

WHITE PAPER

# Securing the Global Networking Infrastructure

Andy Ogielski, PhD



Critical logistics and infrastructure, from the U.S. government's supply chain to the North American power grid, depend increasingly on secure and reliable network connectivity. New mandates have ordered the interconnection of highly sensitive networks, making each network's security interdependent on the others. Nearly all non-classified networks rely on transit routes across foreign networks into which there may be little or no visibility. In an increasingly interconnected environment, problems and vulnerabilities in any one network can impact them all.

Today, the end users and organizations responsible for critical communications and command of physical infrastructure have little or no control over what happens on the networks that interconnect them. Current security systems focus on perimeter defenses for user and application security. As such, they generally overlook fundamental vulnerabilities in IP network routing. The policies that control routing decisions are typically difficult to maintain and are almost never coordinated from one network to the next. The Border Gateway Protocol (BGP) can be fooled using a range of attacks, and routing policies are often wrongly configured or even maliciously reconfigured. These basic vulnerabilities can lead, and have led, to significant losses of connectivity and control.

Lacking visibility into the state of network routing, organizations can do little to defend against attacks on the routing infrastructure or stabilize and secure their routing policies. If these organizations had transparent visibility across all of their networks of interest, they could spot open vulnerabilities, identify attacks and policy errors as they occur, and mitigate the potential for and impact of critical connectivity failures due to attack or error. A system that can monitor routing on networks of interest, regardless of who controls them, is necessary to secure global, interconnected communications networks and the Internet.

Renesys Corporation, a leader in Internet monitoring, delivers global situational awareness services and solutions for the public Internet as well as for private and sensitive network environments. As part of its web-based subscription service, Renesys operates a large, distributed sensor network that monitors, aggregates and correlates routing information from the public Internet. From this sensor network, Renesys performs significant fusion of data to reconstitute a global network view from hundreds of local views using sophisticated algorithms and intelligent software. Renesys solutions are proven in critical government network environments and are available today.

## **Facing The Internet's Security Challenges**

The Internet is not one well-defined entity controlled by a single authority. It is a loose confederation of public and private IP networks that have voluntarily interconnected—and continue to do so—at an exponential rate. With few exceptions, these globe-spanning public and private networks are built atop a small set of common packet routing technologies: the “ground rules” that all networks agree upon for exchanging traffic and moving it toward its final destination.

Chief among these critical technologies is the BGP. BGP does not incorporate particularly stringent security or authentication features. It was designed to make it simple to interconnect two networks, allow them to exchange maps of what's available on either side of the new interdomain gateway, and implement local policies for allowing appropriately addressed traffic to flow through it.

As the number of interdomain gateways, or border routers, has increased exponentially, the complexity of policy management has emerged as a serious challenge. When policies are uncoordinated or erroneously configured, they can cause routing instability, trigger connectivity outages, or even open doors for specific types of network attacks.

Network connectivity failures, whatever their cause, can create significant, real-world problems, affect the stability of the economy, and impede the effective functioning of government. A long list of lifeline services depends on secure and reliable networking, including control over power plants, dams and the national power grid; shipping, trains and the air traffic control system; food, water and energy distribution; commerce and the financial system; law enforcement, public safety, and emergency response; supply chains and logistical processes; and both military and intelligence communications.

As the number of high-value targets continues to grow, attackers are becoming more determined and sophisticated. Meanwhile, as interconnections among critical networks proliferate, policy inconsistencies and configuration errors at the borders make large scale failures nearly inevitable. Protecting national infrastructure, commerce and communications will require that all stakeholders work together to monitor, detect, and manage the impacts of these attacks and failures.

### **Threat Model: Exploiting the Internet's Failure Modes**

Attacks and policy errors create their biggest problems when they cause organizations to lose control over or become unable to connect to their "networks of interest." A network of interest may be defined as any network that is critical to an organizations' communications, control over physical infrastructure, or ability to conduct operations. The revolution in global interconnectivity is expanding the number of networks of interest for all network operators. Vulnerabilities or failures in any one could have notable affects on them all, because of the nature of the BGP and the ways in which its routing policies are configured.

Attacks on the Internet's routing infrastructure fall into three major categories. The first involves local or distributed attacks where routing update messages are crafted deliberately to exploit the trusting nature of the BGP protocol. This can include spoofing advertised BGP routes, injecting inauthentic routes or withdrawing legitimate routes, or rewriting the policies that control route forwarding. They can also include the forced withdrawal of routes by simulating unstable connectivity on upstream routers; the distribution of an excessive number of erroneous routes to legitimate networks to force routers to drop authentic routes; "blackholing" networks by advertising routes to them with an inauthentic origin; and filtering out the redistribution of legitimate routes. Any of these types of attacks can lead to widespread losses of connectivity and traffic disruptions, as the misinformation injected by the attacker propagates throughout the global routing system.

