Getting Started with OAT v3.0

This step by step guide will demonstrate how OAT can be used as a security assessment of your enterprise OCS/Lync infrastructure.

OAT is an open source security tool designed to check the password strength of Microsoft Office Communication Server and Lync server users. After cracking the password, OAT demonstrates various other UC/VoIP attacks like Presence Stealing, IM Spamming, and Call Walking.

VIPER Lab created OAT because OCS and other Microsoft products are frequently being used as part of a unified communications infrastructure in many enterprises. Our mission is to help IT managers and security practitioners evaluate the security architecture of their deployments and ensure that their mission-critical communications and systems are protected.

The following features are currently supported by OAT:

1. Online Dictionary Attack
2. Presence Stealing of SIP Enabled users from target domain
3. Single user flood mode
4. Multi-user flood mode
5. Call Walking
6. Play SPAM audio
7. Report Generation

The following features are new in OAT version 3.0:

1. Slight UI upgrade
2. Speed enhancement for the Online Dictionary Attack
3. Play SPAM audio bug fixes
4. New Active Directory options

OAT attack Pre-requisites

The following pre-requisites are required by OAT to carry out different attacks.

1. *SIP URI of legitimate user to launch dictionary attack.(e.g. sip:bob@contoso.com)*
2. *FQDN of target OCS server. (e.g. ocs.contoso.com)*
3. *Domain name of the target network.(e.g. contoso.com)*
4. *SIP URI of victim for Single User Mode IM Flood.(e.g. sip:alice@contoso.com)*
5. *A dictionary file containing list of passwords.*

In OAT v3.0, new Active Directory options have been added which allow the user to specify the domain name of the Active Directory server and an Active Directory username of the target SIP user. These features will be explained in more detail below.

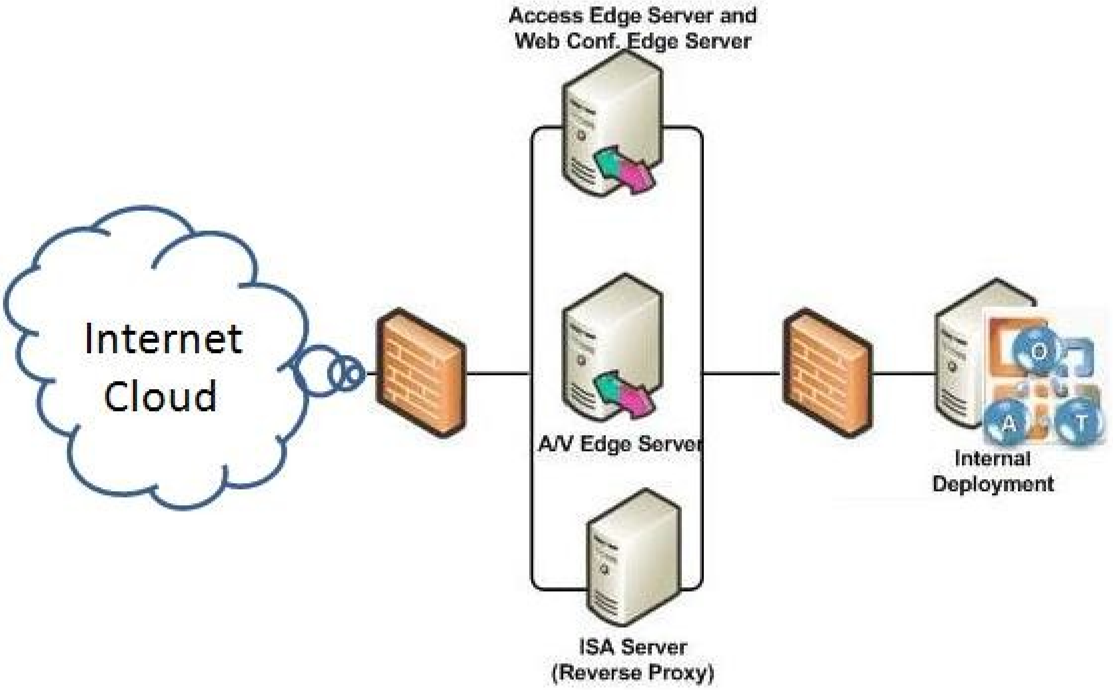
With the OAT security assessment tool, you can perform:

- Internal Assessment
- External Assessment
- Report Generation

A security professional can launch OAT and try the password strength test against the known SIP URI. Once the dictionary attack is successful, OAT can be used to simulate malicious Proof of Concept attacks like IM Flood and Call walking against OCS/Lync users.

Internal Network Deployment

Consider the following network topology in the case of internal assessments where OAT will launch attacks from an internal IP network against the OCS R1/R2/Lync Server.

