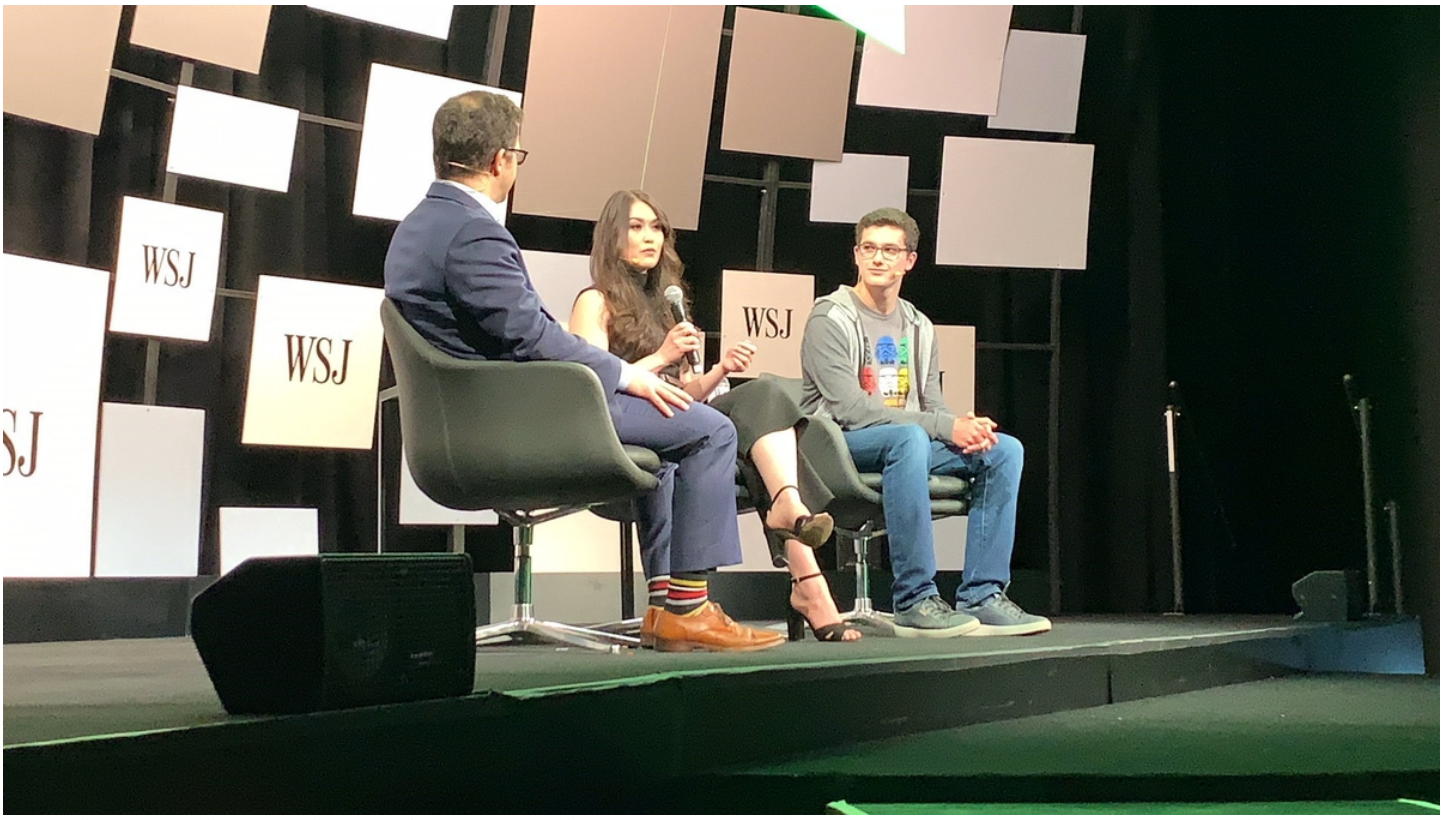
Army

How one teenager took out a secure Pentagon file sharing site

Andrew Eversden

August 29, 2019



Reina Staley, co-founder of the Defense Digital Service, and Jack Cable, right, discuss culture at the Wall Street Journal's Future of Everything conference in May. (DDS)

By last October, the Pentagon's Vulnerability Disclosure Program had processed thousands of loopholes in the Department of Defense's websites.

Then it received a report from Jack Cable.

On Oct. 25, Cable, who worked for the Defense Digital Service and was a freshman at Stanford University, reported a problem to the department through the Pentagon's HackerOne vulnerability disclosure page.

Typically, vulnerabilities sent to the DoD through a disclosure program operated by HackerOne, an ethical hacking company that manages reporting programs for various organizations, require a simple reconfiguration or software patch. Of the 16 problems reported to the DoD on the average day, 11 tend to require action by the Pentagon, Kris Johnson, director of the Vulnerability Disclosure Program (VDP) at the DoD's Cyber Crime Center (DC3), told Fifth Domain in an exclusive interview.

Cable has quite the list of accomplishments. In 2018, TIME Magazine ranked him as one of the Top 25 most influential teens. At age 17, he found 30 vulnerabilities in Air Force websites during the 2017 rendition of the "Hack the Air Force" competition. He ended up winning the contest.

