Executive Brief

Perfect Forward Secrecy: The Next Step in Data Security

With the ever-growing risk of security breaches, organizations need to evaluate the use of Forward Secrecy

Symantec™

Norton™ SECURED
powered by Symantec

This executive brief provides a concise explanation of the findings in "White Paper: An Experimental Study of TLS Forward Secrecy Deployment."

When it comes to security, IT leaders need to be thinking ahead. An eavesdropper who records traffic today may successfully decrypt it in the future, perhaps through a government request for a server's long-term private key or compromised key security. That avenue of attack joins long-standing criminal and other threats. A solution that protects data transactions against such dangers is **Forward Secrecy, which uses transient session keys that cannot be recovered**. The technique that currently seems most promising for this is called Perfect Forward Secrecy.

Unfortunately, a large survey of Internet sites reveals that the vast majority of Forward Secrecy implementations are misconfigured. That makes them less secure than approaches based on RSA, which is the industry's leading encryption system. However, a September 2013 study conducted by Stanford University and Carnegie Mellon University shows that **when Forward Secrecy is implemented using Elliptic Curve Cryptography (ECC), it is more secure than RSA algorithms and can actually improve performance**.

This performance advantage will grow greater in the future as longer RSA keys are implemented. Consequently, IT professionals should strongly consider Forward Secrecy and Elliptic Curve Cryptography, as implementing both together will increase security and boost the ability of servers to perform such tasks as delivering a web page in response to a user request.

Securing an Unsecure World

Public key encryption is an essential component of today's online world. As the basis for SSL (Secure Sockets Layer) encryption, it safeguards username and password credentials, bank or credit card information, and other sensitive data. Businesses can be held financially liable if their customer information is compromised, and end consumers can face stolen identities and other material losses. Thus, for consumers and businesses, the security and performance of encryption is critical. Satisfying those needs is one reason why, in 2014, Yahoo! started using a 2048-bit key and implemented SSL for information moving between data centers, as well as to and from users.

However, what's safe today may not be so tomorrow. An eavesdropper could record all current traffic with the hopes of cracking it in the future. **If keys are used for any length of time, the loss of current or even recent keys makes traffic accessible to cyber-criminals or cyber-terrorists.** They know this, which is why they continue to try to steal keys.

More powerful computers or better algorithms could make this possible. So, too, could social engineering that snags an old encryption key, which could then be used to decrypt recorded messages.

Also, there are reports, most famously by Edward Snowden in his disclosures about the PRISM program and other NSA efforts, that governments seek to decipher user messages on the most popular sites. Governments at some point in the future could compel a business to surrender encryption keys, thereby opening up recorded messages to inspection.

Perfect Forward Secrecy helps to address these security concerns by encrypting messages using **a random, transient key that cannot be recovered or produced to unlock encrypted data**. By its nature, ECC can yield stronger encryption and, studies have shown, better Forward Secrecy performance than RSA-based implementations.

An Unsettling Survey

When it comes to Forward Secrecy, Stanford University and Carnegie Mellon University's September 2013 survey of the top million global sites contained both good news and bad.

The good news: Nearly 50% of the sites support at least one of two ephemeral key exchange methods. That is, the sites have deployed either Diffie-Hellman key exchange (DHE) or Elliptic Curve Diffie-Hellman key exchange (ECDHE), or both. Since these both enable the use of temporary keys, their presence indicates the sites could support Perfect Forward Secrecy.

The bad news: The same survey revealed that most of these sites are misconfigured. Many, for instance, used DHE ciphers that are weaker, and therefore less secure, than those offered by RSA, the leading alternative. The reasons for this could be due to unfamiliarity with Forward Secrecy and what it takes to implement it. For example, in the case of DHE, servers are free to choose the key strength for a session, but unfortunately, some opt for relatively easily broken encryption.

Support for the idea that servers are misconfigured out of the box is found in the ECDHE results. **In all cases, the Elliptic Curve-based solutions were secure.** For ECDHE, the smallest key size found to be supported is far stronger than 2048-bit key length RSA. In part, this could be a consequence of Elliptic Curve Cryptography being roughly 10,000 times harder to crack than the better known RSA.

RSA may be the most popular cryptosystem because it was the only one that has been available for decades. Now there are alternatives. For instance, Symantec now offers ECC certificates for no charge with the purchase of SSL products.

The Right Solution

The Stanford-CMU team also tested the performance of various encryption methods in four configurations:

1. RSA key exchange with RSA signatures;
2. DHE key exchange with RSA signatures;
3. ECDHE key exchange with RSA signatures; and
4. ECDHE key exchange with an Elliptic Curve Digital Signature Algorithm, or ECDHE-ECDSA.

The researchers used these four techniques to gauge server response to various tasks, such as fetching simple, complex and multi-domain web pages. **In all cases, the all-Elliptic-Curve approach gave the best performance.** For instance, it topped out at 405 requests per second for simple pages — far better than the all-RSA approach, which peaked at 265.

These results mean that Forward Secrecy can be even better than free: ECC can actually increase website performance by increasing load capacity and reducing response times at the same time that it improves security.

What's more, that performance edge will grow as the trend toward longer RSA public keys — which create a greater computing burden — continues. Because Elliptic Curve techniques are cryptographically more secure, there is less of a need to make the key length longer. Thus, as time goes by, ECDHE-based methods will be increasingly attractive from a performance perspective.

The Next Steps

To take advantage of these security and performance benefits and defend against today's array of cyber-threats, Google, Twitter and other top sites have already implemented Perfect Forward Secrecy. Indeed, security experts have called for all sites to begin evaluating how to do so. The Online Trust Alliance (OTA) recommends websites be protected by always on SSL (AOSSL) — a practice that uses SSL and its successor, Transport Layer Security, across an entire site to protect users at all times during their visits. The OTA periodically raises the bar of what's needed to get on its honor roll, and in 2014, that requires beginning trials of ECC and Perfect Forward Secrecy.

As a further step toward security, **sites should disable insecure methods of connection**. The use of automated testing sites, such as the one from Qualys SSL Labs, can help pinpoint implementation problems and ensure the best possible security.

Given all the advantages, IT professionals should strongly consider deploying ECC and Perfect Forward Secrecy. Doing so will increase security, particularly against future threats, and can even boost performance. When implemented together, these technologies will allow users a faster, more secure, and likely better online experience.

More Information

Visit our website
http://www.symantec.com/ssl

To speak with a Product Specialist in the U.S.
1-866-893-6565 or 1-520-477-3111

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 21,500 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

Symantec™

Norton™ SECURED
powered by Symantec