Understanding the Critical Ramifications of Apple's Impending iOS VPN Changes

M@D mobile active defense
The Smartphone Security Company

www.mobileactivedefense.com

Introduction

Apple's release of the first iPhone only a few years ago was the catalyst for an epic paradigm shift in technology which has affected the way people live, play and work. The risk of attack to mobile devices now grows every day as billions of 'always on', Internet connected devices have become the centerpiece of users' productivity and increasingly contain and transmit valuable confidential data as they connect to corporate networks. Hacktivists, nation state actors, organized crime rings and identity thieves have set their sights on attacking this vast new treasure trove of data and money.

Organizations concerned about security have attempted to treat mobile devices as 'another end point', although each mobile operating system has unique nuances of how it can be networked and secured. However, every organization (enterprise customers, ISV's, mobile carriers, etc.), which is a part of this new global mobile economy/ecosystem, is dependent on mobile operating system manufacturers like Apple, Google and Microsoft to provide adequate features and tools to securely deploy and utilize mobile devices. To a great extent, we are all at the mobile OS manufacturers' mercy.

A few years ago Android's Gingerbread Operating system contained very few enterprise APIs and had sparse Virtual Private Network (VPN) options while Apple's iOS device users enjoyed many enterprise ready APIs and the ability to use enterprise grade security without extreme modifications. Android users simply had to accept these conditions. Within the last year Android with the help of hardware providers like Samsung with Samsung SAFE has achieved the same if not a better level of enterprise usefulness as iOS. This underscores both the speed at which mobile is changing, and the reliance enterprises have on the operating system and device manufacturers.

This paper will discuss how a forthcoming change in Apple's iOS operating system will have a major impact on the usability and security of iOS devices worldwide and how to best prepare for this change.

Executive Summary

The only secure way to fully protect data in motion on mobile devices is through an IPSec VPN. Other forms of data transfer like SSL VPN exist but each have well documented security flaws. The ability to do and utilize IPSec VPN on iOS has been available for the most part from the creation of the iPhone, with Android just starting to provide more support for this functionality with its latest OS versions in the last year. Further, the most secure way of deploying such a technology is to take the control out of the hands of the user, and automate it – even better if the user cannot turn it off. This now guarantees data is being transferred securely from the mobile device to the network and that the user cannot change that. It also provides for a long list of security functionality and benefits which we will not delve into in this particular paper.

The industry calls this 'On Demand VPN' – and for the more secure environments, if architected properly this provides the same level of network security for mobile devices as one would expect at a workstation in the office to include things like content filtering and an administrative firewall, etc. (the list of security benefits is long). Many organizations in the public and private sector enjoy this type of secure mobile solution today and others strive for it, however On Demand VPN is also used by companies just wanting to secure specific data as it relates their company, and are less interested in securing all data.

Either way, this is very much a network security related topic that is now relevant and needing thought, leadership and guidance for mobile. For the sake of this paper, we will focus on Apple's iOS, as this is a major change that has just been announced which will affect enterprise and government users of iPhone and iPads worldwide with the next iOS update.

Apple disclosed, the week of April 1, 2013, that the company will be changing the behavior of the VPN On Demand feature on iOS devices (running iOS 6.1 or later) through a software update to be released later in the same month. These changes are due to a judgment against Apple late last year and a lost appeal this year in a patent lawsuit brought by a company called VirnetX.

Further details are outlined by the support page dedicated to this change on the Apple website. In short, if you are currently using an iOS device that automatically connects the VPN when you use it – be it all the time or just when you access the company network in some form –this change will directly affect you and your company. Apple is suggesting they will address this functionality with alternatives in a future software update.

Apple and pundits will have you believe this is simply a matter of inconvenience in now needing to have the device user manually start the VPN (which it is, and for many employees is enough of an issue in itself) – however this also poses a far more reaching issue for organizations that choose the secure approach of sending all traffic over the VPN, placing them in a position where the user can disable this at any time. This could turn off content filtering, and a list of other important security features.

