

On the security of PDF Signatures

Vladislav Mladenov & Simon Rohlmann
Ruhr University Bochum



PDF Days Europe 2022 | Berlin

Portable Document Format (PDF)



“De facto standard for electronic exchange of documents”

- *Adobe*

FIRST VERSION RELEASED IN

1993

BY ADOBE

320 BILLION

PDF DOCUMENTS OPENED with ADOBE DC in 2021

PDF-2.0

RELEASED IN 2017, LAST VERSION
FROM ISO

TRILLIONS

PDFs IN EMAIL, CLOUD & WEB

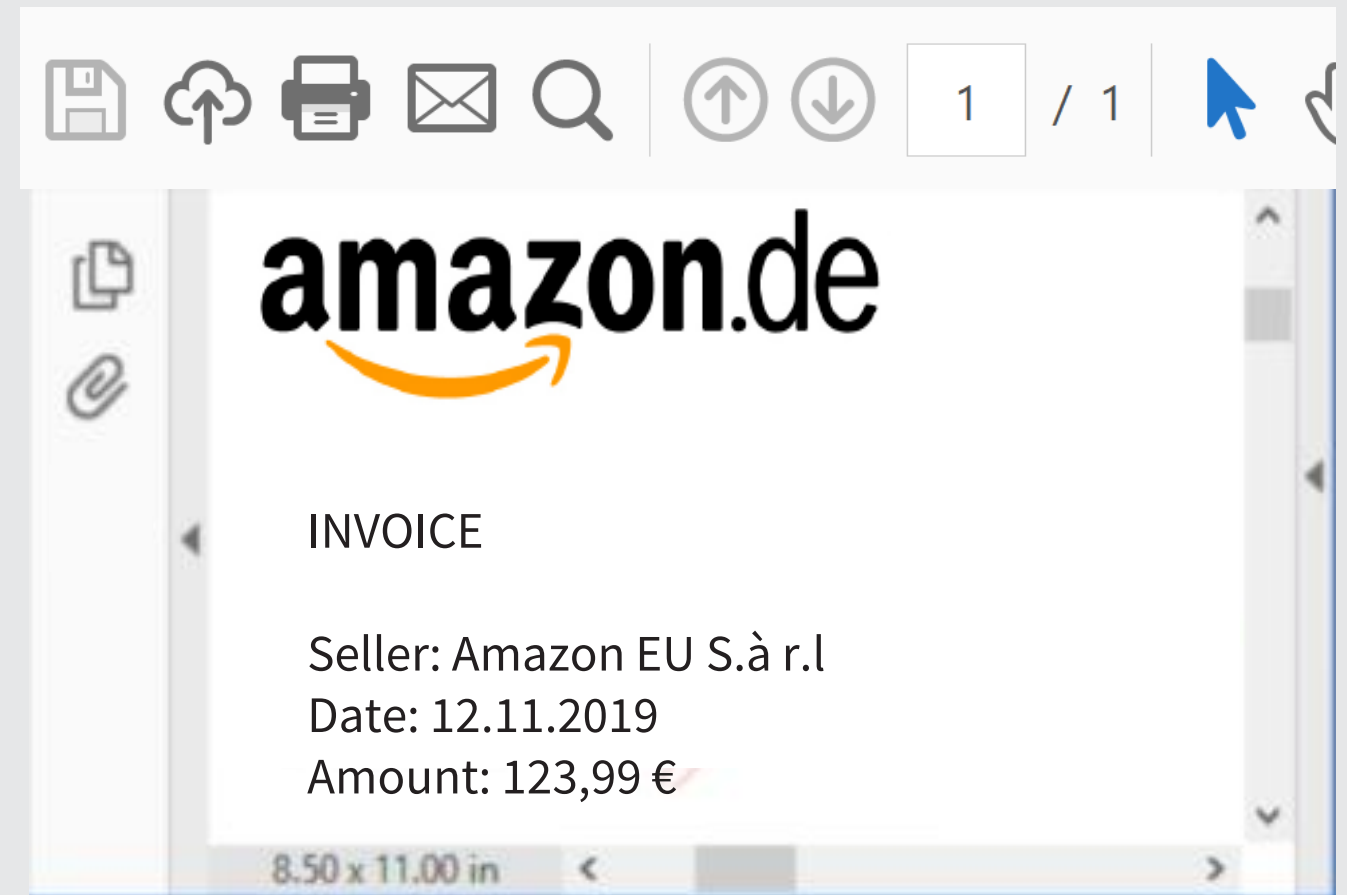
USED BY

~99%

COMPANIES AND GOVERNMENTAL
INSTITUTIONS **WORLDWIDE**

[Adobe Financial Analyst Meeting, December 16, 2021](#)

PDFs are Application Independent



PDFs can be Interactive



PDF viewer toolbar: Save, Upload, Print, Email, Search, Previous, Next, Page 1 / 1, Mouse, Hand, Zoom Out, Zoom In, 50%

Left sidebar: Document thumbnails, Bookmarks, Attachments, Layers

Form fields (highlighted with red borders):

- Details of the payee: Name, Surname/Company (max. 27 characters)
U n i c e f
- IBAN
D E 5 7 3 7 0 2 0 5 0 0 0 0 0 0 3 0 0 0 0 0
- BIC of the credit institution (8 oder 11 characters)
B F S W D E 3 3
- Amount: Euro, Cent
1 0 0 0 , 0 0
- Client-Reference number
1 2 2 3 4 4
- Subject
D o n a t i o n
- Account Owner
V L A D I S L A V M L A D E N O V
- IBAN
D E 08
- Date
31/01/2020
- Signature

Vertical text on the left: Art.-Nr. ZV 570 / ZV 572


PDFs support JavaScript



PDF viewer toolbar: Save, Star, Cloud, Print, Search, Up, Down, 2 / 2, Mouse, Hand, Zoom In, Zoom Out, 100%, Find, More, Link, Email.

#2 Readable Date format, Calendar shown below Field

```
FormRouter_PlaceCalendar(this.getField("DateTest2"),true,"ddd mmm d, yyyy");
```

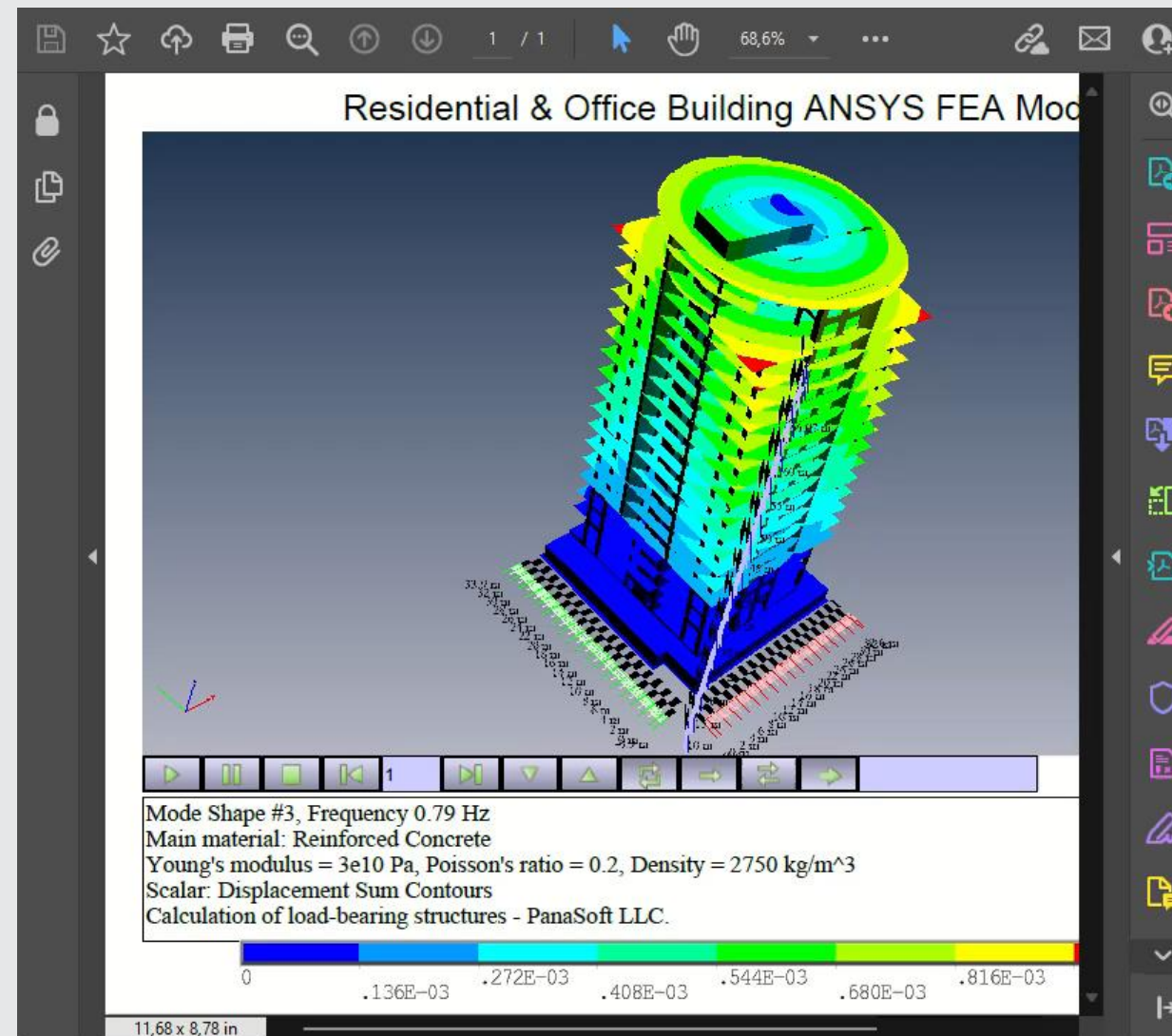
Date Test 2:  Thu Jun 23, 2022

#3 Shows how to use the instance of a field on a different page

Field "FormDateField" is the duplicate of the field in the example on the first page. This field was duplicated below. In order to use the duplicate we have to pass in the widget for the duplicate. Notice the "dot" notation used in the field name.

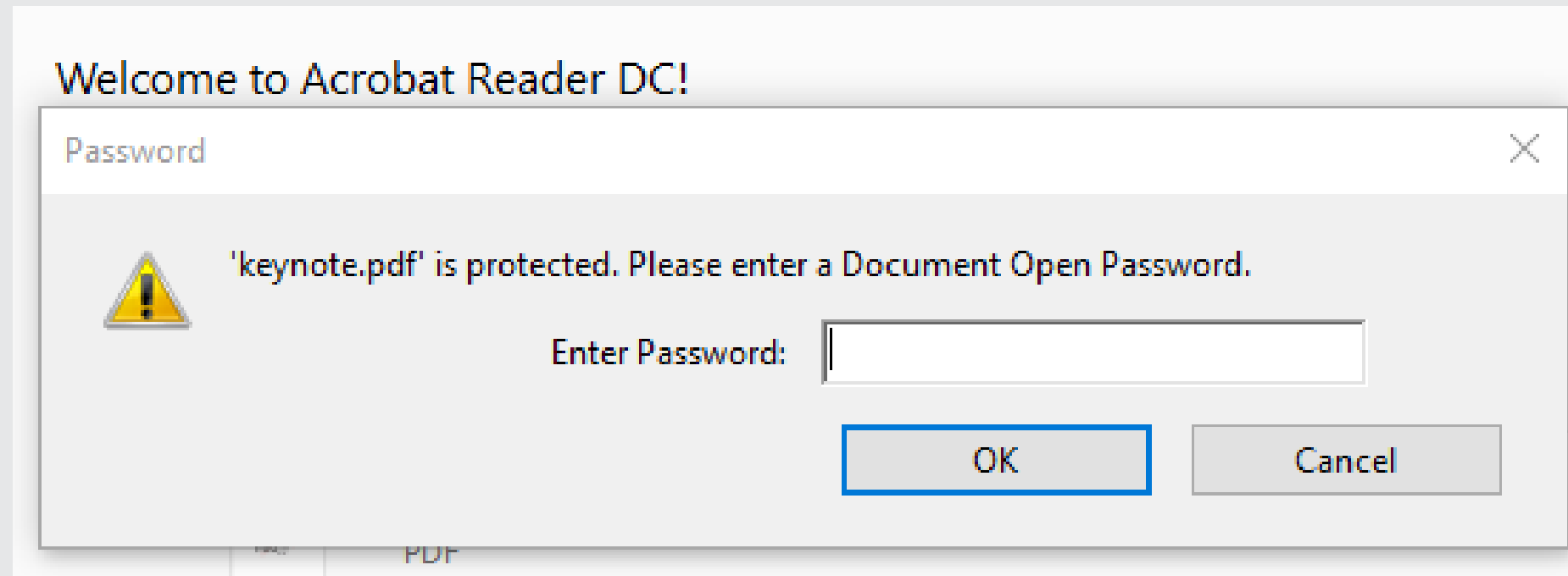
```
FormRouter_PlaceCalendar(this.getField("FormDateField.1"),true,"mmm d, yyyy")
```

PDFs support Multimedia (Audio/Video/3D)

