

RUB

RUHR-UNIVERSITÄT BOCHUM

How to Break Microsoft Rights Management Services

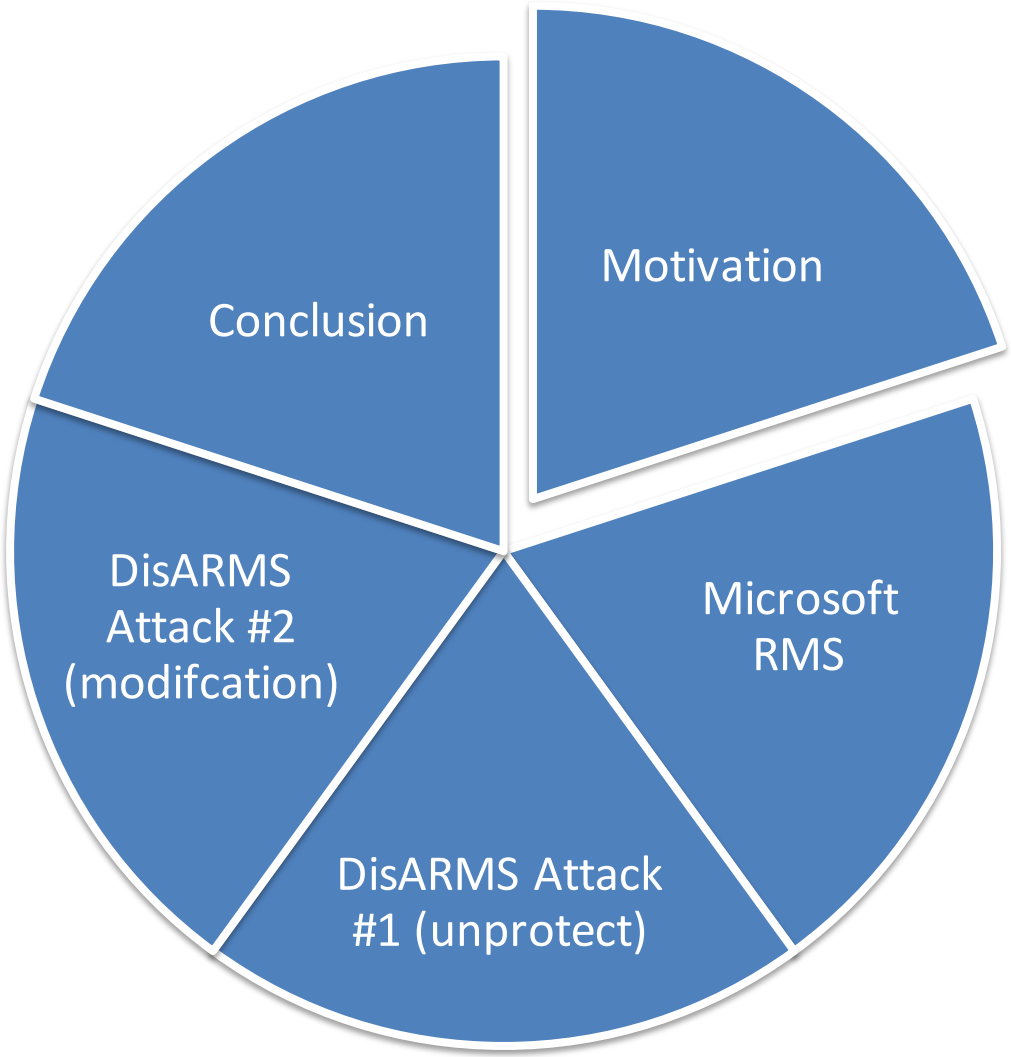
Workshop on Offensive Technology

Christian Mainka, Paul Rösler,
Jörg Schwenk and Martin Grothe

hgi NDS

Bildquelle: http://www.google.com/about/datacenters/gallery/#/tech/12

Agenda


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

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

RUB

You are here: Latest News › Biztech News

Bank Of India De
Rig

Jun 11, 2012 16:45 IST
#AD RMS #Bank of India #Information Protection #Microsoft #RBI

Microsoft AD RMS integrates deep into Microsoft Of
experience for Bank of India end users to protect sen
augment its security strategy by protecting informati
stored. **AD RMS also prevents sensitive information**
confidential e-mail messages) from intentional or ac
protected information to be accessed on other platfo