For this contest, Cable was trying to hack the Army's file-sharing system that was used to send files too large to send over email. The system was formally known as the Army Aviation and Missile Research Development and Engineering Center Safe Access File Exchange (AMRDEC SAFE) and had been used since "around 2001," according to an Army spokesperson.

But what Cable found in the DoD's secure filing system stood out. He discovered a vulnerability known as an "insecure direct object reference," which involves brute forcing reference numbers in the URL to access different files without authentication.

For a secure file sharing system holding files up to 2 gigabytes, the implications would be severe if exploited. This is the story of SAFE's mysterious disappearance and how defense organizations took down the system that was used to transfer approximately 11,000 packages a day, or 4.1 million files a year for 600,000 unique users.

"If properly exploited you could bypass two-factor authentication and you could jump from package to package within the ARMDEC website and then download," Johnson said.

In other words, attackers could move through all the files loaded on the SAFE website unencumbered.

Action was swift. On Nov. 1, the site was disabled. SAFE's construction had critical flaws. And as a result, the Pentagon took the file sharing site offline for four months.

"This is one of the rare examples of a website that had some architecture designs on the back end that really had to be brought down and have some core components rebuilt in order to mitigate the vulnerabilities," Johnson said.

Johnson said that his team contacted Cable hours after he reported the vulnerability. Over the following days, Cable and Johnson's team reviewed the vulnerability and confirmed it was real.

Together they created a step-by-step replication of the vulnerability, submitted it to the Joint Force Headquarters Department of Defense Information Network (JFHQ-DoDIN) and to Army Cyber Command.

How bad was the problem? To categorize vulnerabilities, the DC3 VDP uses the Common Vulnerability Scoring System to score the severity of the loophole. This system rates each vulnerability from "low" to "critical." This vulnerability was scored as "critical." DC3 VDP itself was created in 2016 and tasked with improving network defenses on public facing DoD websites using ethical hackers.

Attackers could've accessed "unclassified information, but it could be 'for official use only.' Some of the data could've contained [personally] identifiable information, and also your personal health information as well," Johnson said. "It could have been a wide variety of data ... if exploited, it could've been a bad day. But thankfully, we got to it before anyone else did."

Johnson then went to JFHQ-DoDIN, which is responsible for the daily defense of DoD's networks, and subsequently Army Cyber Command, both of which took the report from the vulnerability team seriously. The issue was also raised all the way up to U.S. Cyber Command.

"It was an immediate reaction," Johnson said. "There was no hesitation or delay on this vulnerability, which is why it gained such quick traction [and] we were able to close it down before anything happened."

The site returned online around Valentine's Day.

"Because of the nature of it and how widely it was used, I believe there was a decision made to really to want to mitigate that risk of exposing any time of data on the backside of SAFE to any adversary or anybody who would want to take that information," Johnson said.

In November, Fifth Domain reported that AMRDEC SAFE was "disabled as a preventative measure after outside agencies identified potential security risks." The Army told Fifth Domain in February that the website was kept down "not due to the potential vulnerabilities, but due to issues with sustainment and maintenance capabilities."

Johnson said that subsequent testing on the system found that the vulnerability Cable discovered had not been exploited.

Cable was not paid for his discovery.

"Our program is built upon reputation points," Johnson said. "So when you submit vulnerabilities for us, if they're of high quality and they're valid, then we give reputation points."

These reputation scores can then get hackers invited to participate in paid programs.

Johnson added the SAFE disclosure emphasized the importance of white hat hackers for DoD's safety online, saying he doesn't "believe that the DoD would ever truly be able to effectively employ enough people or to have enough systems on the line to cover every single aspect of it."

Leaders at Army Cyber Command concurred.

"This was a good example of how across the public and private sector, ethical hacking and bug bounties can help to save time and resources to find technical vulnerabilities, quickly remediate, and persistently harden cybersecurity defenses," Army Cyber Command said in a statement.

On Aug. 15, DISA launched its own secure file sharing system. That same day, AMRDEC SAFE was taken offline for good.

About Andrew Eversden

Andrew Eversden is a federal IT and cybersecurity reporter for the Federal Times and Fifth Domain. He previously worked as a congressional reporting fellow for the Texas Tribune and Washington intern for the Durango Herald. Andrew is a graduate of American University.

NSA veteran explains deception tech

Craig Harber is a veteran of the NSA and the CTO of Fidelis. He shows Fifth Domain how his company is employing deception technology.

Catching rogue devices with their 'fingerprints'

▶ Play Video

How would feds be able to use their own devices for work?

▶ Play Video

What's in store for facial recognition in 2020?

▶ Play Video

Top Headlines

Cyber National Guard Task force will focus on network defense

The Army's cyber school now teaches information operations

No cellphones, laptops were allowed to go with Army 82nd paratroopers deploying to Middle East

How the Defense Digital Service revamped Army cyber training

Here's how the Army plans to visualize cyberspace

Newsletters Contact Us

Civilian DoD Congress Critical Infrastructure International Workforce Industry Thought Leadership

Terms of Use
Terms of Service
Privacy Policy

Get Us
Newsletters & Alerts
RSS Feed

Contact Us
Help & Contact Info
Advertise

About Us
About Us
Careers

Military News
Air Force News
Army News
Marine Corps News
Navy News
Defense News
Federal News
C4ISR
Cyber
History