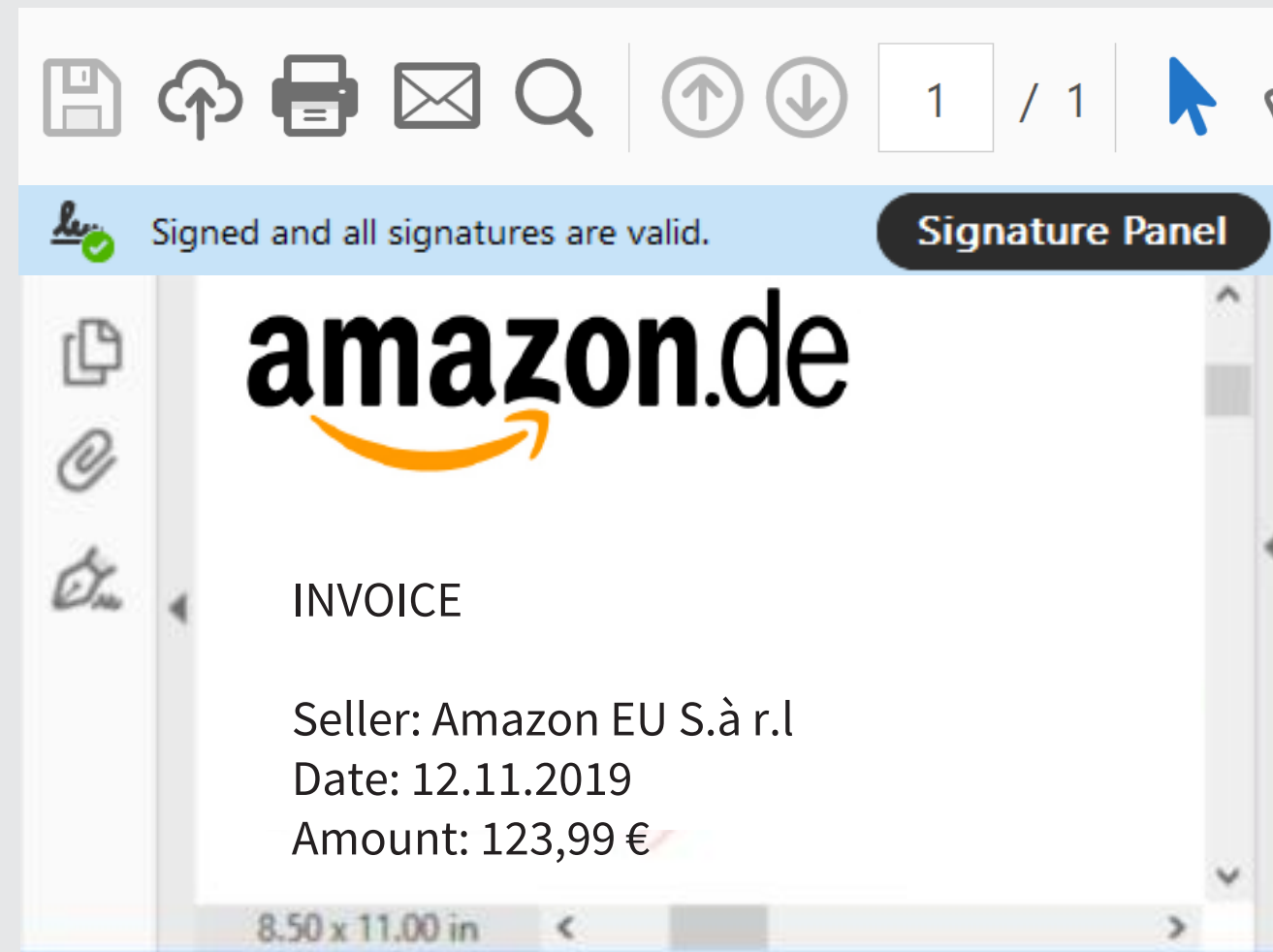


https://www.pdf3d.com/wp-content/uploads/2021/01/ansys_apartment_building_animation_450k_v4.pdf