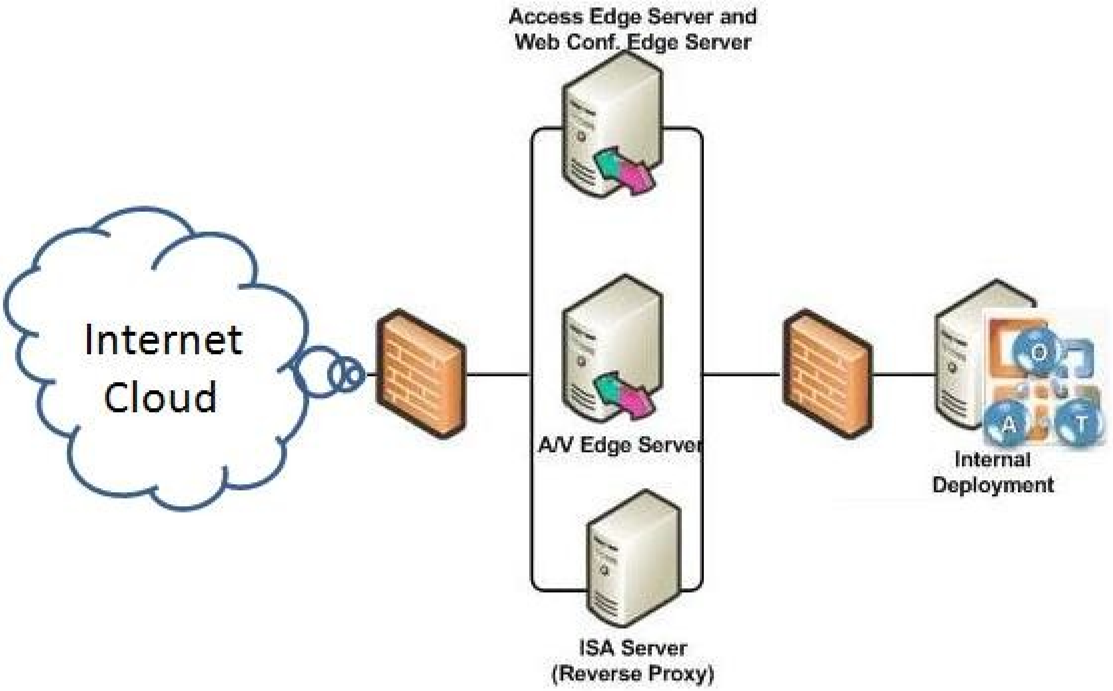


Internal network is a deployment scenario in which OCS users have unfiltered network connectivity to the OCS/Lync server and the domain controller.

From an internal deployment, OAT allows users to launch attacks like the Online Dictionary Attack, Domain User Enumeration, Presence Stealing, Contact List Stealing, Domain IM Flood, Domain Call Walk, and Call DoS.

External Network Deployment

Consider the following network topology in the case of external security assessments where OAT will launch attacks from the public Internet against the OCS R1/R2 Server.



External Network is a deployment scenario where OCS users have to connect through the Edge server. This connection is usually over TLS and users do not have access to the domain controller unless they are connected via VPN.

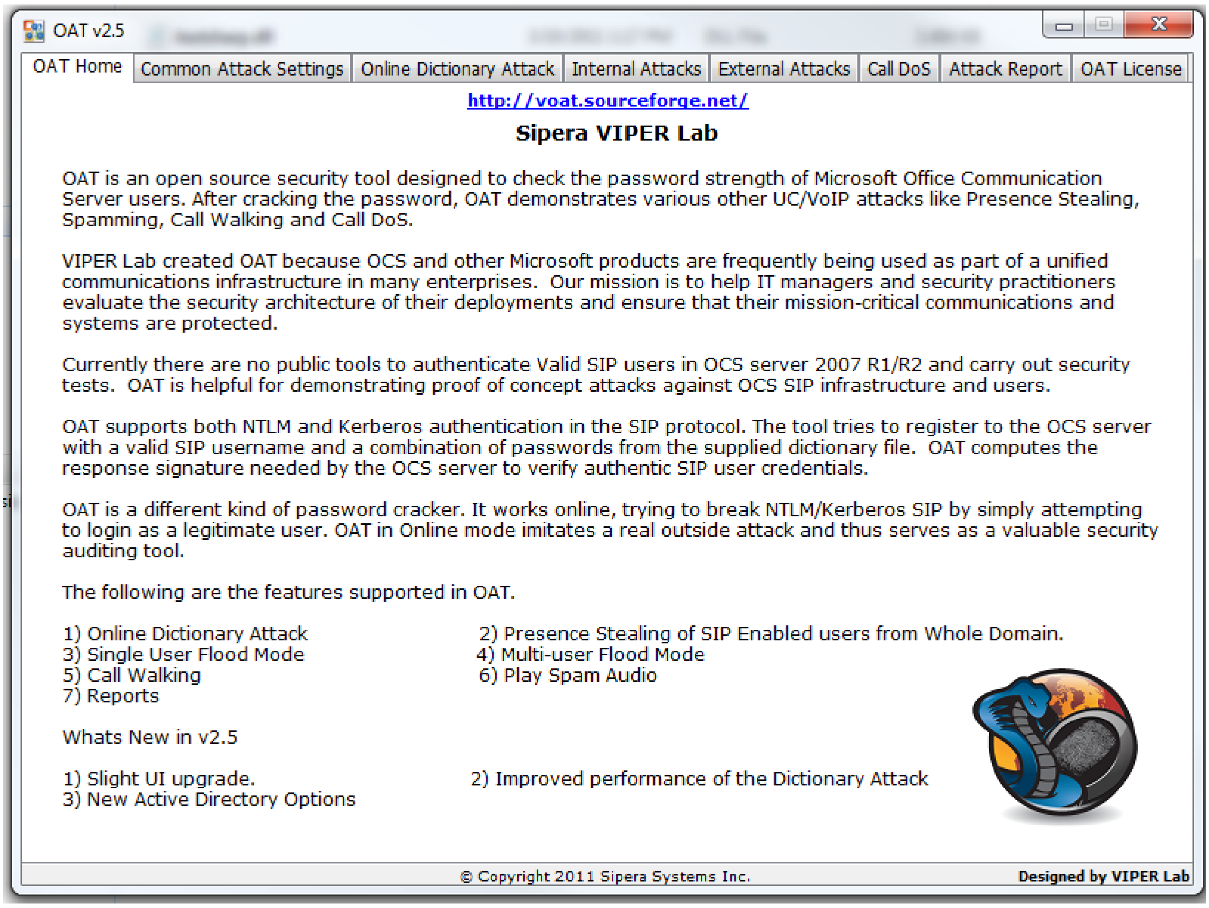
In this typical network scenario, OAT allows us to launch attacks like the Online Dictionary Attack, Contact List Stealing, Presence Stealing, IM Flood, Call Walk, and Call DoS.

