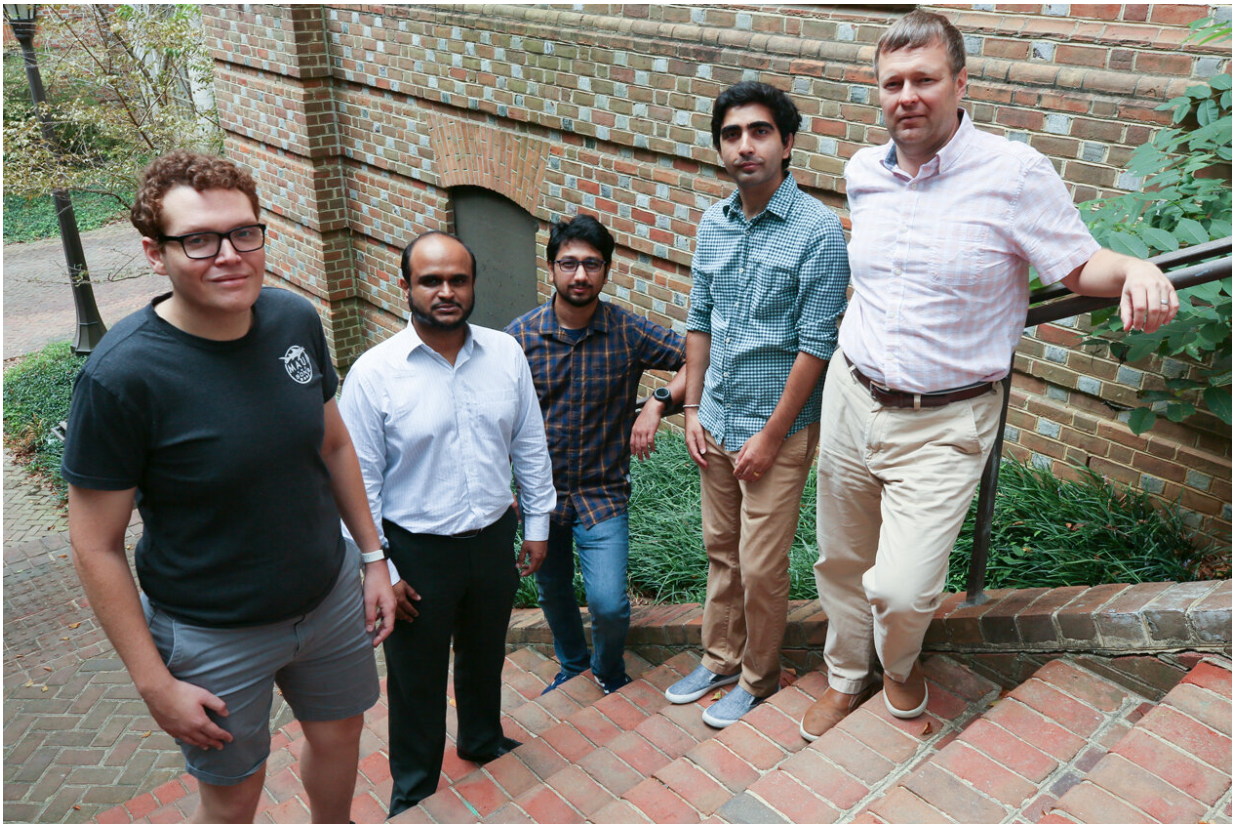
Off-the-shelf crypto-detectors give a false sense of data security

September 14 2022, by Joseph McClain



Co-authors on "Why Crypto-detectors Fail" are (from left) Nathan Cooper, Adwait Nadkarni, Amit Seal Ami, Kaushal Kafle and Denys Poshyvanyk. Nadkarni and Poshyvanyk are faculty in William & Mary's computer science department. The others are Ph.D. students in the department. Ami is lead author on the paper. (Not pictured, former Ph.D. student Kevin Moran.). Credit: Stephen Salpukas

The security of data relies on the use of proper, well-executed cryptography—the science and art of constructing algorithms that make information safe from prying and possibly malicious eyes.

"Cryptography establishes properties like confidentiality of information and integrity of information," Amit Seal Ami said. "They are based on very strict mathematical principles. Often, software engineers or programmers rely on Application Programming Interfaces—kind of like pre-built programs—that they use to try to achieve those properties in applications."

He explained that developers' reliance on those off-the-shelf, one-size-fits-many Application Programming Interfaces, or APIs, often results in a departure from sound cryptographic principles—and therefore leads to confidential data being ripe for exposure.

"So it's like they're trying to do the right things, but they're doing it in an incorrect way," Ami explained. "That's what misuse is about. Then, we have crypto-API misuse detectors, which are analysis tools that help us find such misuse in software. However, these crypto-detectors can have flaws. And if we don't know about those flaws, we have a false sense of security."

Ami is a Ph.D. candidate in William & Mary's Department of Computer Science, and the lead student author of the paper "Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques," which he presented at the 43rd Symposium on Security and Privacy of the Institute of Electrical and Electronics Engineers (IEEE).

Co-authors on the paper include Ami's advisors, Adwait Nadkarni and Denys Poshyvanyk, both faculty in the William & Mary Computer Science department, and a trio of current and former CS Ph.D. students: Nathan Cooper, Kaushal Kafle and Kevin Moran.

Ami, who was selected as a 2022 Commonwealth of Virginia Engineering and Science (COVES) Fellow and was awarded the Commonwealth of Virginia, Commonwealth Cyber Initiative (CoVA-CCI) Dissertation Fellowship in the same year, says the current state of crypto-API detectors includes a distressingly large quantity of flaws.

"What we're trying to do is to help people make better detectors—that is, detectors that can detect misuse in practice," Ami explained.

The collaborators set out to probe the flaws in crypto-API detectors that have the job of policing and correcting security weaknesses due to crypto-API misuse. They established a framework they call MASC to evaluate how well a number of crypto-API detectors work in practice.

"What we do first is look at what we know about the misuse in the first place—the ways crypto-APIs are used and misused," Ami said. "But what are the other ways they can be misused?"

Using MASC, the collaborators take those known and established vulnerabilities and tweak them, creating mutations. Then, Ami said, they study those mutations using the detectors being evaluated.

"And then we try to see if the detectors can find those mutated or changed misuse cases," he said. "And when they can't, we know that something is going wrong there."

The MASC framework revealed flaws in the detectors: "Some of the vulnerabilities missed by detectors were somewhat obvious," Ami said. "But some were very obvious.", i.e., which the detectors should have caught.

The collaborators went back to the developers of the flawed detectors to discuss the why and the how of the flaws problem. Ami said they found

differences in perspectives. Some of the developers were focusing on technique, working towards a result based on security compliance standards.

"What we were doing, on the other hand, is looking at these tools from a hostile perspective," he said. "Because when people are trying to take advantage of the flaws, they're not going to be nice about it."

The group advocates a paradigm shift: that developers abandon their technique-centric approach in favor of a more security-focused approach.

"That's what we would like to contribute," Ami said. "All these detectors, when they're being developed, should go through a hostile-review approach, so the developers can make their tools more reliable by adopting our approach."

More information: Amit Seal Ami et al, Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques. arXiv:2107.07065v5 [cs.CR], arxiv.org/abs/2107.07065

Amit Seal Ami et al, Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques, *2022 IEEE Symposium on Security and Privacy (SP)* (2022). DOI: 10.1109/SP46214.2022.9833582

Provided by The College of William & Mary