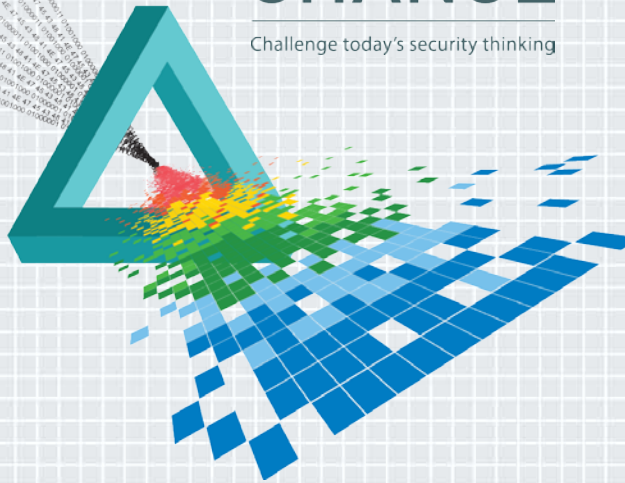
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: HTA-W01

# Dissecting Office Malware for Fun and Espionage

**Jonathan Grier**

Principal
Grier Forensics
jdgrier@grierforensics.com

# Lockheed Martin Suffers Massive Cyberattack

"Significant and tenacious" attack targeted multiple U.S. defense contractors and may ha[ve] [re]lated hack of RSA SecurID system.

Lockheed Martin Hacked, Pentagon to Consider Cyber Attac[k] of War

THE WALL STREET JOURNAL. ≡ | BUSINESS

BUSINESS

## Lockheed Martin Hit By Security Brea

By NATHAN HODGE And IAN SHERR

Updated May 27, 2011 10:34 p.m. ET

Hackers may have infiltrated the networks of top U.S. weapons manufacturer Lockheed Martin Corp. , according to a person with

POPULAR ON WSJ

1. Dave Barry: T[he] Greatest (Part[y] Generation

ALL REVIEWS LAPTOPS / TABLETS / PHONE

Home / Reviews / Software / Security / March RSA Hack Hits Lockheed, Remote Systems Breached

# March RSA Hack Hits Lockheed, Remote Systems Breached

BY DAVID MURPHY MAY 28, 2011 01:55PM EST CO

## Lockheed Martin Network Disru Connected to RSA SecurID

KYT DOTSON | MAY 31ST

READ MORE

Tweet g+1 0

Share 2

Last Friday, the network of Lockheed Martin, the largest U.S. defense contractor, suffered a disruption that has reportedly been connected to RSA SecurID tokens—little keychain fob dongles

# RSA: SECURID ATTACK WAS PHISHING VIA AN EXCEL SPREADSHEET

## F-Secure Analyzes Malicious Excel S
## Penetrated RSA's Network

By Fahmida Y. Rashid | Posted 2011.09.26 Email Print

cnet Search CNET

CNET › Security › Attack on RSA used zero-day Flash exploit in Excel

## Attack on RSA used zero-day Flash exploit in Excel

RSA blog details how the secur
still does not say what data wa

Executive Summary

mised but

In March of 2011, a spear-phishing email containing an Excel spreadsheet with an embed
malicious Adobe Flash payload led to a serious security breach at security firm RSA. This
allowed attackers to compromise the integrity of the RSA SecurID authentication system.
Attackers subsequently used information obtained via this breach in attacks against milita
contractors such as Lockheed Martin, Northrup Grumman and L-3 Communications.

# Duqu: Steal Everything

**Duqu is a sophisticated Trojan that seems to have been written by the same people who created the infamous Stuxnet worm. But unlike Stuxnet, whose main purpose was performing industrial sabotage, Duqu was created to collect intelligence about its targets.**

SECURELIST

THREATS ▾ CATEGORIES ▾ TAGS ▾

## Incident #2: Iran

At the moment, the highest number of Duqu incidents have been recorded in Iran. Th
the Stuxnet story and raises a number of issues. But first, let's look into some details

- Part Three. Detection of the main missing link – a dropper that performed the initial system infection. November 02, 2011

# The Mystery of Duqu: Part Three

By Alexander Gostev on November 2, 2011. 4:35 pm

**Dropper and 0-day.**

Now, for some much more interesting news. It turned out that the continuing research by the Hungarian la Crysys has led to the detection of the main missing link – a dropper that performed the initial system infect

As we expected, a vulnerability was to blame. An MS Word doc file was detected that was sent to one of t victims by the people behind Duqu. The file contained an exploit for a previously unknown vulnerability in

