Certificate Authority Module

lab 1 issue and revoke of certificate authority

Introduction	2
Quick introduction to LAMP	2
Quick introduction to certificate authority	2
Implementation	2
Network topology on GENI	2
Setup LAMP on GENI	
Install MySQL:	4
Install Apache	5
Install PHP	6
Install the extension packets of PHP and MySQL	7
Enable SSL connection of Apache	7
Install and enable browser on GENI	
For Windows operation system:	
For MacOS operation system	
For other Linux operation system	
Test Apache service and PHP service	
Test Apache service	
Test PHP service	
Set up certificate authority on GENI	
Build Certificate Authority	
On web server node	
Issue a digital certificate	
Result of issued digital certificate	
Revoke a digital certificate	
Result of revoke a digital certificate	

Introduction

Quick introduction to LAMP

LAMP is short for the software bundle of Linux operating system, Apache HTTP Server, MySQL database management system and PHP programming language.

This bundle can realize the role and function of a web server, which can drive Web applications. Although not actually designed to work together, these open source software is comparatively simple and easy to use. Besides this four software, this software bundle can also be combined with many other free and open-source software packages

Quick introduction to certificate authority

Certificate Authority is a trusted third party that issues electronic documents that verify a digital entity' s identification on the Internet. In cryptography mean, certificate authority verifies the ownership of the public key of the named subject of the certificate.

Implementation

Network topology on GENI

The network topology of our experiment will be the following one:



The node named CA will be the certificate authority in this experiment. The node named WS will be the web server in this experiment and we will install LAMP on this node to enable it to be a web server.

Notice: we must wait for all the GENI node turn green, which means the remote machines are ready for us to use, then we can continue the following steps. This may take a while.

Setup LAMP on GENI

We already have the GENI node. In other words, we already have a Linux operation system, so we only need to install the remaining Apache, MySQL, and PHP. We should pay attention to the installation order of LAMP, I recommend we install the MySQL and Apache firstly, leave the PHP in the end. The order of installation of MySQL and Apache can be reversed because they are not depending on each other. However, the PHP must be installed after we finish the installation of MySQL and Apache because PHP server depends on the services of Apache and MySQL.

Using SSH log onto the WS node. The following installation will be on this node.

Before installation, we should download the package lists from the repositories and "updates" them to get information on the newest versions of packages and their dependencies.

Command: "sudo apt-get update"

Install MySQL:

Command: "sudo apt-get install mysql-server"

kqing051@ws:~\$ sudo apt-get install mysql-server Reading package lists... Done Building dependency tree Reading state information... Done The following extra packages will be installed:

In this process, it will ask you to enter the password for the MySQL administrator, set up the password in this prompt window.



After installation of MySQL, we should check whether this is installed successfully.

Command:" sudo netstat -tap | grep mysql"

If it shows the listening port of MySQL as following, then we prove it is

installed successfully.

root@ws:,	/users/kg	qing051# sudo netstat	-tap	grep mysql
tcp	0	0 localhost:mysql		*:*
	LISTEN	9842/ mysql d		
root@ws:,	/users/kg	qing051#		

Install Apache

Command: "sudo apt-get install apache2"

```
root@ws:/users/kqing051# sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
    apache2-bin apache2-data libaprutil1-dbd-sqlite3 libaprut
il1-ldap
```

We can run the browser to check whether it is installed successfully or

not. But don' t hurry; we need to involve third party software to enable

the graphics showing on GENI node. We will cover this content in the

following.

Install PHP

Command:" sudo apt-get install php5 libapache2-mod-php5"



After this installation, it will create a folder named "www" under var.

This folder will be reserve the source code of the website.

root@ws:/var# ls						
backups	emulab	local	log	opt	spool	www
cache	lib	lock	mail	run	tmp	

Install the extension packets of PHP and MySQL

Command:" sudo apt-get install php5-mysql php5-curl php5-gd php5-intl php-pear php5-imagick php5-imap php5-mcrypt php5-memcache php5-ming php5-ps php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl;"

Notice: the GENI node is initiated with an Ubuntu operation system following its default setting. If you choose other operation systems rather the default operation system, there might be a warning message showing on the screen and it may be failed to initiate the GENI nodes. Therefore there is no need to set up another operation system, but if you do so, either it will not affect much in this experiment.

Enable SSL connection of Apache

Because we need to install the digital certificate later, so we need to enable SSL connection of Apache.

First, just a brief introduction of Apache configuration file.



As we can see, there are several configurations in Apache folder.

In the old versions of Apache, there is only one configuration named "httpd.conf" .

And as for the latest version, the main configuration file is "apache2.conf". We can take a guick look of this file.

```
# LogLevel: Control the severity of messages logged
error_log.
# Available values: trace8, ..., trace1, debug, inf
e, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level fo
ular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn
# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf
# Include list of ports to listen on
Include ports.conf
```

As we can see, there are many "includes" command in this file. It means the apache server will firstly read this file and the other configuration files will be linked using these "include" command.

As for the SSL configuration file, it's in the "sites-enabled" folder. We can use this command to create a configuration file for SSL connection. "sudo

/etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-enable

d/default-ssl.conf "

Then we modify this default-ssl.conf like follows:



We temporary named our server name as jhuws.edu, and the digital certificate name is jhuws.crt, the private key of digital certificate name is jhuws.key. Of course you can make the name as you like, but make sure to use the same name in the later.

