Introducing: SIRA Semi-automated iOS Rapid Assessment

Justin Engler | Seth Law | Joshua Dubik | David Vo

THE NEED FOR TESTING iOS APPS

- US iOS App Store
  - Over 680,000 applications
  - 1,121 new apps PER DAY
  - Average iOS device: 108 apps installed
- How secure are those apps?
- Are they all protecting your privacy?

The need for automation in testing

- Apple's testing insufficient
    - Privacy - Contact Lists
        - Many popular apps were found to be accessing contact lists
        - In many cases, contacts were sent back to a remote server, in some cases without encryption
        - New versions of iOS will require a user confirmation

The need for automation in testing

- Privacy - Location tracking issues
    - Apps were found to be tracing user location without any confirmation
- Security Testing
    - Compliance to Apple's policies vs Actual Security?

THE NEED FOR AUTOMATION IN TESTING

- Technical knowledge required
  - Average iOS users cannot adequately test apps themselves
  - Need to know:
    - Network traffic analysis
    - iOS file system
    - Application reverse engineering (specific to iOS)
    - Cryptographic attacks
    - Jailbreaking
    - iOS app development
    - Web Application Security

THE NEED FOR AUTOMATION IN TESTING

- Even a technically skilled user is unlikely to have a solid understanding of all of the above (present company excepted)
- Time investment is high
  - Every app requires a bespoke, manual analysis (1,121 PER DAY)
- Currently available automation is not sufficient
  - Blacklist “AV”-type applications?
  - Can protect against actively malicious apps, but not against apps with unintentional security holes

THE NEED FOR AUTOMATION IN TESTING

- Some tools help
  - Proxies
  - Specific-issue finders
  - Tool to find apps that use the contact list
- Some of these are helpful, but a manual assessment still takes too long

THE NEED FOR AUTOMATION IN TESTING

- Full automation is not sufficient
  - App interfaces are unpredictable
  - Custom apps require custom testing
  - Some vulnerability types require a human
    - Machines can’t read intent (yet)
    - Authorization issues
    - Special encodings or “encryption” might not be transparent to a tool. A human tester might intuitively discover these issues

THE NEED FOR AUTOMATION IN TESTING

Manual tester + Automation Tools

=

True security of an application

SIRA Features

- Install Applications
- Record Application Activity
- Automatically “Drive” applications
  - Single app at a time, certain apps already implemented.
  - Most apps require credentials before accessing functionality
    - “Sign Up/Sign in” before credentials are used
      - Sent/Stored in Plaintext

SIRA Features

- “Drive” application (cont’d)
  - Find application controls (buttons, fields, etc.) and give them feasible values
  - Fuzz!

SIRA Features

- Search for issues
  - Issues in the file system
    - Cleartext credentials, etc.
  - Issues in network traffic
    - Lack of SSL
  - Privacy issues
    - Contacts are accessed
  - Correlate
    - Enter a known test contact into iOS contacts, watch for it to be accessed, watch for it to be sent to the server, watch for cleartext data

SIRA Features

- Manual Analysis Support
  - Allow manual intervention at any step
  - Automatic app driving to register an account doesn’t work? Manually run the app while all of the “recording” functionality is running
  - Display all automatic findings and confidence levels
  - Display raw data to allow analyst to easily find more issues

SURVEY OF APPLICATIONS

SURVEY OF APPLICATIONS (CONT'D)

- For the X applications tested, we noted several trends
  - Session ID storage
  - Credential storage

TOWARDS THE FUTURE

- To the crowd!
  - Testing still takes too long
  - Let users upload their test results?
  - Allow non-technical, non-jailbroken users to view security and privacy “ratings” for an app before install

TOWARDS THE FUTURe

- Are there any app developers who care about security?
  - How about a model where a developer can fund a semi-automated assessment?
  - The newly revised rating gets shown on the ratings site along with a special marker showing that the rating was manually validated?

Q&A