UND Port 25 Filtering Plan

Table of contents

I. Purpose
II. Background
III. Implementation
IV. Timeline
V. Potential Issues
VI. Definitions
VII. Effective Dates
VIII. Contacts

I. Purpose

E-mail is a critical service for all UND faculty, staff, and students. Our campus community depends on email to communicate with one another and with the outside world. It is important to have the proper controls in place to protect the integrity and availability of this critical service. This proposal outlines a plan and timeline for implementing a commonly accepted best practice of filtering port 25 to limit email communication only through known email servers on our network.

II. Background

Historically, spammers used vulnerable servers and open-relays to send large amounts of unsolicited email. The current trend is for spammers to infect end-user workstations with remote-control trojans to create what is referred to as a spam “zombie”. These spam zombies are used in distributed spam-rings to send unsolicited email directly without going through a server or open-relay. Since these zombie computers are on the UND network sending spam, our network, as well as the entire NDUS network, is at risk of being blacklisted, thereby limiting, or even eliminating, our ability to send email to the outside world. Implementing this proposal will restrict zombie computers from sending email off campus and will require email to go through authorized email servers on our network.

III. Implementation

In order to limit the risk of a wide-scale implementation, the recommended plan is to first filter email traffic on a single network (department/college) to monitor for any unanticipated consequences. This would involve identifying the legitimate email server(s) on this network and only allowing email traffic (outbound and inbound port 25) from this server. During this initial time-period, all departments and individuals will be given one month to register their legitimate email servers through a web registration process. At this point, there will be no approve/deny process for the registration of email servers, therefore any email server registered through the web interface will be permitted to send and receive TCP port 25 traffic, as long as the email server is
not being used to violate acceptable use policy (http://www.ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2551), i.e., for a personal business. After successful implementation on the single network and the resolution of any issues, all outbound port 25 traffic will be restricted to email servers which were identified during the registration period.

At this time, only filtering of traffic on TCP port 25 is being recommended, but additional ports may be added in the future as necessary.

IV. Timeline

*Tuesday, Feb 21, 2006*  
Filter port 25 for Business School (Gamble Hall) allowing traffic to and from mail.business.und.edu and from internal hosts outbound to on-campus email servers

*Monday, April 3, 2006*  
Launch Server Registration on http://itsecurity.und.edu/email/server_registration.html

*Monday, May 15, 2006*  
Restrict outbound and inbound port 25 traffic to registered campus email servers

V. Potential Issues

- Individuals who have their email client configured to communicate directly with off-campus SMTP servers will be blocked after May 15, 2006. Users who are not identified during the registration process and have a legitimate need to send email traffic to off-campus email servers will be identified after-the-fact and allowed to send traffic after review by the UND ITSO. Implementation of this plan will not affect any email web clients, such as hotmail, yahoo, or gmail, as they do not use port 25 to communicate.

- Any email server which is not registered prior to May 15, 2006 will be blocked from sending and receiving email off campus. It is possible that a legitimate email server may not be identified during the registration period; however, the server can still be registered after May 15 and will be given ability to send and receive email after a review by the UND ITSO.

VI. Definitions

Port 25 filtering  
*Simple Mail Transfer Protocol (SMTP)*, documented in RFC 821, is Internet's standard for sending email and traditionally operates over TCP, port 25. Blocking unauthorized traffic that is using TCP port 25 will in effect restrict that computer from sending email without going through an authorized email server. Only authorized email servers will be allowed to send email traffic using port 25.

Blacklist  
Lists of known spammers, their IP addresses, and/or their ISP (Internet Service Provider). Using this information, spam filters can block all messages coming from known spammers and/or their ISPs. ISPs that fail to discipline spammers may find all email from their legitimate customers blocked by large numbers of recipients.
VII. Effective Dates

Effective Date: March 29, 2006
Revised: N/A

VIII. Contacts

<table>
<thead>
<tr>
<th>Contact</th>
<th>Title</th>
<th>College/Department</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brad Miller</td>
<td>UND IT Security Officer (ITSO)</td>
<td>ITSS - Security</td>
<td>7-3587</td>
</tr>
<tr>
<td>Kevin Danielson</td>
<td>Senior Network Engineer</td>
<td>ITSS - Network Srvcs</td>
<td>7-4066</td>
</tr>
<tr>
<td>Keith Wildermuth</td>
<td>Lead Server Administrator</td>
<td>ITSS - Server Support</td>
<td>7-4784</td>
</tr>
<tr>
<td>Steve Ristau</td>
<td>Server Administrator</td>
<td>ITSS - Server Support</td>
<td>7-3889</td>
</tr>
<tr>
<td>Caylan Larson</td>
<td>Unix Administrator</td>
<td>Aerospace Sciences</td>
<td>7-2322</td>
</tr>
<tr>
<td>Harold Bruce</td>
<td>Lead Client Support</td>
<td>Business Administration</td>
<td>7-3945</td>
</tr>
<tr>
<td>John McCauley</td>
<td>Network Administrator</td>
<td>EERC</td>
<td>7-5146</td>
</tr>
<tr>
<td>Michelle Rakoczy</td>
<td>Network Administrator</td>
<td>Residence Services</td>
<td>7-0754</td>
</tr>
<tr>
<td>Carl Warrene</td>
<td>Systems Administrator</td>
<td>Law Library</td>
<td>7-5075</td>
</tr>
<tr>
<td>Kem Wilkerson</td>
<td>Electrical Equipment Technician</td>
<td>Chemistry</td>
<td>7-3989</td>
</tr>
<tr>
<td>Barry Pederson</td>
<td>Application Analyst</td>
<td>Medical School</td>
<td>7-2283</td>
</tr>
<tr>
<td>Cindy Filler</td>
<td>Advancement Services Director</td>
<td>Alumni Association</td>
<td>7-2611</td>
</tr>
</tbody>
</table>