SUCCESS STORY

FFG
Promoting Innovation.

SBA Research

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET K1

Type of project: Combinatorial Security Testing (CST), strategic, 6 weeks, single-firm

VULNERABILITY IN REVERSE VENDING MACHINES

THE CST TEAM OF **MATRIS RESEARCH GROUP** (SBA RESEARCH) DETECTED A SECURITY VULNERABILITY IN A REVERSE VENDING MACHINE FOR DEPOSIT BOTTLES

As the effects of climate change are becoming more visible to the public, citizens, governments, and international organizations are pursuing new ways to stifle global warming. In order to encourage recycling and thus help preserve resources, the Austrian government enacted a bill that will introduce a deposit on plastic bottles and beverage cans by 2025. As the primary point of contact for returning such containers, reverse vending machines are integral infrastructure components.

Not least because of this increased importance, it is essential to consider that reverse vending machines may have vulnerability issues, as with every automated device. Therefore, the Combinatorial Security Testing (CST) team of the MATRIS Research Group (SBA Research) performed an investigation of potential attacks against such devices. Security researcher Jovan Zivanovic was able to manipulate deposit receipts using an off-the-shelf receipt printer (available to everybody at low cost), eventually enabling him to obtain free products from a supermarket.

The security of reverse vending machines depends on two related properties: authenticity and integrity. *Authenticity* ensures that only receipts that have been issued by a real reverse vending machine and installed by the respective store (or chain) are accepted; *integrity* means that modifications to existing vouchers – e.g., by adding bottles that were never returned and thus increasing the value of the receipt – can be detected. Additionally, it is important to ensure that reverse vending receipts can be used only once, for instance by using a central online registry that keeps track of all issued vouchers, and documents whether they have been redeemed. Together, these security measures help to prevent fraud and unforeseen losses; however, they are not always implemented correctly, as the recent investigation shows.

Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

Version 01/2020

As Zivanovic points out, simple office equipment, a little know-how, and some spare time would be sufficient to manipulate reverse vending machines in order to gain money through fraud. Moreover, according to the investigation by the CST team, the vulnerability was not specific to one store, but rather an issue that impacts vending machines deployed throughout the whole supermarket chain. Dimitris Simos, head of MATRIS Research Group, emphasizes that other vulnerabilities in reverse vending machines may exist. Such issues would likely impact predominantly older models – as these are not equipped to classify containers based on their shape, material, and weight – and may struggle to accurately identify bottles. CST team lead Manuel Leithner underlines that the upcoming Austrian bill should be seen as an opportunity for supermarket chains to replace vulnerable reverse vending machines, thus avoiding fraud. Alternatively, he suggests that proprietary security mechanisms may offer sufficient protection against such attacks.

Impact and effects

After implementing a proof of concept, our researchers were able to redeem fraudulent reverse vending receipts in a Viennese supermarket. As these types of vulnerabilities are not limited to a single supermarket chain and can regularly occur in old reverse vending machines, this topic concerns not just stores, but also the vendors of such devices. Consequently, the MATRIS group notified the supermarket chains and vendors of the affected machines to remediate current vulnerabilities and help avoid similar issues in the future.

MATRIS Research Group Members
From right to left: Dominik Schreiber, Michael Wagner, Jovan Zivanovic, Ludwig Kampel, Manuel Leithner, Bernhard Garn, Dimitris Simos, *Ilias Kotsireas (External)* © SBA

Subsequently, SBA Research published a press release in German and English to raise public awareness; the press release was picked up by some of the most popular Austrian newspapers, radio channels, and technology magazines, including Heute, Kronehit, Future Zone, and Börse-Express. By raising public awareness, we hope to motivate affected stakeholders to strengthen their defenses against vending machine fraud.

Project coordination (Story)
Priv.-Doz. Dr. Dimitris E. Simos,
Key Researcher
MATRIS Group Leader
SBA Research
T +43 (0) 1 505 38 88
dsimos@sba-research.org

SBA Research gGmbH
Floragasse 7, 5. OG
1040 Wien
T +43 (0) 664 4111588
mklemen@sba-research.org
www.sba-research.org

This success story was provided by the centre management for the purpose of being published on the FFG website. SBA-K1 is a COMET-Centre within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the City of Vienna. The COMET Programme is managed by FFG. Further information on COMET: www.ffg.at/comet