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

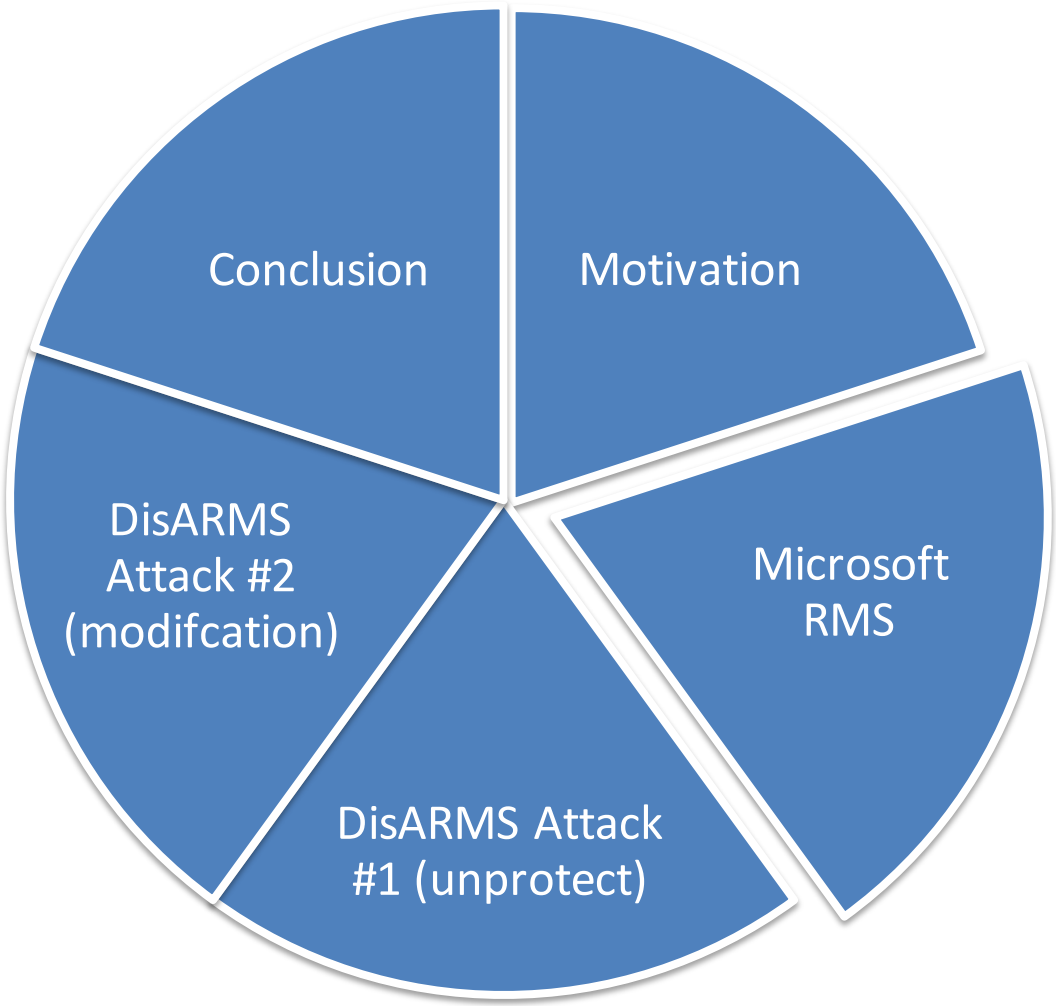
UK MoD looks to be more agile with its IT service delivery, and Microsoft is playing a big part



