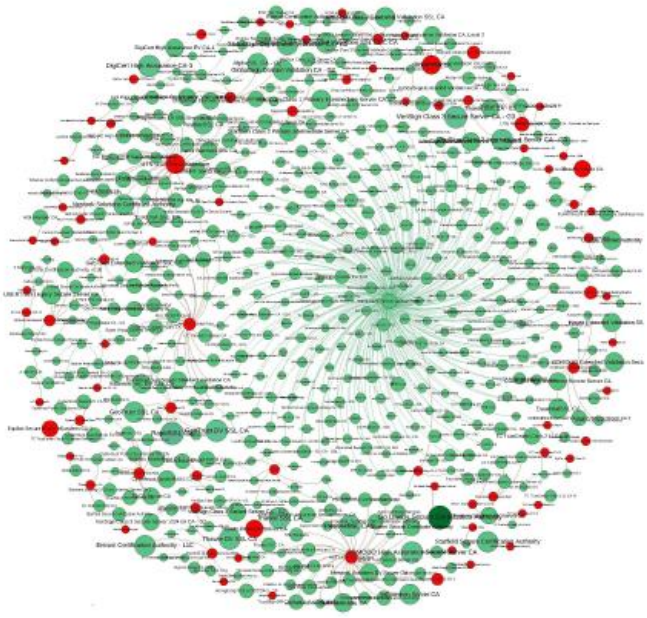
Cyber-defense and forensic tool turns 20

August 5 2015, by Aaron Dubrow



The interactive Tree of Trust diagram helps clients identify malicious certificates by providing a third-party perspective on what they should expect to receive from a server. Credit: ICSI

Sometimes a new idea or product can burst into the world fully-formed,

but more often than not it takes time for things of value to evolve, improve, emerge and find an audience.

In 1995, Vern Paxson, then a computer science Ph.D. student at the University of California, Berkeley, began writing what would eventually become Bro, the ground-breaking open source cybersecurity software that defends innumerable networks today, including key government and business enterprises in the U.S. The name, "Bro," is a reference to Big Brother, an Orwellian reminder that monitoring comes hand in hand with the potential for privacy violations.

On Tuesday, at its annual meeting of users and cybersecurity engineers, Bro celebrates its 20th Anniversary.

Now a professor at the University of California, Berkeley and the leader of the Networking and Security Group at the International Computer Science Institute (ICSI), Paxson wasn't exactly setting out to build a network monitoring framework that would be used by many of the largest supercomputing centers, national labs, university campuses and even Fortune 10 companies.

But with long-term continuing support from the National Science Foundation (NSF), and early adopters at the Lawrence Berkeley National Laboratory (LBNL)—which started using Bro operationally in 1998 and was one of the first labs in the world to automate its cyber-defenses—Bro has exploded out of the ivory tower and into the world of real world cybersecurity.

Protecting high-value assets

A little known fact: Labs like LBNL and research centers like the National Center for Supercomputing Applications (NCSA) face almost constant cyber attacks.

For example, in July 2015, the Bro implementation at LBNL identified and blocked more than 125,000 hostile IP addresses.

These networks are tantalizing targets for individuals hoping to use their clusters of superfast processors for bot-based attacks, bitcoin mining or other malicious uses. They also can provide entrees to more sensitive systems (such as national labs that conduct classified research) due to the complex trust relationships between different institutes.

Most of these attacks are unsophisticated, but others are carefully targeted and require an equal level of care and sophistication to detect and root out.

Bro provides a powerful framework for performing network monitoring and traffic analysis. But it is used not only to detect and thwart. It also enables security experts to perform complex cyber-forensics so they can study the patterns of attacks, assess the damage and design better ways to block them in the future.

