

# Взлом и защита Android-приложений



**Данил  
Перевалов**

Циан



@princeparadoxes



**Mobius**  
2023 Spring



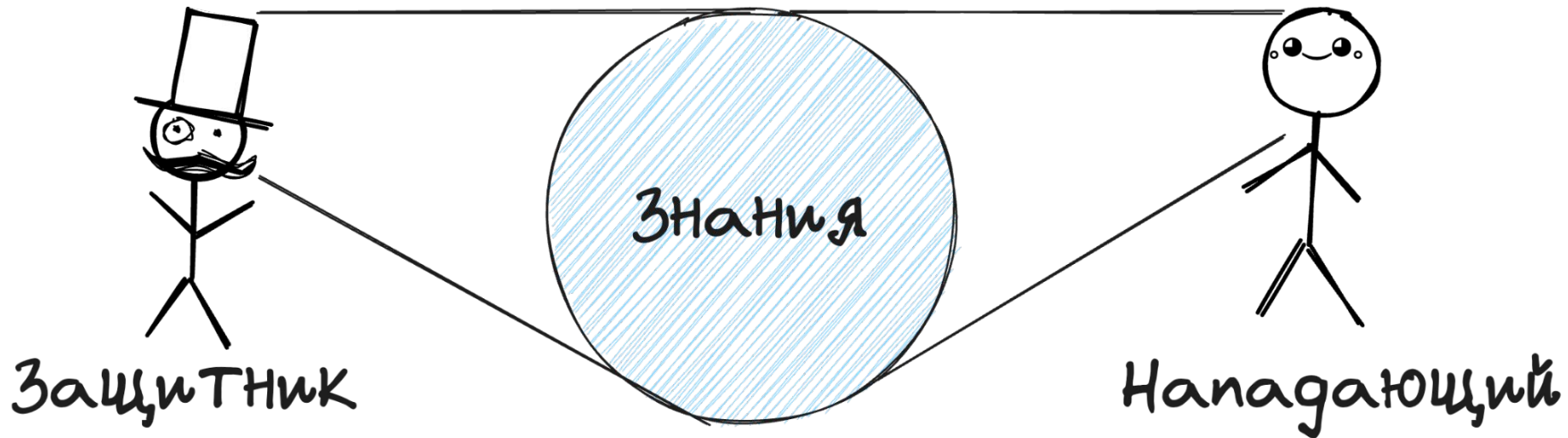
**Циан**

Давайте  
знакомиться  
Данил Перевалов  
Android Developer



# Почему сразу и про взлом, и про защиту?

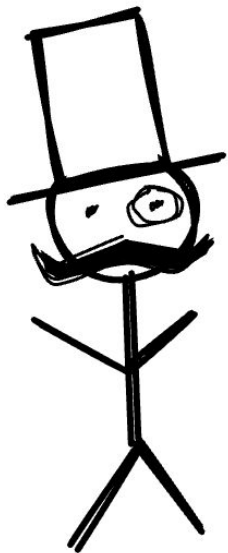
3



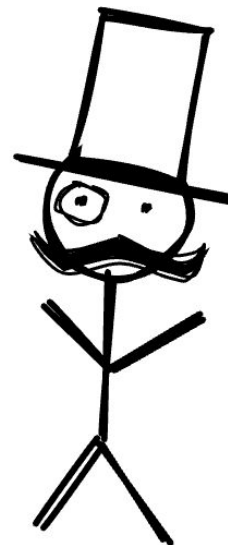
# Я таким не занимаюсь



# Всё ради защиты



Защитник



Защитник

# Про что говорим

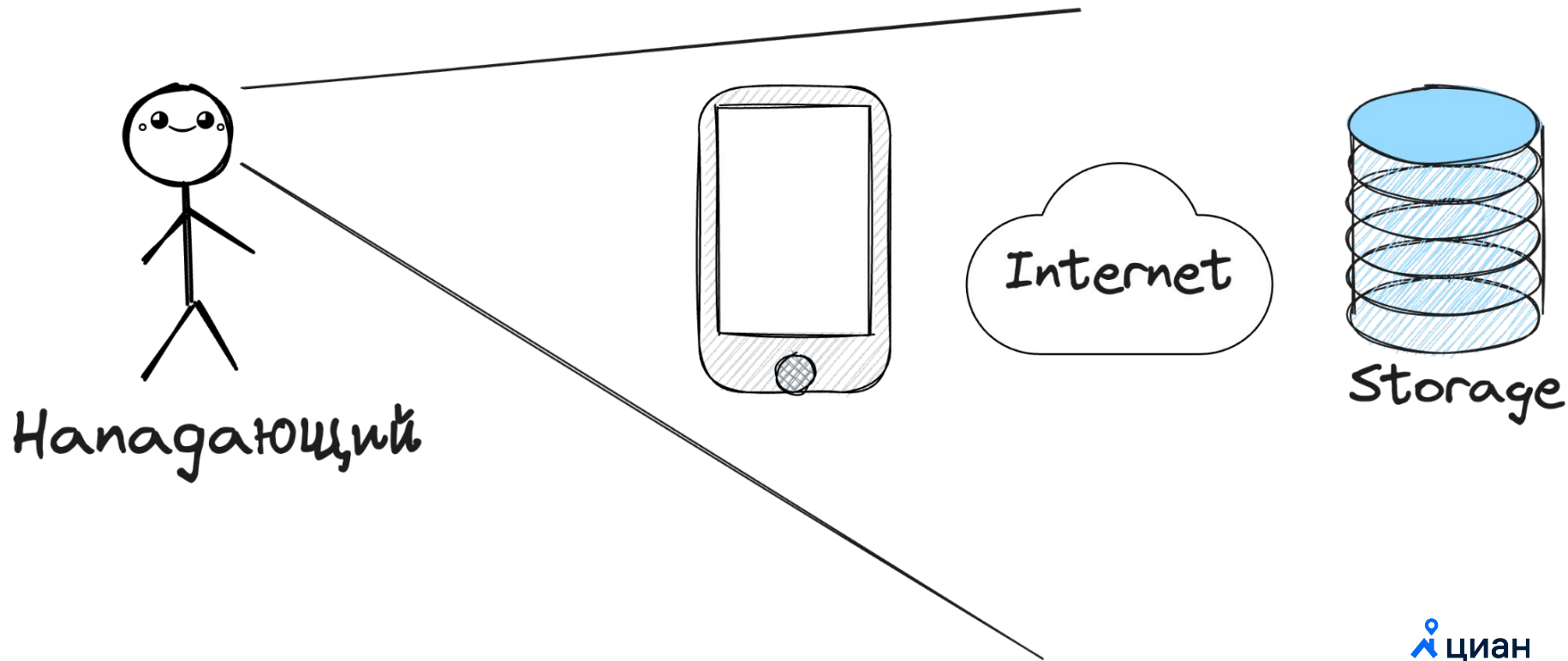
- Процесс внешнего воздействия.
- Процесс внутреннего воздействия.
- Процесс изменение поведения.
- Выводы.



Зачем вообще  
что-то  
взламывать?

