Permission Re-Delegation: Attacks and Defenses

paper summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

When an application with specific permissions performs privileged task for an application without that permissions, then permission re-delegation occurs. This is dangerous as it may lead to user privacy violations. Application with privileges can be referred to as a deputy and this problem is a confused deputy problem. Permission re-delegation applies to web browsers (web applications), as well as smart phone operating systems (smart phone applications). The authors performed case study, in which they examined a set of 872 applications and found that, 37% applications are at risk of facilitating permission re-delegation. Also, they found 15 delegation vulnerabilities in 5 system applications. As a defense, the authors propose 'ipc inspection'. "When an application receives a message from another application, they reduce the privileges of the recipient to the intersection of the recipient's and requester's permissions"[1]. The basic rules are, first, they make a list of current permissions of each applications, second, they build privileged reduction in systems' inter application communication process, third, they allow receiving application to accept or reject messages[1]. The important problem arises when deputy may need to service user and multiple app requesters simultaneously. The solution is to create one instance per request. Also, the authors set different rules according to the types of communication. Author's claimed that their technique was able to stop both broken application and system application based attacks.

2 Contribution

The authors highlighted permission re-delegation issue. They contributed by proposing 'ipc inspection', as a remedy to the permission re-delegation problem.

3 Strengths

The paper explains the problem and the solution very well. I liked that the authors highlighted permission re-delegation problem and emphasized on remidifying this dangerous problem as soon as possible.

4 Limitations

I think the important limitation is performance. As, creation of new instance is costly, if multiple instances are created for multiple apps, then the performance degradation will be higher, also it will consequently affect battery life.

5 Future Work

I think in future, system applications should designed to prevent permission re-delegation. Also more work can be done to prevent prevent permission re-delegation attacks using return values from request-reply ipc.

References

[1] Felt, Adrienne Porter and Wang, Helen J. and Moshchuk, Alexander and Hanna, Steven and Chin, Erika, *Permission Re-delegation: Attacks and Defenses*, SEC, (2011)