



Preventing toll fraud through Embedded Messaging on the 3300 ICP

V 1.0, March 2009

Mitel systems have been the target of some toll fraud attacks using Embedded Messaging on the Mitel 3300 ICP. This is a direct result of NOT setting the appropriate voice mail passcode restrictions. Mitel systems allow the administrator to set the following restrictions on voice mail related passcodes:

1. Passcode length – the default is 4 numeric characters, but can be 3-6 characters long.
2. Mailbox lockout capability, after three failed attempts. (Release 9.0 UR1 and later)

Furthermore, Mitel systems require the end user to change the default passcode on first login.

Toll fraud attacks can be prevented by following the security recommendations described below:

1. Use passcodes with a length of 6 characters to decrease vulnerability to brute force attacks.
2. Use passcodes that are not easy to guess (avoid passcodes like 123456, 987654 or 444444).
3. Ensure that administrator and user mailbox passcodes are changed frequently based on the organization's security policies.
4. Ensure that only appropriate personnel have mailbox create permissions to prevent toll fraud attacks originating from within the network.
5. Use strong passwords (at least 8 characters with numbers and special characters) for all GUI-based administration/management interfaces.
6. On creating a new mailbox, it is recommended that the administrator immediately change the default passcode, and provide this new passcode to the user. This will prevent toll fraud attacks occurring during the interval from creating a mailbox and the user changing the default passcode.
7. Use appropriate call routing restriction rules to control outbound calling.
8. If Recorded Announcement Devices (RAD's) are implemented, ensure that appropriate security measures are in place to prevent unauthorised dial through.

Contact your system maintainer for further information regarding the above points.

Mitel provides the administrator with the tools/configurations to prevent toll fraud attacks. However, the administrator should make use of these configurations and follow the organization's security policies to ensure that toll fraud attacks are prevented.

For any questions in this regard, please contact the Mitel Security Team at security@mitel.com and visit www.mitel.com/security for more information.