CONTENT SECURITY

KRAMER'S APPROACH TO SECURING DATA WITHIN WIRELESS TRANSMISSION

KRAMER WHITE PAPER

Executive Summary

There has been a fundamental shift in how people collaborate in today's meeting spaces, and how they are also connecting to technology. Previously, meeting space participants only had to know which hardwired cable they needed to plug in to connect to a display or projector. Even so, those cables came with their own connectively issues; specifically, the HDMI cable. With HDMI, users were presented with connectivity challenges ranging from damaged pins to HDCP issues.

Today's meeting space utilizes wireless connectivity, which neatly solves just about all of the aforementioned connectivity problems. However, that does not mean that wireless connectivity comes free of caveats! One of the biggest challenges facing wireless environments today is security; how do you secure content while transmitting it wirelessly from a "bring your own device" (BYOD) tablet or smartphone to a display or projector? Meeting participants may well wonder, "What is my wireless presentation/collaboration solution doing to ensure my content is not vulnerable to cyber theft or hacking?"

According to research and advisory firm Gartner, Inc., "A failure to manage information accurately can be fatal to the success of MDM programs." The company has also stated, "By 2016, 20 percent of CIOs in regulated industries will lose their jobs for failing to implement the discipline of information governance successfully."

Wireless presentation and collaboration products are growing in popularity, but most of them provide little to no security or protection against unauthorized users and data hacks. This paper will cover the processes by which Kramer's VIA technologies provide encryption and data protection for all content being transmitted and shared from tablets, smartphones, and laptops.

Content Security

Wireless presentation and collaboration solutions have flooded the market place within the past 5 years. These products vary in capabilities from consumer-grade connectivity for in-home movies and photo sharing to commercial-grade connectivity meant for the rigors of an office or classroom setting.

Unfortunately for today's consumer, the story we are not hearing is how this new generation of presentation/collaboration products will impact the security of corporate, educational, and institutional IT networks. Network security is a critical issue. It seems that each passing week brings fresh news of a "hack" into supposedly secure networks run by major retailers, colleges and universities, and even the federal government.

Manufacturers have spent considerable time and money promoting features of their individual wireless solutions. Even so, virtually every manufacturer has ignored even the most basic levels of content security. Worse, many depend solely on existing security within a network such as firewalls to protect content, leaving you responsible for any possible data breaches.

> *"Through 2016, spending on governing information must increase to five times the current level to be successful."*
>
> - Gartner

Independent research has confirmed that organizations must invest in internal infrastructure to protect and secure data being transmitted over their networks, especially when BYODs are used. According to Gartner, It follows that every presentation/collaboration product connected to an enterprise network should have security at the top of its list of features – and not just one layer, but multiple layers of secure connectivity.

Kramer's VIA platform was specifically designed with the understanding that although wireless connectivity and collaboration is the wave of the future, the security of content cannot be ignored. Let's take a closer look at how VIA handles data security.

Kramer VIA Data Protection Technology

Wireless Protection

Normally, VIA Collage, VIA Campus and VIA Connect PRO would be connected to a third-party Wi-Fi access point. These devices provide one level of secure communication through the Wi-Fi Protected Access 2 (WPA2) protocol.

WPA2 combines the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES) to dynamically generate 128, 192, or 256-bit cryptographic keys each time someone logs in wirelessly to a VIA session. (For wireless access points using the older WPA standard or mixed WPA/WPA2 modes, the Temporal Key Integrity Protocol (TKIP) provides 128-bit keys for every packet.)

Protecting Communications Through the Network with Encryption

Within VIA Collage, VIA Campus and VIA Connect PRO, another layer of secure communication is present with the Transport Layer Security (TLS) 1.2 protocol, both for authentication and for data flowing in and out of VIA. TLS replaces the Secure Socket Layer, an earlier form of security for electronic commerce through Web (HTTP) pages. TLS protocols provide communication security over a computer network by using X.509 certificates, which negotiate symmetric session keys that are then used to encrypt data flowing between the parties. This becomes the backbone of the Kramer VIA encryption process.

By implementing the TLS Record Protocol, VIA also provides connection security with an encryption method (the Data Encryption Standard (DES)), while the TLS Handshake Protocol (Figure 2) allows each VIA unit and user to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. By using TLS, a secure connection is created within the VIA Collage, VIA Campus and VIA Connect PRO between client software and server software.

