CommandHub
securing sensitive information

CommandHub White Paper

Protecting Sensitive Information in a Mobile World

By Daniel Townsend

April 2018

Executive Summary

As the Information Age morphed into the New Media Age, computing devices and how we used them changed dramatically. We transitioned from mainframes, to mini computers, and then personal computers. As computing devices became smaller and more powerful, the Mobile Age was ushered in with the introduction of laptops, tablets, and smart phones.

Our business and personal appetites for smaller, faster, more ubiquitous computing is growing at an exponential rate but so, too, are the dangers to the information we have on those devices.

Mobile devices now supplement, and often replace, personal computers. They are used to process, store, or transfer information that is often sensitive in nature. For instance:

- Mobile devices for personal use may include passwords, social security and credit card numbers, banking and other private information;
- Business users often store and process commercially confidential documents, such as contracts and proposals, right through to board-level material, and
- Mobile devices used by government personnel often contain sensitive or protected data, such as taxpayer information, transportation capabilities, operational security information and emergency preparedness plans.

A mobile device offers many benefits to the user, but along with those benefits come inherent risks. If the device is lost or stolen, the sensitive information is easily compromised. Additionally, when the device is used to transmit sensitive information via email or through a mobile browser, multiple vulnerabilities exist making the protection of the information suspect.

However, despite these radical changes to technology, the methods used to protect the sensitive information on our mobile devices have, by-and-large, remained the same as those used on personal computers.

Email is now the most prevalent means of electronic communication, yet the weaknesses and vulnerabilities that exist in email clearly demonstrate that it is not a safe means of sharing or transferring sensitive information.

Additionally, accessing data using web browsers or file sharing applications on mobile devices introduces further vulnerabilities that can be easily exploited in order to capture this sensitive information.

Cyber crime, malware pandemics, corporate theft and hacking (criminal and state sponsored) are at an all-time high, yet most people still rely on the manufacturers' built in security.

This white paper will describe the challenges that face us when trying to protect our sensitive information in a mobile world. While there are several common approaches that attempt to protect sensitive information - either by securing the data or by securing the endpoint - they do not provide a complete solution, and certainly not one that protects data at all times!

After illustrating the inherent security vulnerabilities, this paper will demonstrate that a holistic approach, using multiple layers of protection that goes beyond data and endpoint protection, must be employed. Most importantly, the data must be accessed through an interface that has a proven level of security to ensure that data is protected at rest, in transit, and while in use.

