



**Georgia
Tech**



The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends



Omar Alrawi*, Chaoshun Zuo*, Ruian Duan, Ranjita Pai Kasturi,
Zhiqiang Lin, Brendan Saltaformaggio

***First Co-Authors**



Cycling as a Mass Gathering

An event during which cyclists gather (possibly and where there is the potential for a delayed response to emergencies) because of unique stops or patterns in other features of the environment and terrain.



Conference



Conference




WIRED

How Hackers Slipped by British Airways' Defenses

The airline also said in its disclosure that the attack impacted its mobile users.



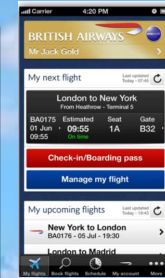
Conference


A photograph of an iceberg floating in the ocean. The top part of the iceberg is visible above the water surface, while a much larger, jagged portion is submerged below. The sky is blue with scattered white clouds. The water is a deep blue, and the horizon is visible in the distance.

More Than
What's on
The Surface

More Than
What's on
The Surface

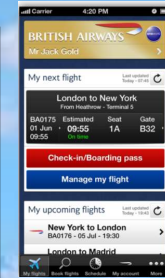
Mobile App



An iceberg floating in the ocean, with a small tip above the surface and a much larger, jagged mass submerged below. The sky is blue with some clouds, and the water is a deep blue.

More Than
What's on
The Surface

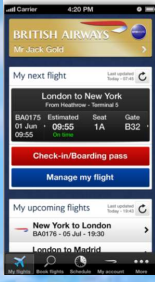
Mobile App



Cloud Backend

More Than
What's on
The Surface

Mobile App



Web App



Cloud Backend

More Than
What's on
The Surface

Mobile App



Web App



Software Services



Cloud Backend

More Than
What's on
The Surface

Mobile App



Web App



Software Services

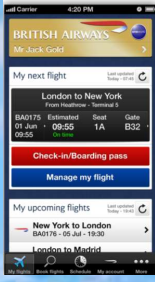


Operating System



More Than
What's on
The Surface

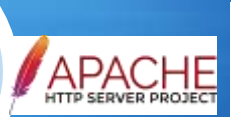
Mobile App



Web App



Software Services



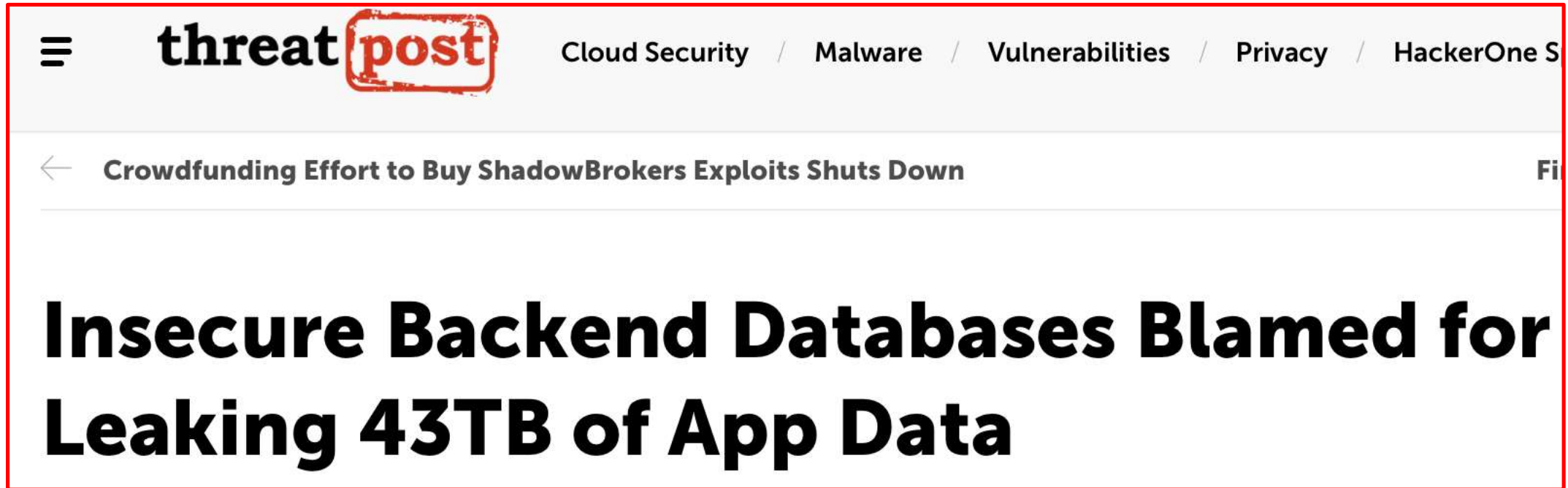
Operating System



(v)Hardware



Mobile Backends All Over the News

A screenshot of a mobile news article header from Threatpost. The page is framed by a red border. At the top left is a hamburger menu icon. The logo 'threatpost' is displayed, with 'post' in a red stamp-like font. To the right of the logo are navigation links: 'Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne S'. Below the navigation is a breadcrumb trail: '← Crowdfunding Effort to Buy ShadowBrokers Exploits Shuts Down' followed by 'Fi'. The main headline is 'Insecure Backend Databases Blamed for Leaking 43TB of App Data' in large, bold black text.

☰ **threat** **post** Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne S

← Crowdfunding Effort to Buy ShadowBrokers Exploits Shuts Down Fi

Insecure Backend Databases Blamed for Leaking 43TB of App Data

Mobile Backends All Over the News

The image shows a screenshot of a web page from Threatpost. At the top, the Threatpost logo is visible, along with navigation links for Cloud Security, Malware, Vulnerabilities, Privacy, and HackerOne S. Below the logo, there is a dark navigation bar for SecurityScorecard with links for Platform, Solutions, Customers, Partners, Resources, and Company. A search bar and a 'FREE SCORE' button are also present. The main content area features a large article title, 'The Calm Before the Mobile API Data Breach Storm', by Imarc, posted on June 2, 2015. The article title is in a large, white, serif font, and the author and date are in a smaller, yellow, sans-serif font.

threatpost Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne S

SecurityScorecard Login Blog Contact HUB **FREE SCORE** RE Fi

Platform Solutions Customers Partners Resources Company

The Calm Before the Mobile API Data Breach Storm

By Imarc
POSTED ON JUN 2, 2015

Mobile Backends All Over the News

The image shows a screenshot of a web browser displaying an article on the Threatpost website. The page is framed with a red border. At the top, the Threatpost logo is visible, along with navigation links for Cloud Security, Malware, Vulnerabilities, Privacy, and HackerOne S. Below the logo, there is a dark navigation bar for SecurityScorecard with links for Platform, Solutions, Customers, Partners, Resources, and Company. The main article title is "Thousands of Apps Leak Sensitive Data via Misconfigured Firebase Backends", with "Thousands of Apps" underlined. The author is Catalin Cimpanu, and the article was published on June 23, 2018, at 05:00 AM. The article features an illustration of a hand holding a smartphone displaying the "playbuzz" app, with a cloud and a crown icon above it.

≡ **threatpost** Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne S

SecurityScorecard Login Blog Contact HUB **FREE SCORE** RE Fi

Platform Solutions Customers Partners Resources Company

Thousands of Apps Leak Sensitive Data via Misconfigured Firebase Backends

By [Catalin Cimpanu](#) June 23, 2018 05:00 AM 0

Prior Work

- The rise of backends
 - Acar et al. "SoK: Lessons learned from android security research for appified software platforms." *IEEE S&P*, 2016.



