Every Signature is Broken:

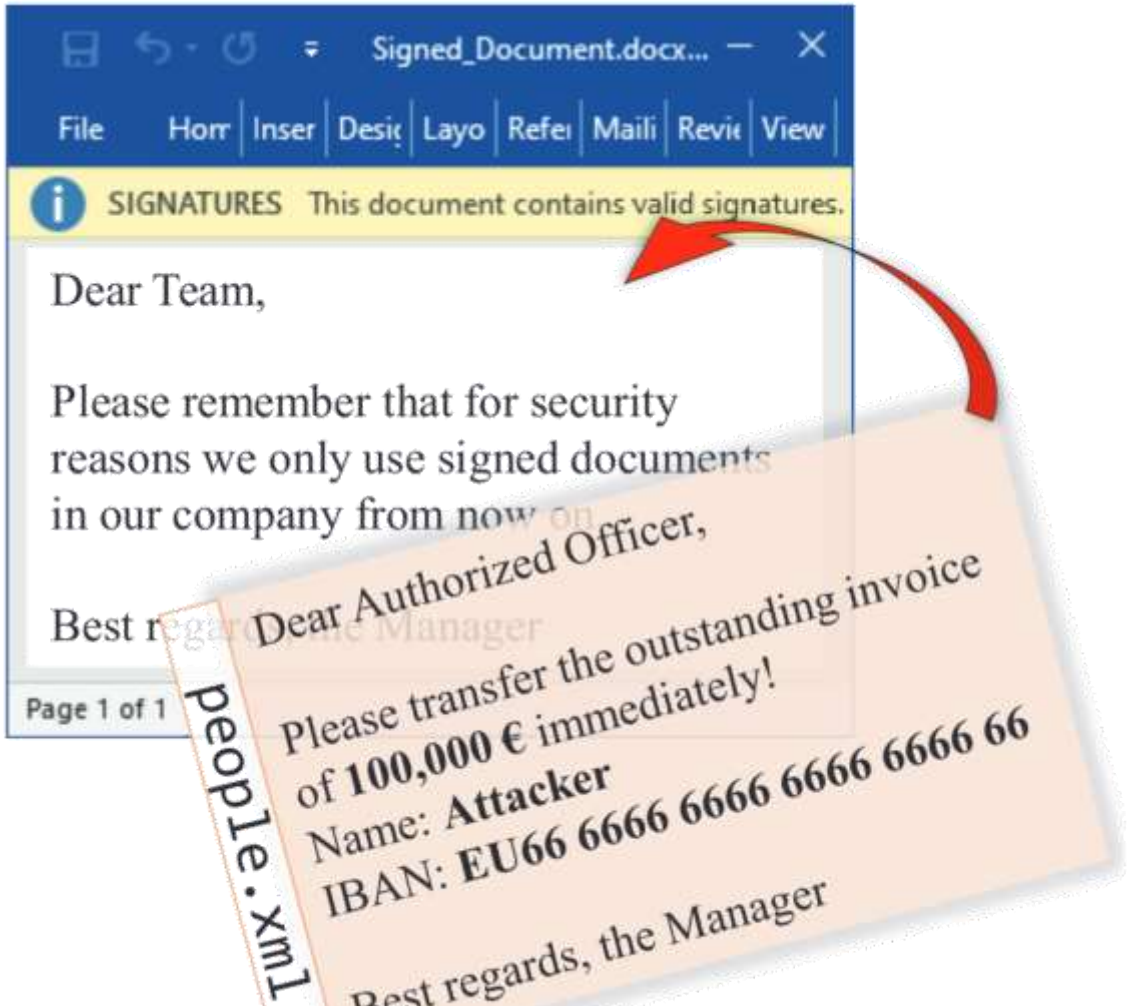
On the Insecurity of Microsoft Office's OOXML Signatures

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

RUB

A digital signature is an electronic, encrypted, stamp of authentication […].
A signature confirms that the information originated from the signer and has not been altered.