And the 172.17.2.41 is the IP address of our web server, you can use

command "ifconfig" to check it out. The "443" is the port number for SSL connection.

You should also use this command" sudo a2enmod ssl" to enable the SSL module of Apache2 if there prompt the problem that you try to connect 443 port to our web server while it refuse.

Then restart the apache2 service using this command" service apache2 restart".

Install and enable browser on GENI

We choose Firefox browser in this experiment. Of course, you can choose other browsers if you like. This part should be done on user node.

Command:" sudo apt-get install firefox"



The operation of next step will be different for windows, Mac and Linux operation systems. For windows and MacOS operation systems, we need to depend on third party software to enable the graphics display on GENI node.

For Windows operation system:

Install the Xming software on your local operation system. Xming is an X11 display server for Microsoft Windows operating systems. Then run it to start the X server. You should see the Xming icon in the taskbar if it is running.

📜 locale	2017/2/12 18:14
📕 xkb	2017/2/12 18:14
COPYING	2007/4/15 20:22
example_Xmingrc	2006/10/29 15:01
🗋 font-dirs	2007/1/31 8:38
🗟 libfreetype-6.dll	2007/5/4 9:31
X plink.exe	2007/5/2 8:16
🗟 pthreadGC2.dll	2007/3/27 13:42
📄 rgb.txt	2004/11/11 0:14
X run.exe	2007/3/27 14:15
SecurityPolicy	2006/2/13 9:02
🗋 unins000.dat	2017/2/12 18:14
🔆 unins000.exe	2017/2/12 18:13
🗋 X0.hosts	2006/3/8 19:40
C XErrorDB	2005/11/24 10:52
X xkbcomp.exe	2007/5/3 18:43
🗋 XKeysymDB	2004/11/11 15:16
📽 XLaunch.chm	2007/4/13 12:17
XLaunch.exe	2007/5/3 18:43
C XLaunch.xsd	2007/1/22 15:56
🗙 Xming.exe	2007/5/3 18:43
😰 Xming	2017/2/12 18:14

Then use PuTTY to log onto the GENI node.

You can see the instruction here about how to log onto GENI node using

PuTTY.

http://groups.geni.net/geni/wiki/HowTo/LoginToNodes

Remember to click the option on X11 option besides the other steps of

logging onto GENI node using PuTTY.

🕵 PuTTY Configu	ration						?	\times
Category:								
Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex Cipher Auth TTY X11 Tunnels Bugs More bugs		Op X11 ferwarding Image: Enable X1 X display lood Remote X11 a Image: MIT-Magic X authority file	tions contro 1 forwardin ation authemiceti c-Cookie-1	on pro isplay	SH X11 forw	horizati	ion-1 Browse	
About	Help			(Open		Cance	I

Then we can run the graphics display on GENI node on Windows operation system.

Command:" firefox"



Wait for a second, and then we can see the browser GUI display is shown

with the help of Xming



For MacOS operation system

Install XQuartz on your Mac. XQuartz is an X server designed for MacOS.

0 0	🛃 Applications			
		Q		\supset
FAVORITES	Name	Date Modified	Size	K
昌 All My Files	Bluetooth File Exchange	Jun 21, 2014 6:28 PM	2.4 MB	A
Applications	Boot Camp Assistant	Jun 21, 2014 6:28 PM	14.3 MB	A
Deskton	💥 ColorSync Utility	Jun 21, 2012 6:25 AM	15.5 MB	A
	Console	Mar 18, 2013 12:46 PM	9.7 MB	A
Documents	Ø DigitalColor Meter	Jun 21, 2012 5:52 AM	1.9 MB	Α
🕒 Downloads	🔊 Disk Utility	Sep 3, 2013 9:28 PM	20.6 MB	Α
Movies	🕅 Grab	Mar 16, 2012 1:15 AM	3.3 MB	Α
Music	阑 Grapher	Mar 6, 2012 8:35 AM	32.9 MB	Α
	🗐 Java Preferences	Jun 23, 2012 7:06 AM	721 KB	Α
Pictures	🖗 Keychain Access	Mar 18, 2013 12:46 PM	14.2 MB	Α
	🍇 Migration Assistant	Jun 21, 2014 6:28 PM	7.6 MB	Α
	🥘 Network Utility	Jun 21, 2012 6:02 AM	3.9 MB	A
	💥 RAID Utility	Jun 25, 2012 2:11 PM	9.9 MB	Α
	🍙 System Information	Sep 3, 2013 9:28 PM	6.5 MB	Α
	🛅 Terminal	Mar 18, 2013 12:46 PM	15.4 MB	Α
	VoiceOver Utility	Mar 18, 2013 12:46 PM	24.7 MB	Α
	XQuartz 💙	Yesterday 9:37 AM	7.9 MB	A
	🇊 Xcode	Jun 13, 2014 8:51 AM	4.94 GB	A

Right click on the XQuartz icon in the dock and select Applications >

Terminal. This should bring up a new xterm terminal windows.



