SECURITY RESEARCH

LIST OF QUESTIONS PENDING ANSWER FROM MICROSOFT

Last update: 21-03-2023

This document contains a list of questions Microsoft was not willing to answer (original inquiry from 2019, partially answered by Microsoft in Nov 2022 [1], request for missing answers 1-3 along questions 4-5 sent on Jan 14, 2023, a kind reminder of the inquiry sent on Jan 23, 2023).

1) Has MS Play Ready technology been used properly in the environment of Canal+ SAT TV operator to protect PayTV content of premium content providers such as HBO, Fox and Canal+ ?

2) does MS Play Ready provide proper (any) security of content if the underlying set-top-box is compromised (its keys are compromised) ?

3) did Canal+ or set-top-box vendor (ADB) violate any agreement signed with Microsoft regarding the use of MS Play Ready technology ?

   As of Mar 2023, both companies are listed as "Approved Microsoft PlayReady licensees" at this location:
   https://www.microsoft.com/playready/licensing/list/

4) Microsoft has been the only party that received access to Security Explorations' MSPR Toolkit codes [2]. Have these been shared with any other 3rd party by your company (such as ADB or Canal+) ?

5) taking into account Microsoft's likely involvement in the development of the mitigation for CANAL+ and other PlayReady licensees ("we expect to be finished with the mitigation in March of 2023" line received on Dec 1, 2022 from the company), is Microsoft planning to make use of any ideas outlined in Security Explorations research / write-up to make PlayReady implementation more secure in the environment of Canal+ (or any other PlayReady licensee) ?

The base idea for HW pairing of cert / license has been described in the README.md file accompanying the research and it has been explained in a more detail at this document (information about the document and its link provided to Microsoft):
https://security-explorations.com/materials/mspr_ideas.pdf

The following additional questions have been sent to Microsoft on Mar 16, 2023:

6) has Microsoft informed any PlayReady licensees of the risks exposed by Security Explorations' research and targeting this technology ?

7) has Microsoft implemented any technological means over the course of last 7+ months (since Jul/Aug 2022, the time of reporting PlayReady research material to the company) and aimed at improving security of PlayReady in the environment of Canal+ (or any other PlayReady licensee) ?

8) does Mar 2023 still holds as the time when mitigation is to be deployed / released for the issues exposed in Canal+ environment ?

9) is Canal+ legally bound (through Microsoft PlayReady license agreement or any other agreement) not to discuss any security matters with a 3rd party such as Security Explorations and pertaining to PlayReady security, even if such a party is willing to assist PlayReady licensee (i.e. provide complete information that could turn out to be helpful during the process of resolution of the issue) ?

10) is there anything published at Security Explorations' PlayReady security research project page that is incorrect or Microsoft does not agree with ?

References

[1] Technical material regarding security vulnerabilities of NC+ Platform from 2019, APPENDIX C
https://security-explorations.com/materials/SRP-2018-02-report.pdf

[2] Microsoft Play Ready Toolkit, Proof of Concept code
https://security-explorations.com/microsoft-playready.html#details