Public Key Infrastructure & SSH

Troy Ligon

⇨What is Public Key Infrastructure?

⇨What does PKI have to do with DBA's and Developers?

⇨What does PKI have to do with SSH?

SUNCOAST ORACLE USERS' GROUP

- How does PKI work?
- How do I setup PKI?
- Using PKI with Putty
- Running an O/S script with PKI
- Running an Oracle script with PKI
- Putting it all together - DEMO

SUNCOAST ORACLE USERS' GROUP

What is PKI?
Public Key Infrastructure

- ⇨Public Key / Private Key Pairs
- ⇨Asymmetric Encryption
- ⇨Authentication

When information is encrypted with a private key, it can only be decrypted with the corresponding public key.

When information is encrypted with a public key, it can only be decrypted with its corresponding private key.

SIMPLE EMAIL EXAMPLE:
Troy wants to send secure email to Bob

1. Troy stores clear text in message.1
2. Troy encrypts message.1 with Bob's public key to produce message.2
3. Troy encrypts message.2 with Troy's private key to produce message.3
4. Troy sends message.3 to Bob
5. Bob decrypts message.3 with Troy's public key to produce message.4 (this ensures the message came from Troy)
6. Bob decrypts message.4 with Bob's private key to produce message.5 (this ensures the message was intended for Bob and only Bob can read the message)

What does PKI have to do with DBA's and Developers?

⇨Strong Authentication – cryptographic verification of the identity of user and server

⇨Data Confidentiality – assurance that only the intended recipient can read the data

⇨Data integrity – verification that no modification of the data has occurred

⇨Non-Repudiation – assured undeniability of participation in a transaction

What does PKI have to do with SSH?

⇨Eliminates need for passing Clear Text passwords over the network

⇨Encrypts the communication channel

- How does PKI work?
- How do I setup PKI?
- Using PKI with Putty
- Running an O/S script with PKI
- Running an Oracle script with PKI
- Putting it all together - DEMO

SUNCOAST ORACLE USERS' GROUP

PKI Setup
Create Public/Private Key Pair

```
$ ssh-keygen -t rsa


Generating public/private rsa2 key pair.
Enter file in which to save the key (/home/twl/.ssh/id_rsa):
Created directory '/home/twl/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/twl/.ssh/id_rsa.
Your public key has been saved in /home/twl/.ssh/id_rsa.pub.
The key fingerprint is:
c4:31:ed:df:5a:63:54:b7:26:9e:db:84:8c:cb:f4:d2 twl@server.com
```

PKI Setup
Create Public/Private Key Pair

$ cat id_rsa.pub

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQC6e8lN0Qcp4A1ntThazeBz11SlB4feSdr7pVHF2hEuU60aUyhtf
CSRGl0JL6ZR0yednyj0eus1QIHAdXXJ/4HHDRks1wxy6LOUhNLWF0JCYKrHtI5DvlaxyS6ESLAqVjYZMRkj
GPV4rZzoebV1yLci5iMrkFkbMNCuaZNsD3S0DQ== rsa2-Troy

