SEEING THE CYBERTHREAT

How the U.S. Army is Using Virtual Reality to Visualize and Defend the Nation's Cybersecurity Infrastructure

U.S. Army Research Laboratory - Aberdeen Proving Ground

OVERVIEW

The U.S. Army's Cyber Protection Teams are about to get a new view into the cyber battle space thanks to virtual reality (VR), the computer-generated three-dimensional world that allows users to interact with data through specialized headgear and hand controls. Researchers are using VR to help information security analysts—those who man the Army network's virtual wall—deal with the huge amounts of data they must constantly sift through to find evidence of intrusions.

U.S. Army Research Laboratory, Aberdeen Proving Ground, MD
Public Affairs Contact: T'Jae Ellis - tanya.j.gibson.civ@mail.mil

Prepared for BEST by
THE CENTER FOR HOMELAND SECURITY AND RESILIENCE

Submission Date
February 12, 2018

IMAGE INFO
Cover and Page One: Source, istockphoto.com

SEEING THE CYBERTHREAT

Army network guardians going virtual to watch for cyber adversaries

It's hard to visualize all the action happening in cyberspace. Even a small business network sees constant communication between desktops, servers, mobile devices, and other machines that comprise it. And all of those machines are sending and receiving huge amounts of data through the channels that physically connect the network to the internet.

For a huge network like the one run by the U.S. Army, the complexity can boggle the mind of all but the most seasoned information technology specialists who understand enterprise-sized operations. More than a million military and civilian personnel spread across the globe actively use the Army's network through an even larger number of devices.

Add to that all the connected systems, from drones and their remote pilots to quartermaster inventory databases and installation management software. Then layer on top of that the temporary tactical outgrowths of the network that must be created anytime units are deployed for combat or other operations.

Potential vulnerabilities abound

There is no such thing as perfectly written code. Estimates vary, but research has shown somewhere around one or two defects for every 100 lines of code written. And modern operating systems and software can easily contain several million lines of code, showing how many potential vulnerabilities exist in the digital tools the military and civilians use everyday.

One database, called the Common Vulnerabilities and Exposures list and kept by the U.S. Department of Homeland Security, includes almost 96,000 publicly known cybersecurity vulnerabilities that attackers can exploit. That number grows daily as new weaknesses are discovered.

With cyberspace so wrought with potentially exploitable interfaces into the nation's digital infrastructure, keeping a massive network like the Army's safe from hackers is a huge challenge. The Army's network is under constant attack from adversaries, a virtual shadow war now occurring 24 hours a day, seven days a week—cyberattacks that are becoming increasingly sophisticated.

One common type of attack is called Distributed Denial of Service (DDoS), where "black-hat" hackers, or those with malicious intent, flood a target network with so much traffic that it stops working. DDoS attacks averaged a gigabit or two of data a second only a few years ago, according to retired Lt. Gen. Alan Lynn, who served as the director of the Defense Information Systems Agency, which operates the department's digital infrastructure, until February 2018. These days, it's common for the same type of attack to direct 600 gigabits of data a second at defense network access points, Lynn said at a gathering of armed forces electronics specialists.

"We do an excellent job of defending the [Department of Defense Information Networks], but the level of attacks that we've seen actually was really truly surprising and it still continues to surprise me just how robust the attacks have become," Lynn said during the speech.

Cyber adversaries are often well trained, well funded and good at their jobs. They might be employed by nation-states like China and Russia, whose state-backed hacking groups actively work to sow havoc and look to steal intellectual property. They could also be non-state actors like the Islamic State or Al Qaeda, groups that attempt to cause destruction for ideological reasons, or organized criminals looking for information to sell or use as extortion.