Prior Work

- The rise of backends
 - Acar et al. "SoK: Lessons learned from android security research for appified software platforms." *IEEE S&P*, 2016.
- Evolution of backends



Prior Work

- The rise of backends
 - Acar et al. "SoK: Lessons learned from android security research for appified software platforms." *IEEE S&P*, 2016.
- Evolution of backends
 - App Thinning¹



[1] Mojica, Gregg. Working with App Thinning in iOS 9 <https://www.appcoda.com/app-thinning/>, Accessed Aug 2019

Prior Work

- The rise of backends
 - Acar et al. "SoK: Lessons learned from android security research for appified software platforms." *IEEE S&P*, 2016.
- Evolution of backends
 - App Thinning¹
- Security of Backends



[1] Mojica, Gregg. Working with App Thinning in iOS 9 <https://www.appcoda.com/app-thinning/>, Accessed Aug 2019

Prior Work

- The rise of backends
 - Acar et al. "SoK: Lessons learned from android security research for appified software platforms." *IEEE S&P*, 2016.
- Evolution of backends
 - App Thinning¹
- Security of Backends
 - Zuo et al. "Authscope: Towards automatic discovery of vulnerable authorizations in online services." *ACM CCS.*, 2017
 - Zuo et al. "Why does your data leak? uncovering the data leakage in cloud from mobile apps." *IEEE S&P*. 2019
 - Appthority²

[1] Mojica, Gregg. Working with App Thinning in iOS 9 <https://www.appcoda.com/app-thinning/>, Accessed Aug 2019

[2] K. Watkins, "HospitalGown: The Backend Exposure Putting Enterprise Data at Risk," Appthority, Tech. Rep., 2017.





**Mel is an app
developer.**

**Mel just wants to
ship his killer app.**



Mobile App

Web App

Software Services

Operating System

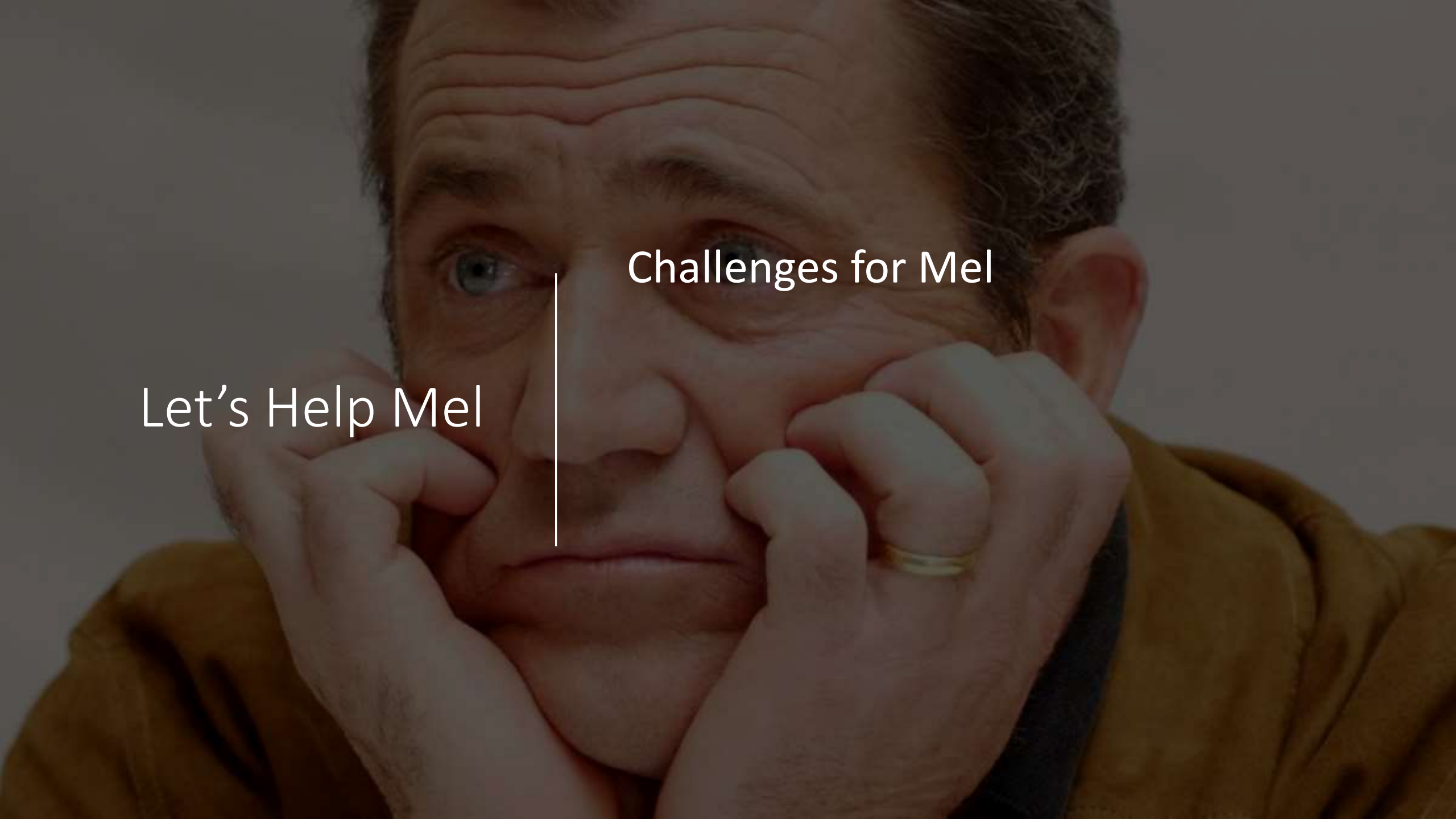
(v)Hardware

**Mel is an app
developer.**

**Mel just wants to
ship his killer app.**



Let's Help Mel



Challenges for Mel

Let's Help Mel

A close-up photograph of a man with a thoughtful expression, resting his chin on his hands. He is wearing a brown jacket and a gold ring on his left hand. The image is dimmed to serve as a background for text.

Let's Help Mel

Challenges for Mel

- What backends does my app use?

A close-up photograph of a man with a thoughtful expression, resting his chin on his hands. He is wearing a brown jacket. The image is dimmed to serve as a background for text.

Let's Help Mel

Challenges for Mel

- What backends does my app use?
- How do I check if they are secure?



Let's Help Mel

Challenges for Mel

- What backends does my app use?
- How do I check if they are secure?
- How do I fix them?



Let's Help Mel

Challenges for Mel

- What backends does my app use?
- How do I check if they are secure?
- How do I fix them?
- Can I fix them (attribution)?

Let's Help Mel



Challenges for Mel

- What backends does my app use?
- How do I check if they are secure?
- How do I fix them?
- Can I fix them (attribution)?

Let's Help Mel



Challenges for Mel

- What backends does my app use?
- How do I check if they are secure?
- How do I fix them?
- Can I fix them (attribution)?

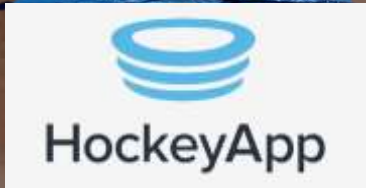
Mel's Dream: Upload APK and vet all backends!



What Backends My App Uses?



What Backends My App Uses?



What Backends My App Uses?



What Backends My App Uses?