- Microsoft



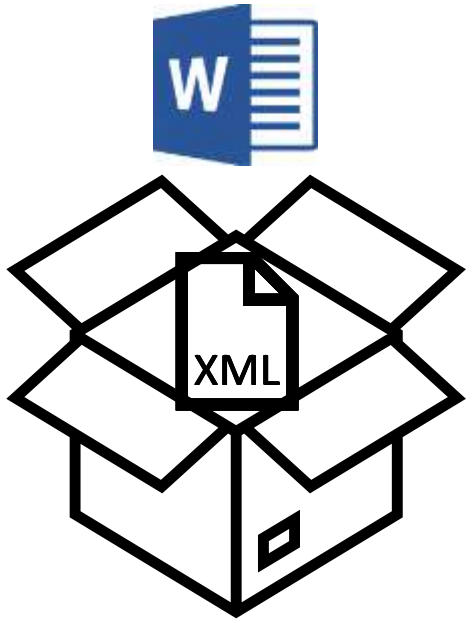
RUHR-UNIVERSITÄT BOCHUM hgi NDS

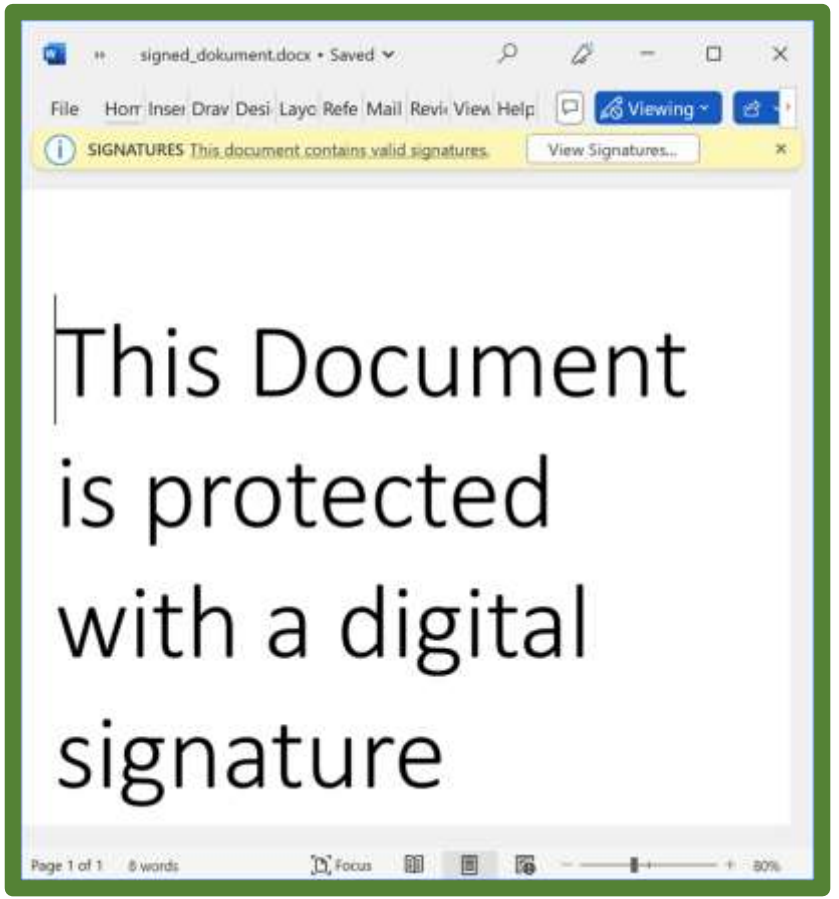
Simon Rohlmann, Vladislav Mladenov, **Christian Mainka**,

