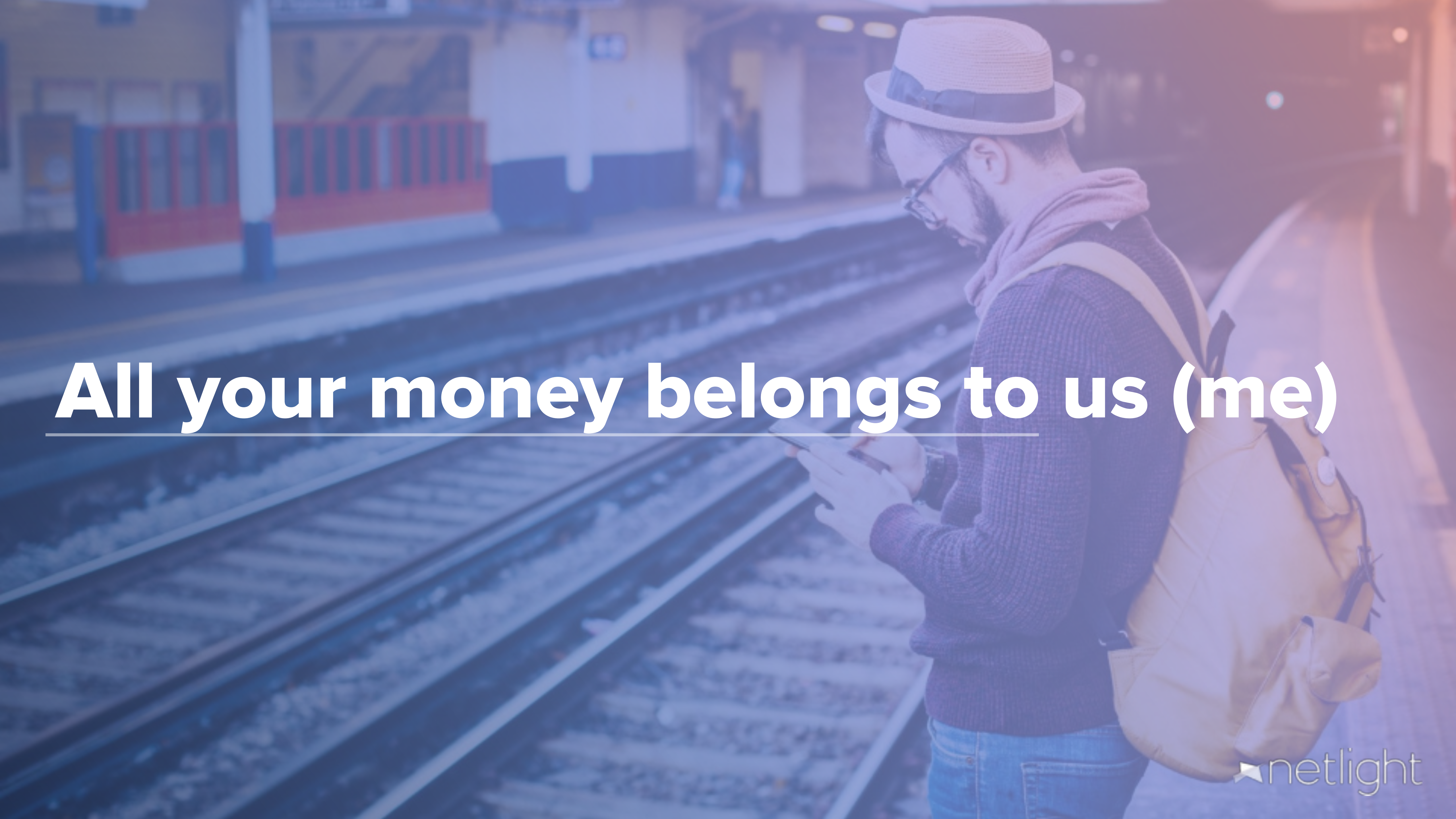


All your money belongs to us (me)

netlight

- WannaCry
- KRACK
- Meltdown
- Spectre
- EFAIL

Agenda

- Why?
- How?
- What?

Let’s hack a tesla

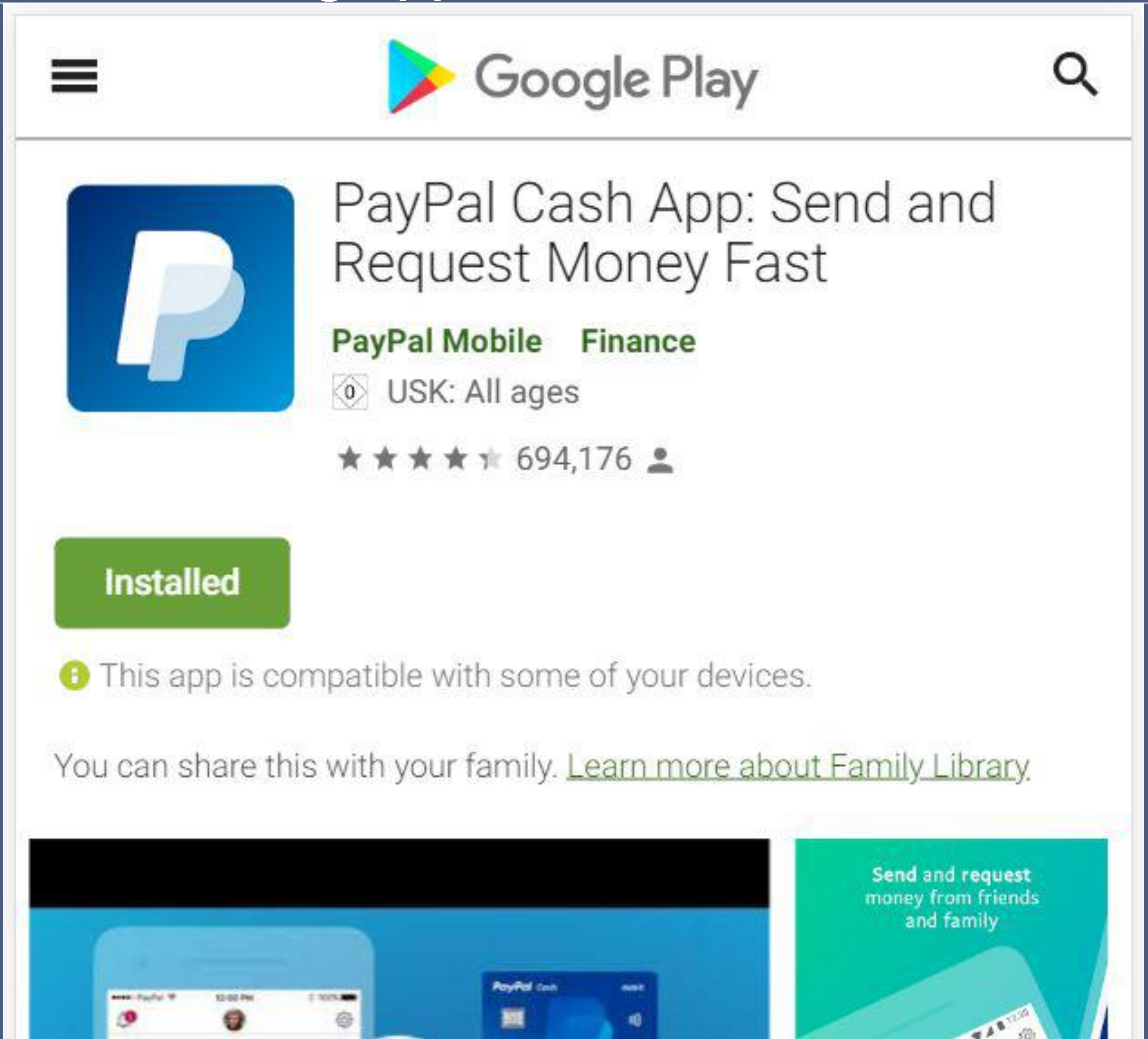
https://youtu.be/5jQAX4540hA

Let’s hack a banking app

https://youtu.be/MYAwe-etEU0

Let’s hack another banking app

Let’s hack another banking app



PayPal Cash App: Send and Request Money Fast

PayPal Mobile Finance

USK: All ages

★★★★½ 694,176

This app is compatible with some of your devices.