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

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



RUB
hgi Horst Görtz Institut für IT-Sicherheit

Microsoft RMS - Intro



Microsoft
Active Directory



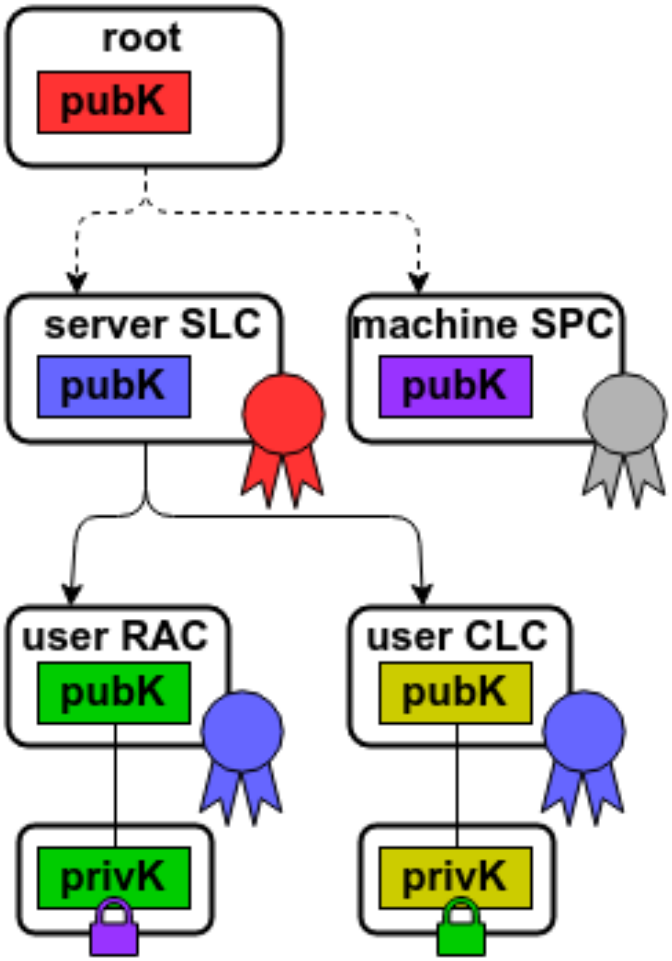
Office 365™

hgi
Horst Görtz Institut
für IT-Sicherheit

Microsoft RMS - High Level

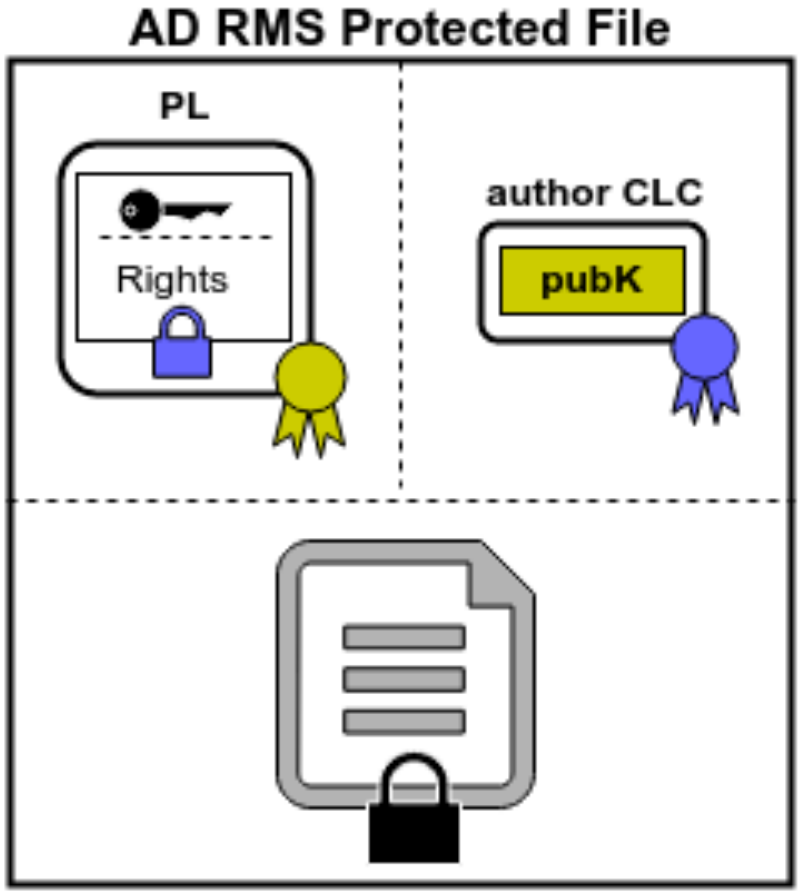
- Set specific rights for a person and/or group via e-mail addr.
- Use sym. and asym. cryptography
  - AES content encryption
  - PKI (RSA)
  - Licenses
- Use license (UL)
- Publishing license (PL)

Microsoft RMS PKI



- Root Cert has separate PrivK
- SLC has separate PrivK
- SLC is signed with $Root_{PrivK}$
- SPC has separate PrivK
- SPC is self-signed
- RAC_{PubK} and encrypted RAC_{PrivK} are signed by SLC_{PrivK}
- CLC_{PubK} and encrypted CLC_{PrivK} are signed by SLC_{PrivK}

Microsoft RMS Create File



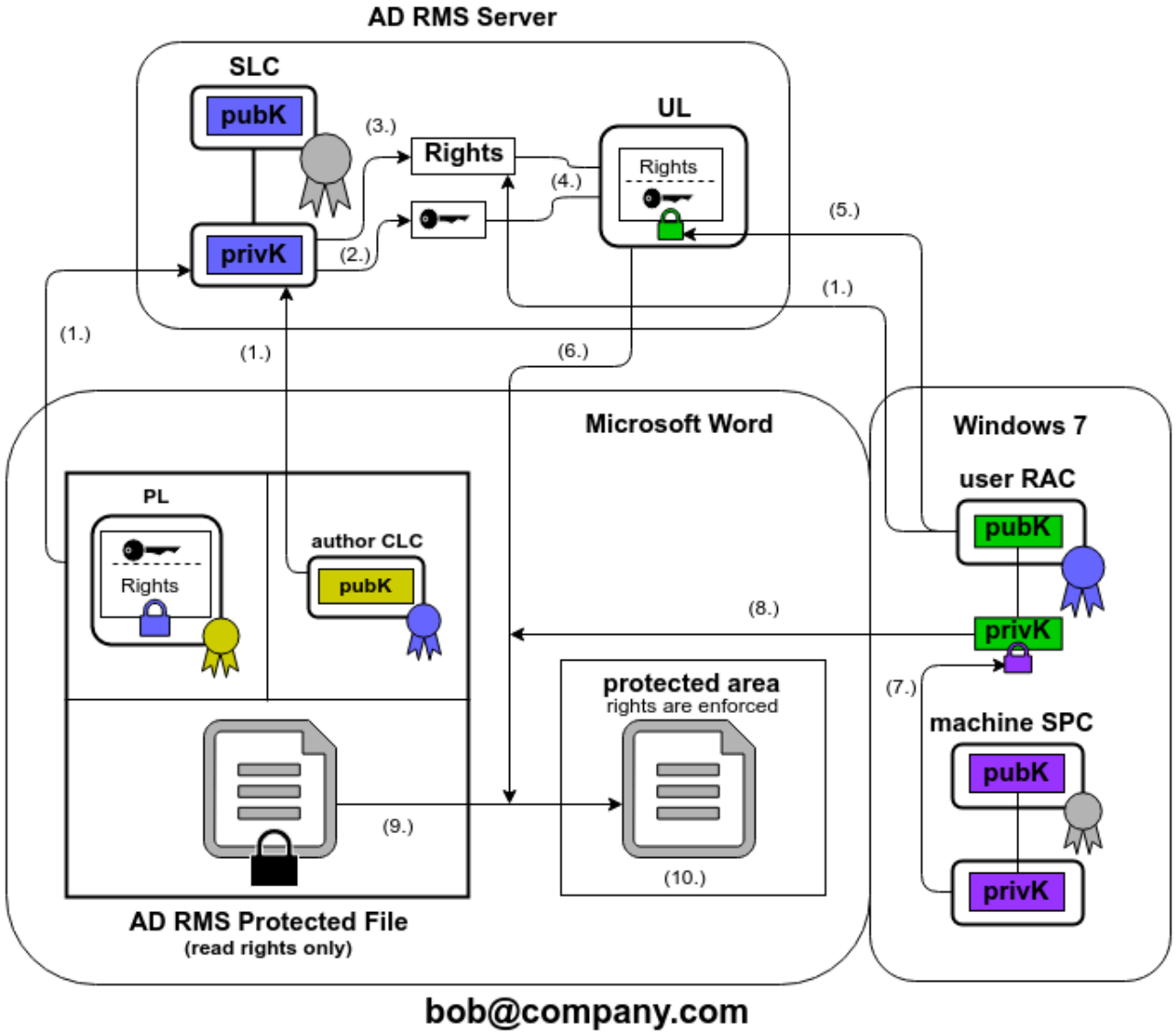
- PL content encrypted with SLC_{PubK}
- PL signed with author CLC_{PrivK}
- Author CLC signed with SLC_{PrivK}