PDFs can be Encrypted

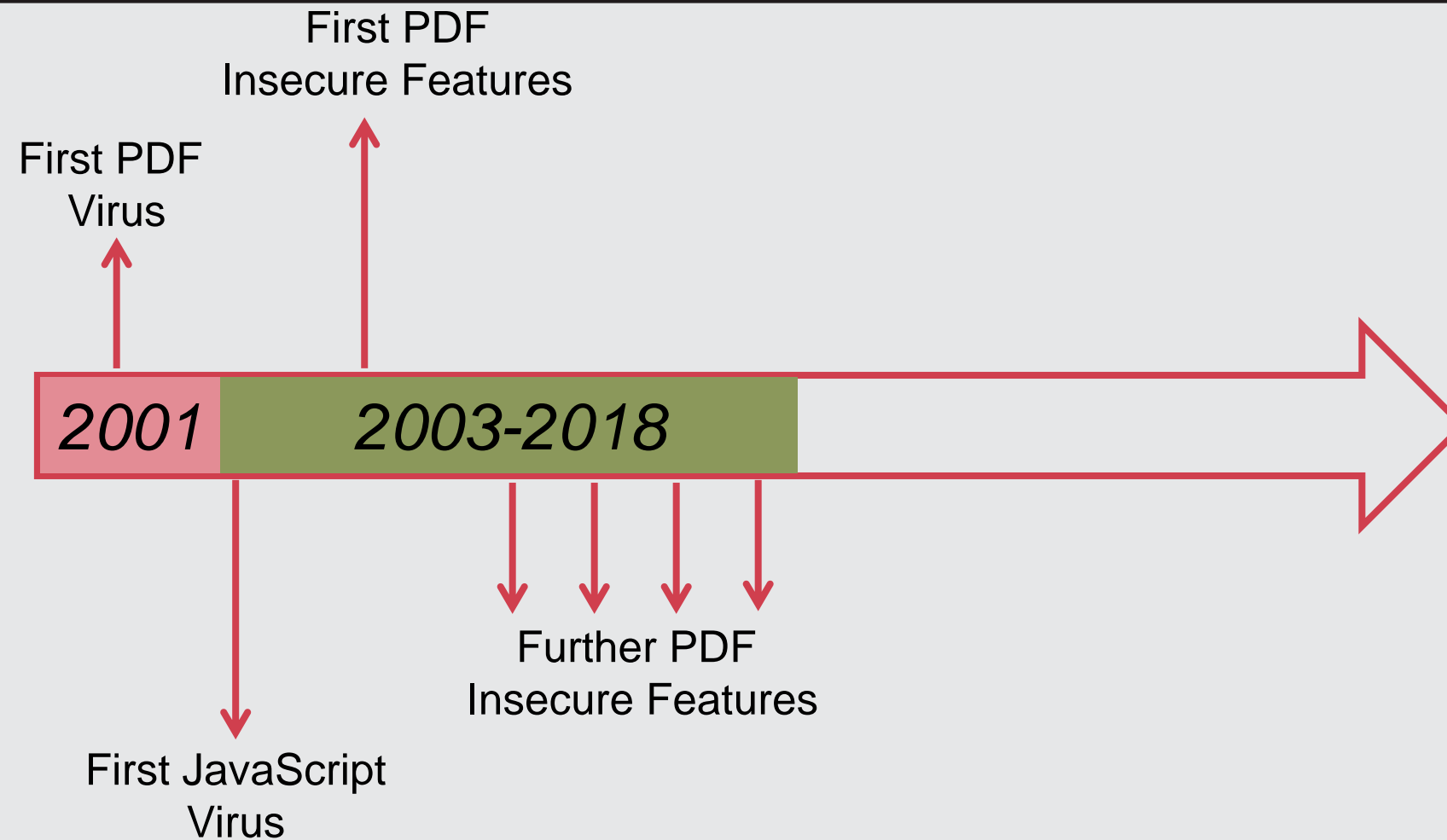


PDFs can be Digitally Signed

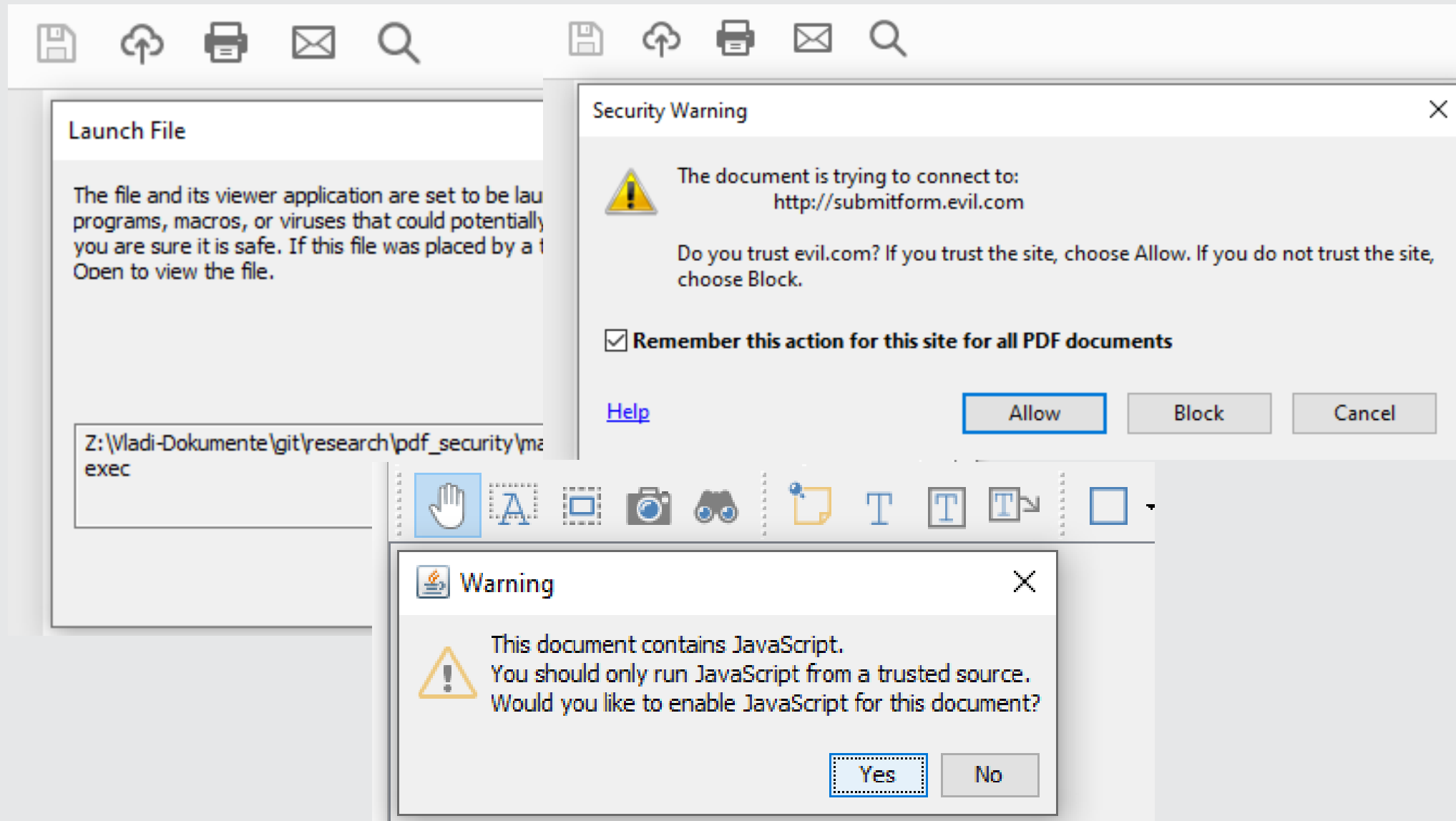


**Hey... it's a PDF.
What can go wrong?**

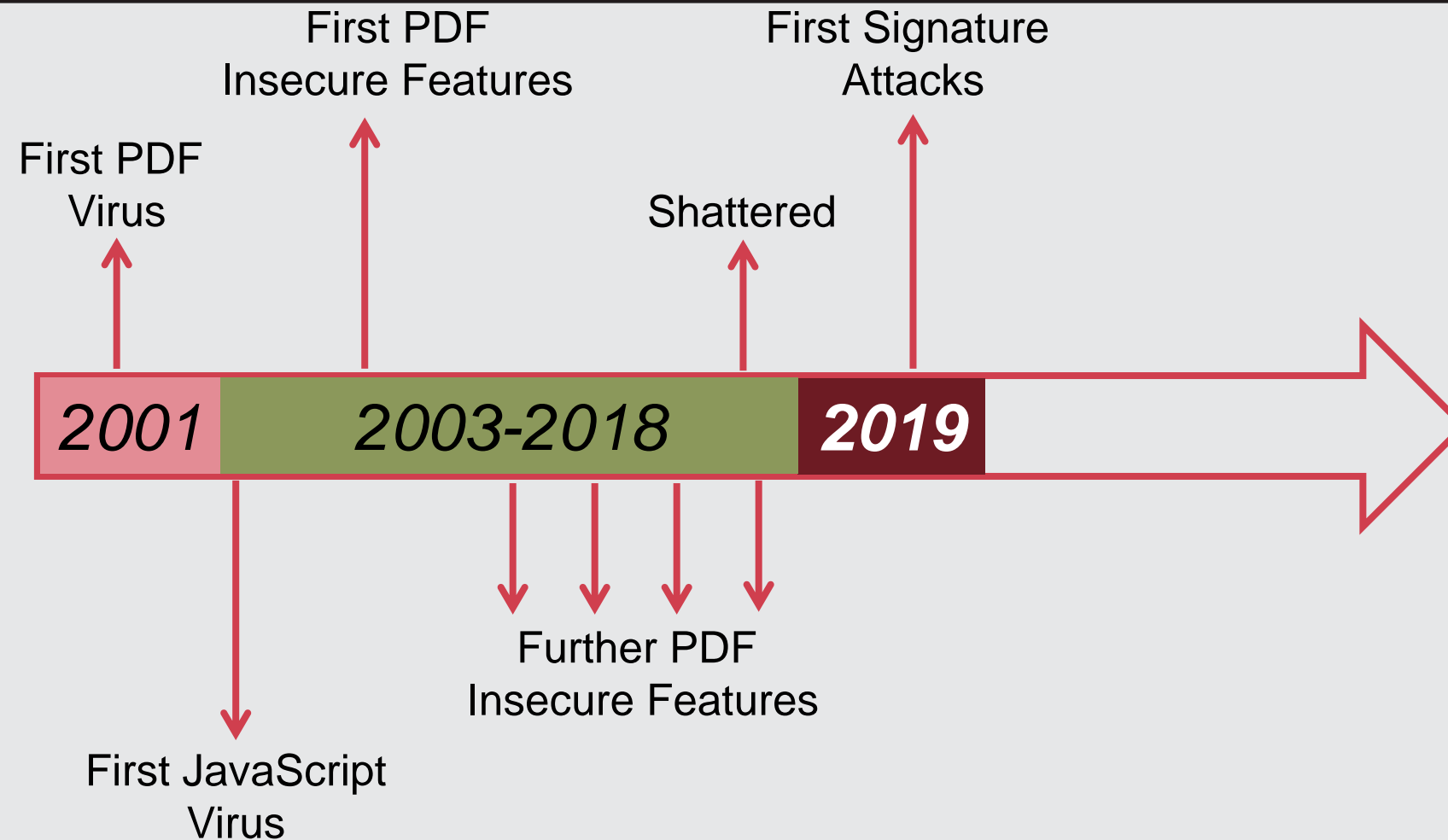
PDF Security Roadtrip

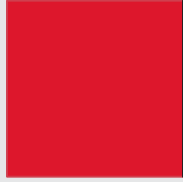


PDF Security Roadtrip



PDF Security Roadtrip





Live Demo

Attacking PDF Signatures (CCS'19)



First comprehensive analysis

Three novel attacks

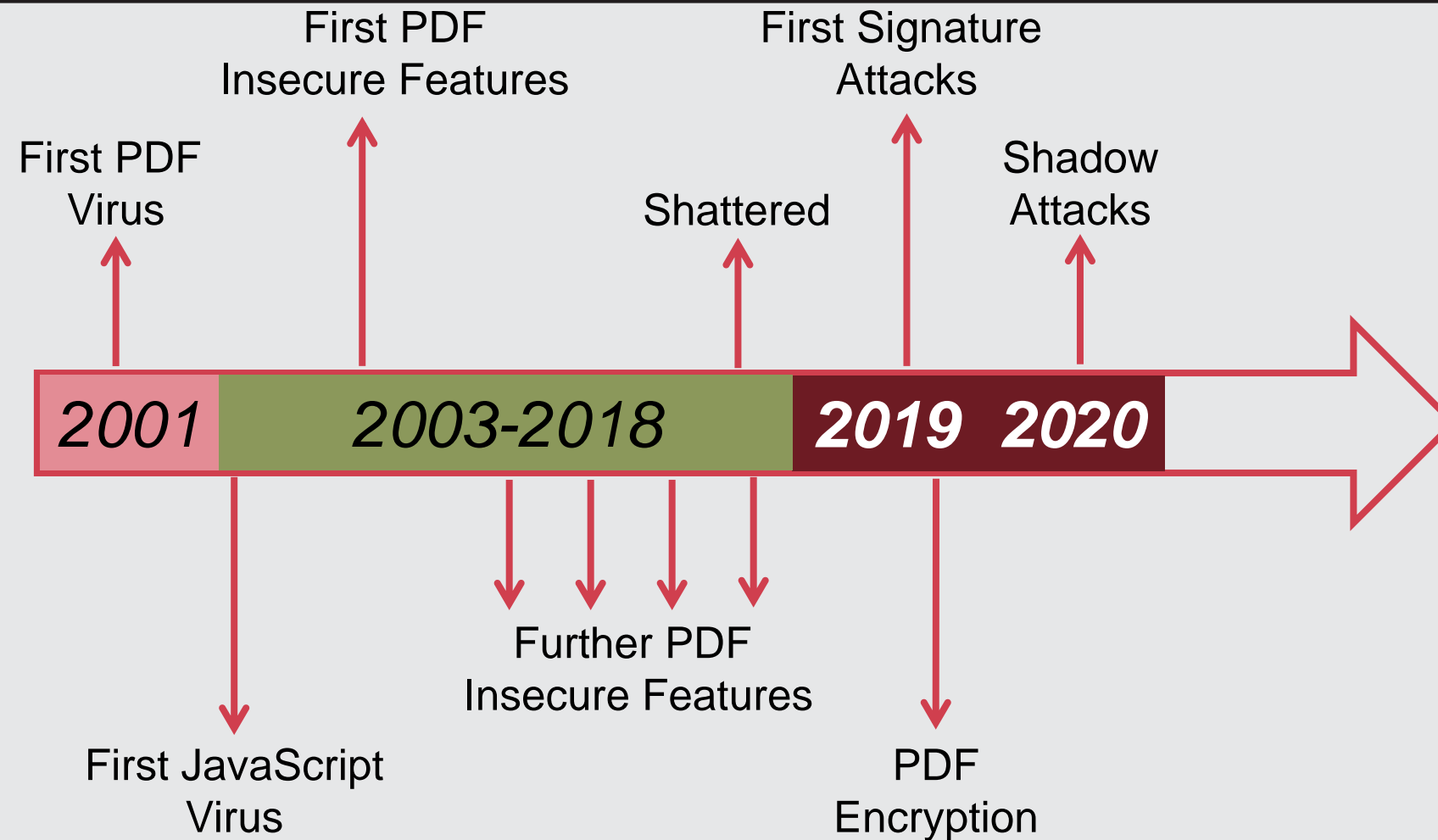
21 of 22 applications are vulnerable

<https://pdf-insecurity.org/>

Product	ISA	SWA	USF	Summary
Adobe Reader DC	○	○	●	●
Adobe Reader 9	○	○	○	○
Adobe Reader XI	○	●	●	●
eXpert PDF 12 Ultimate	○	●	○	●
Expert PDF Reader	○	●	○	●
Foxit Reader	●	●	○	●
LibreOffice (Draw)	◐	○	○	●
Master PDF Editor	●	○	○	●
Nitro Pro	◐	●	○	●
Nitro Reader	◐	●	○	●
Nuance Power PDF Standard	○	●	○	●
PDF Architect 6	○	●	○	●
PDF Editor 6 Pro	◐	●	◐	●
PDFelement 6 Pro	◐	●	◐	●
PDF Studio Viewer 2018	●	●	○	●
PDF Studio Pro	●	●	○	●
PDF-Xchange Editor	○	●	○	●
PDF-Xchange Viewer	○	●	○	●
Perfect PDF 10 Premium	●	●	○	●
Perfect PDF Reader	●	●	○	●
Soda PDF Desktop	○	●	○	●
Soda PDF	○	●	○	●
Total	11/22	17/22	4/22	21/22

- Full Signature Bypass
- ◐ Limited Signature Bypass
- Not vulnerable

PDF Security Roadtrip



Shadow Attacks on PDF Signatures (NDSS'21)



New Attacker Model

Three novel attacks

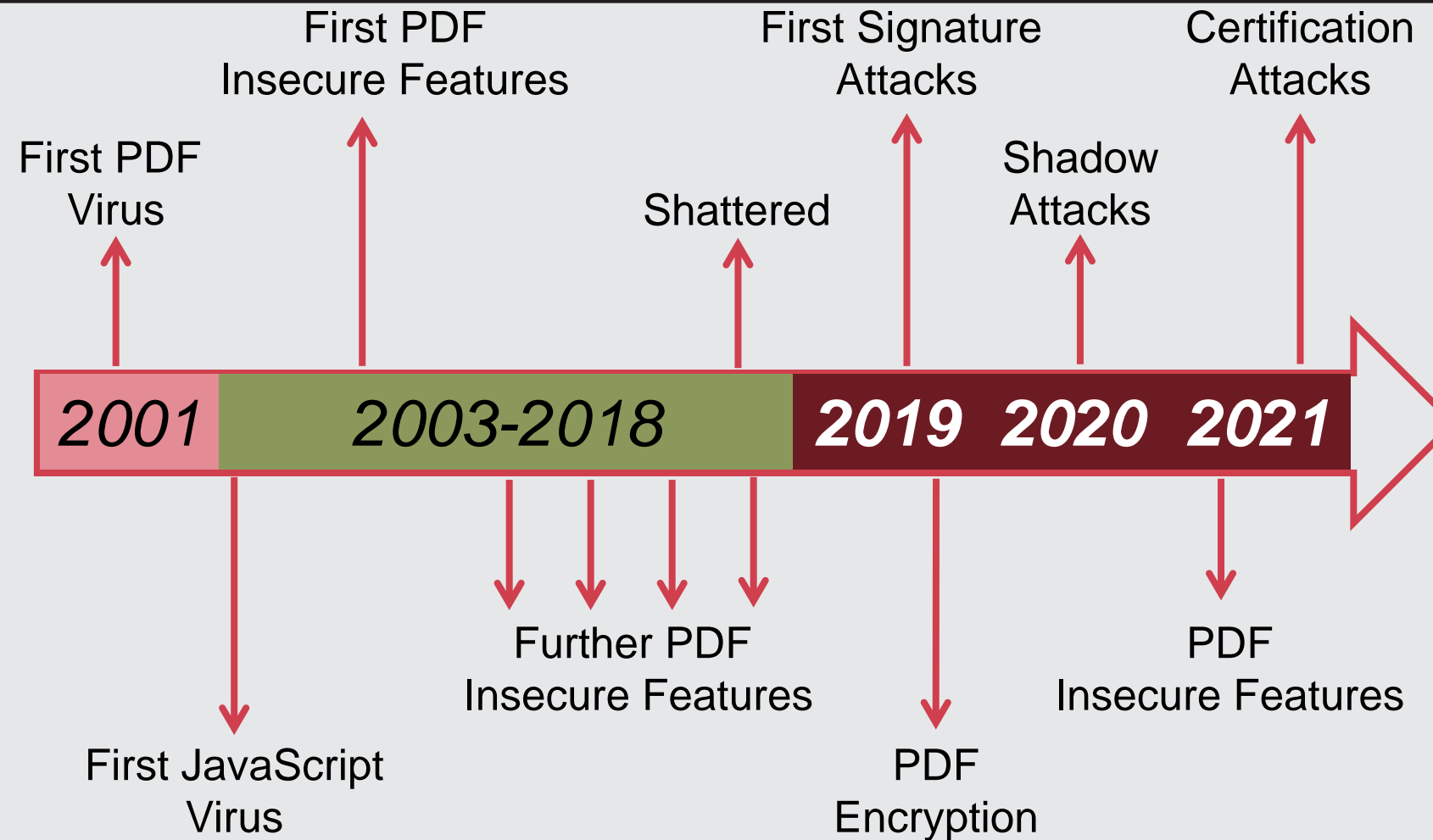
16 of 29 applications are vulnerable

<https://pdf-insecurity.org/>

Platform	Product	Hide	Replace	Hide-&Replace
	Adobe Reader DC	●	●	●
	Adobe Pro 2017	●	●	●
	Expert PDF 14	◐	◐	◐
	Foxit Reader	○	●	●
	Foxit PhantomPDF	○	●	●
	LibreOffice Draw	○	◐	◐
	Master PDF Editor	○	●	●
	Nitro Pro	◐	◐	◐
	Nitro Reader	◐	◐	◐
	PDF Architect 7	◐	◐	◐
	PDF Editor 6 Pro	●	●	●
	PDFElement	●	●	●
	PDF-XChange Editor	◐	◐	◐
	Perfect PDF Reader	◐	◐	◐
	Perfect PDF 8 Reader	●	●	●
	Perfect PDF 10 Premium	●	●	●
	Power PDF Standard	●	●	●
	Soda PDF Desktop	○	◐	◐
	Adobe Reader DC	●	●	●
	Adobe Pro 2017	●	●	●
	Expert PDF 14	●	●	●
	Foxit Reader	●	●	●
	Foxit PhantomPDF	○	◐	◐
	LibreOffice Draw	○	○	○
	PDF Editor 6 Pro	○	○	○
	PDFElement	○	○	○
	Master PDF Editor	○	●	●
	LibreOffice Draw	○	◐	◐
	Okular	●	●	●
Summary	29	12/29	16/29	16/29

- Full Signature Bypass
- ◐ Limited Signature Bypass
- Not vulnerable

PDF Security Roadtrip



Breaking the Specification: PDF Certification (S&P'21)






