Checkmate! Researchers outsmart Intel copy protection HDCP

November 28 2011, by Jens Wylkop

For over a decade, Intel's widely used copy protection HDCP has been trusted by the media industry, which carries out business in high-resolution digital video and audio content worth thousands of millions. Researchers from the working group on secure hardware led by Prof. Dr.-Ing. Tim Güneysu of the Ruhr-Universität Bochum were able to checkmate the protection system of an entire industry with relatively little effort using a so-called "man-in-the-middle" attack.

They will be presenting their results next week at the international security conference ReConFig 2011 in Cancun, Mexico.

HDCP is now found in almost every HDMI or DVI-compliant TV or computer flat screen. It serves to pass digital content from a protected source media, such as a Blu-ray, to the screen via a fully encrypted channel. There have been concerns about the security of the HDCP system for some time. In 2010, an HDCP master key, which is intended to form the secret core element of the encryption system, appeared briefly on a website. In response, the manufacturer Intel announced that HDCP still represented an effective protection component for digital entertainment, as the production of an HDCP-compatible chip using this master key would be highly complex and expensive.

That caught the attention of Bochum's researchers. "We developed an independent hardware solution instead, based on a cheap FPGA board" explained Prof. Dr.-Ing. Tim Güneysu, who set to work with the final year student Benno Lomb. "We were able to tap the HDCP encrypted data streams, decipher them and send the digital content to an unprotected screen via a corresponding HDMI 1.3-compatible receiver." We used the commercial ATLYS board from the company Digilent with a Xilinx Spartan-6 FPGA, which has the necessary HDMI interfaces and a serial RS232 port for communication.

In their studies, the aim was never to find a way of making illegal copies. "Rather, our intention was to fundamentally investigate the safety of the HDCP system and to financially assess the actual cost for the complete knockout" reported Prof. Güneysu. "The fact that we have achieved our goal in a degree thesis and with material costs of approximately 200 Euro definitely does not speak for the safety of the current HDCP system."

This "man-in-the-middle" attack in which a middleman (the ATLYS FPGA board) manipulates the entire communication between the Blu-ray player and the flat screen TV without being detected is of little interest for pirates in practice due to the availability of simpler alternatives. The scientists do, however, envisage a real threat to security-critical systems, for example at authorities or in the military. Although Intel is already offering a new security system, HDCP 2.0, due to the backward compatibility, the weak point will also remain a problem in coming years, concluded Prof. Güneysu.

Provided by Ruhr-University Bochum

Citation: Checkmate! Researchers outsmart Intel copy protection HDCP (2011, November 28) retrieved 9 April 2024 from https://phys.org/news/2011-11-checkmate-outsmart-intel-hdcp.html