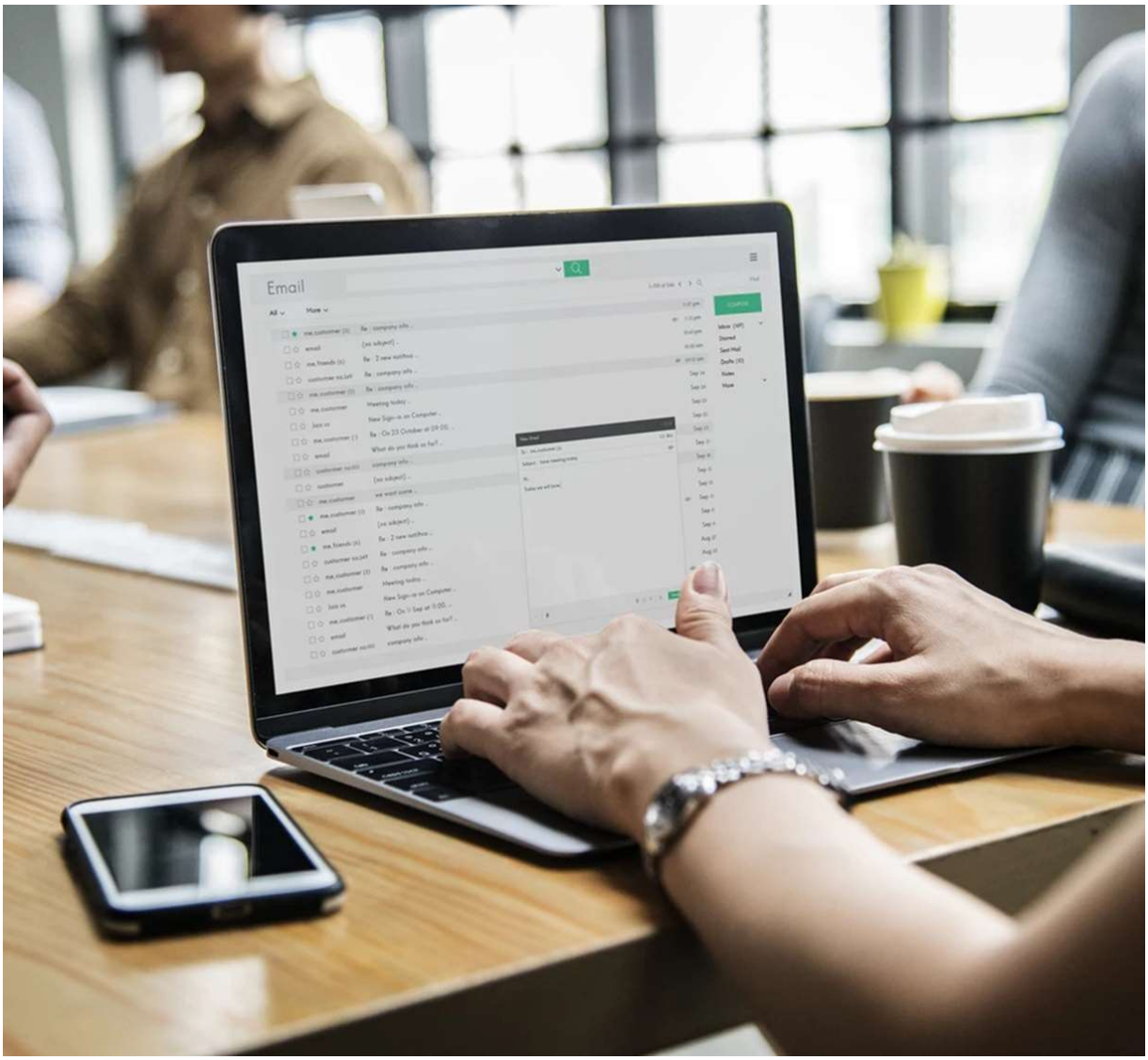
Finally, the paper offers CommandHub as a solution that addresses the vulnerabilities and provides the secure interface that is required to protect sensitive information in today's mobile world.

Business Communications via Email

Electronic mail (email) has revolutionized business communications, becoming a critical means of communication for corporations and governments. With its wide-spread adoption starting in the early 1980s, businesses and governments began to recognize the benefits of email and started to implement corporate email systems. The simple nature of creating and delivering email messages led to the rapid adoption - and eventual reliance - on email.

However, as businesses and governments began to rely on email as their primary means of communication, it became apparent that email did not provide the level of security and privacy required for the transmission of sensitive information.

According to a study published by the Radicati Group in March 2018, the total number of emails sent and received per day will exceed 281 billion in 2018 and is forecast to grow to over 333 billion by year end 2022[1].



1. The Radicati Group Inc., March 2018, http://www.radicati.com

Email Delivery

To understand the vulnerabilities that insecure email presents it is important to first understand the typical sequence of events for email delivery. The following figure illustrates this sequence:

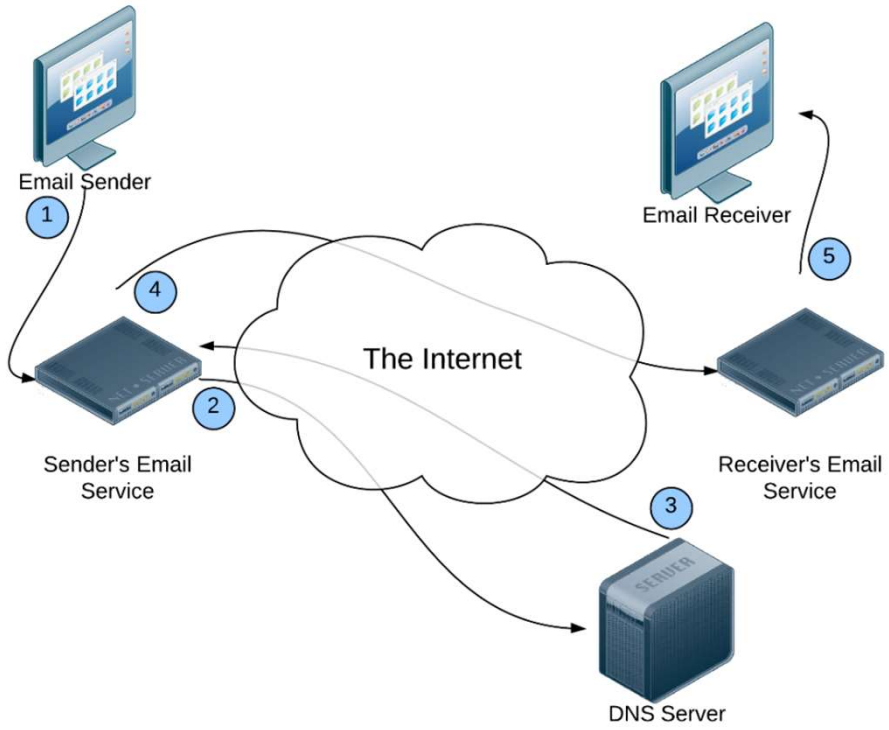


Figure 1: Email Delivery Process

Email systems use a store-and-forward technique during the email delivery process. As an email message is transmitted, a copy is stored at each server before being forwarded to the next destination. This storage of the email - as well as any email attachments - presents a significant risk of data compromise. Additionally, the email sender has no way of specifying when (or if) the email message is deleted from any of the computers along the email delivery path, so any information stored in the email may be discovered and compromised at any time in the future.

According to the latest data presented in the Symantec Shadow Data Report, 32% of emails and attachments are broadly shared throughout an organization, shared externally with contractors and partners, or shared with the public. Of these email messages, 9% contain sensitive data such as Personally Identifiable Information (PII), Payment Card Information (PCI) and Protect Health Information (PHI)[2]. Clearly, this volume of unsecured sensitive data presents a significant level of security concern for businesses and governments that are sharing information via email.

Another concern with email security is that email providers may store email messages and attachments for extended periods of time (or never delete your email from their email servers). As long as your email and attachments remain on the server of an email provider, your data can be compromised. Additionally, email providers will possibly data mine your email as it passes through their email services. These email providers capture and retain potentially sensitive information that is contained in your email, providing yet another avenue for data loss.

2. Symantec Corp., 2018, https://go.symantec.com/shadow-data

A Partial Solution: Secure the Data

A common solution currently employed to protect sensitive information in email is to attempt to secure the data itself using two primary methods – data encryption and secure connections.

Data Encryption

The two most commonly used types of email encryption are symmetric and asymmetric (also known as public key) encryption.

Using symmetric encryption, the email sender uses a unique key (a word, number, or unique string of characters) and applies it to the data to encrypt it. The same key is also used to decrypt the data. The simplicity of using a single key is also its weakness as anybody that has access to the key is able to decrypt the file. If the key is sent in an insecure manner (e.g. via email), then it could be intercepted and used to decrypt the data.

Asymmetric encryption addresses the weakness of symmetric encryption by incorporating two related keys for encryption and decryption. These two keys are known as a key pair (private key and public key). The private key is used to encrypt the data. This key is secret and only known to the person that encrypts the data. A public key is made freely available to anyone who needs to decrypt the information sent to them.

The strength of asymmetric encryption is that the encryption and decryption process require the use of both the private and public keys. Any data (text, files, or documents) that is encrypted by using the public key can only be decrypted by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

Unlike symmetric encryption, you don't have to worry about passing public keys over the Internet because these keys are intended to be public. Though asymmetric encryption is a secure method of protecting data, there are several roadblocks to its adoption. First, it requires the setup and configuration of complex secure email systems and technologies which increase the possibility that email encryption may not be configured correctly.

Then there is the second consideration, which is the ease of use for the end user. Asymmetric encryption adds additional overhead to email users by requiring them to take additional steps to secure their email. If the email users find the process too onerous, they are much more likely to bypass the encryption process and send unencrypted email. This is especially the case on mobile devices, further exacerbating the issue due to the explosion in the adoption of these devices for business usage.

Secure Connections

Yet another form of protecting data contained in email is by setting up a secure connection using Transport Layer Security (TLS). TLS uses encryption at the network connection level, creating a secure, private tunnel between the sender and receiver. The intent of a secure connection is to prevent eavesdropping or the tampering of messages that are sent on unsecured networks, such as the Internet. Since TLS is the primary method for securing a connection, it also presents a significant target as nefarious users make a concerted effort to discover vulnerabilities and exploit them. TLS has been cracked using attacks such as BEAST, BREACH, and RC4. In one example, a tool was developed that deceives users and web browsers into thinking that they are on a secure web site when, in fact, they are not. This tool is readily available on the Internet.

The multi-hop nature of email delivery also complicates the process and introduces unintended vulnerabilities.

A Partial Solution: Secure the Data

A secure connection is only effective if the secure connection exists for the entire length of the transmission, including each transfer from one server to another. If the secure connection is not maintained for one of the hops, the email is not secure and can be intercepted and viewed. For example, TLS interception proxies may be used to inspect contents of communications by inserting themselves in between the traffic flow of the sender and receiver of a TLS encrypted message. The interception proxy acts as a man in the middle (MITM), decrypting the message for analysis then encrypting it again before sending the message to the endpoint. Instead of a single point-to-point secure connection, the result is two separate secure sessions that are terminated in the middle where the data is readily accessible because it is no longer encrypted. This presents significant exposure vulnerability.

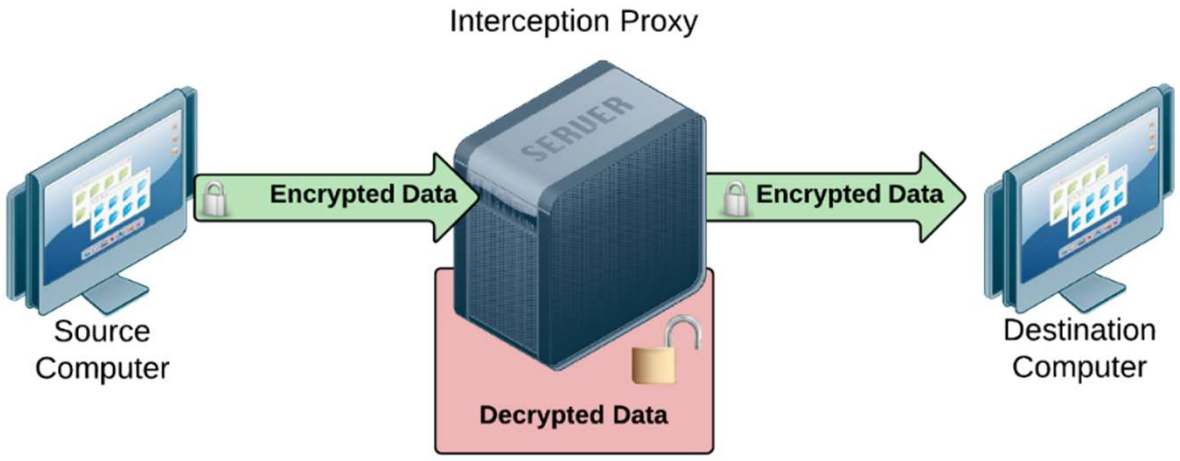


Figure 2: Interception Proxy Exposes Sensitive Information

Setting up TLS can also be complicated and therefore easily misconfigured. If the secure certificates or the secure connection is not properly configured, the initial connection becomes susceptible to attack. Secure connections do provide a layer of security, but they are still not the total solution for information security.

A Partial Solution: Secure the Endpoint

Another significant vulnerability present in the email sequence is the security of the endpoints used to write, deliver, and read email. These endpoints include laptop computers, smart phones, and tablets which increasingly include Bring Your Own Device (BYOD), thus presenting a challenging dilemma for any IT department. The proliferation of portable and mobile computing devices has led to their rapid adoption by businesses and governments and their numbers are expected to increase exponentially.