Two novel attacks

21 of 26 applications are vulnerable

Abusing legitimate features of the specification

<https://pdf-insecurity.org/>

Platform	Product	EAA	SSA
	Adobe Reader DC	●	●
	Adobe Pro 2017	●	●
	Expert PDF 14	●	●
	Foxit Reader	●	○
	Foxit PhantomPDF	●	○
	LibreOffice Draw	◐	◐
	Master PDF Editor	●	●
	Nitro Pro	●	○
	Nitro Reader	●	○
	PDF Architect 7	●	●
	PDF Editor 6 Pro	○	●
	PDFElement	○	●
	PDF-XChange Editor	●	●
	Perfect PDF 8 Reader	●	●
	Perfect PDF 10 Premium	●	●
	Power PDF Standard	◐	●
	Soda PDF Desktop	●	●
	Adobe Reader DC	●	●
	Adobe Pro 2017	●	●
	Foxit Reader	●	○
	Foxit PhantomPDF	●	○
	LibreOffice Draw	◐	◐
	PDF Editor 6 Pro	○	○
	PDFElement	○	○
	Master PDF Editor	●	●
	LibreOffice Draw	◐	◐
Summary		26	18
		15	

Agenda



Digitally Signed PDFs



Core Issues

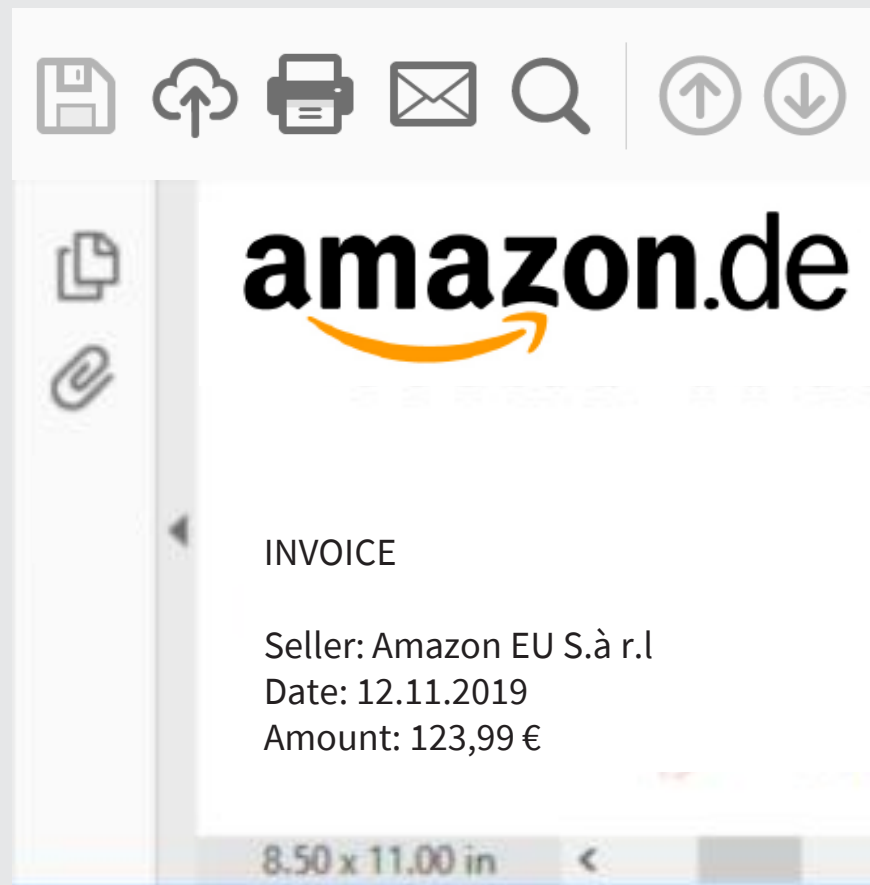


Beyond PDF Signatures

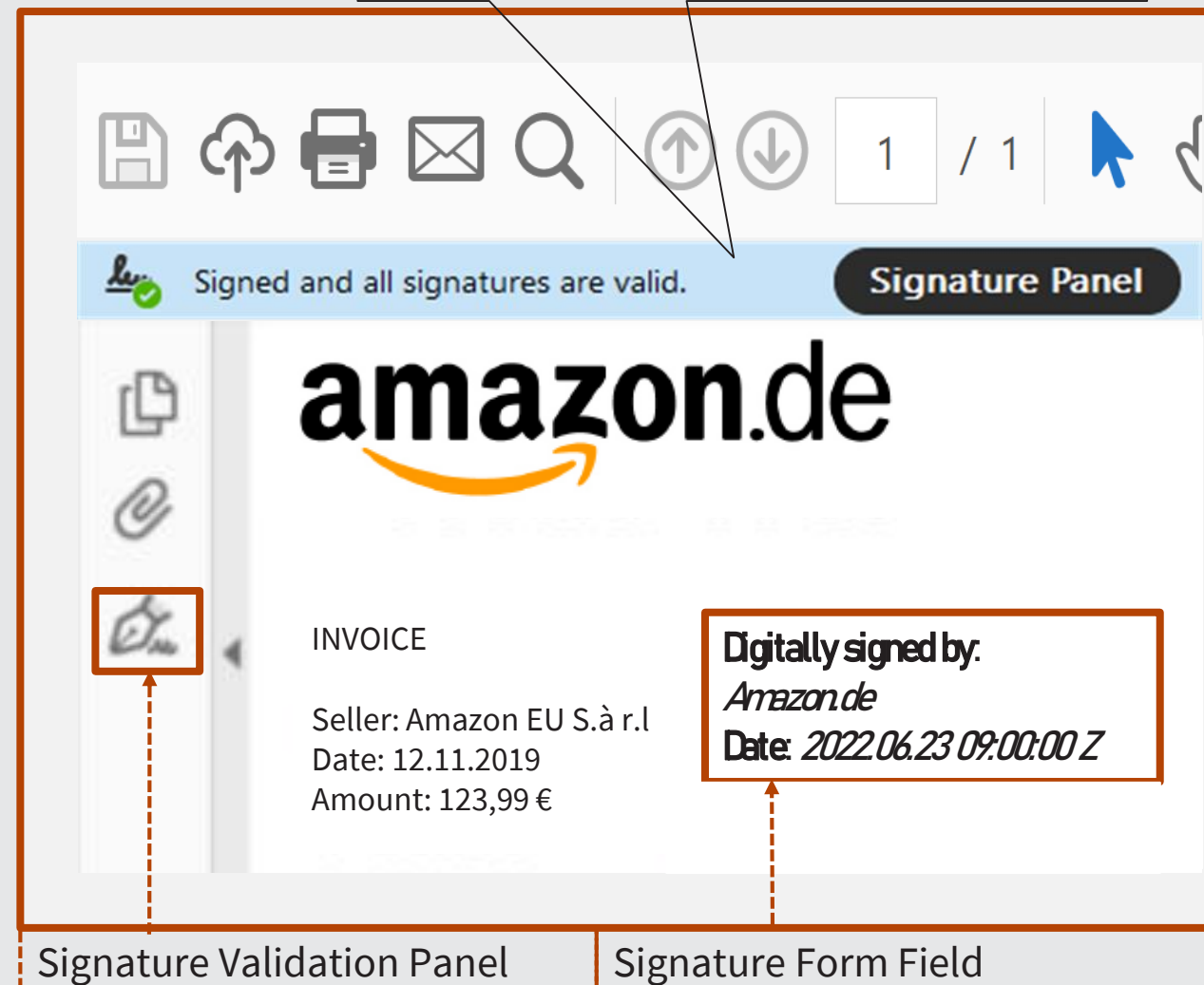


Lessons Learned

Unsigned vs. Signed PDFs



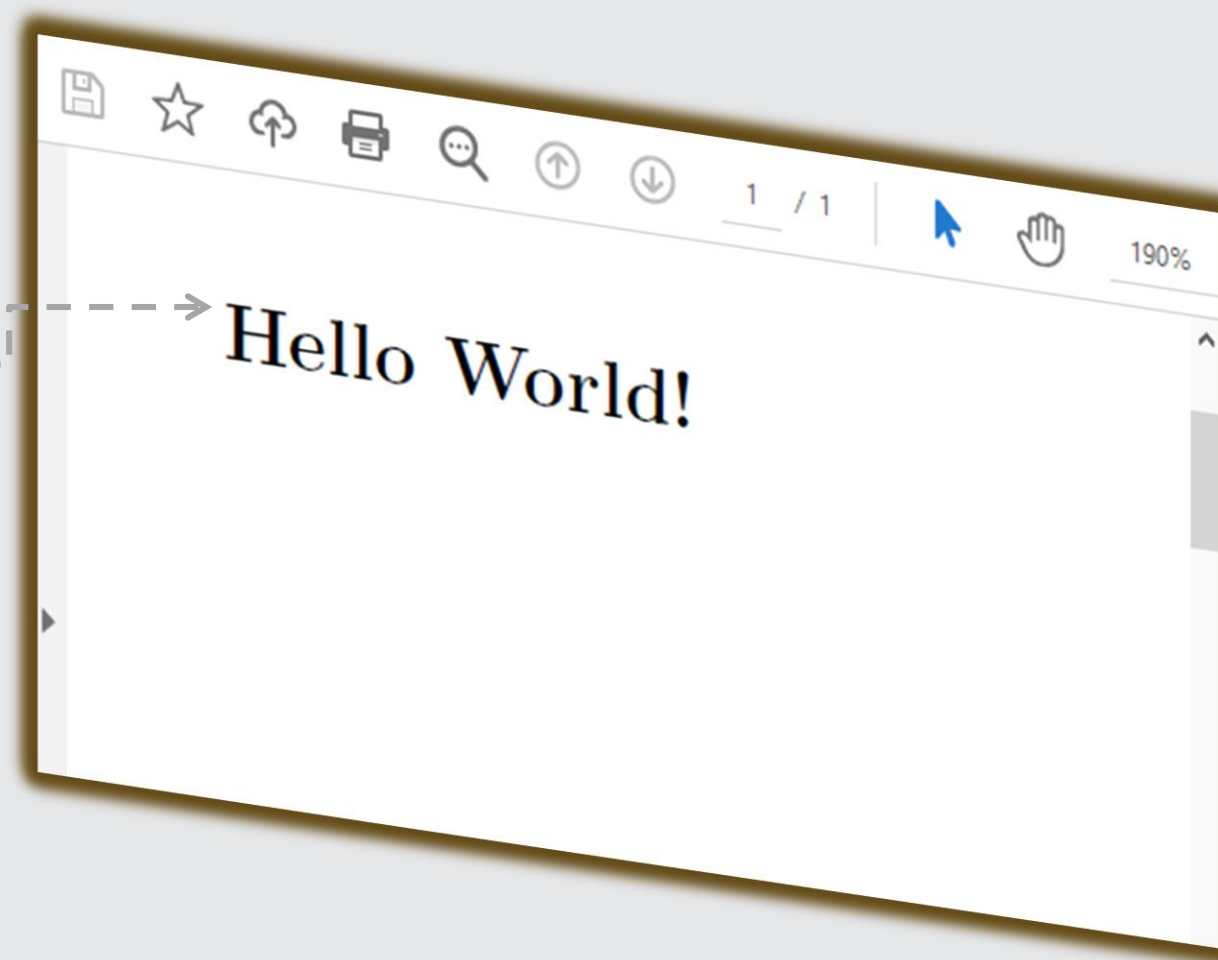
Cryptographic protection



Signing PDF Documents



%PDF-2.0	
1 0 obj (/Catalog) endobj	
2 0 obj (/Pages) endobj	
3 0 obj (/Page) endobj	
4 0 obj	
... (Hello World!)	
endobj	
xref	trailer



