

Broadcast Terrorism

Keeping the Intruders Out

Danny Wilson, President
Pixelmetrix Corporation, Singapore

Terrorism is becoming more rampant and is now a worldwide concern. In the television world, the rise in hacking incidents, particularly into a communication or broadcast network, has grown to be a serious industry issue.

With the advancement of technology, the physical protection of assets that used to be the norm is no longer sufficient. With the control of media being a big prize for the terrorists – and an unthinkable loss for broadcasters, preserving broadcast integrity is more crucial than ever.

On top of security measures that can be implemented to enhance security, monitoring systems deployed at various checkpoints along the video transmission chain can identify security penetration threats, intrusion attacks as well as provide operational performance data. A strategy consisting of an effective monitoring solution that can identify problem areas and provide and deliver essential technical information to the right people in a timely and meaningful manner will ease this threat of uncertainty that looms in these times.

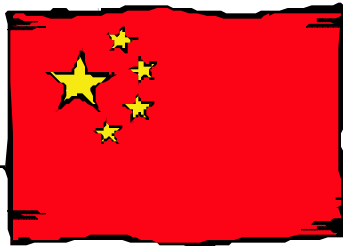
Terrorism Defined

Terrorism is a systematically organized activity with the sole purpose to coerce and gain control. The recent activities in the global arena had made terrorism more blatant and caused many to see the reality and seriousness of its impact.

Telecommunication and broadcast networks are of great importance to national security. It is a medium for armed forces alerts and a means to reach every single resident in the country. Naturally, it is a valuable national asset. With media being the most influential medium for the spread of information, ideas and beliefs, it is not surprising that it is the terrorist groups' fantasy to take control of media. The bad news is, this is no longer a 'fantasy' for them.

Terrorist Attack!

In the midst of the World Cup heat last June, CCTV, the Chinese network, was hacked. Top broadcast officials charged that the June 23 incident took place on the Chinese-run Sinosat satellite – on a channel the government uses to beam TV programmes to remote areas of China that have little access to outside news. A total of nineteen hours of religious messages relating to the Fa Lun Gong was illegally broadcasted. This hijacking of television signals to broadcast Fa Lun Gong messages happened again during events to mark the fifth anniversary of Hong Kong's hand over to China. It was the sixth time since the beginning of 2002 which hackings have taken place on the Chinese airwaves. In 2001, Fa Lun Gong supporters have interrupted cable broadcasts in at least six cities, often simply showing banners that say "Falun Dafa is good" - Falun Dafa is another name for the spiritual movement, which China has denounced as an "evil cult" [1].

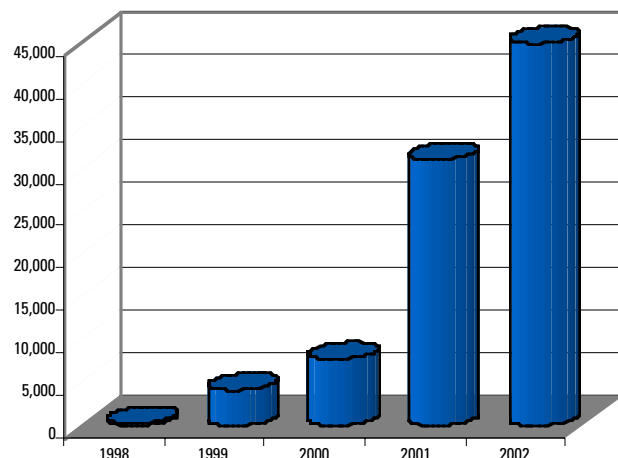


Hacking - A Growing Concern

Hacking into a communication or broadcast network is becoming a serious industry-wide concern. In today's world, the Internet and the television, being the most effective forms of communication in terms of broadcasting information and potential reach or number of receivers, are obvious targets for attack.

According to security experts, hack attacks are on the rise in Asia. Hackers based in Indonesia and Malaysia have been launching digital attacks on neighboring countries. In October last year, the month of the Bali bombings incident, heightened attacks were seen. South Korea, Australia, China, Taiwan and Japan have been the victims of hundreds of hack attacks causing millions of dollars worth of damage. China has suffered estimated damage of more than \$865 million in 2002; South Korea \$449 million and Australia has lost over \$309 million.

The rise in hack attacks is definitely no laughing matter. An estimate of hack attacks made from 1998 to 2002 is shown below [2].



1998	1999	2000	2001	2002
269	4,197	7,821	31,322	>46,000

In both cyberspace and the television world, broadcast terrorism is becoming a real issue. Terrorists are hacking into the network to broadcast tampered content, disrupt a transmission in progress, or corrupt IT and management information. Thankfully, with the use of the right tools and technology, you can fight them.

