First complete sabotage attack demonstrated on a 3-D printed drone propeller

October 20 2016

Researchers from three universities combined their expertise to demonstrate the first complete sabotage attack on a 3D additive manufacturing (AM) system, illustrating how a cyber attack and malicious manipulation of blueprints can fatally damage production of a device or machine.

In their paper titled "Dr0wned," researchers from Ben-Gurion University of the Negev (BGU), the University of South Alabama and Singapore University of Technology and Design detail how to sabotage the quality of a 3D-printed functional part, which leads to the destruction of a device.

A proof-of-concept video shows how the researchers destroyed a $1,000 quadcopter UAV drone by hacking into the computer used to control the 3D printing of replacement propellers. Once they penetrated the computer, the researchers identified the propeller blueprint file and inserted defects undetectable by visual inspection. During flight tests, the sabotaged propeller broke apart during ascent, causing the drone to smash into the ground.

More than 100 industries, including aerospace, automotive and defense, employ additive printing processes. According to the Wohlers Report, the AM industry accounted for $5.165 billion of revenue in 2015. Furthermore, 32.5 percent of all AM-generated objects are used as functional parts.

"Imagine that an adversary can sabotage functional parts employed in an airplane's jet engines. Such an attack could cost lives, cause economic loss, disrupt industry, and threaten a country's national security," says Prof. Yuval Elovici. Elovici is a member of BGU's Department of Software and Information Systems Engineering, director of the Deutsche Telekom Innovation Labs @ BGU and the BGU Cyber Security Research Center (CSRC). The CSRC is a collaboration between the University and Israel's National Cyber Bureau, focused on advanced cyber security topics.

"With the growth of additive manufacturing worldwide, we believe the ability to conduct malicious sabotage of these systems will attract the attention of many adversaries, ranging from criminal gangs to state actors, who will aim either for profit or for geopolitical power," says Elovici.

"'Dr0wned' is not the first article that raises this issue. However, all prior research has focused on a single aspect of a possible attack, assuming that all other attack elements are feasible," the researchers say. "This is the first experimental proof of a complete attack chain initiated by sabotaging the 3D-printed propeller."

The collaborative study addresses the dangerous consequences of cyber attacks, and proposes a systematic approach for identifying opportunities and a methodology for assessing the level of difficulty of an attack involving AM.

Provided by American Associates, Ben-Gurion University of the Negev