




black hat[®]
EUROPE 2023
DECEMBER 4-7
EXCEL LONDON / UK

AutoSpill

Zero Effort Credential Stealing from Mobile Password Managers

Ankit Gangwal, Shubham Singh, Abhijeet Srivastava
IIT Hyderabad, IN

Introduction



Introduction

Internet ~~Information~~ Age

Connect the world



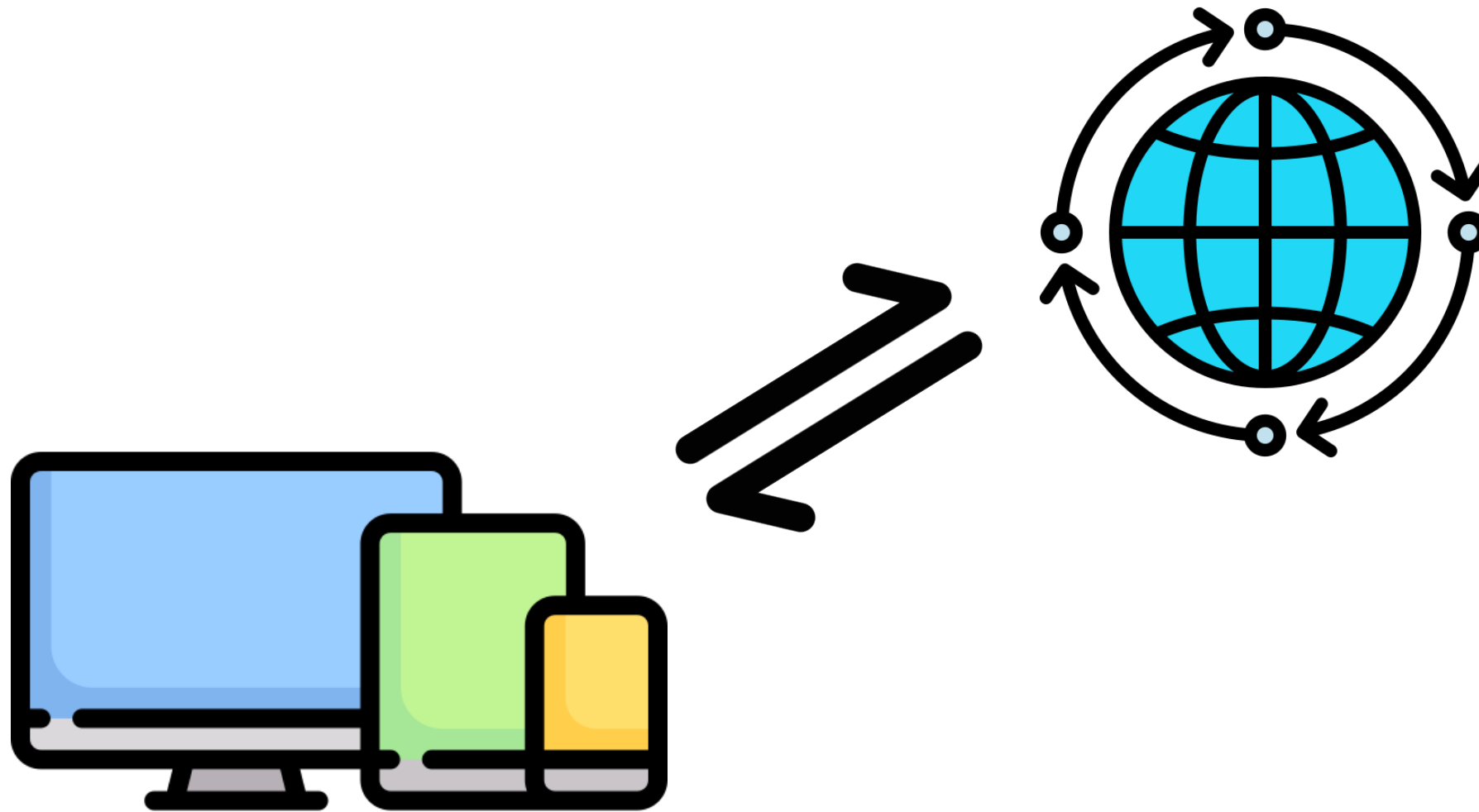
Introduction

Become the world



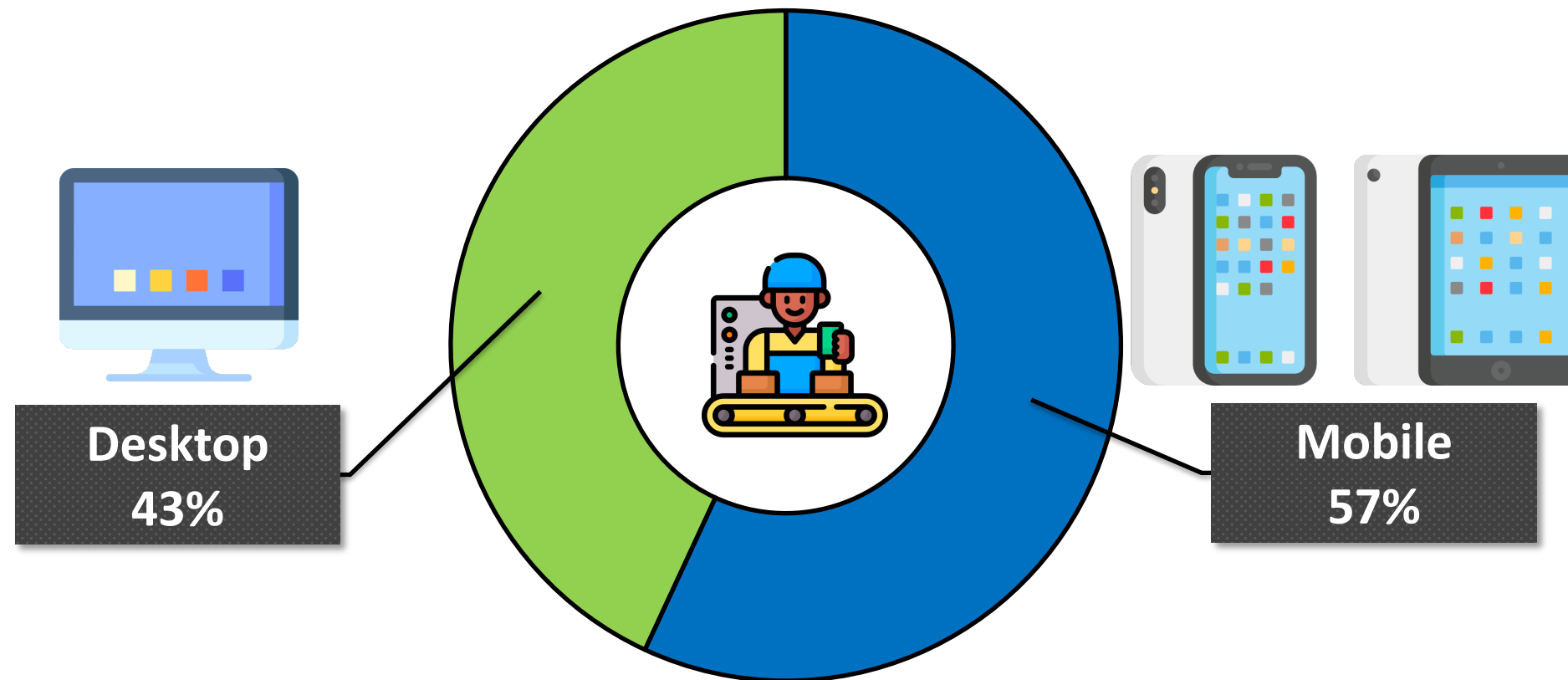
Introduction

Connecting to the Internet



Different devices

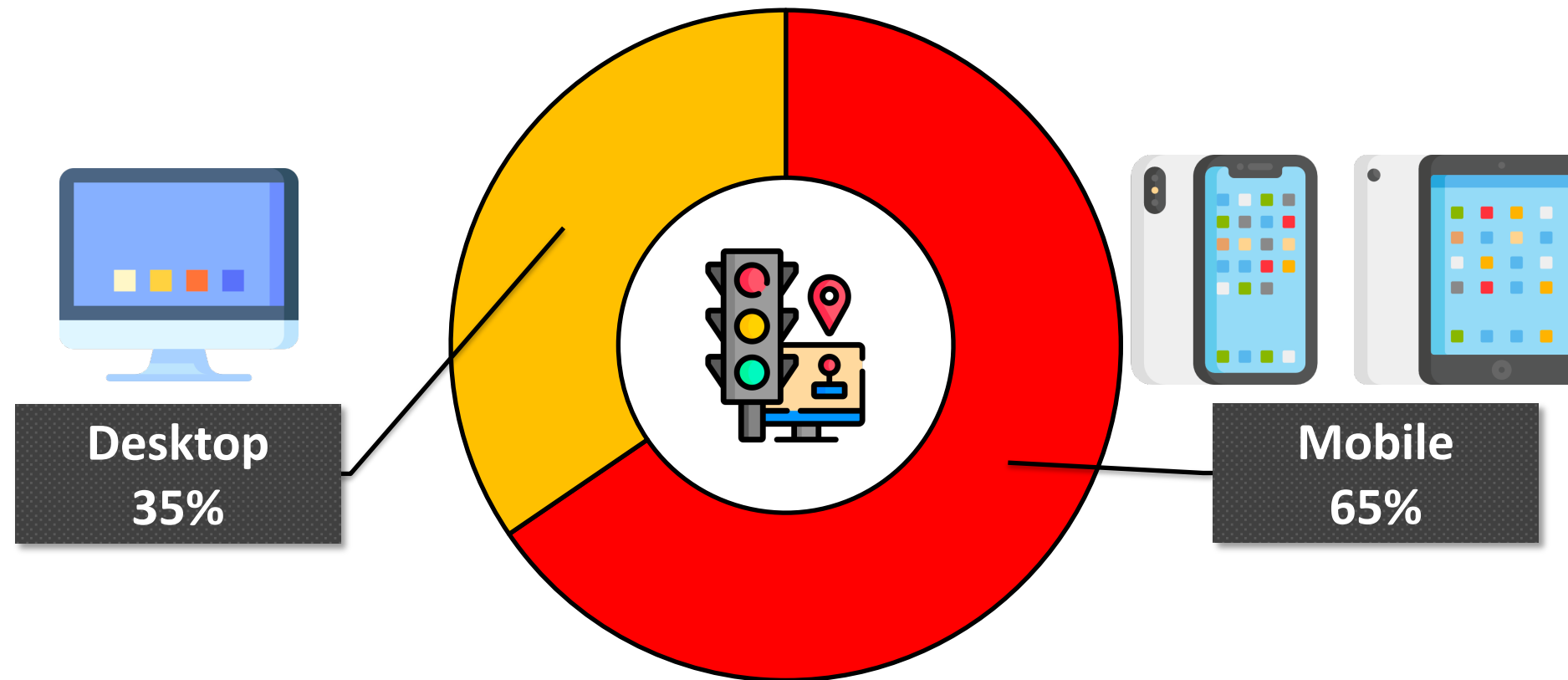
Desktop vs. mobile



Worldwide device market share - 2023

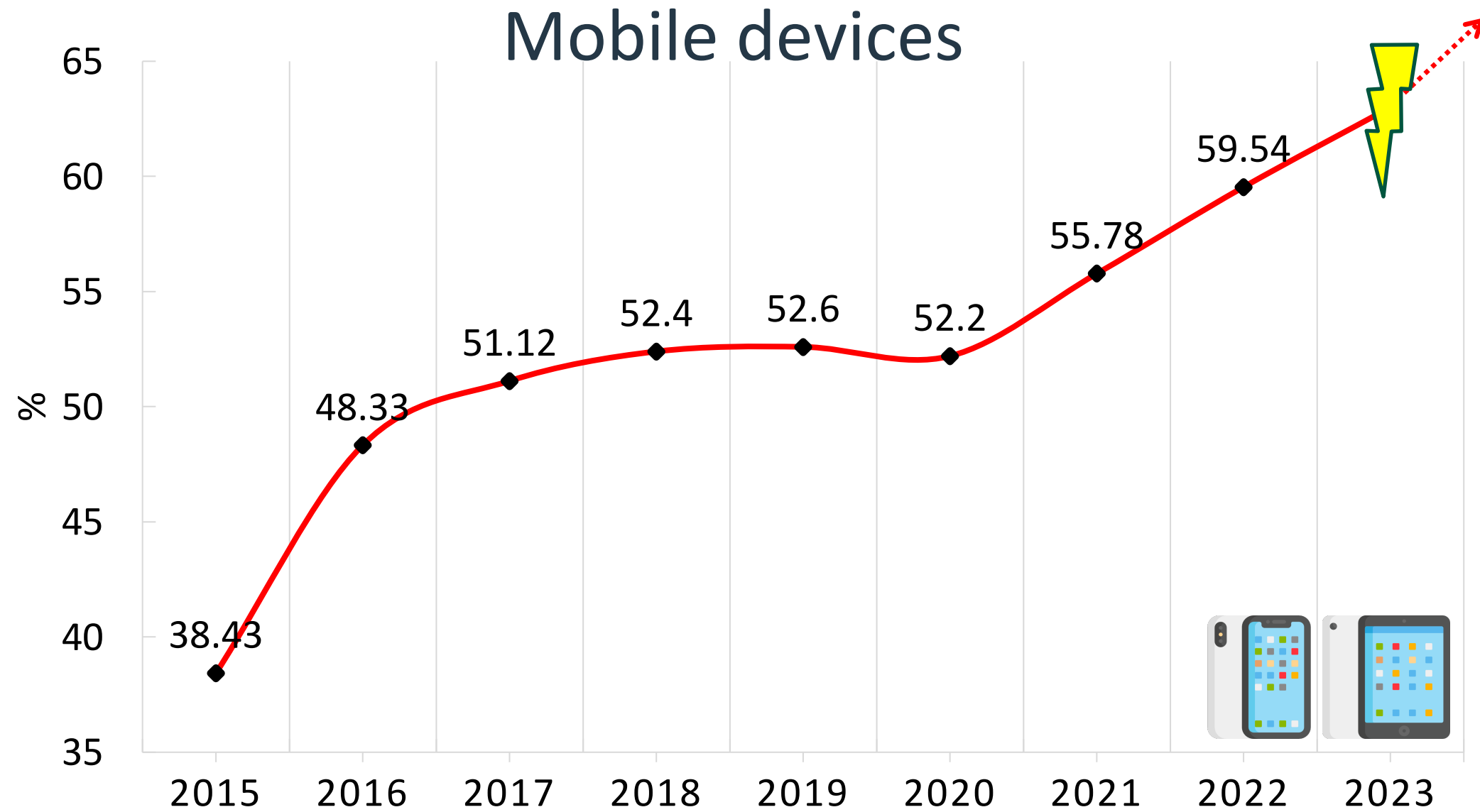
Introduction

Desktop vs. mobile



Worldwide Internet traffic share - Q1 2023

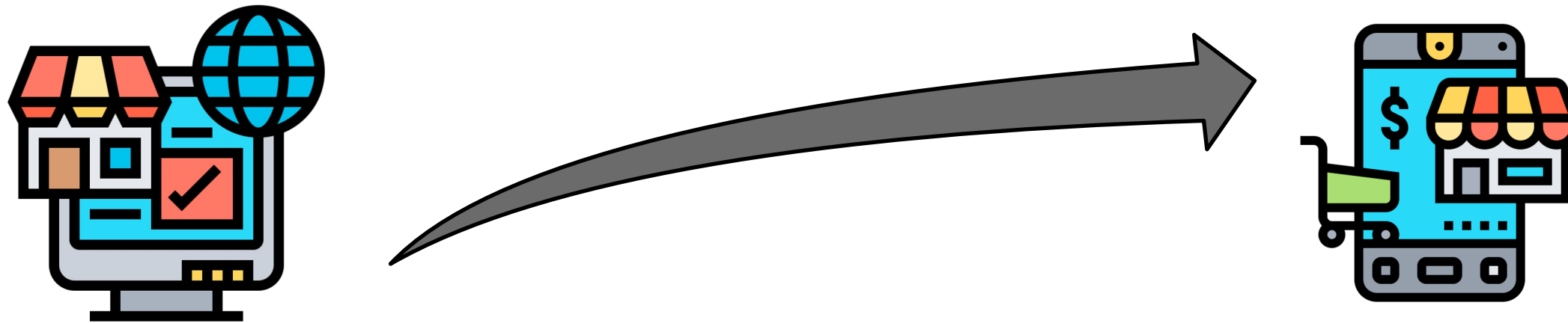
Introduction



Worldwide mobile Internet traffic trend



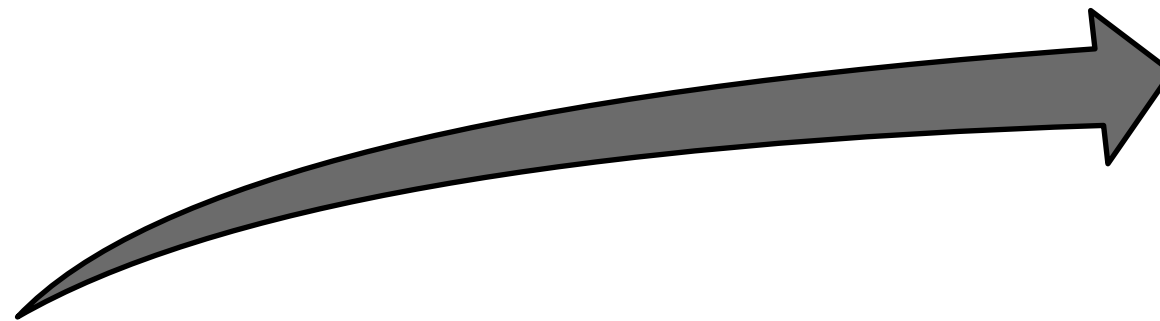
The big shift - Oh my!



Introduction

The big shift - Oh my!

LOG IN



Introduction

The big shift - Oh my!



LOG IN



Introduction

The big shift - Oh my!



The big shift - Oh my!



☰ CBS NEWS 🔍

U.S. >

Common passwords like "123456" and "admin" take less than a second to crack, research shows

BY CAITLIN O'KANE
NOVEMBER 15, 2023 / 1:28 PM EST / CBS NEWS

f t

Forbes

INNOVATION • CYBERSECURITY

These Are The World's Most Hacked Passwords -- Is Yours On The List?

Kate O'Flaherty Senior Contributor ©
Cybersecurity and privacy journalist

Follow

Apr 21, 2019, 12:01am EDT

☰ The New York Times

'Password,' 'Monkey' and the Other Terrible Passwords We Choose

📺 Share full article ↗ 📖

This year's worst passwords, according to one creator of security applications, include "starwars," "iloveyou," "monkey," "hello," "freedom," "qazwsx" and "trustno1." Damian Dovarganes/Associated Press

By Niraj Chokshi

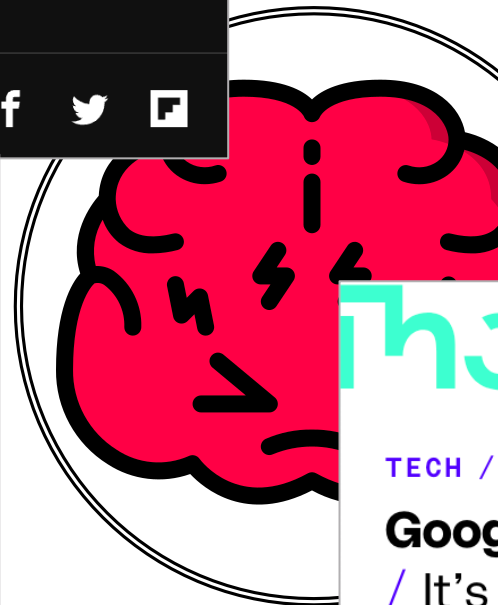
