Edith Cowan University
Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2008

Assessing and Mitigating VIP Vulnerabilities in the Corporate Environment

Hoi Z. Wong
Edith Cowan University

DOI: 10.4225/75/57b653c334761
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/61

Assessing and Mitigating VIP Vulnerabilities in the Corporate Environment

Hoi Zung Wong
School of Computer and Information Science
Edith Cowan University, Australia
michael.wong@pcsworld.com.au

Abstract

Video over IP (VIP) is becoming a tool of communication in corporate environments to reduce the time spent conducting meetings face-to-face. This has been driven by efficiencies of time saving, management's monitoring of staff and to communicate with flexibilities - without placing additional disadvantages on employees who must regularly attend personal meetings amongst hectic business schedules. With technology excelling beyond the old telegraphy of analogy video over hard copper wire to dark fibre technology, VIP is a technology that is starting to receive more attention in the corporate world as more organisations have the equipment to support this additional plug-in. But whilst corporate management may consider VIP a cost saving enterprise, the security implications it may pose to the information environment and internal networking communications are still a valid concern. This paper will review the risks for VIP systems in the corporate arena, and relevant models used in these systems will be analysed and reviewed for their specific networking vulnerabilities. This paper suggests much is still unknown about the risks VIP poses to uneducated corporate users and the technologically reliant business sector, and presents certain cases that support this argument.

Keywords

VIP, IP, corporate.

INTRODUCTION

VIP is a new concept that is being adapted in the world of corporate communications, especially compared to old audio and video methods. Today's business sector is reliant on technology driven efficiencies like fast broadcasting of video feeds into the intranet or internet and the demand for secure information transfers is a paramount concern for corporate management. VIP is often utilised in situations that warrant a video transfer of information, however little is known about the vulnerabilities that coincide with VIP transactions. Though VIP is a valuable resource in business practicality, there are still major risks for employees and overseeing manager who utilise VIP for corporate meetings without additional security measures in place. These safeguards vary in nature but combine to ensure VIP is not considered a weak link in an organisation's complete network communication system. It can be said utilising VIP without any secure measure in place will make the system exploitable and susceptible to hackers. This paper will focus on the advantages of applying VIP data transfers in the corporate environment, whilst also supplying a list of VIP vulnerabilities and appropriate countermeasures that will harden the feature for VIP and future data communications.

VIP METHODS

According to Video over IP Pros (2005) there are three available methods applied to network communications that can involve video transactions. These are video broadcasting, video on demand, and video conferencing. These options offer different services but are altogether reliant on network consistencies and an organisation's open network communication structure. Video broadcasting and video on demand are usually configured to adopt a one way transmission methodology, whereas video conferencing is generally considered a full duplex application.

