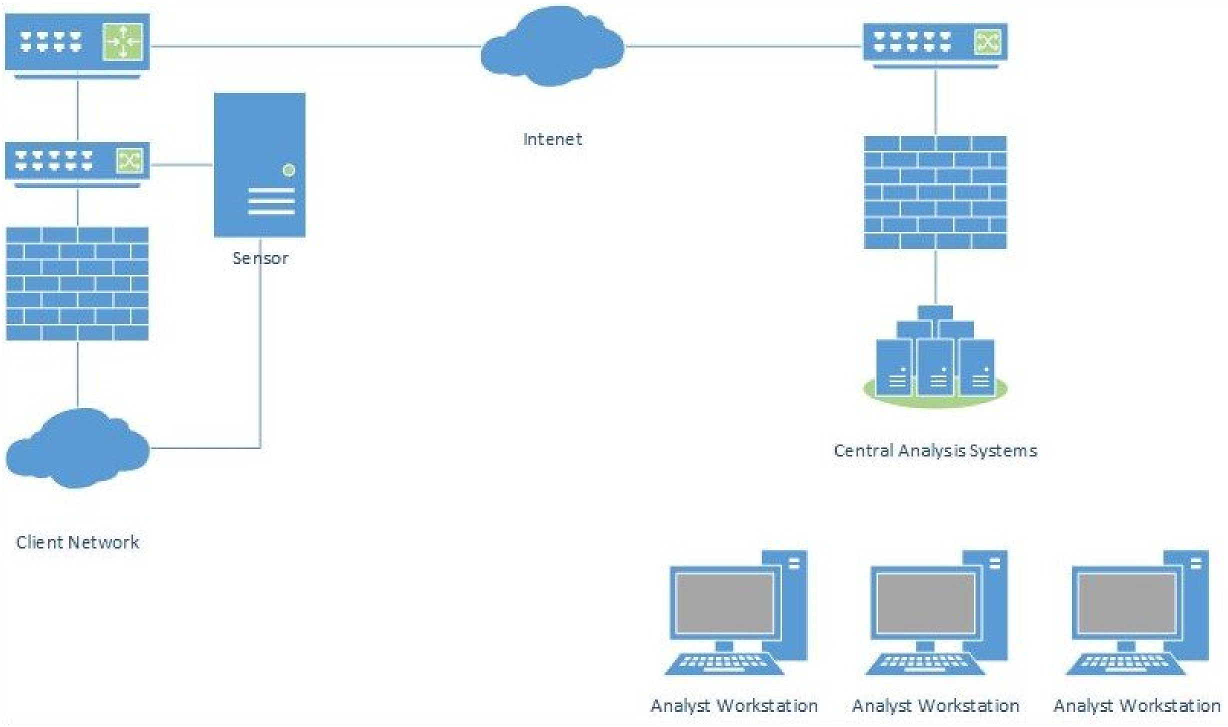
Army researchers identify new way to improve cybersecurity

April 17 2019



ARL scientists may have identified a way to improve the cybersecurity of distributed network intrusion detection. Credit: U.S. Army

With cybersecurity one of the nation's top security concerns and billions of people affected by breaches last year, government and businesses are spending more time and money defending against it. Researchers at the U.S. Army Combat Capabilities Development Command's Army

Research Laboratory, the Army's corporate research laboratory also known as ARL, and Towson University may have identified a new way to improve network security.

Many cybersecurity systems use distributed network intrusion detection that allows a small number of highly trained analysts to monitor several networks at the same time, reducing cost through economies of scale and more efficiently leveraging limited cybersecurity expertise; however, this approach requires data be transmitted from network intrusion detection sensors on the defended network to central analysis severs. Transmitting all of the data captured by sensors requires too much bandwidth, researchers said.

Because of this, most distributed network intrusion detection systems only send alerts or summaries of activities back to the security analyst. With only summaries, cyber-attacks can go undetected because the analyst did not have enough information to understand the network activity, or, alternatively, time may be wasted chasing down false positives.

In research presented at the 10th International Multi-Conference on Complexity, Informatics and Cybernetics March 12-15, 2019, scientists wanted to identify how to compress network traffic as much as possible without losing the ability to detect and investigate malicious activity.

Working on the theory that malicious network activity would manifest its maliciousness early, the researchers developed a tool that would stop transmitting traffic after a given number of messages had be transmitted. The resulting compressed network traffic was analyzed and compared to the analysis performed on the original network traffic.

As suspected, researchers found cyber attacks often do manifest maliciousness early in the transmission process. When the team identified malicious activity later in the transmission process, it was usually not the first occurrence of malicious activity in that network flow.

"This strategy should be effective in reducing the amount of network traffic sent from the sensor to central analyst system," said Sidney Smith, an ARL researcher and the study's lead author. "Ultimately, this strategy could be used to increase the reliability and security of Army networks."

For the next phase, researchers want to integrate this technique with network classification and lossless compression techniques to reduce the amount of traffic that needs to be transmitted to the central analysis systems to less than 10% of the original traffic volume while losing no more than 1% of cyber security alerts.

"The future of intrusion detection is in machine learning and other artificial intelligence techniques," Smith said. "However, many of these techniques are too resource intensive to run on the remote sensors, and all of them require large amounts of data. A cybersecurity system incorporating our research technique will allow the data most likely to be malicious to be gathered for further analysis."

Provided by The Army Research Laboratory

Citation: Army researchers identify new way to improve cybersecurity (2019, April 17) retrieved 25 April 2024 from https://phys.org/news/2019-04-army-cybersecurity.html