In recent years, mobile computing devices have seen huge growth. The mobile computing revolution began with the introduction of smartphones. By the end of 2010, smartphone shipments surpassed PC shipments (100 million versus 92 million)[3] and the pace hasn't slowed. According to a new forecast from the International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, worldwide smartphone shipments are expected to maintain positive growth through to 2021. IDC expects shipments to grow from 1.47 billion in 2016 to just over 1.7 billion in 2021[4].

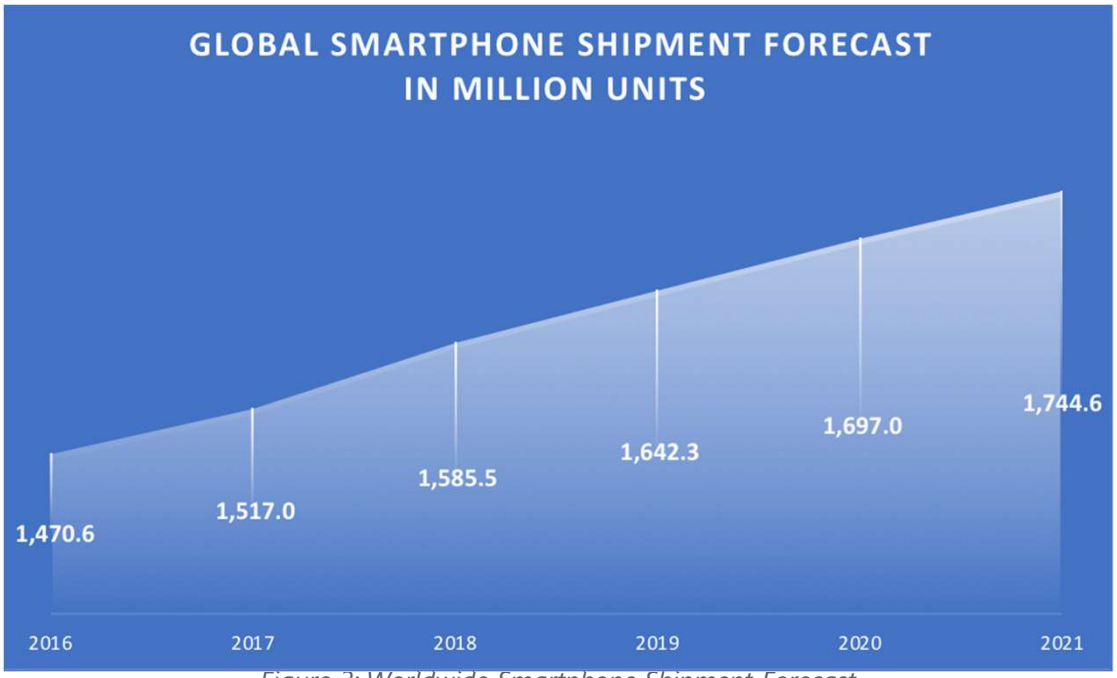


Figure 3: Worldwide Smartphone Shipment Forecast

As mobile computing grew, people started using their mobile devices to supplement their personal computers. In the beginning, mobile devices were most frequently used to consume content. But as the devices become more powerful, with more sophisticated software capabilities, they are now being used more frequently as content creation devices.

Additionally, email access from mobile devices is trending higher over the years. According to a report published by Litmus, just 17% of email messages are opened on a desktop, while webmail and mobile account for a combined 83%[5].

3. IDC Worldwide Quarterly Mobile Phone Tracker, January 2011, http://www.idc.com
4. IDC Worldwide Quarterly Mobile Phone Tracker, August 2017, http://www.idc.com
5. Litmus, January 2018, https://litmus.com