Daniel Hirschberger, Jörg Schwenk

OOXML Structure

signed_document.docx**.zip**





OOXML Structure

sig1.xml

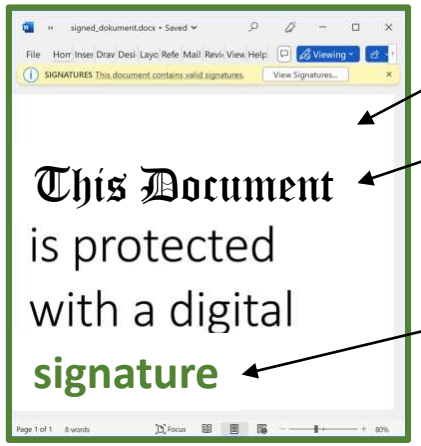
document.xml.rels

[Content_Types].xml

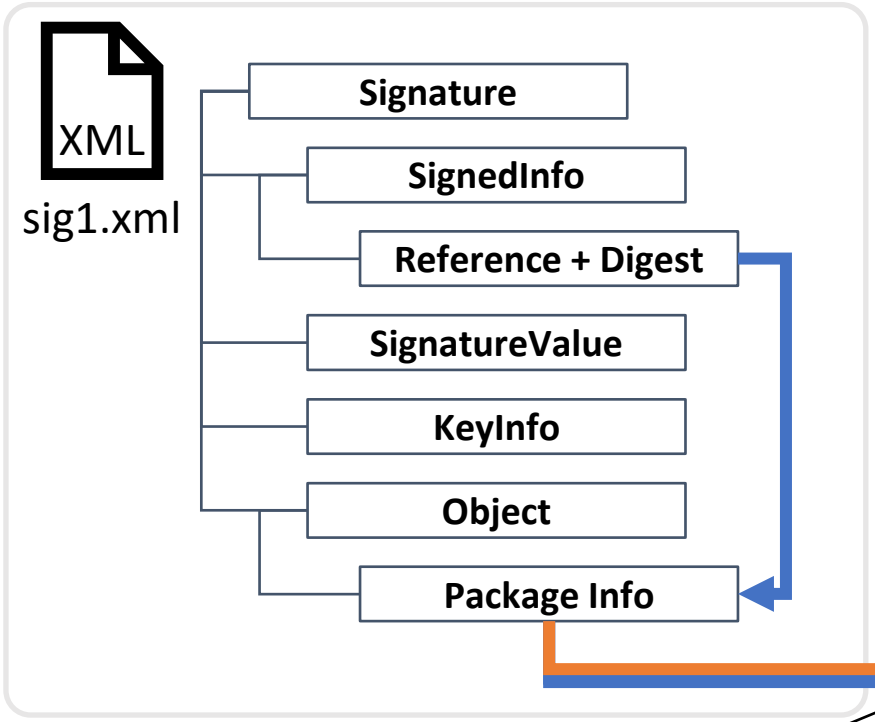
document.xml

fontTable.xml

styles.xml



OOXML Signature