Then make an ssh connection to the GENI node on this terminal windows.

			and the second	the all and	
🗑 🖯 🕀			X xterm		
bash-3,2\$ Desktop Documents bash-3,2\$ bash-3,2\$	ls Downlo Librar cd Desktop/ ls	oads °Y	Movies Music	Pictures Prezi	Public
Collabora Prezi.app Terminal id_geni_ss prezi for bash-3.2\$	stive Detect: h_rsa mac ssh -i id_ge	ion of Cove eni_ssh_rsa	rt Storage Ch 1 -X -Y kqing	annels.zip 0510pc2.geni.it	∴cornell.edu -p 3103
/ The auther 7)' can't RSA key fi Are you su Warning: F 37' (RSA)	ticity of h be establish ngerprint is re you want 'ermanently a to the list	ost '[pc2.g med. s 00:a0:ac: to continu added '[pc2 of known h	eni.it.cornel 5a:00:99:d6:2 e connecting !.geni.it.corn posts.	l.edu]:31037 ([b:bc:49:24:be:4 (yes/no)? yes ell.edu]:31037,	192,122,236,81]:3103 H6;d1:92:fe. .[192,122,236,81]:310
		Enter yo "id_geni	ur password _ssh_rsa".	d for the SSH	key
		Passwore	d:		
			Show p	assword	
			🗌 Remen	nber password	in my keychain
				Cance	! ОК

We can enable the graphics display of browser on GENI node with the

help of XQuartz software.

Command:" firefox"

000	X Mozilla Firefox						
() about:startpage × +							
③ Search or enter address	। ×	Search	☆自	+	A	◙	≡
<pre>(Firefox:19889): 6Donf-WARNING **: Client failed to com //bin/dbus-launch terminated abnorwally without any error //bin/dbus-launch terminated abnorwally without any error (Firefox:19889): 6Donf-WARNING **: Client failed to com //bin/dbus-launch terminated abnorwally without any error [Parent 19889] WARNING: pipe error (44): Connection ress inefox-sdnpce/firefox-51.0,1+build2/ipc/chromium/src/chr osix.cc, line 323 [Parent 19889] WARNING: pipe error (45): Connection ress inefox-sdnpce/firefox-51.0,1+build2/ipc/chromium/src/chr osix.cc, line 323 [Parent 19889] WARNING: pipe error (46): Connection ress inefox-sdnpce/firefox-51.0,1+build2/ipc/chromium/src/chr osix.cc, line 323 [Parent 19889] WARNING: pipe error (48): Connection ress inefox-sdnpce/firefox-51.0,1+build2/ipc/chromium/src/chr osix.cc, line 323 [Parent 19889] WARNING: pipe error (48): Connection ress inefox-sdnpce/firefox-51.0,1+build2/ipc/chromium/src/chr osix.cc, line 323 ###!!! [Parent][OnNagbeDequeue0ne] Error: Channel error: ###!!! [Parent][OnNagbeDequeue0ne] Error: Channel error: ####!!! [Parent][OnNagbeDequeue0ne] Error: Channel error: ##################################</pre>	<pre>nect to the D-BUS daemon: or message nect to the D-BUS daemon: or message et by peer: file /build/f rome/common/ipc_channel_p et by peer: file /build/f rome/common/ipc_channel_p et by peer: file /build/f rome/common/ipc_channel_p et by peer: file /build/f rome/common/ipc_channel_p : cannot send/recv : cannot send/recv</pre>						

For other Linux operation system

It' s much simple when you are using Linux operation system.

Just ssh into the Linux system of your choice using the -Y argument.

[02/20/2017 16:35] root@ubuntu:/home/seed# ssh -i id_geni_ssh_rsa -Y kqing051@pc 2.geni.it.cornell.edu -p 31037 The authenticity of host '[pc2.geni.it.cornell.edu]:31037 ([192.122.236.81]:3103 7)' can't be established. RSA key fingerprint is 00:a0:ac:5a:00:99:d6:2b:bc:49:24:be:46:d1:92:fe. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '[pc2.geni.it.cornell.edu]:31037,[192.122.236.81]:310 37' (RSA) to the list of known hosts. Enter passphrase for key 'id_geni_ssh_rsa':

Then run Firefox browser.

Command:" firefox"

Termina	l 🔀 🕏 ♣ 🖡 ୶)) 4:37 PM
	🛛 🖨 🔲 Mozilla Firefox (on ws.ca.ch-geni-net.geni.it.cornell.edu)
	New Tab × +
	() Search or enter address
	😣 🖨 🗉 kqing051@ws: ~
	(firefox:20018): GLib-GObject-CRITICAL **: g_object_ref: assertion 'obj count > 0' failed
	(firefox:20018): GLib-GObject-CRITICAL **: g_object_unref: assertion 'o f_count > 0' failed
	(firefox:20018): GLib-GObject-CRITICAL **: g_object_ref: assertion 'obj count > 0' failed
102	

Test Apache service and PHP service

Now because we already installed and enable the browser. We can test

the Apache service and PHP service installed before.

Test Apache service

Open the Firefox browser using command "firefox"

Enter "127.0.0.1" on the browser. If it shows the following image then it

means the Apache service is installed successfully.



Test PHP service

We can write a simple PHP website and then run it to test whether the

PHP service is installed successfully or not.

For the convenience, we can use the WinSCP software to write PHP source code. The instruction of how to log onto GENI node using WinSCP can be found in this link:

http://mountrouidoux.people.cofc.edu/CyberPaths/winscp.html

Кеу ра	Key passphrase - kqing051@pc2.geni.it.cornell.edu ×						
	Searching for host						
	Connecting to host						
	Authenticating						
	Using username "kqing051".						
	Authenticating with public key "imported-openssh-key".						
Passphrase for key 'imported-openssh-key':							
	OK Cancel <u>H</u> elp						

We need to give the privilege to edit the "www" folder under the /var. As

I mentioned before, "www" folder contains the website source code.

