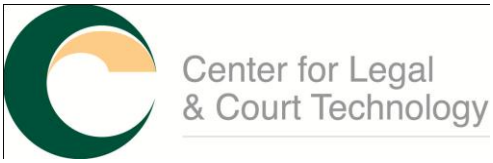
Apple TV for Trial Presentation

Limitations and Practical Use

Authored by: Manker, Concetta T



William & Mary Law School
P.O. Box 3050, Williamsburg, VA 23187
757-221-2494, FAX: 757-221-3708
www.legaltechcenter.net, clct@wm.edu

Apple TV for Trial Presentation

Limitations and Practical Use

Apple TV has proven to be a wonderful tool for home users to control their Apple components wirelessly; however, deploying Apple TV in a business, corporate or government environment is challenging but there are creative ways to still enjoy all the advantages of Apple TV.

Personal Computers or PCs have always enjoyed *PC sharing* and *PC mirroring* features, but with the recent popularity of the Apple iPad, this *old but new again* concept has re-entered the market through a feature called Apple Airplay. Airplay is wireless technology that is fully integrated to allow you to stream music from your iTunes library, photos, and videos wirelessly from your iPad, iPhone, iPod Touch or from any Mac and Windows PC to your Apple TV and Airplay enabled speakers (Apple, 2012).

Before businesses can enjoy this new-found freedom, there are some things that must be understood before upgrading everyone in the office with the latest iPads.

- **Only a limited number of products are currently Airplay-compatible:** Right now, only a handful of products offer Airplay compatibility and they tend to be rather expensive.

- **Video and photo streaming options are limited.** At the moment, Apple TV is the only product that allows you to stream video and photos to your TV from your iPhone, iPad, or iPod Touch.

Center for Legal & Court Technology

- **There are very few applications that support Airplay.** Currently, only a few applications (apps) are available to be viewed by Airplay. This is a big blow to the business world, which uses programs like PowerPoint for presentations.

- **WiFi is better than Bluetooth but it's still not perfect.** Airplay works over your Wi-Fi network and, as anyone who uses Wi-Fi knows, the connection is not always rock-solid.

…Bonjour challenge, wireless vendors….are developing hardware and fairly complex network configurations….

.

Challenges

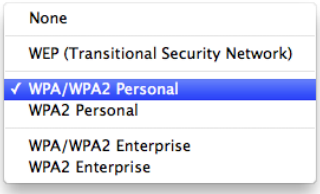
When incorporating Apple TV into your environment, you'll learn that Apple TV does not support enterprise security protocols. Apple has built this market niche on the extremely limited Bonjour protocol, which is non-routable and extremely difficult to scale and administer on large wireless networks. Users want to make use of these very slick living-room-oriented devices at work, as there are many potential uses. To meet the Bonjour challenge, wireless vendors like Aerohive, Aruba, and Cisco are developing hardware and fairly complex network configurations that may or may not be suitable for all network environments.

Security Protocols

WPA and WPA2 have two modes:

1. Personal mode, which relies on the capabilities of Temporal Key Integrity Protocol (TKIP) or AES-CCMP without requiring and authentication server, and

2. Enterprise mode, which uses a separate server, such as a Remote Authentication Dial-In User Service (RADIUS) server, for user authentication.



Wi-Fi Protected Access (WPA) and WPA2

WPA and WPA2 use specifications that bring together standards-based interoperable security mechanisms that significantly increase the level of data protection and access control for wireless LANs. WPA and WPA2 provide wireless LAN users a high-level assurance that their data remains protected and that only authorized network users can access the network. A wireless network that uses WPA or WPA2 requires all computers that access the wireless network to have WPA or WPA2 support. WPA provides a high level of data protection and (when used in Enterprise mode) requires user authentication (Apple, 2012).

TKIP provides enhanced data encryption by addressing the Wired Equivalent Privacy (WEP) encryption vulnerabilities, including the frequency with which keys are used to encrypt the wireless connection. Both 802.1X and Extensible Authentication Protocol (EAP) provide the ability to authenticate a user on the wireless network (Apple, 2012).

WPA and WPA2 Personal

For home or Small Office/Home Office (SOHO) networks, WPA and WPA2 operate in Personal mode, taking into account that the typical household or small office does not have an authentication server. Instead of authenticating with a RADIUS server, users manually enter a password to log onto the wireless network. When a user enters the password correctly, the wireless device starts the encryption process using TKIP or Advanced Encryption Standard with Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (AES-CCMP) which takes the original password and derives encryption keys mathematically from the network password. The encryption key is regularly changed and rotated; the same encryption key is never used twice. Other than entering the network password, the user isn't required to do anything to make WPA or WPA2 Personal work in the home (Apple, 2012).

