Interested in learning more?
Check out the list of upcoming events offering "Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec
Security on Internet Satellite - any different than Wired or Wireless?

Nancy Voorhis
SANS Security Essentials
GSEC Practical Assignment - Part 1 (paper)
Version 1.2c
May 28, 2001

Introduction

On May 24, 2001, Michael L. Cook, Vice President and General Manager of Hughes Network System's Spaceway™ global broadband satellite network system testified before the U.S House of Representatives Small Business Committee with the following statement "Our message to you today is simple. The only technology that will ubiquitously provide cost-effective broadband access across the entire United States is satellite technology." Cook was testifying before the committee to advocate further opening of bandwidth licensing to allow their DirectPC product, a satellite Internet service, to reach further into the consumer market place.

There has been increasing discussion and awareness about wireless security. Any number of references point out that the demand to be free of the wire is on the increase. Most information systems professionals would probably agree with Sean P. McAleer that "These [wireless] devices are here to stay" [PCM] and have increasing awareness that wireless systems have vulnerabilities not present in wired systems. These vulnerabilities need to be addressed if the same level of security is to be present on connections regardless of whether they are made across a wired or wireless medium [MCM][CH].

The recent discussion of wireless security has tended to focus on the threats to wireless LAN's, PDA's and other mobile technologies and the new protocols, such as Bluetooth, being developed for wireless. One type of wireless that has not yet received much attention is that of satellite Internet communications. Satellite links have been providing data services for some time now, providing global links for Internet Service Providers and multicast links for video conferencing, distance learning and other IP multicast applications. Development of satellite technology, investment in infrastructure, lowering prices and consumer demand for more bandwidth are bringing satellite technology to the consumer market place, and making it competitive with terrestrial technologies such as DSL and cable services. Announcements such as the one made on May 14, 2001 by Gilat Satellite Networks Ltd. and partners "Star One, UOL and Gilat Satellite Networks’ StarBand Latin America business introduce Brazil's first consumer two-way satellite, broadband Internet service" [GIL] are being made almost weekly and are likely to continue. The Gartner Group states in their January, 2001 report on the future of small and midsize business networking, "Satellite services make sense where other broadband alternatives are unavailable (e.g. rural areas or in less-developed countries)." [GAR]
There are currently 200 operational satellites, with the total predicted to rise to over 2000 by 2008 [TIA].

It seems clear that the use of satellites for providing broadband Internet access to the consumer market has only just begun. So what's the deal? Is satellite just another wireless technology with the same threats and risks as any other wireless technology?

**Characteristics of Internet Satellite Technology**

Broadband Internet Satellite consumer services are currently being deployed using 2 main types of technology. The 2 types of systems are commonly referred to as "one-way" and "two-way" systems. The one-way systems are also referred to as hybrid satellite-terrestrial systems. They require a standard terrestrial link (dial-up or otherwise) and work by sending outgoing requests on the terrestrial link, with inbound traffic returning on the satellite link. Systems typically use a satellite card and a satellite dish installed at the end user site and work in conjunction with a proxy server/gateway which makes the actual request to the destination host and communicates the response back via the satellite. Further explanation of the topology of these systems can be found in the research paper "Asymmetric Internet Access over Satellite-Terrestrial Networks" [ASBD].

More recently being deployed are "two-way systems" which provide a data path for both upstream and downstream data. These systems also use a satellite card and a satellite dish installed at the end user site and bi-directional communication occurs directly between the end user node and the satellite.

Both technologies have asymmetric speeds, providing faster download speeds than upload speeds. Maximum download speeds on systems currently deployed range from 400Kbps - 2200 Kbps and are higher for future planned systems (see Table). Upload speeds for one-way systems are based on the speed of the terrestrial link, while upload speeds for two-way systems range from 20 Kbps - 20 Mps. The speeds experienced by users can be affected by atmospheric conditions, and actual speeds reported by users vary considerably.

More technically, communication satellites being used to provide broadband Internet access are commonly Geostationary Orbit (GSO) or Low Earth Orbit (LEO) orbiting at 22,300 m and less than 1000 miles respectively, as well as Middle Earth Orbit (MEO) satellites. Satellite signals are currently limited to the operating in the C band (6GHz (uplink) and 4GHz (downlink), in the Ku band (14/12 GHz) and the Ka band (30/20 GHz).

Several key differences exist between satellite and other wireless technologies. One of the major differences is the long distance the signal must travel between earth and the satellite. The longer the distance, the longer the propagation time for the signal, creating
latency (delayed response time) at the end user node. Using satellites that are closer to
the earth (LEO) to reduce propagation times requires using additional techniques to
address the use of multiple satellites to provide continuous cover at the user (terrestrial)
node. Another difference in the technology, also due to the distance the signal must
tavel, is that the link has a decreasing signal-to-noise ratio with increasing distance. This
results in susceptibility of the link to atmospheric effects such as rain, distortion created
by large objects such as buildings being in the path and higher error rates. A further
difference is that satellite links have considerably higher bandwidth potential available.
The theoretical throughput for VSAT systems is 40 Mbps downstream and 76.8 Kbps
upstream and satellites planning to be deployed have even higher rates.