Partial coverage:
Only <Relationship> Elements

XML
document.xml.rels

XML
[Content_Types].xml

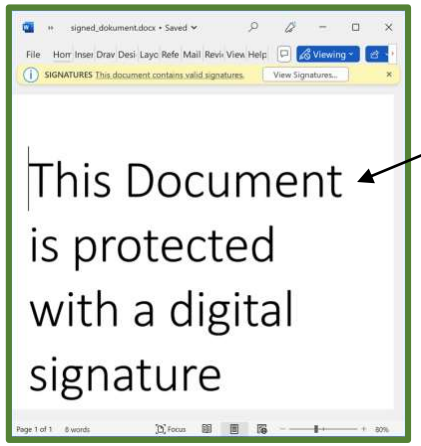
XML
document.xml

XML
fontTable.xml

XML
styles.xml

Full coverage

No Protection



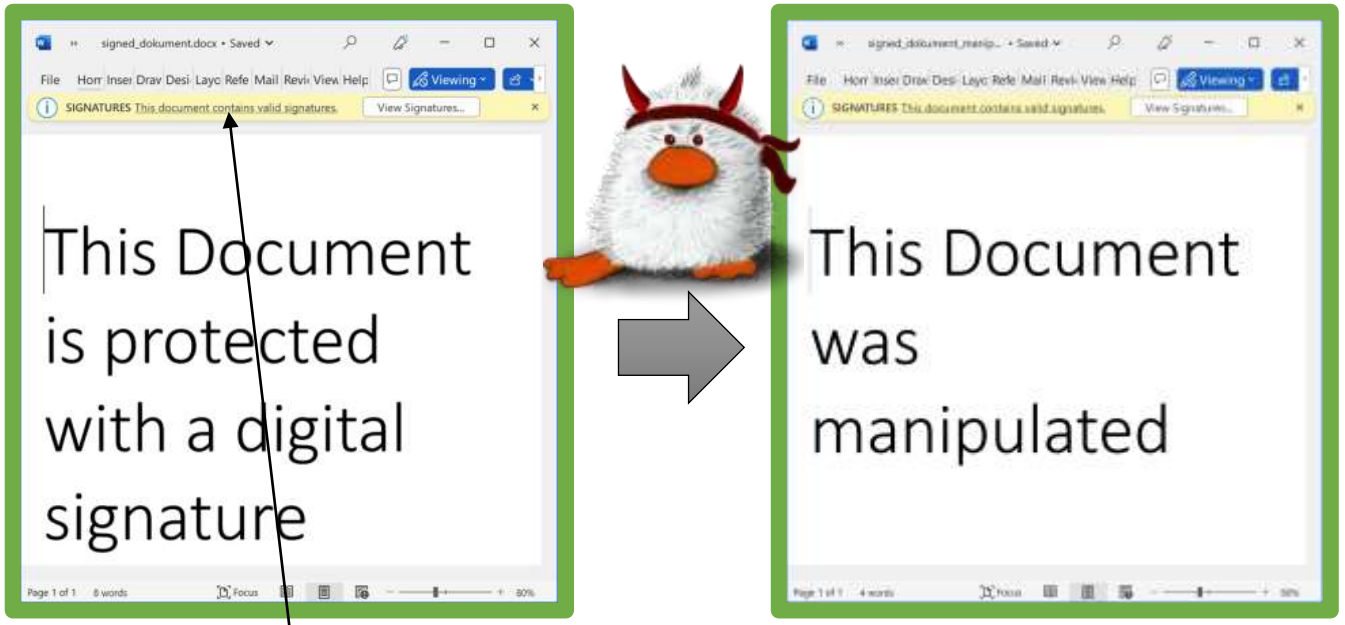
Specification Flaw #1/3: Content Injection Attack

