The Last Byte

Security Arms Race

Scott Davidson

In the classic short-short science fiction story "The Swordsmen of Varnis," by Clive Jackson, a warrior hero and Martian princess are facing the enemy. Swords flashing, our heroes are about to win until one swordsman says "Bah, this is ridiculous," takes out his ray gun and blasts our poor heroes out of existence. You might remember a similar scene in "Raiders of the Lost Ark" where Indy, about to duel a bad guy, just shoots him instead.

What has this to do with *IEEE Design&Test* and this special issue on security? Both stories show the importance of a balance of weapons.

The articles in this issue are about defensive weapons to be deployed against offensive weapons such as side-channel attacks and fault injection to determine keys for encryption.

Each defensive weapon has a cost in time, effort, performance, and money. Some, like tests to prove that Trojans have not been inserted in an IC by a suspect fab, do not affect the end customer. Some, like checks for fault injection, do, though no such attack may ever occur for a particular part type.

Knights in armor in the olden days were protected from many attacks, but at the cost that if they fell off their horses, they could hardly stand again. Sometimes, I feel that half my CPU cycles are used by antivirus software, antiadware software, download scanning, and so on. We do not want our computer equipment to be so heavily armored that it can barely move.

I think it would be helpful if articles on techniques to thwart various threats give an indication of the likelihood of the threat occurring and the cost if the threat becomes real. The article by Konstantinou et al. in this issue describes a method that can detect ransomware attacks. The frequency and severity of these are well known. Some other articles address threats that can cause severe damage but are perhaps less likely.

Consider security for a retail store. It certainly makes sense to lock up valuable merchandise. It might make sense to put up protection for store windows. It is unlikely to make sense to make this protection strong enough to resist attack by a tank. Someone who can afford to buy a tank is not going to be interested in robbing your candy store.

There are more unskilled attackers, such as those who call you every day, than skilled ones. If an attack requires a team of highly paid experts, you only need to worry if you have something extremely valuable to protect. Counterfeiting or stealing chips is easy. Inserting Trojans is hard. Unless there is a specific reason to target a chip, the criminals will do what is easiest for them. Fort Knox, where gold is stored in the United States, needs protection against tanks. If a criminal sees a grate on a candy store window, he will go somewhere else.

Let us include a section in the introduction of articles on security that looks at the problem from the attackers' point of view. Then those deciding what security to implement will have a better idea of the risks and rewards. ■

Digital Object Identifier 10.1109/MDAT.2022.3178347
Date of current version: 22 June 2022.

■ Direct questions and comments about this department to Scott Davidson; davidson.scott687@gmail.com; Twitter: @scottd687.

2168-2364/22©2022 IEEE Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC