iSECpartners
part of nccgroup

Bugged Files

Is Your Document Telling on You?

Daniel Crowley, Damon Smith

Who are we?

iSECpartners
part of nccgroup

- Damon Smith

- Daniel Crowley

What is this talk about?

iSECpartners part of nccgroup

Files that trigger outbound traffic when parsed

Without being an executable format
Regardless of format complexity
Without the use of exploits

…and the implications of all that

Why is this important?

iSECpartners part of nccgroup

- Privacy
  - DRM
  - DLP
  - De-anonymization
- Security
  - NTLM credential capture/relay
  - CSRF
- "It's a feature, not a bug"

Demonstration

- RTF
- WMV

What formats are already known to allow this?

iSECpartners part of nccgroup

- Office formats
  - .docx
  - .pptx
  - .xlsx
- PLS playlists
- Shortcut (.lnk) files
- Desktop.ini files
- HTML

Other NTLM trigger silliness

iSECpartners part of nccgroup

- HTML in IE
- Linked images in emails opened in Outlook!

What did our work focus on?

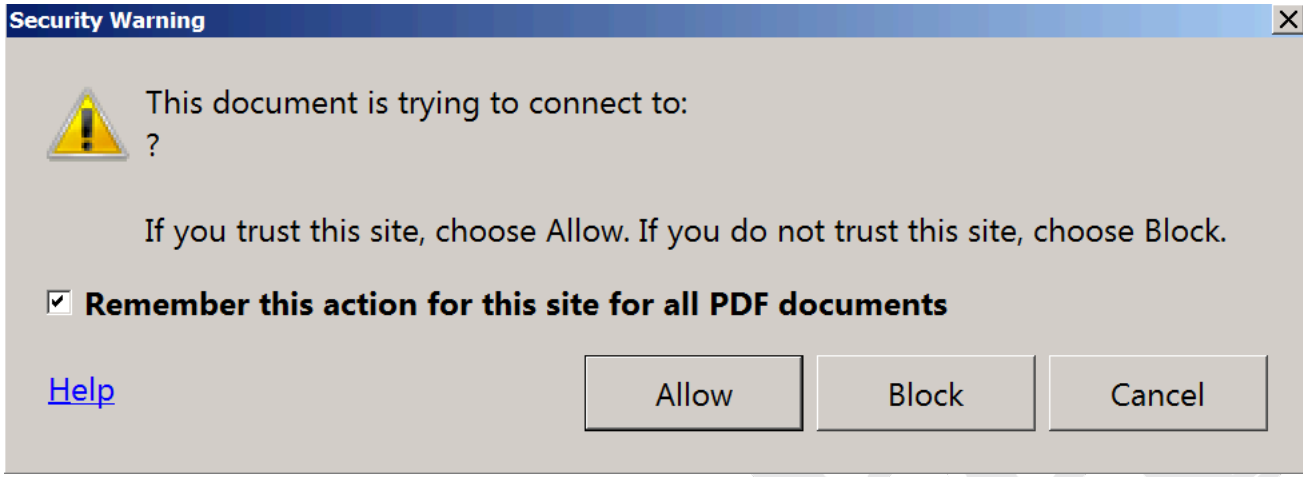
iSECpartners part of nccgroup

- Document formats
- Media formats
- Meeting/scheduling related formats

PDF

iSECpartners part of nccgroup

- Remote image
  - No warning, no NTLM
- App.media.openPlayer()
  - Warning, NTLM possible
- getURL()
  - Warning, NTLM possible



RTF

iSECpartners part of nccgroup

- Linked document on UNC share
  - Warning (ignored), NTLM possible

SVG (Scalable Vector Graphics)

iSECpartners part of nccgroup

- Remote XML stylesheets
- Javascript

M3U / PLS / ASX

iSECpartners part of nccgroup

- All these formats support remote media
  - Even UNC paths…

```
1 #EXTM3U
2
3 #EXTINF:123, Sample artist - Sample title
4 \\10.0.2.2\Test\test.mp3
```

MP3

- ID3 tag
  - LINK frame
  - APIC frame
- Not supported on any major player we tested ☹

ASF (WMA/WMV/ASF)

iSECpartners part of nccgroup

- URLANDEXIT
  - Launches default browser with specified URL
- DRM functionality abuse
- Subtitles
  - Can include arbitrary HTML

TORRENT

iSECpartners part of nccgroup

- HTTP tracker URLs in "announce-list"
  - As many as you want
- URL seeds allowed in "url-list"
  - Clients can implement any URL handler
    - Must support one or both of HTTP & FTP
  - Not universally supported

VCF (vCard format)

iSECpartners part of nccgroup

- Free/Busy URL
  - No warning, NTLM possible
  - Requires specific actions by recipient

ICS (iCalendar format)

iSECpartners part of nccgroup

- VALARM
  - ATTACH parameter is a URL
  - AUDIO and PROCEDURE alarm types
- ICS is the iCalendar format
  - Not even Calendar.app will let you accept PROCEDURE ☹

Delivery methods

iSECpartners part of nccgroup

- Email
- Open file share
- Watering hole
- P2P distribution
- Honeypot

Digital Rights Management

iSECpartners part of nccgroup

- Dystopian future DRM could call home
  - Probably already does in some cases
- Goes beyond deterrence into identification

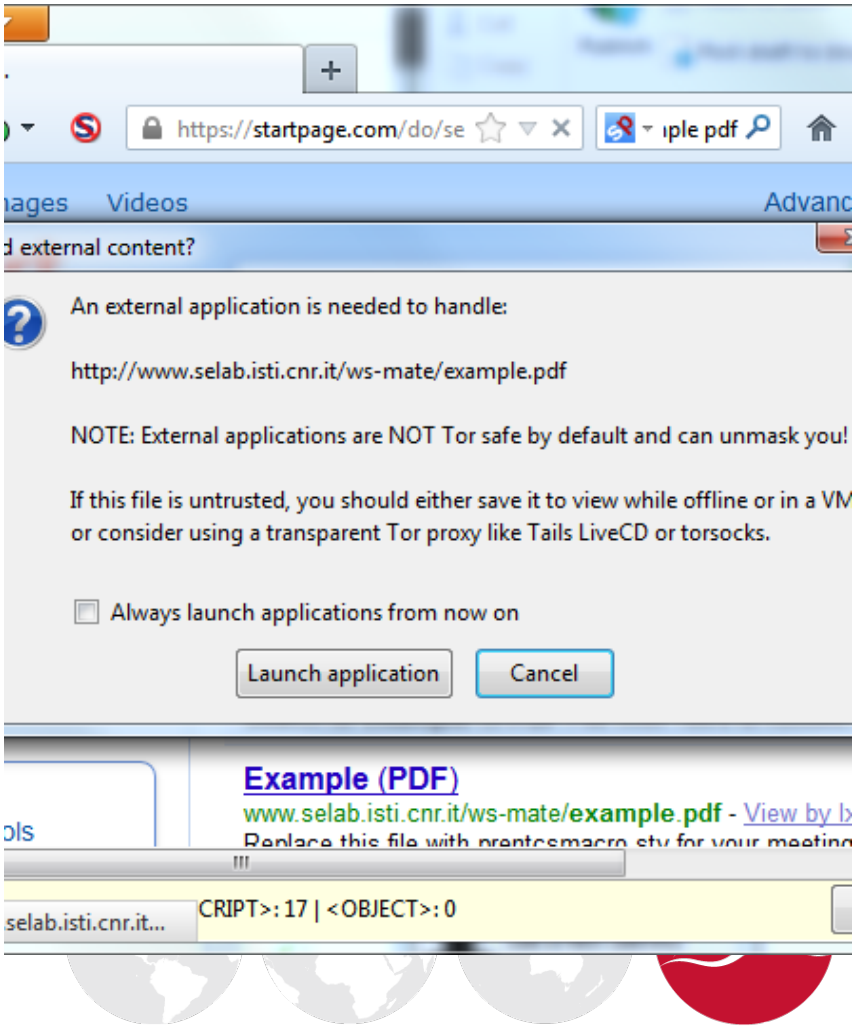
Data Loss Prevention

iSECpartners part of nccgroup

- Imagine being a whistleblower-to-be
  - In a fascist country
- The document you exfiltrate calls home
  - From your work computer
  - From your home computer
  - From your friend's home
  - From your lawyer's office
  - From a journalist's office
- You get disappeared

De-Anonymization

- Tor Browser only routes browser traffic through Tor
  - External programs don't route through Tor
- You don't control that jihad wiki
  - But maybe you can upload a bugged PDF



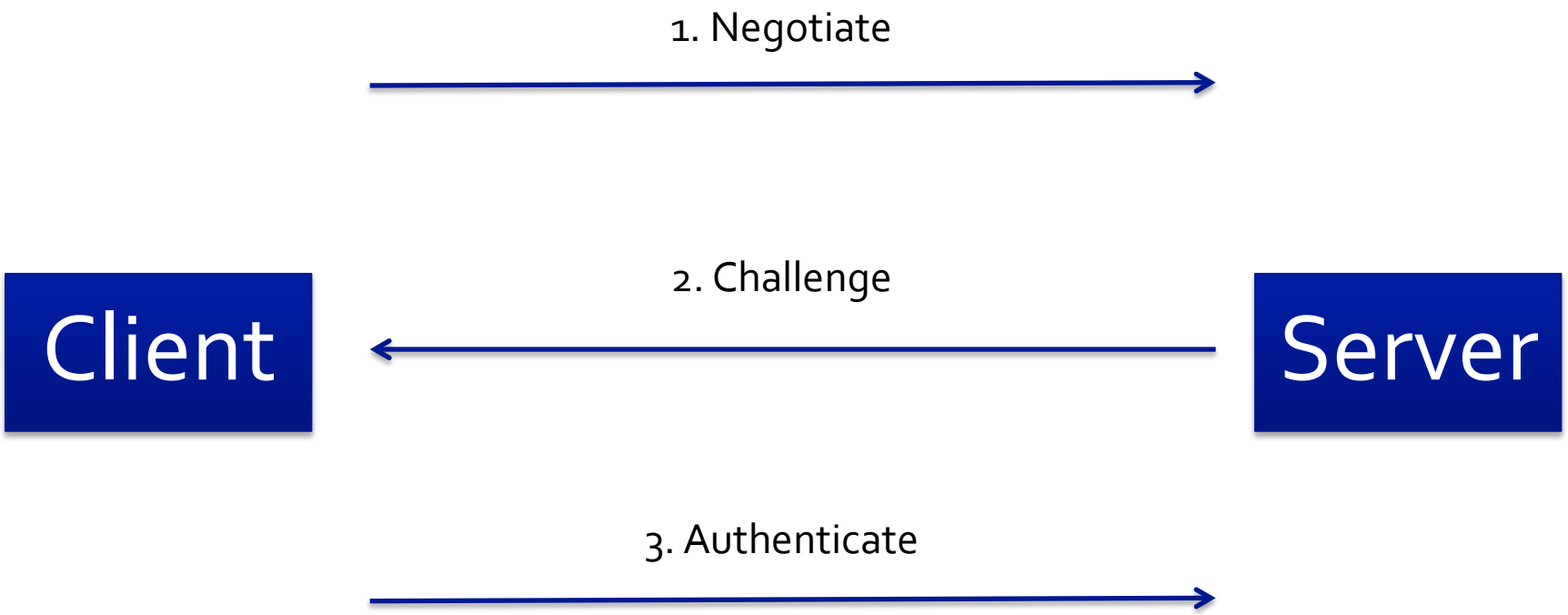
NTLM Credential Capture/Relay

iSECpartners part of nccgroup

- Windows will auto-auth when accessing SMB
- Files can in some cases initiate SMB traffic
  - Embedding remote file:// resources
  - UNC path as file
  - Javascript/other active content
- NTLM auth can be cracked or relayed

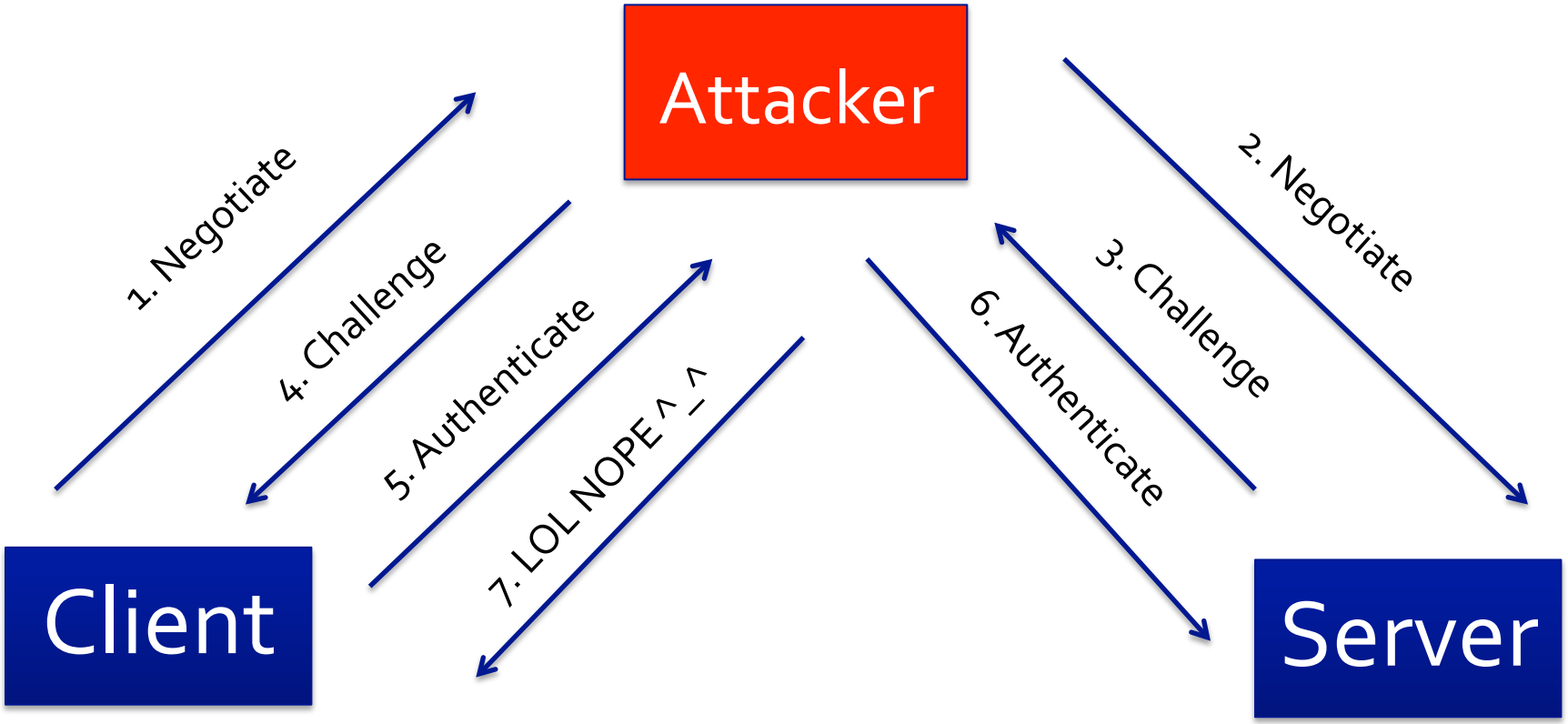
NTLM overview

iSECpartners part of nccgroup



NTLM relay overview

iSECpartners
part of nccgroup



CSRF

iSECpartners part of nccgroup

- Initiating traffic from privileged positions is fun
  - Exploit router vulns
  - Exploit NAS/Printers
  - Exploit IoT devices

Possible Mitigations

iSECpartners part of nccgroup

- AV?
  - Too many formats and variations
  - Possibility of false positives
- Format changes?
  - Too much inertia, too many formats
- Application-level firewalls?
  - Easy for RTF
  - Not so easy for M3U

Possible Mitigations

iSECpartners part of nccgroup

- Warnings?
- Proxychains with strict_chain and bad proxy
  - Doesn't work for some applications
- Egress filtering?
  - Doesn't stop internal connections
  - Might stop legitimate functionality

iSECpartners
part of nccgroup

Questions?

Daniel Crowley, Damon Smith