The main difference between Internal and External Deployments usage is that OAT can attack all available UC users when used from an internal network, whereas it is limited to attacking users from the victim's contact list when used from an external network. Refer to the **"External Attacks"** section for more examples.

Getting Started

Let's get started with some actual examples. First, launch OAT v3.0. OAT will create the folder "**OAT_ReportDir"** under the **"My Documents"** folder of the currently logged in user to save generated reports.

After successfully launching OAT, you will be presented with the following screen:



http://voat.sourceforge.net/

Sipera VIPER Lab

OAT is an open source security tool designed to check the password strength of Microsoft Office Communication Server users. After cracking the password, OAT demonstrates various other UC/VoIP attacks like Presence Stealing, Spamming, Call Walking and Call DoS.

VIPER Lab created OAT because OCS and other Microsoft products are frequently being used as part of a unified communications infrastructure in many enterprises. Our mission is to help IT managers and security practitioners evaluate the security architecture of their deployments and ensure that their mission-critical communications and systems are protected.

Currently there are no public tools to authenticate Valid SIP users in OCS server 2007 R1/R2 and carry out security tests. OAT is helpful for demonstrating proof of concept attacks against OCS SIP infrastructure and users.

OAT supports both NTLM and Kerberos authentication in the SIP protocol. The tool tries to register to the OCS server with a valid SIP username and a combination of passwords from the supplied dictionary file. OAT computes the response signature needed by the OCS server to verify authentic SIP user credentials.

OAT is a different kind of password cracker. It works online, trying to break NTLM/Kerberos SIP by simply attempting to login as a legitimate user. OAT in Online mode imitates a real outside attack and thus serves as a valuable security auditing tool.

The following are the features supported in OAT.

1) Online Dictionary Attack
2) Presence Stealing of SIP Enabled users from Whole Domain.
3) Single User Flood Mode
4) Multi-user Flood Mode
5) Call Walking
6) Play Spam Audio
7) Reports

Whats New in v2.5

1) Slight UI upgrade.
2) Improved performance of the Dictionary Attack
3) New Active Directory Options

© Copyright 2011 Sipera Systems Inc.

Designed by VIPER Lab

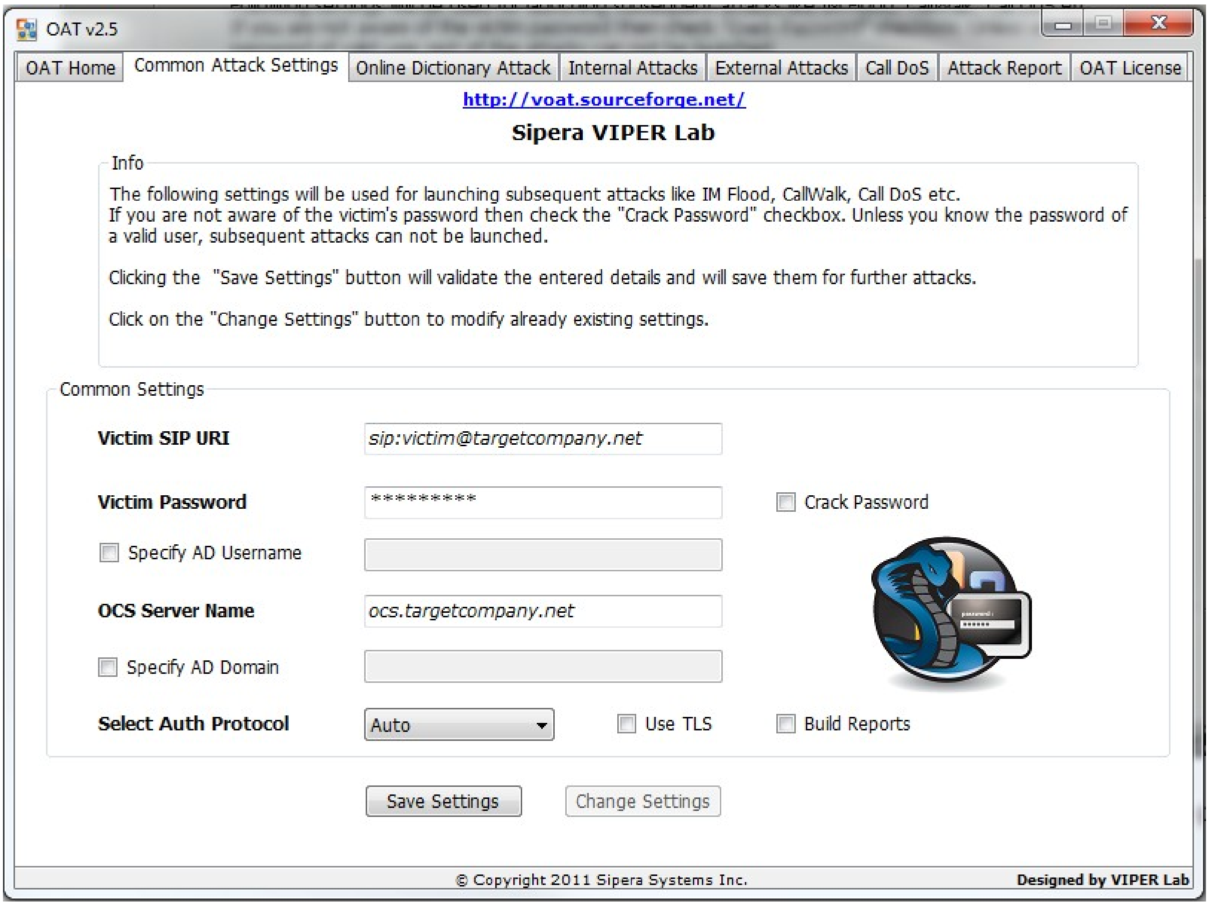
As you can see, OAT has several tab pages, each one responsible for various features supported by OAT. Each tab page also has a brief description about what it is used for.