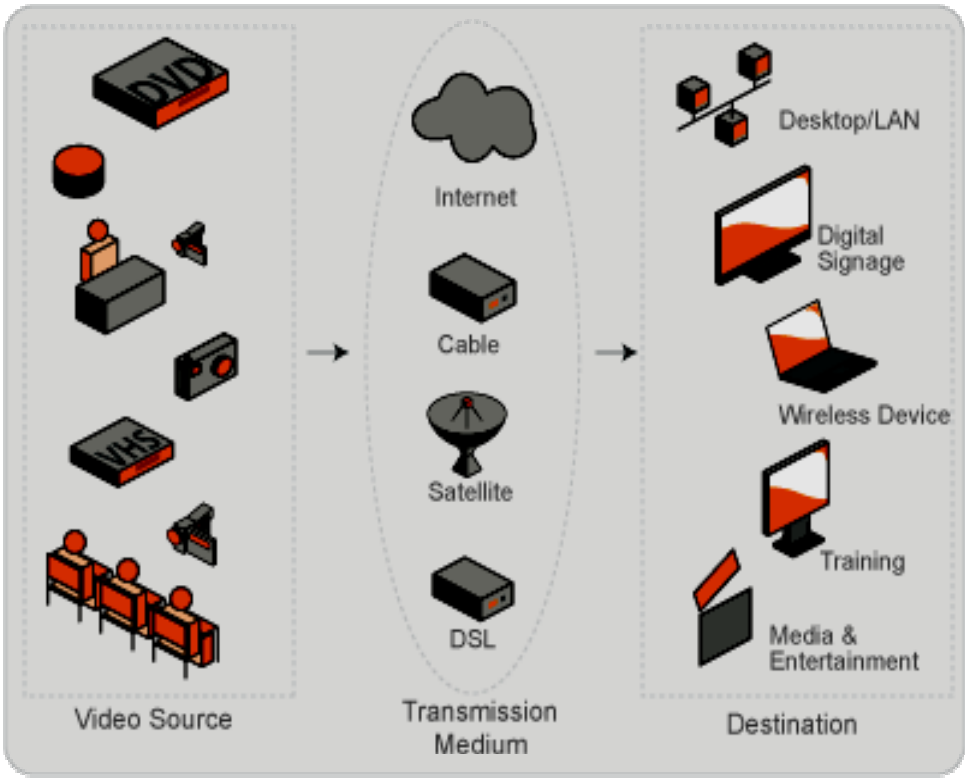

Figure 1. Video over IP Options in the Corporate Environment. (VIP Pros, 2005).

The above figure portrays the link between the video source, various transmission mediums, and the video's eventual destination. VIP allows video signals to be managed and streamed over IP networks which contain numerous advantages for those in staff and management positions. Though this paper's focus is on pure IP transmissions, it is important to recognise the adaptability of the VIP function, as it can also be applied via satellite and cable networking.

ADVANTAGES

VIP has many advantages for large organisations pushed for time and resources in the current corporate climate. It is a necessity in some cases where meeting face to face is practically improbable whilst demanding little of staff setup arrangements. The following is a list of VIP advantages in the corporate environment.

Practicality

Telecom (2003) authors first relayed their thoughts on VIP practicality via their light reading website. They alluded to the fact that some advances in technology have made the concept of running video over copper local loops more of a practical proposition. One advantage is that new video compression technologies can squeeze high quality video into modest bandwidths, whilst another advantage refers to the simple combination of Ethernet and IP to transport video across core networks that feed DSL periphery. These practical networking components appeal to corporate management who must use rely on predetermined bandwidth allocations and IP data transfers across varying network protocols.

Cost Effectiveness

VIP is a cost effective enterprise for those utilising the feature within the bounds of a company's bandwidth capabilities and IP network compounds. The VIP process itself is quite simple but is made complicated through users' preconceived conceptions of video transmissions. To counteract these old misconceptions, companies such as Avaya, Polycom and Cisco have pioneered new VIP directions and have made the option appealing to corporate departments and less costly to the enterprise. For a starting price of fifteen thousand dollars, companies can introduce and configure VIP to suit their immediate needs. Much depends on the bandwidth limits organisations are subject to, however the real cost savings are realised when one compares the cost of

new VIP transmissions to the old legacy based analogue video technologies which once dominated video markets in a digitally deprived world.

Flexibility

VIP is flexible in that it only requires two different stations and a medium of transmission for effective data relay. Generally a video server is required for efficient data transmissions and logging materials, however very little is demanded of receiving clients once video transmission has been achieved. VIP also offers users the opportunity to pre-record videos and stream them to clients at a later time, different video compressive functions, and obvious live feed capabilities that suit busy business timelines. The following figure represents a situation in the corporate environment. It is an example of the numerous options available through VIP by using Polycom and Avaya devices, and relevant VIP software applications.

