Tracking Windows User Authentication

When a user successfully logs into a Windows Active Directory domain the event is recorded on the Domain Controller for that domain. By default, user logouts are only recorded on the local PC. This action can be changed forcing logon and logoff events to be recorded by the DC for the domain along with any unsuccessful logon attempts. Altering the default behavior requires that all PCs and users involved exist within the domain used for authentication.

Windows event logs are stored in a binary format and are not easily parsed by conventional script based methods. Microsoft does produce a tool, Log Parser, which allows "SQL like" queries to be made for retrieval of events from any Windows event log. To quote Microsoft,

"Log Parser 2.0 is a powerful, versatile tool that makes it possible to run SQL-like queries against log files of almost any format and produce the desired information either on the screen, in a file of any desired format or into a SQL database. Log Parser is available as a command-line tool and as a set of scriptable COM objects."

Commercial alternatives exist for parsing the log files created by Windows. The most prominent one is GFI Languard Security Event Log Monitor. SELM has both a server and workstation component that together provide monitoring of all security events within a domain. While this solution is very appealing in its abilities, it is cost prohibitive. 25 servers = $2135. 1000 workstations = $1599. While these prices seem low at first glance, keep in mind that this product provides a specialized functionality.

Given the variety of labs at UTC, the resources required to place all of the lab PCs into a single domain prohibit that plan of action. Any plan for recording authentication events would have to be "cross-domain." If recording of such information is required, a simpler and cheaper method must be found. Using a simpler authentication, such as RADIUS, maybe part of the solution.

UTC's Networking Group has already implemented a FreeRADIUS server for authentication. This server authenticates using the existing LDAP tree provided by Onenet. That is, the same username and password used for Onenet will authenticate against the FreeRADIUS server and that authentication will be recorded by the server. Windows PCs can be made to use RADIUS for authentication but this would interfere with authentication to any domain in which that PC currently belongs. Also, this method does not account for recording logoff events.

An even simpler method could be used which doesn't depend upon the authentication method; rather it relies upon a successful logon or logoff. Applications can be executed upon logon and logoff. A small, specialized application the mimics a similar event recording (logon/logoff) in Unix could be written which sends a small UDP packet to a syslog server to record the event. This would allow traditional methods of log parsing to be applied to the record of Windows authentications.

External References:

LogParser
http://www.microsoft.com/windows2000/downloads/tools/logparser/default.asp

Auditing Logon/Logout in Windows 2000 Active Directory
http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/monitor/logonoff.mspx

Microsoft Systems Management Server
http://www.microsoft.com/smserver/

GFI Languard SELM
http://www.gfi.com/lanselm/

FreeRADIUS
http://www.freeradius.org/

Windows 2003 Security Log
http://www.windowsitpro.com/Windows/Article/ArticleID/45269/45269.html