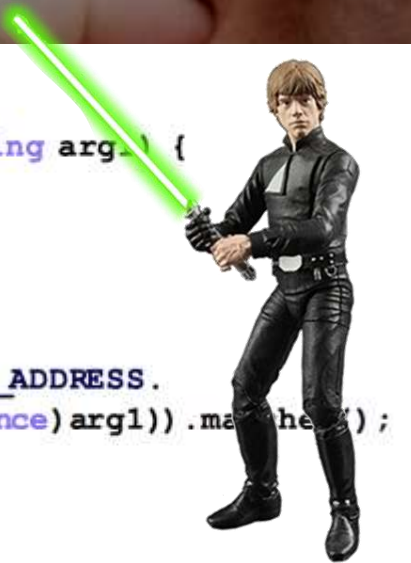


FacebookSDK



What Backends My App Uses?

```
public class al {  
    ...  
    public static boolean a(String arg1) {  
        boolean v0;  
        if(arg1 == null) {  
            return false;  
        }  
        else {  
            v0 = Patterns.EMAIL_ADDRESS.  
                matcher(((CharSequence) arg1)).matcher("");  
        }  
        return v0;  
    }  
}
```



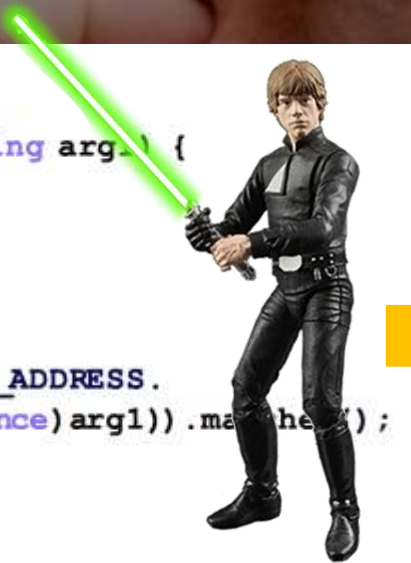


FacebookSDK



What Backends My App Uses?

```
public class al {  
    ...  
    public static boolean a(String arg1) {  
        boolean v0;  
        if(arg1 == null) {  
            return false;  
        }  
        else {  
            v0 = Patterns.EMAIL_ADDRESS.  
                matcher(((CharSequence) arg1)).matcher("");  
        }  
        return v0;  
    }  
}
```

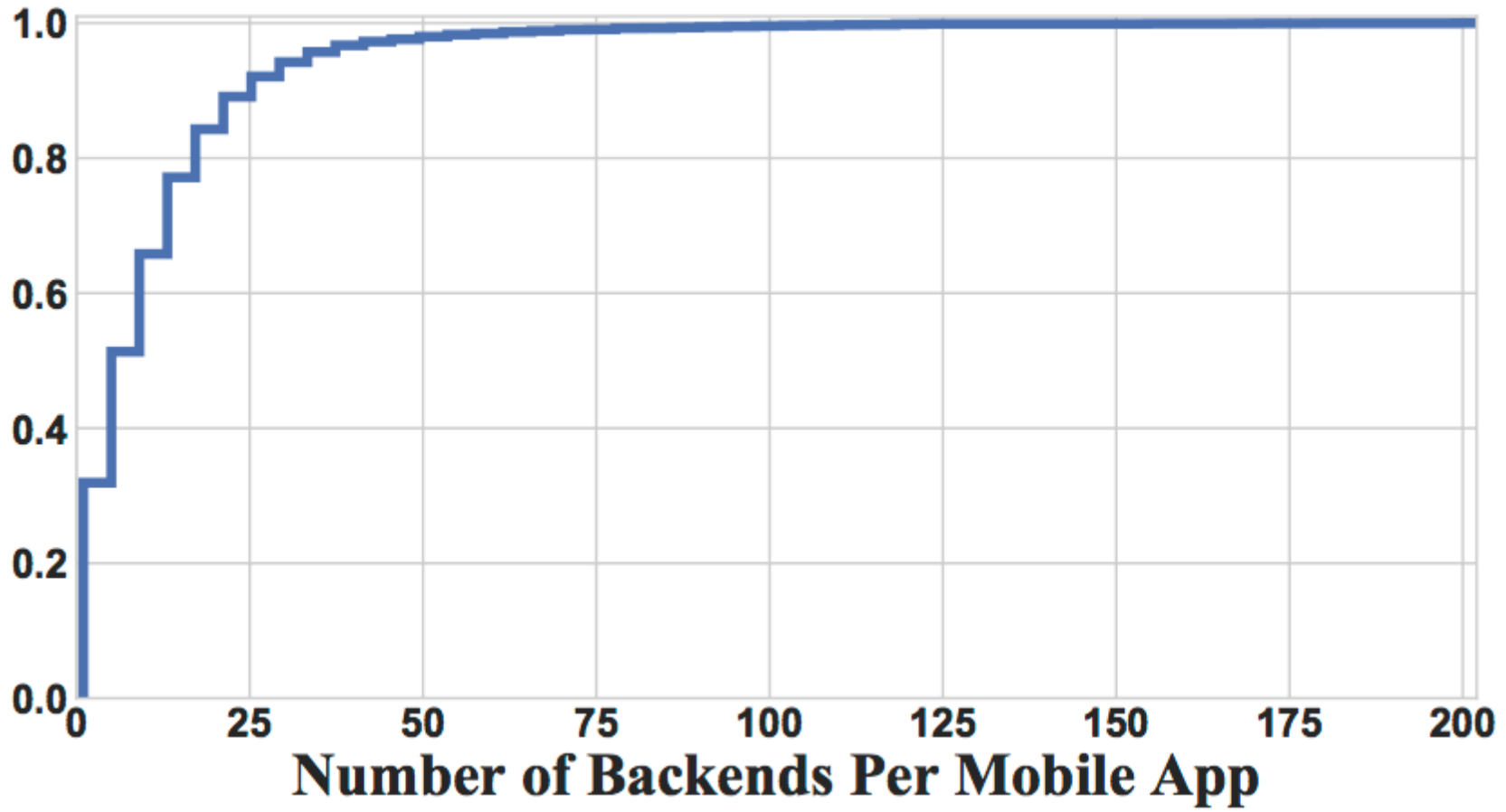


PUT /api/v9/forgotpassword?key=d12121c70dda5edfgd1df6633fdb36c0
HTTP/1.1
Content-Type: application/json
Connection: close
User-Agent: Dalvik/1.6.0 (Linux; Android 4.2)
Host: sm.shopclues.com
Accept-Encoding: gzip
Content-Length: 73

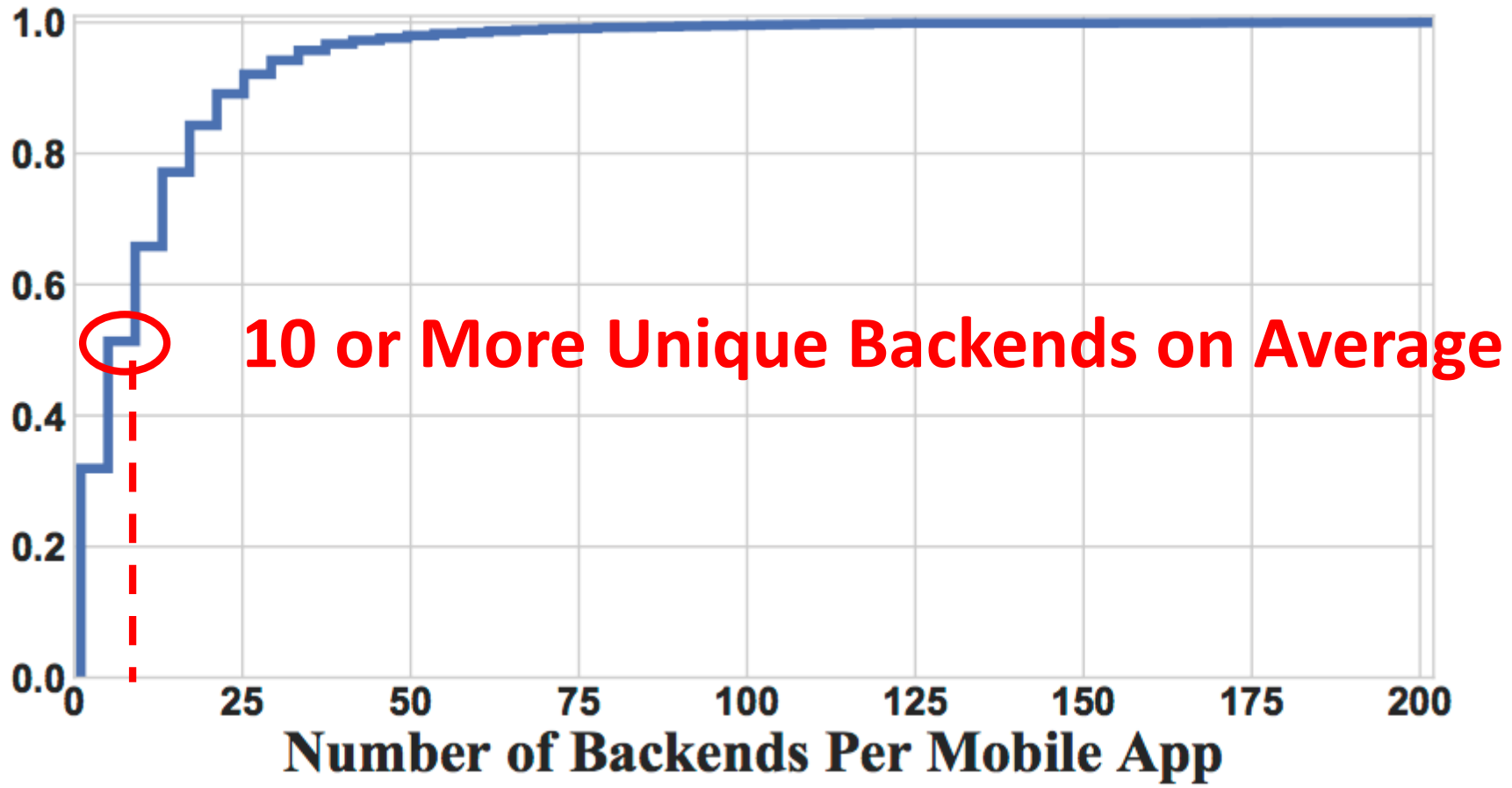
{"user_email": "testmobileserver@gmail.com", "key": "d12121c70dda5edfgd1df6633fdb36c0"}



