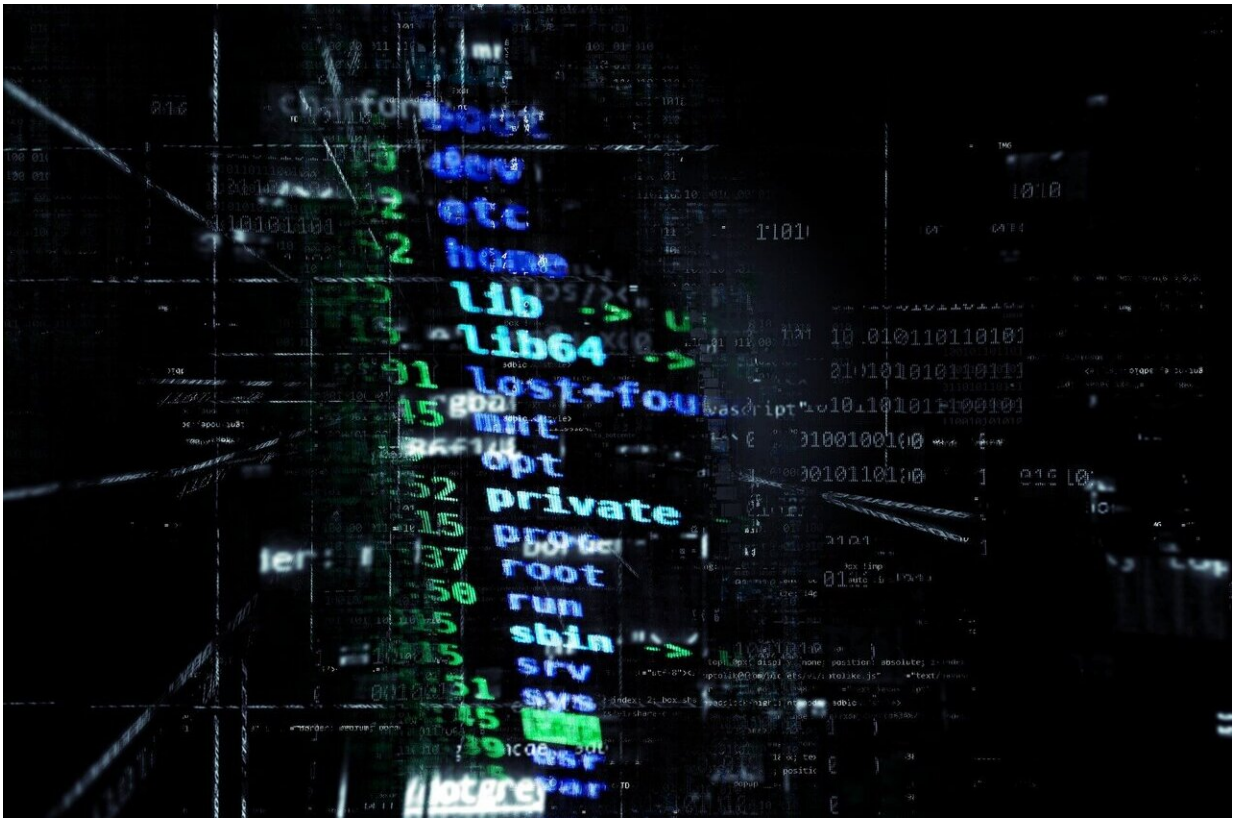
Researchers unveil new cyber protections against "logic bombs"

December 10 2021



Credit: Pixabay/CC0 Public Domain

Cybersecurity researchers at Rutgers University-New Brunswick and the Georgia Institute of Technology have proposed new ways to protect 3D printed objects such as drones, prostheses and medical devices from

stealthy "logic bombs."

The researchers will present their paper, titled "Physical Logic Bombs in 3D Printers via Emerging 4D Techniques," at the 2021 Annual Computer Security Applications Conference on Dec. 10.

Rapid prototyping is the quick fabrication of a part, model or assembly using 3D computer aided design, usually using 3D printing or "additive manufacturing." Additive manufacturing is increasingly used in a range of industries to produce safety-critical products, but there currently are no trustworthy methods for verifying their integrity against adversarial pre-print design modifications.

"Next-generation, cyber-physical additive manufacturing enables advanced product designs and capabilities, but it increasingly relies on highly networked industrial control systems that present opportunities for cyber-attacks," said principal investigator Saman Zonouz, an associate professor of electrical and computer engineering in the Rutgers-New Brunswick School of Engineering. "The predominant approach to defending against these threats relies on host-based intrusion detectors that sit within the same target controllers, and hence are often the first target of the controller attacks."

The researchers looked into Mystique, a new class of attacks on printed objects that leverage emerging 4D printing technology to introduce embedded computer code—or logic bombs—by manipulating the manufacturing process.

Mystique enables visually harmless objects to behave maliciously when a logic bomb is triggered by a stimulus such as changes in temperature, moisture, pH or modifications to the materials used initially, potentially causing catastrophic operational failures when they are used.

The researchers successfully evaluated Mystique on several 3D printing case studies and showed that it can evade prior countermeasures. To address this, they proposed two strategies.

The first solution focuses on designing a sensor that can measure the composition and diameter of raw materials passing through the printer's extruder to ensure they meet expectations before the object is printed. A dielectric sensor can detect a change of 0.1mm in filament diameters and a change of 10% in concentration composition.

The second solution uses high-resolution computed tomography images to detect residual stresses in printed objects that contrast benign and malicious designs before activation of the attack. This CT detection has an accuracy of 94.6% in identifying 4D attacks in a single printing layer.

The research team plans to provide guidelines to tie together resilience solutions in software security, control system design and signal processing, and to incorporate reliable and practical cyber-physical attack detection into real-world manufacturing.

"Our proposal is a novel potential attack vector that needs to be considered and mitigated effectively in additive manufacturing platforms. The idea is to use new physical logic bombs in 3D printed objects, such as industrial gears and personal protective equipment like COVID-19 masks," Zonouz said. "These logic bombs can later be activated by the adversaries using physical stimulus like moisture or heat whenever suitable for them to make the printed objects malfunction, such as to make a COVID mask lose its protection against the viral infection."

More information: Paper: www.openconf.org/acsac2021/mod … n=summary.php&id=117

Provided by Rutgers University