A Partial Solution: Secure the Endpoint

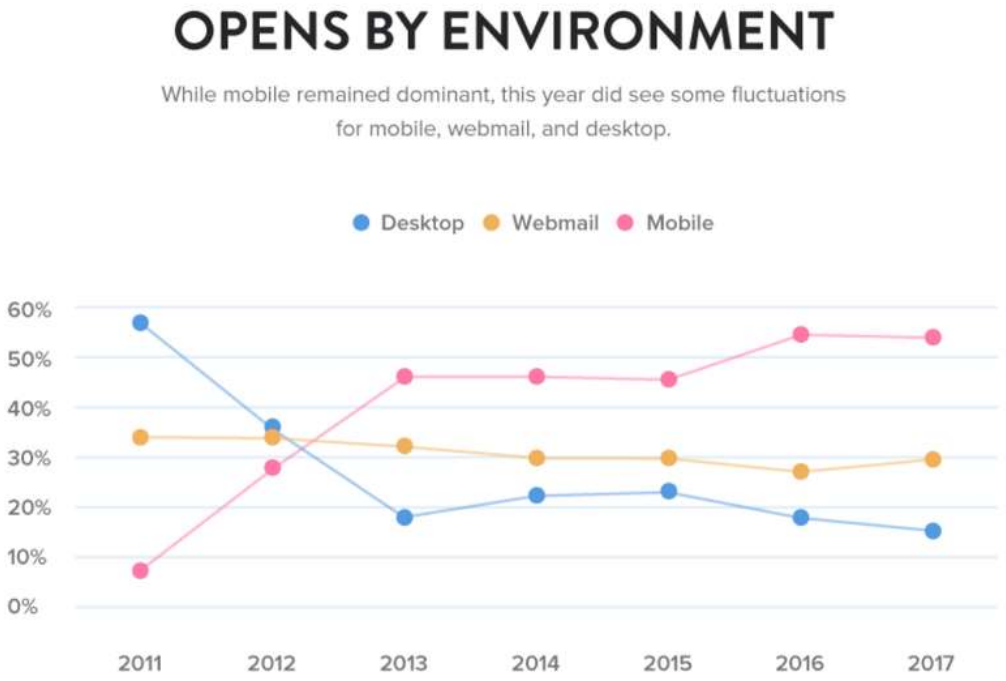


Figure 4: Percentage of Email Opened by Device

Mobile devices have security vulnerabilities and weaknesses that are unique to the platform such that the benefits of mobile devices also result in many of their security weaknesses.

Because they tend to be small and portable, physical device security has become a greater concern than it ever was for computer workstations. Let's face it, smartphones and tablets are easily left behind or stolen.

Additionally, the adoption of passcodes or other security authentication factors is still not prevalent with the majority of mobile device users. Despite the obvious security concerns, users have not adopted new processes to address these weaknesses and continue to follow the same methods they use on their personal computers.

The lack of device security was recently highlighted by Pew Research Center which, according to a survey conducted in 2016, found that 28% of smartphone owners have no lockscreen on their phone[6]. More concerning is that the most prevalent form of security for these devices is a simple passcode, which can quickly and easily be cracked.

Smartphone manufacturers are starting to take additional security measures to protect the sensitive information on their devices. In the case of the Apple iPad, the operating system (iOS) provides additional security features such as AES256 encryption and a remote wipe capability. However, these measures do not adequately secure the device from a determined attacker who, with a readily available Internet tool, can bypass the device's passcode so that the standard encryption key is accessible, and thus the contents can be revealed. The remote wipe can also be bypassed simply by turning off its cellular or wireless network access.

6. Pew Research Center, 2016, http://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-ownersdont-take-steps-to-secure-their-devices/ft_17-03-14_smartphonesecurity_access/

The Complete Solution: Secure the Process

Data security and endpoint security each have their place in the protection of sensitive information, but these forms of protection only address specific areas of concern and overlook the totality of information security. To truly secure sensitive information a holistic approach, that goes beyond data and endpoint protection, must be employed.

The solution is to take a multi-layered security approach that secures the entire process by protecting the data, the connection, and the endpoint in a single, secure, end-to-end solution. This ensures that the data is fully protected 'at rest, 'in transit, and while 'in use'.

Separate Sensitive Information from Email

The first step in securing the process is to separate sensitive information from email since, as discussed, email is not a secure solution for disseminating sensitive information.

To ensure that sensitive information is secured and protected, email should be supplemented by a solution that separates such material from the email. Sensitive data files should instead be sent via a highly secure process. Once the sensitive information has been separated from the email, it can be fully protected.

Protect Data at Rest

The foundation of protecting sensitive information is to protect it at rest. Whether the information is in the cloud or on a mobile device, it must be protected via data encryption and intrusion protection.