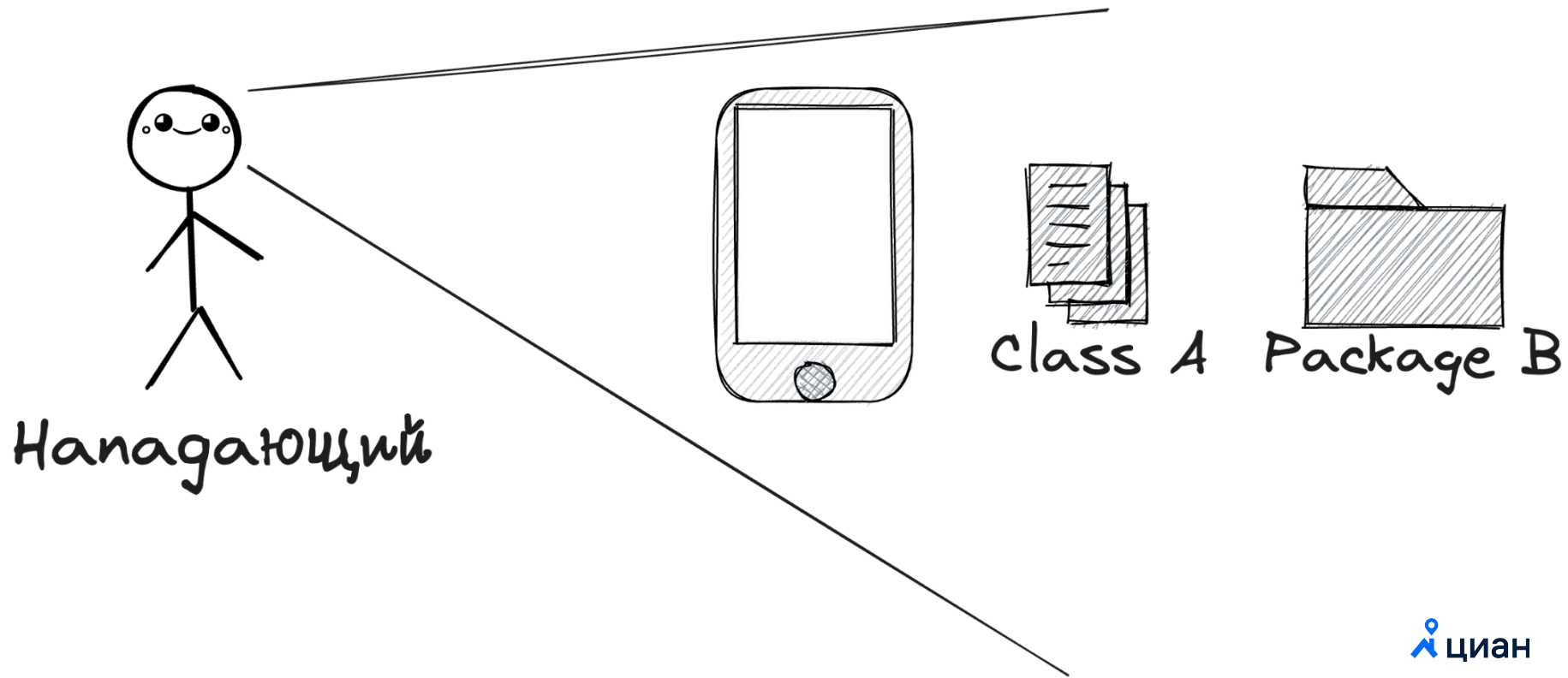


# Посмотреть данные

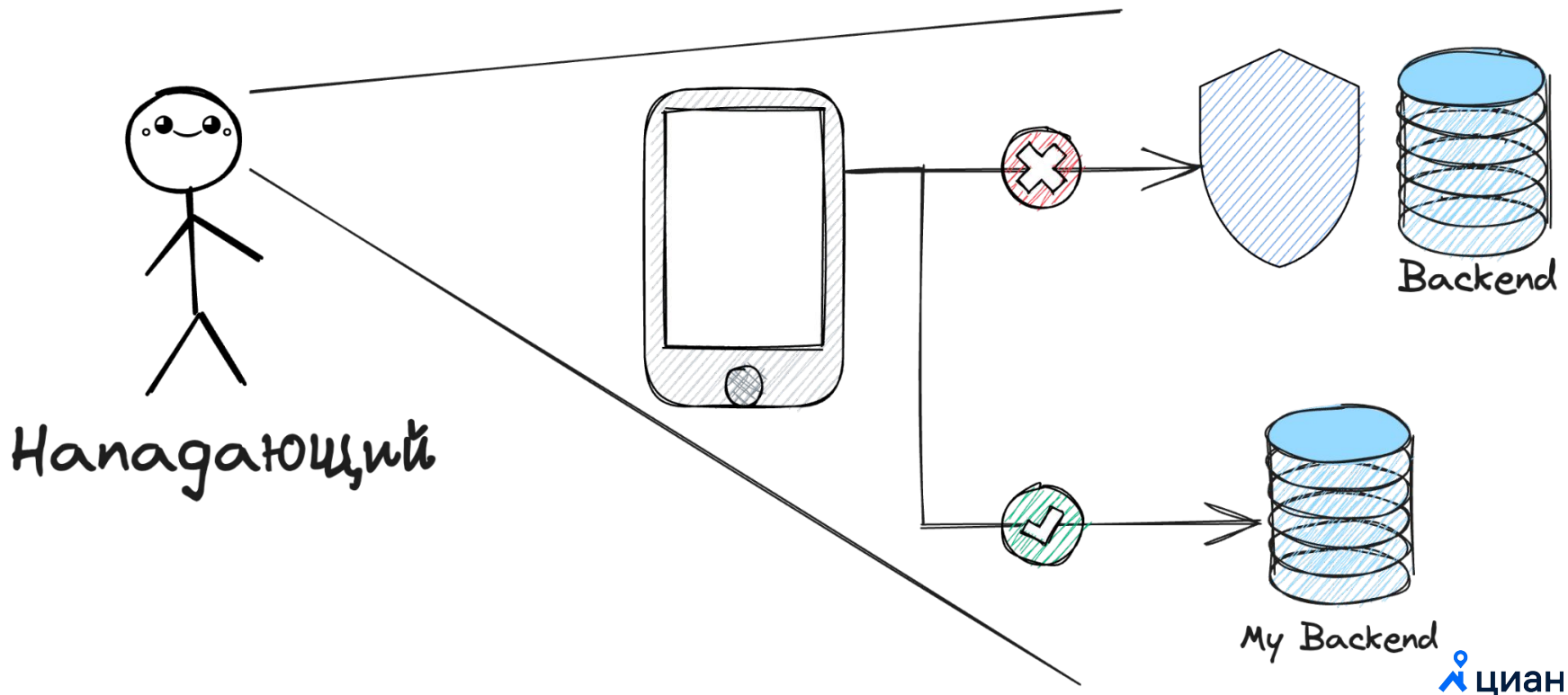


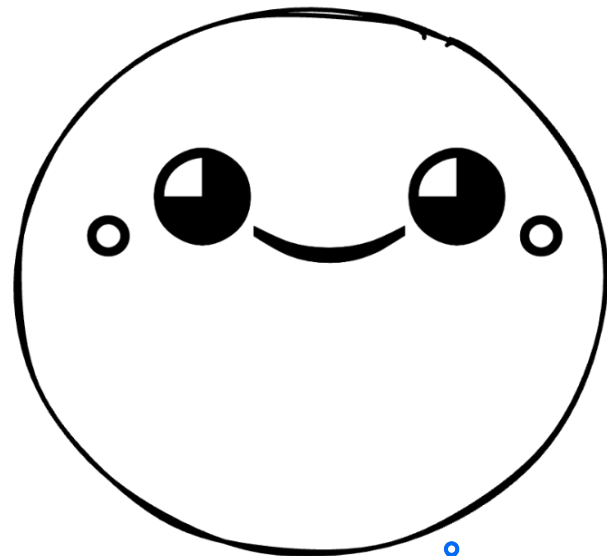
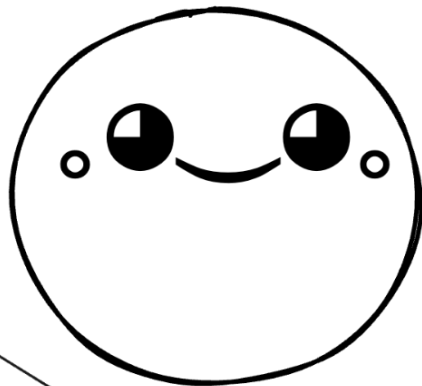
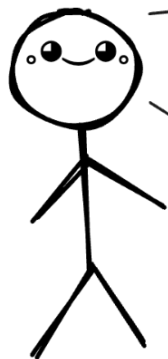


# Узнать, как что-то работает



# Изменить