Command:" sudo chmod 777 /var/www"

kqing051@ws:/var/w	ww\$	sudo	su
root@ws:/var/www#	chmo	d 777	html
root@ws:/var/www#			

Under the "www/html" folder, create a file named "info.php" and then write the following code into it: <?php phpinfo();

?>				
/var/www/html				
Name	Size	Changed	Rights	Owr
<u>↓</u>		2017/2/20 20:31:04	rwxrwxr	vx roo
info.php	1 KB	2017/2/20 20:39:02	rw-rr	kqir
💿 index.html	12 KB	2017/2/20 18:40:34	rw-rr	roo
/var/www/html/info.p	ohp - kqing0	51@pc2.geni.it.corne	ell.edu - Editor ·	WinSCP
🔲 🔓 🖻 👘 🔺 💼 🕽	(a 🍤 C	🗄 🏙 🎭 🗟 🖷 🛛 E	ncoding 🕶 🗌 🤇	Color 🕶 🍇
php</td <td></td> <td></td> <td></td> <td></td>				
phpinfo();				
?>				

And then we need to restart the Apache service.

Command:"sudo /etc/init.d/apache2 restart"

```
kqing051@ws:/$ sudo /etc/init.d/apache2 restart
* Restarting web server apache2
kqing051@ws:/$
```

Run the browser and this time enters "127.0.0.1/info.php" into the browser. If we can see the relative configuration information of PHP then it means that PHP service is installed successfully.

📵 phpir	nfo() - Mozilla Firefo	×					_		\times
phpinf	'o()	× +							
(•) ()	127.0.0.1/info.php		C Q Sea	rch	☆自	÷	î		\equiv
	PHP Versio	on 5.5.9-1ubun	tu4.21		P	h			•
	System	Linux ws.ca.ch-geni-net Tue Jul 29 16:45:05 UTC	.geni.it.cornell.e 2014 x86_64	du 3.13.0-33-g	eneric #58	Ubunt	u SMP		
	Build Date	Feb 9 2017 20:54:17						1	
	Server API	Apache 2.0 Handler]	
	Virtual Directory Support	disabled							
	Configuration File (php.ini) Path	/etc/php5/apache2							
🧬 kqing	051@ws: ~				-		×	1	
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	t failed to without any	connect to t error messag	:he D-BUS Je	daem	on: ^		
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	nt failed to without any	connect to t error messag	:he D-BUS Je	daem	on:		
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	nt failed to without any	connect to t error messag	:he D-BUS Je	daem	on:		
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	nt failed to without any	connect to t error messag	:he D-BUS Je	daem	on:	_	
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	t failed to without any	connect to t error messag	the D-BUS Je	daem	on:		
(firefo //bin/d	x:21342): GCon bus-launch ter	f-WARNING **: Clien minated abnormally	t failed to without any	connect to t error messad	the D-BUS	daem	on:		

Set up certificate authority on GENI

GENI node is pre-installed OpenSSL. OpenSSL is a general purpose cryptography library that provides an open-source implementation of the SSL and TLS.

We can take a quick view of OpenSSL on GENI node. The folder is in the location of "/etc/ssl" We can see three documents already in this folder. The "certs" is a folder to store the digital certificate of this machine. "Private" is the folder to store the private key of the digital certificate.

"openssl.cnf" is the main configuration document of OpenSSL.

kqing051@ws:/etc/ssl\$ ls certs openssl.cnf private kqing051@ws:/etc/ssl\$

Right now, the documents of enabling the whole function of OpenSSL is not enough. We need to do some configurations.

Build Certificate Authority

Firstly, we need to do something on certificate authority node, which is CA node in our topology to let it be able to play a role as a certificate authority.

Create some new documents in this folder.

root@ca:/etc/ssl# ls								
cacert.pem	index.txt.attr	private	ws.csr					
certs	index.txt.old	serial						
crl	newcerts	serial.old						
index.txt	openssl.cnf	ws.crt						
root@ca:/etc	c/ssl#							

We must create newcerts folder and index.txt. If we don't then we will

get stuck with the issue step.

Create a serial document and set the serial number.

```
kqing051@ca:/etc/ssl$ sudo touch serial
kqing051@ca:/etc/ssl$ sudo echo 01 > serial
-bash: serial: Permission denied
kqing051@ca:/etc/ssl$ sudo su
root@ca:/etc/ssl# echo 01 > serial
root@ca:/etc/ssl#
```

And then make changes in openssl.cnf.

To succeed it, we should give the privilege to write openssl.cnf.