Menu +

TECH / GOOGLE / SECURITY

Google is on a mission to stop you from reusing passwords / It's adding its Password Checkup tool to the Security Checkup dashboard

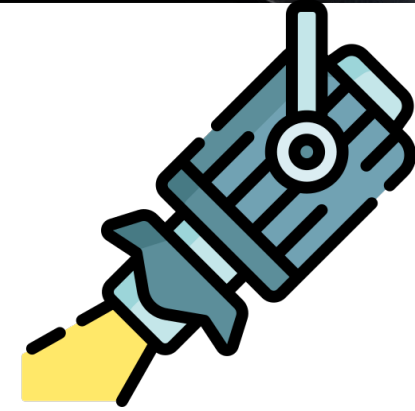
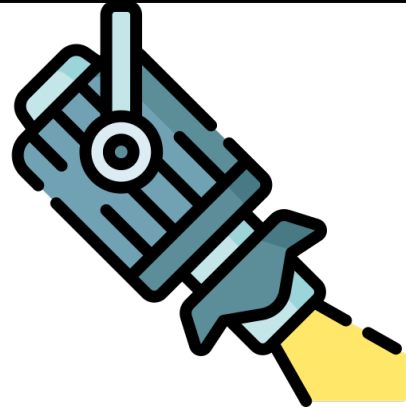
By Jay Peters, a news editor who writes about technology, video games, and virtual worlds. He's submitted several accepted emoji proposals to the Unicode Consortium.

Jun 23, 2020, 5:30 PM GMT+5:30 | 0 Comments / 0 New

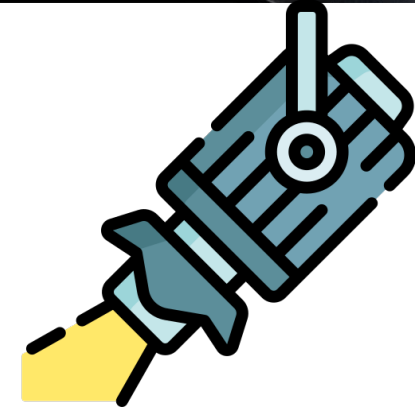
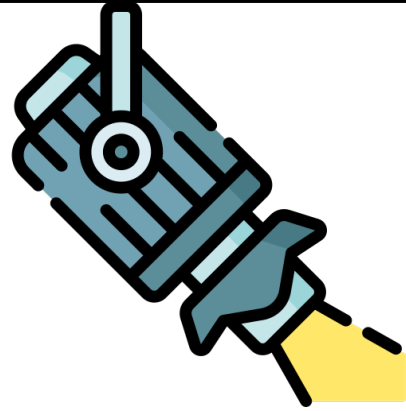


The Verge

Introduction



Introduction



Cancel

Log in with

f Facebook


g+ Google

Username or Email

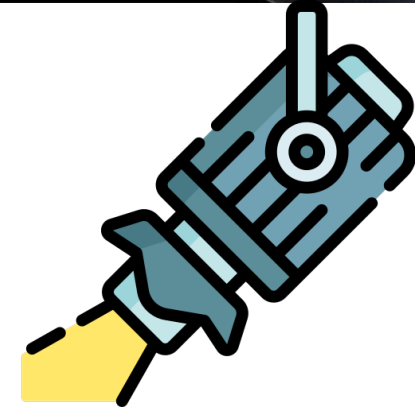
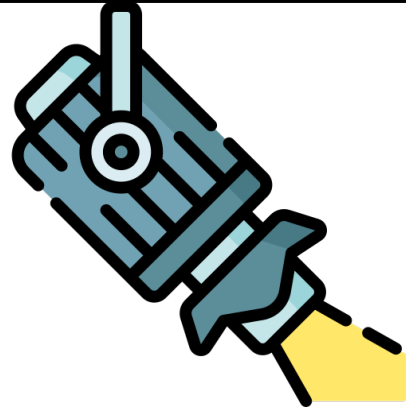
Password

Log in

Forgot your password?



Introduction



Cancel

Log in with

f Facebook


g+ Google

Username or Email

Password

Log in

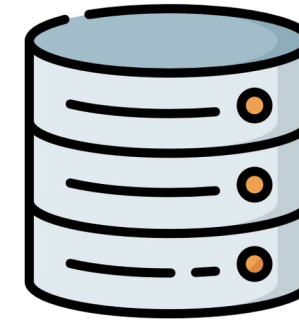
Forgot your password?



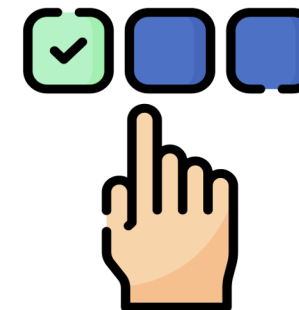


Password Managers (PMs)

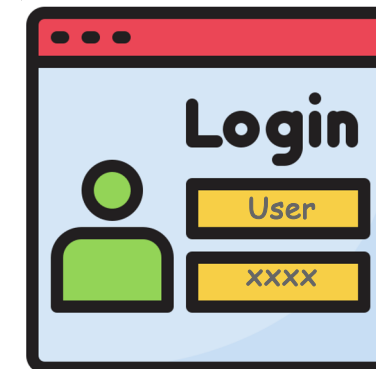
Store & manage



Choose stronger passwords



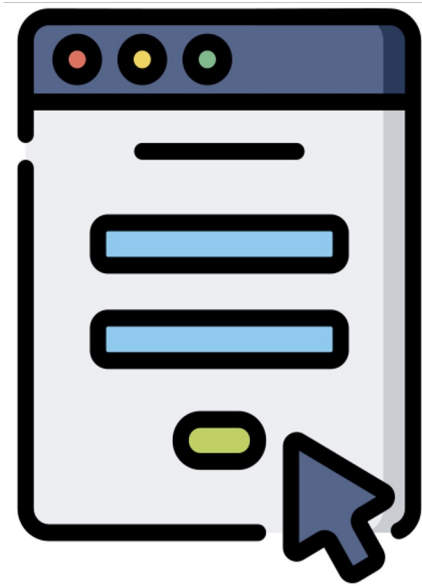
Automatically fill (autofill)



Background

PMs are becoming increasingly common

Computers as well as mobile devices (e.g., smartphones) [1, 2]



[1] Sean Oesch, Anuj Gautam, and Scott Ruoti, “The Emperor’s New Autofill Framework: A Security Analysis of Autofill on iOS and Android,” In Annual Computer Security Applications Conference. 996-1010, 2021.

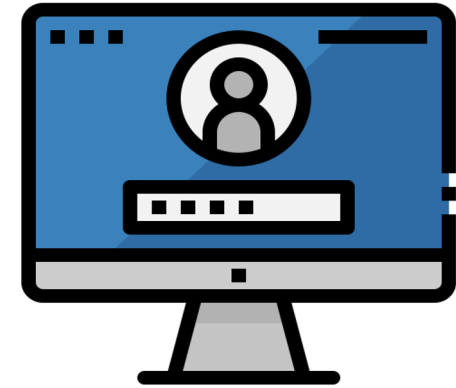
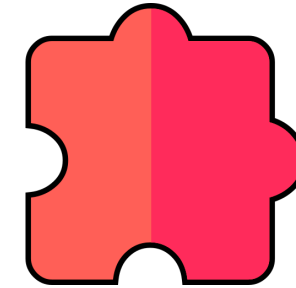
[2] Sean Oesch and Scott Ruoti, “That was then, this is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-based Password Managers,” In USENIX Security Symposium. 2165-2182, 2020.