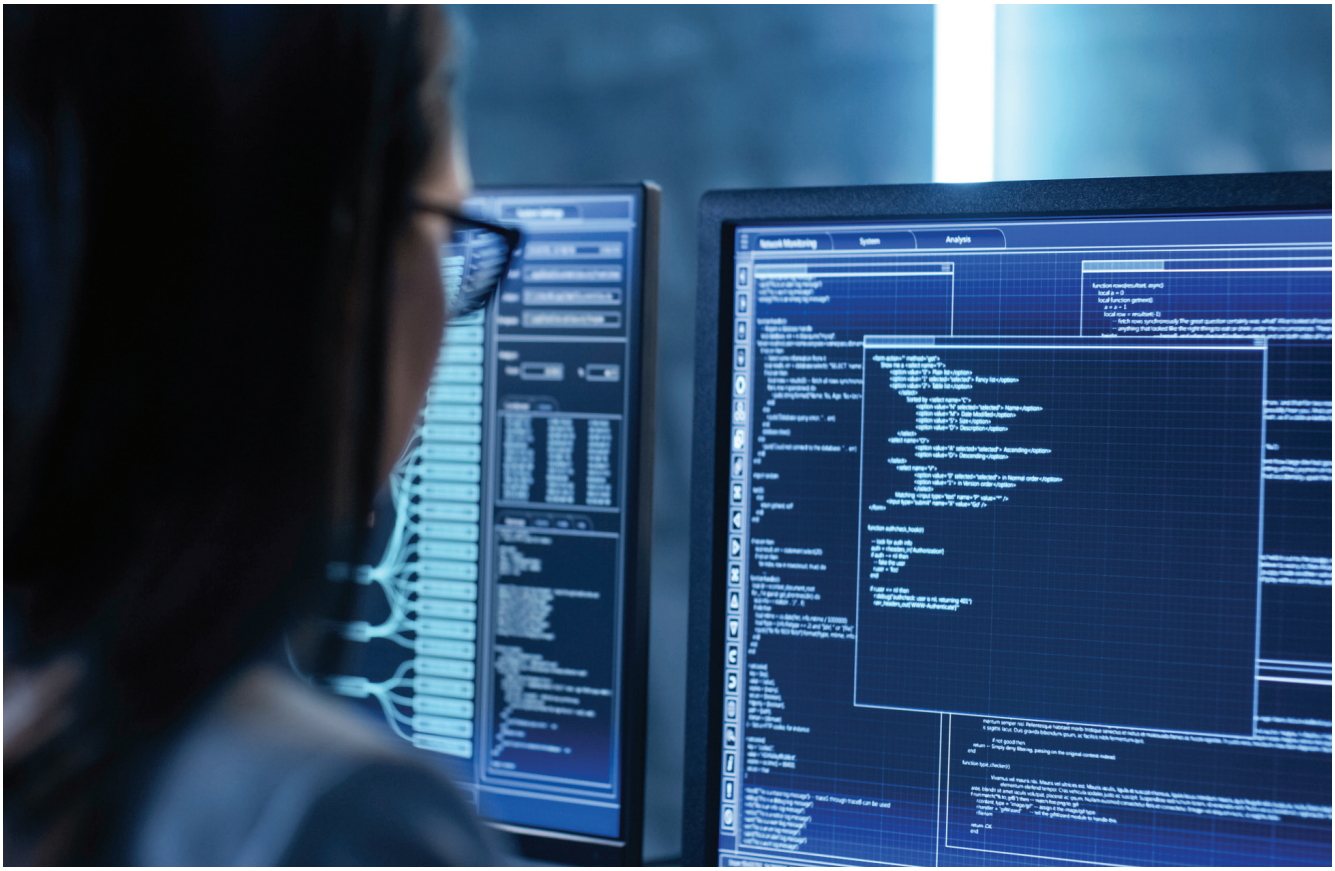
Ramping up for future cyber fights

In a foreword to Army Field Manual 3-12, Maj. Gen. John Morrison, Jr., commander of the U.S. Army Cyber Center of Excellence, wrote that the service is aggressively improving network security because failures that let bad actors in will put soldiers and objectives in danger.

"We must anticipate that future enemies and adversaries will persistently attempt to infiltrate, exploit, and degrade access to our networks and data," Morrison wrote. "A commander who loses the ability to access mission command systems, or whose operational data is compromised, risks the loss of lives and critical resources, or mission failure."

Army leaders believe that in order to grasp the scope of the problem, people need to be able to see it. That's why trying to explain the complexity and danger of cyberattacks on systems, a world whose only physical constituents are silicon microprocessors, cables, antennas and circuit boards, to anyone who isn't an information technology professional is difficult.

"We still need to work on how we visualize this domain so we can make it understandable by commanders at every level," Brig. Gen. J.P. McGee, the U.S. Army Cyber Command's deputy commander of operations, said at a recent conference at Fort Benning, Georgia.



But visualizing the threat is difficult even for those who are charged with protecting the network.

