



Offre n°2024-08385

Internship - Analysis of TLS handshakes in Android apps (F/M)

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : Stage

Niveau de diplôme exigé : Bac + 4 ou équivalent

Fonction : Stagiaire de la recherche

A propos du centre ou de la direction fonctionnelle

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region. For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

Contexte et atouts du poste

Research team:

The student will join the Spirals project-team led by Lionel Seinturier (Professor, Spirals) <lionel.seinturier@univ-lille.fr>. Spirals is a joint project-team between Inria and the University of Lille, within UMR CRISTAL.

Mission confiée

Scientific Context:

In the 1990s, Netscape introduced [SSL \(Secure Sockets Layer\)](#), a security protocol designed to secure Internet communications. SSL enables an encrypted connection between a client (such as a Web browser) and a server (such as a Web site). This encryption protects data exchanged between the two parties from eavesdropping and ["man-in-the-middle" attacks](#) in which unauthorized third parties attempt to hijack communications. Today, SSL has been largely replaced by a more secure version called TLS (Transport Layer Security) [Dierks99, Dierks06, Dierks08, Rescorla18], which addresses a wide range of potential attacks. Over the past decade, the scientific community has developed several tools to analyze attributes present in the "Client Hello" and "Server Hello" phases of the TLS protocol. These initial, unencrypted exchanges negotiate the encryption protocols that will secure the rest of the session, and tools have been developed for both [server-side](#) and [client-side](#) analysis. It is even possible to create unique TLS-fingerprints of websites (both legitimate and malicious) [Althouse15, Althouse23]. On Android, however, fewer tools are available and TLS customization options are more limited. Often, the TLS library used is part of the operating system (in 84% of apps) and can only be updated through an OS update [Razaghpanah17]. As a result, Android applications may be more susceptible to security vulnerabilities during the TLS handshake.

Internship Project

This project aims to collect various relevant attributes from the TLS handshake initiated by applications running on Android devices. Analyzing the distribution and frequency of these attributes will make it possible to identify and quantify the security vulnerabilities present in these applications. This study can be conducted across multiple versions of Android devices and systems, allowing for a comparison of the impact that different models and OS versions have on the TLS configuration security of these applications.

References:

- [Razaghpanah17] - Razaghpanah, A., Niaki, A.A., Vallina-Rodriguez, N., Sundaresan, S., Amann, J., Gill, P.: **Studying TLS Usage in Android Apps. Conference on Emerging Networking EXperiments and Technologies.** pp. 350–362. (CoNEXT'17), Association for Computing Machinery. <https://doi.org/10.1145/3143361.3143400>
- [Althouse15] - Althouse, J.:**TLS Fingerprinting with JA3 and JA3S.** 2015 <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967/>
- [Althouse23] - Althouse, J.:**JA4+ Network Fingerprinting.** 2023 <https://blog.foxio.io/ja4+-network-fingerprinting>
- [Dierks99] - Dierks, T., Allen, C.:**The TLS Protocol Version 1.0.** 1999 <https://www.rfc-editor.org/rfc/rfc2246>
- [Dierks06] - Dierks, T., Rescorla, E.:**The Transport Layer Security (TLS) Protocol Version 1.1.** 2006 <https://www.rfc-editor.org/rfc/rfc4346>
- [Dierks08] - Dierks, T., Rescorla, E.:**The Transport Layer Security (TLS) Protocol Version 1.2.** 2008 <https://www.rfc-editor.org/rfc/rfc5246>
- [Rescorla18] - Dierks, T., Rescorla, E.:**The Transport Layer Security (TLS) Protocol Version 1.3.** 2018 <https://www.rfc-editor.org/rfc/rfc8446>

Principales activités

The objective of this internship project is to collect attributes (TLS version; cipher suites; extensions...) from the TLS handshake initiated by applications running on different versions of Android devices and systems. Then, the intern will create an overview of the security of Android applications and identify vulnerabilities, both general and specific for each Android OS version.

Internship Programs

1. **Conduct a State-of-the-Art Analysis** Perform a thorough analysis of existing TLS handshake analysis tools and techniques, including both active and passive methods, as well as client-side and server-side approaches, particularly on mobile devices.
2. **Identify Relevant Attributes:** Compile a comprehensive list of relevant attributes from the TLS handshake that warrant collection. Subsequently, create a detailed dataset of these attributes gathered from various Android versions and devices.
3. **Prepare Security Overview and Vulnerability Analysis Reports**
 - **Security Overview Report:** Draft a report that outlines the overall security status of Android applications, highlighting patterns and distributions of security attributes.
 - **Vulnerability Analysis:** Conduct a focused assessment of vulnerabilities associated with different Android OS versions, identifying trends and discrepancies among them.
4. **Develop a Comparison Report** Create a summary that compares how security attributes vary across different Android versions, including actionable recommendations for enhancing security in newer OS releases.

This project will benefit from our experience in the domain of browser and android devices fingerprinting, Android apps development as well as through the datasets collected by the AmiUnique.org website and [application](#).

Compétences

Technical skills and level required

The student should be proficient in at least one programming language. During the internship, they will develop their skills in Javascript, Web privacy, Android apps, as well as statistical data analysis.

Languages:

- English (minimum B2) is mandatory.
- French is optional.

Relational skills:

The student should be comfortable working in teams as well as individually.

Other valuable practice:

As is a common practice in the Spirals research team, all source code is expected to be open sourced, and

the student is encouraged to participate in open source and online communities.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + possibility of exceptional leave (sick children, moving home, etc.)
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

The student will work 35 hours per week, and they will receive the minimum gratification for an intern in a French public institution (€4.35/hour net in 2024).

Informations générales

- **Thème/Domaine** : Sécurité et confidentialité
Systèmes d'information (BAP E)
- **Ville** : Villeneuve d'Ascq
- **Centre Inria** : [Centre Inria de l'Université de Lille](#)
- **Date de prise de fonction souhaitée** : 2025-03-01
- **Durée de contrat** : 6 mois
- **Date limite pour postuler** : 2025-02-03

Contacts

- **Équipe Inria** : [SPIRALS](#)
- **Recruteur** :
Fayolle Iliana / iliana.fayolle@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

This internship project is aimed at Master 1 or Master 2 students for a period of 4 to 6 months.

Please read these articles to familiarise yourself with the subject:

- Agarwal, A.: **TLS Fingerprinting using JA3 for Android Application**. 2024 <http://www.theseus.fi/handle/10024/866474>
- Razaghpanah, A., Niaki, A.A., Vallina-Rodriguez, N., Sundaresan, S., Amann, J., Gill, P. **Studying TLS Usage in Android Apps**. Conference on Emerging Networking EXperiments and Technologies. pp. 350–362. (CoNEXT'17), Association for Computing Machinery. <https://doi.org/10.1145/3143361.3143400>
- Althouse, J.: **JA4+ Network Fingerprinting**. 2023 <https://blog.foxio.io/ja4+-network-fingerprinting>

During the interview, your understanding of the articles mentioned above will be assessed.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :

Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST).

L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.