You can share this with your family. Learn more about Family Library

DEMO

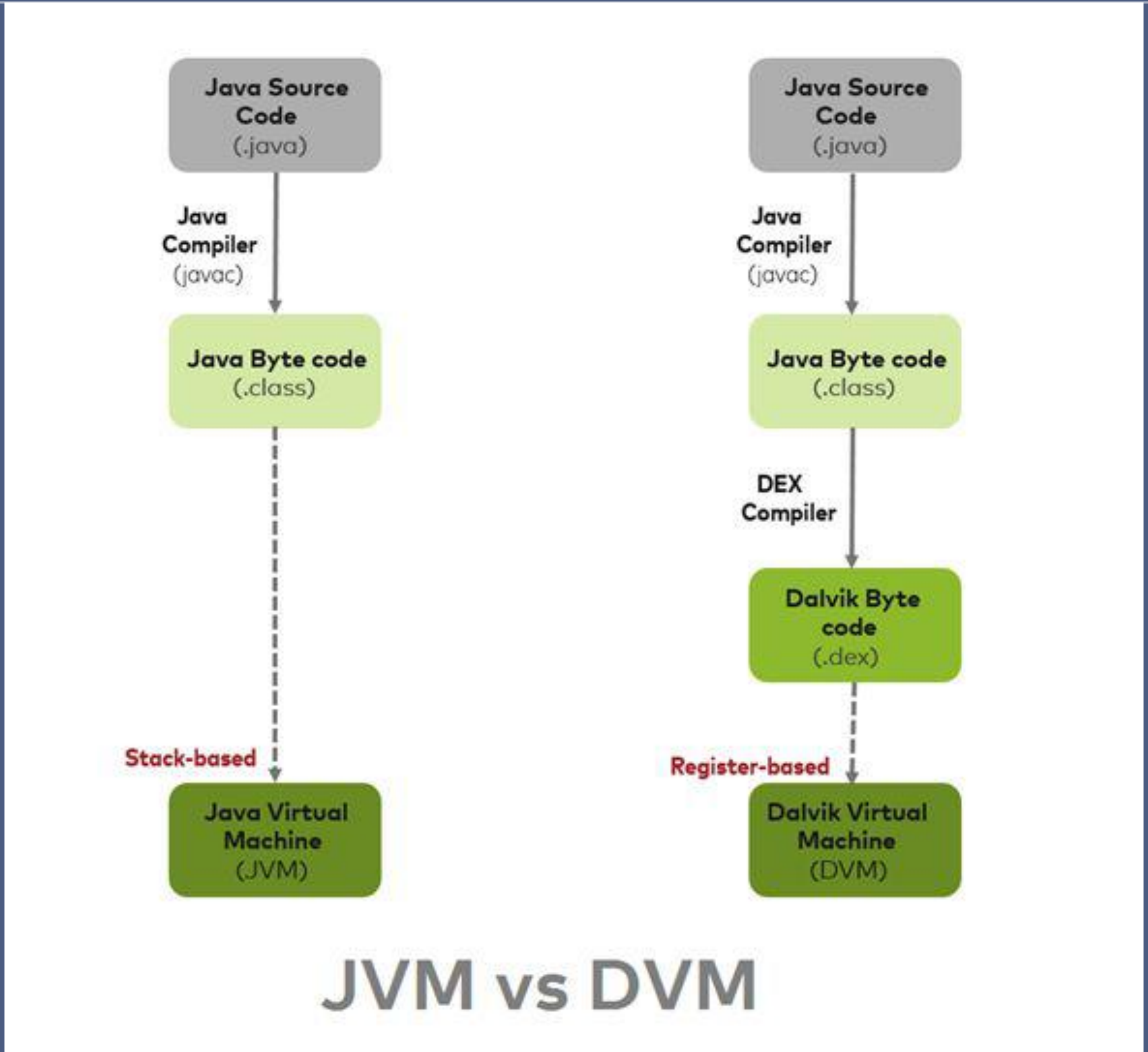
DEMO

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?



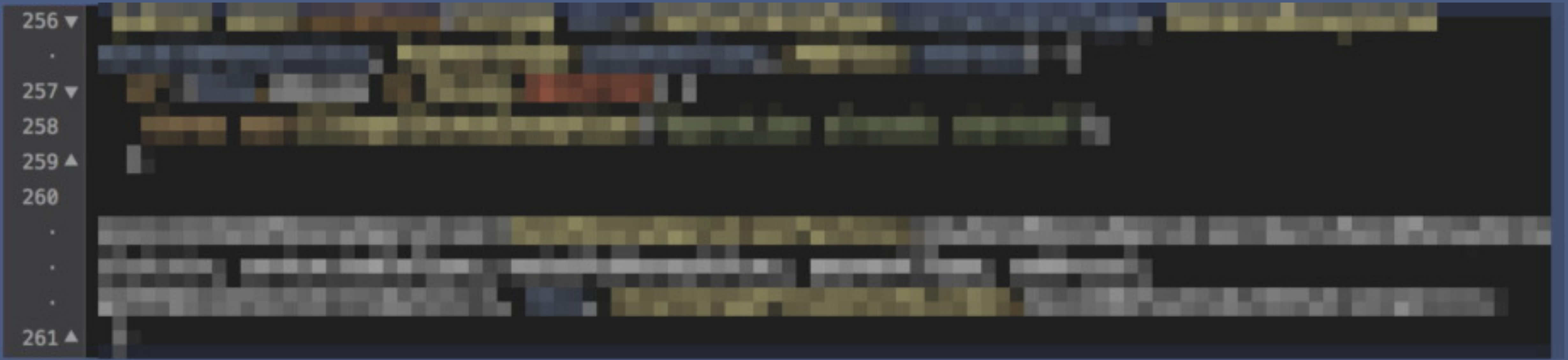
JVM vs DVM

http://bit.ly/2OupfMg

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?

