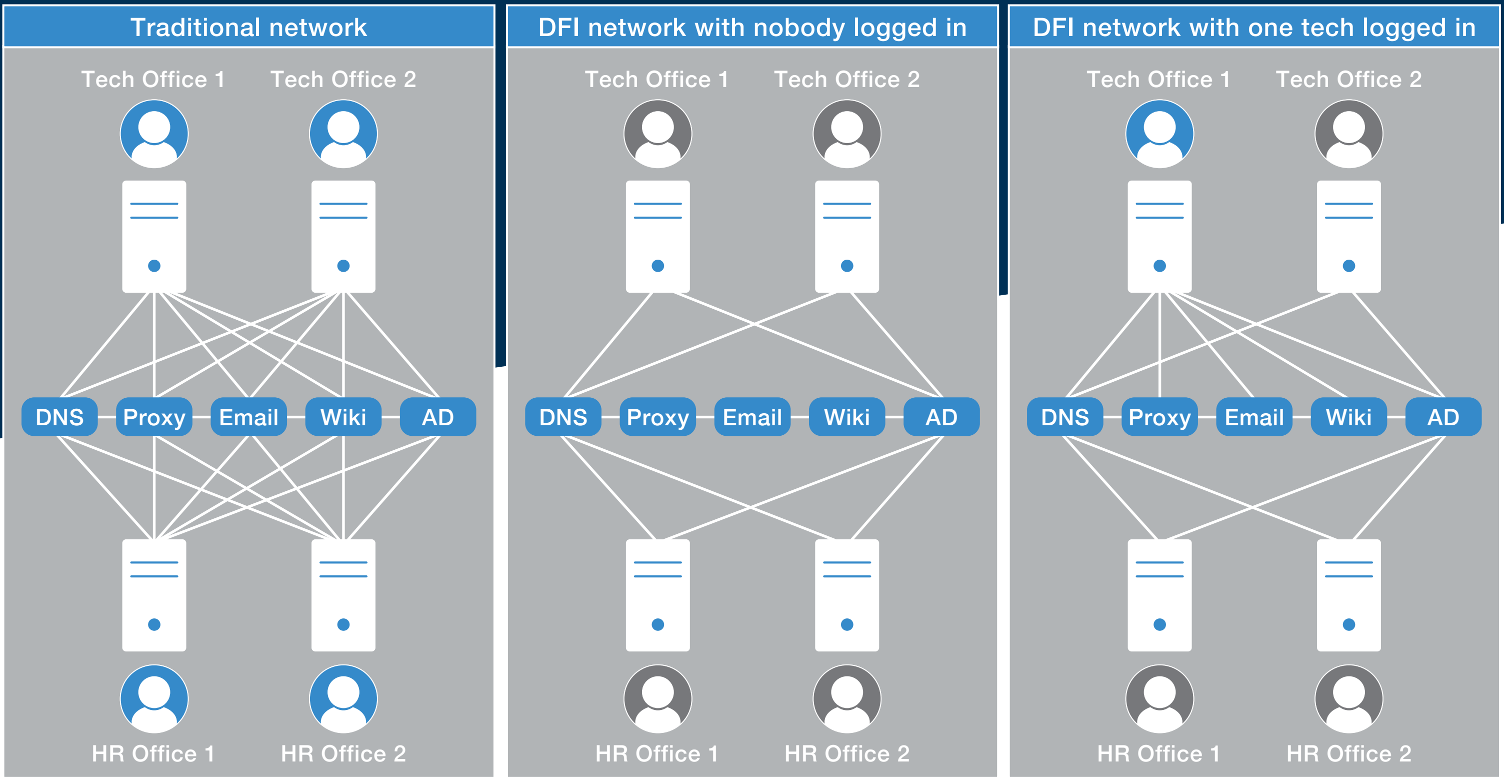
MIT LINCOLN LABORATORY

INNOVATION HIGHLIGHT

Technology in Support of National Security

WWW.LL.MIT.EDU

Dynamic Flow Isolation



In typical enterprise networks, all workstations have full connectivity in the network layer, potentially allowing attackers unrestricted access to the entire network. In the DFI strategy, systems logged off the network can only access the active directory (AD) and domain name system (DNS), and individuals are restricted to needed services.