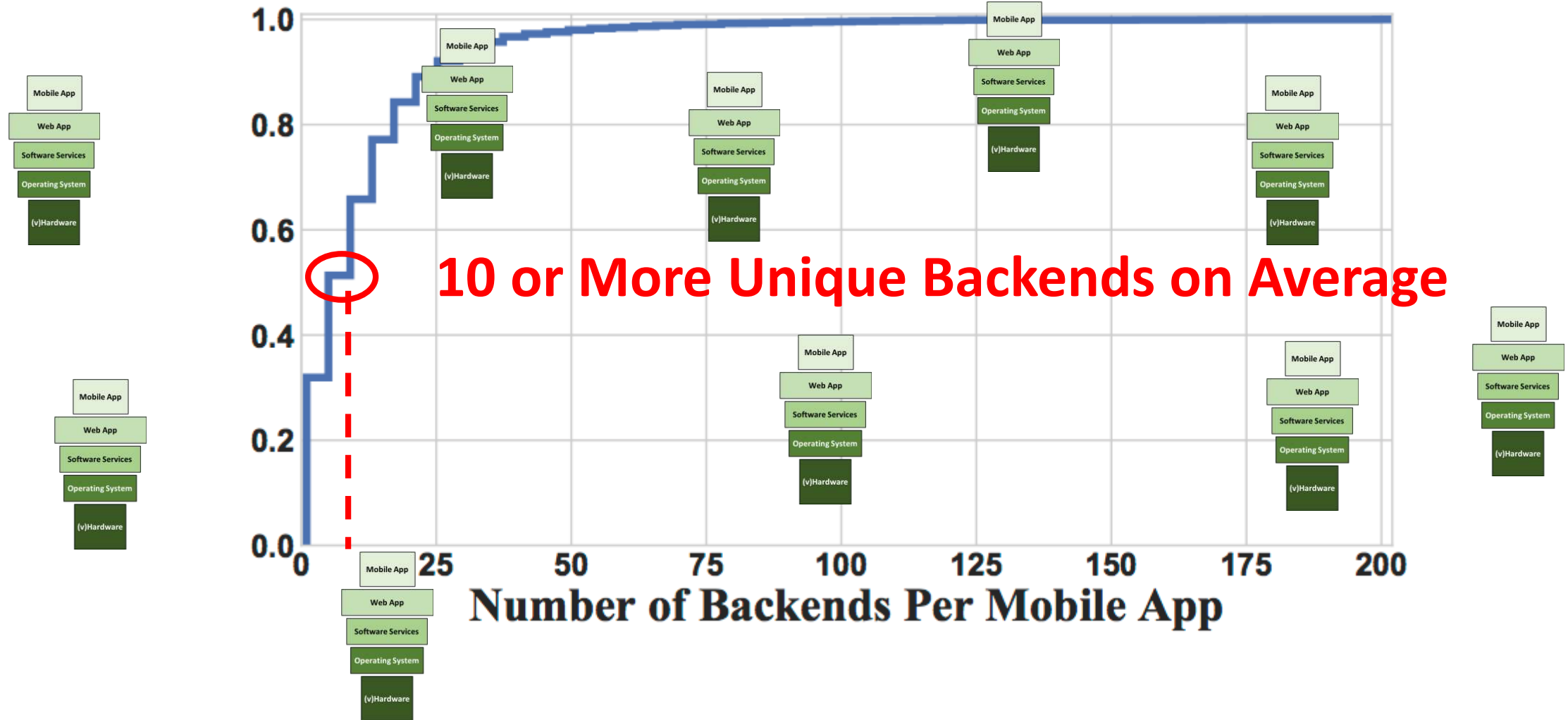
How Many Backends?



How Many Backends?

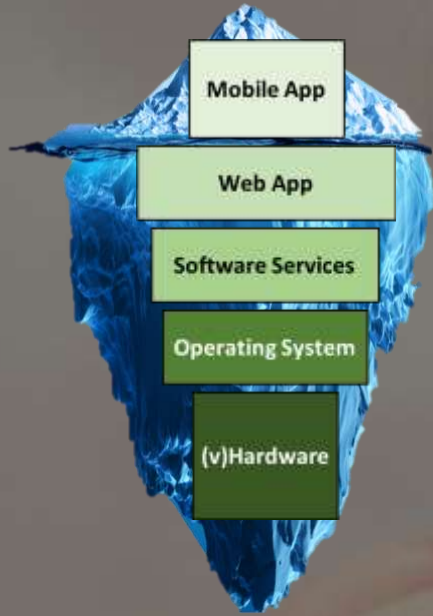


How Many Backends?

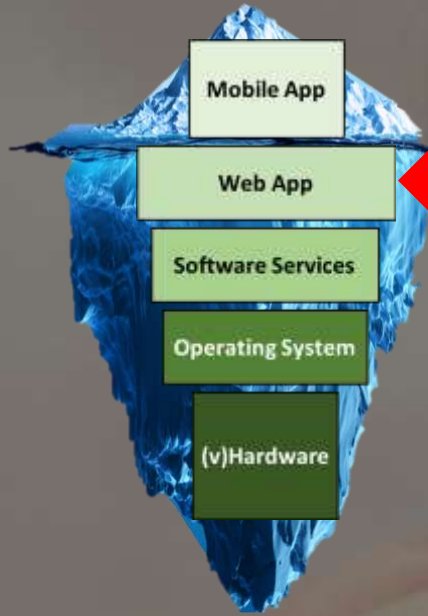




How Do I Check If They Are Secure?

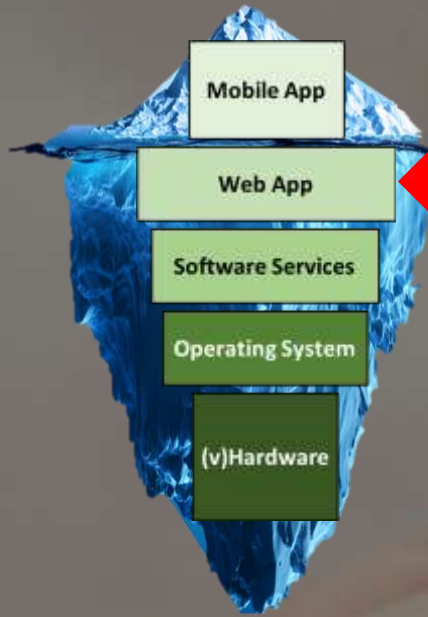


How Do I Check If They Are Secure?



