Pipeline
Knowledge Is Power

www.pipelinepub.com **Volume 6, Issue 3**

Manning the Watchtower: The Security Aspect of Network Monitoring

By Tim Young

"He is most free from danger who, even when safe, is on his guard." -Publilius Syrus, First Century, BC.

Network monitoring, as the many and experienced voices in this month's issue of Pipeline prove, is a valuable thing. It's crucial to maintain awareness and, therefore, control of the activity taking place on your network for a variety of reasons. Communications being a business, the chief reason is generally going to be to maintain profitability by ensuring QoE to end users, recognizing leaks in the system, rescuing stranded assets, and so forth. However, we cannot forget the security implications of network monitoring. Fraud, malice, and policy violations are a serious threat to the security of a company and, in many cases, have deeper implications for the wider security of entire nations and regions.

Maintaining profitability is what makes network monitoring mission-critical to the bottom line. Maintaining security is what makes network monitoring mission-critical to the safety of companies and the wider world.

A wide world of threats

Warfare and terrorism are painful realities of the material world around us, but are, of course, unwelcome residents in the cyber world, as well. ""Our CSP customers tell us that the security threats they face today are global, both on the economic and political fronts", Les Niles, VP of Product Management for Narus Systems (a firm dedicated to network monitoring with extensive work of the security side) told Pipeline. "These threats are becoming more and more complex and difficult to detect as new types of attacks, ranging from network-based to application-based, are unleashed almost daily." Some specific areas that are being threatened by cyber attacks, according to Niles, include critical infrastructure (water, power, banking), sensitive information (which can be obtained through cyber espionage), and the networks themselves, which can be shut down to disrupt the conduct of business and the workings of the media, and can even be made to play unwilling host to the political messages and propaganda of the attackers.

Sources at Narus point to an alarming increase in cutting-edge threats like polymorphic worms, zero day attacks (attacks perpetrated on software prior to the first day of vendor awareness that a security problem exists—the "zeroth day" of knowledge), and a movement from flood-based to application-based attacks.

However, it should be noted that just a few weeks ago, a number of media outlets were whipped into a frenzy over a DDoS (distributed denial of service) attack against US and South Korean websites that was reported by many to have been perpetrated by the North Korean government. US Representative Pete Hoekstra (R-MI) urged retaliation, claiming that the attack couldn't have been perpetrated by amateurs and that a "show of force" was needed. However, Kim Zetter of Wired Magazine pointed out, following the attacks, that the source of the traffic that flooded the sites, causing outages, was a "pilfered five-year-old worm … under the control of an unsophisticated hacker who apparently did little to bolster his borrowed code against detection." In the weeks since, it has come to light that, while North Korea may have been behind the attacks, none of the activity can be traced back to anyone inside North Korea. It is likely that the perpetrator was someone sympathetic to North Korea residing outside of that nation.

So, certainly, attacks are becoming more advanced, or are at least capable of becoming more advanced, but the case of the 5-year-old worm and the (possible) weekend-warrior hacker prove that an attack doesn't have to be sophisticated to cause serious concern and drum up fears of an impending cyber war.

Furthermore, threats are becoming much easier to become exposed to. Noted iPhone hacker and security consultant Charlie Miller spoke at the Black Hat conference in Las Vegas July 30, and demonstrated how a malicious SMS text can disable an iPhone, and a series of texts can, effectively, take the phone over. The attack is particularly insidious because all a hacker would need would be the phone number of an iPhone user, which is readily available.

Cracking the problem

So what are service providers doing about this combination of new threats and old threats that seem determined to continue their destructive habits? Well, whatever they're doing, they're not talking about it an awful lot. Barbara Lancaster, an analyst with LTC International and a Contributing Editor with Pipeline relates a story from a recent panel discussion at a conference she attended. "For about an hour and a half, the panelists talked about everything but security," said Lancaster. "When the Q&A came around, someone stood up and said 'I work in security, and none of you has said a word about security. What's the matter with you?'" Lancaster said that the panelists looked at one another for a little while until one of the panelists came back with the answer that "security is table stakes." Of course, they said, it's mission-critical, but everyone knows that and it isn't worth talking much about.

However, is that the case? Is security a given and not necessarily worth further discussion? Lancaster didn't seem to buy that answer, and I don't think many in the OSS/BSS world would, either. The truth is that not all networks and all systems are protected as well as they should be, but who would ever use security as a differentiator? Trevor Hayes, also with LTC International, pointed out that "in order to say that your security is better than everyone else's security, you'd have to point to specific examples, and, by doing so, expose weakness." No one wants to do that, so security remains the elephant in the room.

However, that's not to say that some firms aren't working diligently on the issue. In addition to Narus, firms like Openet, Sandvine, Zeugma, Camiant, and others are exploring the security and lawful intercept side of network monitoring all the time, attempting to increase visibility to ultimately allow service providers to eliminate threats. "We see more and more network monitoring solution vendors leveraging their network monitoring capabilities and moving into the network and application security analysis area," said Narus's Niles. "Their installed base of network monitoring technology provides the network instrumentation or data collection upon which the new security analysis applications can be built. These applications can co-exist with the quality assurance and similar existing applications."

Firms with background in real-time traffic monitoring, like Narus and Openet, can expand into the security space by using what they already know to monitor and analyze network traffic, and to detect and mitigate anomalous or malicious traffic, while alerting to the presence of the traffic and determining policy to deal with that traffic. "Communications Service Providers need to put more effort into understanding the behavior of their network," said Niles. "There is no longer a clear distinction between networks and the applications and services enabled by those networks. This means that CSPs need to take a holistic, unified approach to protecting and analyzing the behavior of their networks and services."

The Implications

In fact, DPI for the sake of security has been in the news lately as allegations have emerged that Iran's government used deep packet inspection (DPI) software from Nokia-Siemens that was intended for lawful intercept purposes to stifle free speech. While NSN has no control over how their software is used by the entities that purchase it, the entire episode brings DPI to the forefront of wider public awareness, and not in a particularly flattering way. However, this brings to mind the fact that a tool is only as noble as the person (or government) that wields it. And how, praytell, can lawful intercept tools be kept from the lawless?

That's yet another question that confronts the world of communications security as it rolls into a future that's plagued by potential problems that can only be controlled through constant vigilance.