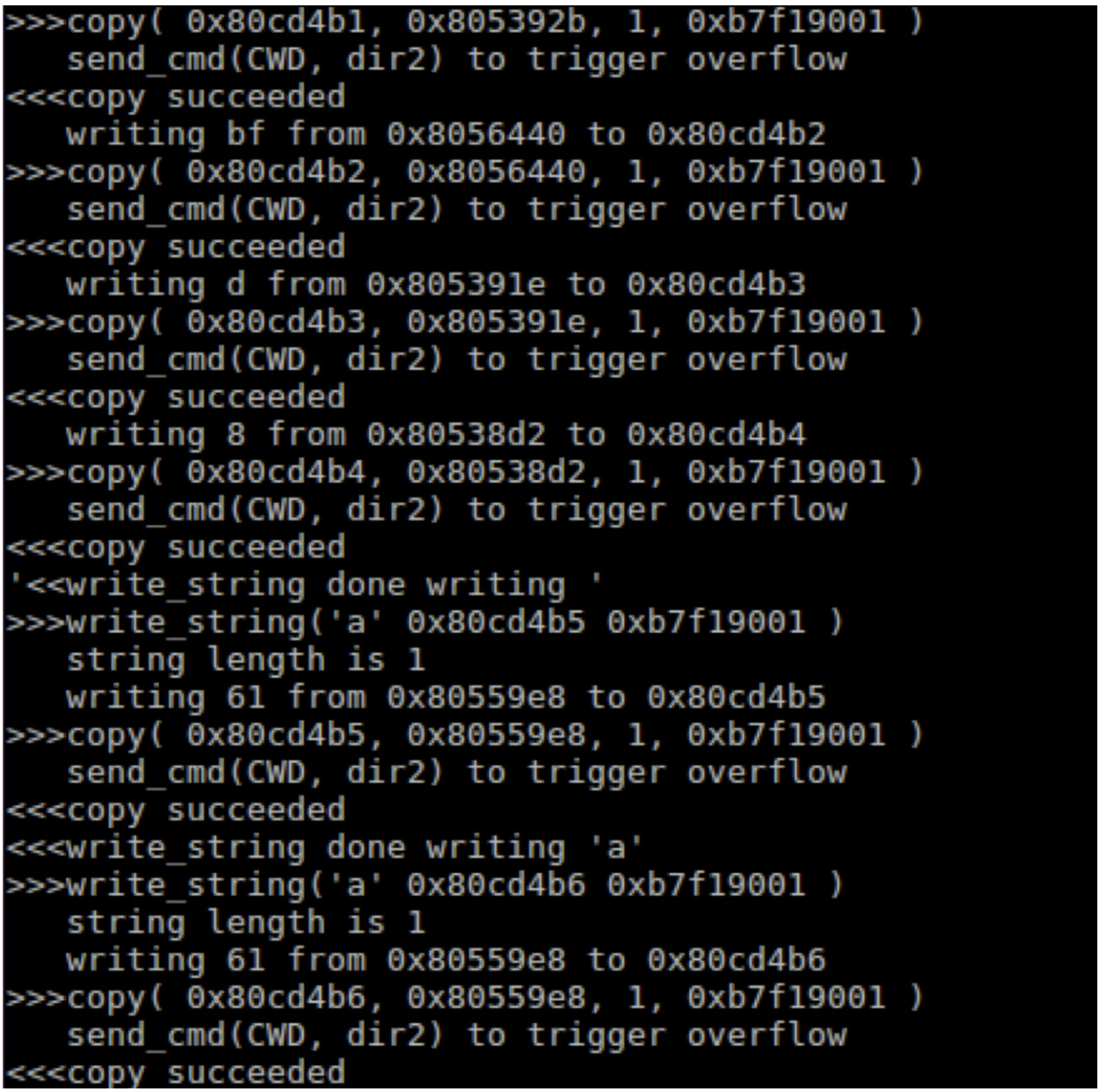
# New exploitation techniques and defenses for DOP attacks

March 7 2019, by Ingrid Fadelli



Credit: Long Cheng

Data-oriented attacks allow hackers to manipulate non-control data and alter a program's behavior, often causing significant damage to the systems affected. Researchers at Virginia Tech, Clemson University, Pennsylvania State University and Aalto University have recently uncovered new exploitation techniques for this type of attack, which could inform the design of more effective defenses.