поведение



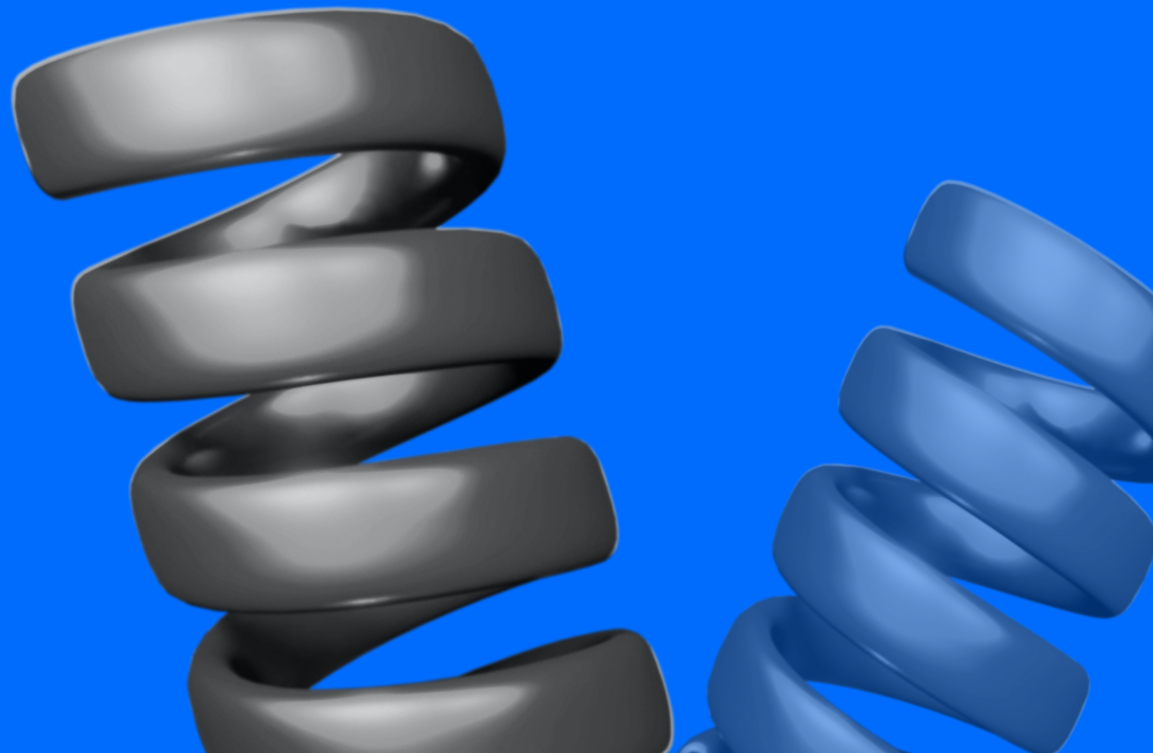


Нападающий

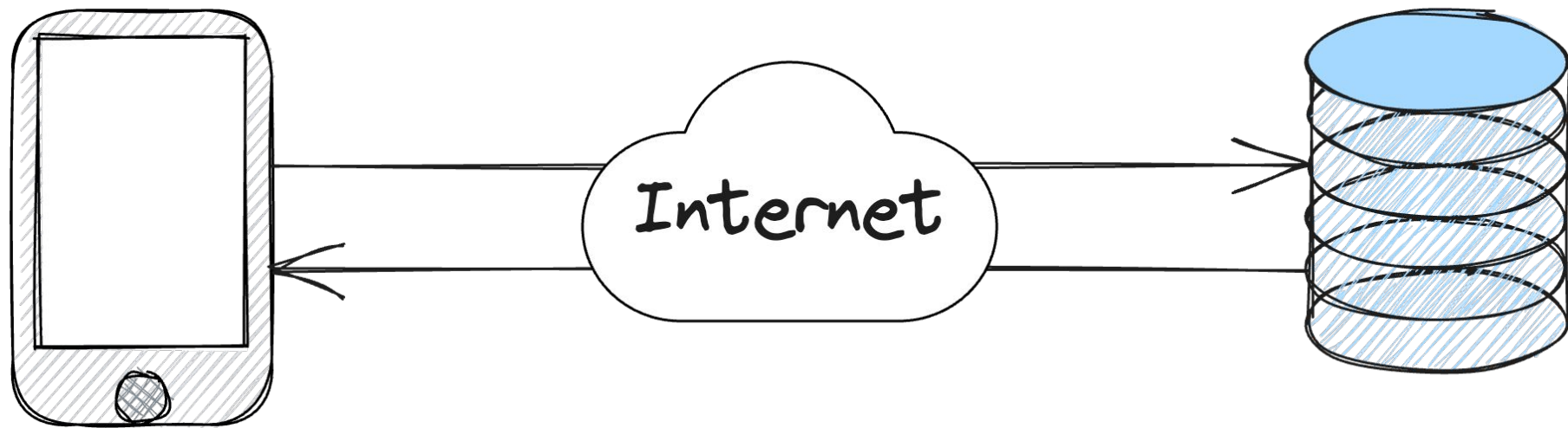
# Просмотр данных



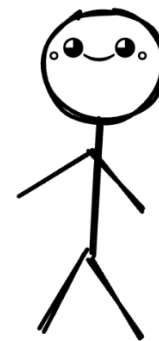
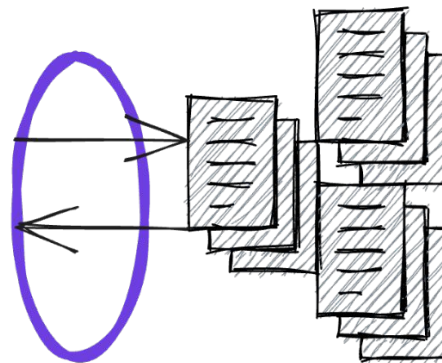
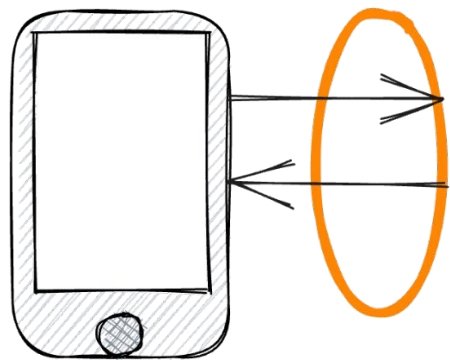
# Сетевой трафик



