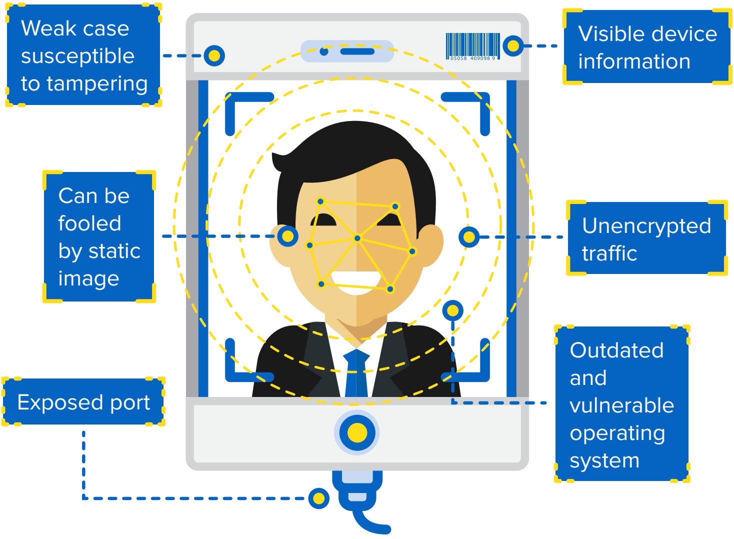
ALL ACCESS

The Problem With Contactless Security Solutions

Access control devices that use facial recognition have become a critical part of the enterprise security infrastructure. Organizations are increasingly deploying these devices to determine who can enter secured premises. We looked into the security posture of specific models of these devices and discovered inherent weaknesses that could severely compromise the businesses that use them. We tested four different devices, exposing them to cyber as well as physical attacks, and found that we were able to bypass their security measures. In one case, we were even able to open doors using only a static image of a person's face.

EDGE-BASED ACCESS CONTROL DEVICES


Weak case susceptible to tampering
Visible device information
Can be fooled by static image
Unencrypted traffic
Outdated and vulnerable operating system
Exposed port

These access control devices are an example of a new computing paradigm called edge computing, an architecture designed to bring compute nodes closer to the sensors and the actuators at the edges of the network. Because of its properties of low latency, data locality, and reduced bandwidth consumption, edge computing has been used in critical applications such as fleet control, smart farming, and building automation.

However, migrating the bulk of the computing tasks to the edge introduces new risks. Edge nodes are often exposed in the field, increasing the chances of tampering and risking access to the rest of the enterprise network. This system also raises the probability of theft and the compromise of any data stored in the devices.

IMPACT ON ENTERPRISES

In our research, we uncovered several weaknesses in edge-based access control devices that are tightly linked to the new device architecture. These security gaps could let malicious actors perform various actions such as:

Breaking the physical security of a building	Adding unauthorized users	Becoming a device administrator
Exfiltrating sensitive enterprise data	Remotely opening doors to private areas	Installing applications on the device

HOW TO PREVENT INTRUSIONS

In our research paper, titled "Identified and Authorized: Sneaking Past Edge-Based Access Control Devices," we discuss some guidelines that can help manufacturers create more secure devices, including encrypting communication, hardening devices, and pushing regular security updates. We also provide advice to help enterprise users mitigate the risks introduced by vulnerable devices: securing devices physically, securing communications, and using network monitoring solutions.

Learn more about how hackers could attack edge-based access control devices and how enterprises could mitigate the risks at http://bit.ly/edgedevicesecurity.

TREND MICRO™ | research