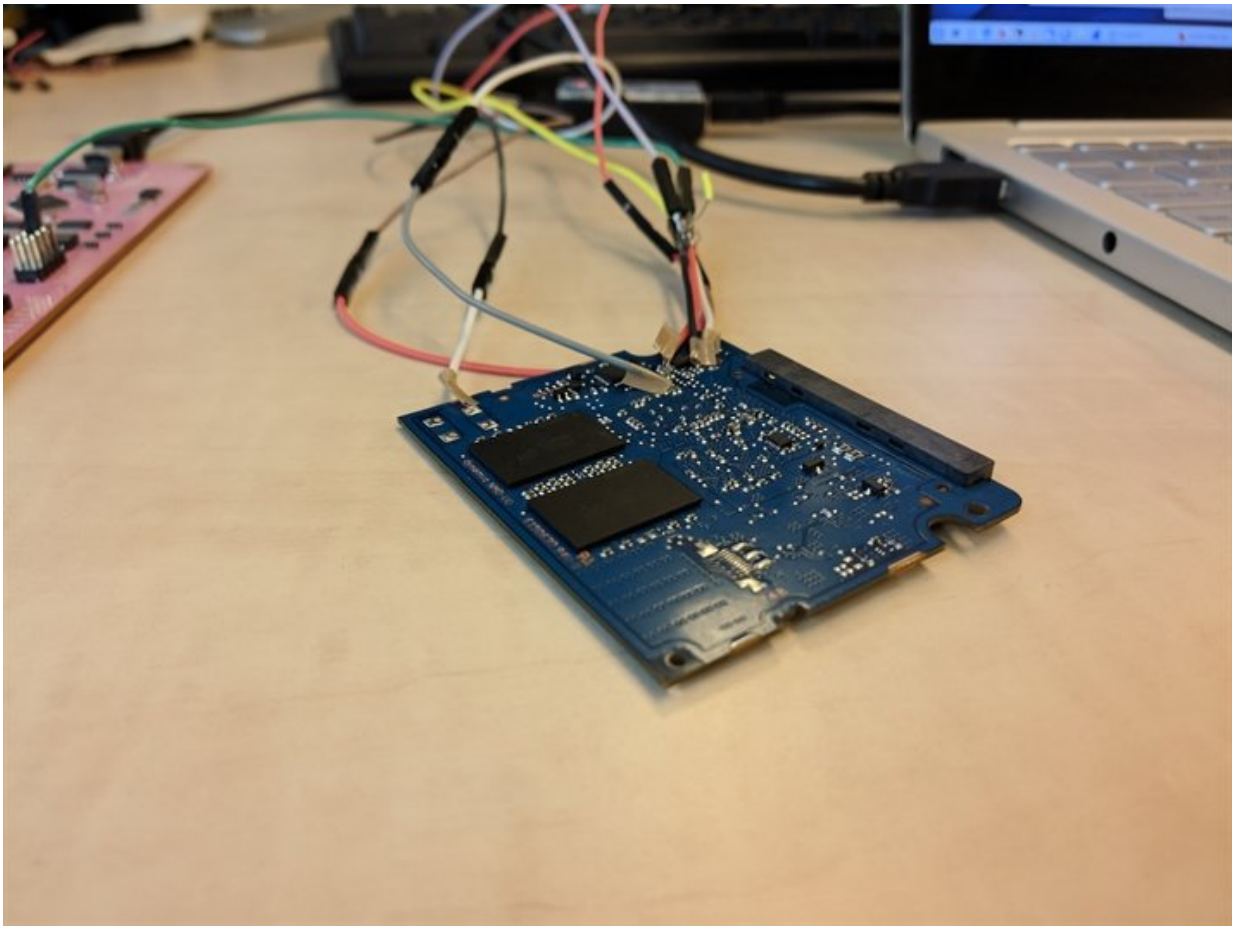
Researchers discover security flaws in widely used data storage devices

November 7 2018



Credit: Radboud University

Researchers at Radboud University in the Netherlands have discovered

that widely used data storage devices with self-encrypting drives do not provide the expected level of data protection. A malicious expert with direct physical access to widely sold storage devices can bypass existing protection mechanisms and access the data without knowing the user-chosen password.

