AndroSSL

DÉVELOPPEMENT D'UNE PLATEFORME AUTOMATISÉE POUR LA VALIDATION DES CONNEXIONS SÉCURISÉES DES APPLICATIONS ANDROID

Colloque de l'ARC dans le cadre du 84e Congrès de l'Acfas, 10 mai 2016, Montréal

Prix étudiants de l'ARC — Édition 2015-2016

MARC-ANTOINE FERLAND et MARC-ANTOINE FORTIER

Étudiants en techniques de l'informatique
Cégep de Sainte-Foy

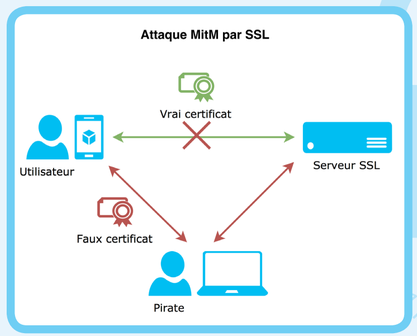
Sous la supervision de
François Gagnon, enseignant

1 contexte

Le monde de la technologie mobile est en pleine croissance et des centaines de millions d'utilisateurs à travers le monde font confiance aux différentes applications qui leur sont proposées. Mais est-ce que ces applications sont dignes de confiance pour ce qui concerne la protection des données ? Malheureusement, le monde du développement Android est dénué de normes de bonne gestion des échanges sécurisés sur le Web, et plusieurs développeurs laissent, sans nécessairement le savoir, de nombreuses failles de sécurité dans leurs applications.

2 objectif

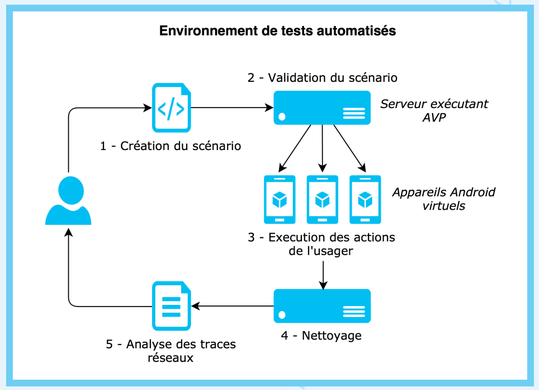
Actuellement, aucune plateforme ne permet de valider facilement et automatiquement la fiabilité et la sécurité d'une application lors de ses connexions réseau avec son serveur. Notre mission a été de développer une plateforme presque entièrement automatisée servant à confirmer la sécurité des applications Android en matière de gestion des échanges de données par le protocole SSL/TLS et, ainsi, de détecter les applications sensibles aux attaques MitM. Une attaque MitM [voir la figure] est une attaque où le pirate s'interpose entre le client et le serveur. AndroSSL permet de valider une quantité impressionnante d'applications avec un effort minime, qui se résume à exécuter une seule fois les étapes.



3 méthodologie

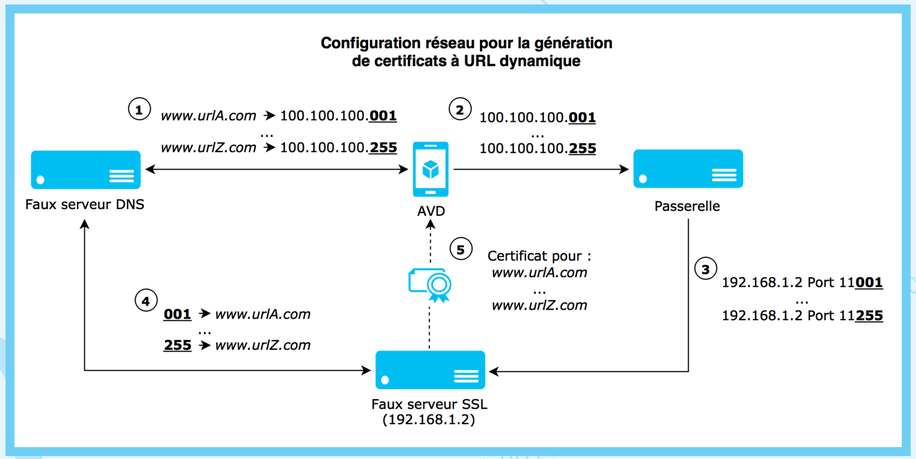
Construction d'un environnement de tests automatisés

Nous avons bâti un outil parallélisable à grande échelle en faisant appel à un système de virtualisation afin d'offrir le plus d'extensibilité possible quant aux types de tests effectués. Notre environnement virtuel permet entre autres d'ouvrir une machine virtuelle Android, d'y installer une application et de l'exécuter. Pour automatiser nos tests, nous avons implémenté des fonctionnalités pour enregistrer et rejouer les interactions d'un usager qui mènent au processus d'authentification sur une application. Nous pouvons ainsi déclencher à volonté les connexions SSL de l'application en envoyant à notre environnement virtuel un script contenant l'application à installer et les commandes préenregistrées.



Mise en place d'une configuration réseau complexe

Cette étape vise à simuler un environnement soumis à des conditions similaires à celles rencontrées lors de l'utilisation normale des applications. C'est grâce à cette configuration réseau minutieusement conçue que nous avons effectué les attaques *man-in-the-middle*, où nous interceptons toutes les communications entre l'application et son serveur. C'est là où nous distinguons les applications sécuritaires de celles qui vont mal vérifier (et accepter) les faux certificats que nous lui avons fournis. Ce sont ces dernières qui nous permettront de décrypter les données sensibles transmises, puisque celles-ci auront justement été encryptées avec des clés que nous avions nous-mêmes générées.



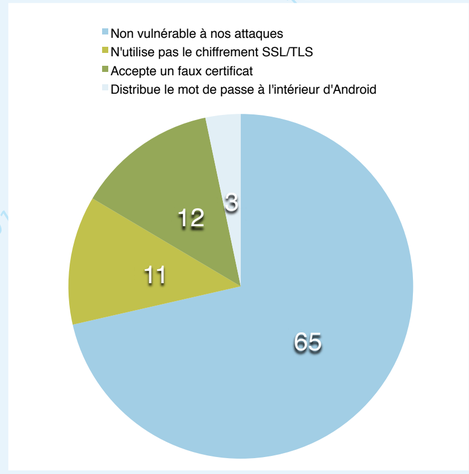
4 résultats

Échantillon

90 applications Android populaires provenant du top 500 de leur catégorie respective dans le Google Play Store.

Applications vulnérables

Si notre échantillon est représentatif des applications les plus téléchargées sur le marché Android, plus de 25 % des applications utilisées par des centaines de millions d'utilisateurs mettent en péril la confidentialité des informations personnelles.



5 conclusion

Si les développeurs testaient leurs applications avec notre outil avant de les rendre disponibles au grand public, cela garantirait que les applications téléchargées vérifient adéquatement l'identité des serveurs distants avec lesquels les utilisateurs échangent les données confidentielles (donc invulnérables aux attaques SSL de type *man-in-the-middle*). Comme ce sont les développeurs d'applications mobiles qui sont responsables de l'implémentation des mécanismes de vérification SSL, nos résultats auront un sérieux impact sur le développement d'applications Android futures.

Révision linguistique : **Le crayon rouge enr.** Design graphique : **Guylaine Hardy Design**