Command:" sudo chmod 777 openssl.cnf"

```
kqing051@ca:/etc/ssl$ sudo chmod 777 openssl.cnf
kqing051@ca:/etc/ssl$
```

And then using WinSCP open it and set the following values as followings:

/etc/ssl/openssl.cnf - kqing051@pc2.geni.it.cornell.edu - Editor - WinSCP								
🗖 🔓 🖻 🤞 🛙	🗅 🗙 a 🆻 C 🛗 🎎 🗟 🗏	📗 Encoding 🗕 🗆 Color 🗕 🎡 🖓						
#################		*****						
[CA_default]								
dir 🤇	= /etc/ssl	# Where everything is kept						
certs	= \$dir/certs	# Where the issued certs are k						
crl_dir	= \$dir/crl	# Where the issued crl are kep						
database	= \$dir/index.txt	<pre># database index file.</pre>						
<pre>#unique_subject</pre>	= no	# Set to 'no' to allow creatic						
		# several ctificates with same						
new_certs_dir	= \$dir/newcerts	<pre># default place for new certs.</pre>						

📝 /etc/ssl/openssl.cnf - kqing051@pc2.geni.it.cornell.edu - Editor - WinSCP						
□ □ □ < □ × □ × □ # req_extensions = v3_req # The	extensions to add to a certificate					
<pre>[req_distinguished_name] countryName countryName_default countryName_min countryName_max</pre>	<pre>= Country Name (2 letter code) = US = 2 = 2</pre>					
stateOrProvinceName stateOrProvinceName_default	= State or Province Name (full name = MD					
localityName	= Locality Name (eg, city)					
0.organizationName 0.organizationName_default	= Organization Name (eg, company) = JHU					
# we can do this but it is not n #1.organizationName #1.organizationName_default	needed normally :-) = Second Organization Name (eg, con = World Wide Web Pty Ltd					
organizationalUnitName #organizationalUnitName_default	= Organizational Unit Name (eg, se					

Then we need to generate root private key for the root digital certificate

for the certificate authority.

Command:" openssl genrsa -out private/cakey.pem 2048"

Create root digital certificate for the certificate authority.

Command:" openssl req -new -x509 -key private/cakey.pem -out ca

cert.pem"

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguish ed Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [US]: State or Province Name (full name) [MD]: Locality Name (eg, city) []: Organization Name (eg, company) [JHU]: Organizational Unit Name (eg, section) []: Common Name (e.g. server FQDN or YOUR name) []:jhuca.edu Email Address []:kqing0515@jhu.edu root@ca:/etc/ssl#

This time we set the server name as" jhuca.edu". You can set what ever as you like, we will do some configuration later so we can visit this server name as you set here.

On web server node

In this part, we need to log onto the WS node, which we have set it to be

a web server before.

Generate private key for web server

Command:" sudo openssl genrsa -out jhuws.key 2048"

root@ws:/etc/ssl# sudo openssl genrsa -out jhuws.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x10001)

Generate certificate sign request for the web server.

Command:" sudo openssl req -new -key jhuws.key -out jhuws.csr"

root@ws:/etc/ssl# sudo openssl req -new -key jhuws.key -out jhuws.csr You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguish ed Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [US]: State or Province Name (full name) [MD]: Locality Name (eg, city) [Baltimore]: Organization Name (eg, company) [JHU]: Organizational Unit Name (eg, section) [ISI]: Common Name (e.g. server FQDN or YOUR name) []:jhuws.edu Email Address []:kqing0515@jhu.edu Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:admin An optional company name []: root@ws:/etc/ssl#

Issue a digital certificate

In this step, CA node needs to get the request sign document .csr from the web server. We can use WinSCP or SCP command to make the transportation. If we want to transport it using WinSCP, we can firstly use command chmod to give out the privilege and then transport it. It's the same in the later using of the WinSCP.

Command:" chmod 777 file_name"

In this case, it should be:" chmod 777 jhuws.csr"

eni.it.cornell.edu (2) 📑 New Session							
» 🗲 🏠 🔂 🛨 🔶 🗣 🗣 🔷 🖉 📽							
📲 📄 Download 👻 📝 Edit 👻 💢 👋 🐩 🕂 👻							
/etc/ssl							
Name	Size	Changed					
↓		3/3/2017 11:22:33					
certs		3/5/2015 5:10:46 PI					
newcerts		3/1/2017 1:50:26 A					
📜 private		2/20/2017 11:01:46					
🗋 cacert.pem	2 KB	3/3/2017 11:43:39,					
🗋 crl	0 KB	2/20/2017 10:46:16					
index.txt	1 KB	3/1/2017 1:50:26 A					
index.txt.attr	1 KB	3/1/2017 1:50:26 A					
index.txt.attr.old	1 KB	2/20/2017 11:30:05					
index.txt.old	1 KB	2/20/2017 11:30:05					
jhuws.csr	2 KB	3/3/2017 11:46:34					
openssl.cnf	11 KB	2/20/2017 11:00:14					
serial	1 KB	3/1/2017 1:50:26 A					
serial.old	1 KB	2/20/2017 11:30:05					

root@ca:/etc	c/ssl# ls		
cacert.pem	index.txt.attr	newcerts	serial.old
certs	index.txt.attr.old	openssl.cnf	
crl	index.txt.old	private	
index.txt 🤇	jhuws.csr)	serial	
root@ca:/et@	c/ssl#		

Then we can sign this digital certificate on CA node.

Command:" openssl ca -in /etc/ssl/jhuws.csr -out /etc/ssl/jhuws.crt -days 3650"

root@ca:/etc/ssl# openssl ca -in /etc/ssl/jhuws.csr -ou							
t /etc/ssl/jhuws.crt -days 3650							
Using configuration from /usr/lib/ssl/openssl.cnf							
Check that the request matches the signature							
Signature ok							
Certificate Details:							
Serial Number: 3 (0x3)							
Validity							
Not Before: Mar 3 17:11:40 2017 GMT							
Not After : Mar 1 17:11:40 2027 GMT							
stateOrProvinceName = MD							
organizationName = JHU							
organizationalUnitName = ISI							
commonName = jhuws.edu							
emailAddress = kqing0515@jhu.edu							
X509v3 extensions:							
X509v3 Basic Constraints:							
CA: FALSE							
Netscape Comment:							
OpenSSL Generated Certificate							
X509v3 Subject Key Identifier:							
07:04:F4:DB:62:9D:64:5B:C4:F5:7A:78:68:BD:E							
E-BC-96-ED-CD-1C							
V509v3 Authority Key Identifier:							
kowid.BE.22.99.56.ED.A6.B2.9D.D2.70.C1.EA.E							
6.02.77.22.02.65.06.30							
0:92:77:32:02:00:A9							



Then we send this digital certificate back to the web server, which is the

ws node. This still can be done by WinSCP.