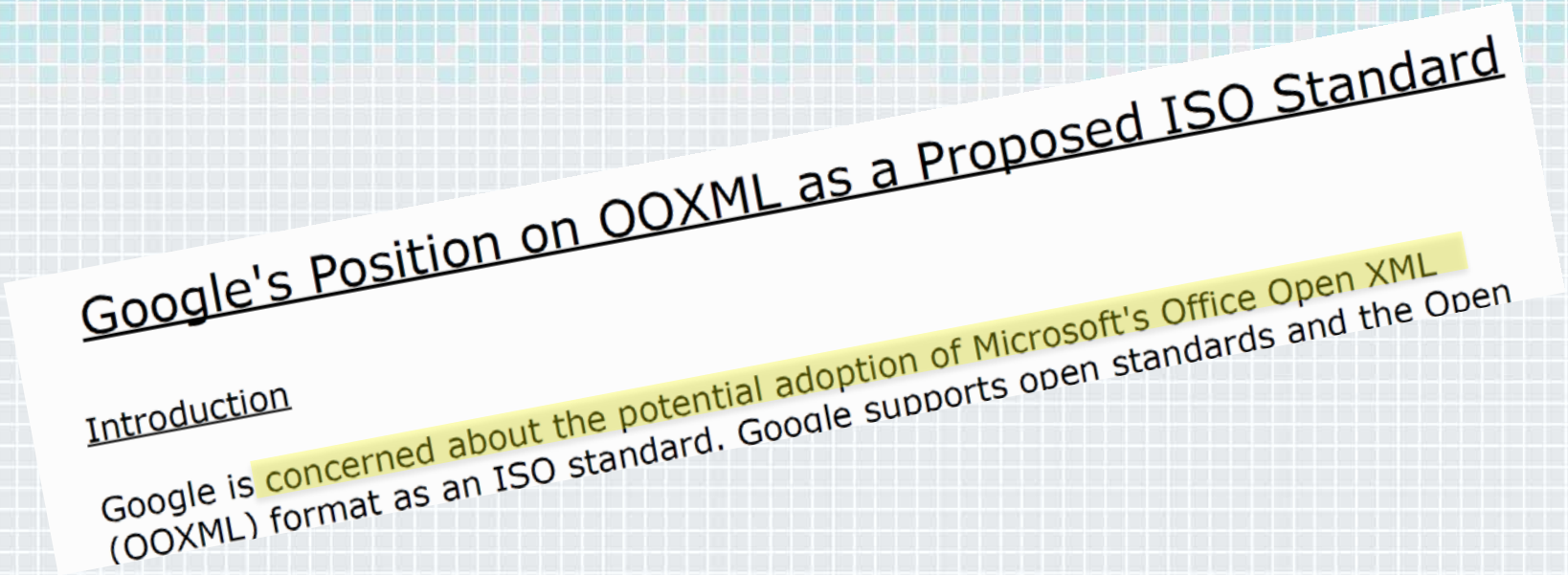
# Why Office?

- Ubiquitous

In a keynote session at the SecTOR conference in Toronto this week, F-Secure security researcher Mikko Hypponen detailed his views on Duqu and the world of online espionage noting that it is very clear to him Duqu is not only based on Stuxnet, but was also written by the same people. According to Hypponen, the Stuxnet source code is not

"Run a system that isn't being targeted and don't run Word, Excel and Powerpoint," Hypponen said. "Make your system different from what the attacker assumes you'll be running."

- Ubiquitous
- **Platform (almost an OS)**



Google's Position on OOXML as a Proposed ISO Standard

Introduction

Google is concerned about the potential adoption of Microsoft's Office Open XML (OOXML) format as an ISO standard. Google supports open standards and the Open

If ISO were to give OOXML with its 6546 pages the same level of review t

standards have seen, it would take 18 years (6576 days for 6546 pages) t

- Ubiquitous
- Platform (almost an OS)
- **VM (to an APT)**

- Ubiquitous
- Platform (almost an OS)
- VM (to an APT)
- **Universal container**