This innovative technique reduces the likelihood of unauthorized users accessing data on a computer network and limits cyberattackers' ability to exploit software vulnerabilities, especially "bugs" not yet detected by network administrators. It enforces a network-layer policy that isolates users to just the resources (e.g., servers, databases, computers) they need to accomplish their tasks, reducing opportunities for misappropriation of data or network intrusion.

KEY FEATURES

- Supports access-control policies based on both low-level network header data and high-level entities like usernames
- Dynamically changes user access in response to policy-relevant events, such as a user's job transfer or an addition of a restricted database to the network
- Maintains a database of current policy directives for enforcing access and auditing user activity

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

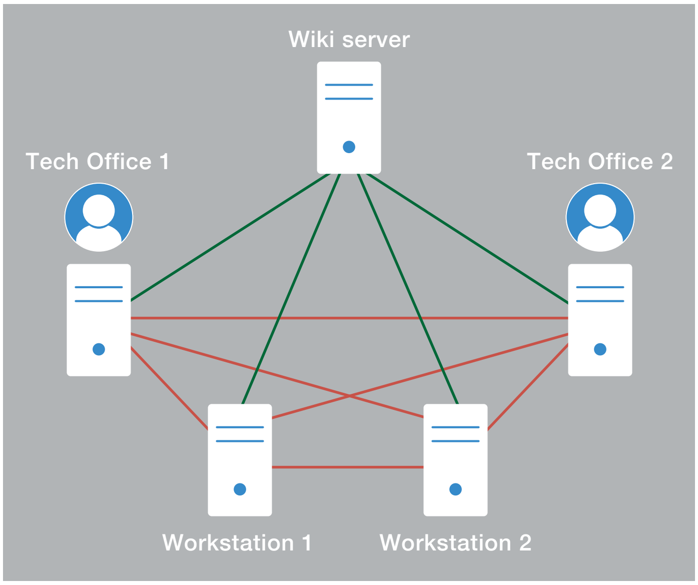
Problem

Cyberattackers can penetrate an organization's network by gaining a foothold in an individual user's computer via a phishing email or a vulnerability such as a "crackable" password. Because traditional networks allow all machines to potentially communicate with all others, the intruders can then infiltrate the network at will to access all the organization's data. In 2017, for example, the NotPetya malware installed itself in networks worldwide through a seemingly legitimate software update. Once cyberattackers find such a "backdoor" into a user's system, they can bypass perimeter defenses like firewalls from inside the network. Intrusion-detection systems deployed on a network often fail to detect attacks fast enough to prevent their spread.

Solution

Dynamic Flow Isolation (DFI) applies the principle of least privilege on the network layer. Commonly seen in operating and file systems, a least-privilege policy restricts user access to only the resources necessary for their current work. In an enterprise network, for example, no logged-off machine is able to access any resource but the authentication server, and no machine in an administrative enclave can communicate with a database of sensitive research results.

The DFI solution leverages software-defined networking (SDN), an architecture that separates the network into a logically centralized software control plane and a programmable hardware data plane. The SDN controller running DFI enforces fine-grained, event-based, adjustable connectivity in enterprise networks. A variety of sensors (e.g., authentication servers, antivirus detectors, and clocks) identify events/actions on the network. When this traffic enters the SDN, DFI compares it against the current access-control policies and directs SDN to dynamically implement, add, or revoke access-control rules. Traffic sensed as a violation of a current policy is dropped before it ever reaches the target machine. In simulations, DFI has shown to have negligible performance impact on permitted traffic and to substantially slow the movement of attackers through a network.



Dynamic Flow Isolation prohibits user access to systems not necessary to the user's work. In this example of a privilege scheme, the workstations may only communicate directly with the wiki server and not each other. This arrangement helps to mitigate attacks that seek to move from one user's workstation to a more privileged workstation like that of a system administrator.

INTERESTED IN ACCESSING THIS TECHNOLOGY?

Contact the MIT Technology Licensing Office
https://tlo.mit.edu/
tlo@mit.edu 617-253-6966

U.S. PATENT #10,778,722

INTERESTED IN WORKING WITH MIT LINCOLN LABORATORY?

https://www.ll.mit.edu/partner-us

Contact the Technology Ventures Office
tvo@ll.mit.edu

Approved for public release; distribution is unlimited. This material is based upon work supported by the Department of Defense under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.