A Large-Scale Study of Mobile Web App Security

Eswarasanthosh Kumar Mamillapalli- 02065985

ABSTRACT:

A lot of network-related services and tools, like network monitoring systems, malware detection, and the systems used by Internet Service Providers (ISPs) for managing routing and billing, rely on being able to tell what kind of data is being sent over the network. Nowadays, with so many people using mobile devices and a huge variety of mobile apps, along with the common use of encryption methods (like TLS), it's getting much harder to classify and understand what type of data is being encrypted and sent across networks on a large scale. This research is about apps you can download for free from Google Play that use their internet browser. A lot of apps do this - about 85% of the free ones. These apps are a bit more complicated to make safely compared to normal web or mobile apps. The people doing the study came up with ways to find security problems in these apps. They looked at nearly a million of them, which is pretty much all the free web browser apps on Google Play up to June 2014. They discovered that more than a quarter of these apps had some security risks. The study also looks at how bad these risks are and tries to find common issues among the risky apps. It turns out that even the apps and tools that are widely used have some big security weaknesses. Finally, the study suggests some ideas for improving the tools used to make Android apps to help solve these security problems.

MOTIVATION:

Security is a big worry in the digital world today, and mobile web apps are now a big part of our daily lives. We use them for all sorts of things, like paying bills and managing our health. It's super important to make sure they are safe. There are more and more mobile devices out there, which means there are more ways for bad guys to try and break into our apps. So, we need to study and understand mobile web app security more than ever before. The motivation behind our project, "A Large-Scale Study of Mobile Web App Security," is rooted in the recognition of this urgency. We aim to address the following key reasons for undertaking this study:

1. **Growing Cybersecurity Threats:** The cybersecurity landscape is constantly evolving, with cyber threats becoming more sophisticated and pervasive. The rise of mobile web applications has made them a prime target for attackers. Our project seeks to uncover the extent of these threats and vulnerabilities, which is crucial for developing effective countermeasures.

2. **User Data Protection:** Mobile web apps often handle sensitive personal and financial information. Safeguarding this data is essential to protect the privacy and security of users. By comprehensively examining the security of these apps, we contribute to the protection of user data.

3. **Knowledge Advancement:** Research in mobile web app security is vital for advancing our understanding of emerging threats and vulnerabilities. The insights gained from this study can contribute to the development of better security practices, tools, and frameworks.

4. **User Confidence:** A secure mobile web app ecosystem fosters user trust and confidence. Our project aims to enhance user confidence in the security of the apps they use, thereby promoting their continued adoption and usage.

5. **Impact on Society:** In an increasingly interconnected world, security is not just a technical issue; it's a societal concern. A robust study of mobile web app security can have a broader societal impact by helping protect individuals and organizations from cyber threats.

INTRODUCTION:

Mobile operating systems let other companies make their own apps. Usually, these apps are made for a specific type of phone and can't easily be used on other kinds. But, developers can use their web programming skills to make a different kind of app called a mobile web app. This app works inside a browser on the phone and shows web content. It's easier to update and move to different phone types. However, keeping these apps safe is tricky and different from regular app or web security.

This study looked at three kinds of security problems in a huge number of these apps (almost a million) for Android phones. They found that 28% of these apps had at least one security issue. The study also showed that many of these issues are worse because the apps use older versions of Android. These problems are found in all kinds of Android apps, even the popular ones. The researchers suggest some changes to Android to help fix these security issues.

The main points of the paper are:

1. The researchers made new ways to find different security issues in mobile web apps.

2. They did a big study on a lot of Android apps to see how common these security problems are.

3. They looked at trends in these issues and found they're common across all Android apps.

4. They recommend some changes to Android to help solve these security problems.

ANALYSIS:

The paper conducts a large-scale study to identify security vulnerabilities in mobile web apps. Here's a simplified explanation of their findings and analyses:

1. **Checking for Risky Web Content**: They saw if apps were loading dangerous stuff from the internet or using HTTP, which isn't very secure. They did this by looking at the web addresses used in the apps, seeing how the apps go from one page to another, and then pretending to use the apps to see if they would go to unsafe places on the internet.