- OOXML Signatures = partial Signatures
- Add unsigned files to show new content

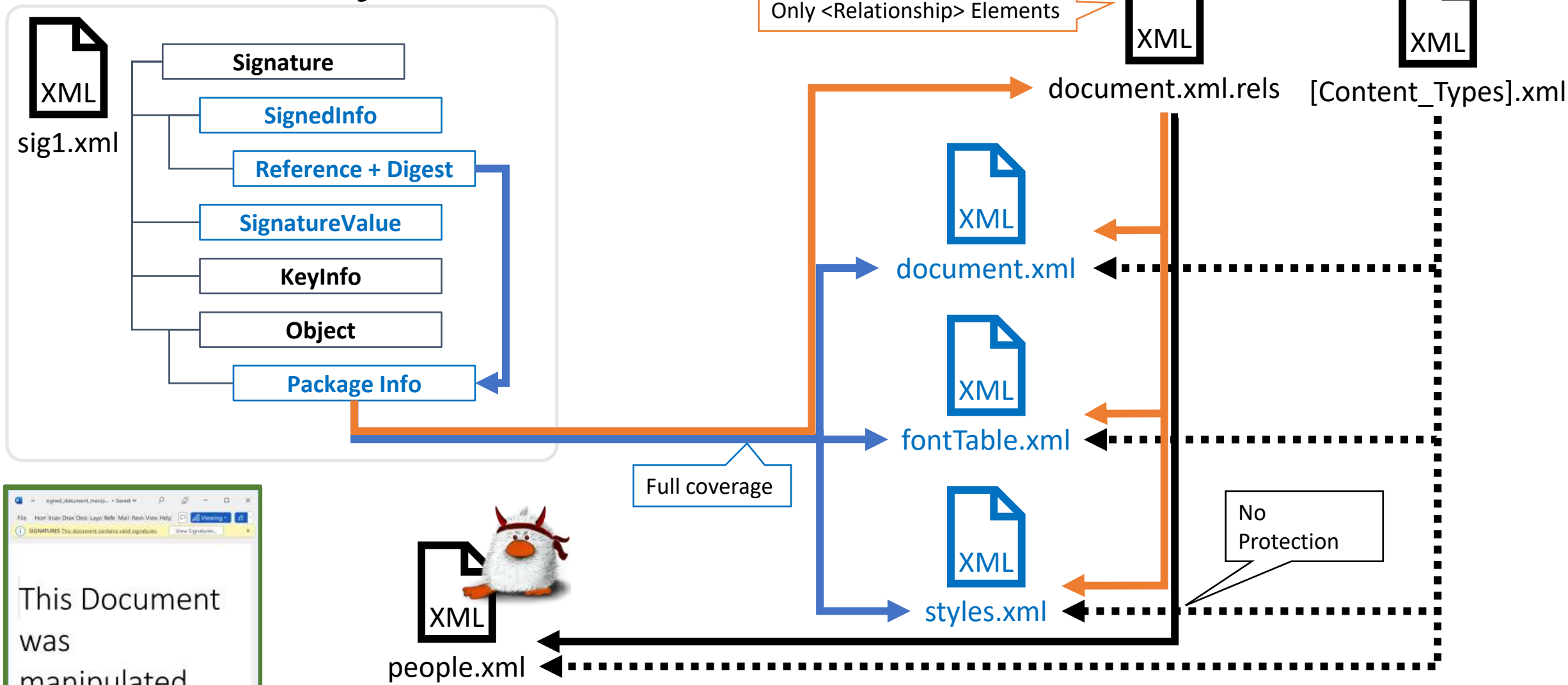
Content Injection Attack

1. Attacker retrieves signed document

2. Attacker manipulates signed document
   - Shows manipulated content