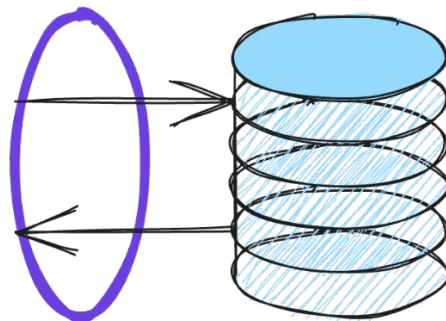
# Общение с сервером



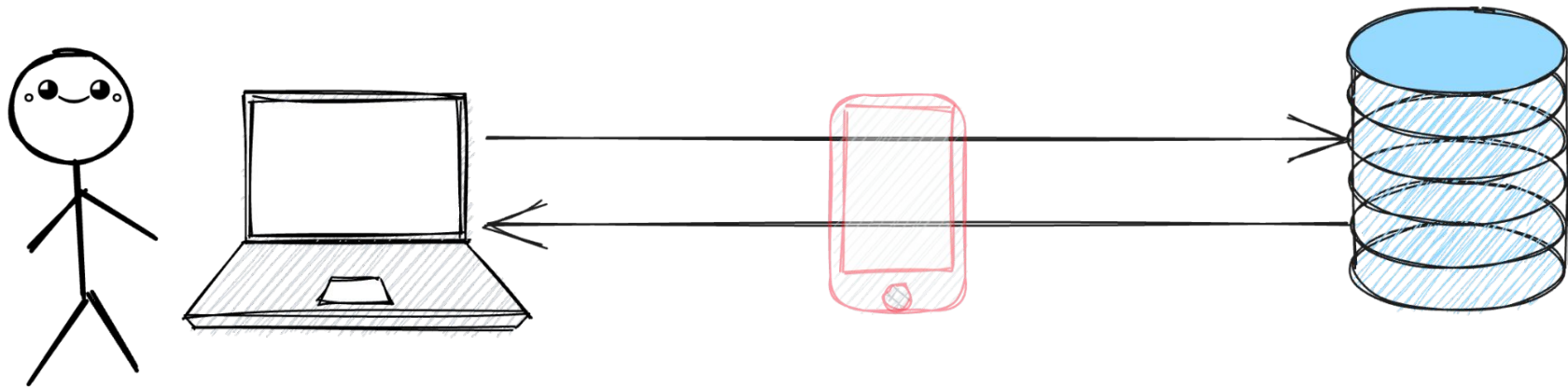
# Что с ним можно сделать? Просмотр данных