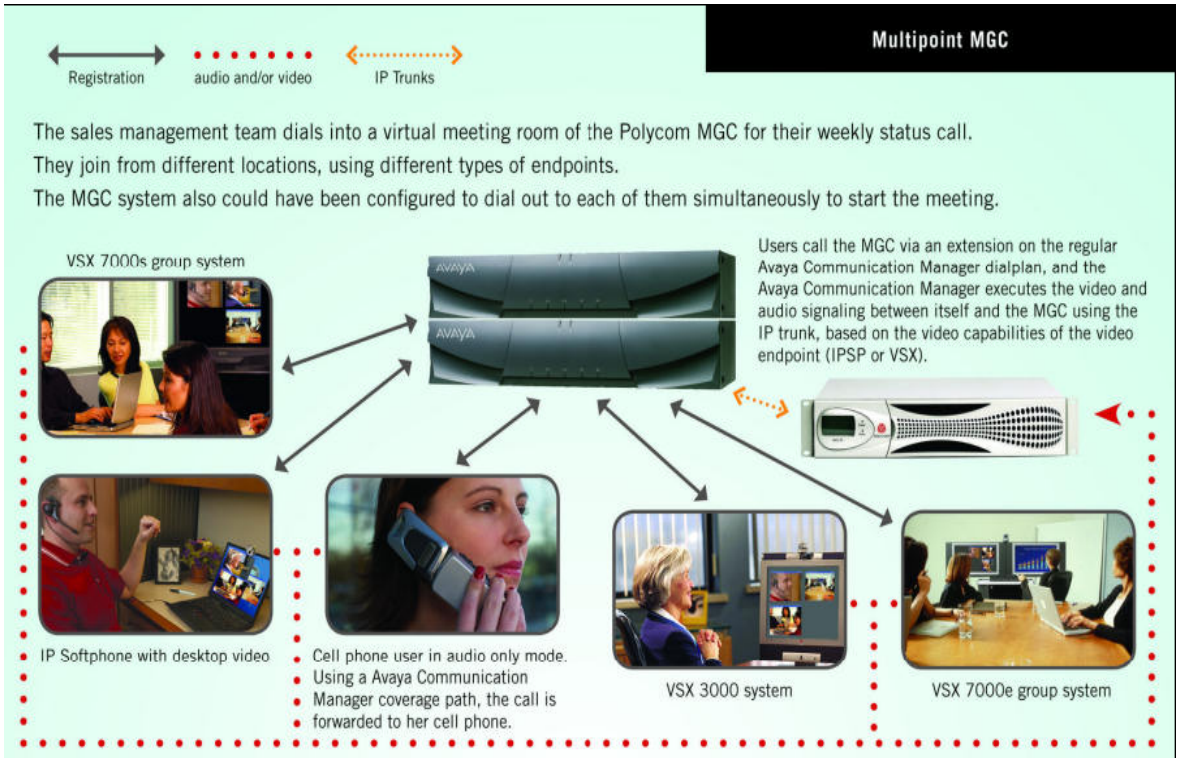

Figure 2. VIP Flexibility in the Corporate Environment. (Kent and Tepper, 2005)

Scalability

VIP is scalable in its own right due to its flexible features that enable users to use another method of IP data transmissions. It can be modified to suit the styles and situations that demand live or pre-recorded video feed for personal face to face agendas. Its scalability to large organisations can be compared to enterprise movements that use video conference capabilities for conference calls - and the small office users who require video options with regular staff liaisons. VIP is scalable in the fact that many organisations can utilise its various methods for different situations.

Network Operability

One of the main benefits of utilising VIP in modern times is that companies only need a workable network grid in order to maintain a constant video capability. VIP is only applicable in situations where networks are a reliable communication resource, as it is dependent on network IP for standard network transmissions. This demands a little more of network bandwidth and accommodating sources, but delivers more in video practicality and advanced face to face meeting options. This means that any corporation utilising networking for

communications is capable of applying VIP to their communication foundations. This ensures VIP is only an extra addition to an already solid networking base which can be adjusted to suit ongoing corporate demands.

New VIP Interest

VIP was once viewed as a special interest product that required additional expenditure and supplementary attention from management. But now that VIP is becoming a cost effective product with little setup requirements, mainstream business organisations are becoming more interested in VIP for its transmission flexibility and overall data operability. The new VIP direction will continue to grow in popularity and increase its technological appeal as companies become more involved in the VIP process. This will breed a new era of VIP dependency and data transmissions via video for important corporate meetings and information transfers using inexpensive IP practices.

VIP VULNERABILTIES

VIP contains vulnerabilities that can impact on its reliability and efficiency in relaying data transmissions over network space. The following is a list of VIP weaknesses in the corporate environment.

Network Capacity Limits

Currently VIP demands more of network capabilities than any other transmission application. VOIP and other audio transmission functions require less of the network's rate and content base, with low latency almost guaranteed with most audio applications in today's technical environment. However VIP is a different product because it asks networks for more bandwidth, bit rates, and network exposure than normal audio transmissions. This can impact on an organisation's network capacity particularly if the VIP application is not configured correctly and is in constant use. This will inevitably affect the network's overall communication cycle and internal video streaming objectives. It could also potentially affect other forms of network communications, such as VOIP, Smartphone telephony, and regular internet transmissions.

Low Latency Demands

Video transmissions are essentially an effective network bottlenecking tool if traffic flow cannot be controlled by Information Technology (IT) staff. VIP demands a low latency level for communications to be effective, and places pressure on a network's capacity to handle latency rises without interrupting VIP data relays. In addition to the latency issue, VIP must also have extremely high throughput compared to voice (usually multiple megabits per video channel instead of 64 kbps for voice) which poses a severe challenge to today's networks whose basic packet forwarding architectures have remained unchanged for over thirty years (Anagran, 2007). The VIP high throughput combined with low latency demands requires additional corrections from IT administrators who must somehow balance the two without upsetting core network communications.

