On the Insecurity of XML Security

Juraj Somorovsky

XML Encryption and XML Signature describe how to apply encryption and signing algorithms to XML documents. These specifications are implemented in XML frameworks of major commercial and open source organizations like Apache, IBM, Microsoft, or SAP. They are employed in a large number of major web applications, ranging from business communications, eCommerce, and financial services over healthcare applications to governmental and military infrastructures.

This thesis analyzes the security of these specifications and presents several practical and highly critical attacks. First, it describes different classical and novel XML Signature Wrapping (XSW) attack techniques, which allow to break integrity of signed XML documents. The attacks exploit weak interfaces between XML Signature validation and XML processing modules deployed in different frameworks. Their criticality is confirmed by applications to cloud and Single Sign-On interfaces: an attacker was able to use them to gain control over victim's Amazon and Eucalyptus cloud instances, or log in as an arbitrary user in Single Sign-On domains of Salesforce and IBM products.

Second, the thesis describes several practical attacks on XML Encryption. The attacks break confidentiality of RSA PKCS#1 v1.5 encrypted ciphertexts (used for key transport) and CBC encrypted symmetric ciphertexts (used for data encryption). An attacker can decrypt such ciphertexts by sending related ciphertexts to a server processing encrypted messages. He can recover the whole ciphertext by issuing a few hundreds or several thousands of requests, depending on the considered scenario.

The work described in this thesis influenced many XML frameworks and systems, as well as the W3C XML Encryption recommendation. These were updated to prevent the attacks. The thesis summarizes best practices to counter all the described attacks in different practical scenarios that were developed in collaboration with developers and members of standardization groups.