Напоминающий



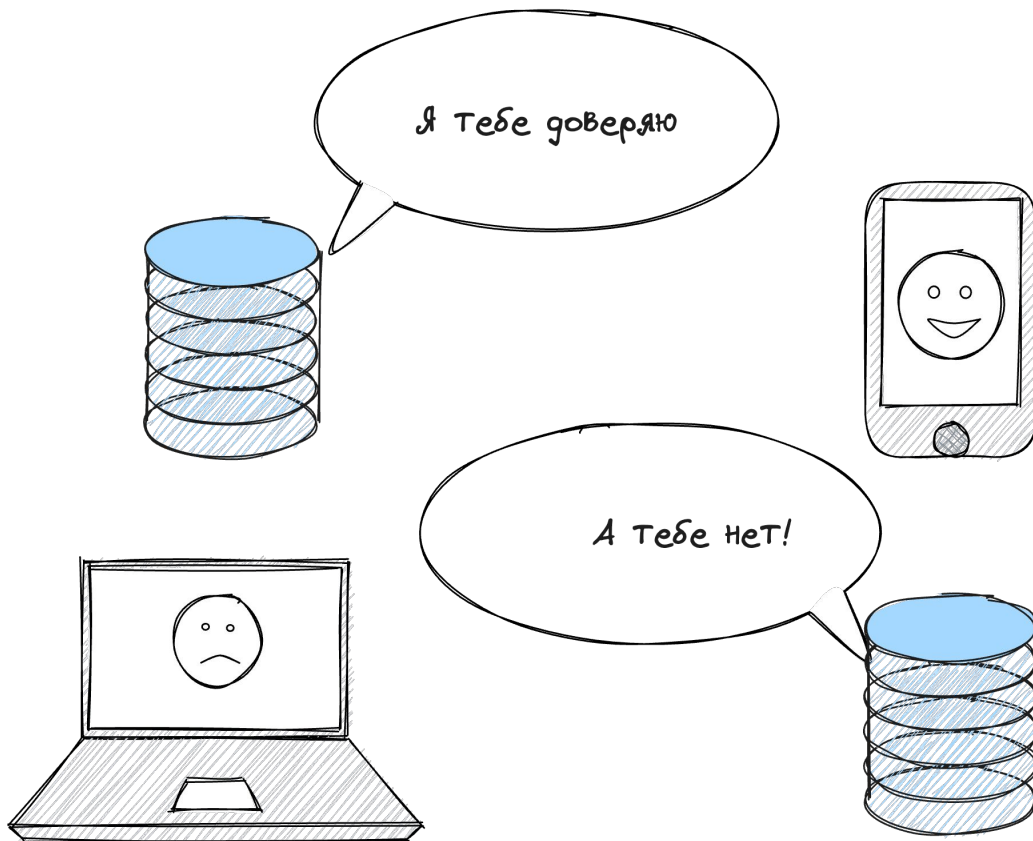
# Что с ним можно сделать? Притворяться



Нападающий



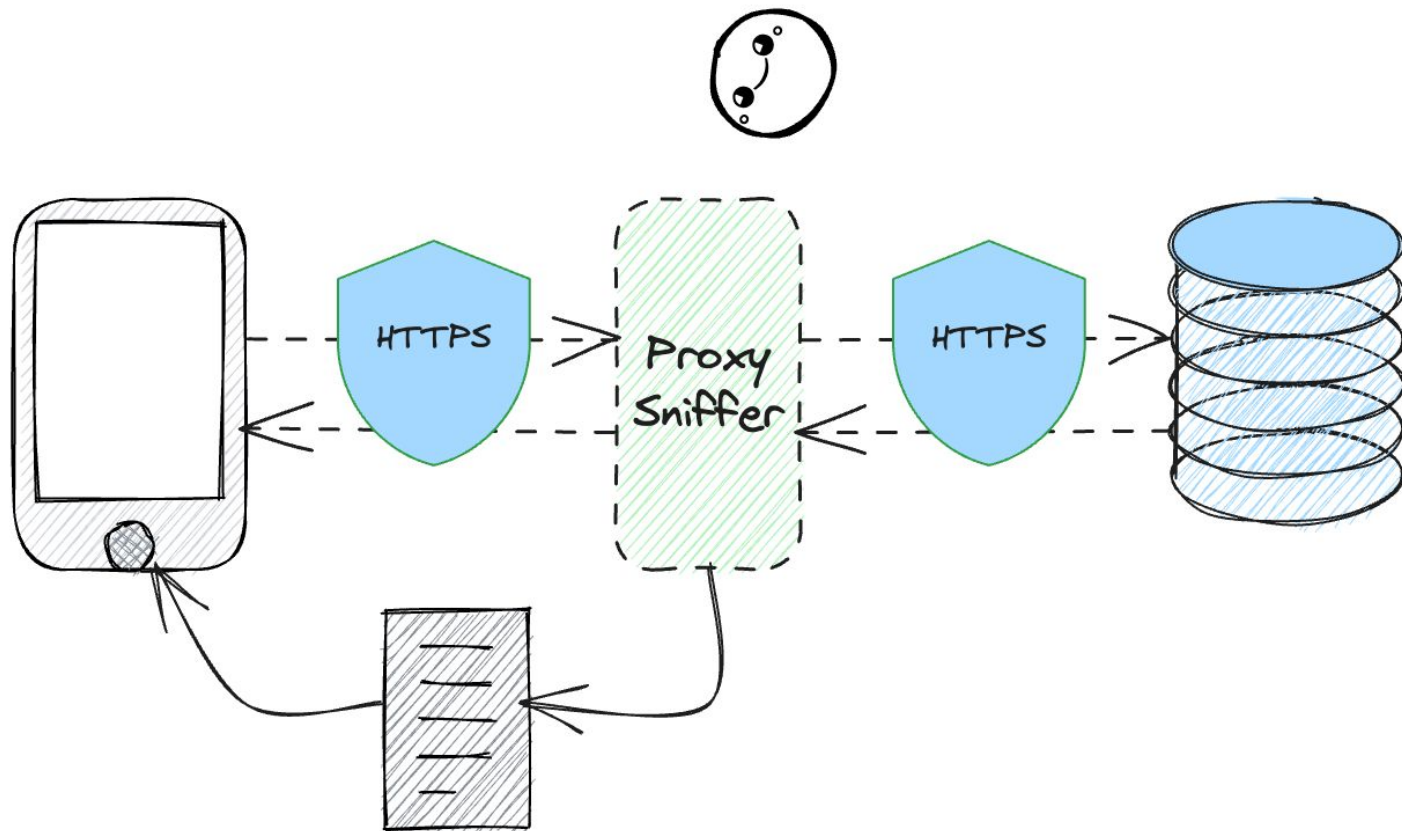
# Почему не Web?