Bandwidth Issues

It is well known that bandwidth is a concern for management in every day office liaisons, without extra VIP applications being used for staff meetings and conference calls. Bandwidth limitations are administered by governing bodies to ensure the function is not abused by one or a group of organisations. This affects the overall bandwidth capacity of VIP in the workplace, as limits can seriously impact on the amount of video calls a company can make on a daily basis, and the overall bandwidth allocations that applies to different communication services. Some companies such as Cisco and Anagran are using various program initiatives to apply bandwidth restrictions on VIP services (such as only using network bandwidth after a client request) but this is still a work in progress. Because VIP demands more of a network's bandwidth, management will continue to see this weakness as a viable concern for introducing VIP for internal/external communications.

Packet Loss Issues

Packet loss is a major concern that accompanies the VIP function in nearly all cases. It usually results in a metallic sound occurring through audio feeds and/or a dropout of video picture feed between transmissions. According to Shoretel (2007) packet loss is caused by congestion, poor line quality and geographical distance, and if users are using Real-time Transport Protocol (RTP) running over User Datagram Protocol (UDP) with their application, there is no way to recover lost packets. The data packet issue with VIP demands more of vendor applications and network capabilities, as most modern managers would require extra software assistance

in this area to ensure packet loss does not negatively impact on video transmissions between clients and internal staff liaisons. Undeniably, the data packet problem in VIP interactions is a major talking point amongst VIP buyers and one that is a constant deal breaker for VIP in corporate communication.

Network Video Time Delays

Generally, IT professionals in the corporate environment must be aware of network limitations in order to gauge the correct levels of standard network practices that make the network run smoothly through daily communications. This process is critical to VIP services, as the network will inevitably suffer from video time delays if the network reaches its capacity through either VIP usage or other network dependencies. Due to the low latency and high throughput demands of VIP, it will be one of the first applications to become affected from network limitations if that instance was to occur whilst VIP calls were being made. This places extra pressures on IT advisors to know the demands of VIP and how it may affect the network's capacity in real time. This can also impact on direct VIP communications, as real time video streaming can force calls to queue exponentially – placing more time delays on network communications and adding further packet loss to congested lines.

Jitter

Jitter is not usually considered a major weakness in VIP applications due mainly to the lessons learnt through VOIP communications; however it can affect VIP transmissions to a severe degree if left unresolved. Fries, Kuhn and Walsh (2005) stated Jitter refers to non-uniform packet delays that can cause packets to arrive and be processed out of sequence, and is often caused by low bandwidth situations which can be exceptionally detrimental to the network's overall Quality of Service (QoS). VIP can be affected by Jitter, usually reflected by direct packet loss or video time delays which stem from out of sequence packets. Due to the developments of vendors concentrating on this area of operations Jitter generally does not raise as much concern to VIP users as latency or bandwidth considerations, but its potential to become a reoccurring issue for management and staff is a real problem for VIP users,

VIP SAFEGUARD PRACTICES

There is little in the way of security testing done by public sources that are reliable in the field of VIP. Due to its recent introduction to IP infrastructure, the testing of VIP security safeguards and specific vulnerability countermeasures are still very much in their initial phases. But there is some security and networking practices that can be administered to ensure VIP is as secure as possible for efficient company communications.

RTP Policy

RTP is essentially an IP based protocol that enables users to have support for the transport of real-time data. Some of the RTP functions include packet loss discovery, time rebuilding and various security measures that are basic in nature. RTP is basically an end to end transport service and the figure below portrays what RTP data may look like in a transmitted packet.

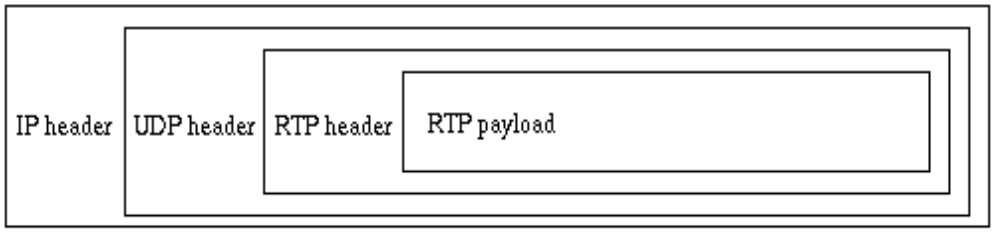

Figure 3. RTP data in an IP packet (Liu, 2000).