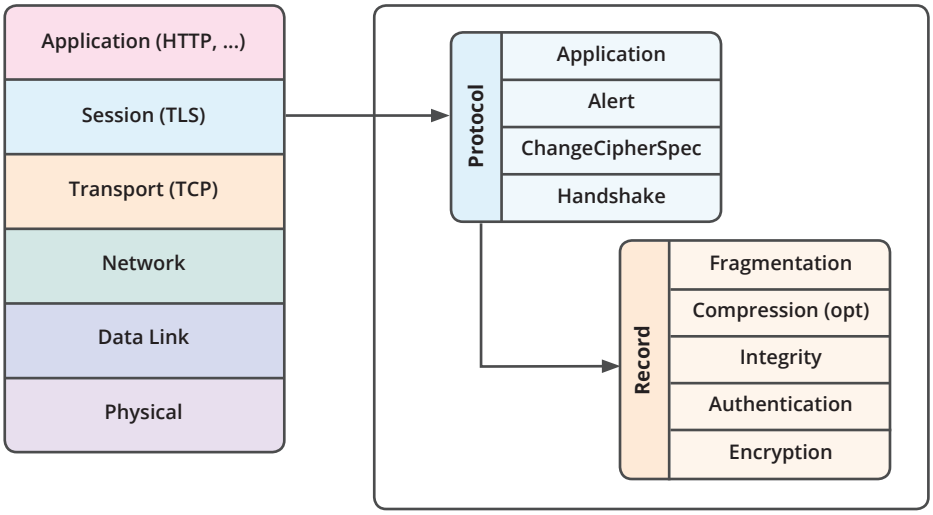

Figure 2

As mentioned earlier, the Advanced Encryption Standard provides 128, 192, or 256-bit cryptographic keys. To date, AES-192 and AES-256 ciphers have not been "cracked" in extensive, repeated tests by the National Security Agency (NSA).

Accordingly, the combination of WPA2/AES and VIA's built-in TLS 1.2 encryption offers a very high level of security for every collaboration session to all mobile/wireless participants. Existing firewalls and VIA's TLS implementation provide equal protection to participants logged in through LAN connections. (Figure 3)

Even so, it is possible that a so-called "brute force" attack could be attempted. Institutions that handle sensitive material, such as proprietary information or financial data often prefer to implement even more robust security measures. One such measure would be to choose passwords with at least 16 characters, mixing letters, numbers, and symbols. Another would be to encrypt the actual files themselves.

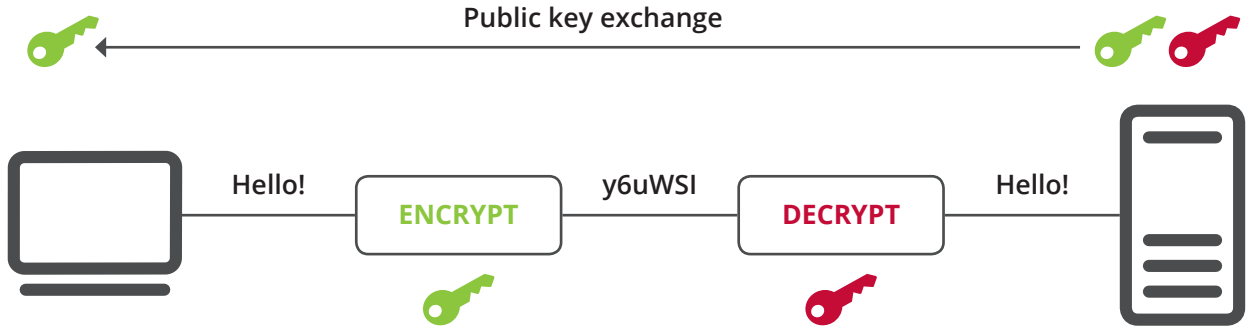

Figure 3

This level of digital security of the material itself is referred to as File Server Security Level (FSSL) encryption, because it requires a considerable amount of time and effort to break the keys. These encryption keys convert any transmitted content from a BYOD device through a network into an unreadable cipher. This is done by applying a set of complex algorithms to the original content, converting the data into streams of seemingly random alphanumeric characters, only decipherable at the receiving end with the proper decryption keys.

Not all Encryption Schemes are Created Equally

It is important to note that there are several types of encryption schemes in use today, but not all of them are secure. Other solutions may use simplified algorithms that are easily broken using modern computing power; another point of vulnerability that must be considered by any IT manager adding a presentation/collaboration solution to their network. Kramer's VIA platform implements the most advanced data protection and security in the industry.