Microsoft RMS Create File

RUB

Demonstration

Microsoft RMS Consume File

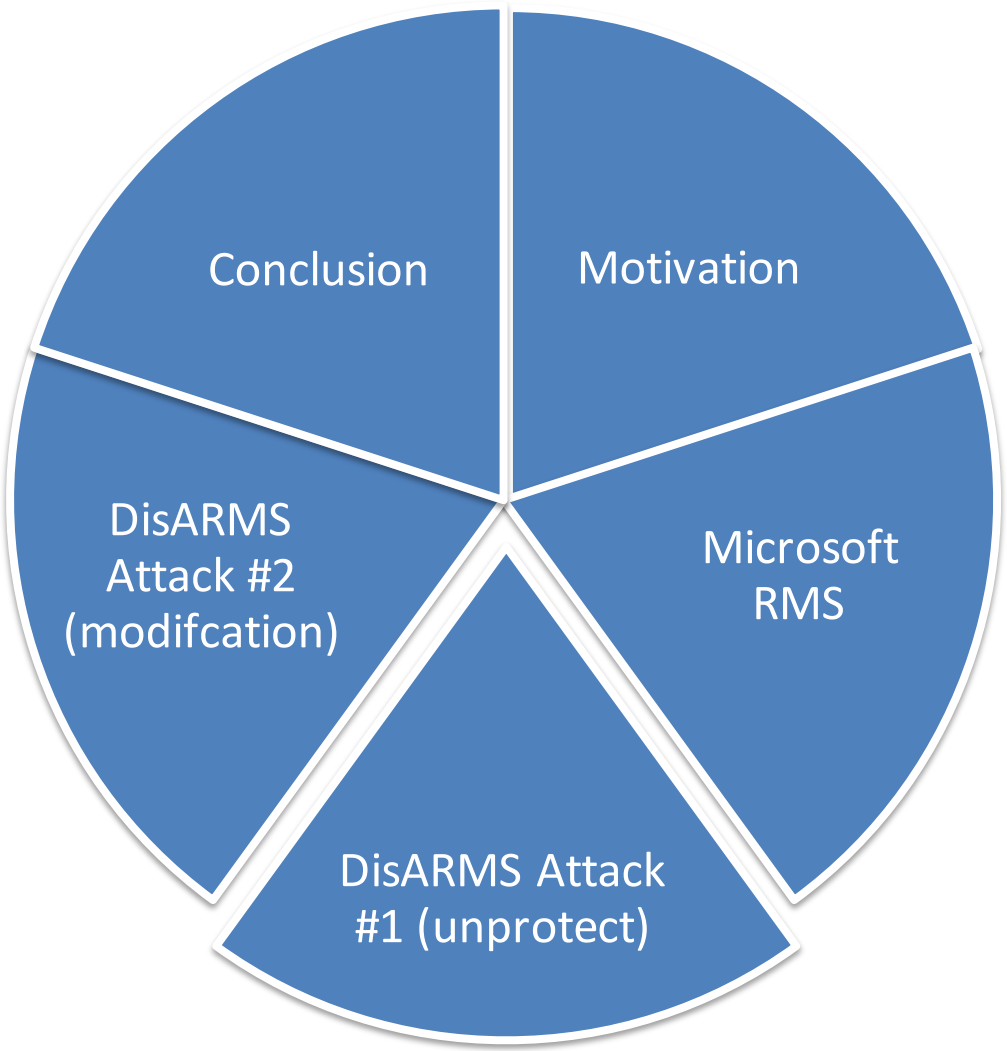


Horst Görtz Institut für IT-Sicherheit

Microsoft RMS Attacks

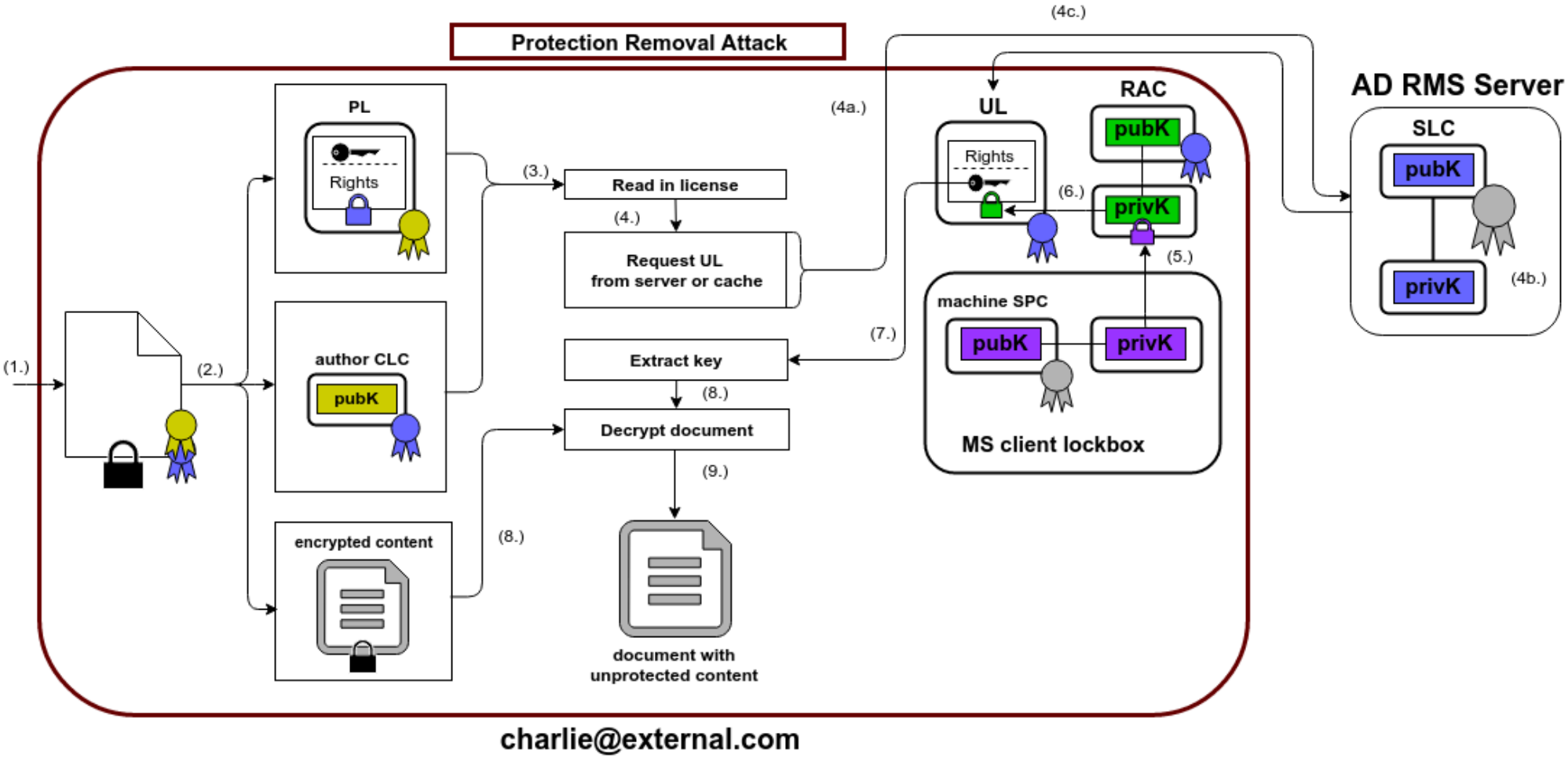
- Responsible disclosed in april 2016
- Case number MSRC 33210
- We used:
  - C++
  - RMS SDK 2.1
- Attack requirements:
  - View access right
  - C++ Redistributable 2015
  - That is all ☺