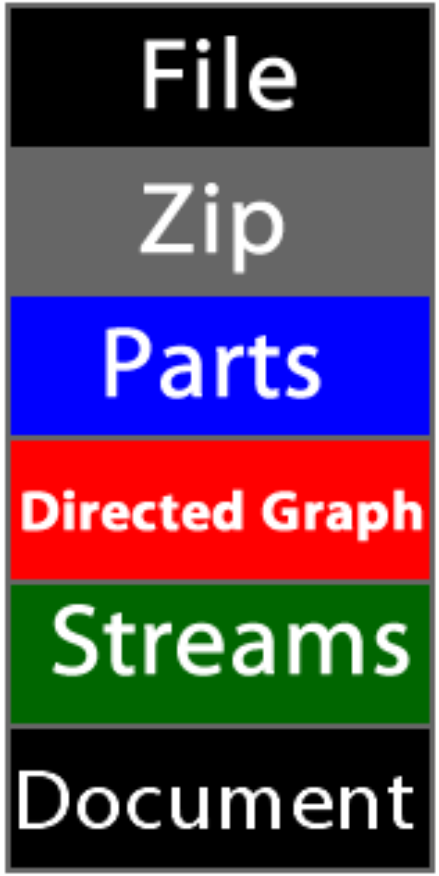
RSAConference2015

San Francisco | April 20-24 | Moscone Center

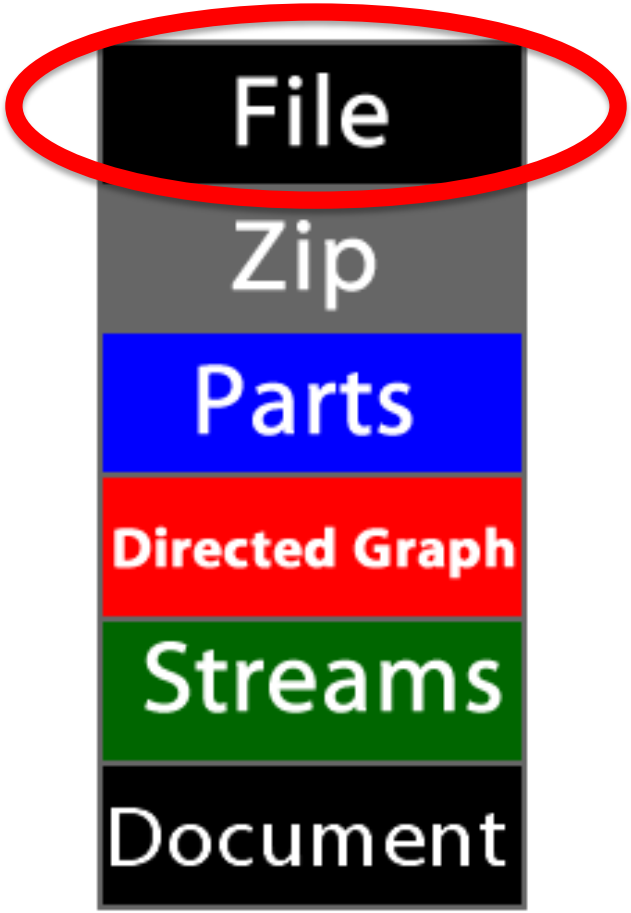
# Deep Dive:
# Office Internals

- DOC
- **DOCX**

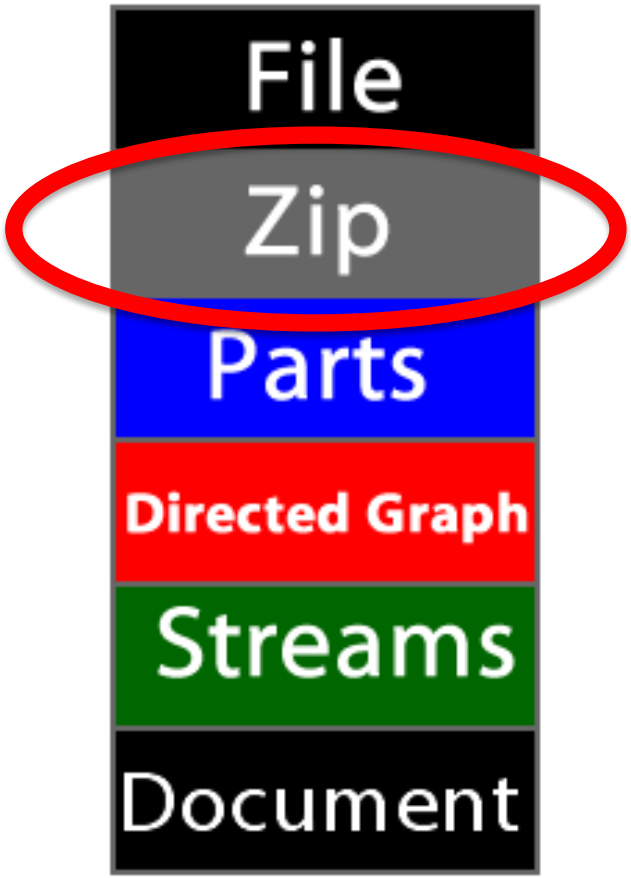
# The Office OOXML Stack



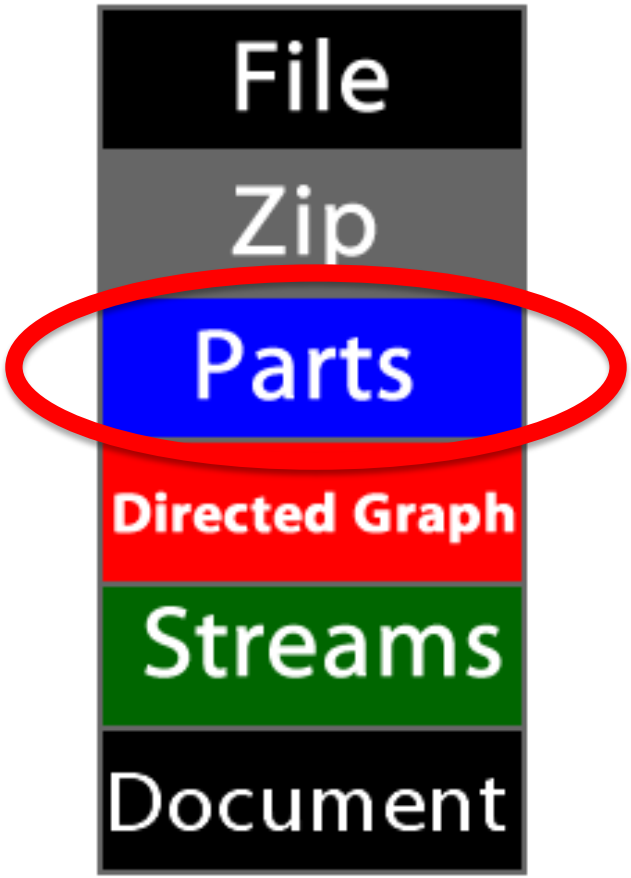
# The Office OOXML Stack



# The Office OOXML Stack



# The Office OOXML Stack



# Office Internals in Two Lines

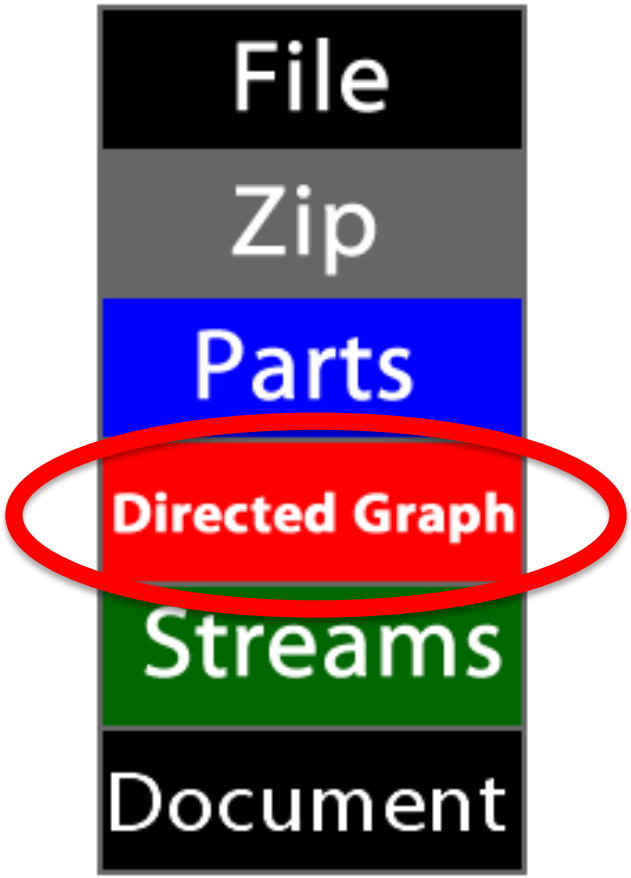
- Content-Types
- Relationships

# Parts (Examples)



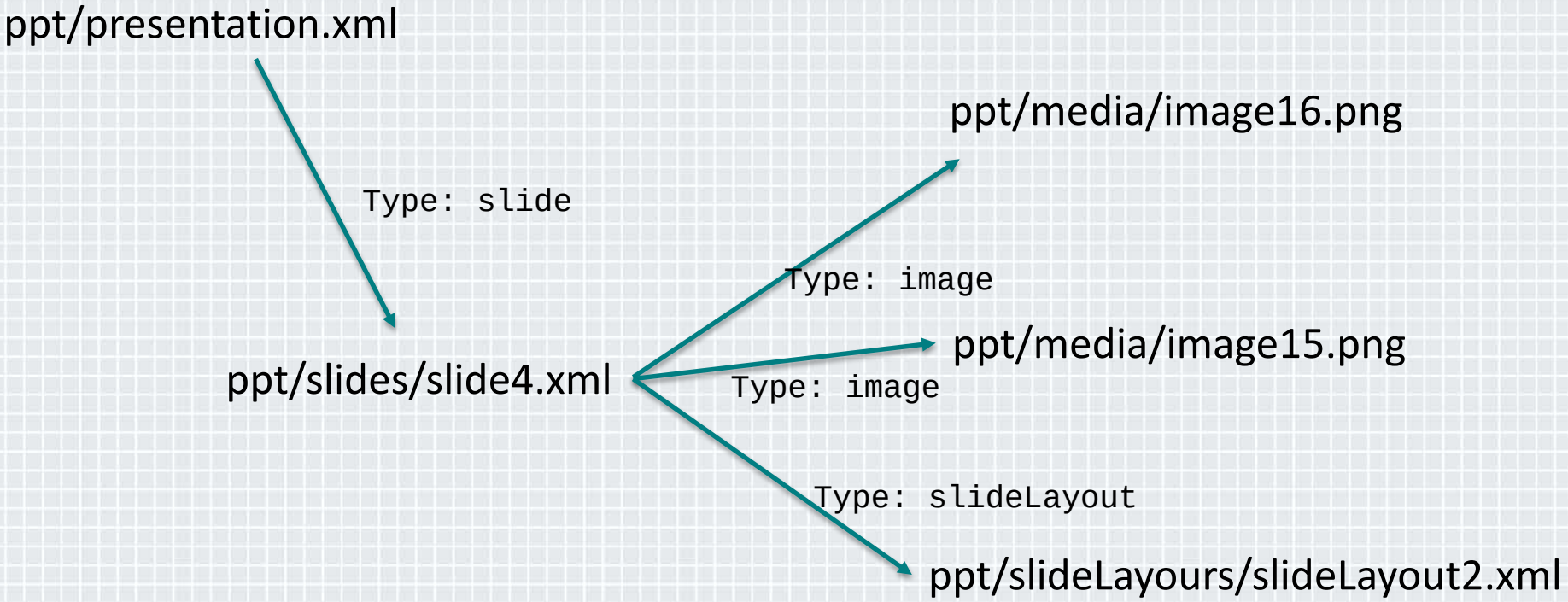
| Part Name | Content-Type | Part Data ("Stream") |
|---|---|---|
