Assignment7

Shu Fay Ung

March 13 2018

1 Threat Model

The MI6 are hacking into a group of researchers' computers, believing they stole private data on the Royal family's genome in an attempt to synthesize a lethal biological weapon to wipe out the monarchy. They have the British government behind their backs as well as the best hackers (coerced) to carry out the task. They have the authority to access background information on the researchers (NHS, General Register Office, Ministry of Education) and their internet traffic from ISPs and mobile carriers. If the need arises, they also have the ability to gain physical access to the researchers' computers through discrete methods.

At the same time, the law itself provides legal avenues of defence for the researchers via the General Data Protection Regulation (GDPR).

2 RSA

RSA is a public-key cryptosystem that utilizes the following relation for all integers m, $0 \leq m < n$:

$$(m^e)^d \equiv m \pmod{n}$$

where e, d and n are very large positive integers that could be practically generated. Here, e and n are the public keys while d is the private key, and m is the message to be encrypted. The message is encrypted with the public key and decrypted with the private key. RSA relies on the fact that with current computational methods, the private key d is extremely difficult to find knowing e, n or even m.

The algorithm involves four steps: key generation, key distribution, encryption and decryption. After the keys are generated by a complicated process involving prime numbers, the receiver sends their public key to be used for message encryption to the sender. The sender uses the receiver's public keys e and n to generate the cipher text $c \equiv m^e \pmod{n}$ and sends it to the receiver. The receiver decrypts the cipher text with their private key d by computing $c^d \equiv (m^e)^d \equiv (m \bmod n)$.

2.1 Weaknesses

Factorization The security of RSA is based on the difficulty of factorizing large numbers and the RSA problem, which involves finding the integer m satisfying $c \equiv m^e \pmod{n}$ given c, e and n. No polynomial-time method for factoring large numbers on a classical computer has yet been found. The difficulty of solving these problems scales with the length of the keys in bits. As of 2010, the largest factored RSA number was 768 bits long. With technological advancement, longer keys could be factored in feasible time, posing a threat to RSA security. Furthermore, Peter Shor proved that a quantum computer could factor integers in polynomial time. For practical purposes, however, it is recommended that RSA keys be at least 2048 bits long.

Timing Attacks If the hardware of the receiver is known in sufficient detail and the decryption time for several cipher texts could be measured, the decryption key d could be deduced quickly. This could be avoided by ensuring that the decryption time is constant for every cipher text. However, this approach can significantly reduce performance. An alternate method, cyrtographic blinding, is employed instead, which de-correlates the decryption time and the value of the cipher text input, rendering timing attacks void.

3 SSH

SSH is a cryptographic network protocol for operating network services securely over an unsecured network. The SSH client uses public-key cryptography to authenticate the SSH server. After the setup phase, the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of data exchanged between the client and sever.

Although SSH stands for Secure Shell, it is not a true shell in the sense of the Unix Bourne Shell and C shell. Rather, it creates a channel for running a shell on a remote computer with end-to-end encryption between the local and remote computer.

Vulnerabilities of SSH include its susceptibility to IP and TCP attacks, traffic analysis attacks and its requirement of a password which leads to insecurities on the user's behalf.

3.1 Proof of Work

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Thu Mar 15 16:44:16 2018 from beavernet-162.caltech.edu

Agent pid 22399
Identity added: /home/controls/.ssh/id_rsa_craigGitlab (rsa w/o comment)
(pyenv) ]0;controls@ws1: ~controls@ws1:~$ dvdv[K[Klaunch
-bash: dvlaunch: command not found
(pyenv) ]0;controls@ws1: ~controls@ws1:~$ LIGONDSIP=localhost dataviewer
Connecting.... done
Warning: Cannot convert string "-adobe-helvetica-medium-r-normal-*-12-*-*-*-*-*-*-*" to
 ↪  type FontStruct
Warning: Not all children have same parent in XtManageChildren
Warning: Not all children have same parent in XtManageChildren
Warning: Not all children have same parent in XtManageChildren
Warning: Not all children have same parent in XtManageChildren
Warning: Not all children have same parent in XtManageChildren
Error in obtaining chan info.
Connecting.... done
Error in obtaining chan info.
(pyenv) ]0;controls@ws1: ~controls@ws1:~$ ipython
WARNING: Attempting to work in a virtualenv. If you encounter problems, please install
 ↪  IPython inside the virtualenv.
```

```
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
Type "copyright", "credits" or "license" for more information.

IPython 2.3.0 -- An enhanced Interactive Python.
?         -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help      -> Python's own help system.
object?   -> Details about 'object', use 'object??' for extra details.

[0;34mIn [[1;34m1[0;34m]: [0mimport nds2

[0;34mIn [[1;34m2[0;34m]: [0mc = nds2.connection('10.0.1.156', 8088)

[0;34mIn [[1;34m3[0;34m]: [0mgpstime = 1201902464

[0;34mIn [[1;34m4[0;34m]: [0mchanName = 'C3:PSL-SCAV_FSS_SLOWOUT'

[0;34mIn [[1;34m5[0;34m]: [0mfrom pylab import *

[0;34mIn [[1;34m6[0;34m]: [0mion()

[0;34mIn [[1;34m7[0;34m]: [0mdata = s.[K[Kc/[K.de[K[Kfetch(gpstime, gpstime+50000,
↪  [chanName])

[0;34mIn [[1;34m8[0;34m]: [0mplot(data[0].data)
[0;31mOut[[1;31m8[0;31m]: [0m[<matplotlib.lines.Line2D at 0x7f885538b950>]

[0;34mIn [[1;34m9[0;34m]: [0mexit
(pyenv) ]0;controls@ws1: ~controls@ws1:~$ exit
logout
```

4 Secure Authentication Mechanisms

A secure authentication mechanism begins with the user having a valid user account configured by the network administrator that specifies the user's permissions and rights. User credentials (passwords, smart cards, digital certificates etc) are associated with this account and stored in a database. When the user wishes to log on, they must provide the correct credentials and access is granted only if those credentials match those in the database.

A strong password could be compromised by a data breach where hackers release the passwords to millions of accounts online.

5 Takeaways

I've learned about the common encryption technique RSA and protocols such as SSH that help protect the privacy and integrity of users. Encryption provides freedom for the individual within the digital realm; this is especially so for those oppressed under politically intense regimes. In terms of the threat model developed above, the RSA encryption scheme could provide an extra layer of protection for communications between the researchers.