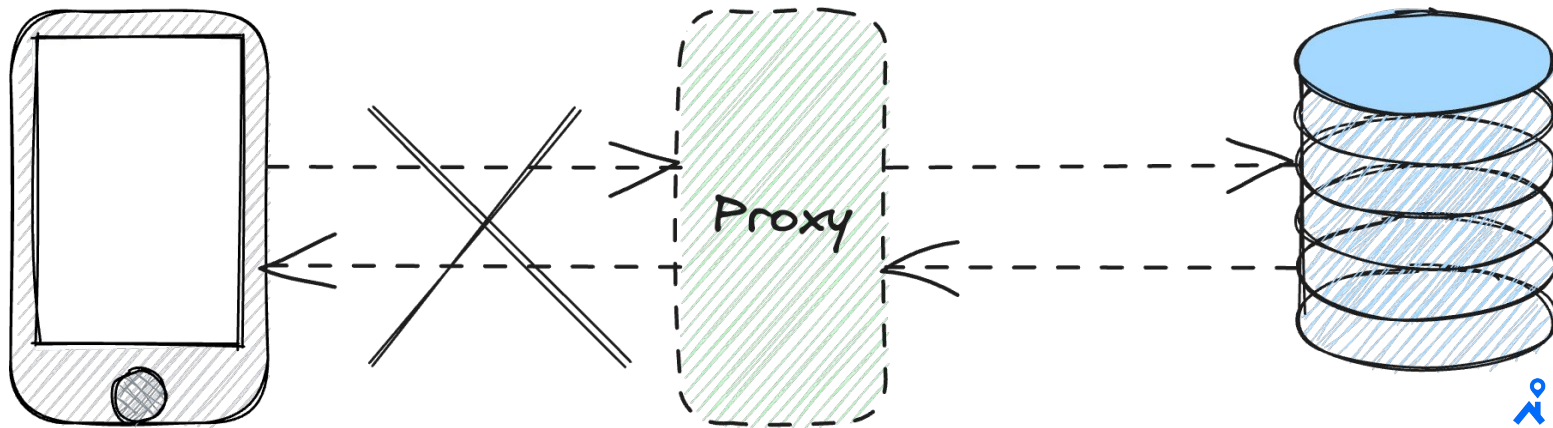
Атака

# Снифферы

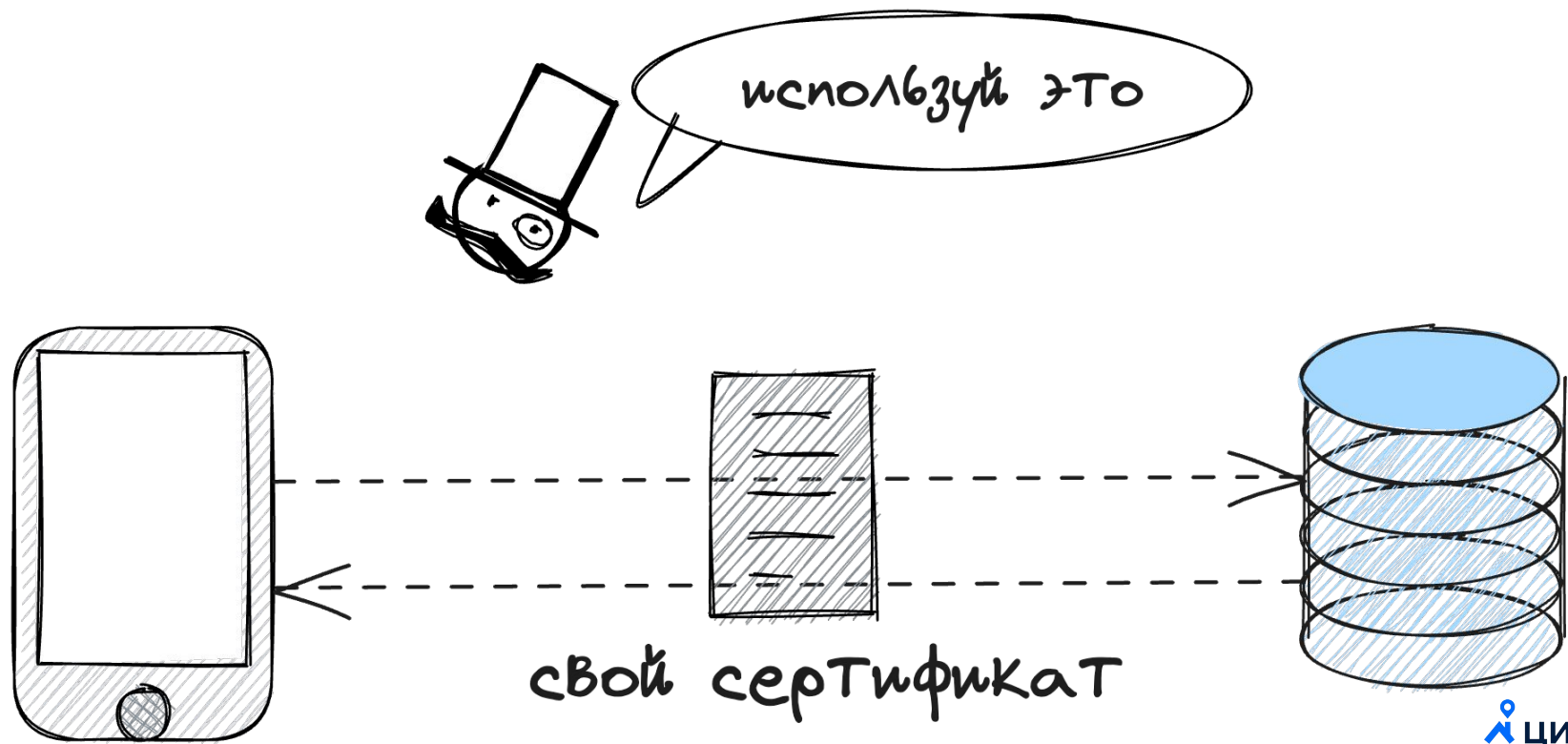


# Защита

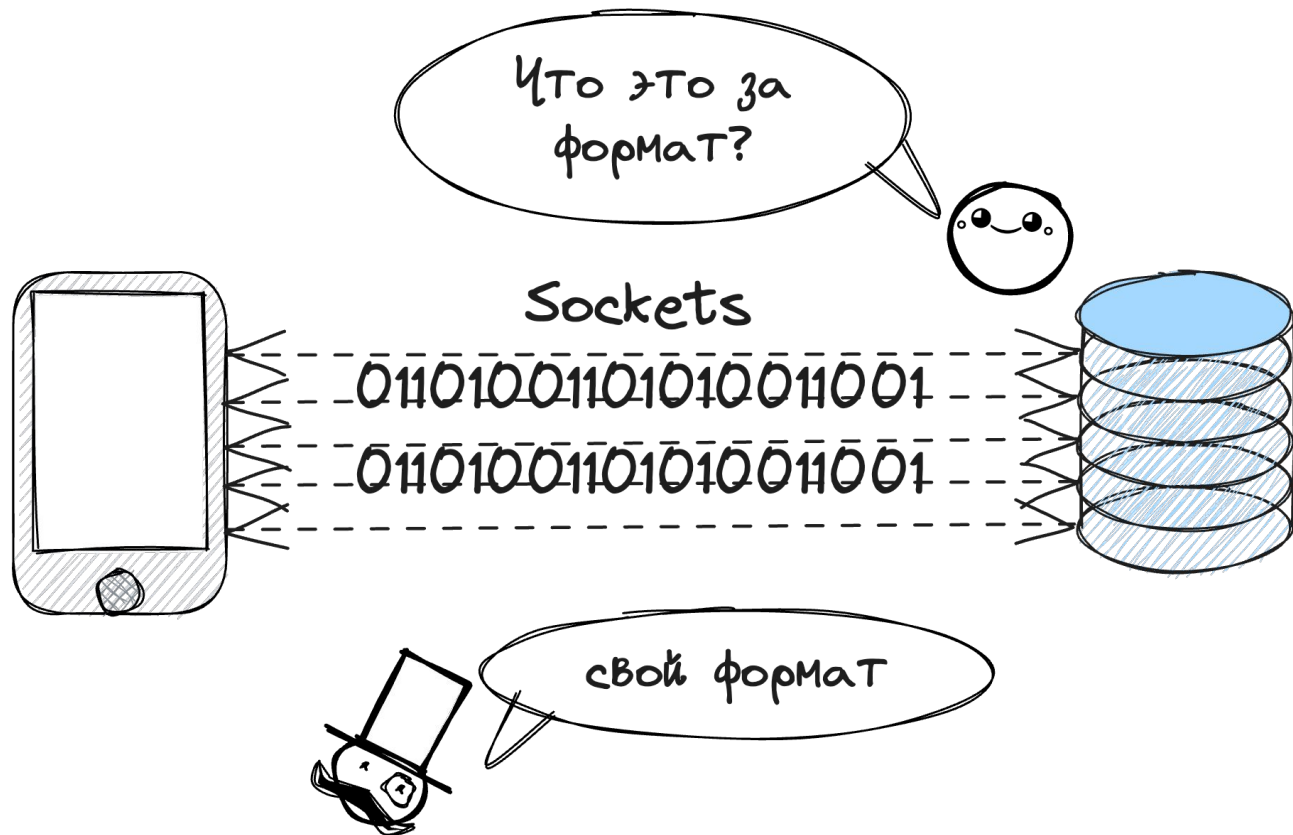
# Защищённый трафик. Защита. Смотрим на Proxy



