PARIS2011 CONFERENCE
12th-15th October

Microsoft Office vs LibreOffice: Security comparison regarding viral attacks

Jonathan Dechaux - dechaux@esiea-recherche.euEric Filiol - filiol@esiea.fr

ESIEA
Operational virology and cryptology Lab.
38 rue des docteurs Calmette et Guérin, 53000 Laval France

Outline

- Introduction
- Microsoft Office and LibreOffice security
- Types of Attacks
- Demos
- Conclusion

Outline

- **Introduction**
- Microsoft Office and LibreOffice security
- Types of Attacks
- Demos
- Conclusion

Cyberwarfare, Cyberweapons and Cyber-terrorism

- Reality of Cyberwarfare with Office document:
  - August 2007: Espionage case of China against German chancellery
    - 163 Gb of Governmental data stolen through a Trojan-infected Office document.
  - 2009 - 2011: Chinese hackers succeeded in stealing economic and financial data from various European Banks, French Dept. of Treasure, EC through malicious PDFs and Office document malware.

Cyberwarfare, Cyberweapons and Cyber-terrorism

- Document as Cyberweapons and Cyber-emails:
  - (Dechaux et al., Hack.lu 2010).
  - Attacks through Office documents has become the norm.
  - Office documents are powerful attack vectors.
  - Many actions/features possible.
  - Microsoft Outlook can be used specifically to perform very powerful attacks, with malicious actions.

Outline

- Introduction
- **Microsoft Office and LibreOffice security**
- Types of Attacks
- Demos
- Conclusion

Office and LibreOffice security

- Both suites have same weak points:
  - It is possible to insert/embed a file within a document archive.
  - Application security is managed externally and relies more or less heavily on the Operating system.
    - Registry base for Microsoft Office
    - User file for LibreOffice
  - It is then possible to split the attack into two (or more) innocent looking parts.

Microsoft Office weak points/features

- One template by default.
- Several trusted locations by default.
  - Managed at the registry base.
  - Case of the malicious registry key (2010).
- Office security is different on different OS.
- Old formats (.doc, .xls, .ppt) still manage for backwards compatibility.
- Proprietary applications
  - Analyzing/auditing the security is more than difficult
  - Design flaws (like RC4 encryption), trapdoors, software flaws...?

Microsoft Office strong points

- One security for each application.
- File type is defined by icon and extension.
  - E.g *.docx (no macro) vs *.docm (with macro)
  - But this can be bypassed by considering different approaches and with respect to carefulness users!
- No possibility to put a hard drive as trusted location.
- Better management of document integrity than for LibreOffice.

LibreOffice weak points

- One security for every application.
- No difference between macro and non-macro document.#
  - Same extension for both cases (with and without macro).
- Put an entire hard drive as trusted location.
- Possibility to create a macro for the entire LibreOffice application.
- Very bad management of cryptography (integrity + signature)

LibreOffice strong points

- One security for every OS.
- No Trusted Location by default.
- Macros are not compiled.
  - Easier to analyze malicious LibreOffice documents than malicious Microsoft documents.
  -
- LibreOffice has no email application (contrary to Microsoft Outlook).

State-of-the-Art

- LibreOffice attacks
  - Journal in Computer Virology (2007)
  - Black Hat Europe 2008.
  - iAWACS 2010.
  - Hack.lu 2010.
- Microsoft Office
  - Hack.lu 2010.
  - PacSec 2009/Black Hat Europe 2009.
  - ECIW 2011.

Outline

- Introduction
- Microsoft Office and LibreOffice security
- **Types of Attacks**
- Demos
- Conclusion

Attacks on Microsoft Office

- We can design a lot of different attacks.
- All those which work on LibreOffice, work on Microsoft Office (except those related to cryptography).
  - Template and Add-Ins attacks.
  - Trusted document on USB key (Office 2010 version).
  - Attacks with Outlook.
- The reverse is not possible (by now). A few Microsoft Office attacks are not possible on LibreOffice.

Demos

- We can make some very powerful attacks against the user, returning his trust against him.
  - How to make a DoS with a Template (Microsoft specific).
  - Outlook emails spying (Microsoft specific).
  - Trusted document on a USB key (Microsoft specific).
  - How to install in Trojan.

Conclusion

- As far as security is concerned many powerful attacks are still possible with both Microsoft and Libre Office.
  - Slight advantage in favor of LibreOffice however.
- Analyzing and auditing security is always possible exhaustively whenever the product is open (source code available).
- Doing security with/on a black-box is illusory.
- LibreOffice has too many features which can be perverted by attackers (e.g. programming languages).
- The ODF has be be managed in a far different way with respect to cryptography (Black Hat 2008 attacks).

Conclusion

- We have initiated contacts and talks with the LibreOffice Foundation to:
  - Secure the source code of LibreOffice (in-depth static analysis with *PolySpace/CodeSonar/Coverity*).
    - By the way doing fuzzing over an application whose source is available [Microsoft, 2011] is a strange approach -:)
  - Design and produce the Trusted LibreOffice suite
    - Talks initiated with OpenOffice developpers... in 2007.
  - Secure the data transfer of LibreOffice Cloud version with optimized version of Perseus.

PARIS2011 CONFERENCE
12th-15th October

Thank you for your attention.
Do you have any questions?