Apple TV and AirPlay

Apple TV is not compatible with older generations of Apple products such as iPad 1, iPhone 4 and Mac OS 4 due to the

limited processing capabilities of those products. These products do not have Airplay built into them and there are no apps available to install the lacking features. AirPlay mirroring requires an iPad 2, Apple TV (3rd generation), iPad 2, iPad 2 Wi-Fi + 3G, iPhone 3GS, iPhone 4S, iPod touch 2nd generation and higher.

Solutions

If you are seriously thinking about using Apple TV in a legal setting, some maneuvering is needed to get it to work as well as the device does in the home. The only real option is one of the following:

1) Insert a rouge wireless router from one of your Ethernet ports (It is doubtful the IT folks will allow this workaround);

2) Configure a laptop, PC, Mac or smart phone as a wireless access point and point the Apple TV to it (This is an easy option but it can be costly for a wireless access point which is usually offered through your cell phone and cable companies);

3) Utilize the public, non-encrypted wireless access that most businesses establish for public users (Not advised for important presentations or legal proceedings);

4) If users really want to incorporate Apple TV into their office environment, it's best to create a separate public wireless environment – separate from the environment that is provided it – for the public with free access, and place all Apple components on that wireless network. It is also a good idea to invest in a Mac server OS to manage components to provide and extra layer of security to the Apple TV. The Mac server OS allows a systems administrator to utilize MAC address access control protocol or the RADIUS access protocol as an extra layer of security. However, this can be a costly option

…create a separate public wireless environment – separate from the environment that is provided to the public with free access…

Center for Legal & Court Technology

If you are determined to take advantage of Apple TVs' benefits without the cost, the options are:

5) Utilize the public, non-encrypted wireless access to connect to the Apple TV, but have Apple TV viewable through a PC or Mac which is wired and encrypted on the network. Then enable the *mirroring* feature on both your PC or Mac and iPad; or

6) Dedicate a PC or Mac as the main computer with all the software and programs that your organization uses for presentations or demonstrations. Utilize the Air Display utility to mirror your iPad to your main computer. Air Display allows you to wirelessly control your computer (PC or Mac) with your iPad without using Apple TV. You can then display and program that is installed in your computer.

   In doing so, your computer becomes a server that manages all your wireless components. This eliminates costly apps for programs with limited functionality and truly is the most cost effective solution that will give you the same bang as the Apple TV to operate wirelessly from your iPad and not a computer. And the best part is: *No network issues*. This solution is a great work-around because everything is displayed and operated through a computer that has already been validated and encrypted on the network. The iPad becomes a remote control for the computer.

McGlothlin Courtroom, William & Mary Law School

The Use of Apple TV at the Center for Legal & Court Technology

Recent upgrades to the McGlothlin Courtroom within William & Mary Law School, operated by the Center for Legal & Court Technology (CLCT), have afforded us the opportunity to integrate Apple products into the courtroom environment. Several locations within the courtroom are outfitted with Mac computers. We've also integrated Apple TV to test functionality and feasibility for use in

Center for Legal & Court Technology

the courtroom environment due to a significant interest expressed by the legal community. We also continue to support Mac Laptops at the podium for presenters.

Limitations

Because Apple TV does not support enterprise security protocols, Apple TV is deployed over the public non-encrypted wireless network at CLCT. This deployment is suitable for a testing environment and for general presentations. However, due to this limitation, other Apple devices such as iPods, iPhone, iPads and laptops have the ability to connect to the Apple TV. This means that those devices knowingly or unknowingly have the ability to disconnect the current presenter and take control of the device during a presentation.

The Airplay wireless connect feature provide the user with first level security such as password connection. Apple also boosts other security protocols such as the ***Media address access control (MAC)*** which allows network administrators to set up a list of MAC addresses and limit access to the network to only those whose MAC addresses are in the access control list. The ***RADIUS access control protocol*** also allows the systems administrator to create a central list of usernames and passwords of wireless devices that can access the network.

Lastly, there are a limited number of apps supported by the Airplay feature for Apple TV. However, if you enable the *mirroring* feature in iPad, you are able to show content from your iPad without needing the Airplay feature. This allows you to present from your apps and show them without Airplay.

Apple TV is fun, and offers numerous possibilities. However, its main function is for home entertainment and when presenting from and iPad to Apple TV. Essentially, the Apple TV device becomes a wireless access point that you can connect to and display from.

Secure Alternative Options

CLCT has integrated a more cost-effective and secure option to utilize iPads for trial presentation without the use of Apple TV. A computer can act as a server to call the functions of that PC or Mac

wirelessly be designating a computer (PC or Mac) that is wired and authenticated through the enterprise network, and installing the software Air Display to that computer, including your iPad. A user can access all the programs currently installed on the designated computer including programs such as Trial Director and PowerPoint. Air Display will mirror what is on your computer to your iPad and give you total control of the PC. When a computer is connected to a larger display, it can be shown for others to see in a presentation.