The remainder of this paper will delve into the operational and technical impact this will have for organizations.

Operational Impact Analysis

Should Apple in fact remove the On Demand VPN functionality for iOS with the next update offered, it will affect a large percentage of companies with employees using iPhones and iPads worldwide that install this update. Without certain considerations and counter measures put into place prior, as outlined in the technical impact analysis below, a large number of corporate users will immediately lose the ability to automatically connect with their corporate network.

From an operations perspective, considerations around securing these devices going forward, need to be identified. These considerations include, but are not limited to, informing employees immediately of changes that will affect their daily use of Apple devices and what kind of network access will be permitted using these devices going forward, given this new risk must be taken into consideration.

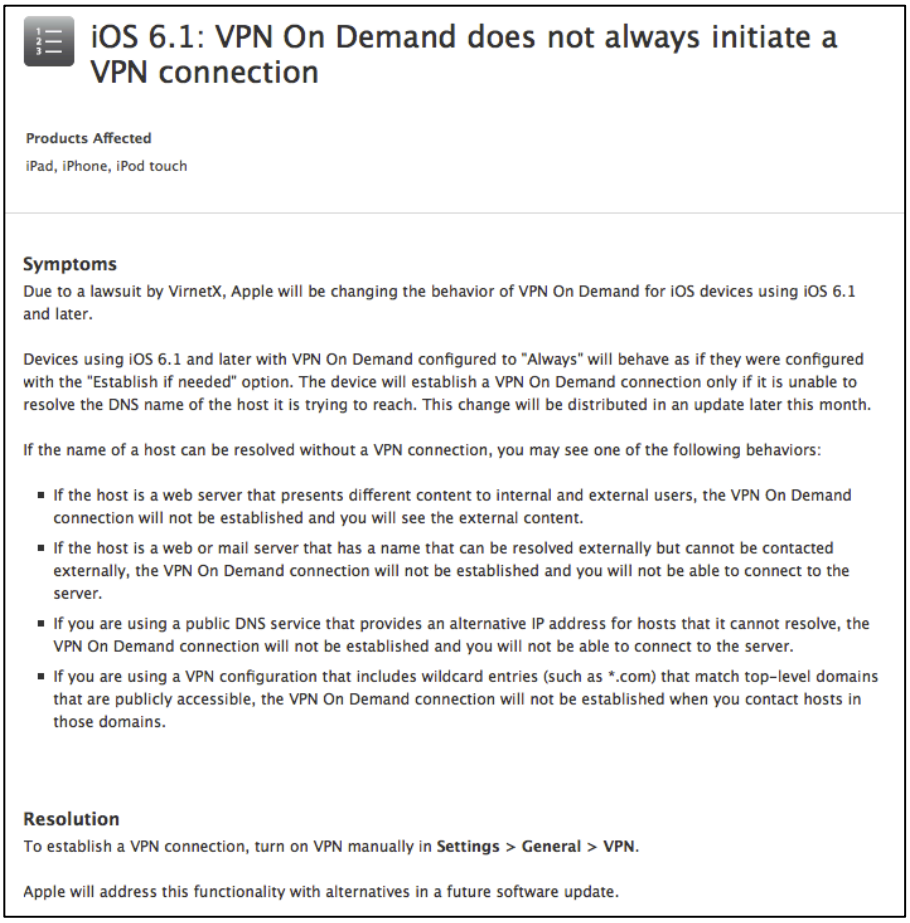
Organizations must also note that this is not the first such disruption caused by Apple that effects the enterprise and won't be the last. The industry term of consumerization, by its very meaning, suggests that mobile devices like iOS and Android are not built for enterprises, thus their creators will go to far lesser lengths when faced by roadblocks either monetary or otherwise to protect that user base from possible major disruption.

This may be as simple as an organization accepting the risk until Apple comes up with a better idea and having employees manually turn the VPN on and off manually, as in the figure to the right.