$ cat .ssh/id_rsa

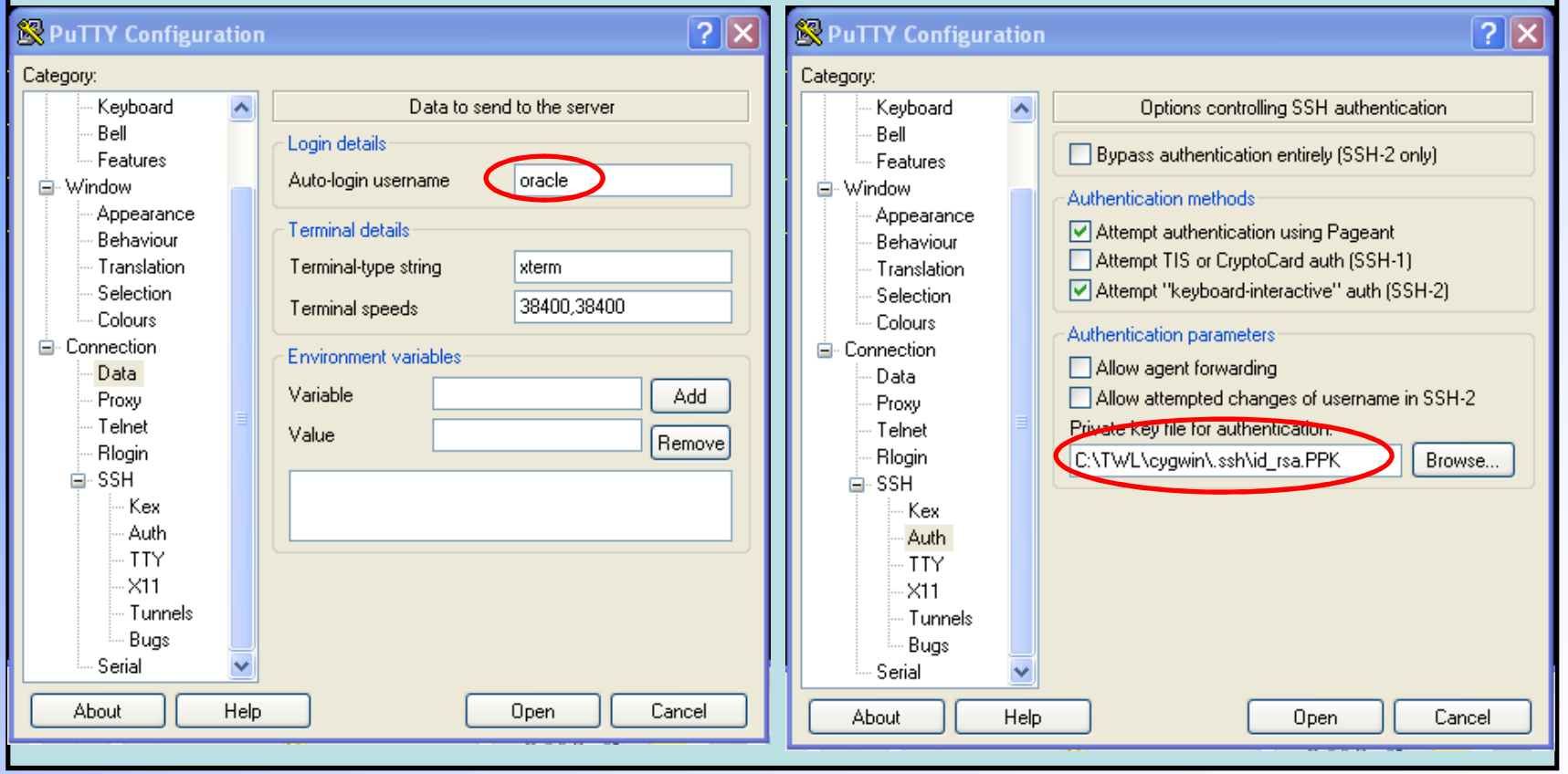
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC6e8lN0Qcp4A1ntThazeBz11SlB4feSdr7pVHF2hEuU60aUyht
fCSRGl0JL6ZR0yednyj0eus1QIHAdXXJ/4HHDRks1wxy6LOUhNLWF0JCYKrHtI5D
vlaxyS6ESLAqVjYZMRkjXYZ4rZzoebV1yLci5iMrkFkbMNCuaZNsD3S0DQIDAQAB
AoGATuYwtYvKzBzPjyFNRp30aQ6h8XDOO25kCDRZ9KveuQsOIiUs5aWwkvPkiQ5w
AA6mpDnCyi13doBkZVlNDLnd3fCwSFWAAONArC/JiK6Ax2wrPBvhzYiAUcOEylT6
Ujcf+TlM6+qQzEM6GpvJZkI8gewytBZDC2EasuT/chle2sECQQDm+/j+KoZCgb71
E56KaIZhTuRhkG7bZvkHPRRC35BCsKzNXzsdbMJGkPRzU/M+XSmurPo6IVkwt25W
TwVvoZ123EAzq4IgvrUimikzzbK5rmfz57gc6g24L2Ms42+9o6BGR1G7jtC6M3I
YyWtNlpmg4fgUbaYqJSC4qVmfEZnSBHdSwABCzIfmLMs48Ze891oKA+1St6hUENZ
1fFVaOohz+zdZI+VbCHbCwyXelQWM8MpPA2nQo2CGJemN8HHIUXLY4y32QJAa3aZ
/mCleoIGj6eRwH3r1mxpkDl6r0hfjEy7aj+WaJSMePpfQ+UbuFGyynweqW1Q+avT
nHP7yhTuQNfqg9KmGQJBALG4ZN4wZMxMODQWowLA8tyfPL/blzsIQ733+6v78QXZ
jac0thBbltp/+Tm1iBSShQykOlo+41G/EQw75sDXsms=
-----END RSA PRIVATE KEY-----

SUNCOAST ORACLE USERS' GROUP

PKI Setup
Place Public Key on Target Server

```
$ cat id_rsa.pub >> ~oracle/.ssh/authorized_keys
$ chmod 755 ~oracle
$ chmod 755 ~oracle/.ssh
$ chmod 644 ~oracle/.ssh/authorized_keys
```

PKI Setup
Point PUTTY at Private Key



- How does PKI work?
- How do I setup PKI?
- Using PKI with Putty
- Running an O/S script with PKI
- Running an Oracle script with PKI
- Putting it all together - DEMO

SUNCOAST ORACLE USERS' GROUP

LIVE DEMOS

(wish me luck!)

Running scripts with PKI

```
vi testfile.sql
      spool testfile.log
      select * from v$database;
      exit
scp testfile.sql  oracle@dayrheocrp019
ssh oracle@dayrheocrp019 cat testfile.sql
ssh oracle@dayrheocrp019 sqlplus "/ as sysdba" @testfile.sql
scp dayrheocrp019:testfile.log .
cat testfile.log
```

Troy's Tools – SERVER_PUSH.SH

get_crontab

get_dba

get_dbsize

get_os_space

Public Key Infrastructure

Troy Ligon
tligon@soug.org

SUNCOAST ORACLE USERS' GROUP