Signing PDF Documents



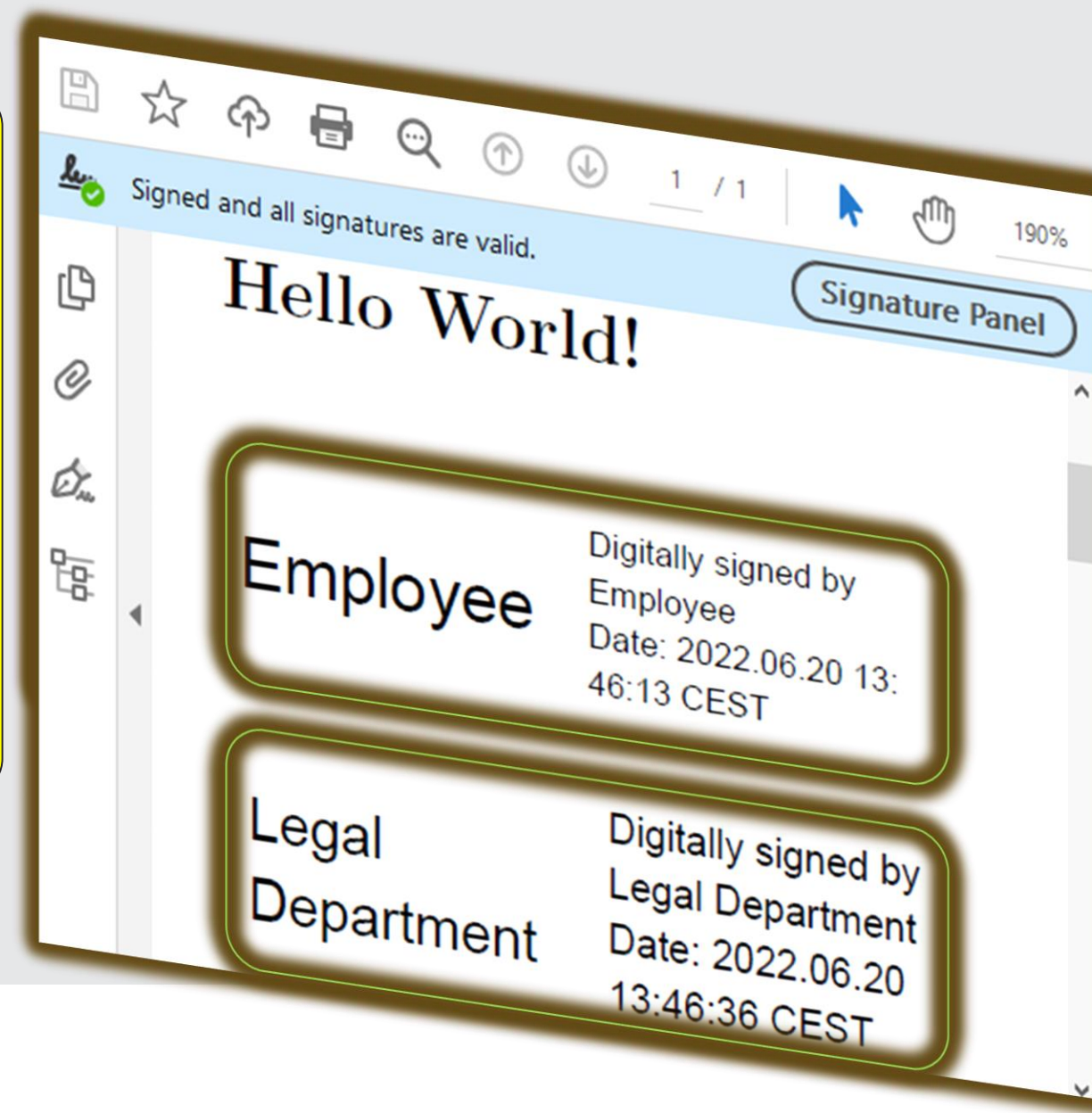
%PDF-2.0		Protected by the signature 1
1 0 obj (/Catalog) endobj		
2 0 obj (/Pages) endobj		
3 0 obj (/Page) endobj		
4 0 obj ... (Hello World!) endobj		
xref	trailer	
Incremental Update:Signature 1		
5 0 obj (/Sig) endobj		
xref	trailer	



Signing PDF Documents



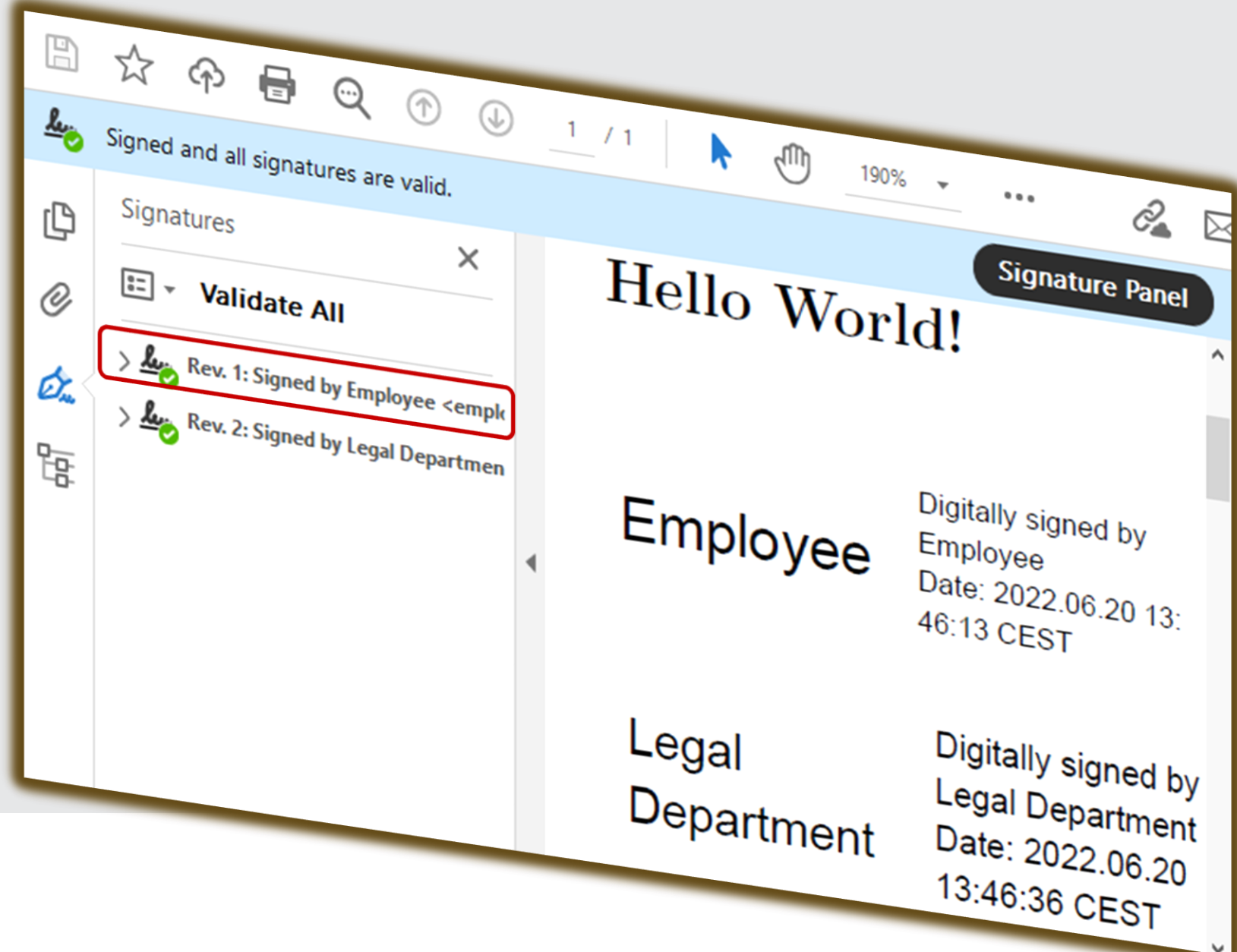
%PDF-2.0		Protected by the signature 1
1 0 obj (/Catalog) endobj		
2 0 obj (/Pages) endobj		
3 0 obj (/Page) endobj		
4 0 obj ... (Hello World!) endobj		
xref	trailer	Protected by the signature 2
Incremental Update:Signature 1		
5 0 obj (/Sig) endobj		
xref	trailer	
Incremental Update:Signature 2		
6 0 obj (/Sig) endobj		
xref	trailer	



Signing PDF Documents



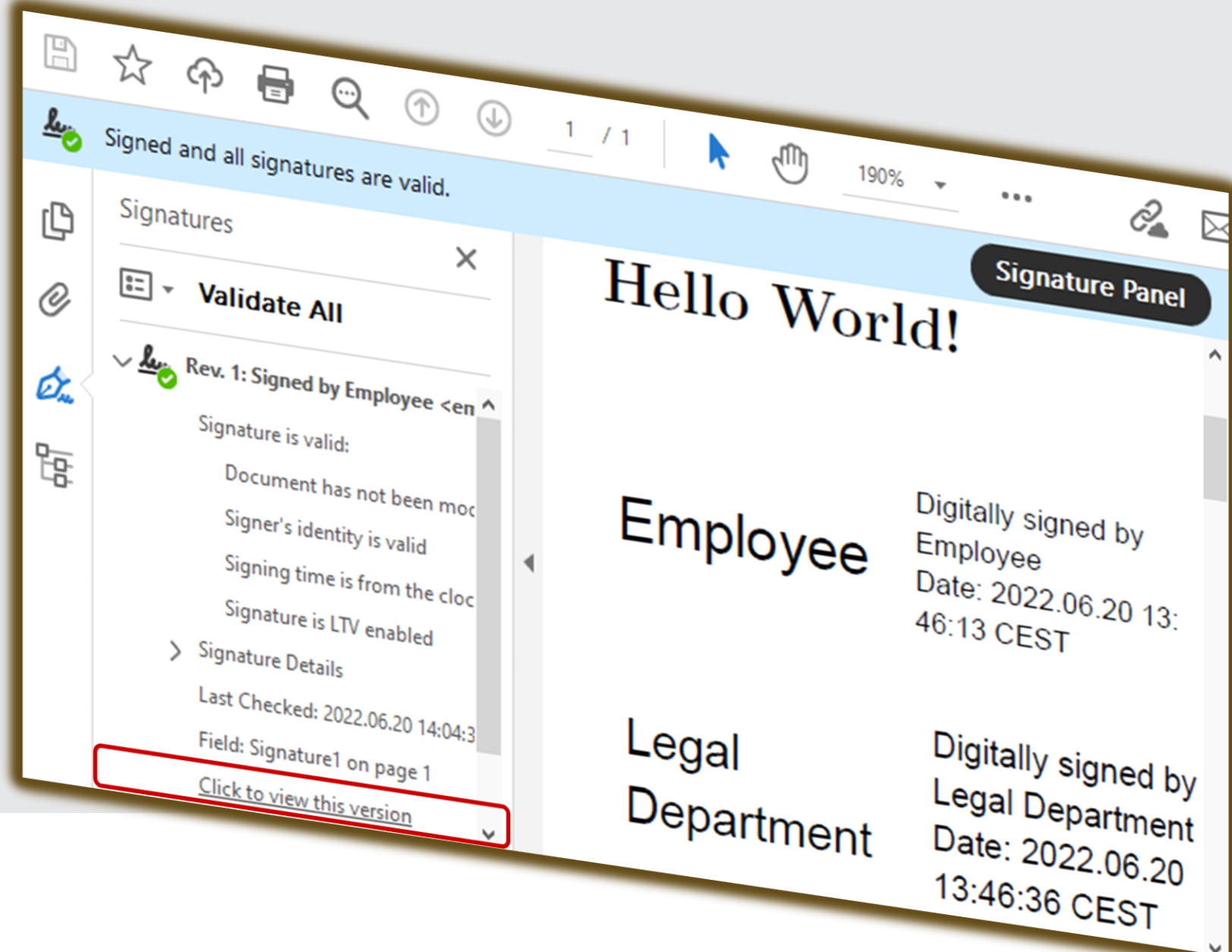
%PDF-2.0		Protected by the signature 1
1 0 obj (/Catalog) endobj		
2 0 obj (/Pages) endobj		
3 0 obj (/Page) endobj		
4 0 obj ... (Hello World!) endobj		
xref	trailer	Protected by the signature 2
Incremental Update:Signature 1 5 0 obj (/Sig) endobj		
xref	trailer	
Incremental Update:Signature 2 6 0 obj (/Sig) endobj		
xref	trailer	



Signing PDF Documents



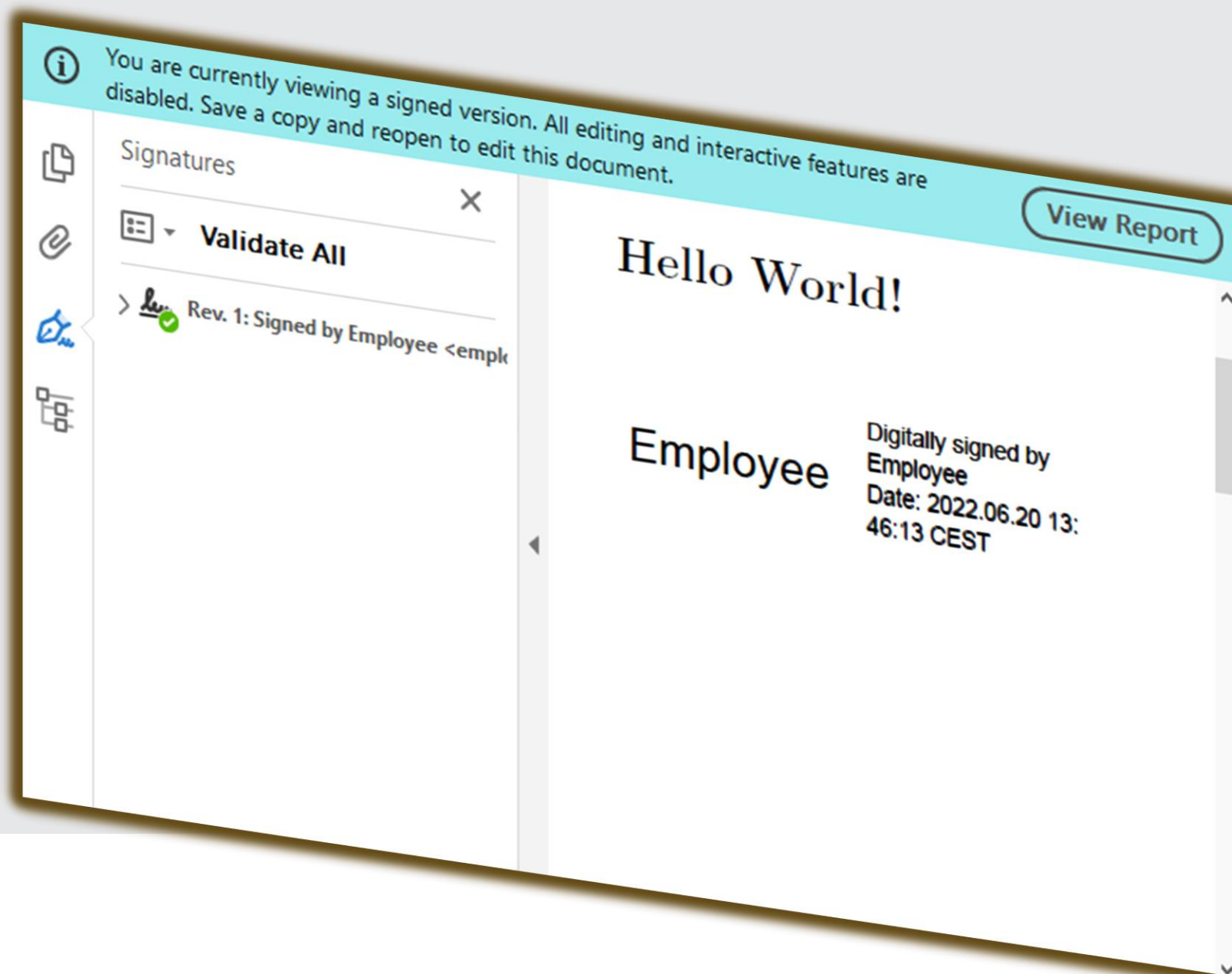
%PDF-2.0		Protected by the signature 1
1 0 obj (/Catalog) endobj		
2 0 obj (/Pages) endobj		
3 0 obj (/Page) endobj		
4 0 obj ... (Hello World!) endobj		
xref	trailer	Protected by the signature 2
Incremental Update:Signature 1 5 0 obj (/Sig) endobj		
xref	trailer	
Incremental Update:Signature 2 6 0 obj (/Sig) endobj		
xref	trailer	