Keeping The Intruders Out

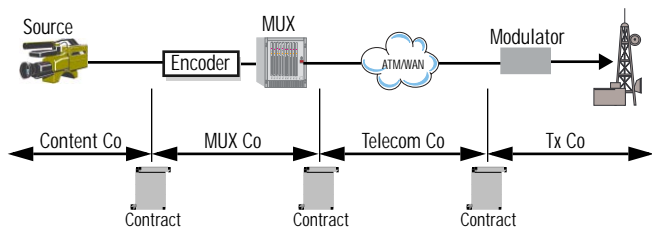
Physical protection of assets used to be the only way people could protect themselves.

However, with the evolution of media and the advance of technology, physical measures such as guards, locks, chains, passwords and alarm systems are no longer sufficient. Advances in technology mean, the intruders need not be physically present to hack into a system – the hacker can be in Brazil and the attacked network in USA.



Take for example the case of the Trippin Smurfs as reported in New Delhi recently. In the heat of the current discussions regarding the US plan to declare war on Iraq, the Islamic Republic News Agency reported that the hacking group, Trippin Smurfs, brought down nine web servers of the US-based premier space organisation, the National Aeronautics and Space Administration (NASA) in protest against the American policy on Iraq [3]. The group put up a 24-line message in not so 'impeccable' language denouncing the US for its determined plan to attack Iraq.

In the broadcast network, there are various points of vulnerability that risk security breach. These can be approached at two levels: internal and external. Internal security threats refer to those that cannot be addressed by technology. Unprotected clients (eg. laptops are not protected when connected to the network) or end-user negligence where there is weak user authentication puts the network at risk of unauthorised access. On the other hand, external security threats refer to technical impingements like hacking. These can take place either within the operational network or on a third party network where there is little or no control. This visibility of what is done outside your network is a concern when a third party engaged down the data transport network is unreliable.

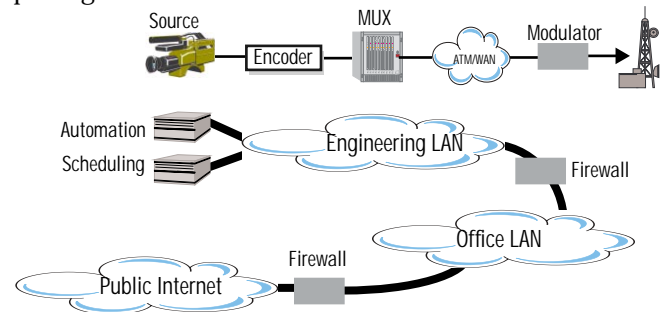


Internal security threats when addressed properly, can protect the network against unauthorised access. Setting the stage on a corporate level, the development of

organisation-wide security policies and education to increase awareness will help to gain staff buy-in, resulting in a environment that has higher security against the 'outside world'. User authentication mechanisms are an easy and relatively simple way to improve security. This may include basic physical efforts like building access identification tags or two or multi-factor authentication (e.g. multiple passwords) for added levels of security. Another technique of security that is gaining popularity is biometrics. Biometrics includes measured physical aspects of a user such as voice authentication, which analyses voice to allow or reject access. Other biometric solutions include thumbprint authentication and retinal scanning.

For external security threats that take place within the operational network, segregation of critical resources are an effective preventive measure. If a virus or worm attacks a network, the damage will be confined to the network under attack. As such, isolated networks – office LAN is separate from the operational LAN where data is transported - help to contain an attack, minimizing damage to the entire network.

Firewalls between each network will help to protect the perimeter and core network infrastructure, thus control network access. This is particularly important where there is access to or from the public Internet domain. Other security tools and measures include Virtual Private Networks (VPNs) for secured connectivity and conditional access tools for data encryption like tunnelling protocols, secure tokens or other methods for protecting and distributing keys to protect data packages.

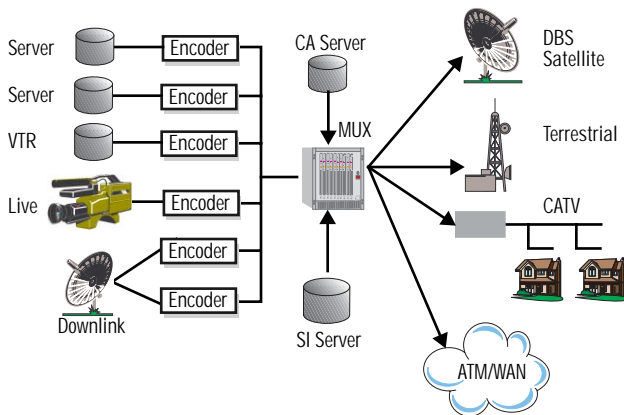


Offenders can attack various points in the data transport stream. They can hack into the scheduling system to influence traffic flow and program schedules, the video server to steal, tamper, or delete information, spread a virus or worm in the systems servers (be it the office servers that is the gateway to the office LANs, automation systems, the video server, or the network management server, the effects of having a virus or worm in the network has unthinkable consequences), make a third party connection into the network or even deploy a satellite hijack to tap and take over airtime, as in the case of China's CCTV in June last year.