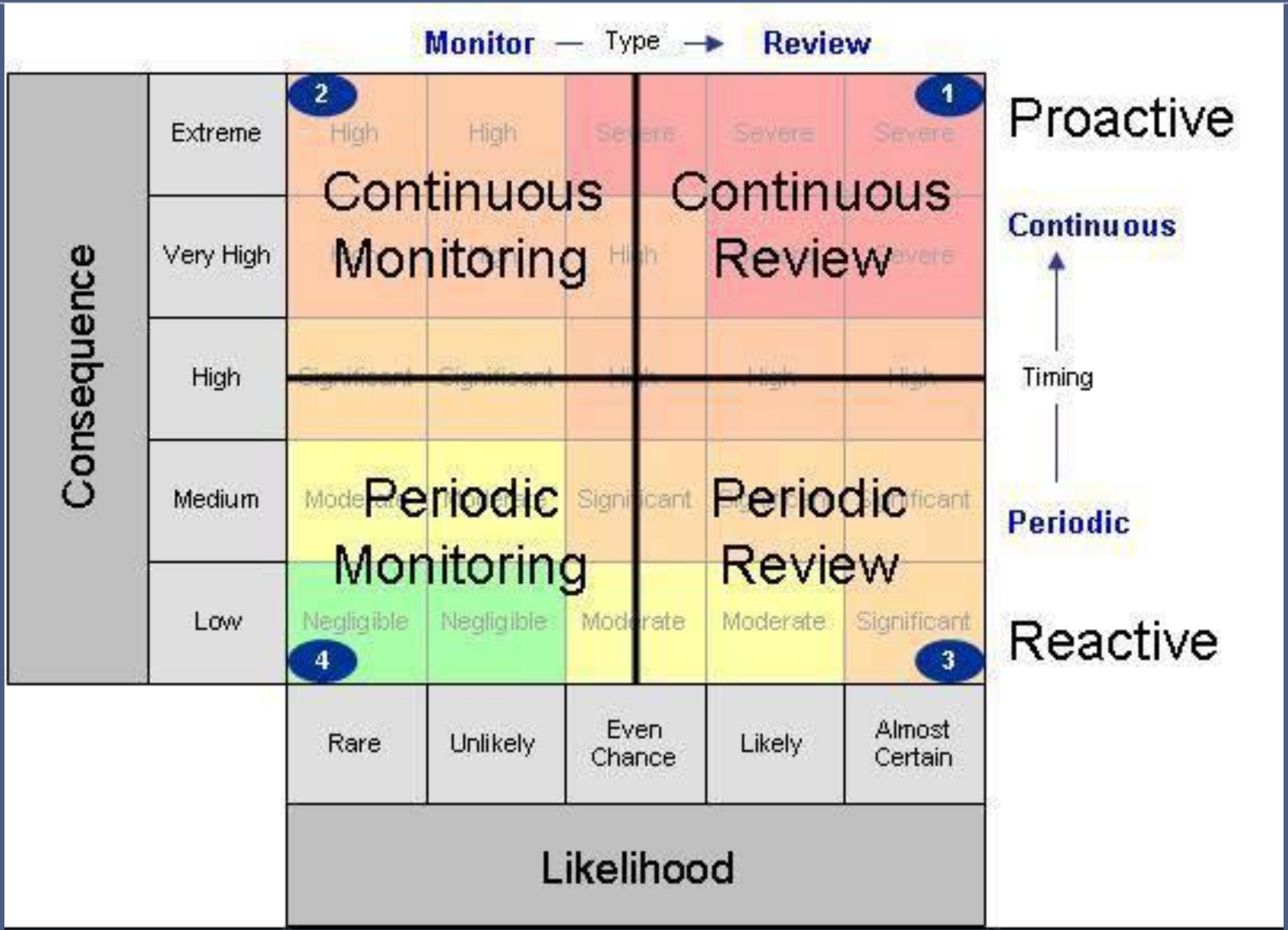


[redacted]

How to deal with it

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

How to deal with it



https://bit.ly/2EBL3Sy

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