A second category of attacks includes denial of service or resource depletion attacks. In these cases, attackers create surges in traffic that cause collateral damage to the routing infrastructure, either by forcing session time-outs due to congestion or by overloading routers' CPUs or memory. As smaller edge routers yield to the attack by crashing or rebooting, performance impacts can spread to the core routers that must cope with the resulting global cascade of re-routing messages. Examples have included the Slammer worm in January 2003 and the Nimda worm in October 2001, each of which resulted in widespread routing instability.

A third type of attack involves the physical destruction of carefully selected cables or peering facilities. This kind of physical attack may fall outside of the traditional realm of network security, but the formulation of an appropriate defensive strategy would be incomplete without an understanding of the network's ability to route around very carefully targeted damage.

We know that the potential for very great damage exists, because these failure modes have already been demonstrated in practice.

The most effective way to defend against routing attacks and routing policy errors is to gain transparent views from one's own networks into interconnected networks of interest. Attaining an outside-in perspective requires an entirely new approach to network security that moves beyond myopic perimeter defenses and provides a continuous, global view of the relevant networking infrastructure, its routes, and its responses to configured policies.

Current security methods do not utilize this sort of outside-in approach. Most focus on patching specific, known vulnerabilities or creating complex defense perimeters that can be, and often are, defeated. A clear co-evolution of threat and response is taking place, much like a networking arms race. For every defense mechanism that is put in place a new means of attacking or defrauding systems is invented. Given the essential impossibility of eliminating routing policy instabilities and preventing malicious attacks altogether, it seems clear that an effective security approach must incorporate continuous, global monitoring and threat analysis.

## Power Generation Control Systems

The electric power generation and transport industry relies on highly networked supervisory control and data acquisition (SCADA) systems to collect information, control power generation, manage distribution, and provide other functions critical to the health of the North American power grid. Given the widespread impacts of the 2003 blackouts, it's easy to see why this set of systems must be protected from potential network attacks as well as connectivity failures.

## Mississippi River Locks

When the Code Red worm hit the Internet in 2001, the Department of Defense (DoD) responded by disconnecting its unclassified NIPRnet from the public Internet. What the DoD overlooked, however, was that the Army Corps of Engineers needed Internet connectivity to maintain control over the locks on the Mississippi River. Without connectivity and control over the locks, shipping could be disrupted on one of the nation's busiest and most critical waterways.

## Presidential Daily Briefing

According to declassified documents, the National Security Agency (NSA) experienced a "catastrophic network outage" in January 2000 which lasted three and one-half days. The outage affected the "signals intelligence information available to national decision makers and military commanders." The impacts of this outage went as far as the White House, where as much as 60 percent of the President's Daily Briefing depends on the NSA's SIGINT network. For three days the briefing was significantly limited in its scope as a result of this loss of connectivity.

Sources: [1,2] Benioff, Marc R. et al. Cyber Security: A Crisis of Prioritization; President's Information Technology Advisory Council; Feb 2005 [3] National Security Agency/Central Security Service, Transition 2001 (Declassified); Dec 2000, p.33.

## "Inside" vs ."Outside" Becomes Irrelevant

The basic philosophy behind traditional network security holds that systems "inside" the perimeter must be protected from "outside" attackers. In other words, if networks were castles, their security would rely almost entirely on building thicker walls and deeper moats. But if the roads between them were full of bandits, then commerce would collapse, and the castles with it.

In an interconnected world, particularly where remote access is increasingly important, the division between "inside" and "outside" disappears. Guarding the castles requires the construction of multiple observation posts that watch not only the points of ingress and egress, but also all of the routes into, out of and between interconnected networks. Transparent observation of both home and transit networks is critical for safeguarding communications infrastructure that relies on carrier transit and the public Internet. Fortunately, the necessary observation posts already exist in the Internet, and the challenge is to turn raw sensor data into actionable information.

## Distribution of Routes with False Origins

On December 24, 2004 the Turkish national telecom operator, TNet, began advertising routes to more than 100,000 otherwise legitimate networks for more than an hour, claiming to be their true owner and the best destination for their traffic. Although TNet typically originates only about 200 routes, they peer with several international backbone networks, some of whom helped to propagate the 100,000 inauthentic routes. The results ranged from destabilized routing in some networks to complete "blackholing" of others. Both the injection of unauthorized routes and advertisement of routes with an inauthentic origin can cause a widespread loss of control in interconnected networks.

## Accidental "Blackholing" by Origin Hijacking

It's common for events that look very much like attacks to be caused by misconfiguration errors. One well-known web monitoring company's routes were stably advertised from its Plano, Texas datacenter via two stable providers, UUnet and AT&T, until June 9, 2004. On that afternoon, a clerical error resulted in a misconfiguration, advertising the customer's routes as routes to

AT&T's own network. All packets intended for this customer were "blackholed" for more than six hours before the erroneous route could be identified and withdrawn, causing a catastrophic outage.

### **Massive Long-term Transit Failures**

Even the largest and best-run provider networks are not immune to meltdown. In 2002, a massively failed upgrade of routers in the UUNET network had a worldwide impact that affected hundreds of large corporations and millions of people for more than 8 hours. In that same year, a large nonclassified US government network suffered a "meltdown" as a result of transit problems at its interconnection points with Qwest's network in the US. Over a 24 hour period, users experienced an extended series of 30 to 40 minute migrating outages separated by flaps (periods of unstable connectivity). Without visibility into the global routing infrastructure—the world outside their borders—network operators had very limited opportunities to understand the problems they faced, let alone work effectively with Qwest to fix them.

### **Gaining Global Situational Awareness by Correlating Local Views**

Whatever one wants to interpret in networks of interest, be it signs of an attack, erroneous routing policies, or problems in route advertisement, it is necessary to have an instantaneous, valid map of those networks and how they exchange traffic. This map can only be derived from bringing together information from multiple observation posts or sensors. For instance, the Turkish Telecom event described above was immediately identifiable by the sudden, radical increase in the number of networks they claimed as their own. A locally focused security system, however, might never have detected the sudden change in the Internet's routing map.

Because networks of interest change rapidly, any attempt to map them must be kept up to date in real time, or in short intervals. Keeping the map in-step with the networks it monitors—including the public Internet—supports global situational awareness. It shows the behavior of critical networking infrastructure and allows rapid identification of malicious or problematic activities. The system that builds and manages this map must provide real-time alarms on factors like inter-domain connectivity, should it be denied or fail, and other security problems such as intrusions, advertisements of inauthentic routes, or faulty policies that destabilize routing.

The global view can be constructed through aggregation and correlation of many local views by utilizing a multi-point approach to gather many streams of independent routing traffic, fusing and correlating them for joint analysis. These local views can be derived from BGP router activities and other local security mechanisms. The aggregated, global view provides the ability to perform broad analysis of trends and events. With archiving it can provide a record for future comparison and investigation.

Altogether the amount of data involved is massive. To keep any solution practical, multi-resolution views and reports ranging from granular detail to large-scale views are necessary in order to examine specific communities of interest. For example, the DoD might have a view of all of its networks and of the global Internet, but at a particular time will want to see only specific routes or networks that relate to one particular service or theater. With a navigable, filterable map, an organization can monitor all of its routing in detail to ensure that its policies are configured correctly and are not being misconfigured, exploited or altered by attacks.

## **Networking Infrastructure Security Solutions Available Today**

Renesys Corporation, founded in 1999, offers a unique set of services and solutions that help government agencies and private enterprises secure their networks of interest on a global basis. As part of a service that can help to secure the Internet's routing infrastructure, Renesys operates a globally distributed sensor network that monitors, aggregates and correlates BGP routing information to provide an instantaneous, global map of the Internet. This BGP routing information is gathered largely through agreements with the major network operators. Importantly, because the approach focuses on passive monitoring of routing infrastructure, it does not interact with or otherwise interfere with enduser application traffic or sensitive communications.

Renesys offers subscription-based access to the global Internet map through a web portal, and can also deliver XML-based web services for integration into existing systems or portals. Renesys performs significant fusion of data to reconstitute the global view from hundreds of local views using sophisticated algorithms and intelligent software. Effective reports and interactive tools then put that intelligence on the desktops of network operators and security analysts, where it provides critically important situational awareness during times of network instability or attack. Renesys has a proven track record of working with large government organizations responsible for sensitive network environments, and providing the common global perspective that makes network interconnection safer and more manageable.

---

Andy Ogielski, PhD, is co-founder, president and chief scientist at Renesys Corporation. He can be reached at [ato@renesys.com](mailto:ato@renesys.com).



**CORPORATE HEADQUARTERS**

1750 Elm Street, Suite 101  
Manchester, NH 03104

T +1.603.643.9300 F +1.603.623.1623

[www.renesys.com](http://www.renesys.com)  
[sales@renesys.com](mailto:sales@renesys.com)