In cases where the external security threat is the third party vendor engaged down the data transport network and there is little or no control of this link, the only recourse apart from putting in a security system for the entire video transmission chain, is to have monitoring systems that can provide simple and easy to use operational performance data, placed at multiple checkpoints along the video transmission chain.

Network Complications

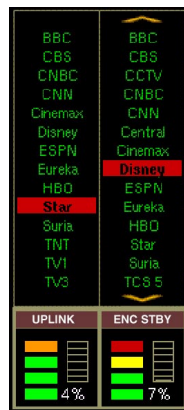
Although there are tools available to build a more secured network, maintaining network security along the transport data stream is not as simple as we hope it to be. This is made complicated by the fact that each link in the video transmission chain might be owned and operated by different companies - certainly the most likely case where the content providers, the broadcaster, the telecommunication company or the satellite owner are different entities. Being separate entities, it is unlikely that there is a unified standard of security throughout the entire video transmission chain. In the case where there is an offensive attack by a hacker, the question then is where in the transport stream did this attack take place and who is responsible for it?



In the situation above, a hacker penetrating the telecom or IP network operator could reconfigure network switches and routers to pass his own malicious content down the chain instead of the proper broadcast content. Alternatively, a rogue element could hijack the satellite transponder (as was the case with the Falun Gong) resulting the wrong content being broadcast to potentially millions of viewers.

A more surreptitious example might be a hostile entity inserting an additional, unauthorized program into the multiplex, or perhaps replacing one out of the many services with their own. Since the hack only affects one out of the many services carried, detection is certainly much more difficult.

In the latter case, since the legitimate and intended content has failed to reach the audience there is no doubt that not only content providers will flip, advertisers could seek hefty compensation. Of course, each link in the transmission chain will claim that it is not their link that failed. As such, it is important to have a strategy that will help parties involved to have a recourse that minimizes their risks. Avoiding possible ambiguous parameters that may lead to unnecessary disputes will put them out of a situation where they will be responsible for something out of their control.



With control of media being a big prize, broadcast integrity is more crucial than ever. The ability to identify security penetration threats is made more complicated by the advancement of television to packet switching and multi-stream technology, and the emergence of MPEG-2 that allows video compression.

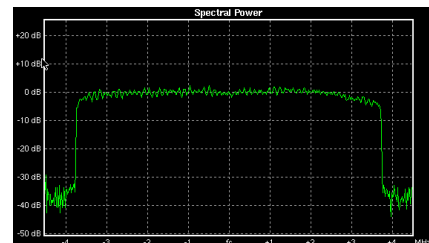
This evolution towards a shared network has caused the dynamics of the television business to be more complex than ever. Each link in the network from the origin of the data to the broadcaster for it to reach the consumer has a delicate close relationship. Unfortunately but true, it only takes one weak link in the video transmission chain to be a welcoming door for the prying eye of the hacker for an opportunity to strike.

Intrusion prevention tools like monitoring and alarm systems help to detect and stop attacks, or at least enable vendors to identify where the attack occurred in the transmission stream. This is particularly important in the broadcast business where the ability to maintain signal quality and program integrity reduces your risk of terrorist attacks.

Error: 2003-6-12 01:09:56.232

**Port 4 (Uplink)
Unknown Service Detected [0x34]**

For television broadcasting, the monitoring must cover the SDI signals that pass through the encoded MPEG and RF signals that reach the viewers' homes. The problem must be isolated by checking each point along the RF, MPEG-2 transport, and multiplex content at each step to identify where the downlink originated. As such, it is necessary to have multiple checkpoints where a monitoring system is deployed so that a critical analysis of system performance can be carried out.



Towards Higher Security

In today's terms, 'network' refers not only to IT infrastructure, but also broadcast and telecommunication. Network security, be it IT or broadcast, is a worldwide concern fundamental to the way we live and do business. When options and solutions for network security are evaluated, it is important for network administrators to consider a system of capable scalability.

There is a need for systems which can identify attacks effectively and provide timely reports for intrusion prevention. Maintaining broadcast integrity in the face of complexity requires a tight monitoring system to provide immediate and timely information to act upon. Network fault and performance alerts should be accessible not only at the monitoring system itself but at locations and in the form appropriate to the organisation. Remote warning alerts of system instability should be made easily available over corporate LANs, the Internet, e-mail and even to pocket pagers and mobile phones via Smart Messaging Systems (SMS). Comprehensive logs should be generated in order that engineers or system administrators get a clear explanation of which system is under attack and when.