Common Attack Settings

Before attacks can be carried out, you must enter the following settings under the “Common Attack Settings” tab:

1. **Victim SIP URI –** This is the SIP URI of the victim you want to pose as for subsequent attacks.
2. **Victim Password –** This is the victim’s password for signing into the OCS/Lync server.
3. **Specify AD Username –** Check this checkbox if the user’s Active Directory username is different than their SIP URI username. For example, if your target user is sip:sara.jones@ocstest.com but their Active Directory username is **NOT** sara.jones, check this box and specify their AD username.
4. **OCS Server Name –** This is the name of the OCS/Lync server.
5. **Specify AD Domain –** This is the domain name of the Active Directory. Specify this if the AD server is different than the OCS/Lync server.
6. **Select Auth Protocol –** This is the authentication protocol used to authenticate the aforementioned credentials. In general, you’ll want to use Auto (NTLM | Kerberos).
7. **Use TLS –** Check this box if the target server only communicates over a secure channel. Otherwise, leave it unchecked.
8. **Build Reports –** Check this box if you want OAT to generate assessment reports.

When you have entered the desired settings, click on the **"Save Settings"** button to lock the settings in place. When you do this, OAT does basic input testing and connectivity checks to make sure that the specified information is valid.



http://voat.sourceforge.net/

Sipera VIPER Lab

Info

The following settings will be used for launching subsequent attacks like IM Flood, CallWalk, Call DoS etc.
If you are not aware of the victim's password then check the "Crack Password" checkbox. Unless you know the password of a valid user, subsequent attacks can not be launched.

Clicking the "Save Settings" button will validate the entered details and will save them for further attacks.

Click on the "Change Settings" button to modify already existing settings.

Common Settings

Victim SIP URI	sip:victim@targetcompany.net	
Victim Password	*********	□ Crack Password
□ Specify AD Username		
OCS Server Name	ocs.targetcompany.net	
□ Specify AD Domain		
Select Auth Protocol	Auto	□ Use TLS □ Build Reports

© Copyright 2011 Sipera Systems Inc.