Data must be encrypted whenever it is stored, preferably using at least two layers of encryption. Multiple encryption layers ensure that if one encryption algorithm is compromised, the information remains protected by the extra layer/s of encryption.

Additionally, having two layers of encryption provides protection that is analogous to the "Two Person Concept" used by the United States military to protect against the accidental or malicious launch of nuclear weapons by a single individual. Using this process, two people must agree that an order to launch the nuclear weapon is valid by comparing the launch order to a previously sealed authentication code. The sealed authentication code is stored in a safe which has two separate locks. Each operator has the key to only one lock so neither one can open the safe alone.

Implementing double file encryption provides a similar level of protection by ensuring that two distinct keys must be used to decrypt the data.

Intrusion protection is provided by adding multiple layers of security between the user and the data. These barriers may include passwords, firewalls, and file permissions. The security barriers are monitored to track the attempted access of sensitive information. If the system detects an intrusion, additional layers of security are implemented to ensure that the data is not compromised.

Protect Data in Transit

Again, a multi-layered approach must be taken to fully protect data while in transit to ensure uninterrupted protection from point to point. In addition to a secure connection, such as TLS, an additional layer of security must be provided for protection from known TLS vulnerabilities. Data encryption should be used prior to transmission in order to provide this additional layer of protection, aligning with the principal of providing multiple encryption layers to secure data.

Transmitting data to and from a mobile device, as well as accessing the data while it's on the device, presents unique security challenges.

The Complete Solution: Secure the Process

As outlined above, the use of an email client for data transmission and access does not provide a sufficient level of security to protect sensitive information.

Web browsers provide a means for transmitting and accessing data, but there are so many vulnerabilities in a modern web browser that it makes a very poor data access and transmission choice.

Web browsers are ubiquitous, which makes them an extremely attractive target for criminal and state sponsored hackers. A common vulnerability often exploited by criminals is the browser plug-in. Browser plug-ins are a software component that add a specific feature, or set of functionality, to a web browser.

Examples of common browser plug-ins are Microsoft ActiveX, Sun Java, Adobe Flash, and Apple Quicktime. Browser plug-ins provide much of the expected functionality of a web site and are an increasingly popular method of attack.

Furthermore, when dealing with web browser security, users have the additional challenge of keeping their web browser current with the latest security patches and also keeping all of the browser plug-ins current.

By default, the address bar doesn't remain visible, so visual cues of site security, such as the lock for SSL enabled sites, are missing. Additionally, it is difficult, or impossible, to see a SSL certificate for a web site, so the user is unable to verify their secure connection and certificate.

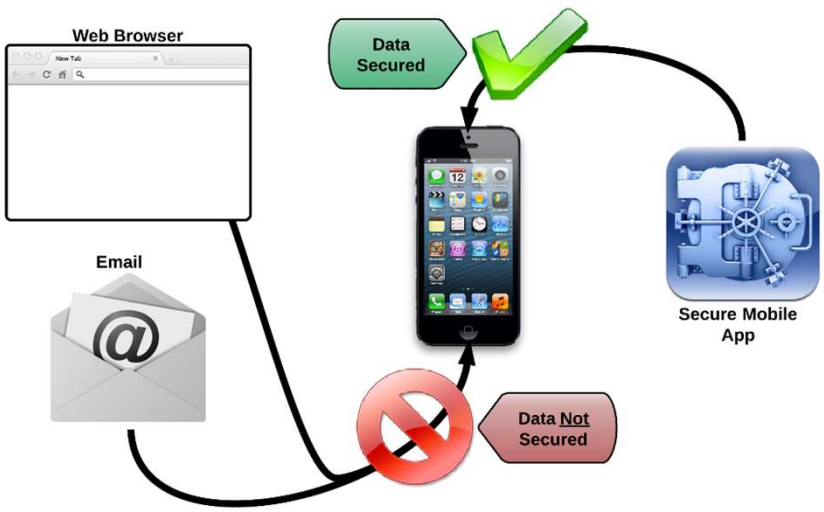
In one known data theft scenario that capitalized on such weaknesses, a compound threat - consisting of SMS text messages, email, and the mobile web browser - was used to launch an attack that silently recorded and stole data on the user's mobile device.

A critical yet often overlooked vulnerability existing when transmitting data is the point where the data transitions from the delivery agent to the device. Even when encrypted, the data is highly vulnerable at this transition point when using email clients, web browsers and file sharing applications.

In order to completely protect the data transmission process, a secure transition is necessary between the delivery agent and entry to or from the secure storage area on the device.

Such protection - not possible with email clients or web browsers - must be based on controlled layers of security that can then be used to compartmentalize sensitive information and fully protect the end-to-end transmission.

Figure 5: Secure Data in Transit to Mobile Device



The Complete Solution: Secure the Process

Protect Data in Use

The third, and most overlooked form of data security, especially on mobile devices, is protection during use. By design, mobile devices have many features that are intended to improve performance and usability. The unfortunate side effect of this is that these design decisions have introduced many security vulnerabilities.

On the Apple iPad, as part of its memory management, unprotected copies of recently viewed information are cached in storage on the device. For example, if a user views information from a mobile web browser or opens a document and begins editing it, the information is cached to the internal storage on the device. The only way to ensure that such information is not cached on the device is to perform all editing functions in memory, thus bypassing the disk caching.

It is important to note that unless an application is specifically designed to work in memory any sensitive information that is viewed or edited from within that application may well be cached to the device. The only way to totally protect the information is to use an application designed to work only in memory - and not save unprotected information to the disk. Email clients, web browsers and file sharing applications do not provide protection from disk caching.

Ease of Use

When users become frustrated with the process they to look for alternatives and begin bypassing security solutions. For example, in an attempt to secure information, corporations and governments have set up security on their computer network environments with the intent of protecting sensitive files and information. While the protection of this information is extremely important, the side effect is that this level of protection often makes it difficult for people to access information and collaborate with other users.

Users then began to look for alternative methods of storing and accessing files, often turning to insecure online file sharing services. This results in the insecure transfer and storage of sensitive business and government information.

To avoid the continued use of unsecured browser delivery or email attachments, the solution must follow a process that is simple, efficient, and effective:

1. Simple: intuitive user interface that requires no training.
2. Efficient: sensitive files are shared quickly without adding any complexity to the process.
3. Effective: corporate IT support is not required; an office administrator, or other non-IT personnel, can manage and control the solution.

The solution also needs to have been developed from the ground up, with a foundation established on security, as opposed to adding security as an afterthought.

CommandHub:
Securing the Data by Securing the Process

The CommandHub® solution protects sensitive information by securing and protecting the process to meet the needs of its most discerning customers. The CommandHub system includes:

- A secure web-based document management solution;
- A mobile application that protects data on mobile devices with private, fully secure file storage, backup, and synchronization, and
- A private, fully secure file storage solution.

The CommandHub system offers the following benefits:

- Sensitive information removed from email, stored in a highly secured environment, and protected at rest using multiple layers of data encryption and multiple layers of intrusion protection;
- Protection that includes a password and encryption key with an automatic 'circuit breaker' that immediately prevents further access, plus 'poison-pill' wiping of the data after a specified number of password failures;
- Multi-encrypted data transmitted securely between the mobile device and a highly secured environment using a secure mobile app vault;
- Secure in-memory document annotation which eliminates exposure of the documents to the native unencrypted file system, and
- Simple, intuitive user interface that does not require time consuming end-user training.

About the Author

Daniel Townsend has over 25 years' experience in Information Technology including system administration, software engineering, cyber security, IT project management, and corporate level technology strategy and implementation. He has extensive experience in the government technology sector managing multi-million dollar software engineering and technology projects for the highest levels of the US Government, Department of Defense, and Intelligence communities. Daniel is a veteran of the United States Air Force serving many Agencies including the Presidential Airlift Group of the United States Air Force, the Defense Intelligence Agency, and the White House Communications Agency of the Defense Information Systems Agency.

About CommandHub

CommandHub has a dedicated team of highly experienced professionals encompassing business process assurance, cyber security and document management disciplines. The company has a 'blue chip' customer base that includes state and federal governments and major corporations around the world. It has trusted partners in Australia, Europe and the United States to provide the highest levels of customer assurance and support.

To learn more, please visit www.commandhub.com.

CommandHub
securing sensitive information