

A man wearing a straw hat, glasses, a dark sweater, and a yellow backpack is standing on a train platform. He is looking down at a smartphone in his hands. The background shows train tracks and a platform with a red railing. The image has a blue and purple color overlay.

All your money belongs to us (me)



- ▶ WannaCry
- ▶ KRACK
- ▶ Meltdown
- ▶ Spectre
- ▶ EFAIL



# Agenda

---

- Why?
- How?
- What?



# Let's hack a tesla



<https://youtu.be/5jQAX4540hA>

# Let's hack a banking app

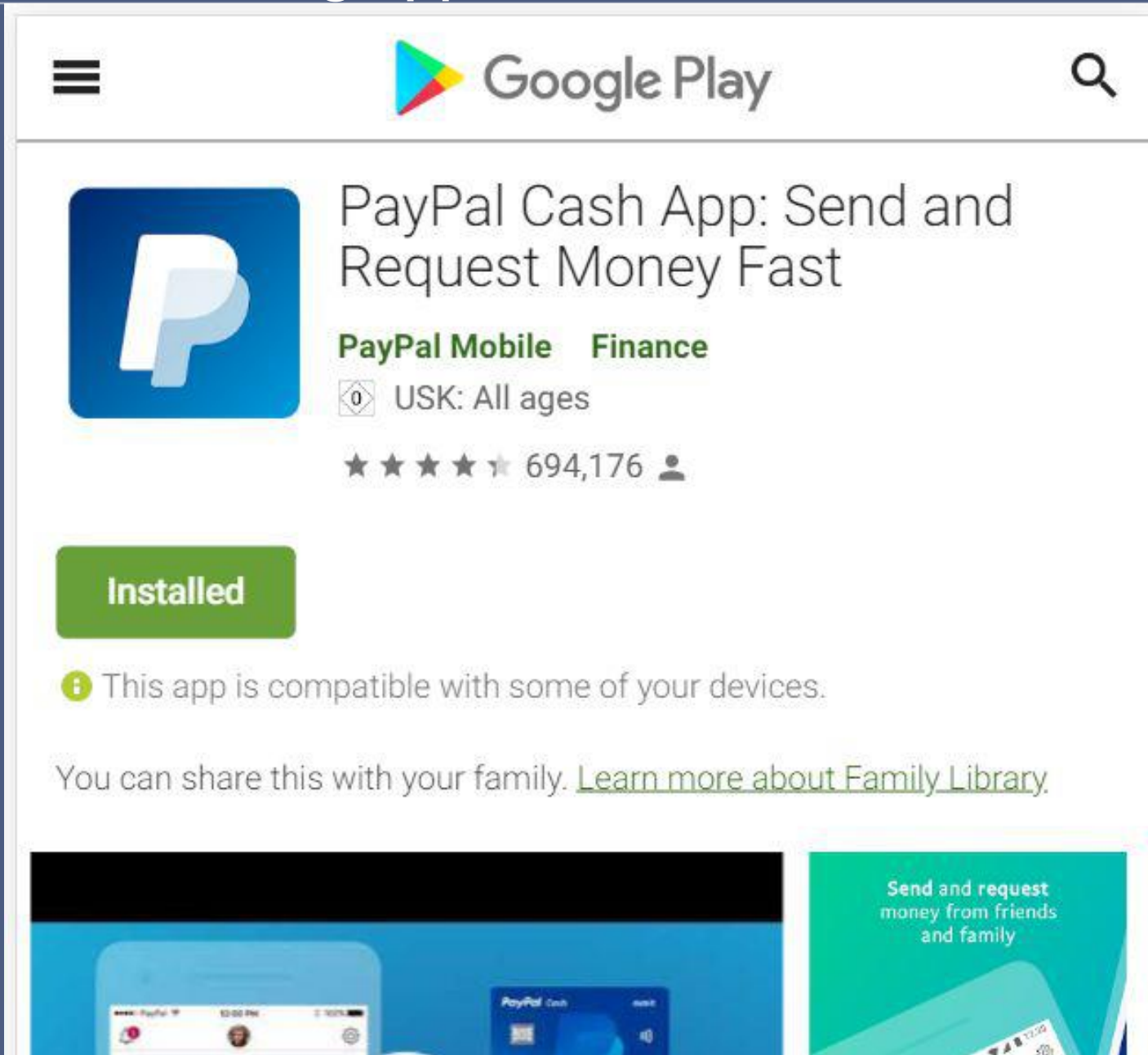


# Let's hack another banking app

---




# Let's hack another banking app



The image shows a screenshot of the Google Play Store interface. At the top, there is a navigation bar with a hamburger menu icon on the left, the Google Play logo in the center, and a search icon on the right. Below the navigation bar, the app listing for "PayPal Cash App: Send and Request Money Fast" is displayed. The app icon is a blue square with a white "P" logo. The title "PayPal Cash App: Send and Request Money Fast" is in a large, dark font. Below the title, the developer "PayPal Mobile" and the category "Finance" are listed. The app is rated "USK: All ages" and has a rating of 4.5 stars from 694,176 reviews. A green "Installed" button is visible. Below the button, there is a compatibility note: "This app is compatible with some of your devices." and a link to "Learn more about Family Library". At the bottom, there are two preview images: one showing the app's interface on a smartphone and another showing a promotional graphic with the text "Send and request money from friends and family".