First: Bug finding via input perturbation

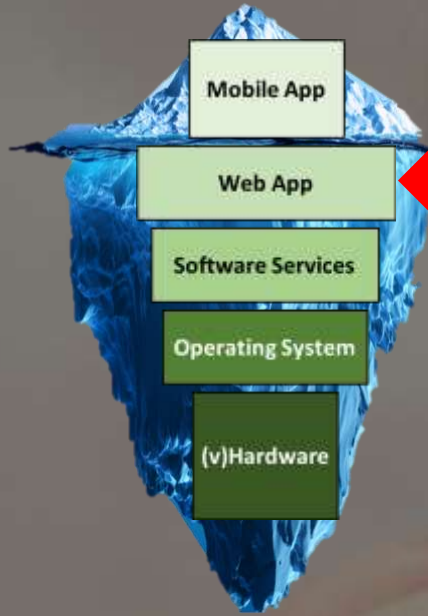
How Do I Check If They Are Secure?



First: Bug finding via input perturbation

How Do I Check If They Are Secure?





First: Bug finding via input perturbation

How Do I Check If They Are Secure?



```
PUT /api/v9/forgotpassword?key=d12121c70dda5edfgd1df6633fdb36c0
HTTP/1.1
Content-Type: application/json
Connection: close
User-Agent: Dalvik/1.6.0 (Linux; Android 4.2)
Host: sm.shopclues.com
Accept-Encoding: gzip
Content-Length: 73

{"user_email": "testmobileserver@gmail.com", "key": "d12121c70dda5edfgd1df6633fdb36c0"}
```



First: Bug finding via input perturbation

How Do I Check If They Are Secure?



```
PUT /api/v9/forgotpassword?key=d12121c70dda5edfgd1df6633fdb36c0
HTTP/1.1
Content-Type: application/json
Connection: close
User-Agent: Dalvik/1.6.0 (Linux; Android 4.2)
Host: sm.shopclues.com
Accept-Encoding: gzip
Content-Length: 73
{"user_email": "testmobileserver@gmail.com", "key": "d12121c70dda5edfgd1df6633fdb36c0"}
```



First: Bug finding via input perturbation

How Do I Check If They Are Secure?



```
PUT /api/v9/forgotpassword?key=d12121c70dda5edfgd1df6633fdb36c0
HTTP/1.1
Content-Type: application/json
Connection: close
User-Agent: Dalvik/1.6.0 (Linux; Android 4.2)
Host: sm.shopclues.com
Accept-Encoding: gzip
Content-Length: 73
{"user_email": "testmobileserver@gmail.com", "key": "d12121c70dda5edfgd1df6633fdb36c0"}
```



SQLi, XSS, XXE



How Do I Check If They Are Secure?

Second: Scan services for known vulnerabilities



How Do I Check If They Are Secure?

Second: Scan services for known vulnerabilities



65K Ports



How Do I Check If They Are Secure?

Second: Scan services for known vulnerabilities

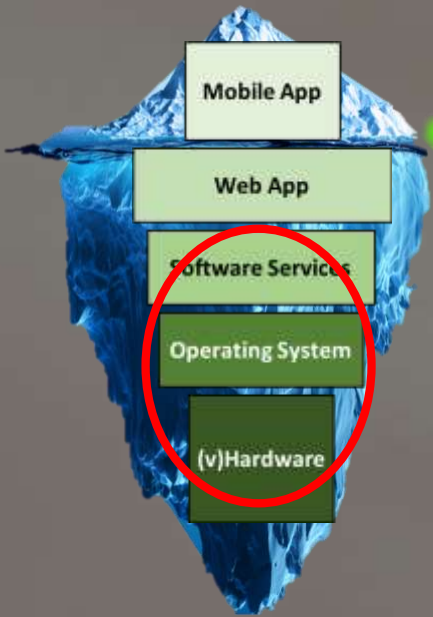


65K Ports



How Do I Check If They Are Secure?

Second: Scan services for known vulnerabilities



65K Ports



How Do I Check If They're Secure?

```
80/tcp  open  http          Microsoft IIS httpd 10.0
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Ask Jeeves
135/tcp  open  msrpc        Microsoft Windows RPC
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http        Jetty 9.4.z-SNAPSHOT
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)
|_ http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Second: Scan services for known vulnerabilities



65K Ports



How Do I Check If They're Secure?

```
80/tcp  open  http          Microsoft IIS httpd 10.0
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Ask Jeeves
135/tcp  open  msrpc        Microsoft Windows RPC
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http        Jetty 9.4.z-SNAPSHOT
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)
|_ http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Second: Scan services for known vulnerabilities



65K Ports



How Do I Check If They're Secure?

```
80/tcp open http Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Ask Jeeves
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKG
50000/tcp open http Jetty 9.4.z-SNAPSHOT
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)
|_ http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows
```



A close-up photograph of a man with a thoughtful expression, resting his chin on his hands. He has light blue eyes and is wearing a gold ring on his left hand. The text "Can I Fix Them?" is overlaid in white on the center of the image.

Can I Fix Them?



Mobile App

Web App

Software Services

Operating System

(v)Hardware

Can I Fix Them?

First-Party: If Mel owns the whole stack

Mobile App

Web App

Software Services

Operating System

(v)Hardware

Can I Fix Them?

First-Party: If Mel owns the whole stack

Mobile App

Web App

Software Services

Operating System

(v)Hardware

Mel is responsible for this portion

Can I Fix Them?





Mobile App

Web App

Software Services

Operating System

(v)Hardware

Can I Fix Them?

Third-Party: If Mel uses an SDK

Mobile App

SDK Access

Web App

Software Services

Operating System

No Access!

Can I Fix Them?





Mobile App

Web App

Software Services

Operating System

(v)Hardware

Can I Fix Them?

Hybrid: If Mel uses a rented platform

Mobile App

Web App

Software Services

Operating System

(v)Hardware

Mel is responsible for this portion

Can I Fix Them?

Hybrid: If Mel uses a rented platform

Mobile App

Web App

Software Services

Operating System

Rented!

(v)Hardware

Mel is responsible for this portion

Can I Fix Them?

Platform Provider is responsible for this portion

A close-up photograph of a middle-aged man with light blue eyes and a thoughtful expression. He is resting his chin on his hands, with his fingers interlaced. He is wearing a gold ring on his left ring finger. The background is a plain, light-colored wall. The overall tone is contemplative and serious.

How Do I Fix Them?



How Do I Fix Them?



How Do I Fix Them?

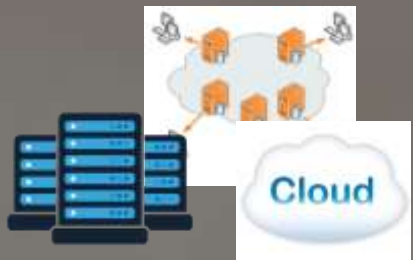
Data
Aggregation
and
Consolidation



Data
Aggregation
and
Consolidation



How Do I Fix Them?



Data
Aggregation
and
Consolidation



How Do I Fix Them?