Unfortunately, being unable to visualize the network to see where it is vulnerable doesn't make those vulnerabilities go away. Though digital communications have ushered in a revolution in how the U.S. executes military operations, each machine also creates a potential new attack surface that can be exploited by enemies.

The Army is building 20 Cyber Protection Teams (CPTs) comprised of 900 soldiers and civilians. Their mission is to defend the service's portion of the Department of Defense Information Network, and to hunt down bad actors banging on the network's virtual doors looking for ways in. But with the sheer volume of data moving between machines both inside and outside the wall, attackers have plenty of opportunities to secretly breach the defense.

CPTs are about to get a new view into the cyber battle space thanks to virtual reality (VR), the computer-generated three-dimensional world that allows users to interact with data through specialized headgear and hand controls. Researchers are using the technology to help information security analysts—those who man the Army network's virtual wall—deal with the huge amounts of data they must constantly sift through to find evidence of intrusions.

Finding a needle in a haystack

Currently, cybersecurity specialists must sit in front of multiple screens to watch network traffic. Each of those monitors is usually crammed with the tabular data and various graphs that represent traffic.

Their job is to monitor patterns of data movement to uncover anomalies, which could indicate any number of problems. Aberrant patterns could mean a DDoS attack is underway, a machine like a desktop or printer has been compromised by malware and is exfiltrating sensitive information from Army servers, or any number of other bad things. Or it could indicate nothing more than a user sending a high-definition video to another user.

Sifting through the information is often mentally exhausting and inefficient—there's just too much information. That's why the Army Research Laboratory (ARL) is building the Virtual Reality

Data Analysis Environment (VRDAE), which will present analysts with a collaborative environment and a variety of 3-D visual tools, including one that can provide a representation of the network, complete with the computers, routers, switches and communication lines between them all.

"There's a lot of information out there on the network, a lot of sensors talking back and forth," says Curtis Arnold, a computer scientist and ARL branch chief leading the VRDAE project. "It's more information than analysts can go through, but the data needs to analyzed by someone. We needed to make that data easier to consume to make sure we're not missing something."

The environment feels like a futuristic science fiction film. Users strap on an Oculus Rift virtual- reality headset, a device that parks a display with a 110-degree field of view in front of their eyes. They use handheld Oculus Touch controllers to enable hand gestures to manipulate and sift through data projected in the space in front of them, and to maneuver around the visual representation of the network, zoom into individual nodes and machines and take a closer look. Traffic anomalies are represented as thicker lines between machines and nodes that are under attack or investigation are surrounded by a red bubble.

The system tracks head movement, so a text bubble with more detailed information pops up when an analyst looks at a component of interest and fixes her gaze on it. And if she needs another set of eyes on the problem, she can invite another analyst into her virtual space. That person might be in the next room or in a base across the country—he'll slide on a VR headset to join her.

"Visualizing the network this way helps people take it in, recall it later and helps them take action," says Arnold, who worked in criminal law and security within the Army Judge Advocate General's Corps before diving deep into his interest in cyber. "You can't get that from a spike chart on a PowerPoint presentation. It's game-changing for cyber."

Since this virtual environment will be projected out of secure computing resources, when analysts are done, they can just remove their goggles and lay down their joysticks without needing to replace files or lock sensitive material away. They can simply leave the workspace as it is for the next session.

This characteristic of the system helps decrease vulnerability associated with human error, one of the biggest problems in maintaining a strong cybersecurity defense. All too often, information security managers say, a simple error like leaving an open file on a desk or forgetting to take a document with sensitive data from a network printer is the open door that hackers use to breach an organization.

Proving out and scaling up

Right now VRDAE is in its early stages and still being tested out by ARL cybersecurity analysts and researchers. The project has been underway since early 2017 and a fully functioning prototype is just starting to come out of the lab. Arnold and his team gave the ARL's Cybersecurity Service Provider—an operation that defends U.S. military, government and business networks around the clock—an early preview. The team stocked the pilot system's virtual environment with samples of three different connected Army networks. The data isn't showing a live view of the networks yet, instead giving test users a historical snapshot to play in.

"We're getting good feedback from the analysts, who say they can see where this is going and it all makes sense to them," says Lee Trossbach, the VRDAE project technical lead, and an Army contractor with ICF, the Fairfax, Virginia-based global consulting and technology services provider.