Background



PMs on computers

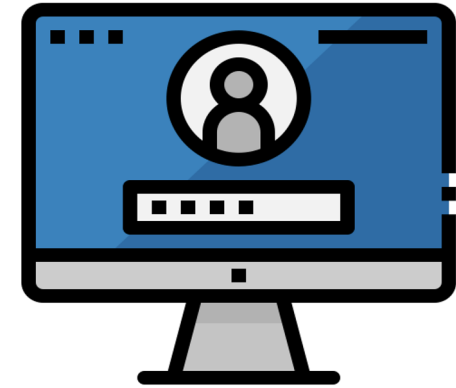
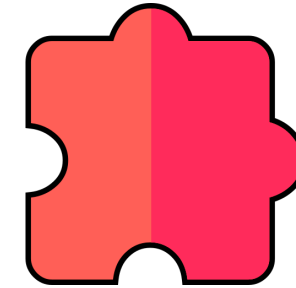
Generally, implemented as browser extension



Background

PMs on computers

Generally, implemented as browser extension



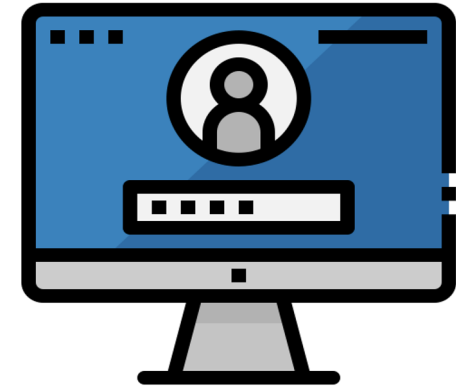
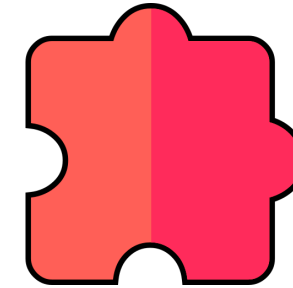
Handles everything

Storing, rendering, prompting, autofilling

Background

PMs on computers

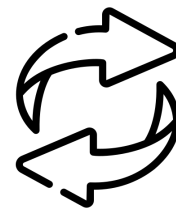
Generally, implemented as browser extension



Handles everything

Storing, rendering, prompting, autofilling

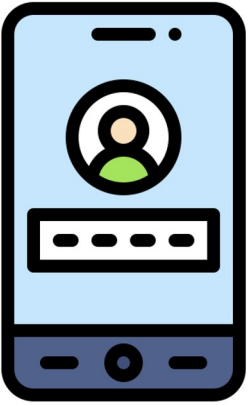
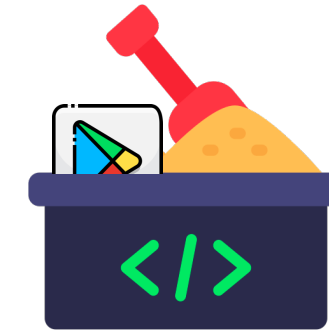
Autofill ceremony involves only two parties



Background

PMs on mobile OSes (e.g., Android)

System-wide autofill frameworks & sandboxing

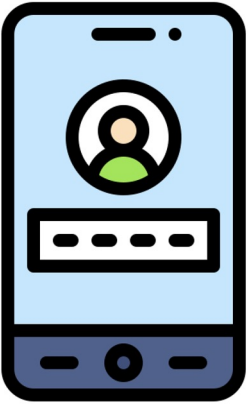
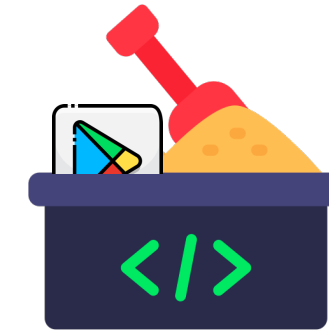


Autofill ceremony involves at least three parties

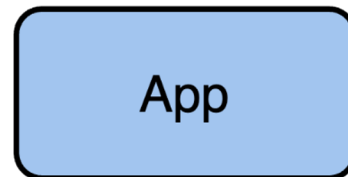
Background

PMs on mobile OSes (e.g., Android)

System-wide autofill frameworks & sandboxing



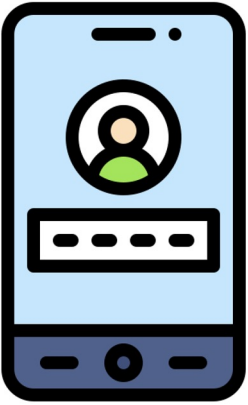
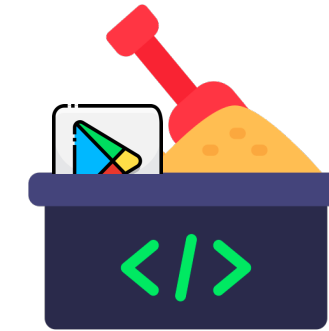
Autofill ceremony involves at least three parties



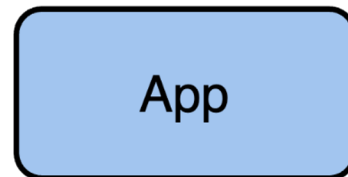
Background

PMs on mobile OSes (e.g., Android)

System-wide autofill frameworks & sandboxing



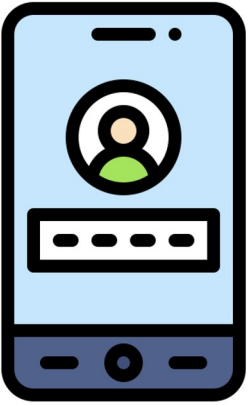
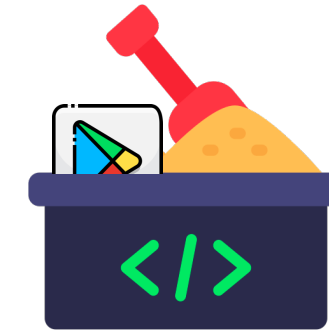
Autofill ceremony involves at least three parties



Background

PMs on mobile OSes (e.g., Android)

System-wide autofill frameworks & sandboxing



Autofill ceremony involves at least three parties

App

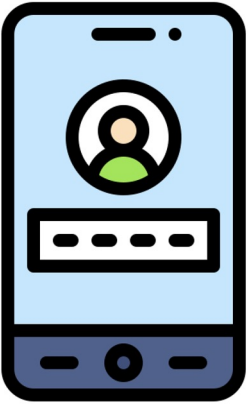
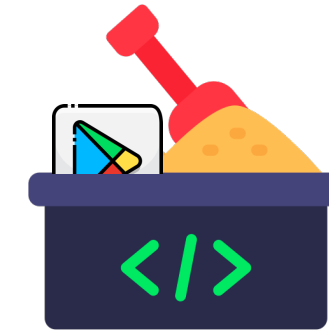
Android

Autofill
Service

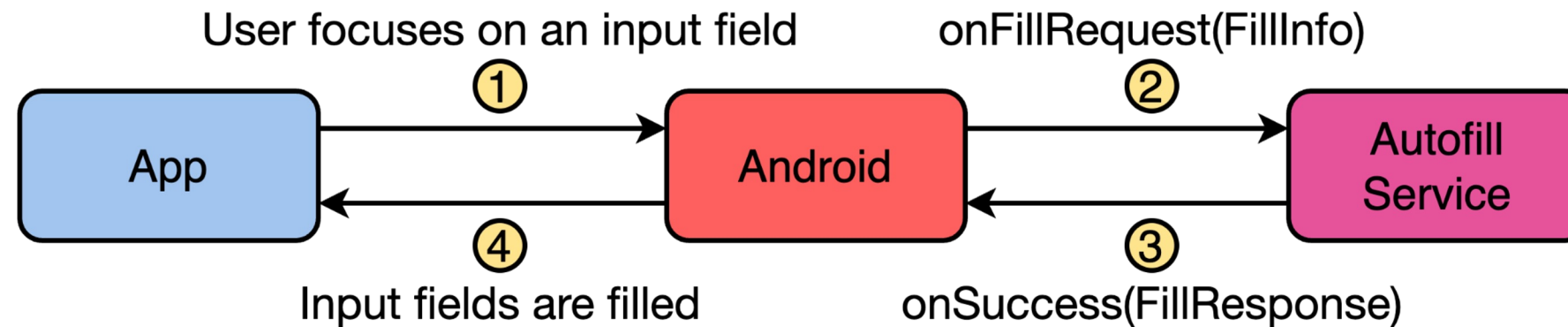
Background

PMs on mobile OSes (e.g., Android)

