitive operations.

We use the JavaPoet library [17] to translate the verified navigation graph into Android source code. The generated source code can be extended by developers with business logic. Such extensions might introduce behavioral inconsistencies between the storyboard and the implementation. To detect such inconsistencies, we plan to generate characterization tests based on the behavioral specifications captured in the storyboard.

Further, not all security properties can be checked statically at the design stage. Such properties can be checked preemptively at runtime, and we plan to explore this possibility.

²An exported screen can be triggered by any component outside the app.

3.4 Stitching a Workflow

As described in Section 2, the methodology will help the user build an app iteratively. First, the user uses the extended version of AJN to create an app’s storyboard. Second, this storyboard is refined with behavioral properties. Third, the storyboard is verified against pre-defined properties after every refinement. Fourth, the structural code is generated once the refined storyboard satisfies the desired properties. Finally, the user extends the structural code to build a working app. The extended code is then tested against the generated characterization tests to ensure that the implementation is consistent with the design. Currently, we have prototyped the methodology (with the exception of characterization test generation step) in Android Studio.

4 What lies in the future?

Going forward, we plan to extend AJN with more features that will enable the analysis of navigation graphs. We will also extend the custom lint checker with more properties based on known vulnerabilities that plague Android apps.

Existing efforts have identified vulnerabilities that commonly plague Android apps [2] and have developed benchmarks to capture them [10]. Most known vulnerabilities can be classified as follows:

1. *Reliance on Data from Potentially Malicious Sources*: If an app X blindly trusts input from an external component not in the app and uses it to manipulate data or perform a critical task, then the app is vulnerable.
2. *Disclosure of Sensitive Information*: An app can accidentally expose sensitive information.
3. *Exposure of Privileged Resources*: An app with access to privileged resources can accidentally allow other apps to access to such resources and enable *privilege escalation*.

The above classes of vulnerabilities can be prevented by SeMA.

As for vulnerabilities that stem from implementation errors (e.g. using HTTP instead of HTTPS when contacting a server). They can be prevented by smart code generation techniques.

5 Challenges

To successfully realize the proposed methodology, the following interesting challenges need to be addressed while developing SeMA.

1. *Storyboard Extensions to Capture Non-UI Behavior*: Today, storyboards of Android apps capture only the UI components of an app and behavior triggered by user actions. However, Android apps also exhibit non-UI related behavior, e.g., reading a file from the app’s storage as shown in the earlier illustrative example. Therefore, existing storyboards will have to be extended with features to capture behavior that stem from non-UI elements without disrupting the workflow and the mental model associated with storyboards.
2. *Context-Aware Analysis*: Android apps do not run in isolation. They communicate with remote servers, other apps on the device, and the underlying Android framework. Therefore, the security of an app depends on the context in which it is operating. Security analysis of app storyboards will have to be aware of such contexts; otherwise, the analysis will be imprecise.
3. *Reactive Nature of Android Apps*: Android apps interact with the underlying platform via platform-defined application lifecycle methods to handle the numerous system and user events. These events could trigger the execution of an app from different entry points. Also, apps have the ability to persist information across different executions. This allows for different executions of an app that start at different entry points to be implicitly related by persisted data. This possibility should be considered to accurately reconstruct the behavior of an app for the purpose of security reasoning.

4. *Scalability of Analysis*: To be accurate and effective, security analysis of Android apps will have to consider various contexts and rich features of the Java (or Kotlin) programming language used to implement the apps. Such analysis is neither scalable [12] nor accurate [14] as they are plagued by the challenges faced by non-trivial source code analysis [8].
5. *Checking Richer Security Properties*: Given the limitations of simple static checkers like Android Lint and the richness of security properties (e.g., temporality), more involved analysis/checking techniques may be needed to check/enforce richer security properties. Such techniques could be adopted from program analysis/verification community or custom techniques could be developed from scratch.

