"Two New Attacks Break PDF Certification"

Submitted by grigby1 on Tue, 05/25/2021 - 2:16pm

Researchers at Ruhr-University Bochum (RUB) have discovered a security issue in the certification signatures of PDF documents. This form of signed PDF files can be used in the conclusion of contracts. The certification signature allows certain changes to be made to the document after it has been signed so that a second contractual party can also sign the document, unlike a normal PDF signature. The researchers at the Horst Gortz Institute for IT Security in Bochum demonstrated that it is possible for the second contractual party to change the contract text when adding their digital signature, without invalidating the certification. The integrity of the protected PDF documents was undermined through the performance of two new attacks called the Sneaky Signature Attack (SSA) and the Evil Annotation Attack (EAA). These attacks allowed the researchers to display fake content in the document instead of the certified content. They did this without rendering the certification invalid or triggering the PDF applications to warn users. Out of the 26 PDF applications tested by the security experts, 24 were found to be affected by at least one of the attacks. They also discovered a vulnerability contained by Adobe products that attackers could exploit to insert malicious code into certified Adobe documents. This article continues to discuss the demonstration of two new attacks that can break PDF certification, along with the discovery of a weakness in Adobe products that can be used to implant malicious code into Adobe documents.

RUB reports "Two New Attacks Break PDF Certification"