But more than likely both the technology and security divisions of companies will want to either somehow alter how much access iOS devices will enjoy until this all gets resolved or change how they interact with the network and accept more risk but continue to allow connectivity as outlined in the technical impact analysis.

Technical Impact Analysis

This paper is being written directly in response to the following support announcement by Apple (http://support.apple.com/kb/TS4550). It is important to note that certain assumptions are being made based on the below Apple announcement and will be updated accordingly should further details be made available.



iOS 6.1: VPN On Demand does not always initiate a VPN connection

Products Affected

iPad, iPhone, iPod touch

Symptoms

Due to a lawsuit by VirnetX, Apple will be changing the behavior of VPN On Demand for iOS devices using iOS 6.1 and later.

Devices using iOS 6.1 and later with VPN On Demand configured to "Always" will behave as if they were configured with the "Establish if needed" option. The device will establish a VPN On Demand connection only if it is unable to resolve the DNS name of the host it is trying to reach. This change will be distributed in an update later this month.

If the name of a host can be resolved without a VPN connection, you may see one of the following behaviors:

- If the host is a web server that presents different content to internal and external users, the VPN On Demand connection will not be established and you will see the external content.
- If the host is a web or mail server that has a name that can be resolved externally but cannot be contacted externally, the VPN On Demand connection will not be established and you will not be able to connect to the server.
- If you are using a public DNS service that provides an alternative IP address for hosts that it cannot resolve, the VPN On Demand connection will not be established and you will not be able to connect to the server.
- If you are using a VPN configuration that includes wildcard entries (such as *.com) that match top-level domains that are publicly accessible, the VPN On Demand connection will not be established when you contact hosts in those domains.

Resolution

To establish a VPN connection, turn on VPN manually in **Settings > General > VPN**.

Apple will address this functionality with alternatives in a future software update.

In short, by switching from 'On Demand' to 'establish if needed' will be required according to the above support page – the iOS VPN will only automatically turn on if it is unable to resolve the DNS name of the host it is trying to reach. There are 3 distinct issues that can be taken away from the above support announcement.

a) Severe issues for organizations wishing to send all traffic over the VPN to a central location or server.
b) Less or no issues in a BYOD type scenario when only IP traffic destined for internal networks needs to be sent over the VPN.
c) The user to have to manually turn the VPN on when they want to use it and login to individual resources based on that VPN session each time.

At first view this causes several issues to VPN users only until you look further into the situation. In regards to point 'a', it is fairly accurate based on this bullet in the support document.

> 'If you are using a VPN configuration that includes wildcard entries (such as *.com) that match top-level domains that are publicly accessible, the VPN On Demand connection will not be established when you contact hosts in those domains.'

This behavior without other engineering will make things like content filtering, server based DLP and most security not possible. The primary reason for this is that in this scenario an organization wants the VPN to turn on every time the user touches the Internet – however any time the user goes to a publically available domain, the VPN connection will not be established. This is a very serious issue for companies requiring real security for their iOS devices.

Point 'b', as it turns out, is more than likely both false and a real issue for many companies simply using an MDM for their mobile management. As stated by Apple:

- If the host is a web server that presents different content to internal and external users, the VPN On Demand connection will not be established and you will see the external content.
- If the host is a web or mail server that has a name that can be resolved externally but cannot be contacted externally, the VPN On Demand connection will not be established and you will not be able to connect to the server.
- If you are using a public DNS service that provides an alternative IP address for hosts that it cannot resolve, the VPN On Demand connection will not be established and you will not be able to connect to the server.

What this means is that if an organization is using an MDM and was using On Demand VPN on iOS only to access internal company networks or for that matter is simply using a proxy – this will still fail with this new paradigm if any of those company domains are externally facing.

An example of this would be if the company's ActiveSync can be accessed from outside of the network, or if they are using OWA with Exchange, or if Exchange is externally facing or even if any network domains have any kind of resolvable addresses that are in the public domain.

