Network Access Control: User and Device Authentication
August 2005

Intel IT is piloting new security methods to provide network access control by authenticating devices as well as users. Since networking has evolved to support both wired and wireless access, securing corporate networks from attack has become ever more essential. Therefore, to effectively enforce network access control policies in a proactive manner, we are developing a method to authenticate users and devices before they connect to the network.

Background

As a global corporation, Intel IT supports more than 90,000 employees and contractors all over the world, and 80 percent of our knowledge workers are mobile and unwired. Network access depends more and more upon wireless LANs and WANs, as well as virtual private network (VPN) remote access. All of these technologies have the potential to open our network perimeter to threats. When we considered the threat of viruses and worms, it was evident that we needed additional controls to secure the enterprise network and its information assets from unauthorized devices and unauthorized people. Figure 1 shows how we could authenticate devices and users as part of the authentication pyramid.

Figure 1. Authentication pyramid

Network Access Control at Intel
- Over 90,000 employees worldwide
- 80 percent of knowledge workers are mobile and unwired
- Over 50,000 remote access users
What is Device Authentication?

When a device is attached to a network, it can report its identity in secure ways that affirmatively identify when a particular notebook computer or handheld device is accessing the network. We can accomplish this with automation, so the user in not inconvenienced; the device identity information exchange happens in the background, seamless to the user.

How We Build a Device Identity Profile

The concept of building a device identity profile is very similar to how we might establish a profile and metadata for a person. We store and retrieve the identity information in a similar way, and attach metadata that describes it.

- Device identity profile is recorded in a central repository
- Device identity profile contains metadata describing the asset

For a device to be secure, we associate it with some unique attributes—for example, is the device managed and security controlled by IT? What attributes need to be measured to ascertain whether the device is compliant to the company’s current minimum acceptable security specification?

Combining User and Device Identity

In many enterprises, anything plugged into the network is given access to the network. Devices can almost immediately begin broadcasting data and reading information, regardless of what they are. Today, networks face many security risks, whether wired or wireless. One of the most common is unauthorized network access by an unknown device (whether harmless or malicious) that connects to a network. These systems can be difficult to scan, patch, or control. Furthermore, an unauthorized device is difficult to identify and locate in a crisis.

At Intel, we are integrating standard technology, 802.1X and Extensible Authentication Protocol (EAP), into an overall device authentication system to check whether a device is identified and compliant before we grant a network connection.

Figure 2 illustrates the process used to grant access to the network. For illustration purposes, we define three types of users. The three user types are contractor, regular employee, and knowledge worker. In each of the three types, we have a different expectation as to the level of access that may be permitted. The knowledge worker is a particular employee type who normally needs to access information that is most sensitive to the network enterprise.

This figure reads from top to bottom, with the ultimate state at the bottom—the known user and known device.
There are many cases where an identified device may not be allowed on the network; for example, if it was reported as stolen, the metadata in the device identity or policy store would indicate that it should not be allowed.

**Applying Device Identity to Control Access**

For protection to be most effective, all access to the enterprise network perimeter edge needs to be secured. Without this, we don’t have a secure network. Using Figure 3 as an example, if we protected wired and wireless LANs, but not remote VPN, there would be an entry point through which someone could enter the network.

**The Authentication Process**

The core of the device identity design revolves around the ability to successfully authenticate a device as it attempts to become a node on the network. Table 1 shows the steps for getting into the network.

To start, we needed to prioritize where we leveraged device identification. We did a risk assessment, by geography and by connection type, and determined that our priority would be to focus on securing wireless LAN access, because 80 percent of Intel’s knowledge workforce is mobile and wireless.

The Authentication Process

The core of the device identity design revolves around the ability to successfully authenticate a device as it attempts to become a node on the network. Table 1 shows the steps for getting into the network:

Figure 4 outlines the authentication process and how our device identity program is configuring the process. Passing the credentials in a secure channel provides mitigation against common threats such as eavesdropping. We use Transport Layer Security (TLS) to establish a secure channel between the device and the authentication service. This is facilitated in much the same fashion as Web security between an Internet browser and a secure Web server, where the Authentication Service provides a certificate for encrypting the traffic and the device validates the certificate before establishing the secure channel and passing the credentials.

As part of our phased approach, we’re adding compliance enforcement, tied to the 802.1x authentication process.

### Table 1. Steps for “getting in”

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who are you?</td>
<td>Device responds to challenge with Public Key Infrastructure (PKI) information for identification</td>
</tr>
<tr>
<td>Were you expected to enter at this time?</td>
<td>Policy server checks identity against stored metadata for authorization</td>
</tr>
<tr>
<td>Are you “Okay” to enter?</td>
<td>Authorization policy decision drives network assignment (go/no-go)</td>
</tr>
</tbody>
</table>
Conclusion

Evolving network connectivity methods create a growing risk of rogue systems connecting to the corporate network. By piloting a program to authenticate devices before permitting production network connectivity, we are reducing the risk of exposure to attacks from malware and are providing a more robust computing environment to the enterprise.

For more information, visit our site on the World Wide Web: www.intel.com/IT

This paper is for informational purposes only THIS DOCUMENT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2005, Intel Corporation. All rights reserved.