PreVeil

Protecting your data even when you're breached.

Your Data is Nobody's Business but Yours - Or So You Think

There's a false sense of privacy being felt by businesses and consumers using cloud-based services like Gmail and Dropbox to communicate about everything – from their personal relationships, to health information, to financials. Because these services are cloud-based and accessible by password, it's automatically assumed that the communications and files being shared are secure and private.

The reality is – they aren't. Users are consistently misled by marketing materials that list services as "secure" and user data as "encrypted" or "protected". The types of encryption used by these companies do not provide any privacy for a user's information. Cloud providers use encryption in transit (which protects data as it is sent from the user to the provider) and encryption at rest (in which the provider encrypts user data with a lock controlled by the provider). However, even with both of these types of encryption, the cloud provider retains the ability to access a user's information, making it more vulnerable to access by others, too.

While these companies don't necessarily tell you they can read your data, their Terms of Service make this clear. They access it in order to sell advertising or to provide additional services to consumers or businesses. For example, a series of 2014 federal and state privacy lawsuits led Google to finally update their Terms of Service, clearly acknowledging that they read your content (including emails). Most users simply don't realize they are making this privacy and security trade-off.

Cloud-Based Services Are Riskier Than Ever Before

Almost half of all IT services are being delivered by the cloud. As the cloud gets bigger, it becomes a larger and more attractive target – especially as companies capture and store important data there.

Because of this, cloud providers are increasingly becoming the central point of attack for hackers. By targeting cloud service providers, hackers are able to access data from multiple companies at once and carry out those attacks from anywhere in the world.

Even if you're not the intended target, if a service provider is breached, your data can be exposed. The vast majority of cloud-based services have this fundamental design vulnerability. Because these services can access user data, it's not possible to guarantee that the data can't be seen by an attacker as well. Using any cloud-based service that doesn't have the right tools in place, such as end-to-end encryption, is **effectively like handing your phone to a complete stranger.**

Making Your Data Your Business – And Your Business Only

New encryption methods such as end-to-end encryption are one solution to protecting your data, ensuring that only the intended recipients are able to decrypt the business information you are sending. With end-to-end encryption, nobody else can read a user's information – not even the service provider.

Recent Breach Attempts Highlight the Inherent Weakness of Passwords

In the middle of July, private sector researchers revealed that they had detected a series of stealthy “slow and low” brute force credential-guessing efforts against a variety of organizational Microsoft Office 365 accounts. Probably using passwords harvested during other breaches, and assuming that their prospective victims had not changed them in the interim, the hackers sought to guess the associated usernames of senior employees at the affected organizations. During a period of approximately six months, the attackers conducted over 100,000 login attempts originating from 67 Internet Protocol addresses.

Although the researchers assessed that no accounts were compromised as a result of the aforementioned attacks, more recent reporting indicates that at least one notable Microsoft user did in fact suffer a breach around the same time. A little more than a week after the researchers announced their findings, hackers posted on the internet the files of an employee of the cybersecurity firm FireEye. In addition to his LinkedIn profile, the attackers appear to have gained access to the analyst’s personal Microsoft OneDrive account as well. Since he kept FireEye documents in this cloud storage service, the intruders were able to gain access to and publicly release these sensitive corporate materials.

If the breach of the FireEye employee’s accounts were related to the large scale Microsoft Office 365 credential-guessing efforts is not clear, due to the fact that the researchers of these brute force attempts anonymized the identities of the targets in their report. Whether or not the two incidents were connected, however, they both hammer home a key point: passwords themselves can be a cybersecurity Achilles’ heel.

The credential-guessers who sought to hijack Office 365 accounts almost certainly knew that more than 80% of people in one study admitted using the same password for more than one service. The hackers could thus rely on already-stolen login information to attempt to breach additional accounts. Furthermore, the fact that the FireEye employee suffered hacks of both his social media profile and OneDrive account simultaneously – along with the posting of his login credentials online by the intruders – strongly suggests that he used the same passwords for multiple platforms.

Since Microsoft is just beginning roll out two-factor authentication for Office 365 email clients, and rates of use for this security technique are probably at the single digit percentage levels, experts expect to see more breaches of Office 365 accounts in the future. This problem is also not unique to Microsoft, due to the similar login and authentication mechanisms that most major providers use.

