

What are some of the major security characteristics pertaining to tomorrow's wired/wireless multimedia convergence?

by Gregg Zepp

To answer this question, we may wish to consider the technologies to be used when setting up wired and wireless networks. Below is the list of key wired and wireless networking technologies (1).

1. Fiber Technologies (e.g. FTTH, FTTC)
2. Wireless LANs (802.11g/n, 802.16)
3. Wireless MANs (Fixed wireless, LMDS, 802.20)
4. Wireless WANs (3G/4G, GPRS, UMTS, GPS, mesh networks)
5. Short-distance wireless communication technologies (Wireless PAN) (e.g. Bluetooth, 802.15.3)
6. Satellite Systems (e.g. Motorola's Iridium)
7. Sensor networks

With the merging of networks, trust boundaries become dynamic (2). Areas where multimedia technologies are more likely to be merged, such as in medium and large networks, because data would need to travel longer distances, wired networks are most prevalent for the responsibility of long distance data traveling. As networks combine to communicate, perimeter security takes on new meaning.

Hardened routers may have to extend router tables, the list of locked down MAC addresses may have to grow, the number of VPN technologies reduced, more authorizations for web service accounts, more tightly or loosely defined firewall rules, and to keep traffic separate, the installation and configuration of more VLANs (3).

Another technology, packet filtering, which adds overhead, but provides the necessary analysis to monitor traffic as it traverses networks, could be implemented in more places. Technologies in network devices such as Access Control Lists (ACLs) (i.e., Cisco's "access-group" statement), IPchains, traffic rules, blacklisting, ingress/egress filtering are ways of implementing security at the router. Packet filtering firewalls, commonly known as stateful firewalls, utilize packet examining techniques offering the ability to analyze packets at various OSI layers.

Other issues to consider include:

1. Being policy compliant while data traverses various enclaves: SOX, HIPAA, DIACAP, NIST 800-53, FISMA, and state governance such as the Database Breach Notification Act [passed in California].
2. Security of services - as per the new Application Security and Development Security Technology Implementation Guide (STIG) released May 23, 2010, WS-Security (Web Services Security, or WSS) is required for web applications. WSS is a *flexible and feature-rich extension to SOAP to apply security to Web services*. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token

formats, such as [SAML](#), [Kerberos](#), and [X.509](#). Its main focus is the use of [XML Signature](#) and [XML Encryption](#) to provide end-to-end security. (4) The specification allows a variety of signature formats, encryptions algorithms and multiple trust domains, and is open to various security token models, such as:

- *X.509 certificates*
- *Kerberos tickets*
- *UserID/Password credentials*
- *SAML-Assertion*
- *Custom defined token (4)*

3. Security information & event management systems (SIEM) - management of HIPS, OS security policies, A/V, permissions, audit logs, etc need to have a global interface console for aggregate management of multiple security apparatuses.

4. Cross-layer/Cross-domain trusts - protections against malicious nodes which may attack at a certain layer will require modulation of functionalities to guard against boundaries, automate routing decisions, provide traffic detection, conduct node reputation credibility calculations, and provide for local trusts. (5)

(1) Selected Readings on Telecommunications and Networking, 2009; Jairo Gutierrez:
<http://www.igi-global.com/bookstore/TitleDetails.aspx?TitleId=884&DetailsType=Preface>

(2) Cloud Security and Privacy; Tim Mather, Subra Kumaraswamy, & Shahed Latif; O'Reilly Media, 2009.

(3) Inside Network Perimeter Security, 2nd ed; Northcutt et al; Sams Publishing, 2005.

(4) Wikipedia: <http://en.wikipedia.org/wiki/WS-Security>

(5) Article: "Establishment of cross-layer trust model for ad hoc networks"; Proceedings of the 11th international conference on Advanced Communication Technology - Volume 2, 2009.
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04809695>