OpenSSH Security Advisory: cbc.adv

This is the second revision of this advisory, correcting an error in the estimated number of connection attempts required for a successful attack.

Regarding the "Plaintext Recovery Attack Against SSH" reported as CPNI-957037[1]:

The OpenSSH team has been made aware of an attack against the SSH protocol version 2 by researchers at the University of London. Unfortunately, due to the report lacking any detailed technical description of the attack and CPNI's unwillingness to share necessary information, we are unable to properly assess its impact.

Based on the description contained in the CPNI report and a slightly more detailed description forwarded by CERT this issue appears to be substantially similar to a known weakness in the SSH binary packet protocol first described in 2002 by Bellare, Kohno and Namprempre[2]. The new component seems to be an attack that can recover 14 bits of plaintext with a success probability of 2^-14, though we suspect this underestimates the work required by a practical attack.

For most SSH usage scenarios, this attack has a very low likelihood of being carried out successfully - each attempt has a low probability of success and each failure will cause connection termination with a fatal error. It is therefore very unlikely for an interactive session to be usefully attacked using this protocol weakness: an attacker would expect around 11356 connection-killing attempts before they are likely to succeed. This level of disruption would certainly be noticed and it is highly unlikely that any user would retry the connection enough times for the attack to succeed.

The usage pattern where the attack is most likely to succeed is where an automated connection is configured to retry indefinitely in the event of errors. In this case, it might be possible to recover on average 44 bits of plaintext per hour (assuming a very fast 10 connections per second). Implementing a limit on the number of connection retries (e.g. 256) is sufficient to render the attack infeasible for this case.

AES CTR mode and arcfour ciphers are not vulnerable to this attack at all. These may be preferentially selected by placing the following directive in sshd_config and ssh_config:

Ciphers aes128-ctr,aes256-ctr,arcfour256,arcfour,aes128-cbc,aes256-cbc

A future version of OpenSSH may make CTR mode ciphers the default and/or implement other countermeasures, but at present we do not feel that this issue is serious enough to make an emergency release.

[1] http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
[2] http://www.cs.washington.edu/homes/yoshi/papers/TISSEC04/