

 Contenuto archiviato il 2024-05-24



Automated Validation of Internet Security Protocols and Applications

Risultati in breve

Analisi dei protocolli crittografici con AVISPA

Nel quadro del progetto AVISPA, sono stati ideati nuovi strumenti che supportano una validazione automatica ma rigorosa dei protocolli di sicurezza Internet. Grazie al formato di input costituito da un linguaggio di specificazione d'alto livello, forniscono il livello di sicurezza richiesto dagli sviluppatori e dagli utilizzatori nello sviluppo dei protocolli di sicurezza della prossima generazione.



In molti servizi e applicazioni di rete, in cui l'integrità, la confidenzialità e altre proprietà di dati sono decisive, i protocolli crittografici rivestono un ruolo di primo piano: permettono infatti l'autenticazione sicura di entità e l'apertura di canali di comunicazione sicuri tra agenti per la condivisione dell'informazione, proteggendo al tempo stesso la privacy degli

input.

Con la grande diffusione di Internet e dei servizi in rete, i nuovi protocolli di sicurezza in corso di sviluppo metteranno le ali all'attuale capacità di analizzarli e validarli in modo rigoroso. Per accelerarne lo sviluppo e al tempo stesso migliorarne l'affidabilità, è decisivo disporre di strumenti automatici robusti per individuare i difetti in un protocollo sensibile alla sicurezza, oppure stabilirne con certezza l'assenza.

Lo strumento AVISPA ha risposto alla sfida in modo sistematico, provvedendo un linguaggio formale modulare e altamente espressivo per la modellizzazione dei protocolli di sicurezza e la specificazione delle loro proprietà ricercate. Le specifiche dei protocolli di sicurezza scritte in HLPSL (High-Level Protocol Specification Language) AVISPA sono tradotte in formalismo RewriteBase, il formato intermedio (IF), prima dell'input in quattro differenti back-end. Un protocollo di sicurezza scritto in IF viene eseguito per un numero finito di iterazioni, oppure interamente se non è implicato nessun loop. Alla fine o viene identificato un attacco o il protocollo è considerato sicuro.

Implementando una varietà di analisi tecniche che vanno dalla falsificazione alla verifica vincolata e non vincolata, i back-end eseguono l'analisi e ne producono i risultati nel formato d'uscita precisamente definito. Lo strumento AVISPA è dotato di un'interfaccia grafica che supporta la modifica delle specifiche del protocollo e permette all'utilizzatore di selezionare e configurare i back-end integrati nello strumento. Una volta terminato, se lo strumento trova un attacco al protocollo lo visualizza come file MSC (Message Sequence Chart) o postscript.

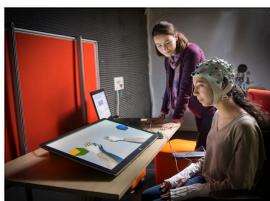
Allo strumento AVISPA si può accedere liberamente attraverso la sua interfaccia Web o scaricando il software distribuito e installandolo. Per maggiori informazioni: <http://www.avispa-project.org> 

Scopri altri articoli nello stesso settore di applicazione



Algoritmi per migliorare le condizioni del traffico sulle autostrade congestionate

6 Settembre 2019



Una formazione personalizzata migliora l'efficacia delle interfacce cervello-computer

16 Giugno 2023





Il multi-tasking ridefinito grazie a una nuova app

16 Gennaio 2018



Modelli comportamentali per potenziare la progettazione dell'interfaccia utente

15 Settembre 2020



Informazioni relative al progetto

AVISPA

ID dell'accordo di sovvenzione: IST-2001-39252

[Sito web del progetto](#)

Progetto chiuso

Data di avvio

1 Gennaio 2003

Data di completamento

30 Giugno 2005



Finanziato da

Programme for research, technological development and demonstration on a "User-friendly information society, 1998-2002"

Costo totale

€ 2 047 586,00

Contributo UE

€ 808 000,00

Coordinato da

UNIVERSITA DEGLI STUDI DI GENOVA

 Italy

Ultimo aggiornamento: 22 Gennaio 2007

Permalink: <https://cordis.europa.eu/article/id/83181-analysing-cryptographic-protocols-with-avispa/it>

European Union, 2025