Signing PDF Documents



%PDF-2.0		Protected by the signature 1
1 0 obj (/Catalog) endobj		
2 0 obj (/Pages) endobj		
3 0 obj (/Page) endobj		
4 0 obj		
... (Hello World!)		
endobj		
xref	trailer	
Incremental Update:Signature 1		
5 0 obj (/Sig) endobj		
xref	trailer	
Incremental Update:Signature 2		
6 0 obj (/Sig) endobj		
xref	trailer	



Signature Coverage in PDF Documents



PDF Document

Header
Body
XRef Section
Trailer



Signed PDF Document

Header
Body
XRef Section
Trailer
Body Updates
<i>Updated Xref Section</i>
<i>Updated Trailer</i>

Protected by the signature 1



2x Signed PDF Document

Header
Body
XRef Section
Trailer
Body Updates
<i>Updated Xref Section</i>
<i>Updated Trailer</i>
Body Updates
<i>Updated Xref Section</i>
<i>Updated Trailer</i>

Protected by the signature 1

Protected by the signature 2



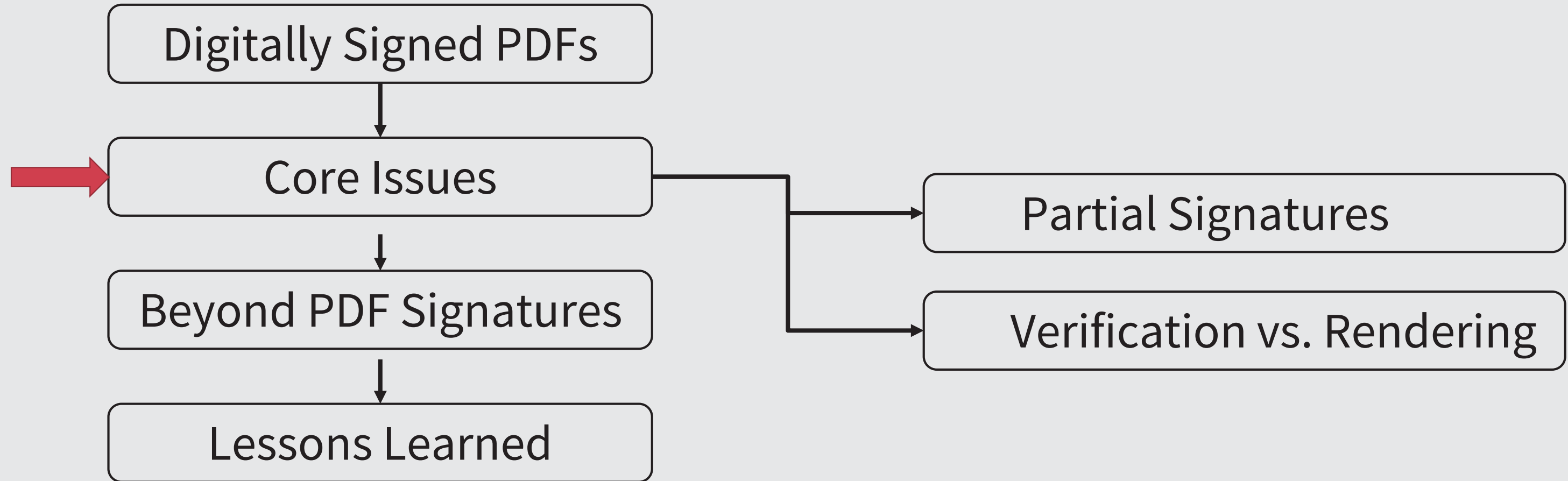
Modified PDF Document

Header
Body
XRef Section
Trailer
Body Updates
<i>Updated Xref Section</i>
<i>Updated Trailer</i>
Body Updates
<i>Updated Xref Section</i>
<i>Updated Trailer</i>

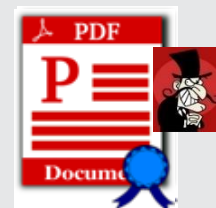
Protected by the signature 1

The signature does not always cover the entire content!!!

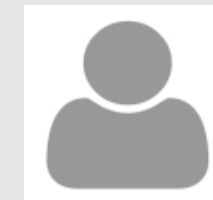
Agenda





The story so far ...




Manipulated Signed PDF





 Signed and all signatures are valid. Signature




Signatures

 **Validate All**

  Rev. 1: Signed by invoicing@amazon.de

Signature is valid:
Document has not been modified since
Signer's identity is valid
Signing time is from the clock on the
> Signature Details
Last Checked: 2019.01.29 17:06:18 Z



Your refund is:
\$ 1,000,000,000,000
(One Trillion USD)

Incremental Saving Attack



Header
Body
XRef Section
Trailer



PDF Document

Header
Body
XRef Section
Trailer
Body Updates
Updated Xref Section
Updated Trailer

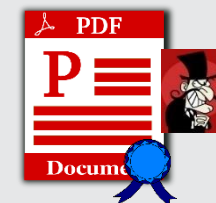
Protected by the signature



Signed
PDF Document

Header
Body
XRef Section
Trailer
Body Updates
Updated Xref Section
Updated Trailer
Malicious Body Updates
Malicious Xref Section
Malicious Trailer

Protected by the signature

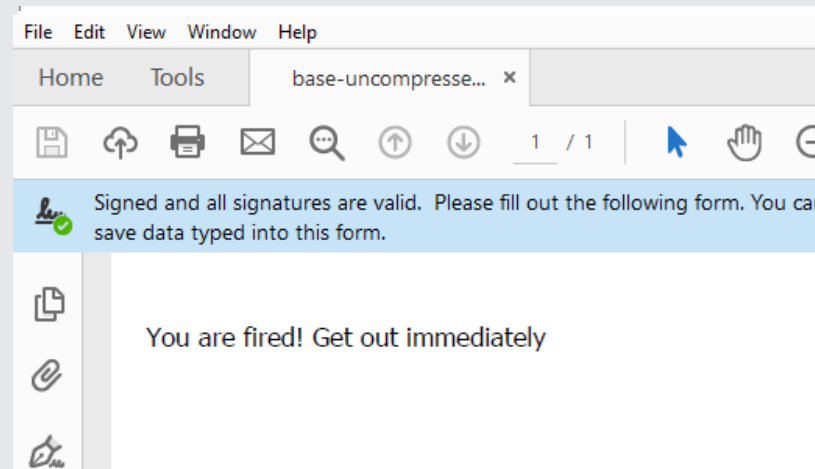


Manipulated Signed
PDF Document

Incremental Saving Attack



%PDF-1.4	Protected by the signature
1 0 obj (/Catalog) endobj	
2 0 obj (/Pages) endobj	
3 0 obj (/Page) endobj	
4 0 obj	
... (Sign the document to get a reward!)	
endobj	
Xref Section	
Trailer	
%%EOF	
Updated Body	Protected by the signature
Signature Objects	
Updated Xref Section	
Updated Trailer	
%%EOF	
4 0 obj	
... (You are fired. Get out immediately)	
endobj	
Updated Xref Section	Protected by the signature
Updated Trailer	
%%EOF	



Attacking PDF Signatures (CCS'19)



Product	ISA	SWA	USF	Summary
Adobe Reader DC	○	○	●	●
Adobe Reader 9	○	○	○	○
Adobe Reader XI	○	●	●	●
eXpert PDF 12 Ultimate	○	●	○	●
Expert PDF Reader	○	●	○	●
Foxit Reader	●	●	○	●
LibreOffice (Draw)	◐	○	○	●
Master PDF Editor	●	○	○	●
Nitro Pro	◐	●	○	●
Nitro Reader	◐	●	○	●
Nuance Power PDF Standard	○	●	○	●
PDF Architect 6	○	●	○	●
PDF Editor 6 Pro	◐	●	◐	●
PDFelement 6 Pro	◐	●	◐	●
PDF Studio Viewer 2018	●	●	○	●
PDF Studio Pro	●	●	○	●
PDF-Xchange Editor	○	●	○	●
PDF-Xchange Viewer	○	●	○	●
Perfect PDF 10 Premium	●	●	○	●
Perfect PDF Reader	●	●	○	●
Soda PDF Desktop	○	●	○	●
Soda PDF	○	●	○	●
Total	11/22	17/22	4/22	21/22

Evaluation results

- Full Signature Bypass
- ◐ Limited Signature Bypass
- Not vulnerable

Attacks on PDF Signatures (NDSS'21)