Agenda


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

Microsoft RMS DisARMS #1

RUB

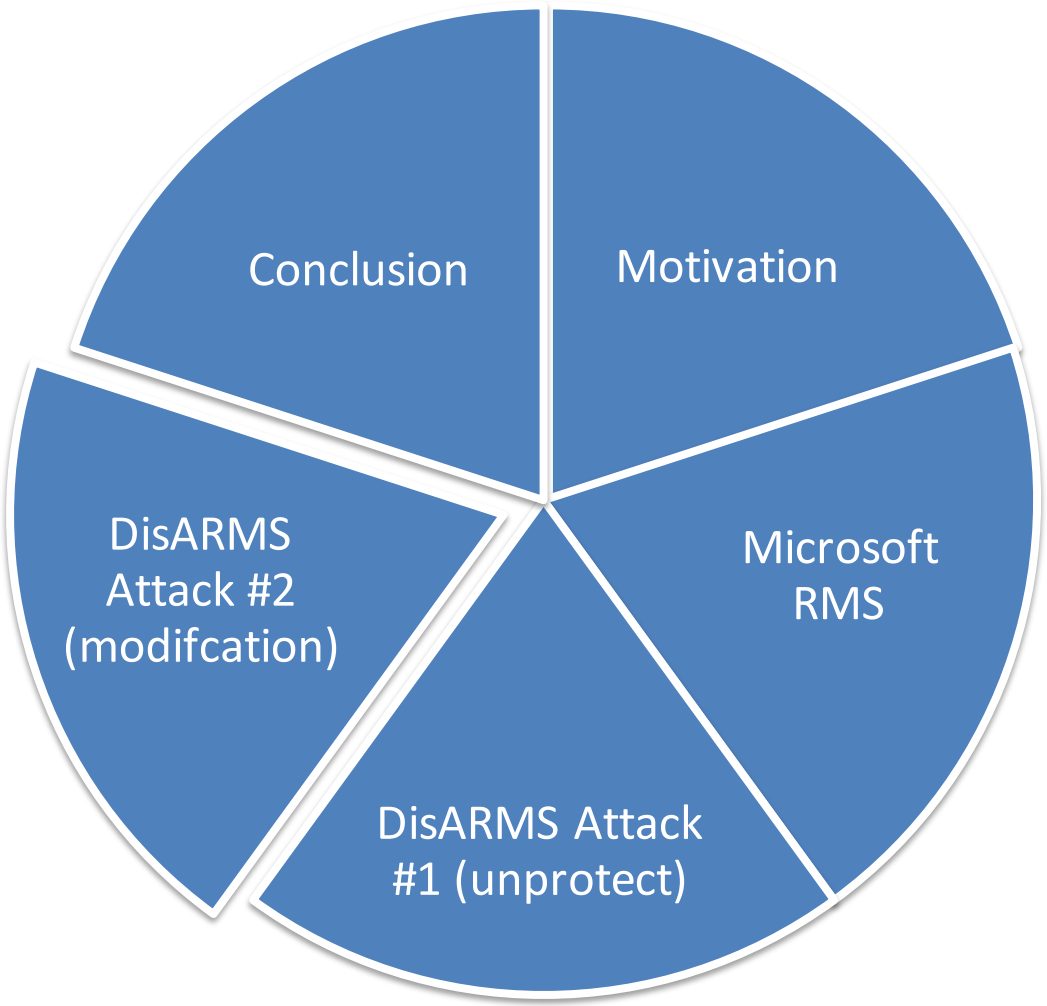


Microsoft RMS DisARMS #1

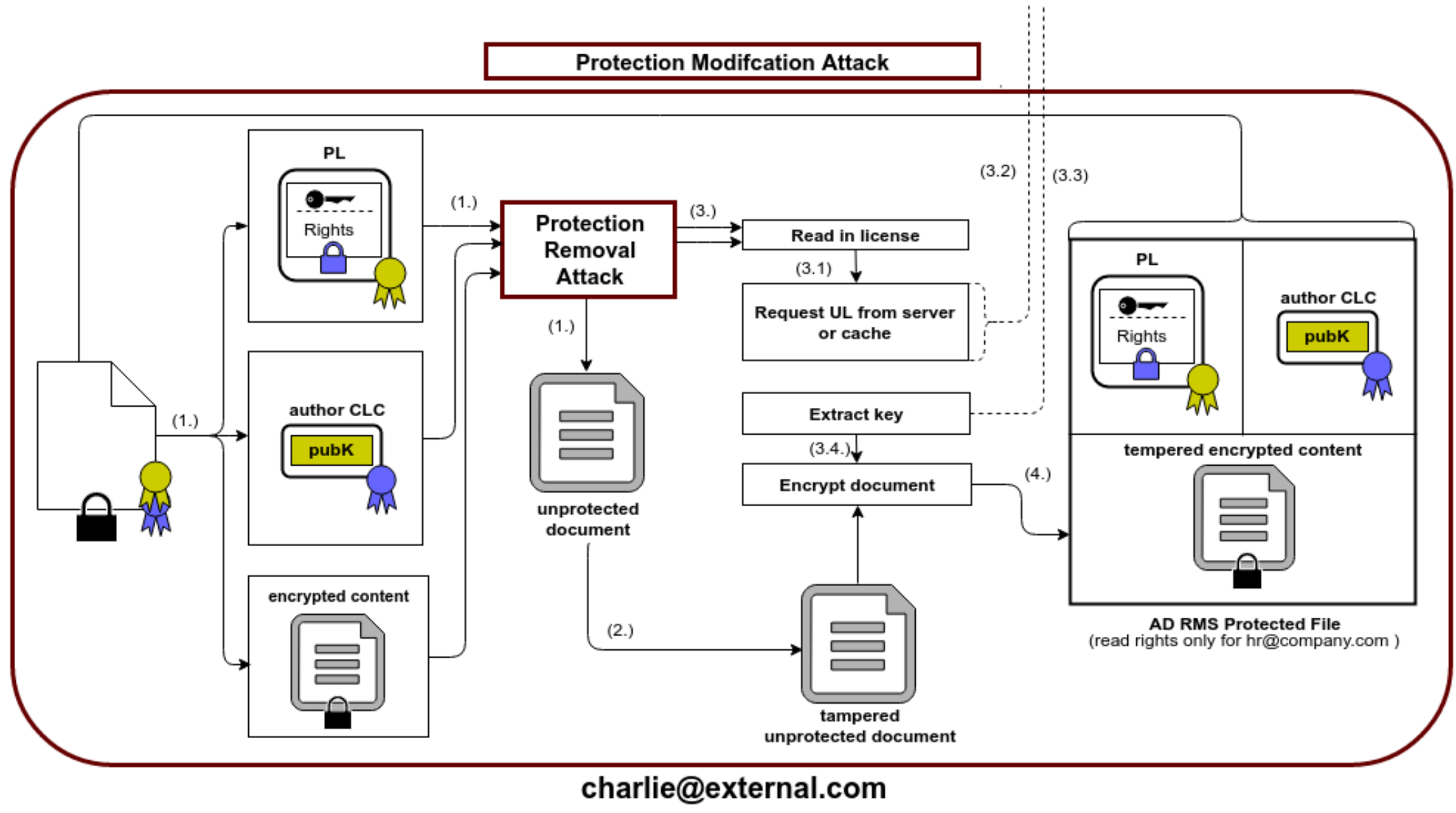
RUB

Demonstration

Agenda


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