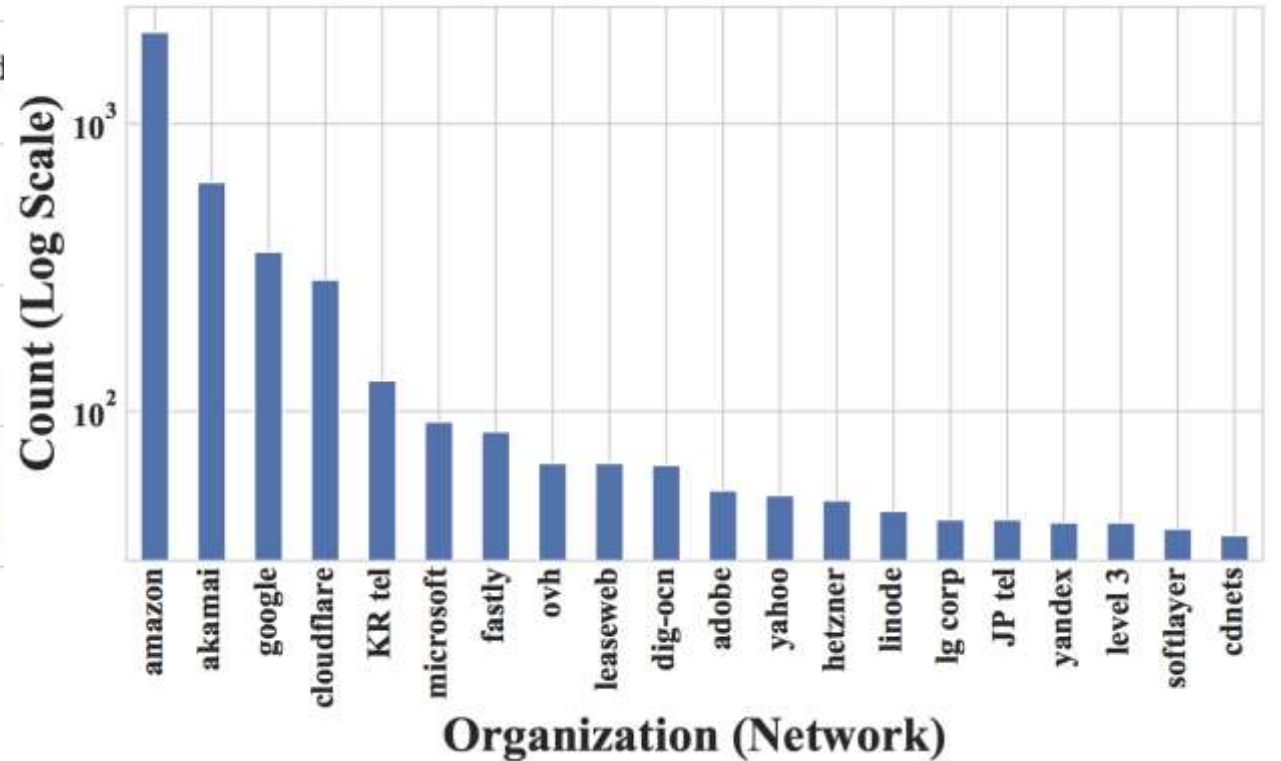
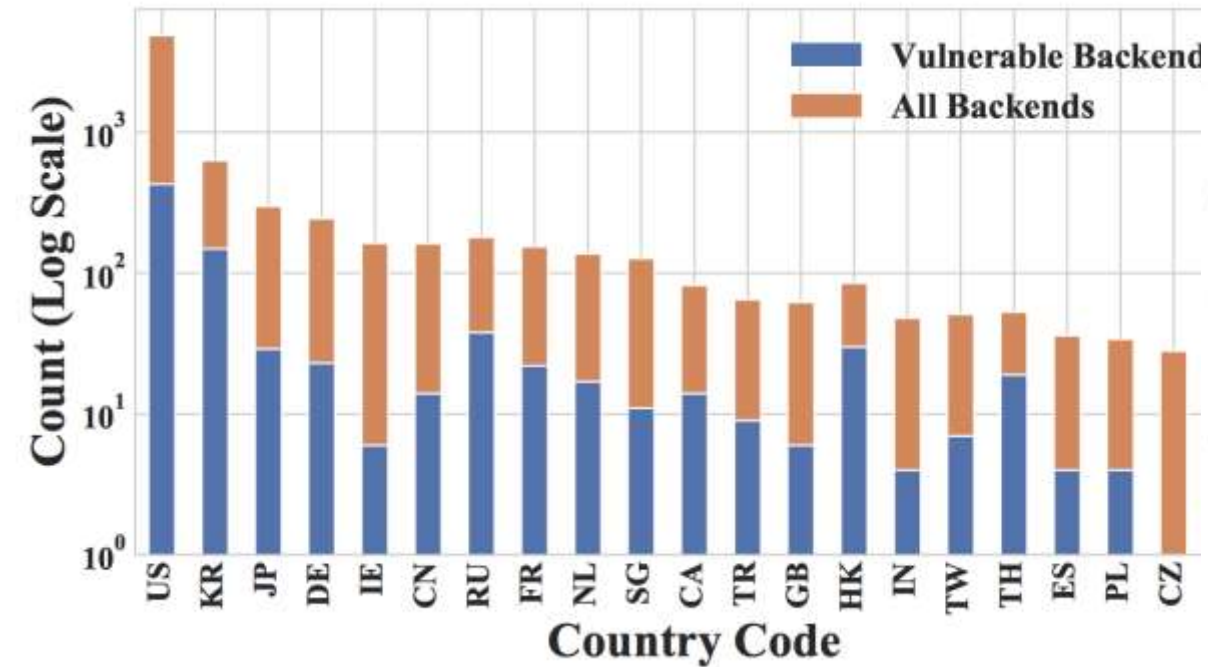
Data
Aggregation
and
Consolidation



How Do I Fix Them?



Geo and Net Distribution



How can Mel be expected to solve everything?



Google Play Store



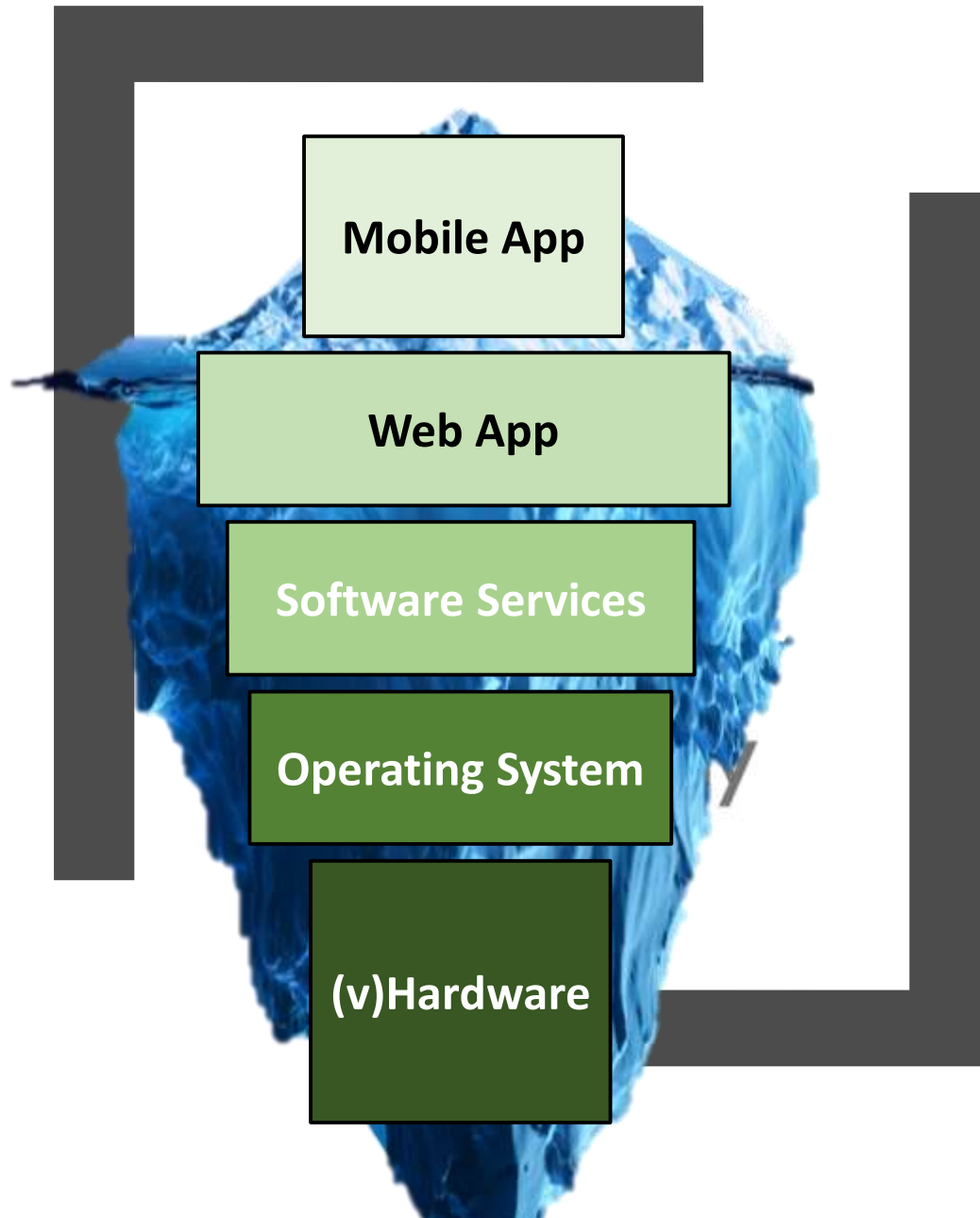
Google Play Store

- Top 5,000 apps from August 2018



Google Play Store

- Top 5,000 apps from August 2018
- We found
 - Over **600 0-DAY**
 - Over **900 N-DAY**