The RTP policy is helpful for all users and is a recommended practice for all corporate communications. RFC 1889 and RFC 1890 have been administered for specific audio and video applications via IP methods, and are useful documents for those applying VIP to existing network infrastructure.

Resource Reservation Protocol (RSVP)

RFC's 2205 -2209 refers to the RSVP policies that has been standardised for network video and audio streaming through various data environments. Real-time applications use RSVP to reserve necessary resources at routers along the transmission paths so that the requested bandwidth can be available when the transmission actually takes place (Liu, 2000). This ensures that allocated bandwidth is used efficiently with VIP calls.

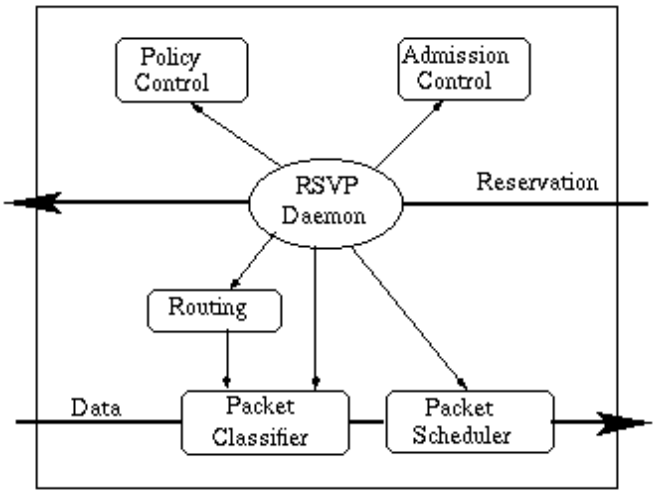

Figure 4. Reservation at a node on the data flow path (Liu, 2000).

RSVP is not a new concept, but additional software may be needed in current environments to ensure that bandwidth issues receive additional attention. RSVP is a minimal requirement but could not be completely relied upon to deliver bandwidth solutions with modern VIP designs.

Timestamps

Timestamps are used in the transmission of networks and are contained in the head of each and every packet segment sent over the wire to its destination. It is very important that this information is available so that the video is delivered on time and without delay, this is also a feature that controls packet reassembly at it destination. With this feature the video can be recompiled when the segment is complete. If the buffer is too small, then it will overflow, and packets will be discarded, leading to a gap in the conversation. Jitter buffers may work by making delay calculations based on the time stamp of the packets, but a simple approach is to just play out a video sample every 125 µsec. If the buffer does empty, the jitter buffer can simply repeat the last packet's worth of Video samples (Petryna & Staves, 2000).

Encryption

Encrypting scalable video calls is a relatively new process that can be applied for the security conscious manager or to offer users additional security measures for transmitted video data. Delp and Eskicioglu (2003) recognised the importance of utilising either partial encryption or progressive encryption techniques by using multiple layer encryption methods and bit rate assessments.

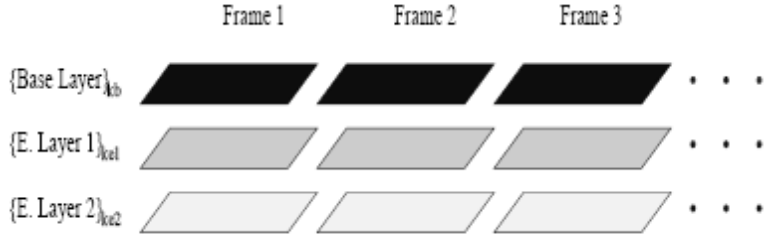

Figure 5. Encryption of multiple layers of a scalable video stream (Delp and Eskicioglu, 2003)

Encryption of video streams is an important aspect of VIP security. It ensures users that data security is applied to VIP transmissions, which is an assuring aspect when one considers the vulnerabilities current VIP data packets currently possess.

Packet Flow Assistance

Anagran is one of the few organisations that can assist corporate departments with packet flow inconsistencies. As determined earlier, packet loss is a major VIP disadvantage when users utilise this transmission base for constant corporate meetings. But with companies such as Anagran providing new packet flow assistance, VIP can be administered without fear of regular packet loss or severe network bottlenecking. In normal circumstances, if six packets were distributed from the outgoing source, up to five would be dropped due to traffic restrictions and video flow limitations. However, as the figure illustrates, Anagran can increase traffic flow with built in intelligence streams and reduce packet loss substantially.