System-wide autofill frameworks & sandboxing



Autofill ceremony involves at least three parties

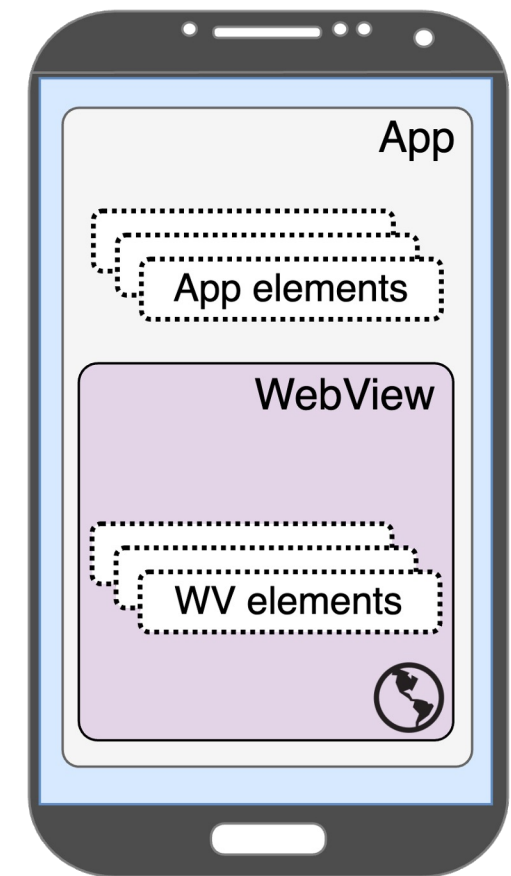


Mobile OSes have developed WebView controls

Act as a minimalistic browser

Empower an app to render web content within itself

Prevents redirection to main browser app

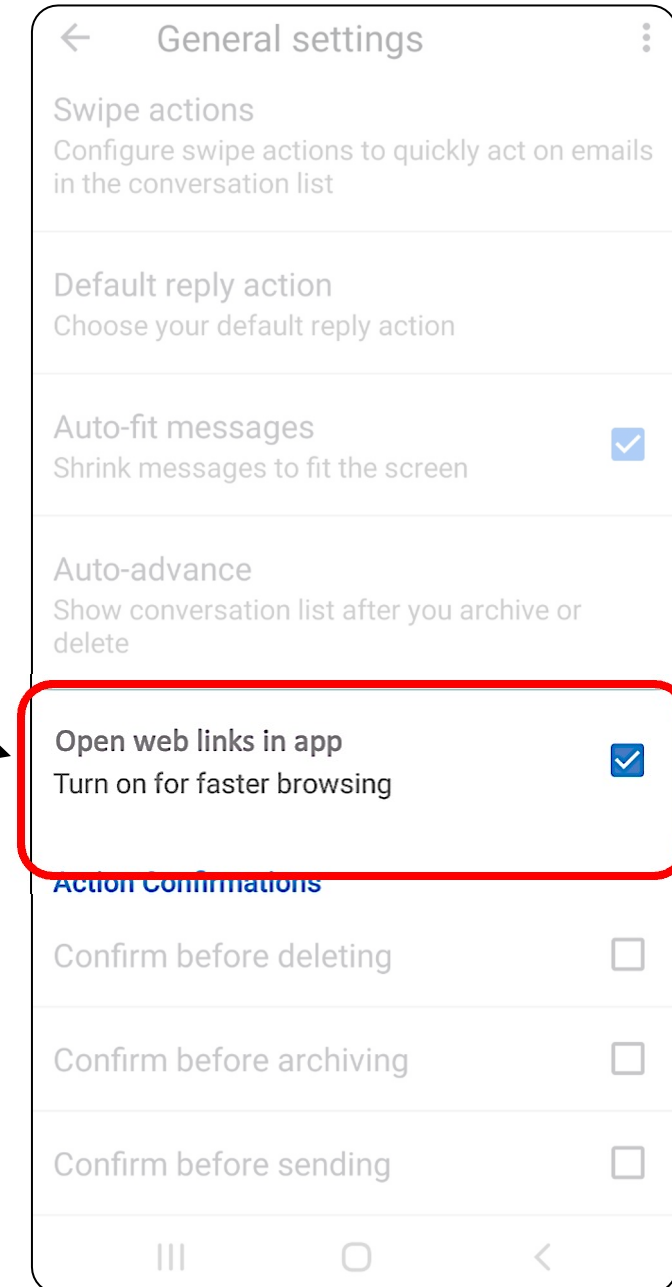


Mobile OSes have developed WebView controls

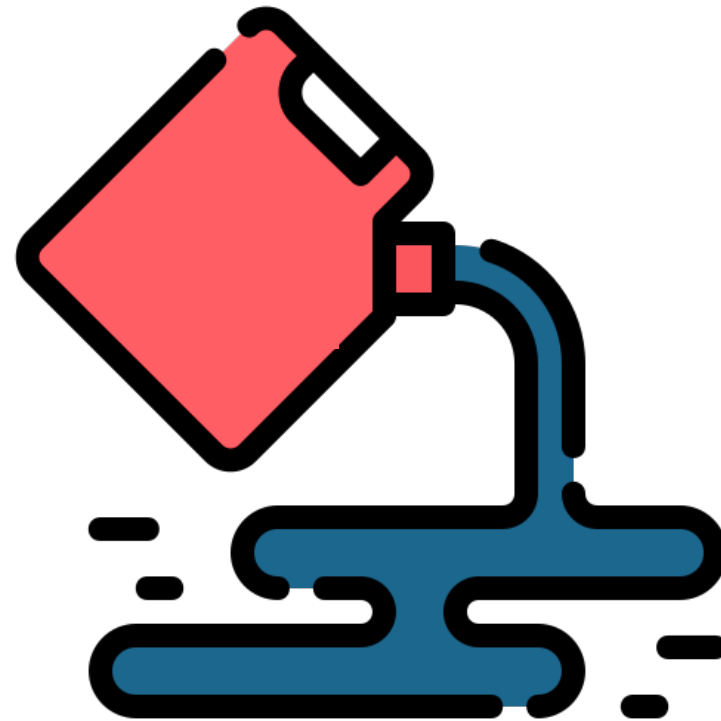
Act as a minimalistic browser

Empower an app to render web content within itself

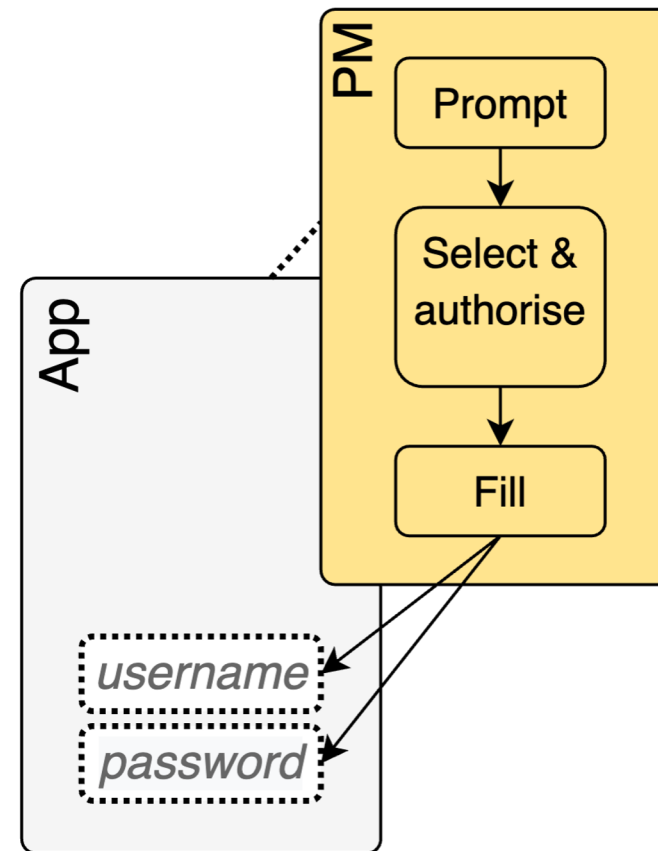
Prevents redirection to main browser app