☰ Google Play 🔍

 PayPal Cash App: Send and Request Money Fast

PayPal Mobile Finance

USK: All ages

★★★★☆ 694,176

**Installed**

*i* This app is compatible with some of your devices.

You can share this with your family. [Learn more about Family Library](#).

Send and request money from friends and family



**DEMO**

**DEMO**



A hand holding a red loyalty card in front of a laptop displaying a website with a 'UP TO 70% OFF' promotion.

**Is it really that bad?**

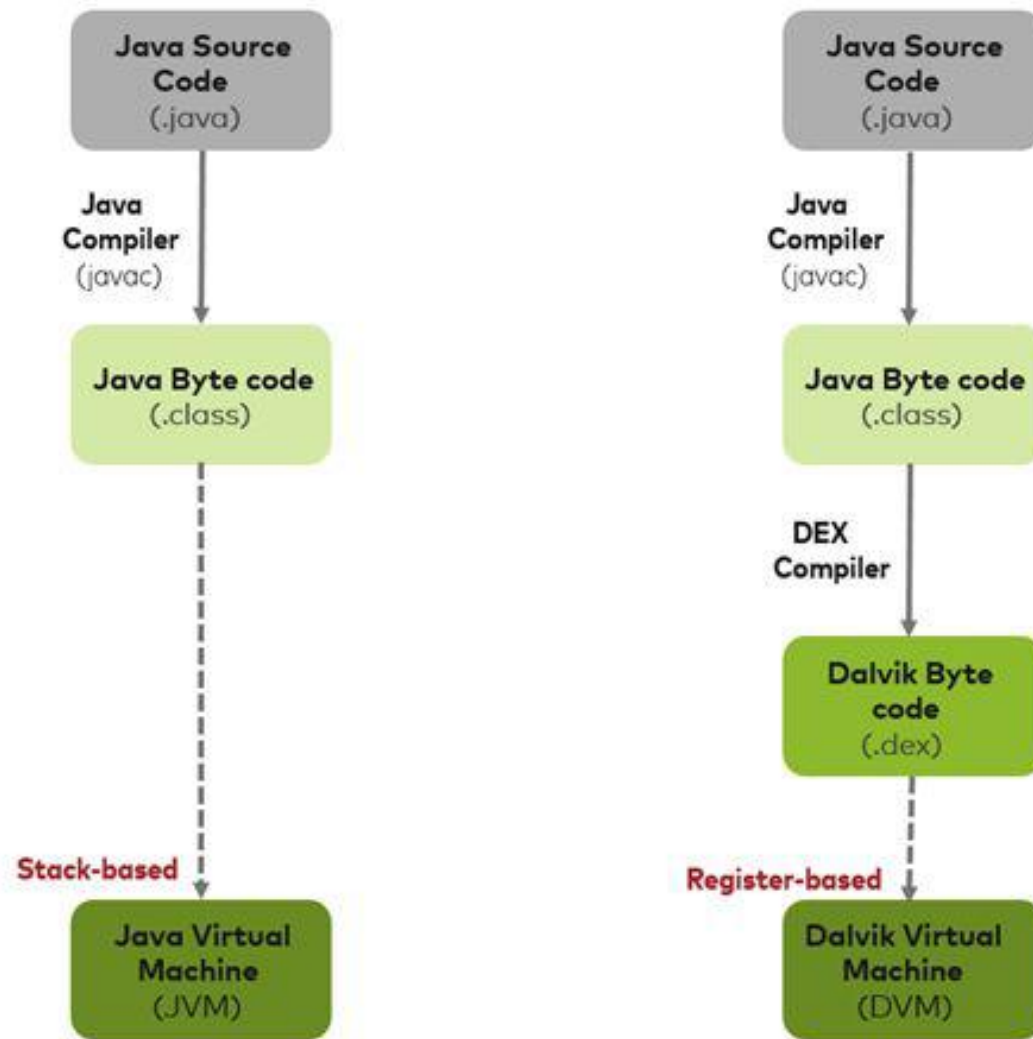
# What did just happen?