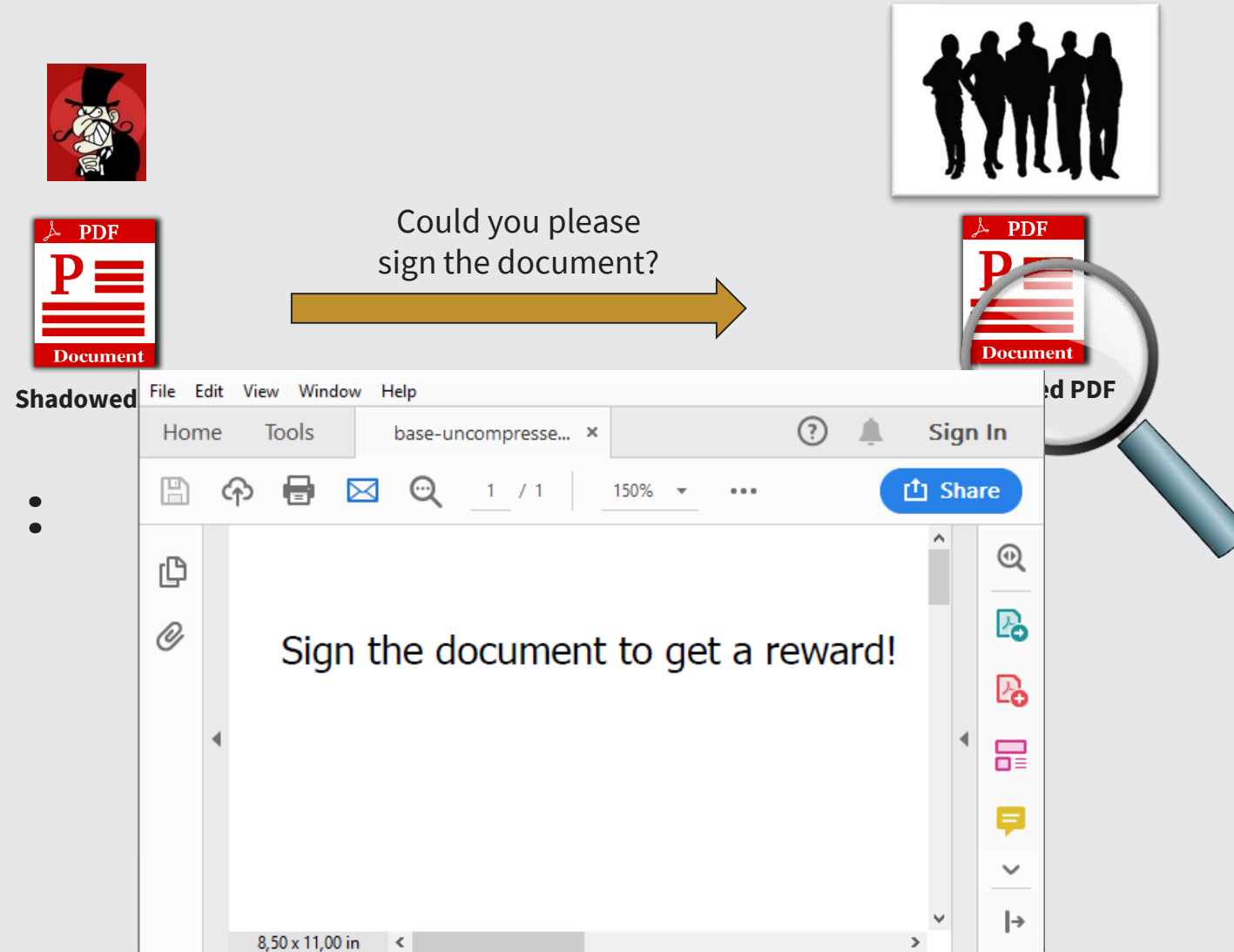
42 0 obj

<<

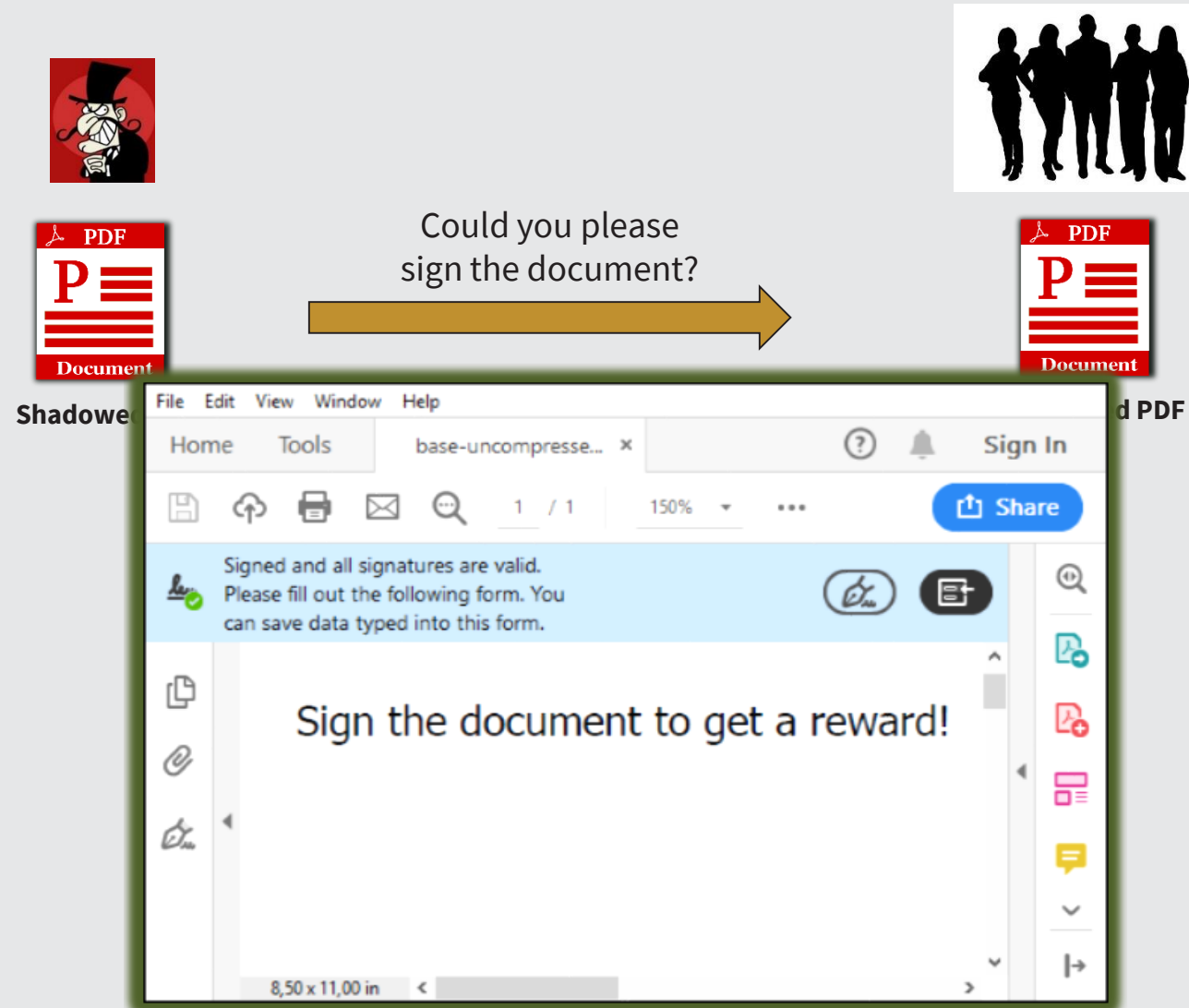
Shadow Obj:

You are
fired!