   - Keeps signature valid



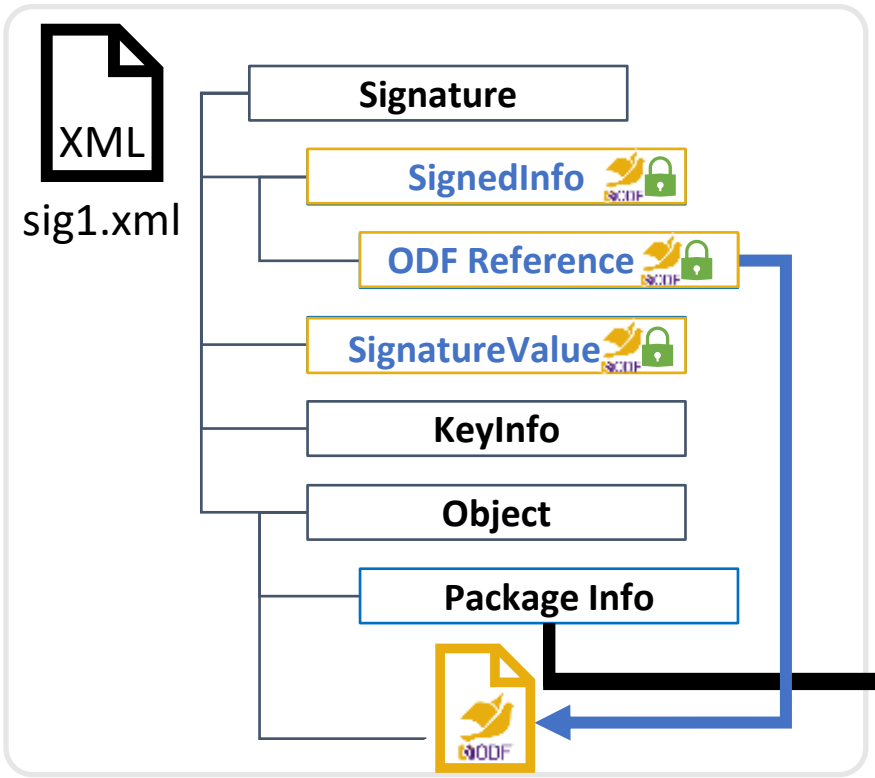
Content Injection Attack

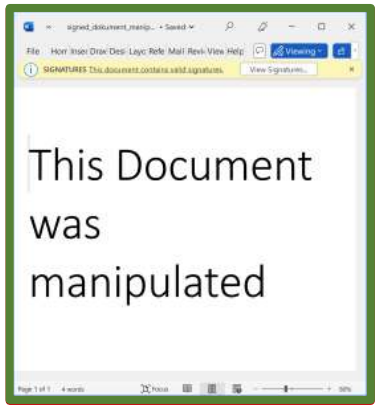


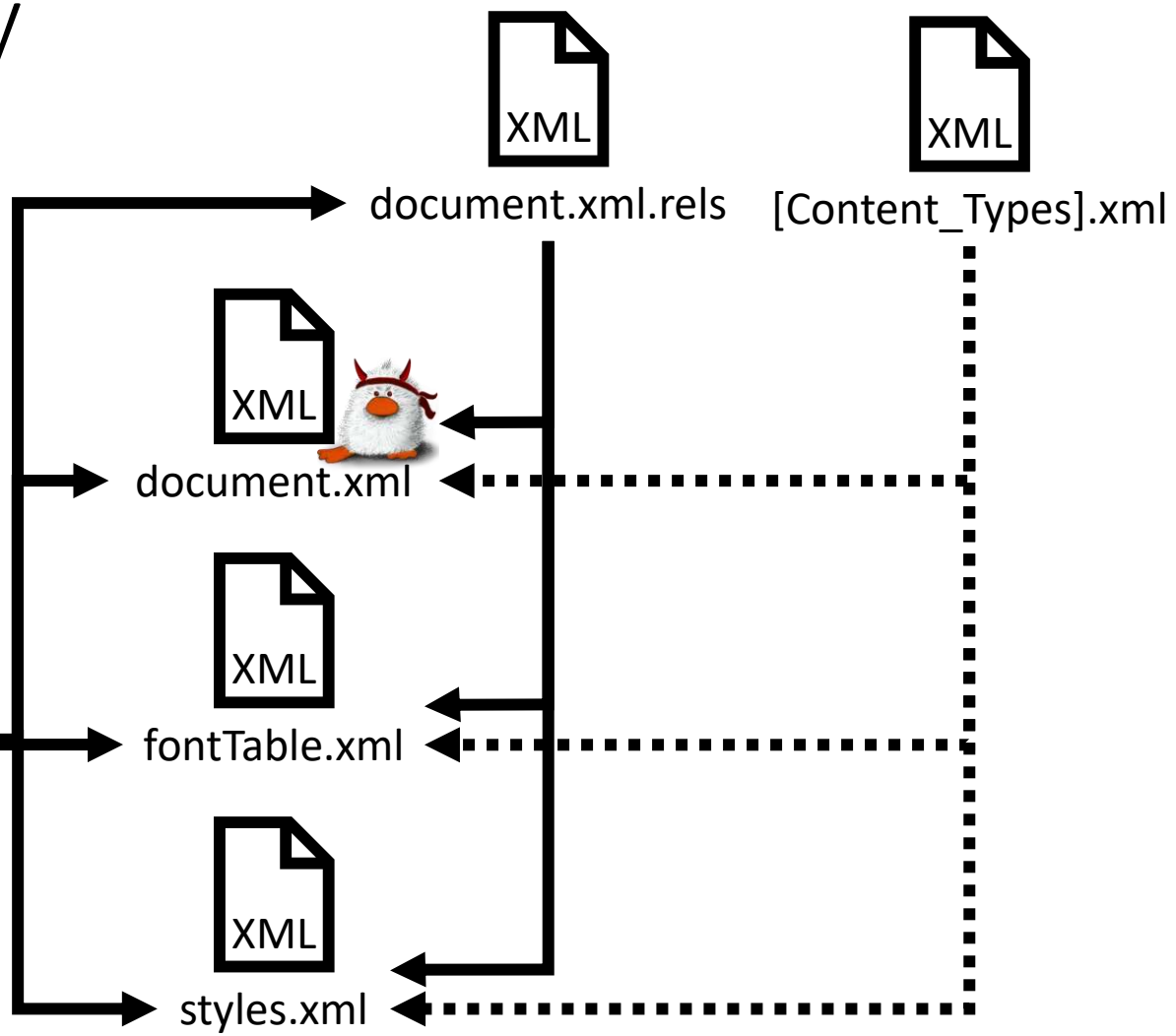
Implementation Flaw #1/2: Universal Signature Forgery