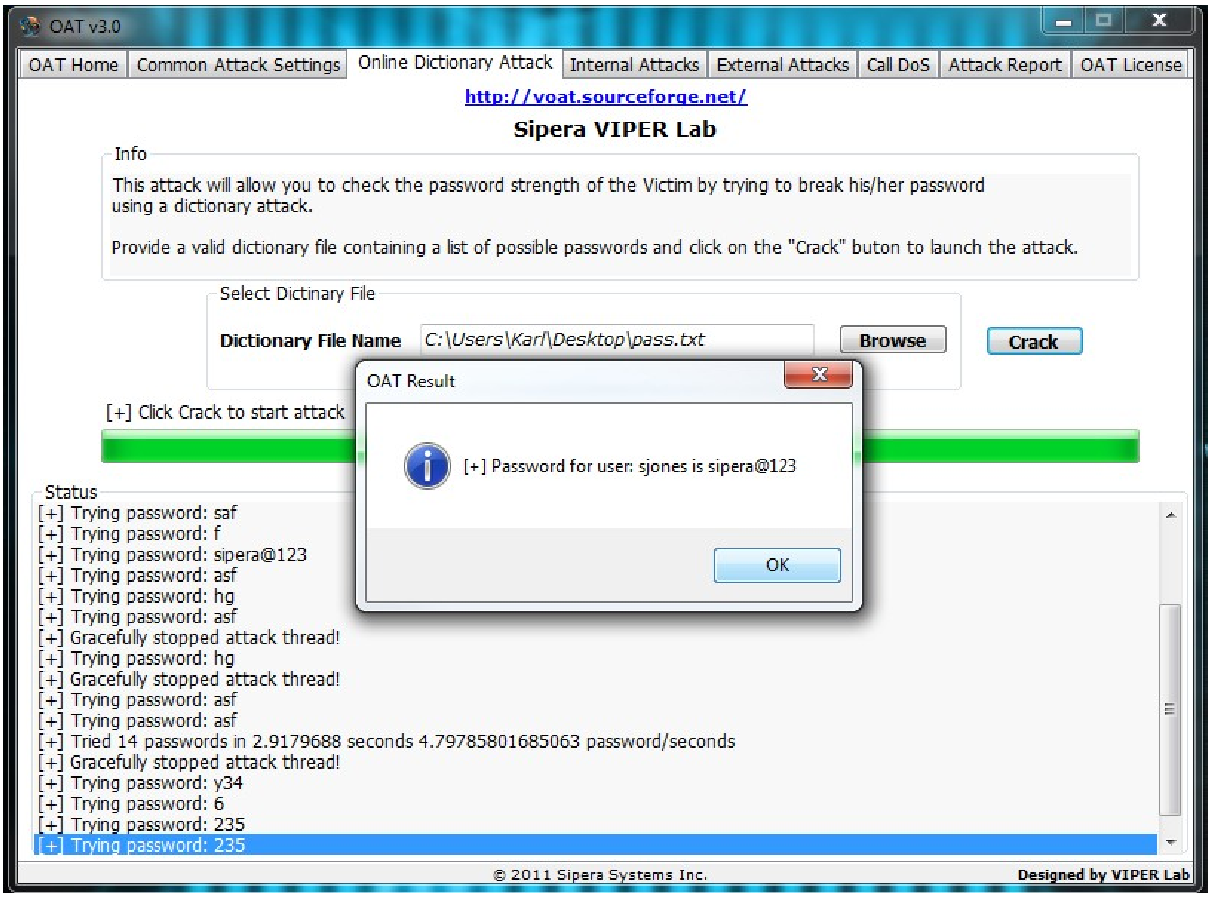
Designed by VIPER Lab

OAT Common Attack Settings Tab

Online Dictionary Attack

The attacker/security auditor can launch OAT and try the password strength test attack against the known SIP URI. Once the attack is successful, OAT can be used to launch malicious attacks like IM Flood and Call Walking against OCS/Lync users.

Let's provide a valid dictionary file as input for the Online Dictionary Attack and press "**Crack**" to start the attack. The dictionary file should have passwords separated by the newline character (One password per line).



http://voat.sourceforge.net/

Sipera VIPER Lab

This attack will allow you to check the password strength of the Victim by trying to break his/her password using a dictionary attack.

Provide a valid dictionary file containing a list of possible passwords and click on the "Crack" buton to launch the attack.

Dictionary File Name: C:\Users\Karl\Desktop\pass.txt

[+] Click Crack to start attack

[+] Password for user: sjones is sipera@123

```
[+] Trying password: saf
[+] Trying password: f
[+] Trying password: sipera@123
[+] Trying password: asf
[+] Trying password: hg
[+] Trying password: asf
[+] Gracefully stopped attack thread!
[+] Trying password: hg
[+] Gracefully stopped attack thread!
[+] Trying password: asf
[+] Trying password: asf
[+] Tried 14 passwords in 2.9179688 seconds 4.79785801685063 password/seconds
[+] Gracefully stopped attack thread!
[+] Trying password: y34
[+] Trying password: 6
[+] Trying password: 235
[+] Trying password: 235
```

OAT will iterate over the whole dictionary file trying every password against the victim SIP URI and will popup the password if it is able to successfully elicit the password.

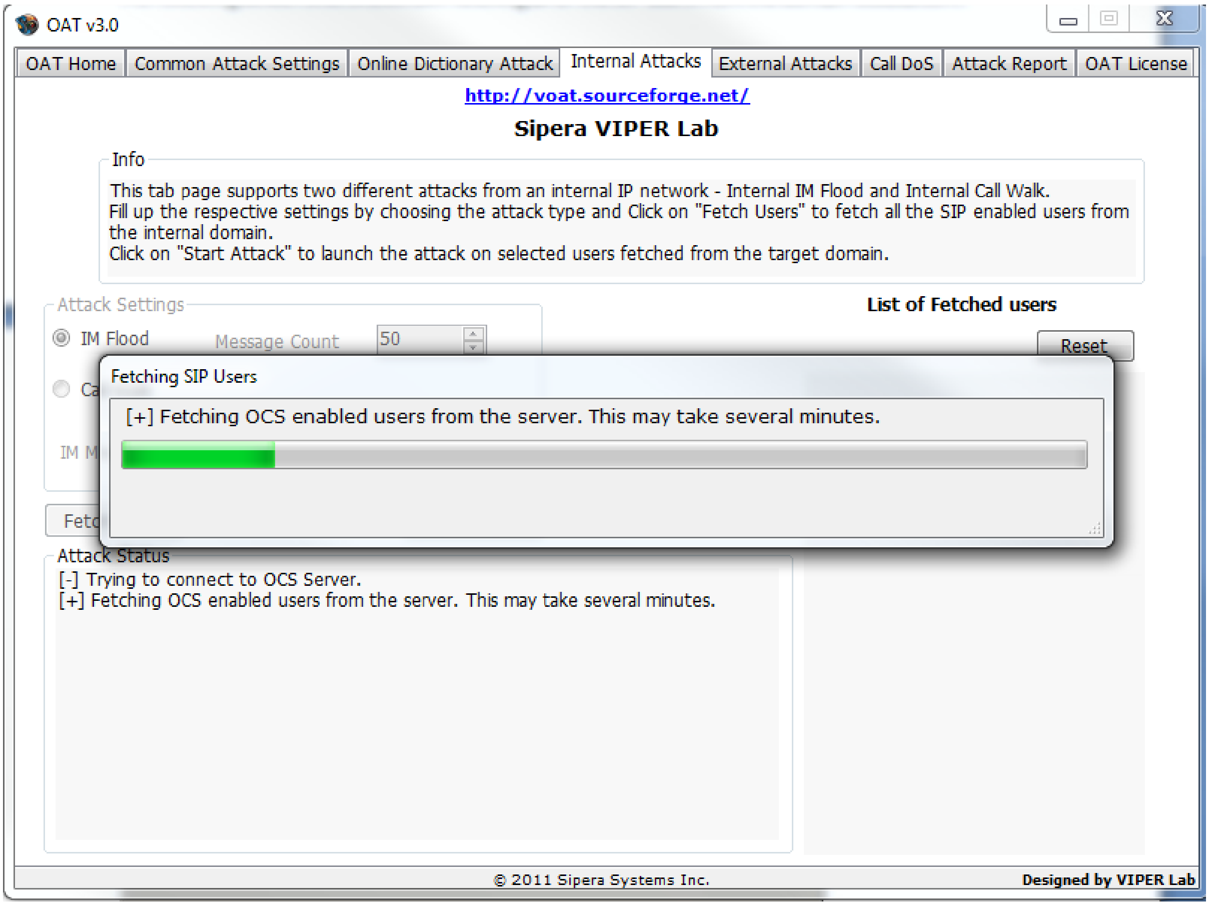
OAT asks for the confirmation to use the cracked credentials of the compromised SIP URI for launching further UC attacks. If the user says “No”, the user will need to change the common attack settings to reflect valid credentials.