DisARMS #2 modification



DisARMS #2 modification

RUB

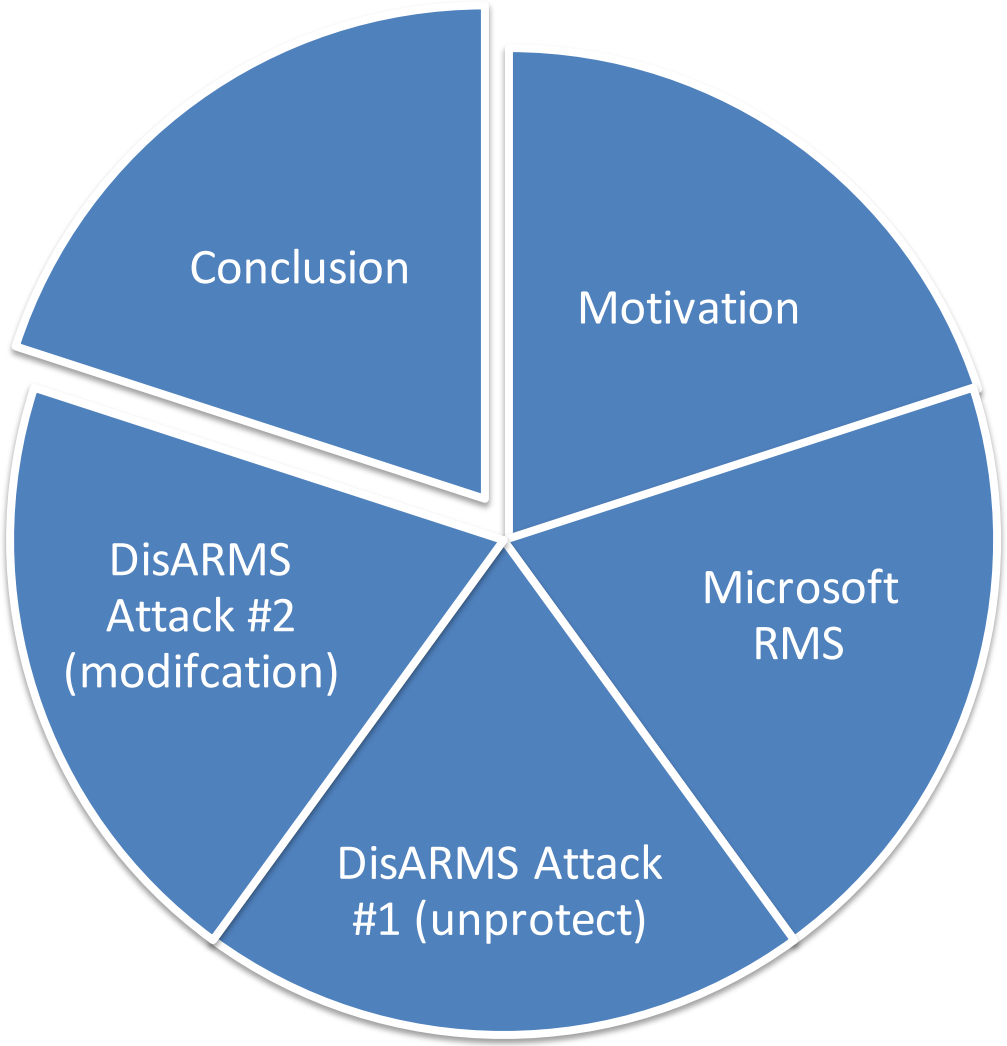
Demonstration

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


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

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

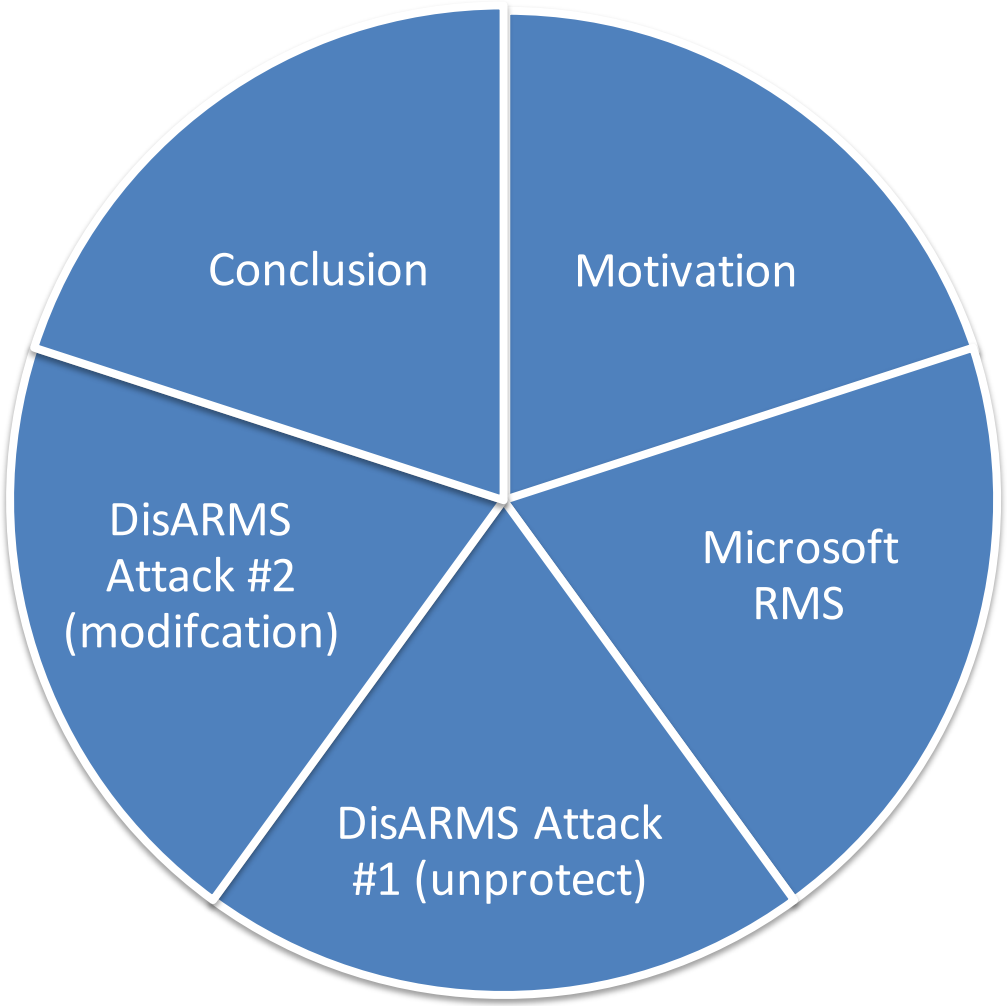
Email: christian.mainka@rub.de
Twitter: @CheariX

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

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

Sponsored by German Ministry for Education and Research

Agenda


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