2. **Checking for Exposed Sensitive Operations**: The researchers checked if apps were letting outside sources trigger important actions without the user knowing, which could lead to attacks.
3. **How Apps Handle SSL Errors:** They looked at whether apps stop loading things when there's a problem with the website's security certificate. Some apps don't stop, which could be risky.
4. **Overall Findings:** Of all the apps they looked at, 28% had some kind of security problem.
5. **Specific Security Issues:**
   - 15% of apps could go to unsafe web places.
   - 40% got content from the internet in a way that's not safe.
   - 27% didn't handle SSL certificate errors well.
   - 1.9% let outside sources trigger important actions inside the app.
   - 10% had issues with leaking web addresses to other apps.
   - 193 apps were loading stuff from web addresses that no longer existed, which is risky.
6. **Problems in Libraries:** Many security issues were found in the libraries the apps use, especially those for ads or app development.
7. **Trends in Vulnerabilities:** Interestingly, more popular, or recently updated apps didn't always have fewer security problems. Some had more issues with certain kinds of attacks.
8. **A Big Problem with JavaScript Bridge:** A big issue was found in apps using something called JavaScript Bridge, especially older ones, which could lead to serious attacks.
9. **How to Fix These Issues:** The paper suggests some ways to make apps safer, like letting developers list safe web addresses, showing users how secure their connection is, and giving warnings during app development for risky actions.

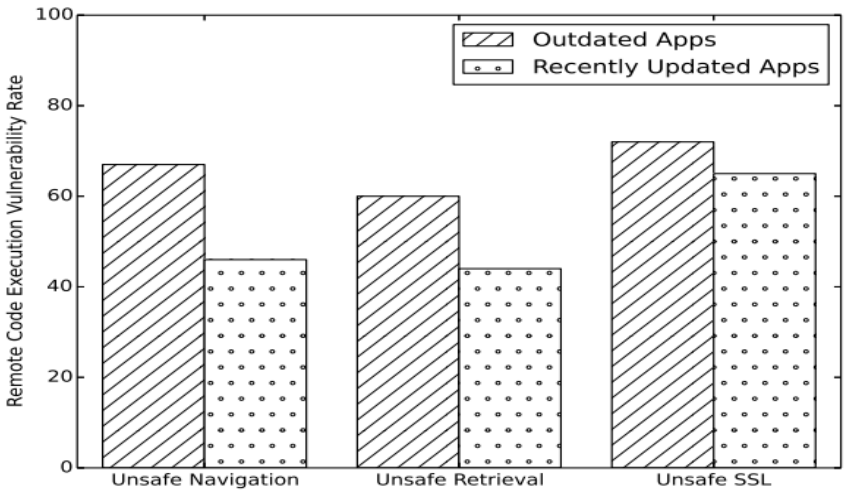
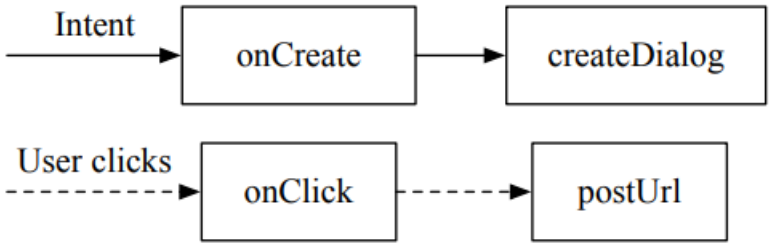


Fig. 6: A comparison of Remote Excecution Exploit rates between apps that have been updated or first published within one year of data collection (June, 2014) and apps that have not been updated recently.

DISCUSSION:

Some security issues in mobile web apps are related to how these apps talk to each other and the Android system. Android uses a special system for this communication called Intents. When an app sends an Intent, it can either pick a specific part of another app to talk to, or it can just say what kind of action it wants to do, like sending an email, searching the web, or taking a photo.