Mobile App

Web App

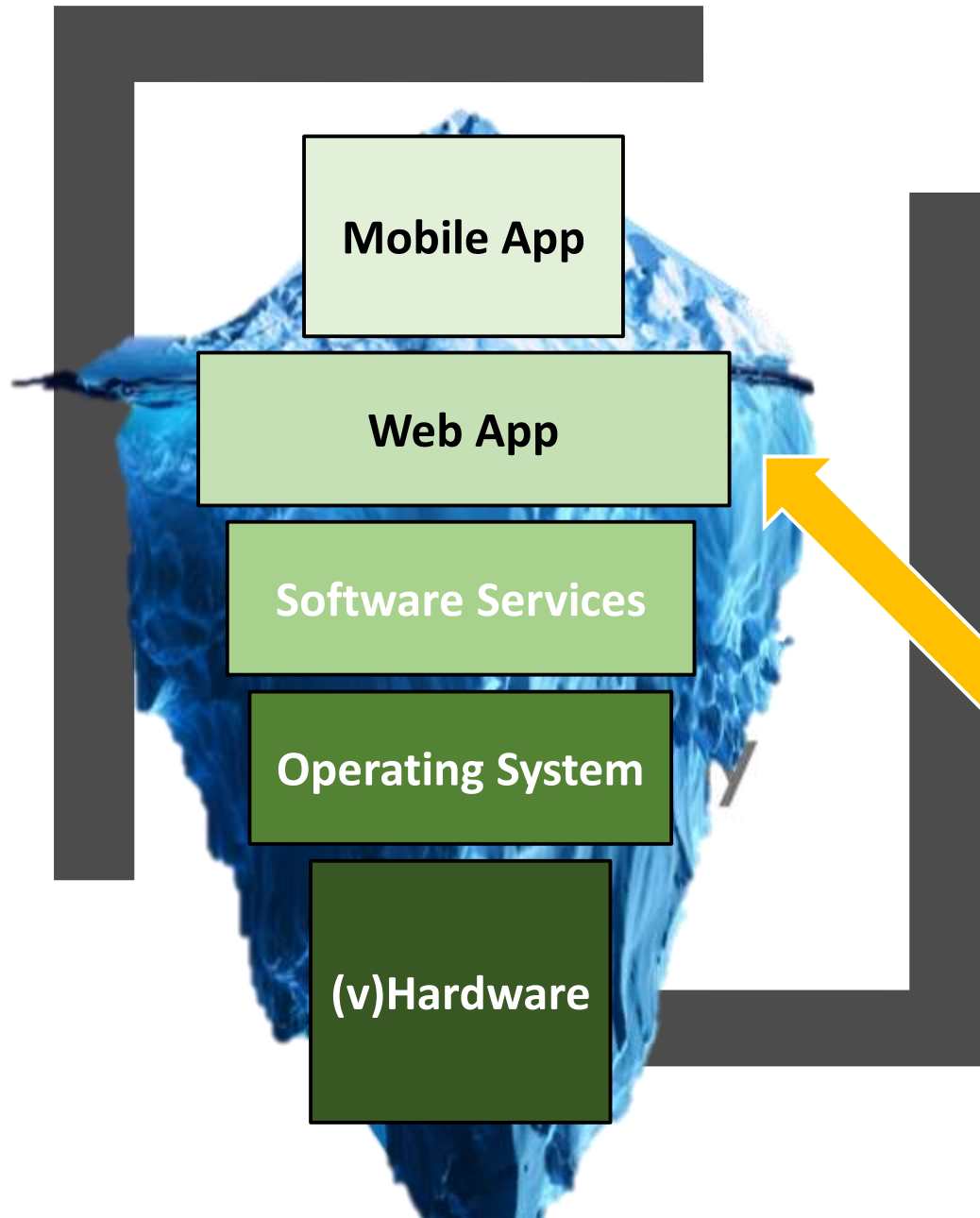
Software Services

Operating System

(v)Hardware

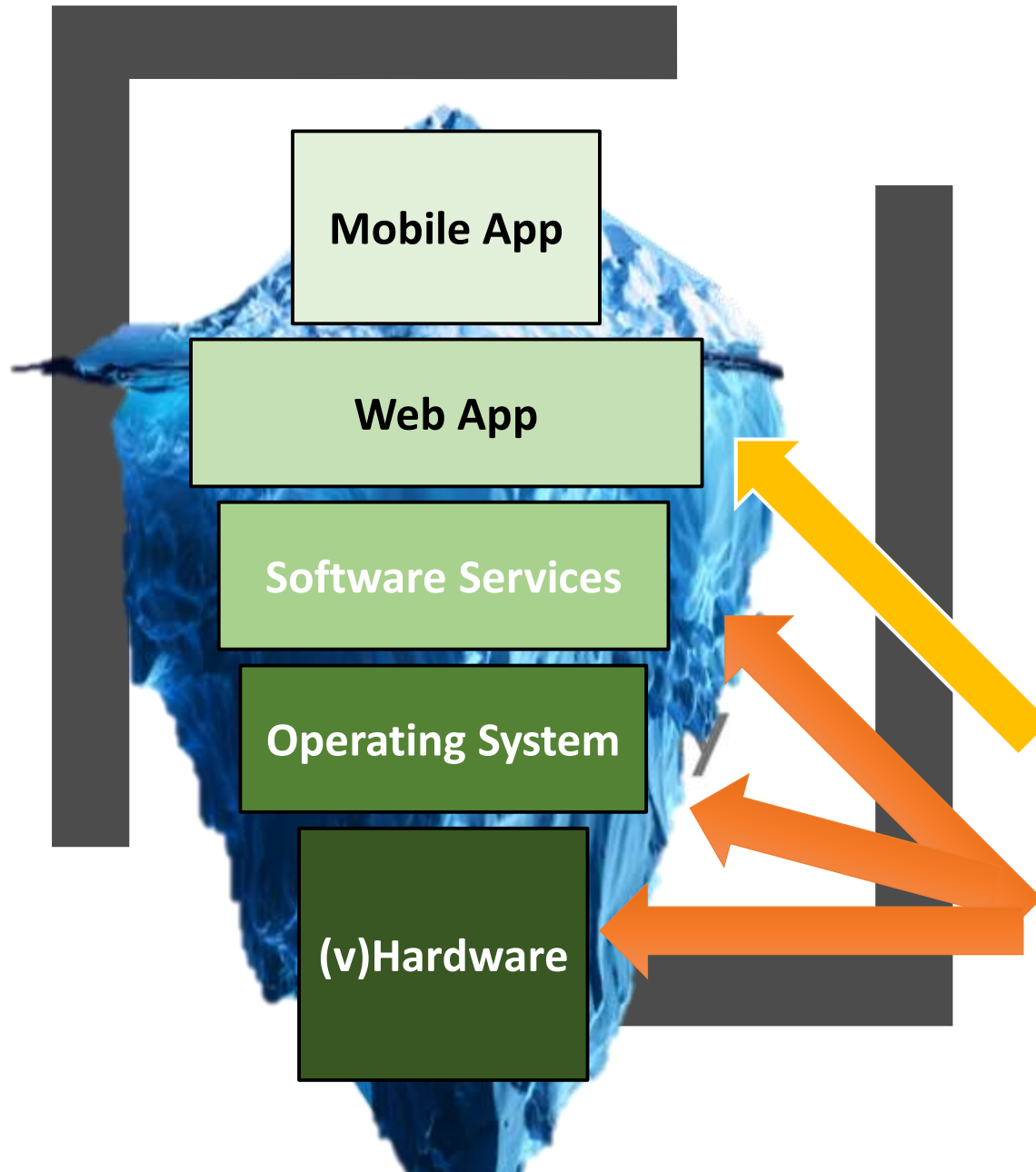
Google Play Store

- Top 5,000 apps from August 2018
- We found
 - Over **600 0-DAY**
 - Over **900 N-DAY**