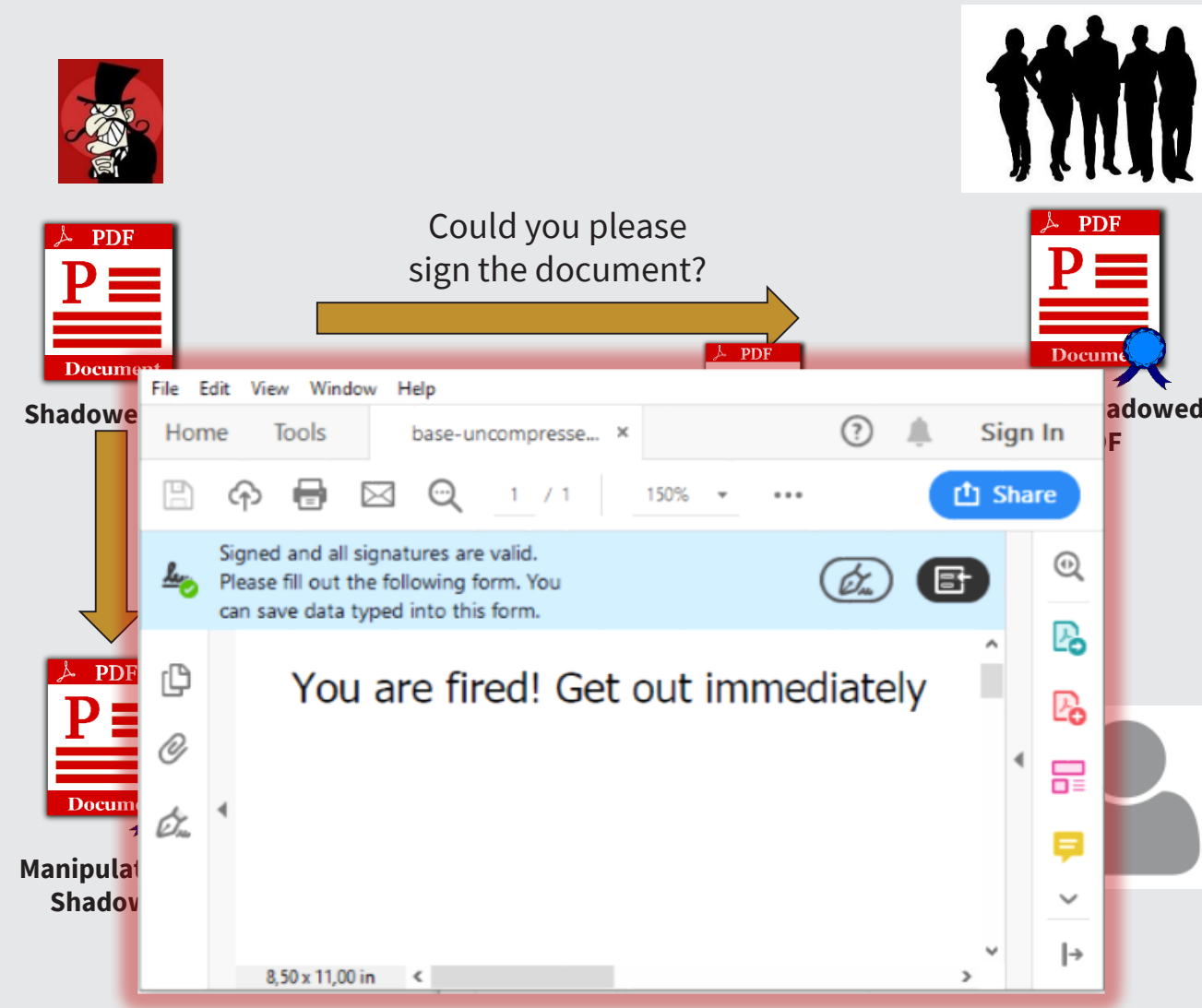
>>



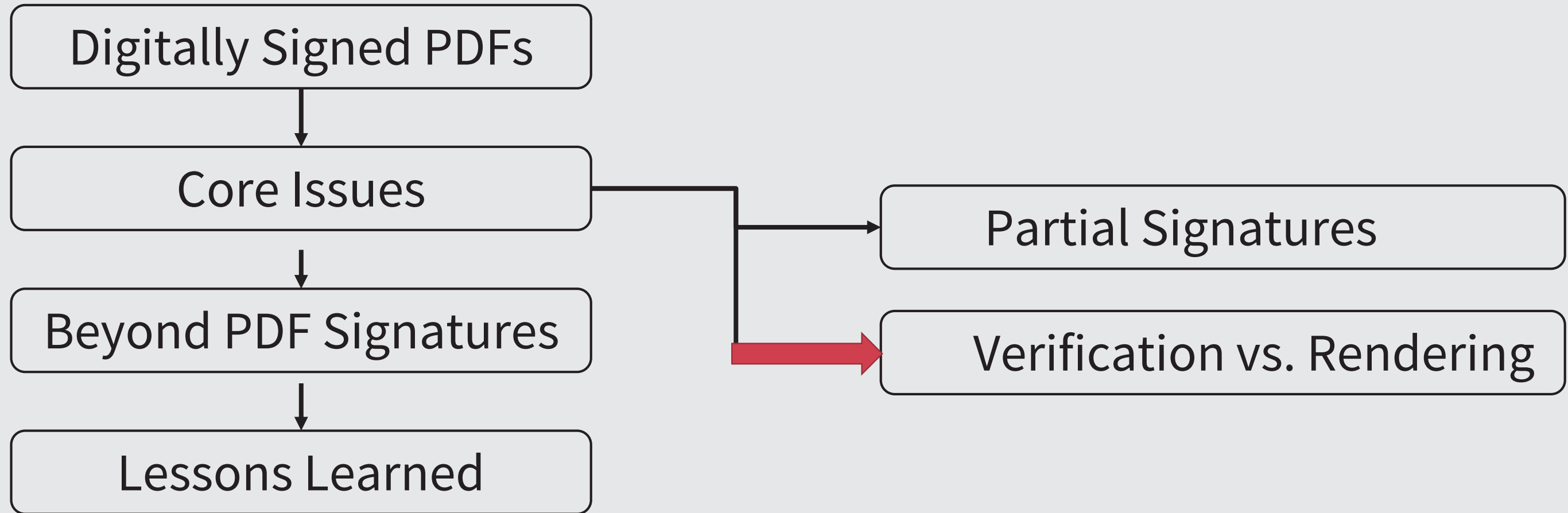
Goals and Prerequisites



Goals and Prerequisites



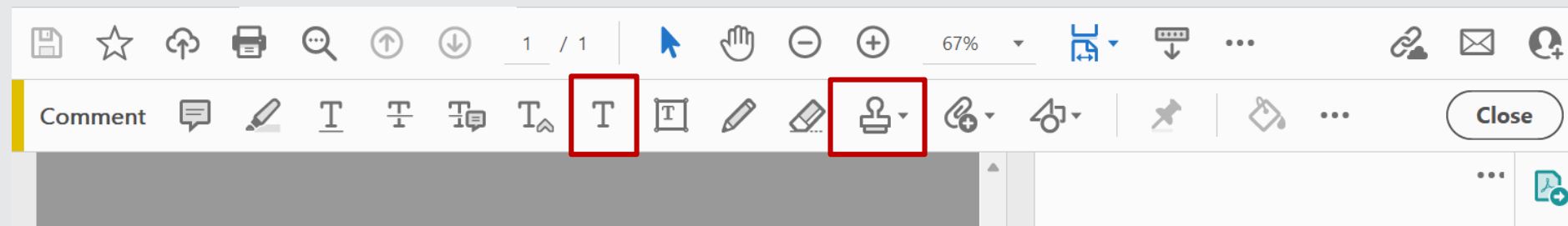
Agenda



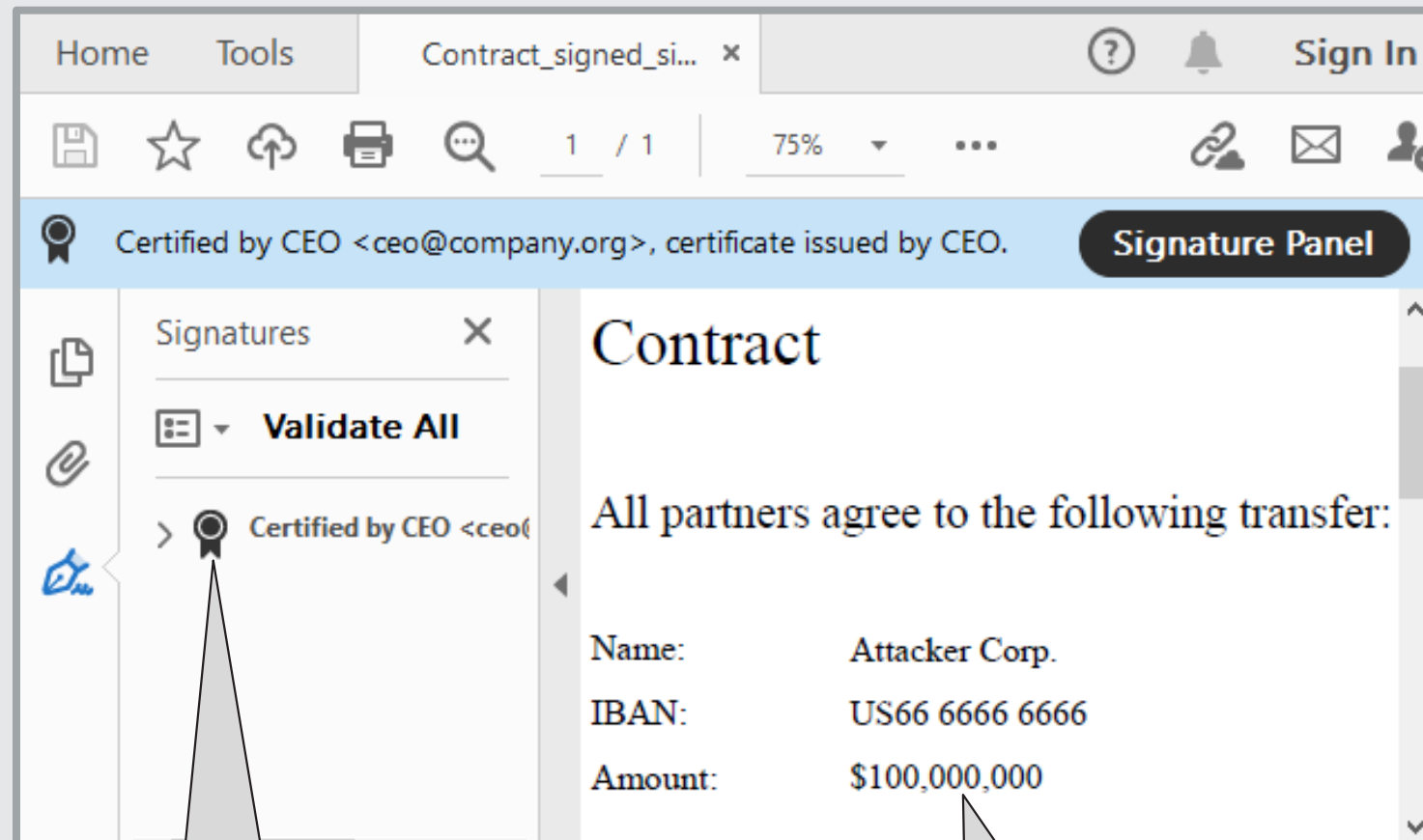
PDF Features: Annotations



- Can be used on signed PDFs
- What can go wrong?



Using Evil Annotations to Change Content (SP'21)



Verification

Rendering

1. Use `/Type /Stamp` to hide content with a white image
2. Use `/Type /FreeText` to add text chosen by the attacker

User Interface (UI) Layers



The screenshot shows a PDF viewer interface with several UI layers highlighted by red boxes and annotated with callouts:

- UI-Layer 1** (top bar): A blue bar containing a certificate status "Certified by CEO <ceo@company.org>, certificate issued by CEO." and a "Signature Panel" button. Callout: "UI-Layer 1 is always displayed when the document is opened."
- UI-Layer 2** (left sidebar): A panel titled "Signatures" with a "Validate All" button and a list of signatures. Callout: "UI-Layer 2 must be opened by the user."
- UI-Layer 3** (right sidebar): A panel titled "Comments" with a "No Comments Yet" message and a list of comment icons. Callout: "UI-Layer 3 must be opened by the user, but makes the modifications detectable."

The main content area displays a "Contract" document with the following text:

Contract

All partners agree to the fol

Name:	Attacker Corp.
IBAN:	US66 6666 6666
Amount:	\$100,000,000

At the bottom, a callout states: "We found implementation Bugs that hide them".

For annotations there is another relevant UI-Layer!

Agenda



Digitally Signed PDFs



Core Issues



Beyond PDF Signatures



Lessons Learned

What About Other Document Formats? (USENIX'22)



Oops... Code Execution and Content Spoofing: The First Comprehensive Analysis of OpenDocument Signatures

Simon Rohlmann
Ruhr University Bochum

Christian Mainka
Ruhr University Bochum

Vladislav Mladenov
Ruhr University Bochum

Jörg Schwenk
Ruhr University Bochum



Abstract

OpenDocument is one of the major standards for interoperable office documents. Supported by office suites like Apache OpenOffice, LibreOffice, and Microsoft Office, the OpenDocument Format (ODF) is available for text processing, spreadsheets, and presentations on all major desktop and mobile operating systems.

When it comes to governmental and business use cases, OpenDocument signatures can protect the integrity of a document's content, for example, for contracts, amendments, or bills. Moreover OpenDocument signatures also protect document's macros. Since the risks of using macros in documents is well-known, modern office applications only enable their execution if a trusted entity signs the macro code. Thus, the security of ODF documents often depends on the correct signature verification.

In this paper, we conduct the first comprehensive analy-

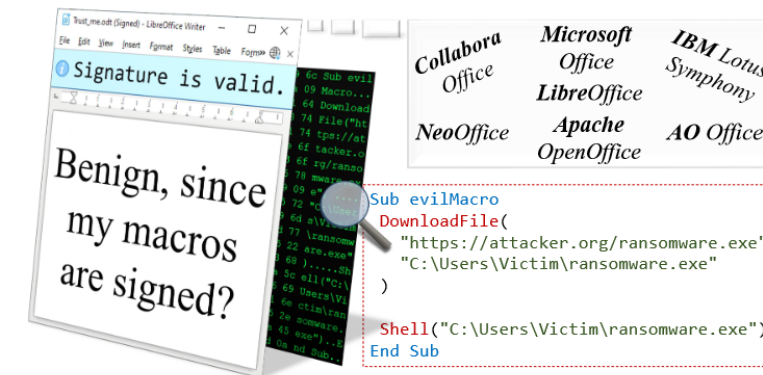


Figure 1: If an ODF document's macro has a trusted signature, its code is automatically executed once the document is opened. We show how an attacker can execute malicious macros and manipulate the entire content by spoofing the digital signature in ODF documents.

What About Other Document Formats? (USENIX'23)



Every Signature is Broken: On the Insecurity of Microsoft Office's OOXML Signatures

Simon Rohlmann
Ruhr University Bochum

Vladislav Mladenov
Ruhr University Bochum

Christian Mainka
Ruhr University Bochum



Daniel Hirschberger
Ruhr University Bochum

Jörg Schwenk
Ruhr University Bochum

OOXML

Abstract

Microsoft Office is one of the most widely used applications for office documents. For documents of prime importance, such as contracts and invoices, the content can be signed to guarantee authenticity and integrity. Since 2019, security researchers have uncovered attacks against the integrity protection in other office standards like PDF and ODF. Since Microsoft Office documents rely on different specifications and processing rules, the existing attacks are not applicable.

1 Introduction

Microsoft Office is one of the most important tools to manage word documents, presentations, and spreadsheets. For Office 365 alone, there were nearly 300 million paying users worldwide in 2021 [1]. Starting with Office 2007, all documents by default are stored as *Office Open XML* documents (OOXML [2]).

OOXML Document Signatures. Similar to competing office formats like PDF and ODF, Microsoft offers digital signatures to protect their electronic documents, for instance, Word, Excel, and Powerpoint.

Agenda



Digitally Signed PDFs



Core Issues



Beyond PDF Signatures

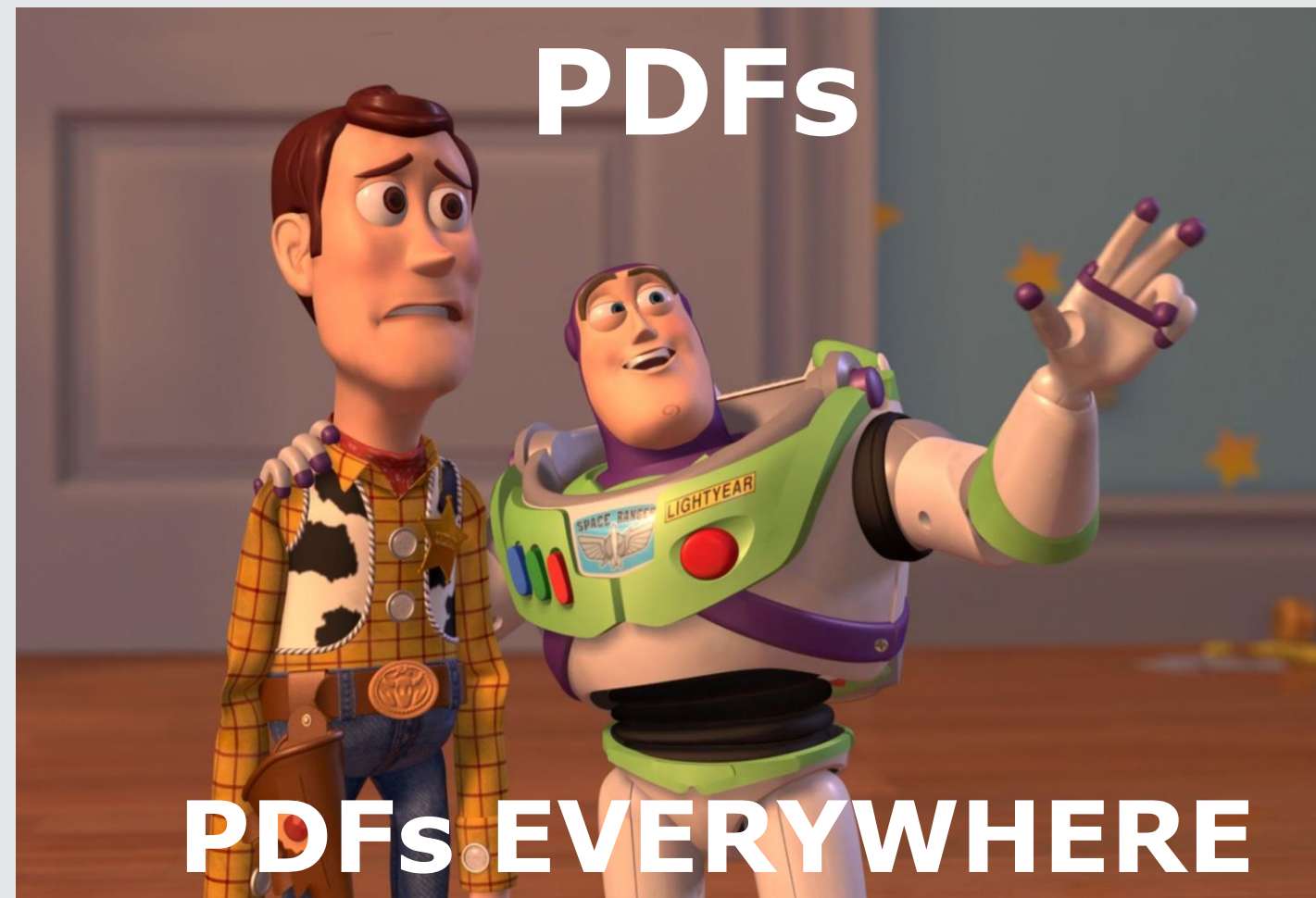


Lessons Learned

Lessons Learned for *Researchers*



„Experienced Standards“ + Crypto = Interesting



Lessons Learned for *Application Developers*



Usable Security



Vladislav Mladenov

Valid

5/25/2018 10:03 AM

Signature Information

Reason: Testing

Location: Los Angeles, CA

Certificate Information

Issuer: Vladislav Mladenov

Valid from: 11/6/2017 1:51 PM

Valid to: 11/4/2027 1:51 PM



Vladislav Mladenov

Valid, but document has been updated

5/25/2018 10:03 AM

Signature Information

Reason: Testing

Location: Los Angeles, CA

Certificate Information

Issuer: Vladislav Mladenov

Valid from: 11/6/2017 1:51 PM

Valid to: 11/4/2027 1:51 PM



Vladislav Mladenov

Valid, but document has been updated

8/9/2018 9:21 AM

Signature Information

Reason: Security

Location: Bochum

Certificate Information

Issuer: Vladislav Mladenov

Valid from: 11/6/2017 1:51 PM

Valid to: 11/4/2027 1:51 PM

Which PDF is valid?

Lessons Learned for *Specification Developers*



Publish Best Current Practices

Internet Engineering Task Force (IETF)
Request for Comments: 7525
BCP: 195
Category: Best Current Practice
ISSN: 2070-1721

Y. Sheffer
Intuit
R. Holz
NICTA
P. Saint-Andre

Recommendations for S
and Datagra

Web Authorization Protocol
Internet-Draft
Intended status: Best Current Practice
Expires: 19 June 2022

T. Lodderstedt
yes.com
J. Bradley
Yubico
A. Labunets
Independent Researcher
D. Fett
ves.com
2021

Web of Things (WoT) Security Best Practices

W3C Editor's Draft 11 April 2022



Q&A Session



More Info

- <https://www.pdf-insecurity.org/>
- Up-to-date research results
- Exploits
- Countermeasures