For the following attacks, OAT needs a valid username and password. It **may** also need a specified Active Directory username and domain. For more information, see page 4 for a description of what those settings do.

Internal Network Attacks

Let’s move on to the “**Internal Attacks”** tab page. As the name suggests, all domain users can be targeted using this attack tab. First, let’s build the target users list by fetching all of the OCS/Lync enabled SIP users from the target domain.

The following screen shot shows OAT fetching all of the SIP users from the domain ocsusa.com:



This tab page supports two different attacks from an internal IP network - Internal IM Flood and Internal Call Walk.
Fill up the respective settings by choosing the attack type and Click on "Fetch Users" to fetch all the SIP enabled users from the internal domain.
Click on "Start Attack" to launch the attack on selected users fetched from the target domain.

[+] Fetching OCS enabled users from the server. This may take several minutes.

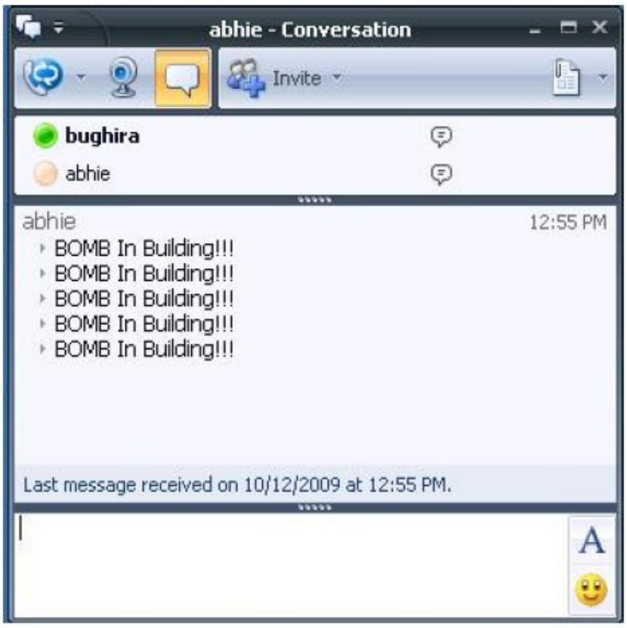
```
[-] Trying to connect to OCS Server.
[+] Fetching OCS enabled users from the server. This may take several minutes.
```

IM Flood

As soon as OAT builds the target list, the **IM Flood** and **Call Walk** attack settings are unlocked.

- Let's choose **"IM Flood"** as our attack and check the **"Select all users"** check box to attack the entire list of users.
- OAT allows users to send a flood of custom IM message specified in the **"IM Message"** text box.
- The message count parameter is to do a strength test on hard phones with IM capabilities.

Once the attack is successful, the target user will be flooded with the specified custom IM message. The following screen shot shows the user *bughira* flooded with the message "**BOMB In Building!!"** 5 times.



abhie - Conversation

bughira
abhie

abhie 12:55 PM
- BOMB In Building!!!
- BOMB In Building!!!
- BOMB In Building!!!
- BOMB In Building!!!
- BOMB In Building!!!

Last message received on 10/12/2009 at 12:55 PM.

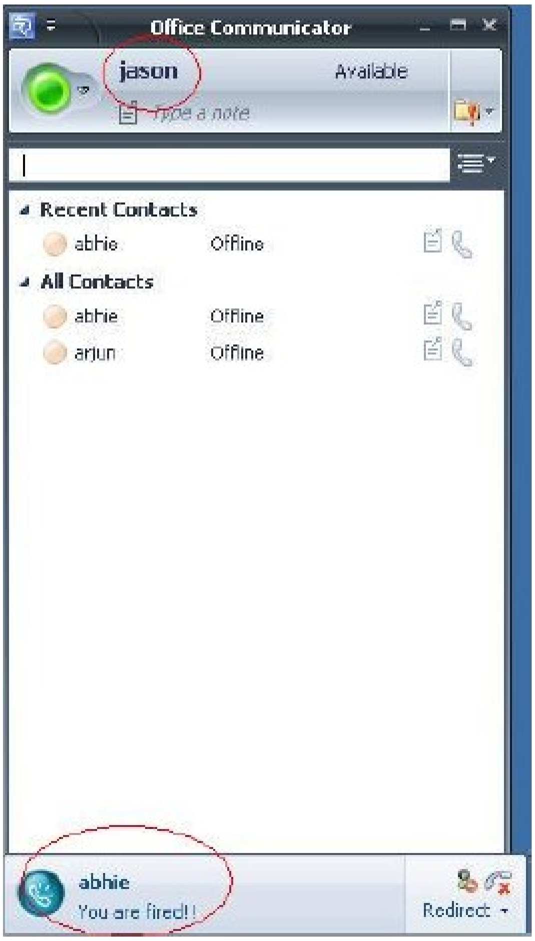
Call Walk

Call walking is a type of reconnaissance probe in which a malicious user initiates sequential calls to a block of telephone numbers to identify what assets are available for further exploitation. This is a modern version of *wardialing*, common in the 1980s to find modems on the Public Switched Telephone Network (PSTN). OAT makes a call to all selected users on after the other, leaving the media flow open unless specified with media to play once the target has picked up the call.

