Technology Offer

Reverse Fingerprinting: Identification of potential security risks associated with internet services

Background

Both corporate and private customers are increasingly using Internet services to process their data, including confidential files. The advantages: Data can be accessed from any location where an Internet connection is available, files can be shared, and software can be used as a service.

However, up-to-date software is vital for data security, as many updates have the main function of closing identified security gaps. This is an important aspect when relying on software used by a provider, such as services, databases, programming environments, server software, server host, server hardware and infrastructure. Consequently, checking the software version is a standard task in auditing processes.

Problem

Up to now, it has not been possible to check what software version is installed without the service provider's support: version numbers are either hidden or can easily be faked.

Due to the fact that maintain software is time consuming and costly, service providers may be refrained from (or unable to) keeping their software up-to-date. However, this uncertainty is worrying for many users, as they are unable to track whether the service provider is installing upgrades in a timely manner, which is essential in terms of data security – especially when using publicly accessible servers.

Existing methods that search for security gaps (security audits) either require special access (vulnerability scanner), and are therefore often carried out by the providers themselves, or use dedicated interfaces to determine the version numbers (penetration tests).

Solution

The novelty of the invented Reverse Fingerprinting (RFP) method lies in the fact that the version numbers of installed software can be determined based on remote user queries without the need for any provider-side support.

When new software versions are released, a unique feature (fingerprint) that differs from the previous versions is identified once and a query pattern is created whose result allows to exclude certain software versions. By repeating this process with selected queries, a user can eventually determine the installed software version. These queries are stored in a database to allow for automated software version checking.

This method allows installed software versions to be verified, including updates and security of the platform used – purely through remote customer interaction.

TLB
Technologie-Lizenz-Büro
der Baden-Württembergischen Hochschulen GmbH

Contact
Dipl.-Ing. Erick Pérez-Borroto Ferrer
TLB GmbH
Ettlinger Straße 25
76137 Karlsruhe | Germany
Phone +49 721-79004-0
perez@tlb.de | www.tlb.de

Development Status
Proof of concept / TRL3

Patent Situation
PCT / EP 19 798 686.2 pending

Reference ID
18/071TLB

Service
Technologie-Lizenz-Büro GmbH manages inventions until they are marketable and offers companies opportunities for license and collaboration agreements.

Advantages

- Software versions used can be verified without provider-side support
- Broad range of applications through the use of intrinsic properties
- Independent of interfaces
- Numerous services such as forums, CMS, programming language, databases, server software and server host can be analyzed
- Efficient and automated execution on multiple systems

Application

This method newly developed by researchers at the University of Mannheim allows for verification of the software versions installed across the service provider's network without having to rely on dedicated interfaces or provider-side support.

Publikationen und Verweise

Christian A. Gorke, Frederik Armknecht:
"Reverse Fingerprinting",
arXiv preprint arXiv:1912.09734 (2019);
https://arxiv.org/abs/1912.09734