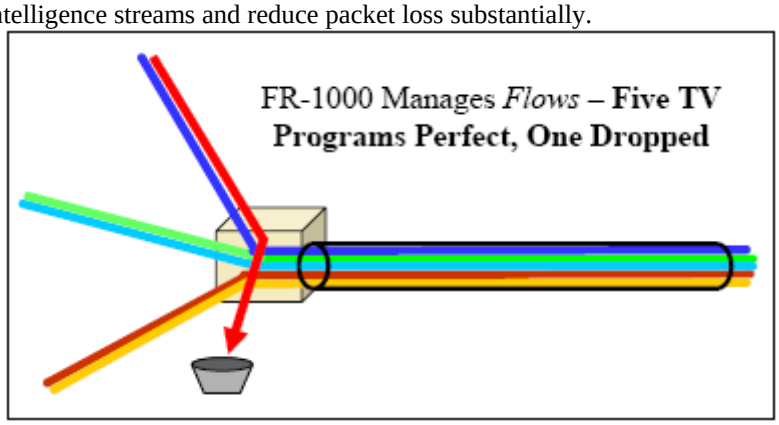

Figure 6. Television Packet Flow IP Representation after Anagran Assistance (Anagran, 2007)

Vendor Assistance

There are currently many vendors, such as the previously mentioned Anagran, that focus on offering specific solutions to the various issues users face with VIP software and industry related hardware. Cisco, Avaya, Nortel, Shoretel and Polycom are model companies that can provide corporate management with options in VIP security hardening, video compression software, packet loss assistance, and bandwidth capability guidance for VIP installation. Cisco's Senior Manager Gupta (2007) stated that when deployed properly, an IP infrastructure's inherent content management and delivery capabilities, application-aware intelligence, and multidimensional scalability – can make it the ideal platform for delivering a compelling, differentiated video experience.

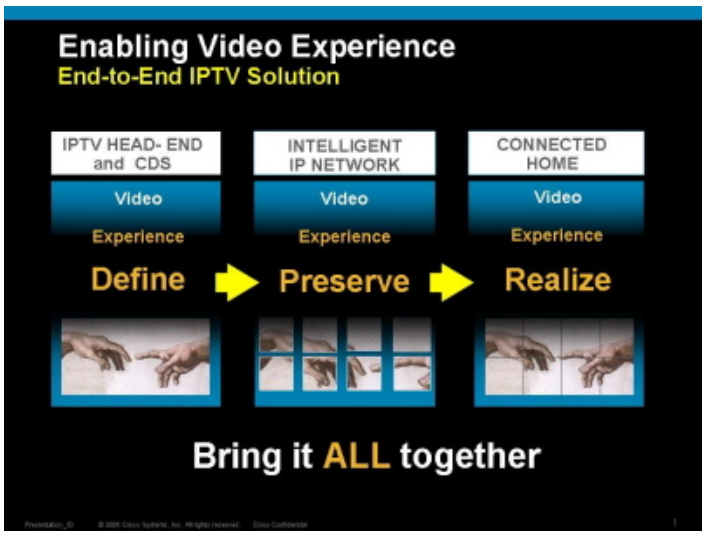

Figure 7. Cisco's VIP Solution (Gupta, 2007).

Corporate users should be aware of the assistance offered through various vendor services and ask for help if network vulnerabilities are consistent after the initial installation. In a perfect situation vendor assistance would be most suitable prior to VIP setup.

H.323 and H.460

H.323 and H.460 are standard protocols introduced to deal with certain IP multimedia vulnerabilities and security issues. As there are still some problems evident in sending high stream media across firewalls and routers (particularly those with Network Address Translation (NAT) capabilities), these protocols offer users specific solutions for this area of IP transmission. H. 460 mainly deals with tunnelling solutions, by offering users a trusted server outside the firewall that acts as a proxy for all video conferencing traffic that crosses the firewall (Bartlett, 2008).

Figure 8. H.460 Server Used for Multimedia Tunnelling (Bartlett, 2008).