We now can see this digital certificate.

We can use the cat command to view it on Linux, or we can just double

click and open it on Windows.

```
root@ws:/etc/ssl# cat jhuws.crt
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 3 (0x3)
   Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=MD, O=JHU, CN=jhuca.edu/emailAddre
ss=kqing0515@jhu.edu
       Validity
           Not Before: Mar 3 17:11:40 2017 GMT
           Not After : Mar 1 17:11:40 2027 GMT
        Subject: C=US, ST=MD, O=JHU, OU=ISI, CN=jhuws.edu/e
mailAddress=kqing05150jhu.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d0:b9:79:57:20:4e:55:cf:e9:0f:31:b9:
                    fb:a4:68:52:a3:82:26:d0:e8:e6:b9:dd:54:
d7:38:
                    57:03:12:ff:b5:45:f0:33:02:70:d8:2e:2b:
```

A	Certificate	×				
Ge	eneral Details Certification Path					
	Certificate Information Windows does not have enough information to verify this certificate.					
	Issued to: jhuws.edu					
	Issued by: jhuca.edu					
	Valid from 3/3/2017 to 3/1/2027					
Install Certificate Issuer Statement						
	ОК					

And we can see clearly that this digital certificate is issued by jhuca.edu,

which is the certificate authority node and is issued to jhuws.edu, which

is the web server in our topology, the ws node.

Use these two commands to install the web server's digital certificate.

In other words, we should put the digital certificate file and key fileinto

the correct folder of the web server.

Command:" sudo cp jhuws.crt /etc/ssl/certs"

Command:" sudo cp jhuws.key /etc/ssl/private"

root@ws:/etc/ssl# sudo cp jhuws.crt /etc/ssl/certs
root@ws:/etc/ssl# sudo cp jhuws.key /etc/ssl/private
root@ws:/etc/ssl#

Now before we open the browser to see the result, we should copy the cacert.pem from ca node to user node, we need to let the ca to verify the digital certificate issued by ca, so we need this file on the web server. And we should change the extension ".pem" to ".crt". If you meet with the alarm of privilege when transport the file using WinSCP, just use command "chmod 777 file_name" to give out the privilege.



Result of issued digital certificate

Now we can view the result of the former work we have done.

The following operations are all on user node.

Firstly log onto the user node.

Because the display of browser on GENI is kind of slow. TO quick test whether we are right by far, we can install the "curl" to perform a quick test.

Curl is a tool to transfer data from or to a server, using one of the

supported protocols.

Use "sudo su" to enter the root account

Use "apt-get update" to update the existed packets.

Use "apt-get install curl" to install the curl.

Then move to the hosts file to do a little modification.



```
Use command " chmod 777 hosts" to give out the privilege.
```

📝 /etc/hosts - kqin	g051@pc2.geni.it.cornell.edu - Editor - WinSCP
■ 4 2 4 ×	🖺 🗙 🗿 💙 🥙 🏙 🎭 🏥 🖷 🛛 Encoding 🗸 🗆 Color 🗸 🍻 🥝
127.0.0.1	<pre>localhost loghost localhost.ca.ch-geni-net.geni.i</pre>
10.10.2.1	CA-link-1 CA-0 CA
10.10.1.1	user-link-0 user-0 user
10.10.3.2	ws-link-2 ws-2
10.10.1.2	ws-link-0 ws-1 ws
10.10.2.2	ws-link-1 ws-0
10.10.3.1	attacker-link-2 attacker-0 attacker
12.17.2.41	(jhuws. edu)
172.17.2.41	www.jhuws.edu

We do these modifications on it. While the "172.17.2.41" is the IP address of ws node, this is the web server in out topology. And jhuws.edu is the server name we set up by ourselves before.

Use command "curl jhuws.edu" to see if it works right.



It returns the HTML response of our web server. It seems it works well.

Then we test whether SSL configuration we modified before is work right.

We use this command "curl https://jhuws.edu --cacert cacert.crt" to test.

```
root@user:/etc/ssl# curl https://jhuws.edu --cacert cacert.
crt
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
 <title>Index of /</title>
</head>
<body>
<h1>Index of /</h1>
 <img src="/icons/blank.gif" alt="[]
CO]"><a href="?C=N;O=D">Name</a><a href="
?C=M;O=A">Last modified</a><a href="?C=S;O=A">Size
</a><a href="?C=D;O=A">Description</a>
  <hr>
<img src="/icons/folder.gif" alt="[DIR
```

It also works well. So we can turn to the browser.

Open the browser on user node. You can refer the instruction before

about how to run and open a browser on GENI node.

We visit the jhuws.edu/info.php first.



It works right, and then we install the digital certificate. We go to the preference option of the browser.



