IT Security of the NWSChat Application

NWSChat Admin Team

Updated April 8, 2010

NOAA's National Weather Service (NWS) has deployed a real-time interactive communications system for the purpose of improving decision support for community decision makers during high-impact events. The use of Instant Messaging (IM) and chatrooms have proved to be valuable for this type of communication in a number of real-time scenarios; therefore, the NWS has deemed NWSChat operational at this time. As with most Internet communication tools, IM technology comes with information technology (IT) security risks. This whitepaper outlines key IT security features of the NWSChat application designed to mitigate these risks.

The key IT security features of NWSChat are listed below:

Server Accessibility and Operating System Security

The NWSChat service is maintained by the NWS Office of the Chief Information Officer (OCIO) and is situated behind NOAAnet firewalls. NWSChat is comprised of a pair of servers configured in a resilient primary/backup configuration, and receives auto-updates for all operating system patches and bug-fixes. The systems are scanned quarterly to identify and correct IT security vulnerabilities as required by NOAA IT Computer Security policy. Future expansion of NWSChat include additional pairs of servers to be distributed across the country for increased redundancy and greater availability of access to the service.

Protocol Security: Identity Protection and Client-to-Server Encryption

NWSChat uses the Extensible Messaging and Presence Protocol (XMPP or Jabber) for communication. XMPP is an open standard and provides several levels of security at the protocol level. Since this security is built directly into the protocol it is globally supported by XMPP implementations.

Identity in XMPP is much stronger than other systems such as email. Users must authenticate to their host server (NWS-controlled) and messages from that user cannot be spoofed by simply replacing headers as is possible with email. This eliminates or reduces the problem of spam. In addition, federation can be easily and tightly controlled by limiting the federated hosts to a small white-list of allowed participants.

There are two types of encryption with XMPP. The first is encryption performed during connection establishment and authentication. Simple Authentication and Security Layer (SASL), an industry standard use by several protocols, is used during this phase. Once the connection is established, all transmissions between the client and server are encrypted using Transport Layer Security (TLS), another industry standard that grew out of the older Secure Socket Layer (SSL) protocol. These properties mean that XMPP is secure since both the connection establishment phase and the communication phase of the protocol are encrypted. NWSChat is configured to accept only encrypted connections. Once the connection is encrypted it stays that way and all messages sent between the client and server are encrypted.

Open Source Client and Server Software
NWSChat utilizes open source (non-proprietary) software for both the client and server applications. Several IM client applications are compatible with NWSChat, but the preferred client is named Pidgin. Pidgin is fairly intuitive and provides a tabbed display environment for simultaneous access to multiple chatrooms/sessions. Unlike commercial IM clients, Pidgin has no advertisements, spyware, or adware associated with the program. Pidgin is open source which means you can download the most recent source code and examine it if you have any questions about what's going on behind the scenes. The IM server software, called Openfire, is also open source and has made great advances in IM utility over the last few years (over 1 million downloads) due to ongoing development and scrutiny by the open source development community.

Encrypted Registration
All access to the NWSChat web server, including user registration for access to the service, is encrypted via the Hypertext Transfer Protocol (HTTP) over SSL or HTTPS. Both HTTP and SSL operate at the highest layer of the TCP/IP Internet reference model, the Application layer; but the security protocol operates at a lower sub layer, encrypting an HTTP message prior to transmission and decrypting a message upon arrival.

Closely Controlled User Accounting and Authorization Process
Individual user accounts are required for NWSChat; shared or group accounts are disallowed. A standardized account naming syntax is also enforced for manageability. To register with NWSChat, users must complete and submit an online form that requires the following information: username, email address, phone number, affiliation, and password, and select a primary office (currently a Weather Forecast Office (WFO), River Forecast Center (RFC), or Center Weather Service Unit (CWSU)) for authorization. Users are also required to acknowledge that they have read and agree to the NWSChat Terms of Use. Once submitted, the selected primary office receives an email of the request, and will approve or deny authorization for each user. Once approved, the requesting user is notified via email and then must complete online training for NWSChat. Only after completing all of these steps is the user's NWSChat account enabled. Documentation for NWSChat (terms of use, online training, IM client configuration, and FAQ's) are available on the web page.

Password Controls
All NOAA IT Security policy applies, including password security. NWSChat passwords must be comprised of 12 characters (mixed-case alphanumeric, special characters/symbols, and non-repeating patterns). Passwords expire after 180 days, after which the NWSChat user account is locked if the password has not been changed. Users are notified via email two weeks, one week, and one day in advance of a pending password change requirement. Users may change passwords at any time via the NWSChat web page. As with other applications, users are advised not to save passwords in the Pidgin client, but rather to enter the password when prompted.

Access Controls
Most multi-user chatrooms on NWSChat are open to NWS partners once they are authorized by the NWS. However, certain rooms are restricted for "members-only" access. This is necessary to secure information in specific chatrooms intended for certain partners only. For example, some information may be required by emergency managers that is not appropriate for media partners due to the sensitivity

of and timeliness of emergency operations. As a result, a members-only chatroom would be provided limiting access to NWS and authorized emergency managers exclusively, for a given location.

Firewall Protection
The NWSChat servers sit behind the NOAAnet firewall(s) which employ specific Internet traffic filtering as required by NOAA IT Security policy. Local (client-side) firewalls will need to allow outbound access for XMPP (TCP port 5222) to the nwschat.weather.gov (IP address: 140.90.113.204) service. All administrative access to the NWSChat servers is restricted to internal networks only.

File Attachments are Blocked
As with email, one of the key IT security threat vectors for IM is through file attachments. File attachments may contain malware such as viruses or trojans and must be scanned and filtered to avoid contamination via IM communications. Currently the NWS does not have a solution for scanning IM file attachments; therefore they are blocked (disallowed) at the server. Future proposals include a file scanning solution which will enable the use of multi-media attachments, such as image, audio, and video files to enhance IM communications.

Logging
All IM conversations in both multi-user chatrooms and person-to-person sessions are logged on the NWSChat server. All user access to the server such as NWSChat registration and logon/logoff activity is also logged. In addition, by using the Pidgin IM client software users have the option to log all of their IM activity and messages on their local workstation.

NWS Accountability
The NWSChat system will be included in the NWS OCIO IT Security Certification and Accreditation package for Internet Server Farms.

References:

NWSChat Webpage
Instant Messaging for NWS and Partners: NWSChat
XMPP Security, Sept 4, 2007, Gaston Dombiak
NWSChat Admin Team: Carlos Diaz (NWSChat Program Manager) Darone Jones, Daryl Herzmann, Shane Searcy, Matt Duplantis, Bob Bunge, Brad Small, Joe Palko