The answer to this problem is to accept that passwords are an inherently flawed way to protect important data stored in the cloud. Fortunately, there is an alternative. PreVeil’s next generation email, file-sharing, and storage system – designed for security and ease of use – is now coming to market. It relies on extremely strong cryptographic keys stored locally on user devices, not easily guessed passwords, to facilitate user access to encrypted information in the cloud. Tools like this likely could have prevented the breach suffered by the FireEye employee, and would make enterprise networks essentially impervious to brute force login attacks.

These tools will be incredibly effective in protecting data – but only if they are actually used. In fact, 45 percent of IT personnel knowingly circumvent their own security policies. So, the encryption strategies and tools used to protect information must allow for “no exceptions”—e.g., providing no risk that IT personnel can expose their enterprises to attacks. It helps, too, if knowledge workers are able to encrypt their emails very easily, with little to no learning curve involved.

Encryption methods are most effective when used in conjunction with well-aligned internal policies. Decentralize access to data when possible, minimize or eliminate accounts with privileged access, and carefully consider the risks when deciding to share data or use SaaS services.

In doing so, companies and consumers alike can be empowered to ensure that their data is their business – and their business only.

Cloud Services Are Vulnerable Without End-to-End Encryption

The growth of cloud services has been one of the most disruptive phenomena of the Internet era. However, even the most popular cloud services (including Yahoo, Gmail, Microsoft Outlook 365, and Dropbox) are vulnerable to attack because their servers operate on unencrypted data.

The move to cloud-based services offers enormous benefits compared with managing these services in-house. The cloud is scalable, cost-effective, easy to manage, and accessible to a wide range of devices anywhere.

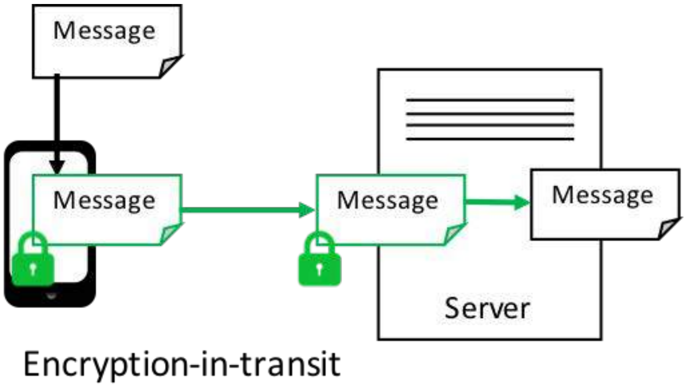
But because cloud services represent a centralized repository of information, they are tempting targets for attackers. If an attacker is successful in breaching a single user's computer or phone, that user's information will be compromised. But if an attack targeting a server is successful, information for all users on that server can be leaked. For example, Yahoo recently disclosed that over a billion user accounts were compromised.

Accordingly, the security industry has invested heavily in technologies and processes to protect cloud servers. Many of these – such as firewalls, threat detection and analysis, and administrative processes – amount to "building taller walls" around the server. But despite great effort and investment, attackers continue to prevail.

Assume the server is breached

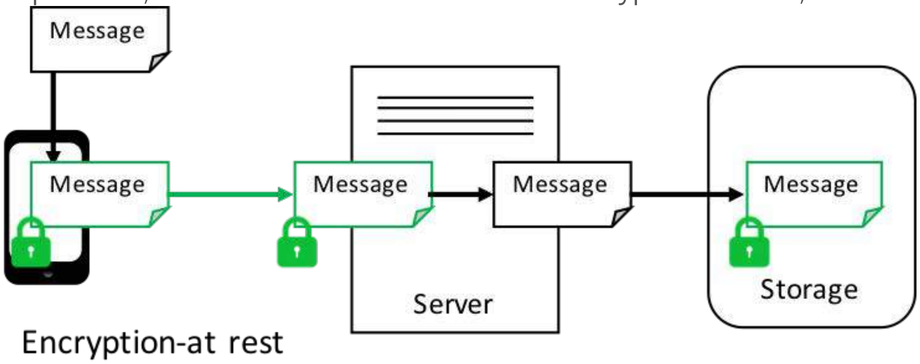
What if the problem is turned around? Instead of figuring out how to protect the server, what if the focus is on protecting the data whether or not the server has been compromised? This can be achieved with **end-to-end encryption**, which means user data is decrypted only on computers or phones; never on the server. Therefore, if the server is breached an attacker will only be able to access encrypted data, which is unintelligible. Unfortunately, end-to-end encryption is rarely used.

