Yui Kee Computing Ltd.

Newsletter

June 2003

Contents

Contents 1
Incident Update 1
BCS and "Matrix Reloaded" 1
SSH Security Advisory 1
Problem 1
Fix 2
Who is Affected 2
Allan Dyer Advocates Defence in Depth 2
Yui Kee at the Information Security Showcase 3

Incident Update

W32/Bugbear-B caused the biggest outbreak of the month, starting on 5th June. It can spread by email or across Windows shares, it attempts to kill many anti-virus and security programs, and it has backdoor functionality.

The list of W32/Sobig variants also grew steadily longer during June, with variants C, D and E discovered early on 1 June (Hong Kong time), 18 June, and 25 June respectively. Each variant so far is programmed to stop spreading on a certain date, W32/Sobig.E, currently listed as the most prevalent virus by MessageLabs, will stop spreading on 14 July 2003.

The persistentW32/Klez.H is still very common; MessageLabs currently list it as no. 2.

BCS and "Matrix Reloaded"

Allan Dyer

I was going to write about the British Computer Society's comments on "Matrix Reloaded", but Rob Rosenberger did it first, did it funnier, and has a cool anecdote, see:

http://vmyths.com/rant.cfm?id=612&page=4

SSH Security Advisory

A minor problem has been discovered in the RSA signature handling functions of SSH Secure Shell and F-Secure SSH. Customers with a valid maintenance subscription should contact us for an upgraded version of SSH Secure Shell or F-Secure SSH that address the problem.

Problem

The handling of RSA signatures is faulty and may expose the users that use RSA keys with SSH Secure Shell or F-Secure SSH to a potential attack. Launching such an attack would be highly impractical and the risk is considered minor.

To conduct a successful attack, the attacker would need to have the public key and would need to pre-compute the signature data so that it looks like a valid PKCS#1signature. This is a non-trivial task to perform and according to analysis it requires a minimum of 2^{67} RSA algorithm operations. Since the RSA algorithm is computationally fairly intensive, the time to undertake such an attack renders it impractical.

This problem however needs to be corrected by a maintenance release.

Fix

New versions of SSH Secure Shell that include the fix for the bug have been generated with version numbers 3.2.5 (for the 3.2 series) and 3.1.8 (for the 3.1 series).

The following versions of F-Secure SSH include the fix for the bug:

- F-Secure SSH Server for Unix 3.2.3 (CRITICAL UPDATE)
- F-Secure SSH Client for Unix 3.2.3
- F-Secure SSH Client for Windows 5.3
- F-Secure SSH Server for Windows 5.2, build 31 (CRITICAL UPDATE)
- F-Secure SSH Client/Server for Unix 1.3.14

Who is Affected

The discovered bug affects all RSA algorithm operations performed by SSH Secure Shell clients and servers for recent versions (3.1 and 3.2 series) and F-Secure SSH versions earlier than those listed above.

More precisely the affected scenarios are:

- Servers that use RSA keys as server hostkeys (not the defaultly used DSA keys)
- Cases where RSA keypairs are user for public key authentication for user authentication
- Cases where X.509 certificates (with RSA keys) are used for user authentication
- Cases where users of SSH Secure Shell clients connect to hosts that have RSA hostkeys
- Cases where hostbased authentication is used (when the SSH Secure Shell Server hostkeys are RSA keys)

SSH usage scenarios that are not affected:

- Cases where SSH servers use DSA keys (the default setting) for hostkeys, and password, hostbased authentication, RSA SecurID (or any user authentication method that does not involve the RSA algorithm)

In effect, most users and customers who run the SSH servers with default settings (ie. DSA host keys) and use password authentication need not worry. However, to be on the safe side it is suggested that they also consider upgrading.

Allan Dyer Advocates Defence in Depth

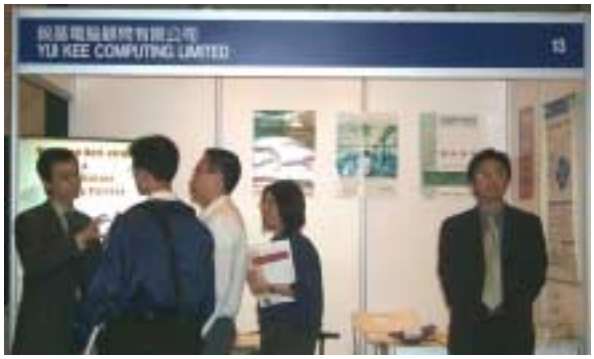
Our Chief Consultant, Allan Dyer, made a keynote speech in his capacity as President of AVAR at the Information Security Showcase 2003 organised by the HKPC. Addressing an audience of about 150, Dyer reflected on a decade of anti-virus in Hong Kong, compared the punishments of notable virus-writers and criticised the University of Calgary for planning to teach virus writing. He discussed defence from machine-local technical

levels, through network and user education to wider co-ordination and social viewpoints. His presentation should be available on the show website soon.

Yui Kee at the Information Security Showcase

Yui Kee exhibited for three days at the Information Security Showcase 2003 organised by the HKPC. The highlighted products were:

- YKAlert - Anti-Virus and Information Security alerts delivered to your mobile.
- Sophos Anti-Virus - Anti-virus for business.
- SSH Secure Shell - Are you securing your business communications?



- Training Courses - Expand your professional options and advance your career in security.
  - CCSP
  - SSH

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE