Using Hardware "Fingerprints" to Enhance Network Security (#5818)

Addressing one of the most significant threats to the security of cyber infrastructure—that is, insider attacks by users with valid username/password credentials

Abdul Raheem Beyah and Cherita Corbett from the School of Electrical and Computer Engineering at Georgia Tech have developed an innovative intrusion detection system (IDS) with an entirely new approach to detecting evolving threats. Using hardware signatures that are innate in network traffic, the Georgia Tech system detects unauthorized devices that are inserted into the network.

This successful solution relies on the signature generated by the “behavior” of data packets—even those that are encrypted—and leaked into normal network traffic by the hardware. This unique hardware signature (akin to a fingerprint) makes it possible to determine whether a node is authorized to access the network, regardless of whether it achieved that access using legitimate login credentials.

Georgia Tech’s network-based approach has significant advantages over the current industry approach of using network access control (NAC) solutions. A NAC solution requires a client on each node that it manages to identify the node and to control access to the network. However, many devices are not NAC enabled because of an unsupported operating system (e.g., Mac OS, UNIX, Linux), and thus a large number of seemingly benign devices such as phones, printers, thermostats, and cameras are unmanageable and cannot be secured. Georgia Tech’s innovation does not require a client and therefore will work for unmanageable devices (which will far outnumber manageable devices in the future).

Benefits/Advantages

- **Long-Term Solution:** Because no software client is required, this technique can be used to identify both current and future unmanageable devices.
- **Failsafe:** Because it relies on inherently unique signatures tied to hardware’s diverse compositions, component manufacturers, and physical differences, the system is difficult to defeat by unauthorized—or even authorized—users.
- **Reduced Vulnerability:** As a network-based solution, this method eliminates the security vulnerabilities associated with software additions at each node.
- **Less Complex:** This approach functions with just a single system per network segment rather than multiple node-based systems.
- **Simple and Low-Cost Implementation:** The system is inexpensive to deploy and leverages existing infrastructure investments.

Potential Commercial Applications

All major companies and governments in the United States and abroad use NAC systems for access control and device management. This new system can be used to extend those systems to supplement current techniques for identifying manageable devices (i.e., devices running software clients) and as a new method that identifies unmanageable devices.

Background/Context for This Invention

A new technology from Georgia Tech is addressing one of the most significant threats to the security of cyber infrastructure—that is, insider attacks by users with valid username/password credentials. Existing attack detection methods have significant limitations that leave many types of devices unmanaged and insecure. This creates the opportunity for malicious authorized insiders to insert unauthorized devices that masquerade as authenticated devices. To be truly effective, the network security system must depend not solely on user authentication but also on device-based authorization.

Dr. Raheem A. Beyah
Dean and Southern Company Chair - Georgia Tech College of Engineering

Dr. Cherita Corbett
Chief Scientist - The Johns Hopkins University Applied Physics Laboratory

More Information

Publications

For more information about this technology, please visit:
https://licensing.research.gatech.edu/technology/using-hardware-fingerprints-enhance-network-security

Images:

The automated sequential delivery of multiple fluids. A varying number of delay gates imprinted in the branches are shown in the figure.

COVID-19 and flu saliva test on paper: (A) The automatic sequential delivery of multiple reagents required for virus test; (B) Water pouring into the device triggers the virus assay, allowing the presence of SARS-CoV-2 and influenza A & B viruses to be visually identified by the color changes in the corresponding detection spot