Many cloud providers tout their use of encryption for security, but the term "encryption" can mean many things. Most services use something called -encryption-in-transit. To show how this works, we'll consider a generic cloud-based email service.



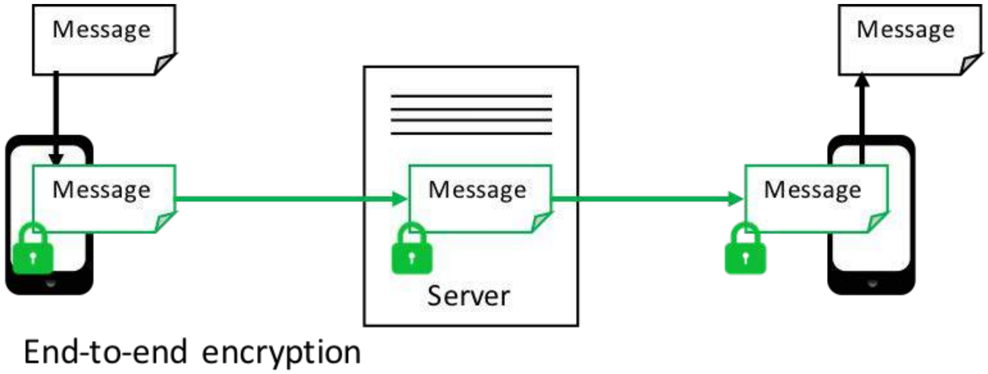
As shown in the diagram here, encryption in transit uses encryption to secure a message when it is being transmitted from a phone or computer to a server, often using technologies like SSL (Secure Sockets Layer) or TLS (Transport Layer Security). This prevents an attacker from watching Internet traffic and gleaning the contents of communication. The decrypted message is available at both the device and the server. This makes the server vulnerable to attack, because a successful breach of the server gives the attacker access to all the decrypted messages.

In attempt to address this problem, some cloud services also use encryption-at-rest, as shown below:



Encryption-at-rest means that data is encrypted in the storage media on cloud servers when not being used. Encryption-at-rest could prevent an attacker from accessing information on physical disks that were stolen from a data center — although such physical attacks are exceedingly rare. Encryption at rest still cannot prevent an attack on the server from leaking valuable user data because the server can still "see" the decrypted information. If the server can access the raw data, so can an attacker.

End-to-end encryption can solve the problem by adding the missing link – encryption-in-use – as shown below:



With end-to-end encryption, the server never has access to decrypted data. The message is encrypted in the device of the sender, and it's not decrypted until it reaches the device of the recipient. Thus, a server attack will not compromise any user information. An attacker may attempt to breach a single user's device, but such an attack affects only that user – not everyone on the system.

What about Gmail, Outlook 365, and Dropbox?

Unfortunately, most major cloud service providers do not use end-to-end encryption – including Gmail, Outlook, Dropbox, Yahoo, and many others. This is because these services rely on servers to process emails and files. The servers absolutely must have access to user data.

PreVeil

PreVeil takes a different approach – basically not trusting the cloud. It uses end-to-end encryption that provides encryption in-transit, in-use, and at rest. The cloud server simply does not have access to unencrypted data so information is protected even when the cloud is breached. Most important of all, PreVeil Email is designed to be very easy to use.   It can work with popular mail programs like Microsoft Outlook and Apple Mail, through a browser on a computer, or with an app for iPhone and iPad. Users are identified by their regular email address; no special email or domain is required.

PREVEIL

Protecting your data even when it's breached.

Born out of research at MIT, PreVeil takes a unique approach to protecting sensitive business data. Whereas traditional cyber defense techniques strive to build taller "walls" around servers to prevent attackers from getting in, PreVeil is designed to protect data even when the "walls" are breached. PreVeil Drive enables users to easily store, sync and share files while protecting the data with end-to-end encryption. PreVeil Email protects emails with end-to-end encryption, with seamless integration into Outlook, Mac Mail and mobile devices.

Learn more about PreVeil. Contact us at sales@preveil.com or call us on 857-957-0345