References

- [1] Apple. Storyboards in Xcode. <https://developer.apple.com/library/archive/documentation/General/Conceptual/Devpedia-CocoaApp/Storyboard.html>, 2019. Accessed: 05-Feb-2019.
- [2] Erika Chin. *Helping Developers Construct Secure Mobile Applications*. PhD thesis, University of California, Berkeley, USA, 2013. Available at <https://escholarship.org/uc/item/4x48p6rz#page-1>.
- [3] Robert France and Bernhard Rumpe. Model-driven development of complex software: A research roadmap. In *2007 Future of Software Engineering*, pages 37–54. IEEE Computer Society, 2007.
- [4] Maria Gomez, Romain Rouvoy, Martin Monperrus, and Lionel Seinturier. A Recommender System of Buggy App Checkers for App Store Moderators, 2014. Available at [Online Tech Report](#).
- [5] John Hatcliff, Xinghua Deng, Matthew B. Dwyer, Georg Jung, and Venkatesh Prasad Ranganath. Cadena: An integrated development, analysis, and verification environment for component-based systems. In *Proceedings of the 25th International Conference on Software Engineering*, pages 160–173. IEEE Computer Society, 2003.
- [6] Google Inc. Android lint overview. Available at <http://tools.android.com/lint/overview>.
- [7] Google Inc. Navigation. Available at <https://developer.android.com/guide/navigation>.
- [8] Li Li, Tegawendé F. Bissyandé, Mike Papadakis, Siegfried Rasthofer, Alexandre Bartel, Damien Octeau, Jacques Klein, and Le Traon. Static analysis of android apps: A systematic literature review. *Information and Software Technology*, pages 67 – 95, 2017.
- [9] Ambrose Little. Storyboarding in the software design process. <https://uxmag.com/articles/storyboarding-in-the-software-design-process>, 2013. Accessed: 05-Feb-2019.
- [10] Joydeep Mitra and Venkatesh-Prasad Ranganath. Ghera: A repository of android app vulnerability benchmarks. In *Proceedings of the 13th International Conference on Predictive Models and Data Analytics in Software Engineering*, pages 43–52. ACM, 2017.
- [11] Arvind Padmanabhan. Storyboards for designing mobile apps. <https://indianengineeringdesignforum.wordpress.com/2015/11/07/storyboards-for-designing-mobile-apps/>, 2015. Accessed: 05-Feb-2019.
- [12] Felix Pauck, Eric Bodden, and Heike Wehrheim. Do android taint analysis tools keep their promises? In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2018, pages 331–341. ACM, 2018.
- [13] Dmitry Prudnikov. UX design techniques for mobile apps. <https://yalantis.com/blog/ux-design-techniques-mobile-app-design/>, 2019. Accessed: 05-Feb-2019.
- [14] Venkatesh-Prasad Ranganath and Joydeep Mitra. Are free android app security analysis tools effective in detecting known vulnerabilities? *CoRR*, 2018.

- [15] Alireza Sadeghi, Naeem Esfahani, and Sam Malek. Mining the categorized software repositories to improve the analysis of security vulnerabilities. In *International Conference on Fundamental Approaches to Software Engineering*, pages 155–169. Springer, 2014.
- [16] Sketch. Sketch Design ToolKit. <https://www.sketchapp.com/>, 2019. Accessed: 05-Feb-2019.
- [17] Square Open Source. A java api for generating java source. Available at <https://github.com/square/javapoet>.
- [18] Sufatrio, Darell J. J. Tan, Tong-Wei Chua, and Vrizlynn L. L. Thing. Securing Android: A survey, taxonomy, and challenges. *ACM Comput. Surv.*, 47(4):58:1–58:45, 2015.
- [19] Rahul Telang and Sunil Wattal. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Trans. Softw. Eng.*, 33:544–557, 2007.
- [20] Marcus Trapp and René Yasmin. Addressing animated transitions already in mobile app storyboards. In Aaron Marcus, editor, *Design, User Experience, and Usability. Web, Mobile, and Product Design*, pages 723–732. Springer Berlin Heidelberg, 2013.