Then go to the Advanced, Certificates options. Click on "View Certificates"



Then import the cacert.crt file we put on user node before.

🔮 Preferences - Mozilia Firefox								×
Apachel Ubunta Default Page 🛪 🖄 Preferen	ces × +	+						
Contraction about preferences#advanced			C Q, Search		会 自	+	÷ 0	, ≡
Centeral Vour Centric Vour Centric Centricate Na Control on Centricate Na Centric on Centric o	ed N Select File containing CA Places Harns Deaktop Deaktop Campater	certificate()) to import certificate()) to import certificate() to import	Carol	Certificate Nia V	R CK			

Trust this certificate authority we build by our own.



Now we can see our certificate authority is in the list of certificate

authorities.

		Certificat	te Manager	x
	Your Certificates People Serve	rs Authorities	Others	
	You have certificates on file that identify the	se certificate authorit	ies:	
	Certificate Name		Security Device	C\$
	ApplicationCA - Japanese Government		Builtin Object Token	-
1	⇒JHU			
4	jhuca.edu		Software Security Device	
	🗢 Krajowa Izba Rozliczeniowa S.A.			
	SZAFIR ROOT CA2		Builtin Object Token	
	⇒LuxTrust S.A.			
	LuxTrust Global Root 2		Builtin Object Token	
	⇒ Microsec Ltd.			
	Microsec e-Szigno Root CA		Builtin Object Token	
	Microsec e-Szigno Root CA 2009		Builtin Object Token	
	∽ NetLock Kft.			
	View. Edit Trust. Import.	Export Delete o	r Distrust	
	Territ Territoria	Tourse		ОК

We visit jhuws.edu/info.php firstly, we can see the connection is unsecure.

a 🥑	phpinfo() - Mozilla Firefox				
5	ohpinfo()	× +				
- () () ji	huws.edu/info.php				
jhuws.edu Connection is Not Secure			>		HP Versio	on 5.5.9-1u
	××	Permissions You have not granted this site any specia	al			
		permissions.			stem	Linux ws.ca.ch-g Tue Jul 29 16:45:
				Bu	ild Date	Feb 9 2017 20:5

Then we visit https://jhuws.edu/info.php

phpinfo() - Mozilla Firefox		
phpinfo() × +		
E C C C C C C C C C C C C C C C C C C C		▼ C Q Search
jhuws.edu Secure Connection	> HP Versio	on 5.5.9-1ubuntu4.21
Permissions		
You have not granted this site any special		
permissions.	/stem	Linux ws.ca.ch-geni-net.geni.it.cornell.edu 3.13.0-33-generic #58-Ubuntu SMP Tue lul 29 16:45:05 UTC 2014 x86 64
	Build Date	Feb 9 2017 20:54:17
	Server API	Apache 2.0 Handler
	Virtual Directory Support	disabled
	Configuration	Jate Inho 5 Janacha 2

And this time we can see there appears a green lock and remind us now

it's a secure connection.

We can view the details of this connection by click the ">" .

ipinfo() - Mozzilia Firefox							-	
pinfo() × +								
🕕 🔒 https://jhuws.edu/info.php			C Q, Se	arth .	合自	+	÷ 5	9 1
Carl Lada Manari bara ad d	PHP Vers	eviseduliritaphp		- a x				
General Details		alona Security		_				
This certificate has been verified for t SSL Client Certificate SSL Server Certificate	the following uses:	du bsibe does not supply own	mship information					
Email Recipient Certificate Object Signer		te orier to today?	No.	View Certificate				
Issued To Cammon Name (CN) Provised Organization (C) (P4) Organizational Unit (DU) (S) Serial Number 0.3 Issued By Cammon Name (CN) (Packedus		ng prior to today? Pormation (cookies) on my ands for this website?	No No	View Cooğies Vieg Saved Pasawards				
Organization (3) P4U Organizational Unit (0U) < Nut Part Of Cert Period of Validity Begins On 03/03/2017 Expines On 03/01/2027	ficate>	(TLS_ECOME_RSA_WITH_A g was encrypted before being cult for unauthorized people to typone read this page as it trave	ES_120_GCM_SHA transmitted over the oview information to eled across the netw	256, 128 bit keys, TLS 1.2) i Internet. aveling between computers. It is of.				
Fingerprints BF: DA: 57: P9:81: 83: 40: 6F: 80:26: SHA. 256: Ringerprint SF-20:44: 91:15: SHA1 Ringerprint S6: P0:44:91:15:	75:52:56:59:72:31:57:39:01:78:54: 55:79:52:40:157:47:54:56:15 58:40:75:58:73:80:03:81:25:30:70:61:31:13:36			Help				
	 Extension	í						

The information we put in when making the digital certificate is shown in this display.

By now, we have already finished the experiment of building a certificate authority and issue a digital certificate.

Revoke a digital certificate

Then we can try to revoke the digital certificate to see how it works and what is the result it will turn out.

To revoke the digital certificate we issue before, we should log onto the

ca node, which is the certificate authority.

Use this command to revoke the digital certificate we issued before. The

name of digital certificate we issued before is "jhuws.crt"

Command : "openssl ca -revoke jhuws.crt"

```
root@ca:/etc/ssl# openssl ca -revoke jhuws.crt
Using configuration from /usr/lib/ssl/openssl.cnf
Revoking Certificate 03.
Data Base Updated
root@ca:/etc/ssl#
```

We can use this command" cat index.txt" to check the index of our

digital certificate. It' s 03, so everything is going right.