Protection from the Outside World

The operating systems in VIA solutions also incorporate Firewall protection to provide protection against malware and viruses. An additional layer of security is provided through the use of random room codes that are only visible to meeting participants who log-in through WPA2 connections or LANs. These room codes can be programmed to change automatically at pre-determined intervals, and can also be displayed on the collaboration platform log-in page or provided by different means (orally, texts, emails). (Figure 4)

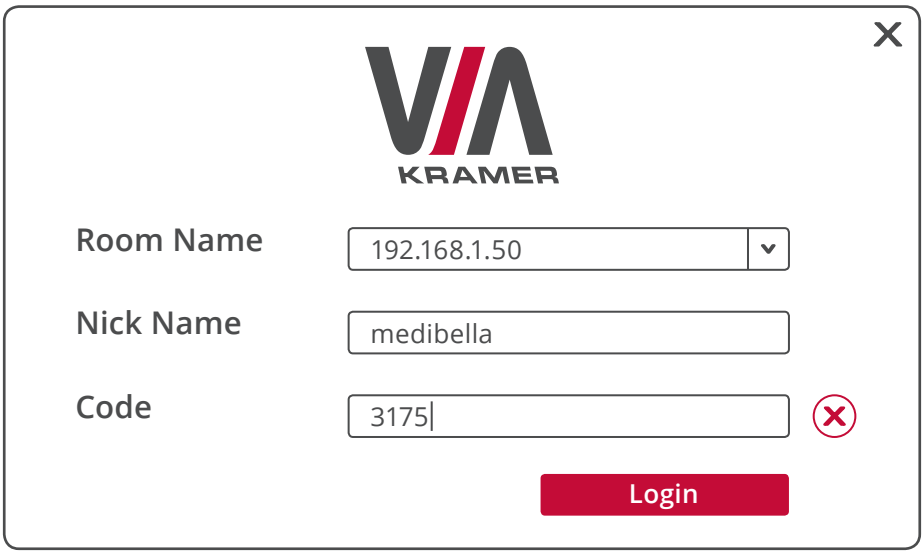

Figure 4

Summary and Conclusion

As you can see, Kramer VIA Solutions there are 4 levels of security when using Kramer VIA Solutions.

Aside from WPA-2 protection in wireless access points, Kramer VIA Solutions provide three additional levels of security, as follows:

- TLS 1.2 protection of communication on the network
- File Server Level Security of files and information sent on the network
- Windows firewall protection between the network and outside world

BYOD devices are becoming more prevalent within corporate and classroom environments. The International Data Corporation (IDC) recently reported that the use and sales of smartphones and tablets will continue to rise with mobile device and app sales reaching $484 billion. More importantly, 18% of tablet sales will be to businesses. This is relevant data because it is a contributing factor to the integration of wireless connectivity products on client networks.

As with any other presentation/collaboration product line, there are a multitude of different solutions to choose from and the selection process can seem overwhelming. Regardless of the in-room needs and business drivers, there is a shared concern that IT manager have, and that is content security. Be sure to consider network security issues and how exactly that specific product handles them.

Taken together, the protections built-in to Kramer's VIA Collage, VIA Campus and VIA Connect PRO, in combination with secure wireless networks, company firewalls, and in many cases File Server Level Security, provide an extremely high level of security for meetings that keeps pace with the needs of today's corporate, educational, government, and institutional networks.

About Kramer

Since 1981, Kramer Electronics Ltd. has been a leading player and pioneer in the Pro AV industry. With 26 global offices across six continents and support and distribution in over 100 countries, Kramer offers an extensive and innovative Pro AV solutions portfolio for Corporate, Education, Houses of Worship, Government, Live Events, Healthcare, and more.

For over three decades, Kramer has built its reputation on strong personal relationships with its customers and providing the highest level of service and support in the industry.

Kramer has won numerous awards, including the 2013 Pioneer of AV Award at InfoComm in honor of its Founder, President & Chairman, Dr. Joseph Kramer. Kramer's award winning analog and IP-driven solutions for collaboration, streaming and control are at the forefront of an ever-evolving Pro AV industry. Kramer's consistent sales growth and expansion into new markets is a testament to the company's commitment to R&D and reliance on customer feedback.
For more information, visit us at: www.KramerAV.com

KRAMER ELECTRONICS, Ltd.

3 Am VeOlamo St.
Jerusalem, Israel, 9546303
Tel: + 972 73 265 0200
Fax: + 972 2 653 5369
E-mail: info@kramerel.com
Web: www.kramerelectronics.com

KRAMER ELECTRONICS USA, Inc.

Headquarters
6 Route 173 West
Clinton, NJ 08809, USA
Tel: (908) 735 0018
(888) 275 6311
Fax: (908) 735 0515

Tech Support after 6pm EST:
Tel: (888) 275 6311
E-mail: info@kramerus.com
Web: www.kramerus.com