---

- ▶ Transfer money receiver was modified during runtime
- ▶ Code Injection Framework (Xposed)
  - ▶ Root access needed -> Device compromised



# How did I do it?



## JVM vs DVM

# How did I do it?

---

- ▶ What do I want to achieve?
  - ▶ All your money belongs to me
- ▶ Decompile Paypal app
- ▶ Understand rough structure
- ▶ Find appropriate classes to modify during runtime
  - ▶ “SendMoney” sounds like a good string to search for



# How did I do it?

---



# How to deal with it

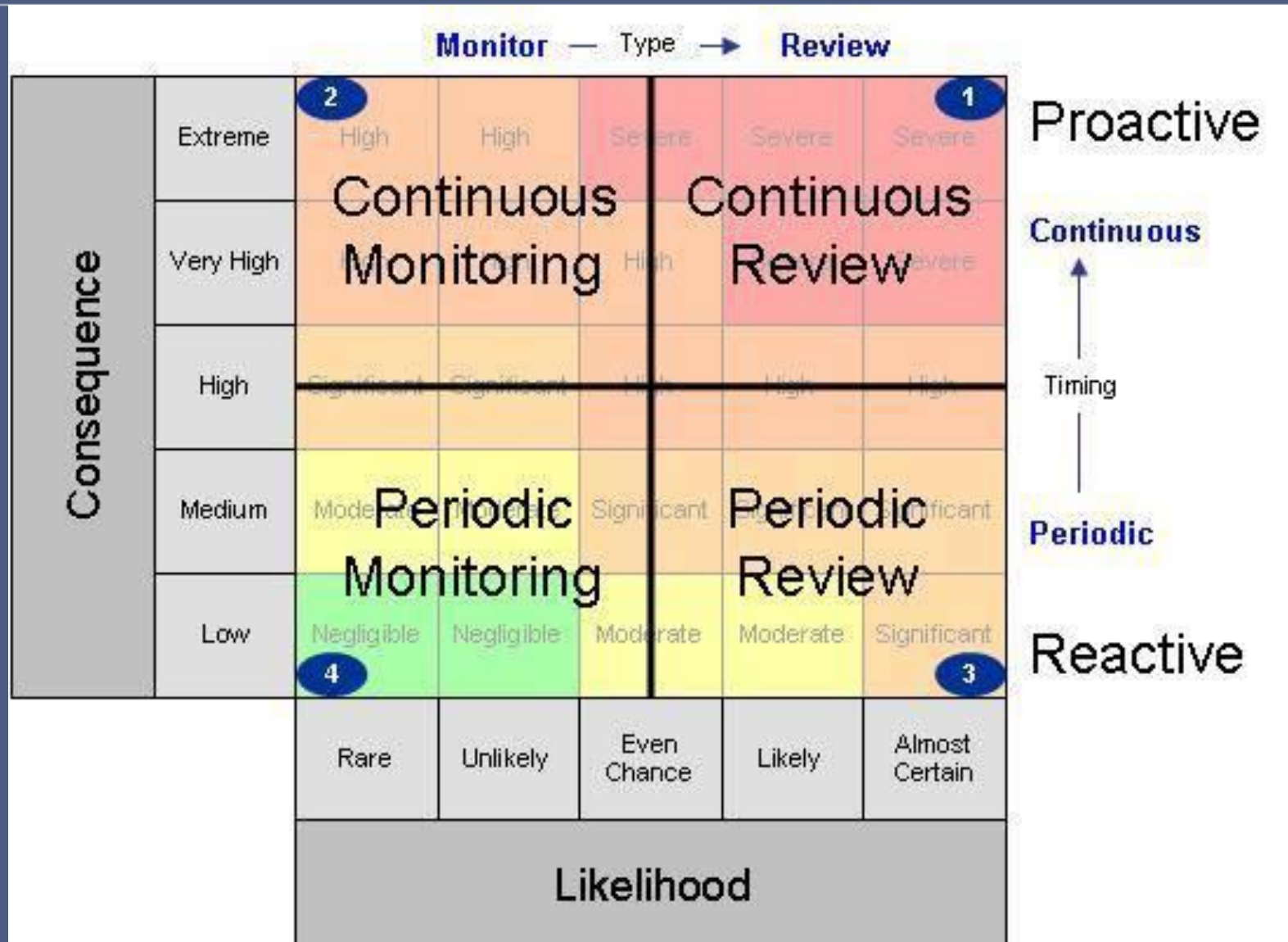
---

- ▶ Risk probability?
- ▶ Risk impact?
- ▶ Is the hack scaleable?





# How to deal with it



# How to deal with it

---

- ▶ Prepare beforehand
  - ▶ Potential hacks?
  - ▶ Audit from a security company
- ▶ Prepare PR/Marketing with input from developers
- ▶ Please update your Phones :)



# LINKS

<https://www.youtube.com/watch?v=5jQAX4540hA>

<https://www.youtube.com/watch?v=MYAwe-etEU0>

# QUESTIONS