- Extract valid XML Signature from ODF, SAML, …
- Embed in OOXML

Universal Signature Forgery







Evaluation Results

"Every Signature is Broken"

“Every Signature is Broken”

	Microsoft Office	Build	Specification Flaws: CIA	Specification Flaws: Content Masking Attack: Font Inj.	Specification Flaws: Content Masking Attack: Style Inj.	Specification Flaws: Legacy Wrapping	Implementation Flaws: USF	Implementation Flaws: Malicious Repair Attack: Dup. Doc	Implementation Flaws: Malicious Repair Attack: Evil Type
Windows	2013	15.0.5423.1000	⊗	⊗	⊗	⊗	⊗	◐	◐
Windows	2016	16.0.5278.1000	⊗	⊗	⊗	⊗	⊗	◐	◐
Windows	2019	16.0.10386.20017	⊗	⊗	⊗	⊗	⊗	◐	◐
Windows	2021	16.0.14332.20303	⊗	⊗	⊗	⊗	⊗	◐	◐
Windows	365	16.0.15028.20248	⊗	⊗	⊗	⊗	⊗	◐	◐
macOS	2019	16.61.22050700	⊗. Direct content manipluation without any detection						
macOS	2021	16.61.22050700	⊗. Direct content manipluation without any detection						
macOS	365	16.61.22050700	⊗. Direct content manipluation without any detection						
	OnlyOffice Desktop								
	Windows	7.1.1.57	⊗	✓	◐	⊗	✓	⊗	⊗
	macOS	7.1.1 (533)	⊗	✓	◐	⊗	✓	⊗	⊗
	Linux	7.1.1.57	⊗	✓	◐	⊗	✓	⊗	⊗

Legend ✓: Not Vulnerable ⊗: Vulnerable ◐: Limited Vulnerability

Conclusion

Conclusion & Lessons Learned

- Major Issues
  - OOXML uses partial signatures
  - Rendering flow involves signed **and** unsigned data
  - Cryptographic verification is complex for documents
- Content vs Metadata
  - Do not render people.xml, styles.xml, ...
- PoC Files
  - github.com/RUB-NDS/OOXML_Signature_Security
- Details in the Paper

Q&A?