| **ppt/slides/slide4.xml** | application/vnd.openxmlformats-officedocument.presentationml.slide+xml | <?xml version="1.0" encoding="UTF-8" standalone="yes"?><br><p:sld<br>xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main"<br>xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships"<br>xmlns:p="http://schemas.openxmlformats.org/presentationml/2006/main"<br>><p:cSld><p:spTree><p:nvGrpSpPr>… |
| **ppt/media/image9.png** | image/png | 00000000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 ; ‰PNG........IHDR<br>00000010h: 00 00 0B 57 00 00 08 59 08 06 00 00 00 5B 0C 71 ; ...W...Y.....[.q<br>00000020h: 3F 00 00 00 09 70 48 59 73 00 00 2E 23 00 00 2E ; ?....pHYs...#...<br>00000030h: 23 01 78 A5 3F 76 00 00 00 19 74 45 58 74 53 6F ; #.x¥?v....tEXtSo<br>00000040h: 66 74 77 61 72 65 00 41 64 6F 62 65 20 49 6D 61 ; ftware.Adobe Ima<br>00000050h: 67 65 52 65 61 64 79 71 C9 65 3C 00 06 DB 52 49 ; geReadyqÉe<..ÛRI<br>00000060h: 44 41 54 78 DA EC DA 41 11 80 00 10 C4 B0 82 7F ; DATxÚìÚA.€..Ä°,▯<br>00000070h: CF C7 CC DA 20 91 D0 77 9F BB 0B 00 00 00 00 00 ; ÏÇÌÚ 'ĐwŸ».....<br>00000080h: 00 00 00 00 00 E0 EF 5E 09 00 00 00 00 00 00 00 ; .....àï^........ |
| **[Content_Types].xml** | application/xml | <?xml version="1.0" encoding="UTF-8" standalone="yes"?><br><Types<br>xmlns="http://schemas.openxmlformats.org/package/2006/content-types"><Default Extension="png"<br>ContentType="image/png"/><Default Extension="emf"<br>ContentType="image/x-emf"/>… |

