New cybersecurity tool checks for weaknesses in software components for internet traffic

May 18 2023

Professor Marc Dacier (left) and Ph.D. student Ilies Benhabbour (right) have developed a method to help detect the invisible components interfering with data being sent by two remote devices. Credit: KAUST; Anastasia Serin

When accessing a website or sending an email, we trust that our

information will arrive intact without being changed or read by any third party. In reality, keeping the information flowing on our vast global networks requires many intermediary processes, which may present security risks.

"In security, we say that the more complex a system is, the more vulnerabilities it has," explains Ilies Benhabbour, a Ph.D. student working alongside Marc Dacier.

"The internet was designed to function as a modular system, with each data transmission component assigned a specific task and enclosed within a layer of protection called encapsulation. During transmission, the data packets are concealed and should not be altered."

However, when a piece of information, such as an email, traverses today's internet, it will encounter several third-party software elements that are typically hidden from users. These network middleboxes, which Benhabbour and Dacier refer to as "semi-active components," generally enhance efficiency and security, for example, by compressing large data packets or checking for viruses.

Despite these useful intentions, some semi-active components may include code that does not meet international standards, is too complex or is just poorly configured. It is also possible that malicious hackers could impersonate middleboxes to steal or modify data.

While several tools exist for detecting semi-active components, they tend to be cumbersome and tailored only to a few specific internet protocols. With this in mind, Benhabbour and Dacier designed a new tool that is simple, modular and scalable to many situations.

They named it NoPASARAN, after the anti-fascist Spanish Civil War slogan "no pasarán" meaning "they shall not pass."

To date, the researchers have applied NoPASARAN to two test cases. The first examined Transmission Control Protocol (TCP), the ubiquitous communications standard for delivering information through networks.

"Our objective was to identify an invisible proxy machine that may be intercepting and reading the traffic," says Benhabbour. "You want to avoid such a scenario when accessing a bank account, for example."

The second test case was the Domain Name Server (DNS) protocol, which serves as the internet's "phonebook." Benhabbour explains, "Without DNS, one would need to remember a website's IP address (such as 5.23.65.23) instead of typing in the website name—for example, www.google.com. We aimed to determine the response received for a single name from two different machines."

Crucially, Benhabbour and Dacier have ensured it is easy for users to apply NoPASARAN without specialist knowledge of how TCP and DNS work. They plan to make the tool globally accessible so that it can be applied to more test cases.

"This research has the potential to enhance transparency throughout the internet and assist nonexperts in identifying network-related problems," says Benhabbour.

The study is published in the journal *Applied Cybersecurity & Internet Governance*.

More information: Ilies Benhabbour et al, NoPASARAN: a Novel Platform to Analyse Semi Active elements in Routes Across the Network, *Applied Cybersecurity & Internet Governance* (2023). DOI: 10.5604/01.3001.0016.1461