NetCap: Data-Plane Capability-Based Defense Against Token Theft in Network Access

Full Bibliographic Reference

O. Bajaber, B. Ji, and P. Gao. “NetCap: Data-Plane Capability-Based Defense Against Token Theft in Network Access”. In the Network and Distributed System Security (NDSS) Symposium. 2026.

Abstract

Tokens play a vital role in enterprise network access control by enabling secure authentication and authorization across various protocols (e.g., JSON Web Tokens, OAuth 2.0). This allows users to access authorized resources using valid access tokens, without the need to repeatedly submit credentials. However, the ambient trust granted to all processes within an authorized host, combined with long token lifetimes, creates an opportunity for malicious processes to hijack tokens and impersonate legitimate users. This threat affects a wide range of protocols and has led to numerous real-world incidents.

In this paper, we present NetCap, a new defense mechanism designed to prevent attackers from using stolen tokens to access unauthorized resources in enterprise environments. The core idea is to introduce unforgeable, process-level capabilities that are bound to authorized processes. These capabilities are continuously embedded in the processes' network traffic to target resources for validation and are frequently refreshed. This binding between process identity and capability ensures that even if access tokens are stolen by malicious processes, they cannot be used to pass authentication without valid capabilities. To support the high volume of requests generated by processes in the network, NetCap introduces a novel data-plane design based on programmable switches and eBPF. Through multiple optimization techniques, our system supports inline generation and embedding of capabilities, allowing large volumes of traffic to be processed at line rate with little overhead. Our extensive evaluations show that NetCap maintains line-rate network performance across a variety of protocols and real-world applications with negligible overhead, while effectively securing these applications against token theft attacks.

Link/DOI to the Published Paper

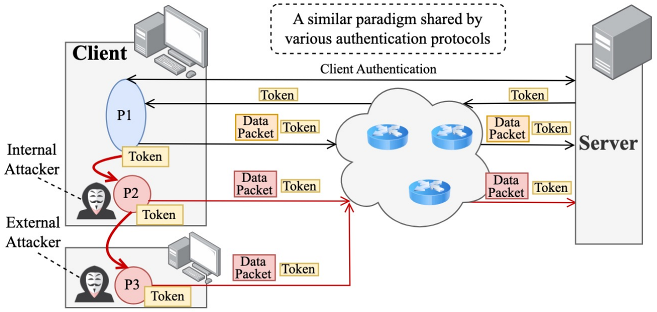
https://dx.doi.org/10.14722/ndss.2026.240273

NetCap: Data-Plane Capability-Based Defense Against Token Theft in Network Access [1]

Osama Bajaber, Bo Ji, Peng Gao

VIRGINIA TECH

(1) Token Theft Allows Malicious Processes to Gain Unauthorized Access

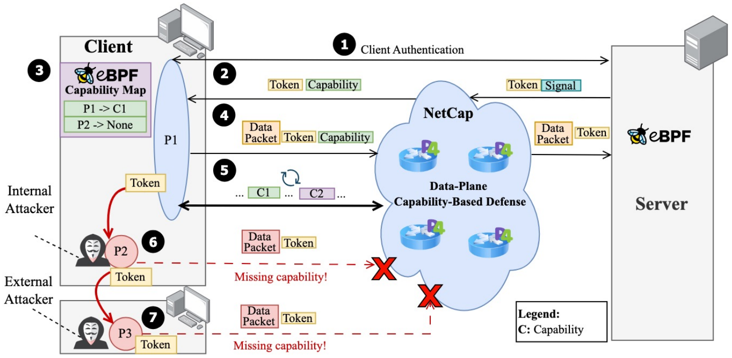


Tokens play a vital role in enterprise network access control by enabling secure network access across various protocols. This allows users to access authorized resources using valid access tokens, without the need to repeatedly submit credentials.

Challenge: Token theft remains a fundamental weakness in network access control, allowing attackers to **impersonate legitimate users** and gain unauthorized access to remote resources across **a wide range of protocols**.

The root cause is **ambient trust**: access tokens are often **not securely bound** to the authorized processes, enabling malicious processes, on the same host or different host, to reuse stolen tokens for **unauthorized access**.

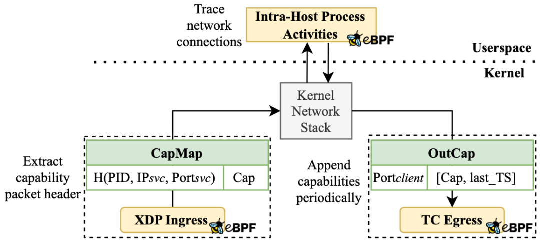
(2) Design of NetCap



Solution: A capability-based defense that **cryptographically binds** a lightweight, unforgeable **capability** to each authorized process and embeds it into network traffic for **continuous authentication**. Even if an access token is stolen, an attacker cannot use it without the corresponding valid capability.

In-Network Design: We leverage programmable switches to process packet headers that carry capabilities, and to inspect and validate them in real time. We also develop lightweight eBPF programs to efficiently trace processes, bind capabilities within hosts, and embed them into outbound traffic.

(3) Lightweight eBPF Programs



Our eBPF programs persist capabilities both within the host and from/to the network with minimal overhead. They perform **in-kernel capability management** by attaching carefully defined **eBPF hooks** in the kernel. This is achieved through:

1. **Extracting capabilities** from incoming packets
2. **Tracing network connections** to lookup the sending process's capabilities
3. **Modifying outgoing packets** to attach a capability header

(4) NetCap Configuration APIs

Configuration API	Description
AddService(IP, port)	Add a new service to NETCAP
AddPort(switch_id, port)	Enable NETCAP on switch port
SetLifetime(switch_id, lifetime)	Set key lifetime for a specific switch
SetHostInterval(IP, interval)	Adjust host's capability packet sending interval
SetSignalTimeout(duration)	Set the timeout for receiving signals from services

NetCap's APIs allow administrators to easily customize capability requirements with **little effort and no low-level data plane programming.**

These APIs let administrators define which services NetCap protects by **specifying** their IP and port addresses. They can also configure **how frequently capabilities** are sent.

This work [1] is supported in part by the National Science Foundation under grant CNS-2442171 and the Commonwealth Cyber Initiative. Any opinions, findings, and conclusions made in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

[1] O. Bajaber, B. Ji, and P. Gao. "NetCap: Data-Plane Capability-Based Defense Against Token Theft in Network Access". In NDSS. 2026.