There are two types of Intent. If an app sends an "Explicit Intent," it goes only to a specific part of another app that it chooses. But if it sends an "Implicit Intent," which is just about an action, any app that can do that action might respond. Apps list what actions they can do in a file called Manifest, which is like a guidebook included with the app. This Manifest tells the system which parts of the app can handle which actions. Apps can also say that they can respond to requests to view certain types of web content by setting up a custom URL pattern in their Manifest.

RECOMMENDATIONS:

The study suggests some ideas to make mobile web apps safer:

1. **List of Safe Websites**: Let app makers add a list of safe websites directly into the app's settings. This would make it easier to keep the app from visiting risky websites, instead of using complex methods to control where the app can go on the internet.

2. **Limiting Special Web Features**: Only let app developers give certain parts of their app the ability to use special web features, and only for websites they trust. This is to stop unsafe websites from using these features, which can be a security problem.

3. **Show How Secure the Connection Is:** Let users see if their internet connection is safe. Right now, people can't tell if their connection is secure, so they don't know if it's safe to put in private information.

4. **Warnings for Handling Web Security in Android Studio:** In the app development tool Android Studio, show a warning if developers are using a certain method that could ignore

web security problems. This is like a current warning about using JavaScript, and it would help developers avoid making apps that don't pay attention to security warnings.

5. **Unique Web Addresses for Apps**: Allow developers to make special web addresses for their apps that no other app can use. This stops apps from accidentally sharing these special web addresses. Android already does something similar for app permissions.

By doing these things, we can make mobile web apps less likely to have security problems and reduce how serious these problems are.

LIMITATIONS AND FUTURE PLANS:

The study had to make some compromises and also suggest areas for future research. Because it looked at so many apps, the researchers didn't go into detail in their analyses. This means they might have missed some security problems or wrongly identified them. They were especially careful when looking at web addresses in the apps, which could mean they didn't find every URL. Their methods for checking security, like for SSL certificate errors, were very cautious. They only pointed out problems if the whole way the app handled these errors was insecure. Also, in their simpler checks for certain kinds of security risks, they sometimes got it wrong – about 16% of the time. Looking ahead, they think future studies should try to be more thorough in their analyses without losing efficiency, get better at finding security issues in apps, and make fewer mistakes in large studies of app security.

CONCLUSION:

Mobile web apps, which let web content interact with app code, have unique security issues that are different from those in regular mobile or web platforms. The study focused on a few specific security problems in these apps and used methods that could work on a large scale to find them. They looked at nearly a million mobile web apps and discovered that 28% had at least one security issue. However, their methods were on the cautious side, meaning the actual number of apps with problems could be higher. They noticed that these security issues were everywhere in the app world, affecting everything from common libraries to the most popular apps. The study also suggested some changes to the Android programming tools that could help make these kinds of security issues less common and less serious.

REFERENCES:

- BARTEL, A., KLEIN, J., LE TRAON, Y., AND MONPERRUS, M. Dexpler: Converting Android Dalvik Bytecode to Jimple for Static Analysis with Soot. In Proceedings of the ACM SIGPLAN International Workshop on State of the Art in Java Program Analysis (2012).

- BARTH, A., JACKSON, C., AND MITCHELL, J. C. Securing Frame Communication in Browsers.
- BUGIEL, S., DAVI, L., DMITRIENKO, A., FISCHER, T., SADEGHI, A.- R., AND SHASTRY, B. Towards Taming Privilege-Escalation Attacks on Android. In Proceedings of the 19th Symposium on Network and Distributed System Security (2012).
- CHEN, E. Y., PEI, Y., CHEN, S., TIAN, Y., KOTCHER, R., AND TAGUE, P. Oauth demystified for mobile application developers. In Proceedings of the 21st ACM Conference on Computer and Communications Security (2014).
- CHIN, E., FELT, A. P., GREENWOOD, K., AND WAGNER, D. Analyzing Inter-Application Communication in Android. In Proceedings of the International Conference on Mobile Systems, Applications, and Services (2011).