AutoSpill

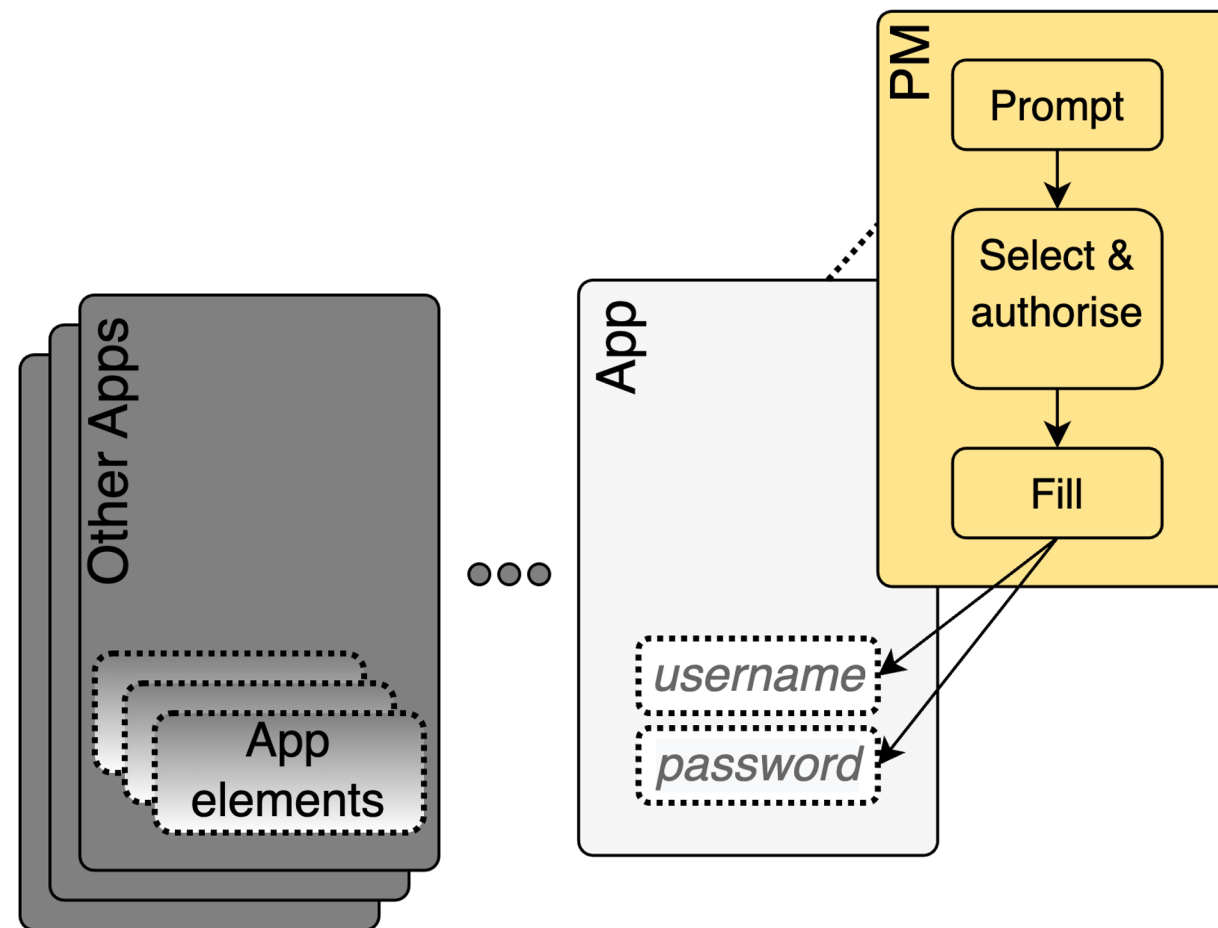


PM is invoked to fill fields in an app



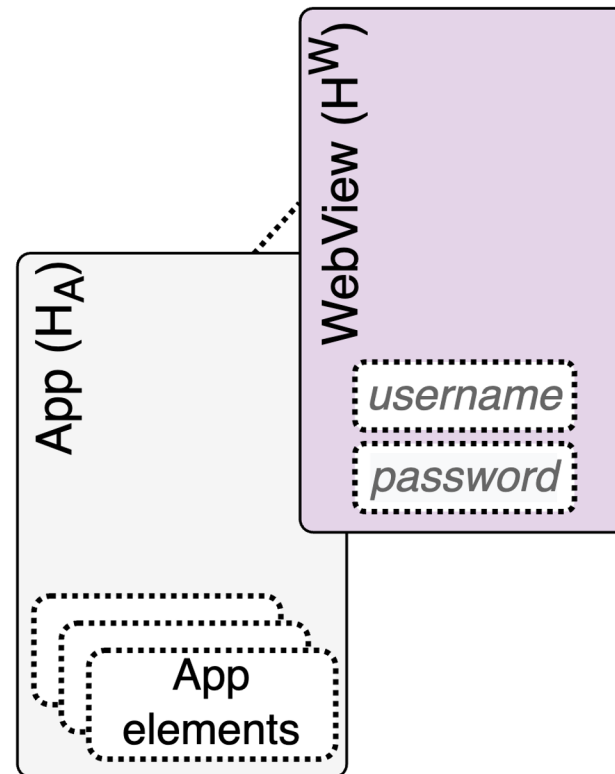


PM is invoked to fill fields in an app

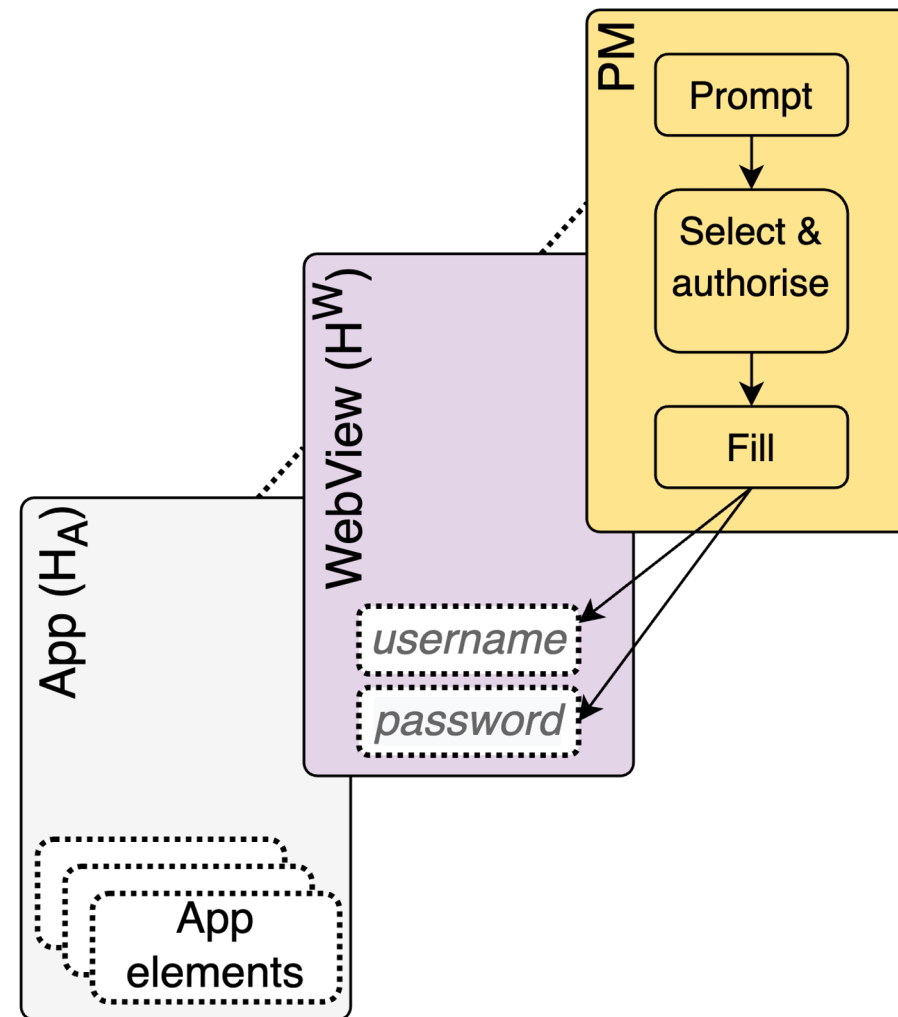




PM is invoked to fill fields in a WebView



PM is invoked to fill fields in a WebView





PM is invoked to fill fields in a WebView

Example 1

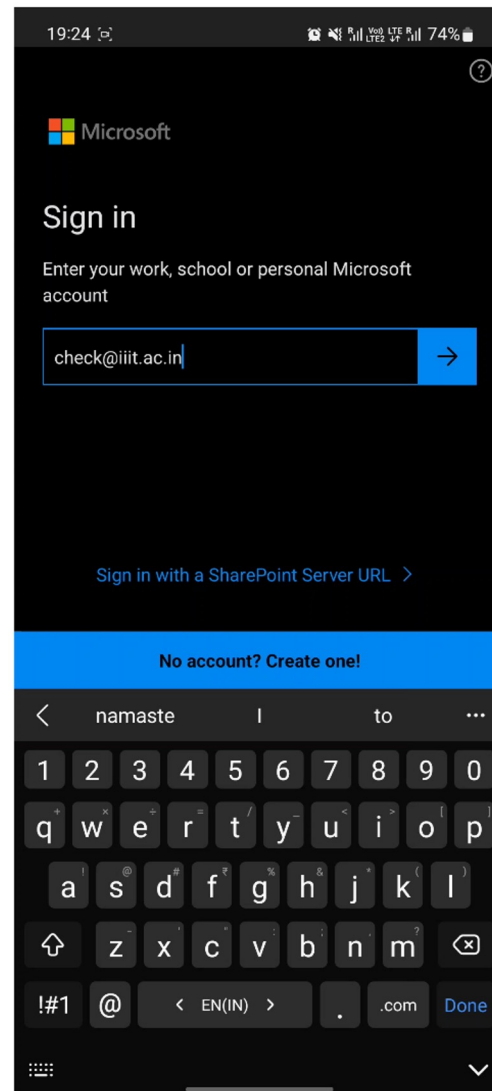


“Login with Apple/Facebook/Google/etc.” buttons



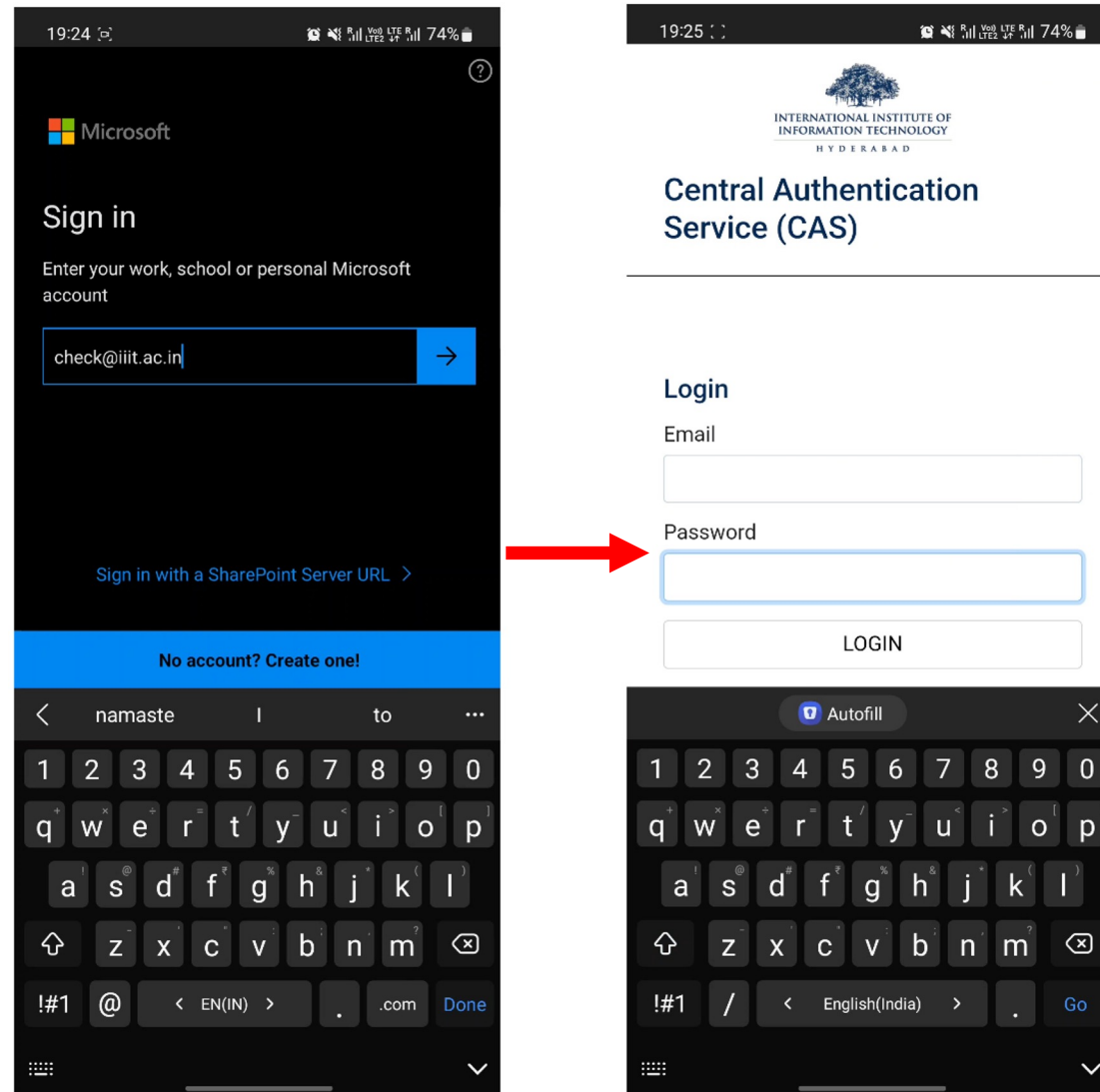
PM is invoked to fill fields in a WebView

Example 2



Logging in OneDrive app, which supports 3rd party authentication

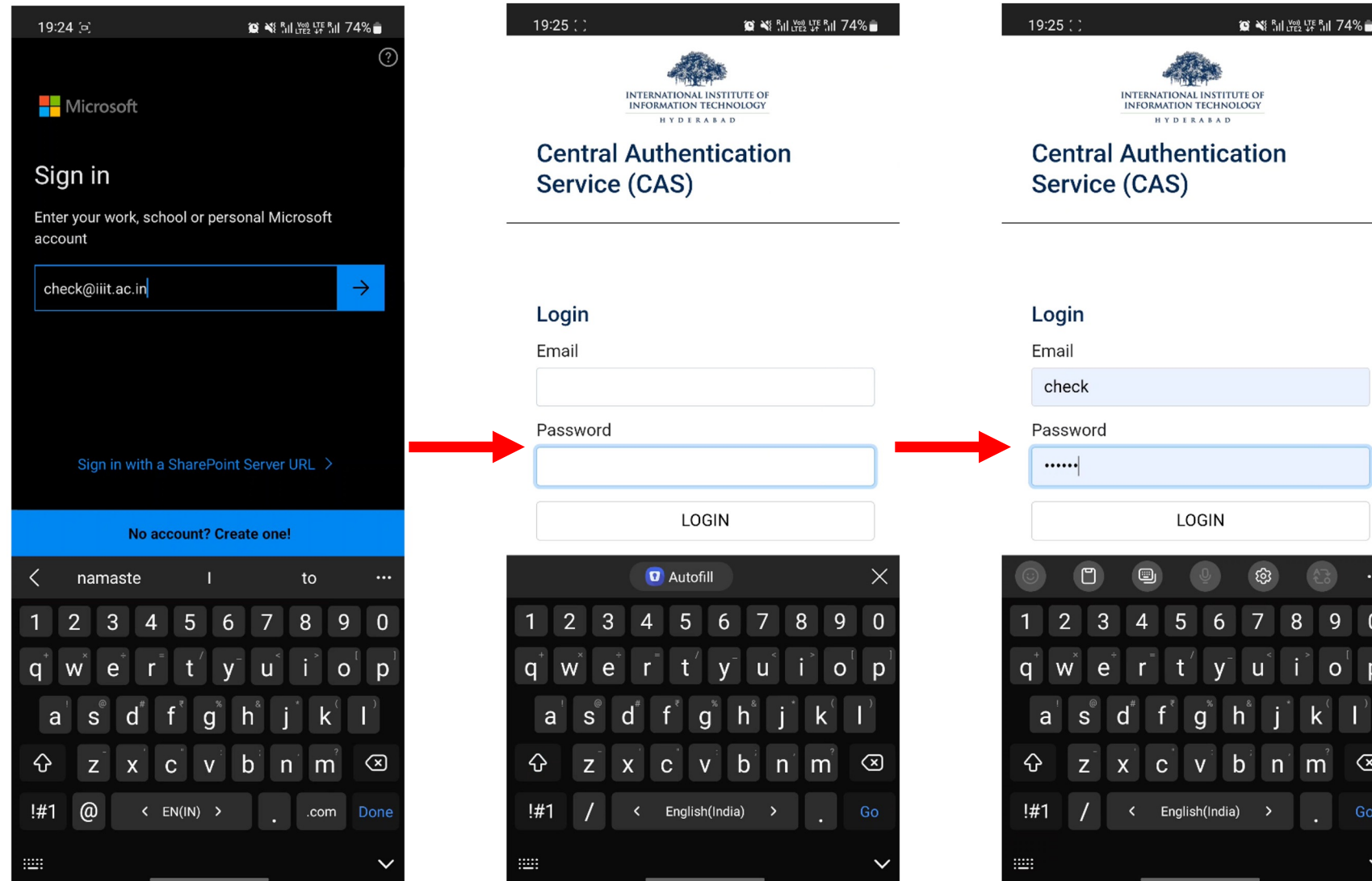
PM is invoked to fill fields in a WebView Example 2



Logging in OneDrive app, which supports 3rd party authentication



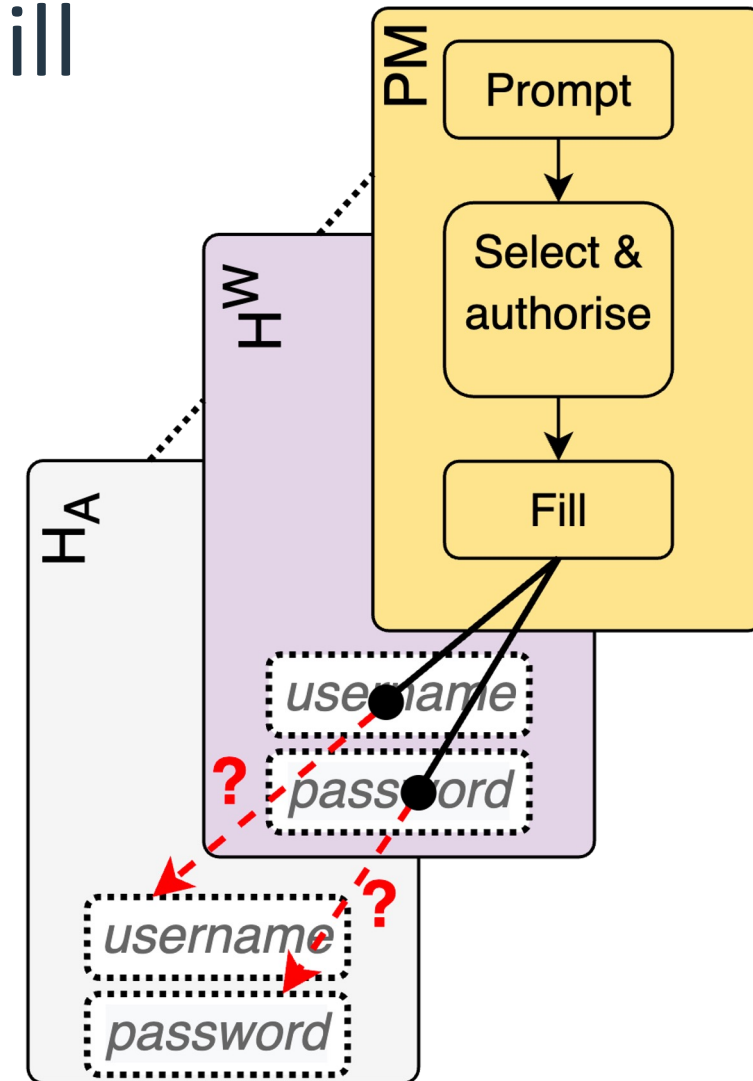
PM is invoked to fill fields in a WebView Example 2



Logging in OneDrive app, which supports 3rd party authentication



Credential leakage from H^W to $H_A = \text{AutoSpill}$

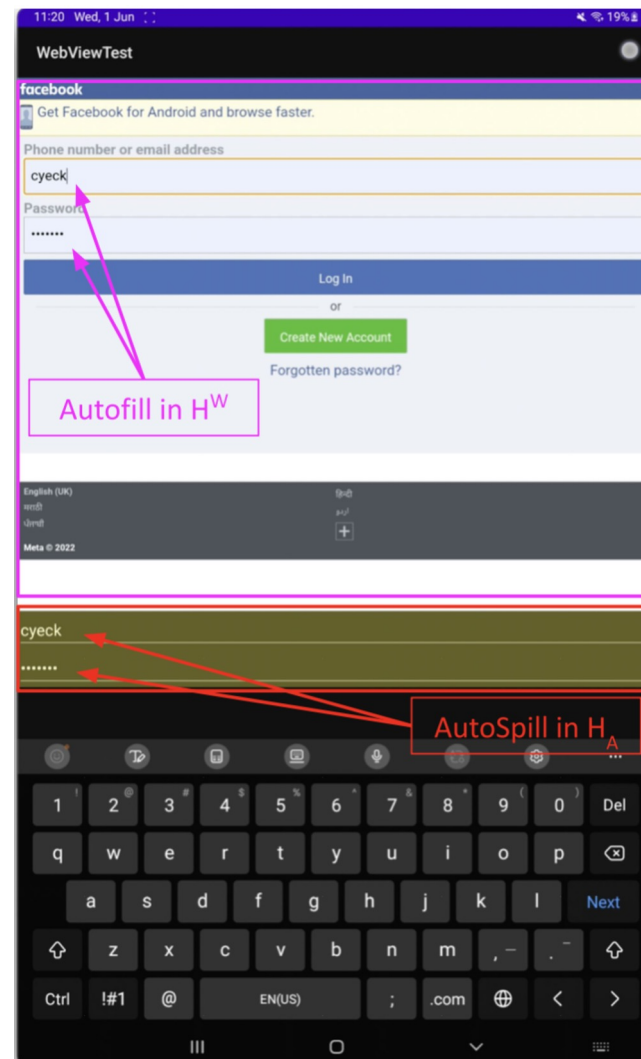


Violation of secure autofill process

Responsibility for leakage is stranded between PM and Android

AutoSpill

Credential leakage from H^W to $H_A = \text{AutoSpill}$



A real-world credential AutoSpill from Facebook page

Biggest **benefit** (rather **risk!**) of AutoSpill

+ **Phishing is not required**

1. Benign app with input fields
2. Invokes H^W
3. Code for processing

+ **No malicious code in app**

Reside on official app store





Created a custom autofill service

Information exchanged during autofill ceremony

App

Android

Autofill
Service



Created a custom autofill service

Information exchanged during autofill ceremony

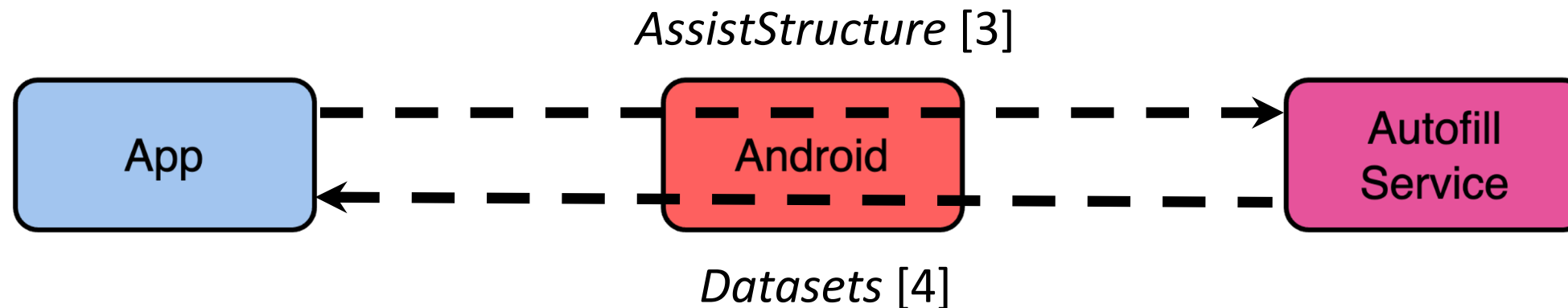
1. Autofill request from Android to autofill service



