How to Break Microsoft Rights Management Services

Workshop on Offensive Technology

Christian Mainka, Paul Rösler, Jörg Schwenk and Martin Grothe
Motivation

• Going to talk about Enterprise Rights Management (ERM)

• Consumer version: Digital Rights Management (DRM)
  – Music, movies, e-books

• ERM goal: protect (digital) company assets

• Useful for different scenarios
Motivation

Ministry of Defence CIO introduces Defence-as-a-Platform with the help of Microsoft

UK MoD looks to be more agile with its IT service delivery, and Microsoft is playing a big part.

Microsoft AD RMS integrates deep into Microsoft Office to provide a consistent and familiar experience for Bank of India end users to protect sensitive information. The tool helps to augment its security strategy by protecting information stored on computers, mobile devices, and in the cloud. AD RMS also prevents sensitive information (confidential e-mail messages) from intentional or accidental disclosure, ensuring that protected information is not exposed to unauthorized access.

Stone also said that he was impressed with the capabilities that Microsoft was offering as part of its cloud services, such as Azure Active Directory, Azure Rights Management and the Enterprise Mobility Suite. Together, these offer a "fantastic set of capabilities" that the MoD aims to exploit to deliver greater mobility, he explained.
Agenda

1. Motivation
2. Microsoft RMS
3. DisARMS Attack #1 (unprotect)
4. DisARMS Attack #2 (modification)
5. Conclusion
Microsoft RMS - Intro

Microsoft
Active Directory

Azure

Office 365
Microsoft RMS - High Level

- Set specific rights for a person and/or group via e-mail addr.
- Use sym. and asym. cryptography
  - AES content encryption
  - PKI (RSA)
  - Licenses
- Use license (UL)
- Publishing license (PL)
Microsoft RMS PKI

- Root Cert has separate PrivK
- SLC has separate PrivK
- SLC is signed with Root\textsubscript{PrivK}
- SPC has separate PrivK
- SPC is self-signed
- \( \text{RAC}_{\text{PubK}} \) and encrypted \( \text{RAC}_{\text{PrivK}} \) are signed by \( \text{SLC}_{\text{PrivK}} \)
- \( \text{CLC}_{\text{PubK}} \) and encrypted \( \text{CLC}_{\text{PrivK}} \) are signed by \( \text{SLC}_{\text{PrivK}} \)
Microsoft RMS
Create File

- PL content encrypted with $SLC_{PubK}$
- PL signed with author $CLC_{PrivK}$
- Author CLC signed with $SLC_{PrivK}$
Microsoft RMS
Create File

Demonstration
Microsoft RMS
Consume File

AD RMS Server

SLC

pubK

privK

Rights

(3.)

(2.)

UL

Rights

(4.)

(3.)

AD RMS Protected File
(read rights only)

Microsoft Word

protected area
rights are enforced

(9.)

(10.)

Windows 7

user RAC

pubK

privK

(7.)

machine SPC

pubK

privK

bob@company.com

HOW TO BREAK MICROSOFT RIGHTS MANAGEMENT SERVICES | WOOT | 08.08.2016
Microsoft RMS Attacks

• Responsible disclosed in april 2016
• Case number MSRC 33210
• We used:
  – C++
  – RMS SDK 2.1
• Attack requirements:
  – View access right
  – C++ Redistributable 2015
  – That is all 😊
Agenda

Motivation

Microsoft RMS

DisARMS Attack #1 (unprotect)

DisARMS Attack #2 (modification)

Conclusion
Microsoft RMS
DisARMS #1

Protection Removal Attack

(1.)
(2.)
(3.)
(4.)
(4a.)
(4c.)
(5.)
(6.)
(7.)
(8.)
(9.)

PL

Author CLC

encrypted content

peer

Rights

pubK

MS client lockbox

UL

RAC

pubK

privK

Machine SPC

SLC

pubK

privK

AD RMS Server

document with unprotected content

charlie@external.com
Microsoft RMS
DisARMS #1

Demonstration
Agenda

- Motivation
- Microsoft RMS
- DisARMS Attack #1 (unprotect)
- DisARMS Attack #2 (modification)
- Conclusion
DisARMS #2 modification
DisARMS #2
modification

Demonstration
Microsoft Response

From: Microsoft Security Response Center
secure@microsoft.com

“. . . The type of attack you present falls in the category of policy enforcement limitations. Policy enforcement capabilities, such as the ability to prevent printing or modifying content to which the user has legitimate access, are not guaranteed by cryptography or other hard technical means . . . ”
Agenda

Motivation

Microsoft RMS

DisARMS Attack #2 (modification)

DisARMS Attack #1 (unprotect)

Conclusion
Conclusion

• RMS is used by important companies and ministry

• AD RMS, Azure RMS, etc. are not secure

• DisARMS #1 can not be prevented (look DRM)
  – Just make it not that simple

• DisARMS #2 can be prevented (see paper)

• Microsoft seems to has no interest in fixing the attacks
Questions?

Email: martin.grothe@rub.de

Email: christian.mainka@rub.de
Twitter: @CheariX

Code on Github: RUB-NDS/MS-RMS-Attacks

Further Infos: web-in-security.blogspot.de

Sponsored by German Ministry for Education and Research
Agenda

Motivation

Microsoft RMS

DisARMS Attack #2 (modification)

DisARMS Attack #1 (unprotect)

Conclusion