References

- [1] CNN.com, 2002, China Broadcast, www.cnn.com/2002/WORLD/asiapcf/east/07/09/china.broadcast
- [2] BBC News, World edition, Technology section, 3 September 2002
- [3] ARNA, New Delhi, Feb 4 2003

For More Information

To learn more about the DVStation, request a demo, or learn how Pixelmetrix might help your optimize video network integrity, contact us today!

On the Internet: sales@pixelmetrix.com
www.pixelmetrix.com

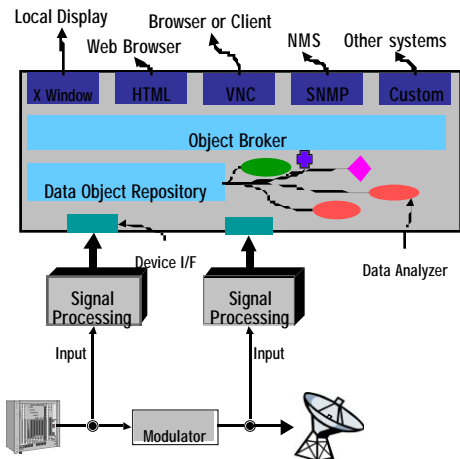
North America: 1-866-PIXEL-US
Europe: +41-79742-7454
Asia Pacific: +65-6547-4935

About the Author
Danny Wilson is president of Pixelmetrix Corporation, manufacturer of the DVStation, a preventative monitoring solution for digital broadcast networks. Mr. Wilson has 15 years previous experience with Hewlett-Packard where he was responsible for the introduction of the MPEGScope transport stream analyzer and the world's first ATM/B-ISDN test system which accelerated the development and deployment of ATM technology worldwide.

The DVStation Family

Pixelmetrix has focused on creating a single self-contained monitoring station that can analyze thousands of parameters within hundreds of digital television signals. Through the use of plug-in modules and parallel processing, we monitor all these parameters in real time, simultaneously and continuously. We've targeted our development efforts to insure the quality of the signal, the integrity of the program service and the delivery of essential technical information to the right people in a timely and meaningful manner.

Our engineers began with a simple premise: Effective monitoring of digital television networks requires the use of real-time, continuous and simultaneous evaluation of hundreds of points along the transmission chain. To receive this necessary network intelligence, adequate data collection, analysis and correlation is needed on three axis – time, layer and geography. Monitoring of all layers – physical, transport, coding, and quality – is essential for a complete maintenance picture.



Plug-in modules allow flexibility and accommodate changes in a fast evolving technical infrastructure. So far, we've focused on three categories of plug-in modules: physical line interfaces (ASI, SPI, RF, ATM etc.); a transport stream processor (TSP); and picture quality processors.

DVStation

DVStation provides monitoring for RF, MPEG-2 transport stream, and content within an easy-to-use and integrated environment. Offering the highest port density in the industry, DVStation is ideal in environments with *many signals in one place* – such as satellite uplink centers, DTH operators, or cable head ends.



DVStation

The design features plug in line interface modules which extract the MPEG-2 transport stream from the native RF or telecom signals and pass that data to a TSP – Transport Stream Processor. All modules provide monitoring capability on the physical layer. For RF interfaces (QPSK, QAM, COFDM, etc.) this provides an easy indication of overall modulation health. The 155 Mb/s ATM optical interface extracts an MPEG transport streams from several VP/VC's in addition to detecting physical layer errors and Sonet/SDH parameters.

DVStation-Remote

Ideal for remote deployments with *a few signals in many places*, the DVStation-Remote consists of a 1U control unit and up to four interface adaptors. Remote diagnostics can be conducted simultaneously from several locations, or alternatively staff can access telemetry directly by attaching a standard keyboard and CRT.



Log files and recorded transport streams can be accessed remotely or downloaded for further analysis.

DVStation-IP

The recent explosive growth and significant technical advances in the Internet has provided broadcasters with a new alternative for program distribution. While IP backbone networks present the promise of the economical delivery of multiple media types **bringing these networks on line still remains more of an art than a science.**



The Pixelmetrix DVStation-IP, a world first of its kind provides advanced video and content analysis and monitoring functionality for IP networks. The compact 1RU form features a multi-speed 10, 100, and 1000 Mb/s interface (gigabit ethernet).

DVStation-Pod

Featuring the same software and user interface of the DVStation and DVStation-Remote, the DVStation-Pod product line consists of several book sized modules containing the interface circuitry. Each module connects to a laptop or desktop PC.



Light and portable, DVStation-Pod offers all the power and functionality of its bigger brothers in an extremely affordable package.