Security Threats

What do these differences imply in terms of security? Do the risks differ than those for
wired or wireless? Is it not possible to use the techniques that are available for assuring
the integrity, confidentiality and authenticity of data travelling a wired and wireless
medium on satellite links? While some of the threats on a satellite link include those for
wireless LANs [MCM], satellite transmission has unique characteristics that demand
security be approached and solutions found which are specifically for satellite
transmissions.

Similar to wireless communications, one of the threats to the confidentiality of the data is
the potential for eavesdropping on the satellite link. The threat of eavesdropping is far
greater than on a land link, given that eavesdropping can occur without detection
anywhere within the location within the range of reception. For satellite links, this range
is large, very large. Eavesdropping could also be used to launch an availability attack
[NASA1].

In general, the systems all use some combination of access technologies, which are
required to share the satellite channel amongst many ground receivers. These are code
division multiple access (CDMA), time division multiple access (TDMA) and frequency
division multiple access (FDMA) and their variations, and make it "at least as difficult as
it will be to intercept a digital cellular signal" [BYTE]. Additional deterrents are "that
the resources needed to monitor a satellite link are not trivial" [NASA1]. Also in use is
the technique of frequency hopping such as that used in the "Bluetooth" wireless
standard, which is a deterrent, but is more effective when used in conjunction with an
encryption scheme [CH].

All of the satellite systems being deployed and planned for include a terrestrial
component: a proxy gateway in the one-way systems or a satellite hub as in the StarBand
two-way system. This introduces the same threats that exist for wired communications as
the data also will travel across standard terrestrial links and requires that end-to-end
security mechanisms should be considered [NASA1].
Issues arise when considering end-to-end security mechanisms for satellite links. Just use a Virtual Private Network (VPN), right? Well, not exactly. The latency in the satellite signal has caused considerable research to be done into enhancing the parameters used for TCP packets in order to boost the performance. Some of the techniques being used impact the ability to apply end-to-end security to the link. TCP Spoofing is a technique that allows splitting of the TCP control link, isolating the satellite portion of the TCP/IP link from the terrestrial portion and allows modifications to the TCP parameters used for the satellite portion of the link, such as window size, that are optimized for the characteristics of the satellite link [ASBD]. According to research done by Byte Magazine's John Montgomery in 1997 and Hughes Network System's (HNS) Dennis Conti, "HNS has been using this technique for over three years to deliver Internet/intranet content at high speed to both consumers and enterprises" yet there exists research which indicates that "this [TCP spoofing] protocol is currently incompatible with end-to-end IP security protocols." [ATM]. In some cases, such as the DirecPC system, a VPN is already in use and therefore the customer cannot set up their own VPN (see Table).

Another technique being suggested by research for improving the performance of TCP over the satellite link is the extension for transactions (T/TCP). This technique would allow data to be sent along with the initiating SYN packet of the TCP connection. Along with the recognition of the potential for decreasing the TCP connection setup time is also the recognition of security implications that have already been identified with sending data in the first segment. [NASA2]

Initially Deployed or Planned for Deployment Satellite Systems

The table below lists some of the main characteristics of a sample of Internet Satellite consumer services currently deployed or planned for deployment. Any information regarding the security of a system that was stated at the product web site, press release information or that was determined to be available to an average consumer is listed. The availability of the information regarding the security measures being deployed are given a rating (poor, medium, good), reflecting the ease with which security information is obtainable.

Table: Main Characteristics of a Sampling of Internet Satellite Consumer Services

<table>
<thead>
<tr>
<th>System Name</th>
<th>DirecPC</th>
<th>DirecPC Satellite Return</th>
<th>Starband</th>
<th>GSI</th>
<th>AstroLink</th>
<th>Internet-In-The-Sky</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Type</td>
<td>one-way</td>
<td>two-way</td>
<td>two-way</td>
<td>one-way</td>
<td>two-way</td>
<td>two-way</td>
</tr>
</tbody>
</table>