And we should renew the crl, which is short for Certificate Revocation List.

The digital certificate we revoked will be given the index and record in

this list.

Use this command:" openssl ca -gencrl -out thisca.crl" to generate the

index of the digital certificate we just revoke.

We can have a look at the thisca.crl file.

```
root@ca:/etc/ssl# cat thisca.crl
----BEGIN X509 CRL-----
MIIBzTCBtgIBATANBgkqhkiG9w0BAQsFADBeMQswCQYDVQQGEwJVUzELMAk
GA1UE
CAwCTUQxDDAKBgNVBAoMA0pIVTESMBAGA1UEAwwJamh1Y2EuZWR1MSAwHgY
JKoZI
hvcNAQkBFhFrcWluZzA1MTVAamh1LmVkdRcNMTcwMzAzMjAyMDU2WhcNMTc
wNDAy
MjAyMDU2WjAUMBICAQMXDTE3MDMwMzE4NTcxN1qgDjAMMAoGA1UdFAQDAgE
BMA0G
CSqGSIb3DQEBCwUAA4IBAQBn9NtW3cCcNJwZ9d8Gc0BThE0FajYHwz62WZm
+0oPM
```

It stores the Certificate Revocation List.

Then we need add content " 00" into " crlnumber", to let the crl start to record.

Each time we revoke a digital certificate, it will add one to itself.



I have revoked twice the digital certificate, so the number shown is 02.

Then we have successfully revoked a digital certificate we issued before.

Result of revoke a digital certificate

To see the result after we revoke an issued digital certificate. Because we are actually not using network to verify. Therefore we need to import the new cacert.crt onto the user node.

Remove the old cacert.crt and import the new cacert.crt. As the same we have done before, we actually move the file "cacert.pem", but we need to change the extension".pem" to ".crt".

```
root@user:/etc/ssl# ls
cacert.crt certs openssl.cnf private
root@user:/etc/ssl# rm cacert.crt
root@user:/etc/ssl#
```

	_		×
n <u>O</u> ptions <u>R</u> emote <u>H</u> elp 🦃	🖁 🎽 Transfe	r Settings '	* 💋 🗸
c2.geni.it.cornell.edu (3) 📑 Ne	ew Session		• •
🛓 📙 SS 🔻 🚰 🕎 🛛 🖛 🕶	-	1 🏠 🄁	»
» 📳 Download 👻 📝 Edit	t - 🗙 📝		» 🕂 *
/etc/ssl			
Name Name Certs private cacert.crt openssl.cnf	Size 2 KB 11 KB	Changed 3/3/2017 3/5/2015 8/20/2014 3/3/2017 8/7/2014	2:16:03 PI 5:10:46 PI 4 5:23:02 I 11:43:39 J 9:47:07 A

Also we should move the thisca.crl which stores the Certificate

Revocation List to the user node.

		_	
ion	Options Remote Help	🕻 🔭 🛛 Transfe	r Settings 🎽 🥑 🗸
pc2	2.geni.it.cornell.edu (4) 📑 N	ew Session	4 F
	📕 ss 🔻 🚰 🕎 🛛 🖛 🕶	E 7	🔒 🔁 🔹 🕺
- »	🛙 📄 Download 👻 📝 Edi	t • 🗙 📝	» + »
	/etc/ssl		
	Name	Size	Changed
1	1		3/3/2017 2:16:03 PI
	📜 certs		3/5/2015 5:10:46 PI
	📕 private		8/20/2014 5:23:02
	acert.crt	2 KB	3/3/2017 11:43:39
	openssl.cnf	11 KB	8/7/2014 9:47:07 A
	thisca.crl	1 KB	3/3/2017 2:40:29 PI

Because our certificate authority is offline, therefore we need to move

these files manually.

Then we can see the result after we revoke a digital certificate. We still use curl tool to find out.

We use this command: " curl https://jhuws.edu --cacert cacert.crt --crlfile thisca.crl" to visit our site we build before. We need the options " —cacert" and "—crlfile" to include the ca document and crl document manually.

root@user:/etc/ssl# curl https://jhuws.edu --cacert cacert. crt -- crlfile thisca.crl curl: (60) SSL certificate problem certificate revoked More details here: http://curl.haxx.se/docs/sslcerts.html curl performs SSL certificate verification by default, usin q a "bundle" of Certificate Authority (CA) public keys (CA certs). If t he default bundle file isn't adequate, you can specify an alternate : ile using the --cacert option. If this HTTPS server uses a certificate signed by a CA repr esented in the bundle, the certificate verification probably failed d problem with the certificate (it might be expired, or the name might

Now we can see the digital certificate has already been revoked.

As for the Firefox browser we installed before, we also need to update the ca document and crl document. But Firefox browser has already remove the user interface on Firefox to import the crl document, so we can't see the result on Firefox since we are the offline certificate authority and need us to import the ca document and crl document manually.

https://wiki.mozilla.org/CA:ImprovingRevocation#Preload_Revocations_

of_Intermediate_CA_Certificates

Remove CRL User-Interface

As of Firefox 24, the user-interface for importing CRLs via Firefox has been removed. Auto-importing/updating of CRLs through Firefox has also been removed. NSS still supports CRLs, but Firefox is moving away from checking CRLs, and moving towards using a revocation list push mechanism.

• Release: Mozilla 24