

# Debian OpenSSL Vulnerability

Andy Saunders and David Ford  
Oxford University Computing Services

# Introduction

- What happened
- What does this mean
- What is affected
- What to do about it

# What happened?

- Debian patch to OpenSSL in Sep 2006
- Random Number Generator broken
- Key space vastly reduced in size

# What does this mean?

- Only ~30K possible keys
- User key space searched in 1.5 hours
- Lists of private keys published
- We need to take action now

# What is affected?

- Debian testing/unstable since Sep 2006
- Debian Etch
- Ubuntu 7.04, 7.10, 8.04
- other OSs where vulnerable keys used

# Which type of keys?

- SSH host keys
- SSH user keys
- X.509 certificates used by secure web servers, mail servers, OpenVPN etc.

# What does compromise mean?

- Server keys - impersonation of your service
- User keys - login to your service

# What to do?

- Apply latest Debian patches
- Includes libssl0.9.8, openssh-server, openssh-client, openssh-blacklist

- The only safe thing to do is to regenerate every key pair

# openssh-blacklist

- debian package containing some vulnerable key fingerprints
- will tell you about some vulnerable keys
- not guaranteed

# Other OSs

- Any private DSA key generated elsewhere and used on Debian is compromised
- RSA key likely compromised

# SSH user keys

- Even if your OS is unaffected, you may have vulnerable user keys
- Check fingerprints (`ssh-keygen -l -f`) against key blacklists
- `dowkd.pl` from <http://wiki.debian.org/SSLkeys>
- Blacklists are not exhaustive

# Server keys

```
# ls -l /etc/ssh  
  
-rw-r--r-- 1 root root 2064867 May 13 15:23 blacklist.DSA-1024  
  
-rw-r--r-- 1 root root 2064867 May 13 15:23 blacklist.RSA-2048  
  
-rw----- 1 root root      672 May 13 16:43 ssh_host_dsa_key  
  
-rw-r--r-- 1 root root      600 May 13 16:43 ssh_host_dsa_key.pub  
  
-rw----- 1 root root    1675 May 13 16:43 ssh_host_rsa_key  
  
-rw-r--r-- 1 root root      392 May 13 16:43 ssh_host_rsa_key.pub
```

# User keys

```
$ ls -l ~/.ssh
```

```
-rw-r----- 1 andy andy 616 2008-05-13 19:05 authorized_keys2  
-rw----- 1 andy andy 744 2008-05-13 19:05 id_dsa  
-rw----- 1 andy andy 616 2008-05-13 19:05 id_dsa.pub  
-rw----- 1 andy andy 542 2008-05-13 19:05 identity  
-rw----- 1 andy andy 346 2008-05-13 19:05 identity.pub  
-rw-r--r-- 1 andy andy 3091 2006-05-05 19:05 known_hosts2
```

# Further reading

- Security advice and links to vendor announcements
- `http://www.oucs.ox.ac.uk/network/security/bulletins/`