Neustar, Computing Technology Product Awards

# Security Innovation of the Year: DNS Shield

**Full Entry:**

The idea of ‘standing on the shoulders of giants’ is a very old one. It’s long been recognised that when we see further, know more, and achieve greater things, we do so only thanks to the insights and inventions that came before. Never has there been a clearer demonstration of this, however, than with information technology: since the mid-Twentieth Century, we have repeatedly made the cutting edge of what is possible trivial to achieve, opening up new vistas of challenge and invention for engineers and developers. Part of the magic of software is that, once it is built, what may once have needed thousands of hours of investment can now be taken care of in a line or two of code.

This exponential advance of the possible has, throughout, created both new security threats and new ways of responding to them. In its very earliest form, cybersecurity meant manually monitoring network activity to try to spot the footsteps of individual intruders. Now, attackers can amass armies of millions through botnets or take advantage of universal access by spear phishing for credentials, while defenders can deploy machine learning to automate detection of unusual behaviour or roll out multi-factor authentication to protect high-value assets.

As progress marches on, we are already anticipating a future of quantum computing attacks on cryptography and the strategies that might mitigate them. Sometimes, however, the most threatening vulnerabilities do not emerge from exotic technology. Instead, they are already baked-in, buried in the vast stack of tools and systems which quietly power the modern world.

The Domain System Name (DNS) is one such giant that we stand on the shoulders of. DNS has been an essential and ubiquitous part of how the Internet functions for decades. While human users work with the Internet through the lens of domain names, actually connecting to those websites requires knowing the right IP address to route to. When a computer doesn’t already know which IP address corresponds to the domain a user is trying to access, DNS provides a way of reaching out to a distributed network of servers, gradually narrowing down the search until the correct IP address is retrieved and – within moments – the user is directed to the right destination.

The decentralised approach taken by DNS is fundamental to the Internet’s capacity for indefinite growth; a unified, centralised solution would long ago have collapsed under the weight of demand. This does not mean, however, that it is a solution without flaws. Its original designers could never have envisaged the weight that now rests on the shoulders of DNS, and it’s only natural that unexpected usage has led to unexpected problems. As the initial step in any online activity, a failure in DNS is a failure in everything.

In cybersecurity, importance is also vulnerability, and many significant attacks now operate through DNS. Cache poisoning, also known as DNS spoofing, is one example, in which compromising a single DNS server allows the attacker to redirect traffic towards a malicious location. Because DNS records are commonly saved locally for later use, this can wreak havoc even after the initial compromise has been dealt with. DDoS attacks are also often conducted via DNS, as attackers can use it to send valid queries from bogus sources which are indistinguishable from non-malicious requests, making mitigation difficult.

There is now little prospect of changing the underlying logic of DNS to eliminate such issues – but for the most sensitive and important services these risks are unacceptable. That’s why Neustar took on the task of creating an approach to DNS which armours clients without affecting compatibility.

As the underlying software functionality cannot be changed, we turned to hardware for the solution. As part of Neustar’s global platform, operating across 30 nodes on six continents, DNS Shield is a network of private DNS connections, independent of the public Internet. By resolving DNS requests through a dedicated network that lifts them out of the general flow of Internet traffic, it takes the most popular protocol for cyber-attacks out of scope for malicious actors.

DNS Shield gives an essential and fragile system the priority and protection that customers with demanding use cases need. Yorkshire Building Society Group, for example, relies on unbroken trust with its customer base in order to operate effectively – trust which can quickly be damaged by even a temporary loss of access to personal accounts. Neustar’s 100% uptime guarantee, in an age when IoT-based DDoS attacks are taking on gargantuan proportions, delivers that.

DDoS mitigation is not the only benefit of DNS Shield, though. Direct control over network design means that Neustar can place DNS Shield nodes physically closer to partner servers – sometimes within 100 feet – giving the system a world-leading sub-5ms response time. This helps websites maintain functionality through peak traffic events like holiday shopping, while the private nature of the network also defends against the knock-on effects which can cascade across the Internet when attacks and outages happen.

As a wholly-owned network, DNS Shield is also a key component of Neustar’s ability to offer tailored solutions to customers. According to the CTO of online estate agency Purplebricks, the “Neustar DNS solution is more nuanced and we are able to configure it with more detail than other DNS products on the market”, helping the company to “ensure our web presence and guarantee a smooth navigation experience for users”.

While we build up to new and better things on the foundations of what came before, progress also gives us the opportunity to re-examine those foundations. In DNS Shield, Neustar offers a new, more secure, more robust vision of Internet architecture, maintaining its scalability and flexibility while mitigating the risks that arise when all traffic shares a common road. With it comes a vision of making some of the most common and disruptive attacks a thing of the past.

**Word count: 969**