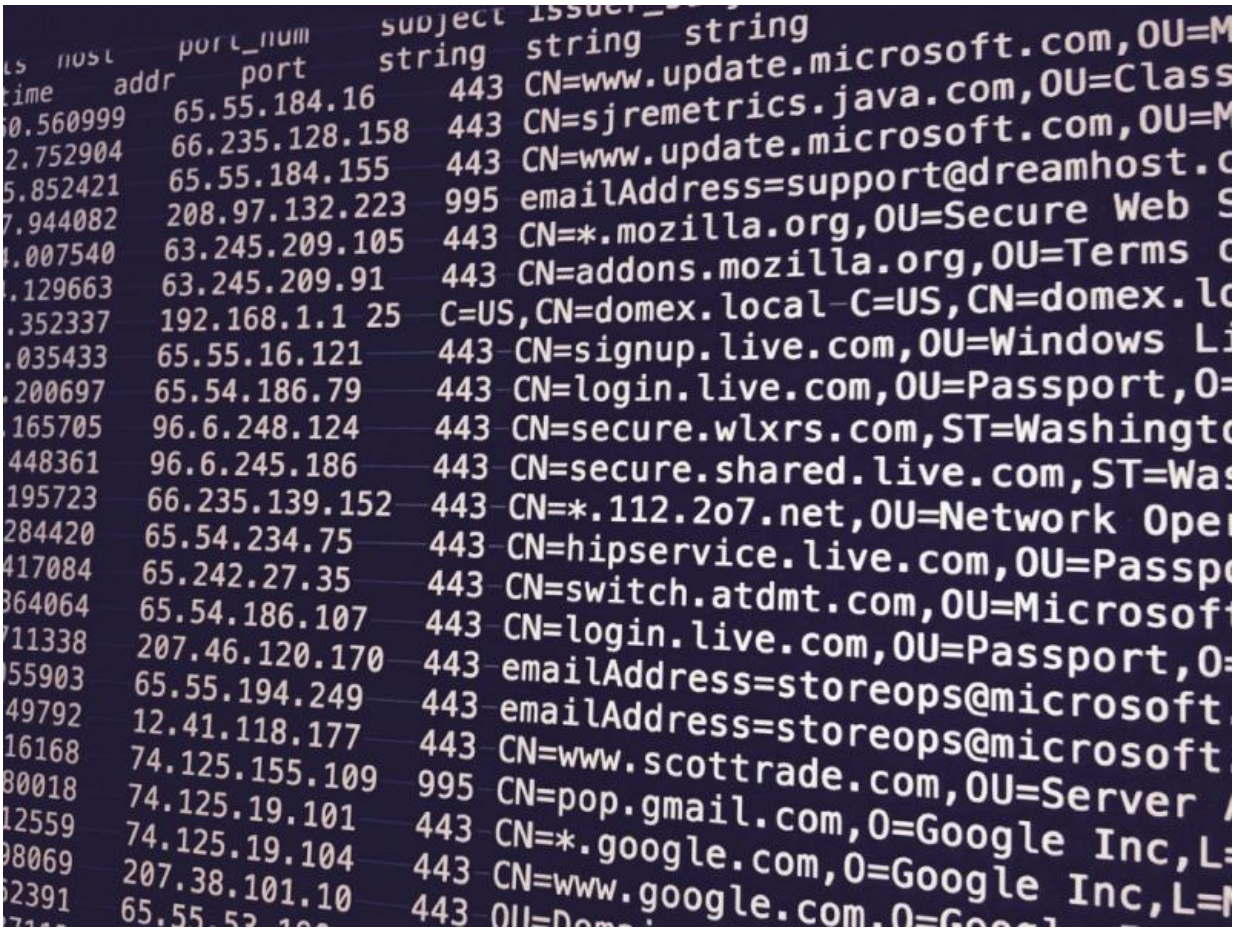
"When you have a security incident, the forensics can help you understand what exactly happened," Paxson said. "That's important, because if you don't recognize all of what the attackers did, they often come back."

As attacks have become more sophisticated, Bro's capabilities have evolved. In recent years, Bro has played a key role in developing the ability to detect the unique characteristics of targeted phishing attacks by extracting message attributes, such as links, that they can then block. Bro was also instrumental in identifying credential thefts that led to the arrest of a hacker trying to sell access to government supercomputers.

"Bro enables deep inspection of network data, allowing us to defend against modern attack techniques," according to Rosio Alvarez, CIO at

LBNL. "For two decades Bro has been the cornerstone of cybersecurity at Lawrence Berkeley National Lab, providing the visibility and flexibility to secure our unique network."

A flexible, open-source cybersecurity tool



The Bro Network Security Monitor provides a comprehensive platform for network traffic analysis. Well grounded in more than 15 years of research, Bro has successfully bridged the gap between academia and operations since its inception. Today, it is relied upon operationally in particular by many scientific environments for securing their cyberinfrastructure. Bro's user community includes major universities, research labs, supercomputing centers, and open-science communities. Credit: Bro

What sets Bro apart from other cybersecurity products on the market (besides being open source and free to use) is the fact that it is highly programmable, ultra-high-speed and flexible. This allows Bro to analyze the unique traffic patterns of one's networks to identify abnormalities.