# The Office OOXML Stack

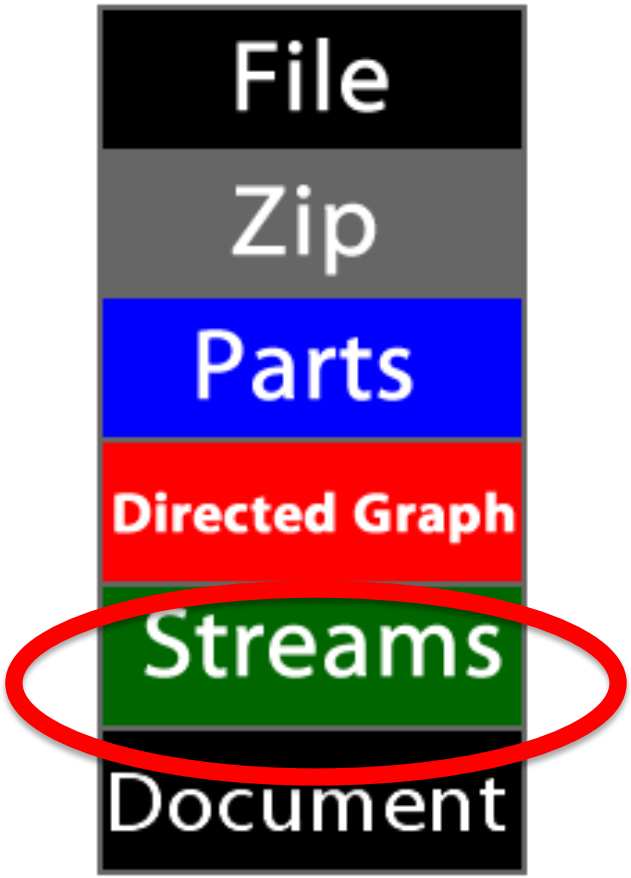


# Relationships (Examples)

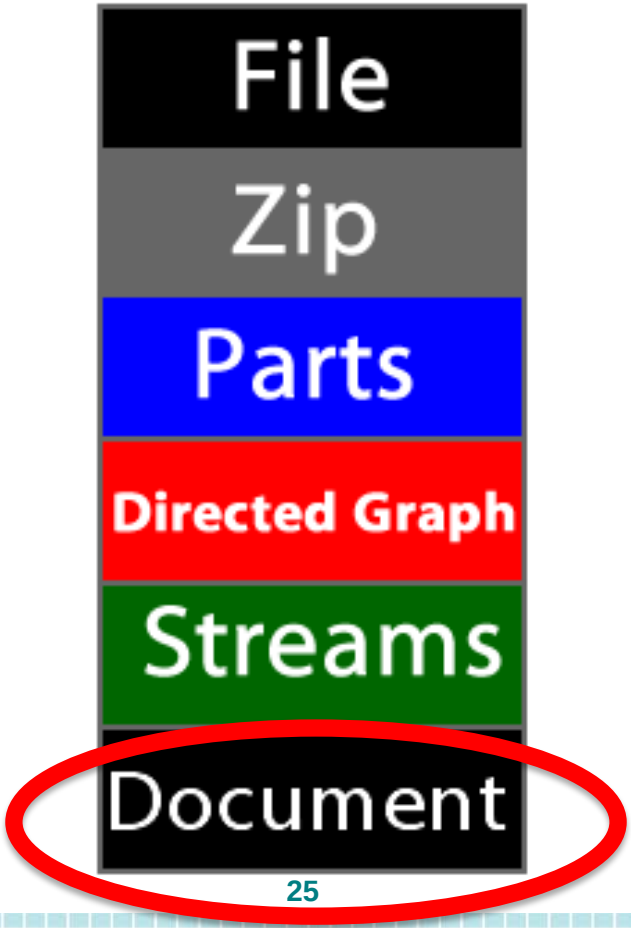




# The Office OOXML Stack



# The Office OOXML Stack



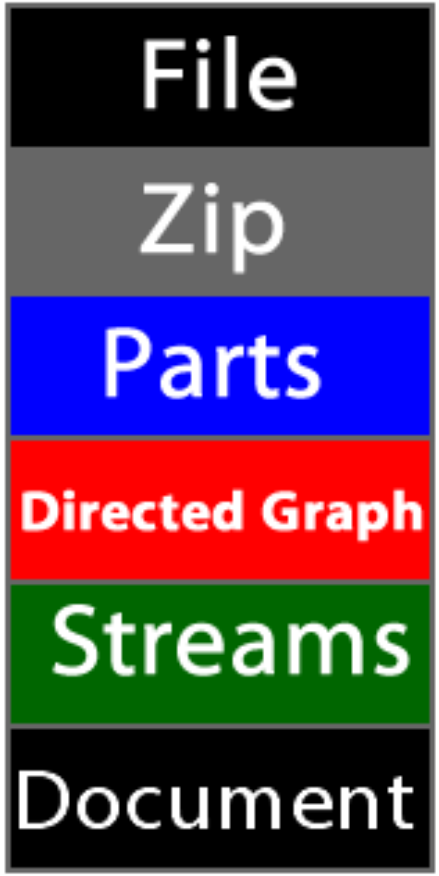
1. Wrapper
2. Obfuscator
3. Vector in its own

RSA Conference2015

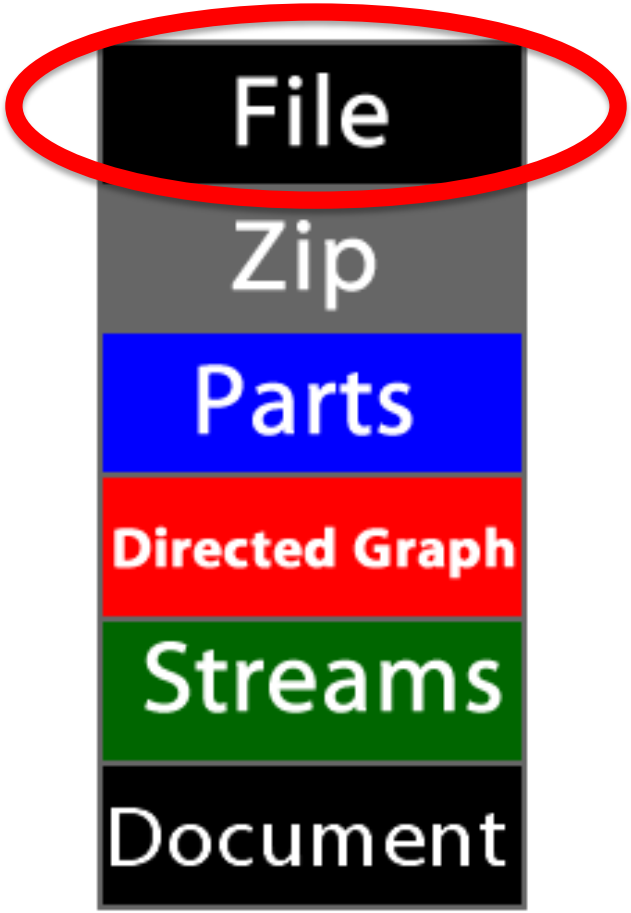
San Francisco | April 20-24 | Moscone Center

