Background White Paper NETGLADIATOR

In February 2012 we released a product to automatically detect and prevent a web application hacker from breaking into a private enterprise. What follows are the details of how this product was born. If you are currently seeking or researching intrusion detection & prevention technology (IPS), you will find the following quite useful. Like many technology innovations, our IPS solution, NetGladiator, resulted from the timely intersection of two technologies.

Technology #1

About one year ago we starting working with a consultant in our local tech community to do some programming work on a minor feature in our NetEqualizer product line. Fiddlerontheroot is the name of their company, and they specialize in ethical hacking. Ethical hacking is the process of deliberately hacking into a high-profile client company with the intention of exposing their weaknesses. ***The key expertise that they provided was a detailed knowledge of how to hack into a network or website***.

Technology #2

Our NetEqualizer technology is well known for providing state-of-the-art bandwidth control. While working with Fiddler on the Root, we realized that our toolset could be reconfigured to spot, and thwart, unwanted entry into a network. A key piece to the puzzle would be our long-forgotten Deep Packet Inspection technology. DPI is the frowned-upon practice of looking inside data packets traversing the Internet.

An ironic twist to this new product journey was that, due to the privacy controversy, as well as finding a better way to shape bandwidth, we removed all of our DPI methodology from our core bandwidth shaping product four years ago. Just like with any weapon, there are appropriate uses for DPI. Over a lunch conversation one day, ***we realized that using DPI to prevent a hacker intrusion was a legitimate use of DPI technology.*** Preventing an attack is much different from a public ISP scanning and censoring customer data.

So how did we merge these technologies to create a unique heuristics-based Intrusion Prevention System (IPS)?

Before I answer that question, perhaps you are thinking that revealing our techniques might provide a potential hacker or competitor with inside secrets? More on this later...

The key to using DPI to prevent a hack revolves around 3 essential facts:

1) A hacker MUST try to enter your enterprise by exploiting weaknesses in your normal entry points.
2) One of the normal entry points is a web page, and everybody has them. After all, if you had no publicly available data there would be no reason to be attached to the Internet.
3) By using DPI technology to monitor incoming requests and looking for abnormalities, we can now reliably spot unwanted intrusion attempts.

Our greatest advantage relative to other IPS devices is that we do not issue false positives or provide thousands of distracting alerts throughout the day. Nor do we block legitimate requests or break web functionality.

We do one thing very well - we catch & stop hackers during their information discovery process - keeping your web applications secure.

Art Reisman, Co-founder & CTO, APconnections, Inc.

When we met with Fiddler on the Root, we realized that a normal entry by a customer and a probing entry by a hacker are radically different. A hacker attempts things that no normal visitor could even possibly stumble into. ***In our NetGladiator solution we have directed our DPI technology to watch for abnormal entry intrusion attempts***. This involved months of observing a group of professional hackers and then developing a set of profiles which clearly distinguish them from a friendly user.

What other innovations are involved in a heuristics-based IPS?

Spotting the hacker pattern with DPI was only part of a complete system. We also had to make sure we did not get any false positives - this is the case where a normal activity might accidentally be flagged as an intruder, and this obviously would be unacceptable. In our test lab we have a series of computers that act like users searching the Internet, the only difference is that we can ramp these robot users up to hyper-speed so that they access millions of pages over a short period of time. We then measured our "false positive" rate from our simulation and ***ensured that our false positive rate on intrusion detection was below 0.001 percent***. NetGladiator is different than other IPS appliances. We are not an "all-in-one solution", which can be rendered useless by alerting you thousands of times a day, can block legitimate requests, and break web functionality. We do one thing very well - we catch & stop hackers during their information discovery process - keeping your web applications secure. NetGladiator is custom-configured for your environment, alerting you on meaningful attempts without false positive alerts.

We also had to dig into our expertise in real-time optimization. Although that sounds like marketing propaganda to impress somebody, we can break that statement down to mean something. When doing DPI, you must look at and analyze every data stream and packet coming into your enterprise; skipping something might lead to a security breach. Looking at data and analyzing it requires quite a bit more CPU power than just moving it along a network. Many intrusion detection systems are afterthoughts to standard routers and switches. These devices were originally not designed to do computing-intensive heuristics on data. Doing so may slow your network down to a crawl, a common complaint with lower-end affordable security updates. We did not want to force our customers to make that trade-off. ***Our technology uses a series of processors embedded in our equipment all working in unison to analyze each packet of Internet data without causing any latency***. Although we did not invent the idea of using parallel processing for analysis of data, we are the only product in our price range able to do this.

NetGladiator detects & prevents these network breaches…

Administrative interface login brute forcing
Denial of Service (DoS) attacks
Directory Traversal
Login brute forcing
Reflected HTTP redirects
Reflected cross-site scripting
Persistent cross-site scripting
URL SQL injection

How did we validate and test our IPS solution?

We did this in two ways: 1) We have been putting our systems in front of beta test sites and asking white knights (ethical hackers) to try to hack into them, and 2) We have been running our technology in front of some of our own massive web crawlers. Our crawlers do not attempt anything abnormal but can push through millions of sites and web pages. This is how we test for false positives blocking a web crawler that is NOT attempting anything abnormal.

Back to the question, does divulging our methodology render it easier to breach?

The holes that hackers exploit are relatively consistent - in other words there really is only a finite number of exploitations that hackers use. They can either choose to exploit these holes or not, and ***if they attempt to exploit the hole they will be spotted by NetGladiator***. Hence, announcing that we are protecting these holes is more likely to discourage a hacker, who will then look for another target.

To Learn More…

We would be a happy to provide a detailed walkthrough of the NetGladiator technology, to help you determine if this is the right solution for you.

Please email **ips@apconnections.net** or call us at **303.997.1300 x123** to schedule a technical discussion.

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and are offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, and Internet Providers on six (6) continents.