Two new attacks break PDF certification

May 25 2021

IT security experts at RUB have found several security issues with digital signatures for PDF documents over the past years. Credit: RUB, Kramer

A security issue in the certification signatures of PDF documents has been discovered by researchers at Ruhr-Universität Bochum. This special form of signed PDF files can be used, for instance, to conclude contracts. Unlike a normal PDF signature, the certification signature permits certain changes to be made in the document after it has actually been signed. This is necessary to allow the second contractual party to also sign the document. The team from the Horst Görtz Institute for IT Security in Bochum showed that the second contractual party can also change the contract text unnoticed when they add their digital signature, without this invalidating the certification. The researchers additionally discovered a weakness in Adobe products that enables attackers to implant malicious code into the documents.

Simon Rohlmann, Dr. Vladislav Mladenov, Dr. Christian Mainka and Professor Jörg Schwenk from the Chair for Network and Data Security are presenting the results at the 42nd IEEE Symposium on Security and Privacy, which is taking place as an online conference from 24 to 27 May 2021. The team has also published the results on the website pdf-insecurity.org .

24 out of 26 applications affected

When using certification signatures, the party who issues the document and signs it first can determine which changes the other party can then make. For instance, it is possible to add comments, insert text into special fields, or add a second digital signature at the bottom of the document. The Bochum group circumvented the integrity of the protected PDF documents with two new attacks—called Sneaky Signature Attack (SSA) and Evil Annotation Attack (EAA). The researchers were thus able to display fake content in the document instead of the certified content, without this rendering the certification invalid or triggering a warning from the PDF applications.

The IT security experts tested 26 PDF applications, in 24 of which they were able to break the certification with at least one of the attacks. In eleven of the applications, the specifications for PDF certifications were also implemented incorrectly. The detailed results have been published online.

Malicious code can be implanted into Adobe documents

In addition to the security loopholes described above, the team from the Horst Görtz Institute also discovered a weakness specifically in Adobe products. Certified Adobe documents can execute JavaScript code, such as accessing URLs to verify the identity of a user. The researchers showed that attackers could use this mechanism to implant malicious code into a certified document. This makes it possible, for instance, for a user's privacy to be exposed by sending his IP address and information about the PDF applications used to an attacker when the document is opened.

More information: Breaking the specification: PDF certification, 42nd IEEE Symposium on Security and Privacy, online conference, 2021,

www.computer.org/csdl/proceedi …
3400b902/1t0x9ObxH8Y

Provided by Ruhr-Universitaet-Bochum