# Live Dissection

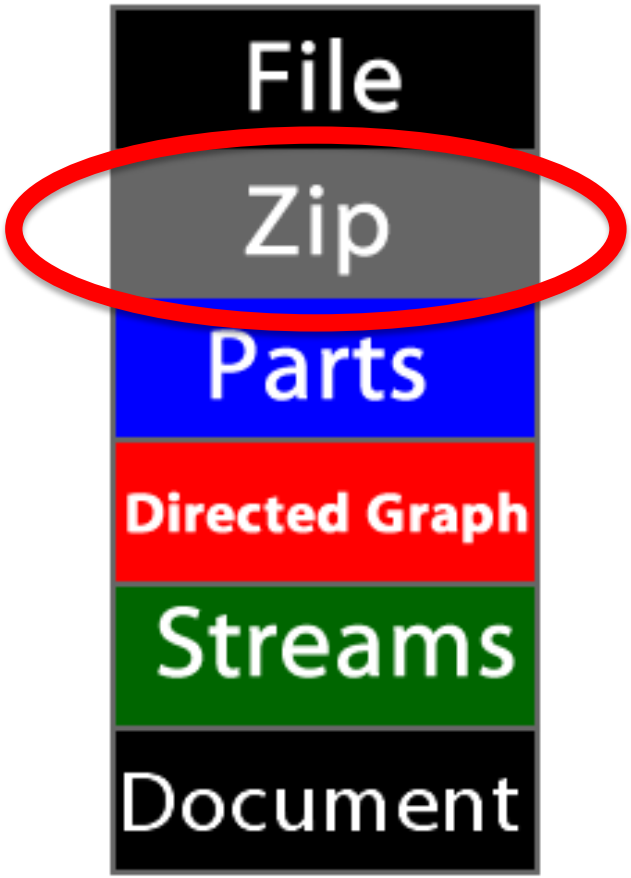
# The Office OOXML Stack



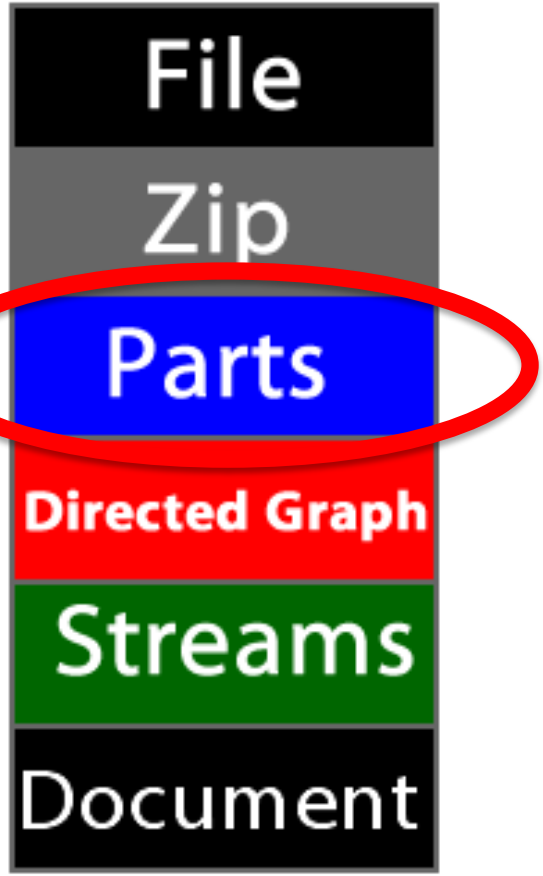
# The Office OOXML Stack



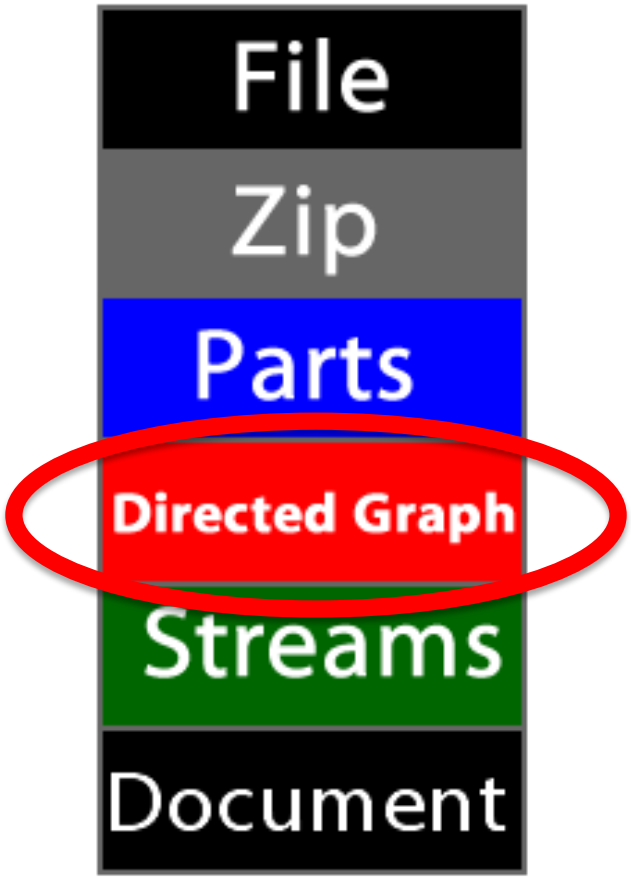
# The Office OOXML Stack



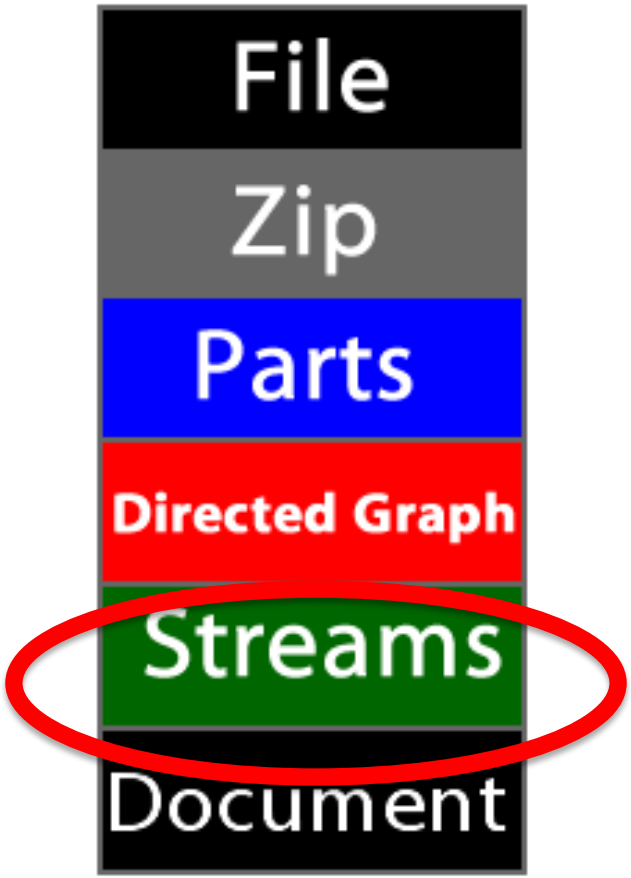
# The Office OOXML Stack



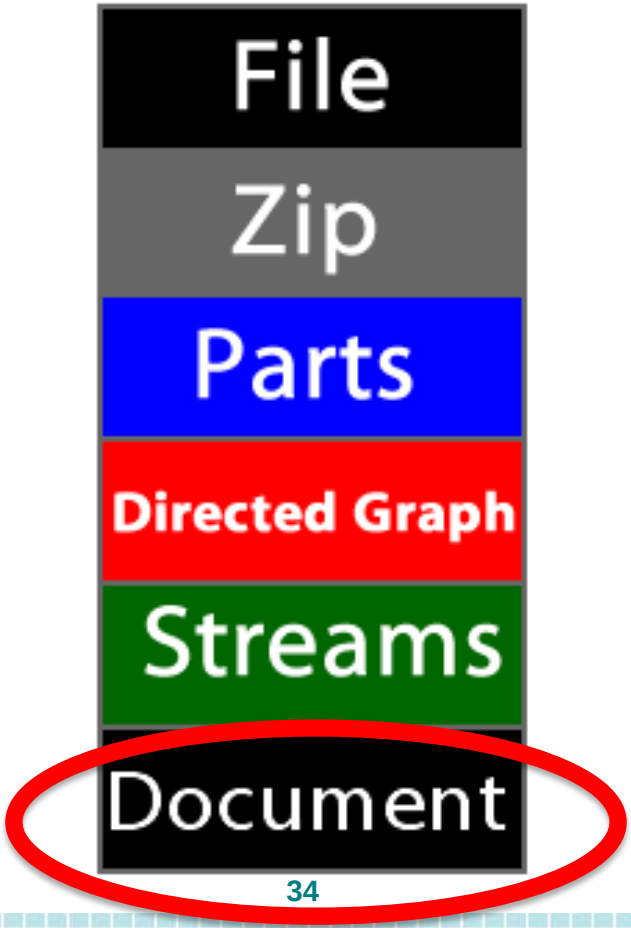
# The Office OOXML Stack



# The Office OOXML Stack



# The Office OOXML Stack



# VM (to an APT)

# Platform (almost an OS)

# For more information

- **www.OfficeDissector.com** – Open Source tool to dissect Office documents
- http://www.officedissector.com/doc/rst/ANALYZING_OOXML.html is a walk-thru including an example tutorial using OfficeDissector
- Feel free to contact me with questions (please be patient if I can't respond immediately)
- *And, if you have a lot of time on your hands, http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html has the ISO/IEC 29500 Office spec (all 6500+ pages)*

# Questions?

# Feedback?

**Please share them with me here**

**Or jdgrier@grierforensics.com**

# Apply Slide

- Next week you should:
  - Install OfficeDissector (Open Source at www.officedissector.com)
  - Work through the tutorial of Office analysis
- Within one month you should:
  - Take a benevolent office document from your organization and dissect it. It will be a great way to concretize what you've learned about Office internals.
- Within three months you should:
  - Find a suspicious Office document (perhaps emailed to someone in your organization) and dissect it
  - Catalog the threat vectors that Office docs constitute for your organization