This alternative is cost effective because it eliminates the need to constantly purchase or update apps and show a user's iPad. Chances are users already have a computer with the necessary programs needed to give a presentation, show pictures, videos, and even run Trial Director from the iPad wirelessly. This requires no wires, no costly apps, no security issues, no public network access, no limitations, and no Apple TV, yet it provides users with the same functionality as Apple TV. It also provides flexibility because when you are away from your office you may not have the luxury of connecting to Apple TV outside of your current organization.

Practical Usage

In the future, Apple TV may offer endless secure possibilities for the legal environment. Many educational institutions have also found creative ways to take advantage of Apple TV's *coolness* factor to deliver lectures. Strictly from an information technology perspective, however, usage in a courtroom is not practical due to the lack of security as discussed earlier in this paper. Implementing any technology wirelessly over an unsecure and/or public network is not considered best practice in any networking environment. Because of this lack of security, lawyers advertently or inadvertently create the opportunity for users of the network to take control of or manipulate files during the presentation.

In addition, it is not a good idea to allow lawyers to bring and present trial from their personal iPads. Personal files, such as documents and photos, have the potential to be accessed over an open public network. An inexperienced user could also mistakenly display some important or inappropriate personal files during a trial presentation. Courtrooms that wish to allow attorneys to use iPads

can avoid this type of embarrassment by loaning iPads specifically for trial presentations.

Conclusion

There are many reasons to utilize and embrace Apple TV. Although originally designed for home entertainment, Apple TV can also be used in any business environment. However, it is best to know the IT infrastructure, rules, and best-practices of an organization and its IT department. If the court supports both Mac and PC, there may already be provisions in place for products like Apple TV. Otherwise, attorneys should be prepared to find a work-around solution if they choose to present from an iPad.

William & Mary Law School
P.O. Box 3050, Williamsburg, VA 23187
757-221-2494, FAX: 757-221-3708
www.legaltechcenter.net, clct@wm.edu

Terms

AES: Advanced Encryption Standard. This is an encryption algorithm for securing sensitive data. AES replaced TKIP.

Airplay: Airplay is wireless technology that is fully integrated to allow you to stream music from you iTunes library, photos, and videos wirelessly from your iPad, iPhone, iPod Touch or any Mac or Windows PC to your Apple TV and Airplay enabled speakers.

Apps: Application software.

Bonjour: Apple implementation of zero configuration networking which allows various devices to connect to the network automatically.

CBC-MAC: Cipher Blocking Chaining Message Authentication Code Protocol – a component of CCMP that provides data integrity and authentication.

CCMP: Counter Cipher Mode Protocol – an algorithm that provides data privacy.

EAP: Extensible Authentication Protocol – an authentication protocol which supports multiple authentication mechanisms without requiring IP addresses.

IEEE: Institute of Electrical and Electronics Engineers – a professional association dedicated to advancing technology innovation and standards.

LAN: Local Area Networks – supplies networking capability to a group of computers in close proximity such as in a home, school, computer laboratory or office building.

MAC address: Media Access Control (MAC) address – a unique 12-digit hexadecimal identifier assigned to a device interface for communication on the network segment.

Mirroring: allows you to present to an external device such as a computer monitor or flat screen TV from what you see on your iPad, iPhone4S, or Mac.

RADIUS server: Remote Authentication Dial In User Service – a networking protocol that manages access to the internet or internal networks, and wireless networks.

TKIP: Temporal Key Integrity Protocol – an algorithm wireless computer network security protocol which is an older protocol adopted for WPA that implements much of the IEEE 802.11i wireless networking standard.

WEP: Wired Equivalent Privacy – a security algorithm that relies on a secret key that is shared between a mobile station and an access point. This privacy protocol provides wireless LAN users protection against eavesdropping.

WiFi: Wireless network technology that uses radio waves. A trademarked term meaning IEEE.

802.1x: IEEE802.1X – the IEEE family of standards for authentication on networks.

WPA: Wi-Fi Protected Access – the IEEE 802.11i that supplies security over WEP protocol.

WPA2: Wi-Fi Protected Access II – replaced WPA and TKIP encryption protocol with CCMP and requires testing and certification for enhanced security.

References:

Apple (2012). Manual for Apple Airplay Networks. Retrieved from http://www/apple.com.

Solomon, M. & M. Chapple. *Information Security Illuminated*. Sudbury; MA: Jones and Bartlett Publishers, 2005.