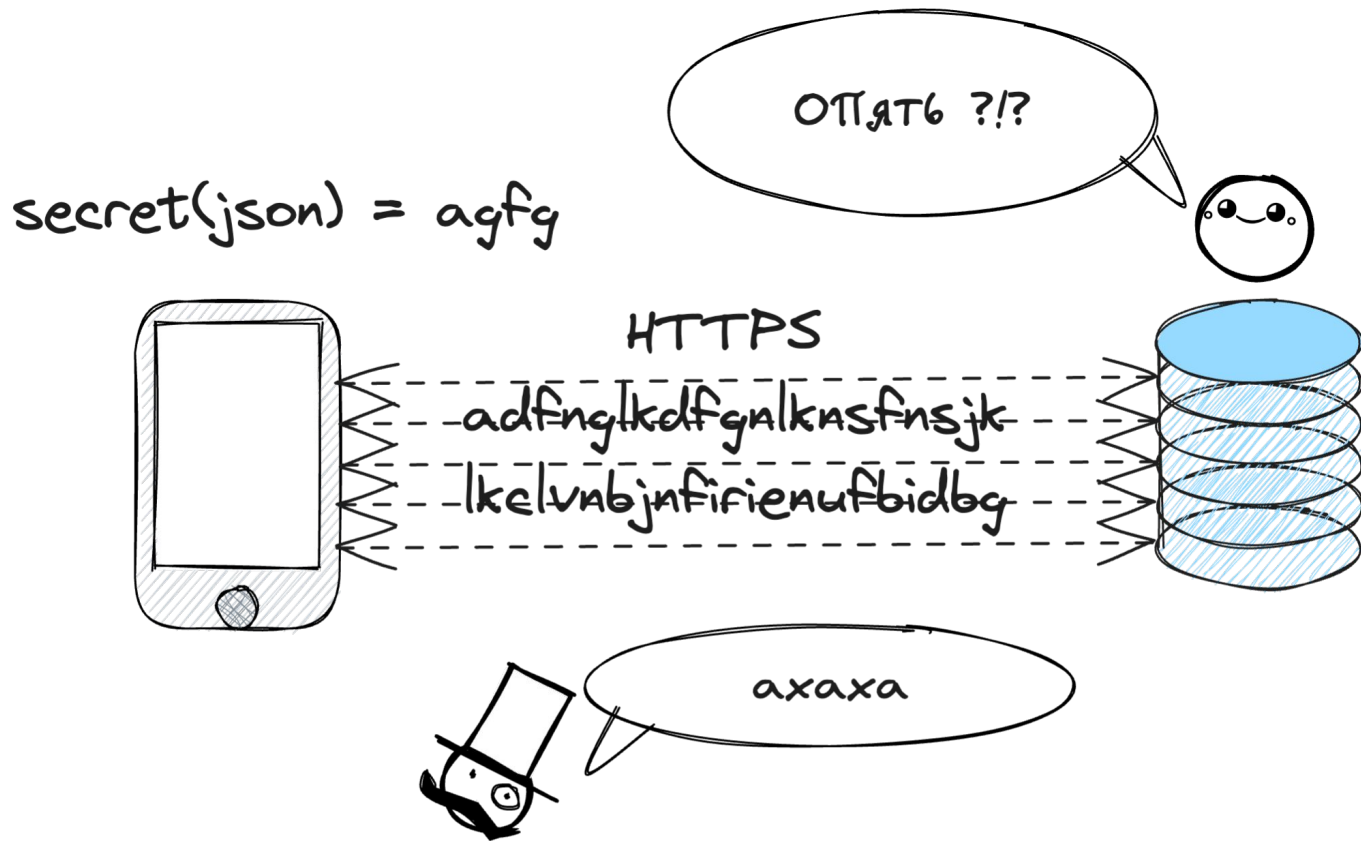
# Защищённый трафик. Защита. SSL Pinning



# Защищённый трафик. Защита. Сокеты



# Защищённый трафик. Защита. Подпись

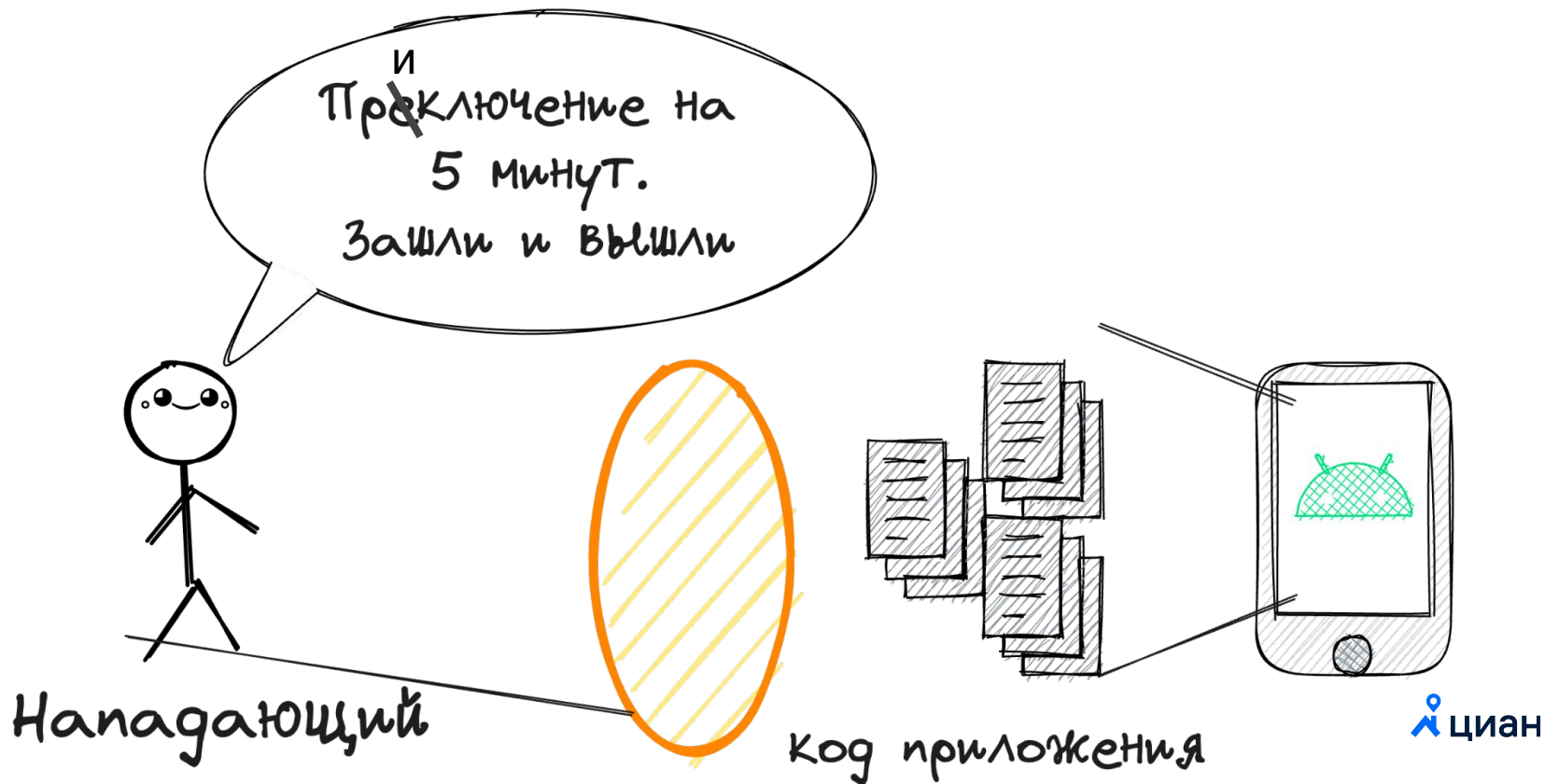






Атака

# Защищённый трафик. Атака. Уже сложнее



# Просмотр кода



# Инструменты



# Инструменты. Android Studio

app-debug.apk x

ru.cian.main.debug (Version Name: 2.293.0-debug, Version Code: 22930300)

APK size: 212 MB, Download Size: 202.4 MB Compare with previous APK...

File	Raw File Size	Download Size	% of Total Download Size
classes10.dex	5.0 KB	5.0 KB	0%
classes19.dex	5.3 KB	5 KB	0%
META-INF	3.6 KB	3.8 KB	0%
classes22.dex	3.7 KB	3.5 KB	0%
classes23.dex	3.2 KB	3 KB	0%
classes25.dex	2.7 KB	2.5 KB	0%
classes24.dex	2.2 KB	2.1 KB	0%

Load Proguard mappings...

This dex file defines **141** classes with **148** methods, and references **149** methods.