Google Play Store

- Top 5,000 apps from August 2018
- We found
 - Over **600 0-DAY**
 - Over **900 N-DAY**
- 0-day vulnerabilities affect web apps



Google Play Store

- Top 5,000 apps from August 2018
- We found
 - Over **600 0-DAY**
 - Over **900 N-DAY**
- 0-day vulnerabilities affect web apps
- N-day affects software below the web apps

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		<i>Operating System</i>	<i>Software Services</i>	<i>Web App (API)</i>	<i>Comm. Services</i>	Total	<i>First-Party</i>	<i>Third-Party</i>	<i>Hybrid</i>	<i>Unknown</i>	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		Operating System	Software Services	Web App (API)	Comm. Services	Total	First-Party	Third-Party	Hybrid	Unknown	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Over 1,600 Vulnerability Instances

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		<i>Operating System</i>	<i>Software Services</i>	<i>Web App (API)</i>	<i>Comm. Services</i>	Total	<i>First-Party</i>	<i>Third-Party</i>	<i>Hybrid</i>	<i>Unknown</i>	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		Operating System	Software Services	Web App (API)	Comm. Services	Total	First-Party	Third-Party	Hybrid	Unknown	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Over 600 ZERO-DAYS!

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		<i>Operating System</i>	<i>Software Services</i>	<i>Web App (API)</i>	<i>Comm. Services</i>	Total	<i>First-Party</i>	<i>Third-Party</i>	<i>Hybrid</i>	<i>Unknown</i>	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		Operating System	Software Services	Web App (API)	Comm. Services	Total	First-Party	Third-Party	Hybrid	Unknown	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Audited over 9,000 backends

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		<i>Operating System</i>	<i>Software Services</i>	<i>Web App (API)</i>	<i>Comm. Services</i>	Total	<i>First-Party</i>	<i>Third-Party</i>	<i>Hybrid</i>	<i>Unknown</i>	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

Overall Vulnerabilities

Category	# Mob. Apps	Vulnerabilities By Layer					Backend Labels				
		Operating System	Software Services	Web App (API)	Comm. Services	Total	First-Party	Third-Party	Hybrid	Unknown	Total
Books & Reference	332	15	49	55	71	190	365	653	501	354	1,873
Business	145	5	22	10	37	74	93	258	150	113	614
Entertainment	1,177	36	108	158	170	472	746	913	942	783	3,384
Games	1,283	34	81	147	106	368	290	804	651	444	2,189
Lifestyle	363	20	50	79	72	221	262	665	311	237	1,475
Misc	199	6	21	45	46	118	76	422	163	105	766
Tools	792	19	84	184	115	402	729	796	812	464	2,801
Video & Audio	689	24	46	89	98	257	267	648	434	357	1,706
Total	4,980	121	356	655	506	1,638	2,492	1,089	3,336	2,506	9,423

**Over 1,000 third-party backends.
Used by multiple mobile apps!**

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App	XSS (various)	262
	SQLi (various)	160
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

BEWARE: Can Install Malicious Apps Through Redirection

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Vulnerabilities

Layer	Vulnerability (Top 3)	#Apps
Operating System	Expired Lifecycle for Linux OS (various)	124
	Windows Server RCE (MS15-034)	64
	Expired Lifecycle for Windows Server	9
Software Services	Vulnerable PHP Version	357
	Expired Lifecycle for Web Server (various)	181
	Vulnerable Apache Version	76
Web App (API)	XSS (various)	262
	SQLi (various)	160
	XXE (various)	86
Comm. Services	Support for Vulnerable SSL Version 2 and 3	997
	OpenSSH Bypass (CVE-2015-5600)	16
	Vulnerable OpenSSL (various)	15

Top Zero-Day Vulnerabilities

# Installs	# Apps	# SQLi	# XSS	# XXE
1B	5	0	0	0
500M	11	0	0	0
100M	116	0	3	1
50M	131	4	10	5
10M	1,049	25	85	15
5M	1,047	54	89	9
1M	2,621	132	316	17

Top Zero-Day Vulnerabilities

# Installs	# Apps	# SQLi	# XSS	# XXE
1B	5	0	0	0
500M	11	0	0	0
<u>100M</u>	116	0	3	1
50M	131	4	10	5
10M	1,049	25	85	15
5M	1,047	54	89	9
1M	2,621	132	316	17

Top Zero-Day Vulnerabilities

# Installs	# Apps	# SQLi	# XSS	# XXE
1B	5	0	0	0
500M	11	0	0	0
<u>100M</u>	116	0	3	1
50M	131	4	10	5
10M	1,049	25	85	15
5M	1,047	54	89	9
1M	2,621	132	316	17

<https://MobileBackend.vet>



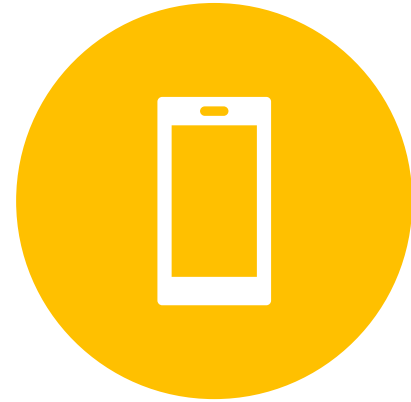
What's Next?



NOTIFICATION



WORKING WITH 3RD
PARTY LIBRARIES



IMPACT ON APP USERS

Related Work

- Backes et al., “Reliable third-party library detection in android and its security applications,” *ACM CCS*, Oct. 2016.
- Arzt et al., “Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps,” *ACM SIGPLAN PLDI*, 2014.
- You et al., “Semfuzz: Semantics-based automatic generation of proof-of-concept exploits,” *ACM CCS*, 2017.
- Durumeric et al., “Zmap: Fast internet-wide scanning and its security applications.,” *USENIX Security*, 2013.
- Li et al., “You’ve got vulnerability: Exploring effective vulnerability notifications,” *USENIX Security*, 2016.
- Durumeric et al., “The matter of heartbleed,” *IMC*, 2014
- Ristenpart et al., “Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds,” *ACM CCS*, 2009.
- Sun et al., “Pileus: Protecting user resources from vulnerable cloud services,” *ACSAC*, 2016.
- Durumeric et al., “Analysis of the https certificate ecosystem,” *IMC*, 2013.
- Fernandes et al., “Security analysis of emerging smart home applications,” *IEEE S&P*, May 2016.



Thank you –
Questions?

Omar Alrawi

alrawi@gatech.edu

<https://alrawi.io>



Recommendation

- Delegate
 - Use reputable 3rd party services
- Dedicate
 - Time and personal to secure development
- Develop
 - A plan to for incidents: backup data, backup providers, etc.
- Defense
 - Use WAFs and CDNs PROPERLY!



Unknown Category

- Backend domains with different effective second-level domain
- Missing registration information
- Privacy WHOIS
- IP address show up as delegated
- IP address in collocation facility, but maybe hosting reseller
- CDNs fronted (can overcome with pDNS)

