The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- What is Encryption?
- Encrypting Stored Information
- Encrypting Information In Transit
- Best Practices and Caveats

Understanding Encryption

GUEST EDITOR

Fred Kerby is the guest editor for this issue of OUCH! He recently retired from the Naval Surface Warfare Center Dahlgren Division where he served as the information assurance manager for the past 16 years. Fred is a senior instructor with the SANS Institute.

WHAT IS ENCRYPTION?

Encryption is a mechanism that protects your valuable information, such as your documents, pictures, or online transactions, from unwanted people accessing or changing it. Encryption works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). The cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication mechanisms, such as passwords, tokens, or biometrics (like your fingerprint).

ENCRYPTING STORED INFORMATION

Sensitive information, including medical, financial, or business records, may reside on your mobile devices, such as your laptop, USB stick, smartphone, or tablet. These devices are easily lost or stolen, and if not encrypted, their contents can be read by anyone who has access to them. One of the best ways to protect data on a mobile device is to encrypt it.

In general, there are three ways to encrypt data stored on your mobile devices. You can encrypt specific files, encrypt entire folders, or encrypt the entire hard drive. Most operating systems support one, if not all three, options. Encrypting your entire disk, commonly called full disk encryption (FDE), is often considered the most secure. FDE encrypts all data on your hard drive, including any temporary files. It also simplifies the process as you do not have to decide what to encrypt and not to encrypt. If you cannot encrypt your entire hard drive, encrypt any files or folders that contain sensitive information.

Mobile devices, such as USB thumb drives, may come with encryption capabilities built into them, or you can encrypt them by installing additional software on your computer. Smartphones and tablets may have encryption capabilities built into them as well. Otherwise, you will have to install

Understanding Encryption

encryption apps; consult your phone vendor's app store or marketplace for information on what's available.

ENCRYPTING INFORMATION IN TRANSIT

Information is also vulnerable when it's in transit. If the data is not encrypted, it can be monitored and captured online. This is why you want to ensure that any sensitive online communications, such as online banking, sending e-mails, or perhaps even accessing your Facebook account, are encrypted. The most common type of online encryption is HTTPS, or connecting to secured websites. This means the traffic between your browser and the website is encrypted. Look for https:// in the URL or the lock icon in your browser. Many sites support this by default (such as Google Apps), and websites like Facebook and Twitter give you the option in your account settings to force HTTPS. In addition, when you connect to a public Wi-Fi network, use an encrypted network whenever possible. WPA2 is currently one of the strongest encryption mechanisms and the type you should choose. Finally, whenever sending or receiving e-mail, make sure your email client is set up to use encrypted channels. One of the most commonly used is SSL (Secure Socket Layer); many e-mail clients use SSL by default.

BEST PRACTICES AND CAVEATS

Regardless of which type of encryption you are using or how you use it, almost all forms of encryption share some common issues you need to be aware of.

Encryption is an important tool for protecting data, but is only effective if you have strong passwords and maintain the overall security of your computer .

- Your encryption is only as strong as your keys. If your key is compromised, so is your data. If you are using passwords to protect your keys, make sure you use strong passwords and protect them well. (See the May 2011 edition of OUCH! on passwords).

- Don't lose or lose access to your keys. If you lose your encryption keys or can't access them because you've forgotten the password that protects them, you most likely cannot recover your data.

- Your encryption is only as strong as the security of your computer. If your computer is infected, the bad guys can compromise your encryption.

Understanding Encryption

- Maintain the overall security of your computer.

Encryption does nothing to protect against viruses, worms, Trojans, unpatched vulnerabilities, or social engineering attacks.

- Always be sure to back up any confidential data securely. This ensures that if you lose your device or your encryption keys protecting your data, you can still recover your data.

- Use encryption based on publicly known algorithms, such as AES (Advanced Encryption Standard) or Blowfish, rather than proprietary algorithms. Also, always be sure you are using the latest version of your encryption programs.

- Consult an IT professional if you need help.

Incorrectly installing, configuring, or using encryption can render your information permanently inaccessible.

RESOURCES

Some of the links shown below have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Full Disk Encryption Tools:

TrueCrypt: http://www.truecrypt.org/

PGP: http://www.pgp.com

Windows 7 Bitlocker: http://preview.tinyurl.com/3xaubbr

File and Folder Encryption:

TrueCrypt: http://www.truecrypt.org/

Windows: http://preview.tinyurl.com/yb29rzn

Mac: http://preview.tinyurl.com/6c2q3cy

USB Encryption

TrueCrypt: http://www.truecrypt.org/

SanDisk: http://preview.tinyurl.com/3nl4g2p

IronKey: https://www.ironkey.com/products

Encryption Standards

AES: http://preview.tinyurl.com/ku33x

WiFi: WPA and WPA2 http://preview.tinyurl.com/am5oa

How HTTPS works: http://preview.tinyurl.com/ya9se7f

How VPN works: http://preview.tinyurl.com/rfc9f

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org