OAT can read all WMA files and insert its contents as media once the call is answered. This attack can be used as SPAM to annoy users.

As we have already fetched the target users, simply select the **"Call Walk"** radio option, enter the call subject and check the **"Play Audio File"** check box for audio SPAM.

Now click on the **"Start Attack"** button to launch the Call Walk attack against the selected users.



Office Communicator

jason Available

Recent Contacts
abhie Offline

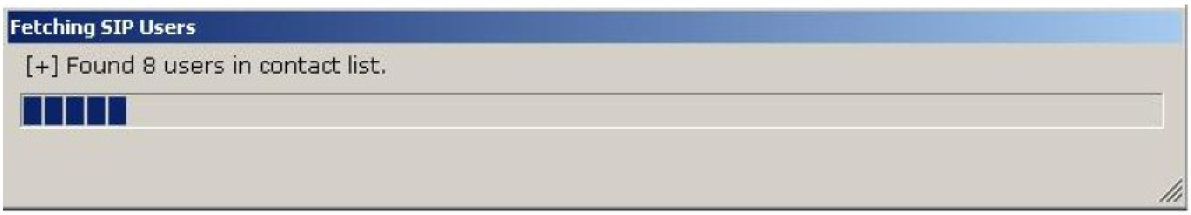
All Contacts
abhie Offline
arjun Offline

abhie
You are fired!!

External Network Attacks

This tab page is responsible for conducting attacks from outside the network. Users connecting from an external network have limited connectivity with the domain controller, so the target users are limited to the contact list of the victim.

Let's click on the **"Get Contacts"** button to fetch the contact list of the victim user. The following screen shot shows OAT fetching the contact list of a victim.



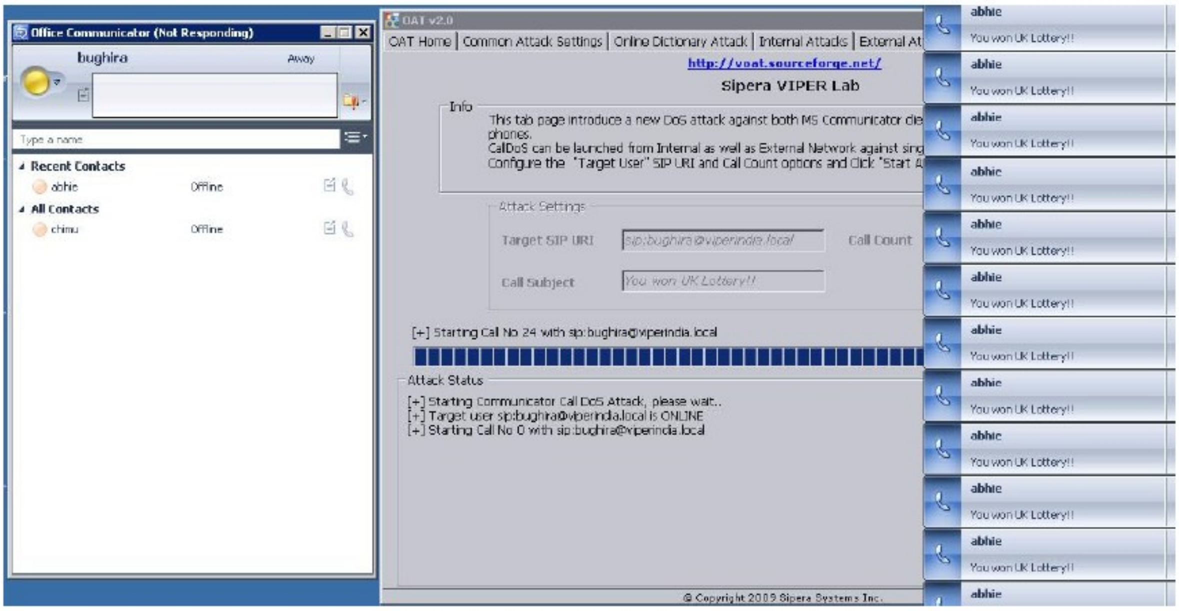
Fetching SIP Users

[+] Found 8 users in contact list.

Once the contact list is fetched and displayed, OAT again unlocks the previously cited **IM Flood** and **Call Walk** attack settings. These attacks are similar to the ones shown before under the "**Internal Network Attack"** page.

Call DoS / Communicator Call DoS

Call DoS produces dire results from both an internal and external deployment. OAT floods the target user with multiple calls which he cannot entertain, thereby knocking the user out of the communication server.
Simply select a victim for the attack and watch the results.



This tab page introduce a new DoS attack against both MS Communicator cli
phones.
CallDoS can be launched from Internal as well as External Network against sing
Configure the "Target User" SIP URI and Call Count options and Click "Start A

Target SIP URI: sip:bughira@viperindia.local

Call Count

Call Subject: You won UK Lottery!!

```
[+] Starting Call No 24 with sip:bughira@viperindia.local
```

```
[+] Starting Communicator Call DoS Attack, please wait..
[+] Target user sip:bughira@viperindia.local is ONLINE
[+] Starting Call No 0 with sip:bughira@viperindia.local
```

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie
You won UK Lottery!!

abhie

OCS and Lync do not terminate idle calls and does not keep track of ongoing call sessions for particular users, causing this attack to be extremely effective.

