February 2015

Perfect Forward Secrecy

Introduction

1. Perfect Forward Secrecy (PFS) is a security feature which can improve the protection of information transmitted across the internet using public key cryptography. PFS can be enabled within a number of cryptographic protocols, such as SSL/TLS or IPSec. When PFS is used correctly, it guarantees that compromise of a private key will not result in the compromise of previous session data – all historical sessions will remain confidential.
2. This document is intended for agency staff considering deploying PFS within their environment.

Advantages of Perfect Forward Secrecy

3. In general, PFS refers to the protocol by which session keys are generated. PFS key agreement protocols typically exhibit three common properties, session keys which are ephemeral, non-deterministic and are not transmitted across the network, even in encrypted form. These three properties limit the loss of confidentiality to a single session if a session key is compromised, and to only future traffic if a private key is compromised.
4. This contrasts with other key agreement schemes, where compromise of a long-term key may result in the compromise of both past and future session keys.

Considerations when implementing Perfect Forward Secrecy

5. While PFS does bring significant security enhancements there are some implementation details which should be considered prior to implementation.
    a. **Client lack of support:** Some clients may not support PFS. When the client does not support PFS, the server can be configured to fall back to other methods of key establishment. If organisations wish to ensure that PFS is used they must also be able to control the client configuration.
    b. **Increased processing load:** Most protocols which implement PFS require a larger computational overhead. Agencies should perform load testing of their environment to ensure equipment can handle the increased workload.

Implementing Perfect Forward Secrecy

6. To enable PFS, the web server or other software must be configured to use ephemeral Diffie-Hellman or ephemeral elliptic curve Diffie-Hellman for key agreement.
7. Information about implementation of PFS on the two most commonly used web servers, Microsoft IIS and Apache, can be found at the following links:

a. Microsoft IIS: http://blogs.technet.com/b/erezs_iis_blog/archive/2013/08/22/perfect-secrecy-in-an-imperfect-world.aspx

b. Apache: https://community.qualys.com/blogs/securitylabs/2013/08/05/configuring-apache-nginx-and-openssl-for-forward-secrecy

Contact Details

8. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

9. Australian businesses or other private sector organisations seeking further information should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.