The team expects to switch the historical network data now feeding the pilot system to a variety of data streams showing actual network conditions by mid-2018. Testing with near real time and retrospective data will be the first hurdle to overcome to show cyber operations leaders that the system can handle real network data at the scale the Army needs.

Arnold expects to provide ARL cybersecurity operators with access to VRDAE for testing in FY- 2019. Then other groups will start assessing if it has a role in their work. The research team has six Oculus Rift units for analysts to interact with the VRDAE, but with thousands of cybersecurity analysts in the Army alone, that number could quickly increase if it the technology becomes widely adopted. And while Oculus Rift is the current gear of choice, Trossbach says the developers intend to enable VRDAE to leverage hardware from other VR vendors as it becomes available, so they can pivot to the best hardware on the market for their software and environment

Arnold says he thinks a number of Army offices beyond cyber operations will welcome the use of digital realities such as VR because the community sees the promise in visualizing complex systems and data. Chemical engineers could benefit from a three-dimensional view of molecules; tank crews can learn the ins and outs of new combat platforms, take them apart and reassemble them again before ever touching the real thing. The list of possibilities keeps growing, Arnold says.

Cyber army plays high-stakes game

Arnold says he's excited about VRDAE's future because young people coming into the service are in a perfect position to exploit the new technology. The combination of the new capability and digitally savvy users make it potentially disruptive to cyber defensive operations.

"VR offers a completely different platform and a paradigm shift," Arnold says. "But everyone coming into cyber is inherently more comfortable VR technologies because they were playing 3- D video games as kids."

That's why there was perhaps no better person to bring in for the technical side of the project than Trossbach, a self-proclaimed geek in both his personal and professional lives. He's also a gamer who has been following the development of consumer VR technologies since 2012, so the idea of using a gaming engine to power VRDAE's virtual environment was a no-brainer. And he was a cybersecurity analyst for six years before taking on this project, so he saw a chance to bring these seemingly disparate worlds together.

"I'm trying to help the me who's doing the network analysis now," Trossbach says. "I want to give them more data and have a more interesting experience. They're going to do better because the best analysts are the ones that are interested in their job."

He was already thinking about the cybersecurity applications for VR when the first generation came out earlier this decade. But his enthusiasm turned to a wait-and-see attitude because it wasn't ready yet due to low resolutions and latency. Still, he was sure of the benefits to moving traditionally text-based presentations of information into the visual space, and once the headsets and the software driving them matured a bit, he knew it was time to bring it to cyber operations.

"Humans process visual information much faster than text—it's virtually instant," he says. "Think of looking at a weather map rather than reading a paragraph summarizing the weather. To see cyber analytics data visually represented in 3-D makes it much more intuitive—it all comes together for a person in a way that just makes sense."

Trossbach says VR hardware and software still have a ways to go before the potential is fully realized. One issue is the headsets are bulky and awkward, often preventing people for using them comfortably for much longer than 30 minutes. They need to get smaller, and the image resolution at which they present the virtual environment needs to increase. Also, some users suffer from motion sickness when using the headsets, an issue that has diminished with recent upgrades, but one that will mean some analysts likely will never have the stomach to use it.

Even with those issues, Trossbach has long been sold on the technology as an educational and professional tool as much as a new way to play games.

He fondly remembers the first time he was blown away by VR. He strapped a headset on to play "Titans of Space," an astronomy educational tool thinly veiled as a game. The game puts the user aboard a spaceship that can be piloted around the solar system. Approaching any celestial body brings up facts about it and the VR environment allows a totally different appreciation for the scale of space.

"You start off looking at the Earth and then the moon comes swooping by and you're like, 'Good god, the moon is huge,'" Trossbach says. "And then you see Saturn and the sun and you're like, 'Wow, it's mind-blowing.' You've read and seen this stuff, but you can't understand the size until you see it at scale like this."

He has taken that same excitement to solving the information consumption problems inherent in defending networks from intruders looking to cause damage.

Taking analysts through their first times using VRDAE, he felt the project would succeed because people were able to navigate the virtual network environment with very little guidance. The virtual reality aligned with users' expectations of what they'd find in computer-created space.

"For cyber operations, we're taking the industry standard network diagram and making it living," Trossbach says. "We're getting a lot of excitement from teams about it because seeing the network represented in the VR environment makes sense to them—the hard part is both automating the construction of traditional diagrams and finding new ways to show the data that is still intuitive."

DoD LabS

TOGETHER, WE'RE INVENTING THE FUTURE