These flaws exist in the encryption mechanism of several types of solid state drives – listed below – of two major manufacturers, namely Samsung and Crucial. The vulnerabilities occur both in internal storage devices (in laptops, tablets and computers) and in external storage devices (connected via a USB cable). The storage devices affected include popular models that are currently widely available.

Researcher Bernard van Gastel: "The affected manufacturers were informed six months ago, in line with common professional practices. The results are being made public today so that users of the affected SSDs can protect their data properly." Researcher Carlo Meijer: "This problem requires action, especially by organisations storing sensitive data on these devices. And also by some consumers who have enabled these data protection mechanisms. But most consumers haven't done that."

If sensitive data needs to be protected, it is in any case advisable to use software encryption and not rely solely on hardware encryption. One option is to use the free and open source VeraCrypt software package, but other solutions do exist. On computers running Windows, BitLocker provides software encryption, and data may not be secure (see "Windows computers" below).

Encryption is the main data protection mechanism. It may be implemented in software or hardware (e.g. in SSDs). Modern operating systems generally offer software encryption for the whole storage. However, it may happen that such an operating system decides to rely

solely on hardware encryption (if hardware encryption is supported by the storage device). BitLocker, the encryption software built into Microsoft Windows, can make this kind of switch to hardware encryption but offers the affected disks no effective protection in these cases. Software encryption built into other operating systems (such as macOS, iOS, Android, and Linux) seems to be unaffected if it does not perform this switch.

The researchers identified these security issues using public information and around €100 of evaluation devices. They bought the SSDs that they examined via regular retail channels. It is quite difficult to discover these problems from scratch. However, once the nature of the issues is known, there is a risk that the exploitation of these flaws will be automated by others, making abuse easier. The researchers at Radboud University will not release such an exploitation tool.

Affected Products

The models for which vulnerabilities have actually been demonstrated in practice are:

- Crucial (Micron) MX100, MX200 and MX300 internal hard disks;
- Samsung T3 and T5 USB external disks;
- Samsung 840 EVO and 850 EVO internal hard disks.

It should be noted, however, that not all disks available on the market have been tested. Specific technical settings (related to e.g. "high" and "max" security) in which internal drives are used may affect the vulnerability (see the detailed information provided by the manufacturers and technical information link below).

Windows Computers

On computers running Windows, a software component called BitLocker handles the encryption of the computer's data. In Windows, the kind of encryption that BitLocker uses (i.e. hardware encryption or software encryption) is set via the Group Policy. If available, standard hardware encryption is used. For the affected models, the default setting must be changed so that only software encryption is used. This change does not solve the problem immediately, because it does not re-encrypt existing data. Only a completely new installation, including reformatting the internal drive, will enforce software encryption. As an alternative to reinstallation, the above-mentioned VeraCrypt software package can be used.

Responsible Disclosure

Both manufacturers were informed of this security problem in April 2018 by the National Cyber Security Centre (NCSC) of the Netherlands. The university provided details to both manufacturers to enable them to fix their product. The manufacturers will themselves provide detailed information to their customers about the affected models; links are listed below.

When discovering a security flaw, there is always a dilemma on how to handle this information. Immediate publication of the details could encourage attacks and inflict damage. Keeping the flaw secret for an extended period could mean that necessary steps to counter the vulnerability are not taken, while people and organisations are still at risk. It is common practice in the security community to try to strike a balance between these concerns, and reveal flaws after up to 180 days after the manufacturers of the affected products have been informed. This practice, known as responsible disclosure, is used as standard by

Radboud University.

The researchers are now about to publish the scientific aspects of their findings in the academic literature. A preliminary version of these findings (pdf, 757 kB) will be published today, 5 November 2018. Once the peer-review process has been completed, a final version will be published in the academic literature. This publication cannot be used as a guide on how to break into SSDs.

Provided by Radboud University