Created a custom autofill service

Information exchanged during autofill ceremony

- 1. Autofill request from Android to autofill service*
- 2. Processing and response from autofill service*



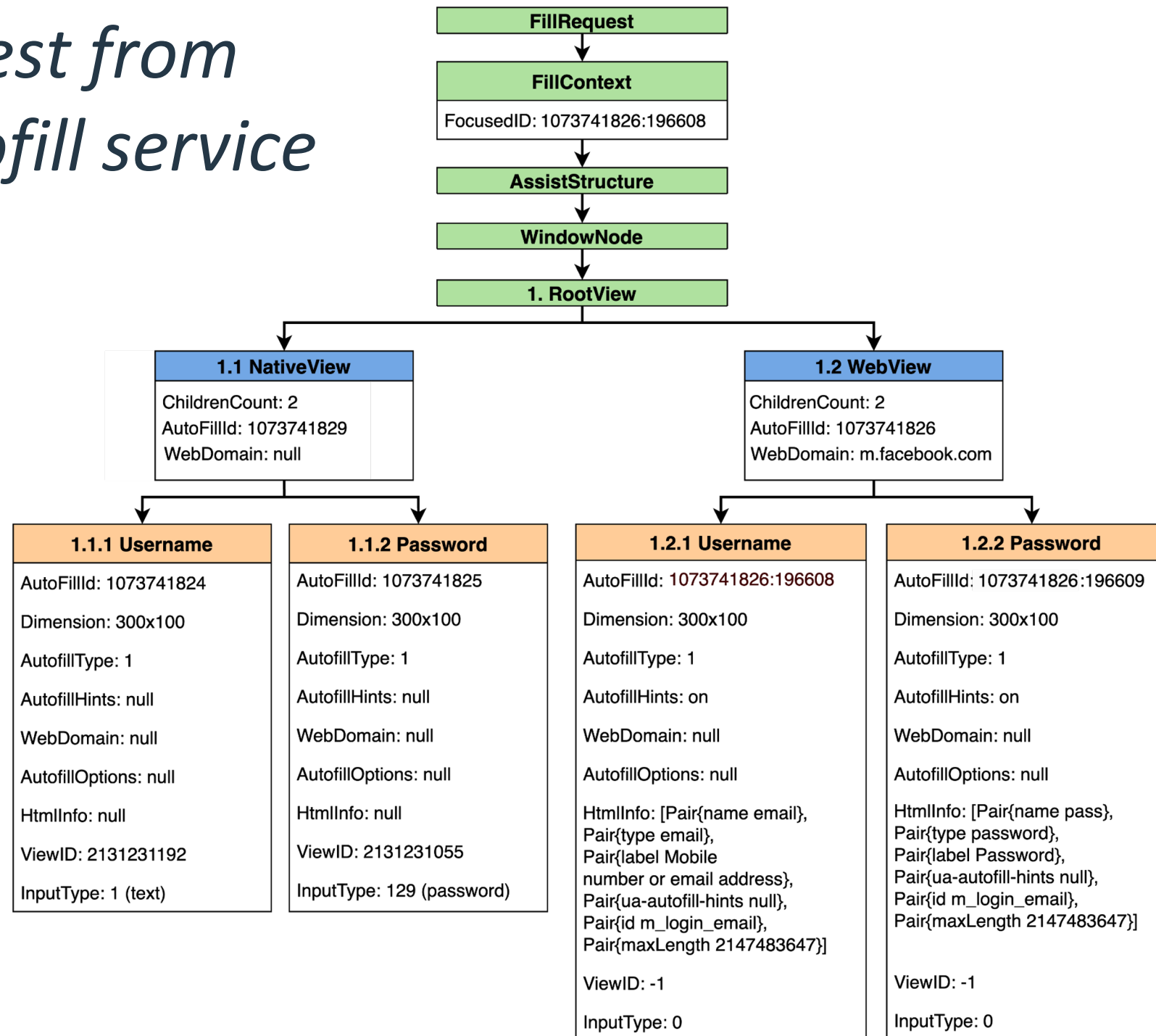
[3] AssistStructure, <https://developer.android.com/reference/android/app/assist/AssistStructure>

[4] Datasets, <https://developer.android.com/reference/android/service/autofill/Dataset>