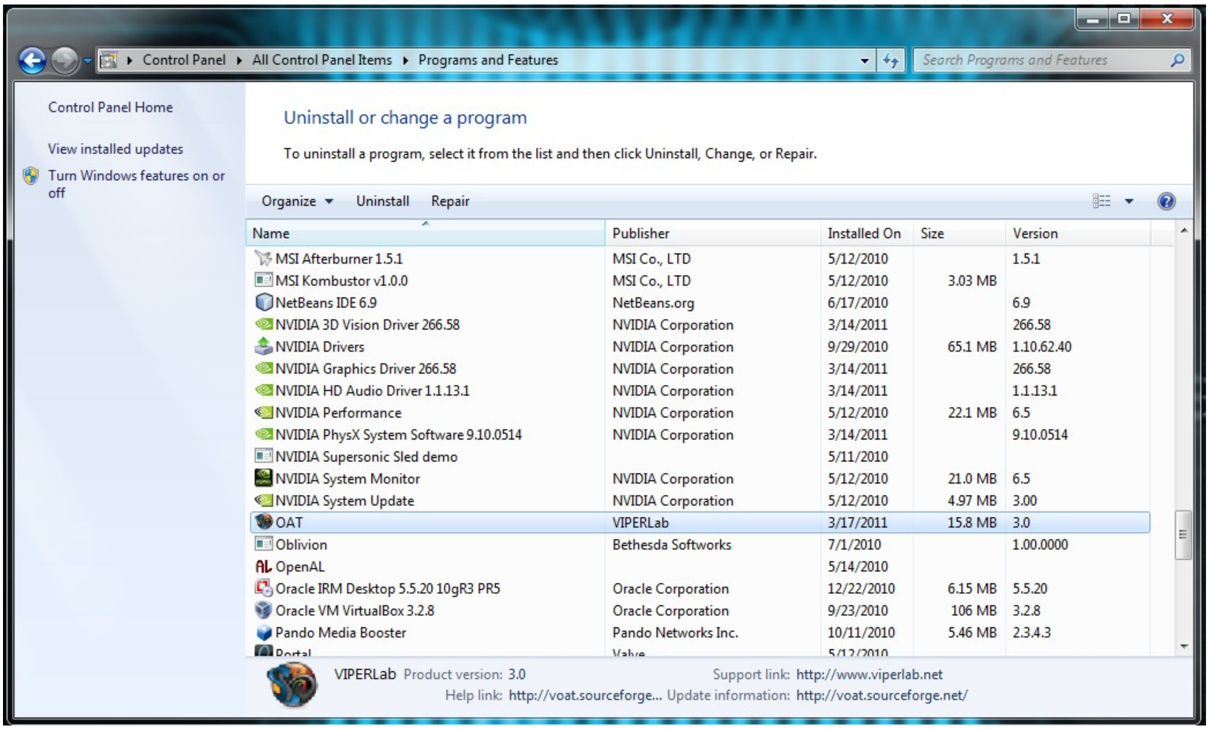
Attack Reports

Report generation is an important feature of OAT as it helps keep track of launched attacks and their status.
OAT generates comprehensive reports of the launched attack sessions with detailed information like settings used for the attack, attack details, and the results of the attack. These reports are handy for a security auditor and can be included in a penetration testing report.
If OAT is not able to create the report directory, all of the generated reports will be stored on the desktop of logged in user.

OAT reports can be saved in different formats including **PDF, MS-Word DOC, RTF, and Text**. Reports are saved under the **"My Documents"** folder of the currently logged in user, or the desktop if the folder could not be created.

Un-installing/Repairing OAT

OAT creates an entry for its uninstall program under Add or Remove Programs from Control Panel.


Control Panel ▸ All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall
Repair

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
MSI Afterburner 1.5.1	MSI Co., LTD	5/12/2010		1.5.1
MSI Kombustor v1.0.0	MSI Co., LTD	5/12/2010	3.03 MB	
NetBeans IDE 6.9	NetBeans.org	6/17/2010		6.9
NVIDIA 3D Vision Driver 266.58	NVIDIA Corporation	3/14/2011		266.58
NVIDIA Drivers	NVIDIA Corporation	9/29/2010	65.1 MB	1.10.62.40
NVIDIA Graphics Driver 266.58	NVIDIA Corporation	3/14/2011		266.58
NVIDIA HD Audio Driver 1.1.13.1	NVIDIA Corporation	3/14/2011		1.1.13.1
NVIDIA Performance	NVIDIA Corporation	5/12/2010	22.1 MB	6.5
NVIDIA PhysX System Software 9.10.0514	NVIDIA Corporation	3/14/2011		9.10.0514
NVIDIA Supersonic Sled demo		5/11/2010		
NVIDIA System Monitor	NVIDIA Corporation	5/12/2010	21.0 MB	6.5
NVIDIA System Update	NVIDIA Corporation	5/12/2010	4.97 MB	3.00
OAT	VIPERLab	3/17/2011	15.8 MB	3.0
Oblivion	Bethesda Softworks	7/1/2010		1.00.0000
OpenAL		5/14/2010		
Oracle IRM Desktop 5.5.20 10gR3 PR5	Oracle Corporation	12/22/2010	6.15 MB	5.5.20
Oracle VM VirtualBox 3.2.8	Oracle Corporation	9/23/2010	106 MB	3.2.8
Pando Media Booster	Pando Networks Inc.	10/11/2010	5.46 MB	2.3.4.3
Portal	Valve	5/12/2010		

VIPERLab Product version: 3.0 Support link: http://www.viperlab.net
Help link: http://voat.sourceforge... Update information: http://voat.sourceforge.net/

You can go to "Add or Remove Programs" from the control panel to uninstall or repair OAT.

Contact VIPER Lab

Visit VIPER Lab for more information on OAT and its features. We would like to hear from you.

Our contact Information:

OAT Official Website: http://voat.sf.net

Email: viper@viperlab.net

Website: http://viperlab.net