If you access internet networks and have Exchange externally facing, no VPN connection will be made automatically– and as a side note, those types of architectures where such internal domains are readily accessible from the outside are not secure anyway.

This now leaves point 'c', or manually turning the VPN on and off. This is both not secure for enterprises as it leaves security to the hands of the user and is equally not practical, as those using iOS do so for the ease and convenience, both of which would be swiftly removed if there is a need to manually operate the VPN every time the user wanted to access company domains.

Solutions Impact Analysis

Mobile Active Defense (M@D) has published this timely White Paper in an effort to continually address the rapidly changing environment of the mobile workforce, as well as to educate and inform the vast user community of how these changes affect their daily use of such devices. As the most respected thought leaders in mobile security, it is incumbent upon us to make sure that not only our customers understand the facts, but that the wider user community understands, as well.

It is also important to note that organizations with secure mobile architectures are far less affected by changes in operating environments like Apple's most recent announcement. M@D is a trusted industry partner and mobile security/management security provider and we always try to educate and recommend strong secure mobile architectures to our customers.

The hallmark of M@D's solution is secure communications – and this means IPSec. On Demand VPN is far from the only key feature involved in this, but is indeed a key component. Therefore, upon Apple's disclosure of its intent to make this change, the impact was immediately assessed and addressed technically by the M@D team. All customers were contacted, alerted and advised as to this important change with Apple Devices.

It is also important to note that M@D customers have, prior to this change, more secure network security tied to their mobile architecture. Addressing the technical issues posed by this On Demand VPN change as listed on Page 4 of this White Paper:

> In short, by switching from 'On Demand' to 'establish if needed' as will be required according to the above support page – the iOS VPN will only automatically turn on if it is unable to resolve the DNS name of the host it is trying to reach. At first view this causes:
>
> a) Severe issues for organizations wishing to send all traffic over the VPN to a central location or server
> b) Less or no issues in a BYOD type scenario when only IP traffic destined for internal networks needs to be sent over the VPN.
> c) The user to have to manually turn the VPN on when they want to use it and login to individual resources based on that VPN session each time.

Although point 'a' should technically be true for M@D, given the ability to have all traffic traverse an On Demand VPN – this is not the case. Obviously the behavior of the solution is effected, however, the engineering team quickly pulled together a way to continue to have our customers enjoy full automated IPSec VPN service and continue to reap the benefits and security of knowing their mobile iOS devices still have content filtering, DLP and all of the other security provided by the solution. Our team is happy to discuss this in more detail, if requested.

Point 'b' simply is not an issue, as under our advisement, M@D customers do not have publically resolving IP or DNS addresses and all ActiveSync traffic is directed at the M@D MECS server. Thus customers utilizing split VPN functionality will not be affected. New customers and prospects are quickly being brought up to speed on best practices for a secure mobile network architecture in general – and more specifically how to make sure there are no issues with this On Demand VPN change and externally resolving addresses.

Point 'c' has not been considered for M@D customers' as it is counter to the mission of the company and security provided to the community.

If this change has affected your organization, or if you are concerned with protecting your company from future OS modifications, regardless of whether it is Apple, Google or Microsoft, please feel free to contact us so we can put you in touch with the M@D team, which consists of some of the finest engineers and thought leaders in mobile security today.

Conclusion

The impact of Apple's announced changes to the VPN security within iOS underscores the substantial risks that organizations face on a daily basis. The reliance on mobile devices and the manufacturers of operating systems to maintain security and integral features of a rapidly changing global economy is a huge risk for any organization. As vendors like Apple implement changes in their OS's which can dramatically impact the integrity of the underlying security of this powerful mobile ecosystem – it is incumbent upon security solution providers to be ready to rapidly assess and assimilate these changes, in order to advise customers and the industry at large about their potential impact.

Contact:

Eric S Green
Mobile Active Defense
T: 914 244 0160
egreen@mobileactivedefense.com