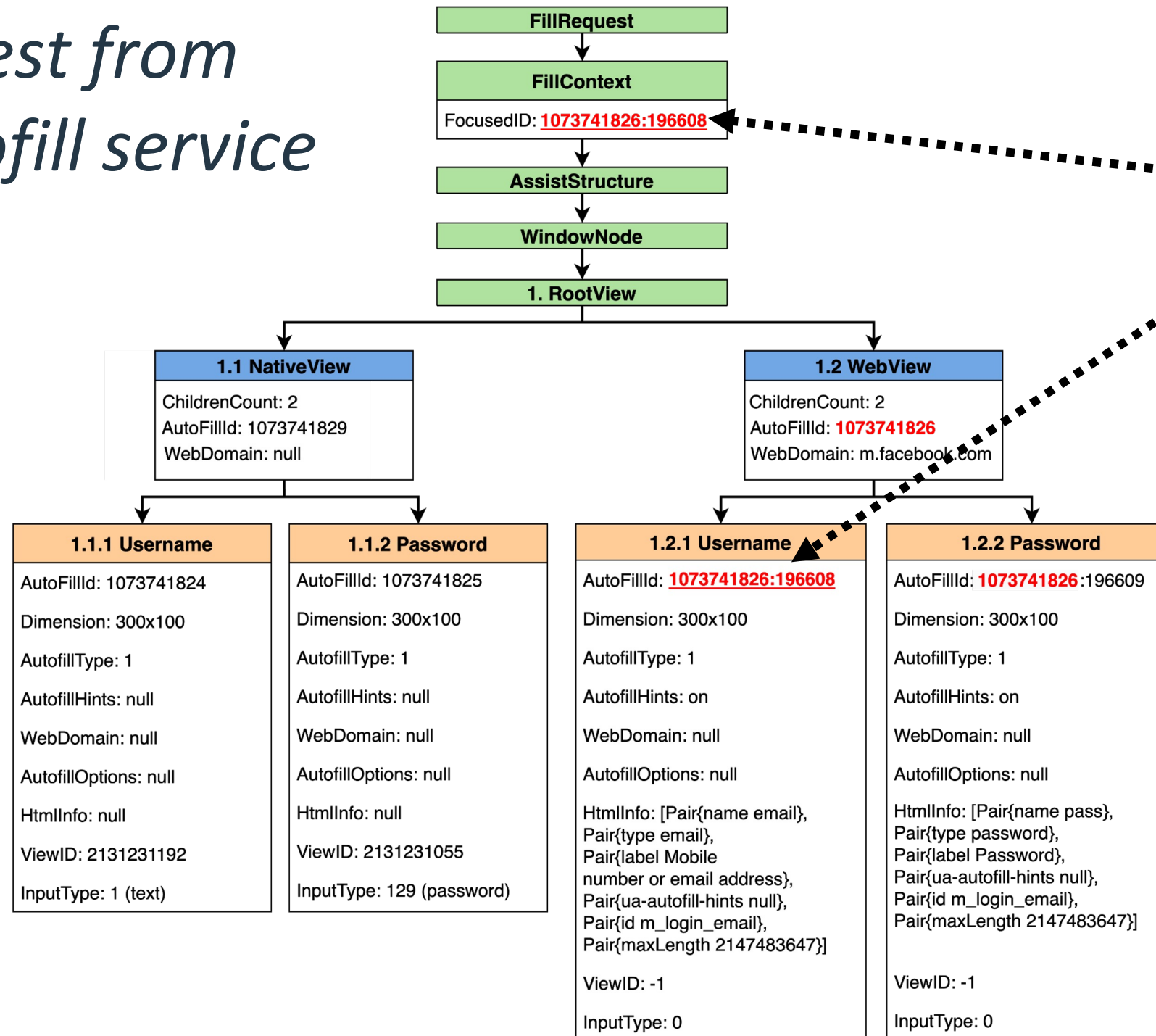
AutoSpill - Investigation

1. Autofill request from Android to autofill service



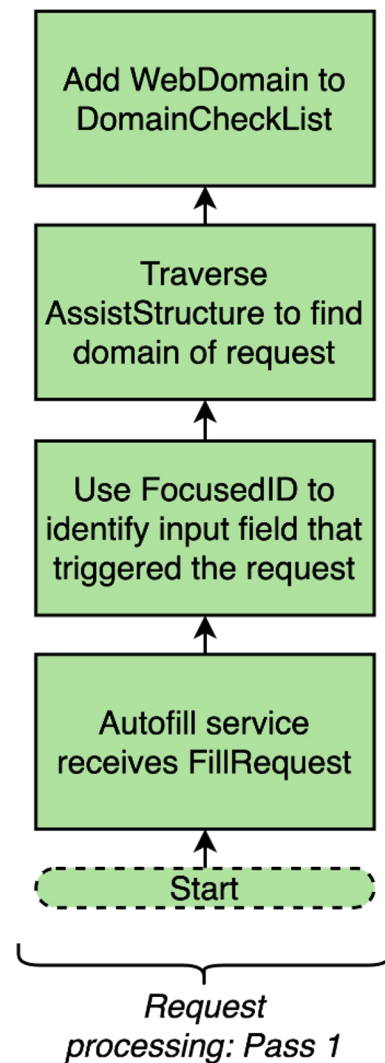
AutoSpill - Investigation

1. Autofill request from Android to autofill service

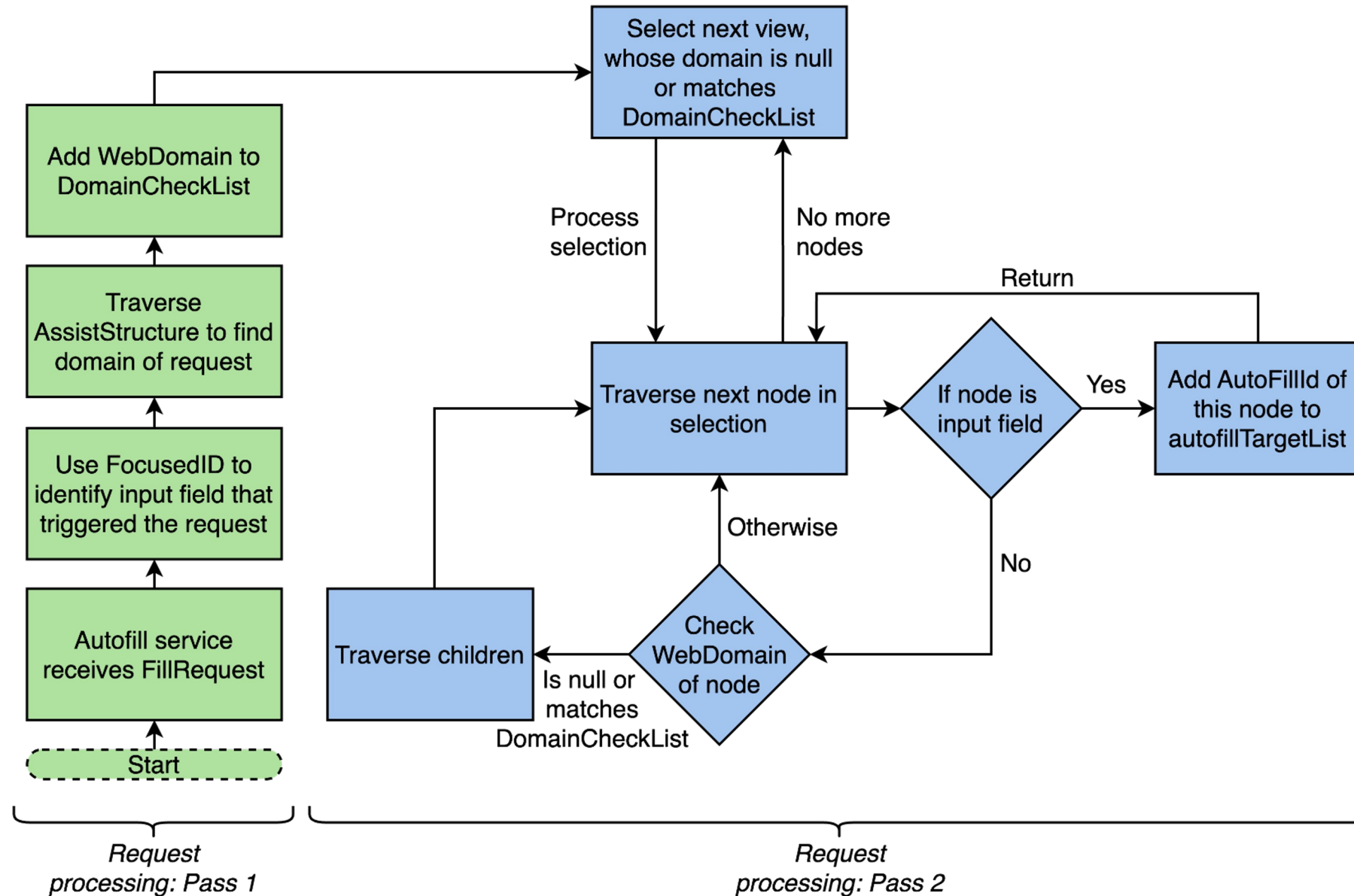




2. Request processing and response from autofill service

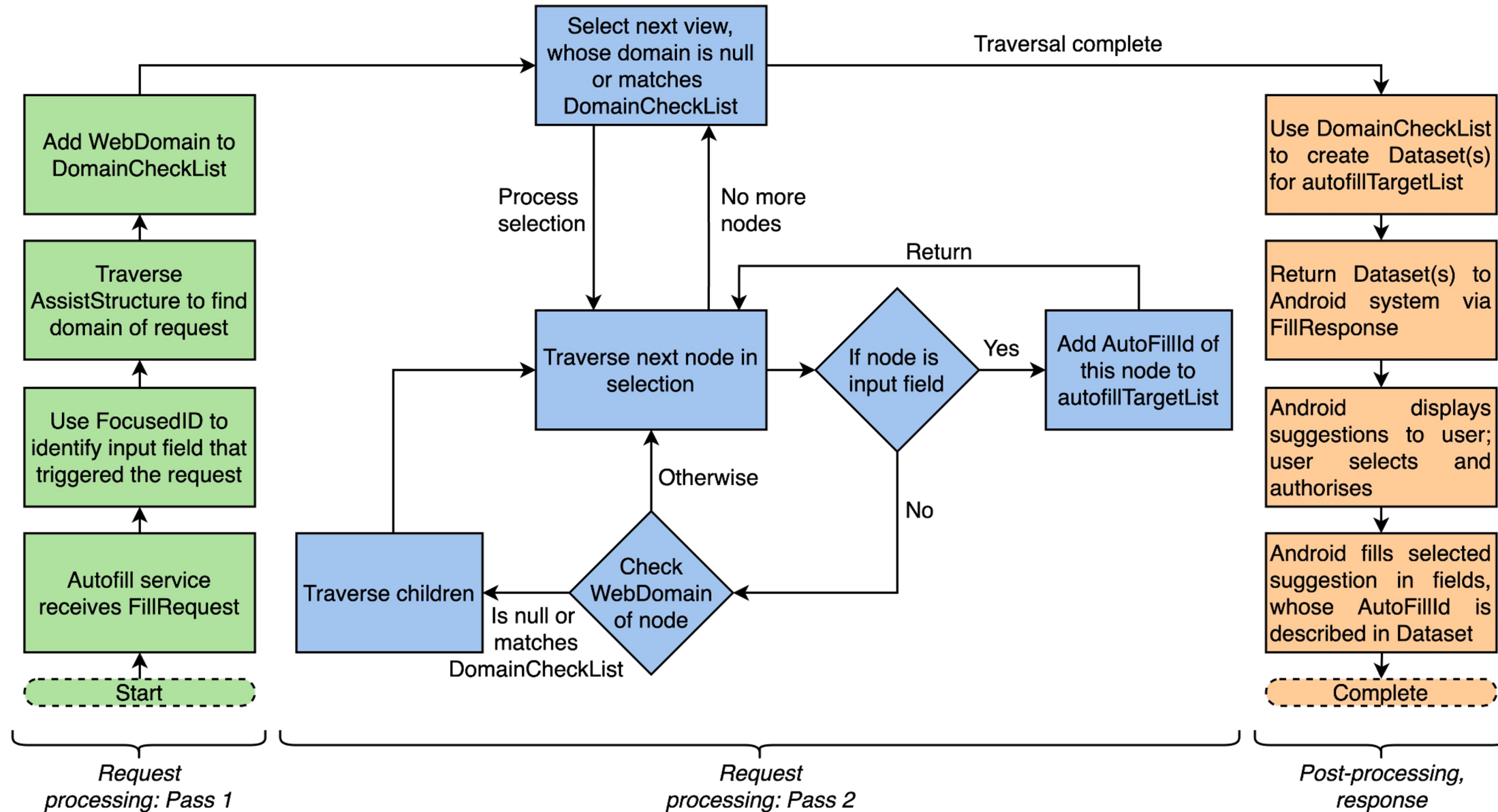


2. Request processing and response from autofill service



AutoSpill - Investigation

2. Request processing and response from autofill service



AutoSpill - Investigation





- + Always renders NativeView data
 - Even for requests from a WebView
 - Creates confusion for autofill service





+ Always renders NativeView data

- Even for requests from a WebView
- Creates confusion for autofill service



+ Parses entire *AssistStructure*

- No track of parent view's *WebDomain*
- Identifies incorrect target input fields



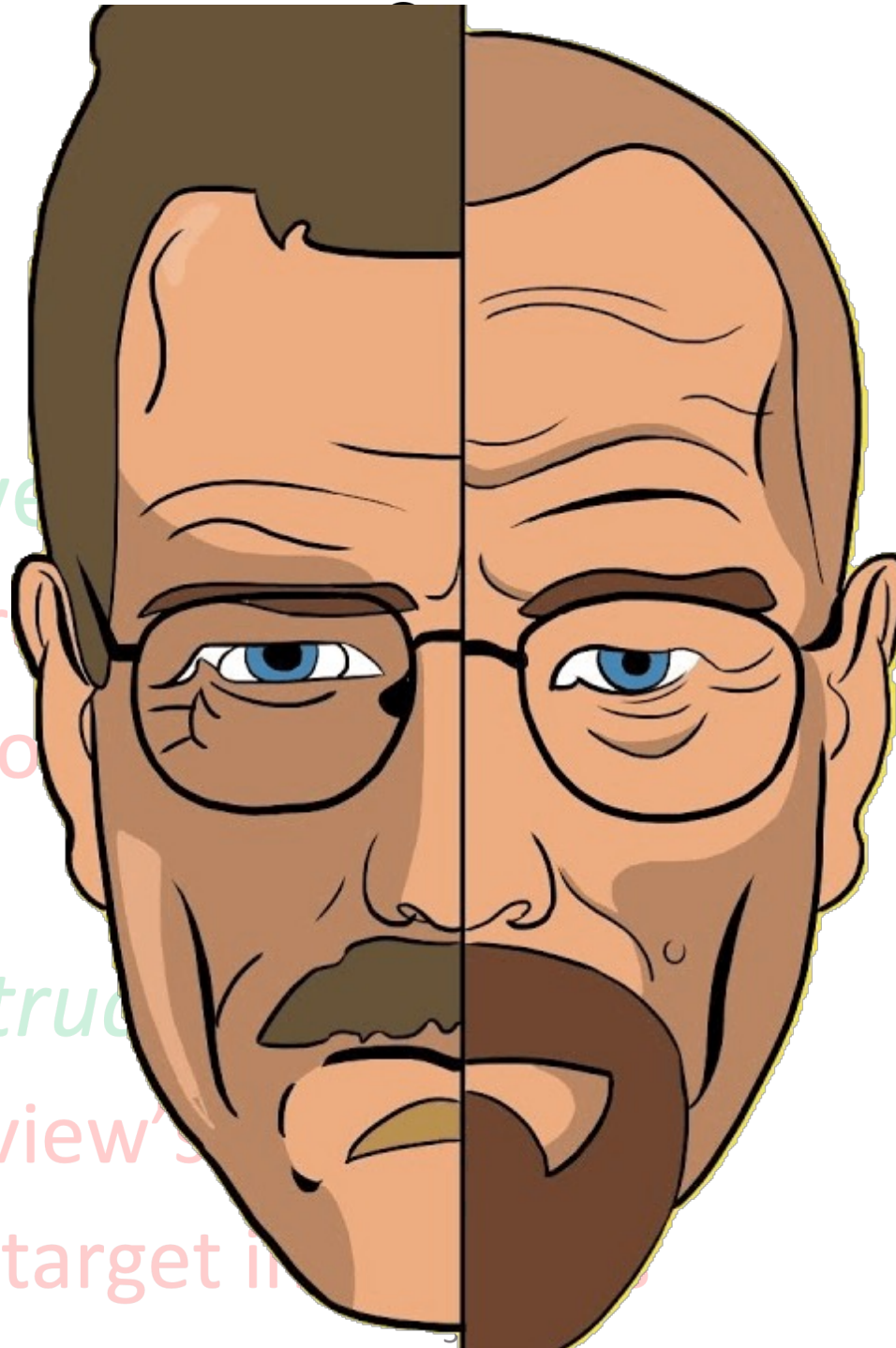
AutoSpill - Investigation

+ Always renders Native

- Even for requests from
- Creates confusion for

+ Parses entire *AssistStructure*

- No track of parent view's
- Identifies incorrect target in



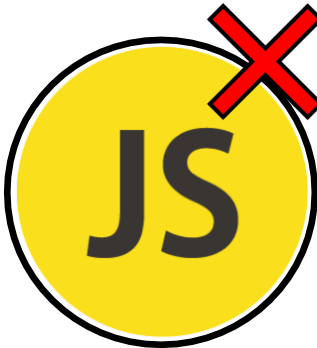
PMs considered

PM	Version	PM's autofill approach
Google Smart Lock	13.30.8.26.arm64	OpenYOLO
DashLane	6.2221.3-arm64-v8a	OpenYOLO
1Password	7.9.4	Autofill Framework
LastPass	5.11.0.9519	Autofill Framework
Enpass	6.8.2.666	Autofill Framework
Keepass2Android	1.09c-r0	Autofill Framework
Keeper	16.4.3.1048	Autofill Framework


Configurations of devices used

Model	Type	Android version	Android security patch
Poco F1	Smartphone	Android 10	December 2020
Samsung Galaxy Tab S6 Lite	Tablet	Android 11	January 2022
Samsung Galaxy A52	Smartphone	Android 12	April 2022

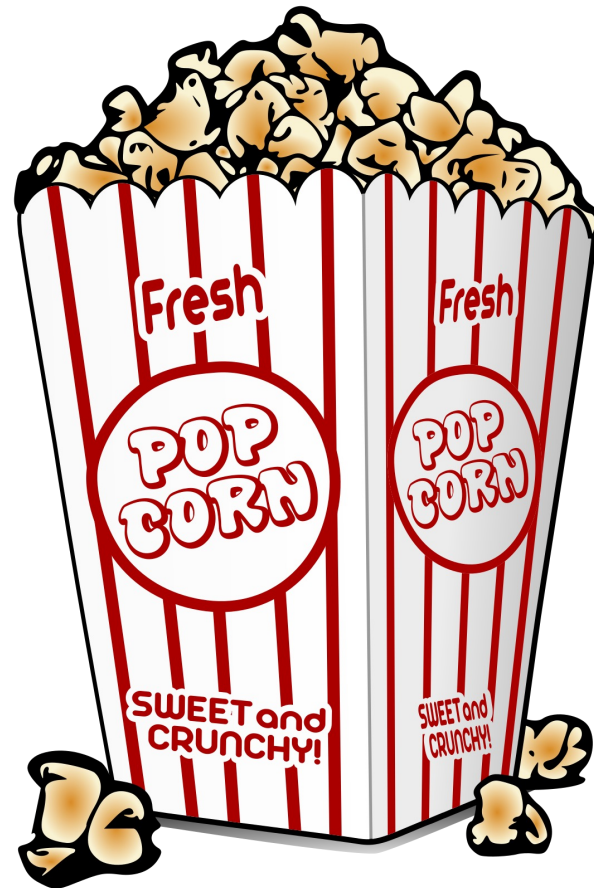
Without JavaScript support

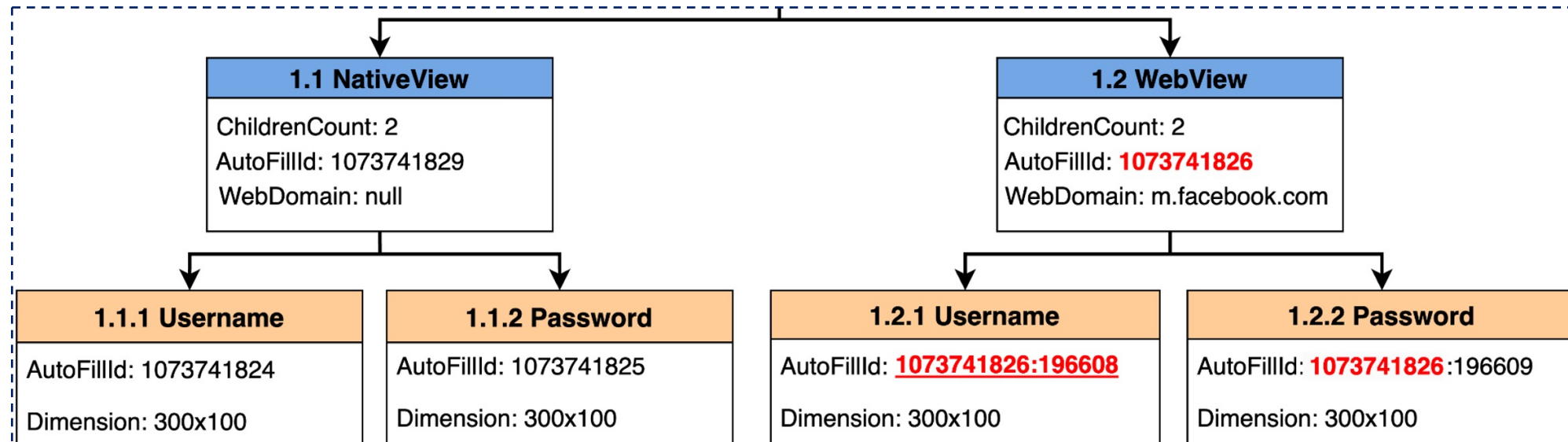
PM	Native fields present in H _A				JavaScript injection
	2 Both username, password	1 Only username	1 Only password	1 Only <i>none</i>	
Google Smart Lock	✓	✓	✓	✓	
Dashlane	✓	✓	✓	✓	
1Password	X	X	P	U	
LastPass	U+P	U	P	U	
Enpass	U+P	U	P	U	
Keepass2Android	U+P	U	P	U	
Keeper	U+P	U	P	U	
✓: No AutoSpill, safe X: Autofilling not working at all U: AutoSpills username P: AutoSpills password U+P: AutoSpills both username and password					

