German researchers break W3C XML encryption standard

October 19 2011

Standards are supposed to guarantee security, especially in the http://www. The World Wide Web Consortium (W3C) is the main force behind standards like HTML, XML, and XML Encryption. But implementing a W3C standard does not mean that a system is secure. Researchers from the chair of network and data security have found a serious attack against XML Encryption. "Everything is insecure", is the uncomfortable message from Ruhr-University Bochum researchers.

XML stands for "eXtensible Markup Language", and is the industry standard for platform-independent data exchange. Companies like IBM, Microsoft and Redhat Linux use XML standards for integrating Webservice projects for large customers. XML Encryption was designed to protect the confidentiality of the exchanged data. Reason enough to have a closer look at its security.

Juraj Somorovsky and Tibor Jager exploited a weakness in the CBC mode for the chaining of different ciphertext blocks. "We were able to decrypt data by sending modified ciphertexts to the server, by gathering information from the received error messages." The attack was tested against a popular open source implementation of XML Encrytion, and against the implementations of companies that responded to the responsible disclosure – in all cases the result was the same: the attack works, XML Encryption is not secure. Details of the attack are presented at this year's ACM Conference on Computer and Communications Security.

"There is no simple patch for this problem", states Somorovsky. "We therefore propose to change the standard as soon as possible." The researchers informed all possibly affected companies through the mailing list of W3C, following a clear responsible disclosure process. With some companies there were intensive discussions on workarounds.

Provided by Ruhr-University Bochum