"The data-oriented programming (DOP) attack, which for the first time allows one to steal private OpenSSL keys from a server without being detected by state-of-the-art security checks, first came out in 2016," Daphne Yao, one of the researchers who carried out the study, told TechXplore. "DOP attacks appear to be quite invincible. Our entire team was intrigued and wanted to find out what kind of detection could stop DOP."

Currently, there are two main types of memory corruption attacks: control-flow and data-oriented attacks. Control-flow attacks can corrupt control data, such as the return address or code pointer, in a program's memory space, ultimately diverting the program's control flow (i.e. order of execution). Data-oriented attacks, on the other hand, are designed to change a program's benign behavior by manipulating its non-control data without violating the control flow's integrity. Despite their differences, both these types of attack can cause serious damage to a computer system.

The main objectives of the study carried out by Yao and her colleagues were to demystify data-oriented attacks, help defenders to better understand them, and identify categories of program behaviors that DOP can impact. In addition, the researchers wanted to provide experimental

evidence of the behavior differences between DOP and normal executions.

The Aalto University researchers, Hans Liljestrand, Thomas Nyman and N. Asokan, reproduced a DOP exploit based on previous research for a machine supporting Intel Processor Trace (PT). This DOP exploit was instrumental in experimentally demonstrating the differences between DOP and normal executions.

"Our intuition is that programs must somehow behave differently under the complex DOP attack," Yao said. "The frequencies of some operations must have changed during DOP. Our work does not invent new data-oriented attacks, yet we offer a comprehensive and in-depth description of them."

Although DOP attacks have become increasingly common, so far, very few studies have tried to address the threats that they pose in detail. These attacks typically corrupt important data variables that are directly or indirectly used for decision making and configuration.

"The danger of data-oriented attacks, including DOP and the newer block-oriented programming (BOP), is that they do not tamper with the control flow of a victim program," Yao explained. "Thus, it evades the popular control-flow integrity (CFI) detection. From an attack perspective, data-oriented attacks are far more advantageous than return-oriented programming (ROP), as the basic ROP attacks extensively violate control-flow integrity and can be easily detected by CFI solutions."

In their study, Yao and her colleagues mapped data-oriented exploits, including DOP attacks, outlining their assumptions, requirements and capabilities. They then experimentally assessed the feasibility of their new anomaly-based detection approach.

"We provide concrete empirical evidence showing that a program under a DOP attack exhibits substantially different behavior patterns in multiple ways, including the frequency of pairwise control transfers, the frequency of function invocations, branch correlations, and incompatible branch behaviors," Yao said. "We showed that these differences caused by DOP attacks manifest in low-level Intel PT, a highly efficient instruction level logging mechanism, logs, which can be collected and observed. For example, normal traces and DOP traces exhibit strong differences in PCA-based clustering analysis."

In their tests, Yao and her colleagues observed that DOP attacks cause side-effects at multiple levels of an affected program's control-flow behavior, which often manifest in PT traces. Although DOP attacks do not change the order of a program's control flow, they can modify its frequency and correlation properties. The researchers also provided a summary of undetectable cases, in which data-oriented attacks do not exhibit any frequency or correlation anomalies. In the future, their findings could aid the development of more effective defenses against DOP attacks.

"In our future research, we plan to address the technical challenges associated with building a deployable DOP defense," Yao said. "We are particularly interested in exploring deep learning in detecting DOP-induced anomalies from the massive amount of low-level PT logs. The key challenge in this area of study is figuring out a way to avoid excessive false alarms in detection."

**More information:** Exploitation techniques and defenses for data-oriented attacks. arXiv:1902.08359 [cs.CR]. arxiv.org/abs/1902.08359

Data-oriented programming: on the expressiveness of non-control data attacks. DOI: 10.1109/SP.2016.62. www.researchgate.net/publicati … control_Data_Attacks