With JavaScript support

PM	Native fields present in H _A				JavaScript injection
	2 Both username, password	1 Only username	1 Only password	1 Only <i>none</i>	
Google Smart Lock	U+P	U/P	U/P	U/P	
Dashlane	U+P	U/P	U/P	U/P	
1Password	X	X	U/P	U/P	
LastPass	U+P	U/P	U/P	U/P	
Enpass	U+P	U/P	U/P	U/P	
Keepass2Android	U+P	U/P	U/P	U/P	
Keeper	U+P	U/P	U/P	U/P	
<p>X: Autofilling not working at all.</p> <p>U+P: H_A accessed and stole both username and password</p> <p>U/P: H_A accessed both username and password, stole credential of choice.</p>					

Video time!





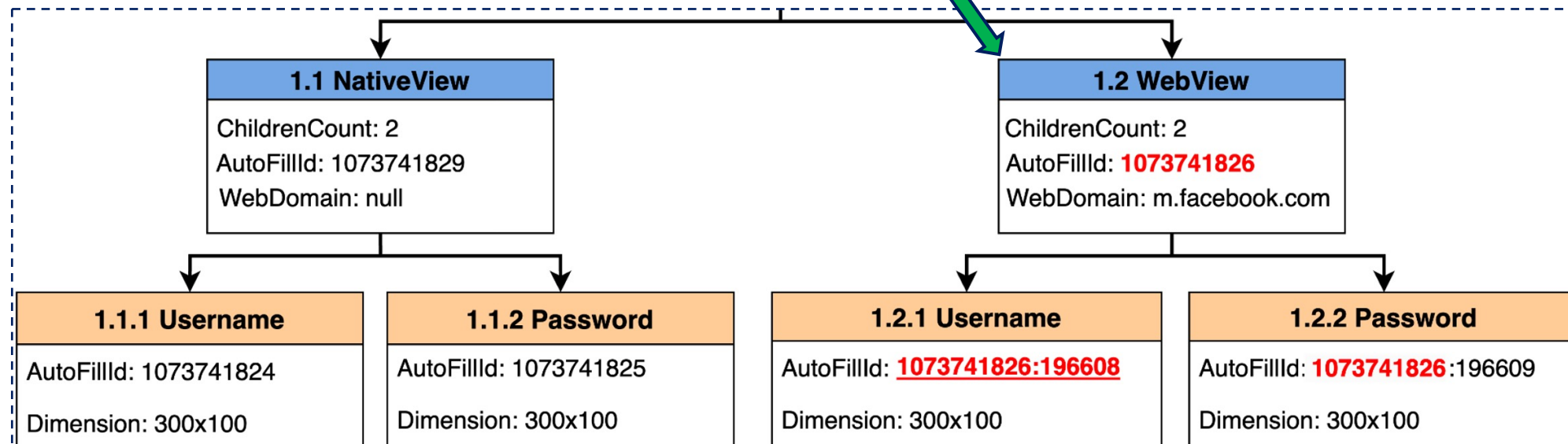
Countermeasures



**No excess
information!**



AssistStructure data for request-triggering view only



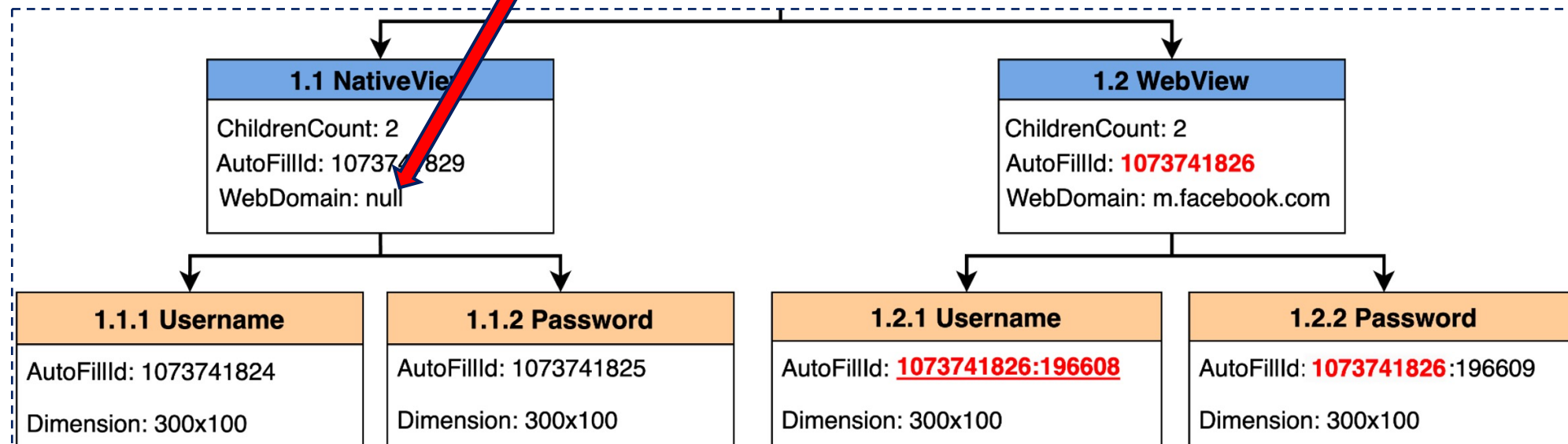
Countermeasures



**No excess
information!**



AssistStructure data for request-triggering view only
Non-null WebDomain into HTML elements



Countermeasures



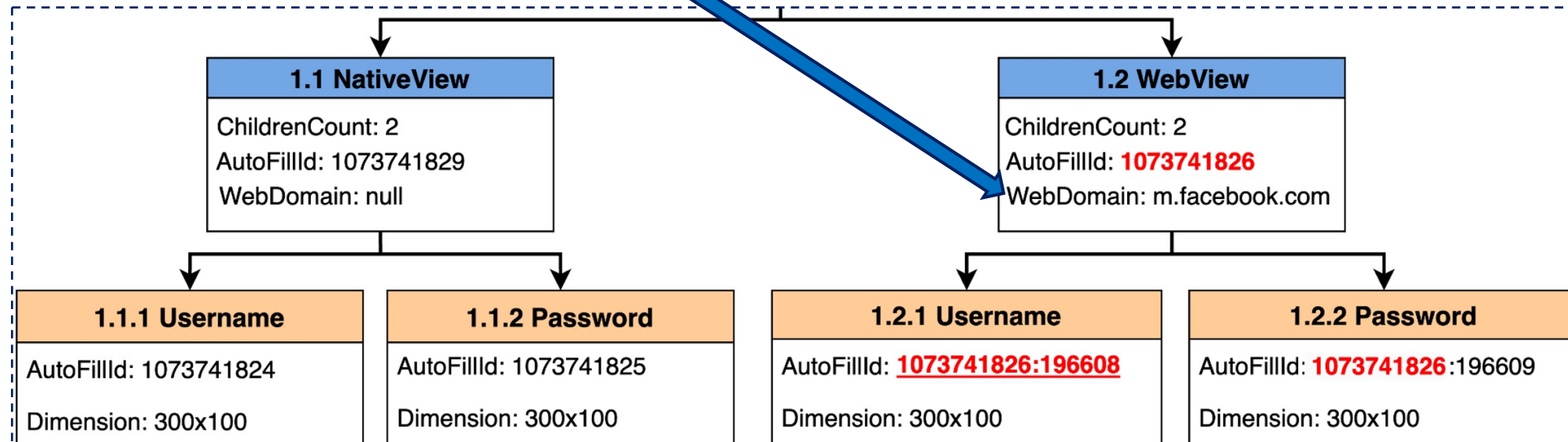
No excess
information!



No excess
processing!

AssistStructure data for request-triggering view only
Non-null WebDomain into HTML elements

Keep a track of parent view's WebDomain



Countermeasures



**No excess
information!**



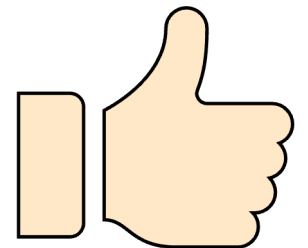
**No excess
processing!**



AssistStructure data for request-triggering view only
Non-null WebDomain into HTML elements

Keep a track of parent view's WebDomain

Run-time AutoFillId from *AssistStructure* to
Identify & process request-triggering field
Supply values back only for request-triggering view



- PMs work under the constraints of Android's app sandboxing
- Excess information (from Android) and excess processing (by PMs) lead to credential AutoSpill
- Android and PM developers must work together to fix AutoSpill





Evil image by Freepik - Flaticon, www.flaticon.com/free-icons/evil
Markus Spiske, Coding, www.pexels.com/photo/technology-computer-desktop-programming-113850
Worldwide image by Prosymbols Premium - Flaticon, www.flaticon.com/free-icons/worldwide
Internet image by Stickers - Flaticon, www.flaticon.com/free-stickers/internet
Devices image by Freepik - Flaticon, www.flaticon.com/free-icons/devices
Routing image by Iconjam - Flaticon, www.flaticon.com/free-icons/routing
Conveyor-belt image by Freepik - Flaticon, www.flaticon.com/free-icons/conveyor-belt
Traffic control image by Freepik - Flaticon, www.flaticon.com/free-icons/traffic-control
iPhone image by Freepik - Flaticon, www.flaticon.com/free-icons/iphone
iPad image by Freepik - Flaticon, www.flaticon.com/free-icons/ipad
iMac image by Freepik - Flaticon, www.flaticon.com/free-icons/computer
Ecommerce images by Eucalyp - Flaticon, www.flaticon.com/free-icons/ecommerce
Login image by bearicons - Flaticon, www.flaticon.com/free-icons/login
Filistic, iOS icon pack, www.etsy.com/listing/1343526218/ios-16-app-icon-pack-with-100-aesthetic
Checklist image by Freepik - Flaticon, www.flaticon.com/free-icons/checklist
Pain image by Smashicons - Flaticon, www.flaticon.com/free-icons/pain
Password image by Smashicons - Flaticon, www.flaticon.com/free-icons/password
Center focus image by Freepik - Flaticon, www.flaticon.com/free-icons/center-focus
Wikimedia Commons, Android, commons.wikimedia.org/wiki/File:Android_robot.svg
Database image by Freepik - Flaticon, www.flaticon.com/free-icons/database
Selection image by Freepik - Flaticon, www.flaticon.com/free-icons/select
Login image by srip - Flaticon, www.flaticon.com/free-icons/login
Form image by Freepik - Flaticon, www.flaticon.com/free-icons/form
Phone image by juicy_fish - Flaticon, www.flaticon.com/free-icons/cell-phone
Desktop image by Vichanon Chaimsuk - Flaticon, www.flaticon.com/free-icons/login
Puzzle image by riajulislam - Flaticon, www.flaticon.com/free-icons/puzzle
Webpage image by Eucalyp - Flaticon, www.flaticon.com/free-icons/webpage
Mobile image by amonrat rungreangfangsai - Flaticon, www.flaticon.com/free-icons/application
Playstore image by justicon - Flaticon, www.flaticon.com/free-icons/playstore
Sandbox image by juicy_fish - Flaticon, www.flaticon.com/free-icons/sandbox
Oil-spill image by nawicon - Flaticon, www.flaticon.com/free-icons/oil-spill
Wikimedia Commons, Mad scientist, commons.wikimedia.org/wiki/File:Mad_scientist_transparent_background.svg
Investigation image by Dewi Sari - Flaticon, www.flaticon.com/free-icons/investigation
Lazy Owl, "The lucifer effect: Why good people turn bad?" www.youtube.com/watch?v=1RwhkZFDYmY
Wikimedia Commons, Popcorn, commons.wikimedia.org/wiki/File:Popcorn.svg
Thank you image by Freepik - Flaticon, www.flaticon.com/free-icons/thank-you
QA image by Freepik - Flaticon, www.flaticon.com/free-icons/qa



AutoSpill attack by:

Ankit Gangwal (gangwal@iiit.ac.in)

Shubham Singh

Abhijeet Srivastava



INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY

H Y D E R A B A D