Like H.460, H.323 version 5 offers user's additional security and multimedia options, and was introduced in 2003 to deliver more stability than previous H.323 versions. MicroMethod's Horizon's H.323 version is becoming more popular because it gives users an additional option in data traversals and is relatively quicker than Session Initialisation Protocol (SIP). In addition to the H.460 option, users can also use proprietary secure traversal, which can either be embedded with H.323 endpoints or act as a sole proxy through which registered internal H.323 devices can communicate with external networks, whilst ensuring clients make outbound connections to the server in a secure tunnel through a single fixed outbound port across the firewall/NAT (MicroMethod, 2008). This ensures firewalls are still active and secure during transmissions and adds more data protection between VIP clients. MicroMethod also stocks SIP applications but this technology is becoming out of date compared to new H.323 methods.

FUTURE VIP DIRECTIONS

The future of VIP in the corporate area will depend on how beneficial and operable the feature becomes to large enterprises. To some individuals, VIP is still a product that demands too much setup time from staff and too much of the network's bandwidth capacities, while also delivering little in the way of communication reliability and data packet consistency. But this image of VIP is not an accurate perception of new video transmission capabilities, as more VIP vendors test and resolve issues with packet loss, bandwidth and problems with time relay. Testing in the VIP area will result in additional security measures becoming more readily available to corporate organisations - which will inevitably result in technical aspects becoming less of a problem to the average office user. Eventually, VIP will be another feature such as VOIP and Skype that will be observed as a hassle free technical beneficiary, other than a hindrance to network operations.

CONCLUSION:

VIP is a relatively new technology that can bring many benefits to the corporate environment in terms of saving money, meetings with internal/external parties, and especially booking those expensive project managers. Time will also be saved and efficiently utilised from a business perspective. This paper has outlined the advantages and disadvantages of VIP, in having an understanding that VIP utilises more bandwidth than the conventional normal network traffic. VIP requires the network to have low latencies to be used efficiently, appropriate

safeguards for security vulnerabilities, and reliable software extensions for packet losses in transmissions over the wire. As mentioned in this paper, VIP will bring many advantages to the corporate arena, similar to VOIP and email communications, and VIP will inevitably become an essential component in enterprise business.

REFERENCES:

Bartlett,. (2008, Sep) Video Tunnels through the Firewall, Retrieve September 20, 2008, from http://www.nojitter.com/blog/archives/2008/09/video_tunnels_t.html

Eskicioglu, (n.d.), An Integrated approach to Encrypting Scalable video, Retrieve September 20th, 2008, from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.2626

Delp, E.J. (n.d.) Video and Image Processing Laboratory (VIPER), Retrieve September 20th, 2008, from http://cobweb.ecn.purdue.edu/~ips/

Gupta, P. (2007, Apr), Delivering Video over IP networks, Retrieve September 20, 2008, from http://www.byte.com/documents/s=10114/byt1176041614458/0416a.htm

I.T. PROS. (n.d.), Video over IP Technology, Retrieve September 20, 2008, from http://www.videooverippros.com/index.html

Kuhn. R, & Thomas. J, & Walsh, & Fries. S, (2008), Security Considerations for Voice over IP Systems, Retrieve September 20, 2008, from http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Kent. R, & Tepper. H, (2005), Enterprise Video Conferencing: Ready for Prime Time, Retrieve September 10, 2008, from http://www.avaya.co.uk/emea/en-us/resource/assets/whitepapers/video%20conferencing%20white%20paper.pdf

Liu, C. (1998, Jan), Multimedia over IP: RSVP, RTP, RTCP, RTSP, Retrieve September 20, 2008, from http://www.cs.wustl.edu/~jain/cis788-97/ftp/ip_multimedia.pdf

LightReading, (2003, Oct), Video over IP, Retrieve September 20, 2008, from http://www.lightreading.com/document.asp?doc_id=40811

MicroMethod, (n.d.), Horizon H.323 – Secure Firewall/NET Transversal, Retrieve September 20, 2008, from http://www.micromethod.com/products/horizon_sheet.pdf

Petryna. B, & Staves. S, (2000, Jul), Meeting the engineering challenges of VoIP communications, Retrieve September 20, 2008, from http://www.edn.com/article/CA47062.html

ShoreTel, (2005, Mar), Is Your Network Ready for IP Telephony, Retrieve September 20, 2008 from http://www.datamart.com/documents/ShoreTel%20-%20Is%20Your%20Network%20Ready%20for%20IP%20Telephony.pdf

COPYRIGHT

[Hoi Zung Wong] ©2008. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.