"Commercial products, out of the box, are only as good as their latest security update," said Anita Nikolich, a program director at NSF. "Bro, on the other hand, looks at what's unique about your network and tailors its defenses based on one's needs."

Furthermore, through a combination of customization and security community crowdsourcing, operators can deploy a programming script - a small bit of implementable code – that can track the vulnerability to the source, see the impact on your network and respond quickly when an attack is detected.

Bro is able to do this lightning-fast analysis on huge networks with very few false positives, in part, because of the sophisticated algorithms that Paxson and his team developed.

NCSA's network, for instance, passes 100,000 packets per second over its 450 Gigabit/second network, delivering data to thousands of users. Bro looks over every one of those packets, automatically raising an alert or triggering an external action like a block when it sees evidence of an attack, with very few errors in its automated judgment.

"Every one of those packets has some meaning and the processing challenge of understanding that meaning is very large," Paxson said. "For that reason, Bro has evolved towards doing large-scale network analysis in ways that are practical."

Growing the Bro community

Between 2003 and 2010, NSF supported the research aspects of the project, but at a certain point it became clear that for Bro to have a major impact, fast, smart and capable algorithms were not enough.

In 2010, NSF provided a $3 million grant to Paxson, along with Robin Sommer (a senior researcher at ICSI) and Adam Slagell (assistant director and chief information security officer at NCSA) to enhance Bro for operational network security monitoring in scientific environments. This involved developing extensive documentation, hiring software engineers to improve the user interface and providing assistance to institutions that wanted to install the framework on their large-scale networks.

A further $3 million award in 2013 helped to found the Bro Center of Expertise for the NSF Community. Housed jointly at ICSI and NCSA, it serves as a central point of contact for NSF communities to leverage Bro technology and expertise in order to protect their cyber-infrastructure.

Blue Waters, one of the most powerful supercomputers in the world, uses Bro to protect its network. Credit: NCSA, University of Illinois at Urbana-Champaign

These grants enabled the team to improve the software, provide documentation, better packaging and also to support Bro developers who were not first and foremost academic researchers.

"Bro is a complex tool and we saw that people needed help getting started and using it effectively," said Sommer. "So we set out to offer them our teams and expertise as a point of contact."

Awards from NSF helped Bro transition from fundamental research in cybersecurity to adoption and use across the NSF community and beyond, according to Nikolich.

"Much of the cybersecurity research NSF supports has the potential to be used in a real operational environment," she said. "But Bro is one of the best examples of getting innovative technology out into the world in support of networking cybersecurity."

"NSF was willing to back that sort of roadmap that was not, first and foremost research and it's really paid off for community and for Internet defense," Paxson said.

The Bro Center of Excellence helped to galvanize the community and create mechanisms to share solutions and offer assistance to each other. More than 100 cybersecurity experts have contributed functionality to the system and scripts that identify patterns of malicious activity or prevent various types of attack. These, in turn, are shared among the broader Bro community.

Today, the tool protects hundreds, and perhaps even thousands, of campuses, labs and high-value scientific installations worldwide. (Because Bro is bundled with other open source tools and included "under the hood" in many commercial packages, the exact number of deployments is hard to determine.) It helps safeguard our data at the nation's largest companies. And, by virtue of its ability to trace events, log them and perform rigorous empirical analyses, it is helping to provide an empirical basis for establishing a "science of cybersecurity".

"Bro gives you the ability to get deep visibility into your network," said Slagell. "This is very useful for security analysts, but it also gives you a model and a complete language to make inquiries in real time.

"Not only might you find security events, look for historical trends, manage assets, and detect failures, you will come across things on your network that will make you think, 'huh, that's a bit strange'. And isn't that how most great discoveries begin?"

Twenty years in, Bro continues to expand and evolve, securing ever larger and faster networks, thwarting new threats as they emerge, and pioneering a more rigorous approach to cybersecurity.

"There are some risks involved when you give researchers the freedom to explore an idea at length, but in this case it paid off hugely," Paxson said. "The Internet is a safer place because of this technology."

Provided by National Science Foundation