© SANS Institute 2000 - 2002
As part of GIAC practical repository. Author retains full rights.
<table>
<thead>
<tr>
<th>Satellite Type</th>
<th>GEO</th>
<th>GEO</th>
<th>GEO (Gilat GE-4 or Telstar 7)</th>
<th>GEO</th>
<th>GEO</th>
<th>LEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectrum</td>
<td>unknown</td>
<td>unknown</td>
<td>Ku-band/ C-band</td>
<td>Ku-2 band (business solution)</td>
<td>Ka-band</td>
<td>Ka-band</td>
</tr>
<tr>
<td>Date of Deployment</td>
<td>currently available</td>
<td>currently available</td>
<td>currently available</td>
<td>currently available</td>
<td>2003</td>
<td>2005</td>
</tr>
<tr>
<td>Target Market</td>
<td>consumer</td>
<td>consumer</td>
<td>consumer</td>
<td>consumer, business</td>
<td>corporate, government</td>
<td>not specific but includes &quot;e-commerce, telemedicine, sales support&quot;</td>
</tr>
<tr>
<td>Download speed (maximum)</td>
<td>400 Kbps</td>
<td>2200 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>155 Mbps</td>
<td>64 Mbps</td>
</tr>
<tr>
<td>Upload speed (maximum)</td>
<td>n/a</td>
<td>128 Kbps</td>
<td>150 Kbps</td>
<td>n/a</td>
<td>800 Kbps, 4 Mbps, 20 Mbps</td>
<td>2 Mbps</td>
</tr>
<tr>
<td>Field tested speeds reported from user base (average)</td>
<td>200 Kbps</td>
<td>2166/19 Kbps (off peak - 5:30AM Sunday)</td>
<td>none</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>System security as stated in marketing information or by company contact</td>
<td>&quot;56-bit DES (Digital Encryption Standard) to encrypt information flowing between a modem and gateway to the Internet&quot; &quot;DirecPC also uses CAS (Condition Access System) to provide one more layer.&quot;</td>
<td>none</td>
<td>&quot;certain applications do not perform efficiently in a satellite-delivered environment, such as ...VPN services...&quot;</td>
<td>&quot;Data transmitted through the GSI satellite link uses the most secure encryption method of data transport currently available. GSI provides the functions of a traditional firewall since the only inbound access from the Internet is &quot;customers will be able to configure virtual private networks (VPN's)&quot;</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>
"Because DIRECPC is already using VPN  
You can not use VPN on it."

anti-virus protection of WinProxy,  
StarBand users can be protected  
against Internet intruders and  
Web-borne viruses."

"prefer not to discuss our security measures"  
[SDC]

downloaded information through the  
satellite connection."

Gateway login client provided employing 128-bit  
encryption and Mac HW address  
authentication.

<table>
<thead>
<tr>
<th>Availability of security information</th>
<th>medium</th>
<th>poor</th>
<th>poor</th>
<th>good</th>
<th>good</th>
<th>poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>direcpc.com</td>
<td>directpc.com</td>
<td>starband.com</td>
<td>gilat.com</td>
<td>rapidwireless.com</td>
<td>networkalpha.com</td>
</tr>
</tbody>
</table>

The table indicates that there is limited information available regarding the security measures being deployed. In some cases, the information is somewhat misleading. For example, the StarBand information implies that a firewall at the end user node provides security. While a firewall is a recommended security measure for a satellite link which is an 'always on' connection, it functions only to prevent inbound attacks, and does not address link transmission security. The development and deployment of security measures seems much the same as in 1997 when Byte magazine's John Montgomery reported "All the vendors I spoke with told me that they were aware of the potential security concerns that customers would have. Few, however, had concrete solutions".

Conclusion

On the horizon, is the potential for large number of consumers to be using satellite links to do everything they currently do "on the Internet", including financial transactions and e-commerce. The need to ensure the security of their data is critical. A glance at the technology indicates there is a need for increased awareness both by companies
deploying the technology and consumers using the technology of the need for the
deployment of end-to-end security.

While larger organizations are quickly becoming familiar with the unique aspects of
security risks posed by wireless connections and are integrating security for wireless
connections into their security policies, other consumers targeted by this new market
need more information from the companies deploying the technology about the security
measures being used on the system. There is also a need for increasing consumer's
awareness of the security threats posed by an Internet satellite service.

The large bandwidth available in a satellite link allows the possibility of applying
techniques of strong encryption and authentication that use processing and bandwidth
which may not be feasible for typical wireless LAN or PDA like devices. Techniques
being proposed for wireless links are frequently based on the premise that there are
"limitations in bandwidth, CPU and memory resources, battery life and user interface"
[VERI]. There is a need for development of security services that are unique to satellite
systems, that can take advantage of the characteristics of satellite links, and can
specifically address the modifications being made in the TCP/IP protocol to enhance the
performance over satellite links. It's not just another wireless technology.

References

[MLC] Cook, Michael L. "Eliminating the Digital Divide… Who Will Wire Rural
America?" http://www.hns.com/news/pressrel/cook_testm_5-24-01.htm Hearing before
the U.S. House of Representatives Committee on Small Business Subcommittees on
Regulatory Reform and Oversight and on Rural Enterprises, Agriculture and Technology,


[GIL] "Star One, UOL and Gilat Satellite Networks' StarBand Latin America business
introduce Brazil's first consumer, two-way satellite, broadband Internet service".

[TIA] Highlights of the Workshop on Global Assessment of Satellite Communications
Technology and Systems. http://www.tiaonline.org/about/satellite_workshop.cfm,

http://www.sans.org/infosecFAQ/wireless/wireless_sec.htm, SANS Information Security


[SDC] Phone and email communication with Sandy Colony, Starband Communications, May 21, 2001.