Class	Defined Methods	Referenced Methods	Size
ru	148	148	974 KB
cian	148	148	974 KB
newbuilding	128	128	932.6 KB
developer	42	42	371.4 KB
documents	40	40	309.8 KB
details	27	27	210.7 KB
kpn	19	19	40.8 KB
runtimesettings	20	20	41.4 KB
java		1	8 B

# Инструменты. APK Scanner



The screenshot shows the APK Scanner application window titled "app-debug.apk - APK Scanner". The interface includes a top toolbar with icons for Open, Manifest, Source, Search, Explo..., Install, Launch, Sign, More, Setting, and About. Below the toolbar are tabs for APK Info, Widgets(0), Libraries(51), Resources(8508), Components(205), and Signatures(1). The main content area displays the following information:

- Циан** [ru.cian.main.debug] ▶
- Ver. 2.293.0-debug / 22930300
- @SDK Ver. 24 (Min), 33 (Target)
- 212.04 MB (222,339,692 Bytes)
- [Feature] Install Location : Internal Only, Scheme v2
- LAUNCHER, START\_UP, Device Requirements
- DEBUGGABLE**

At the bottom, there is a section for "[Permissions] - Display the entire list ⚙️" with a dropdown menu set to "API Level 33". Below this are four icons representing different permission categories: R (Read), ? (Unknown), ? (Unknown), and ! (Warning).

# Инструменты. APK Scanner. Android Manifest

31

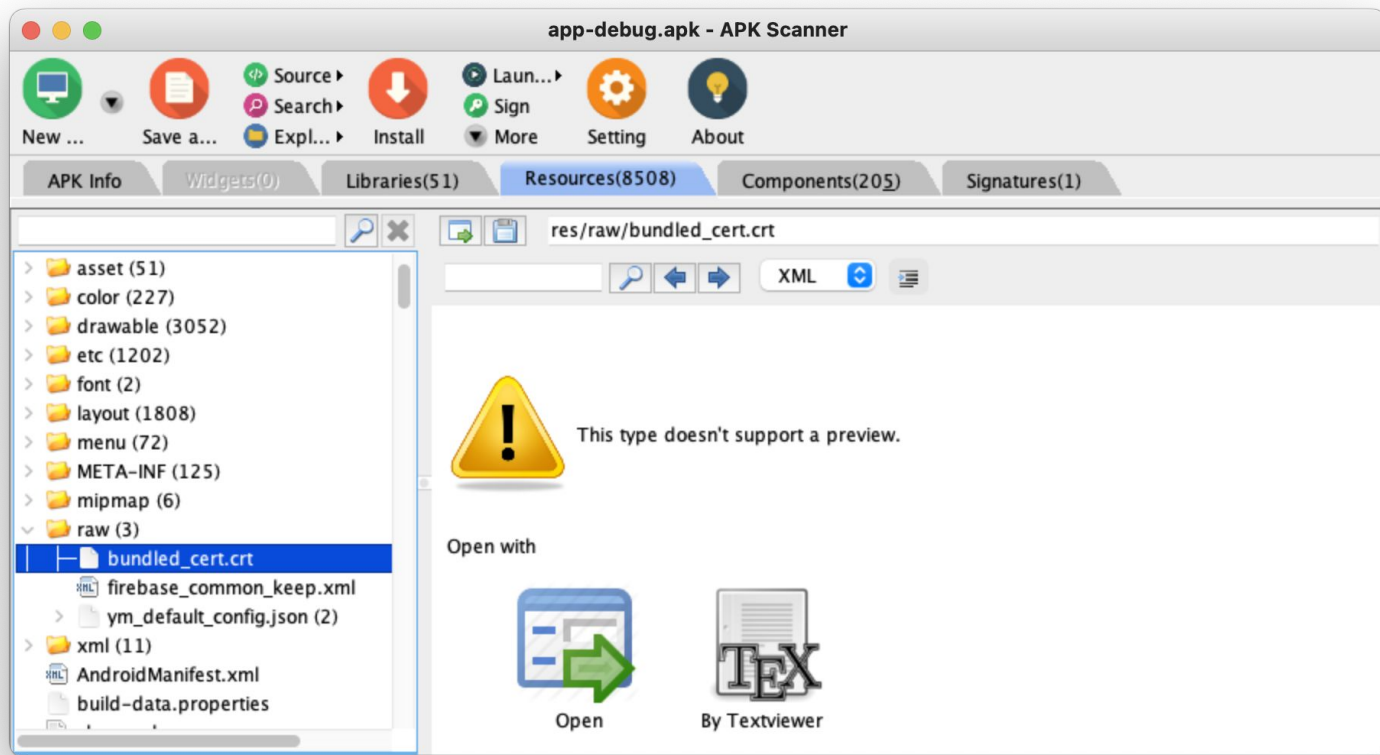
The screenshot shows the APK Scanner application interface for 'app-debug.apk'. The top navigation bar includes buttons for Open, Manifest, Explo..., Install, More, Setting, and About. Below this is a tabbed interface with 'Components(205)' selected. A search bar labeled 'CLASS' with a dropdown arrow and the text 'Filter by Class name' is present. The main area displays a table of components:

Class	Type	Enabled	Export	Permission	Startup
ru.cian.main.StartActivity	launcher	O	O	X	X
leakcanary.internal.activity.LeakLauncherActivity	launcher-alias	O	O	X	X
androidx.compose.ui.tooling.PreviewActivity	activity	O	O	X	X
com.facebook.flipper.android.diagnostics.FlipperDiagnosticAc...	activity	O	O	X	X
com.google.android.gms.auth.api.signin.internal.SignInHubAct...	activity	O	X	X	X
com.google.android.gms.common.api.GoogleApiActivity	activity	O	X	X	X
com.google.android.gms.tagmanager.TagManagerPreviewActi...	activity	O	O	X	X

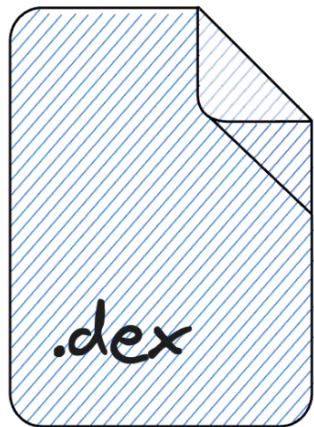
Below the table is the 'XML Construction' view showing the following XML code:

```
1 <activity android:theme="@style/UIKitAppTheme.Splash"
2     android:label="Циан"
3     android:name="ru.cian.main.StartActivity"
4     android:exported="true"
5     android:screenOrientation="locked">
6     <intent-filter>
7         <action android:name="android.intent.action.MAIN"/>
8         <category android:name="android.intent.category.DEFAULT"/>
9         <category android:name="android.intent.category.LAUNCHER"/>
10    </intent-filter>
11 </activity>
```

# Инструменты. APK Scanner. Ресурсы







## Smali Bytecode

```
.class public class LStartActivity;  
.super Lcom.android.Activity;  
.source "StartActivity.kt"
```

## Smali Bytecode

```
.class public class LStartActivity;  
.super Lcom.android.Activity;  
.source "StartActivity.kt"
```

→ dex2jar →

## Java

```
class StartActivity extends Activity {  
    void onCreate() {  
        .....  
    }  
}
```



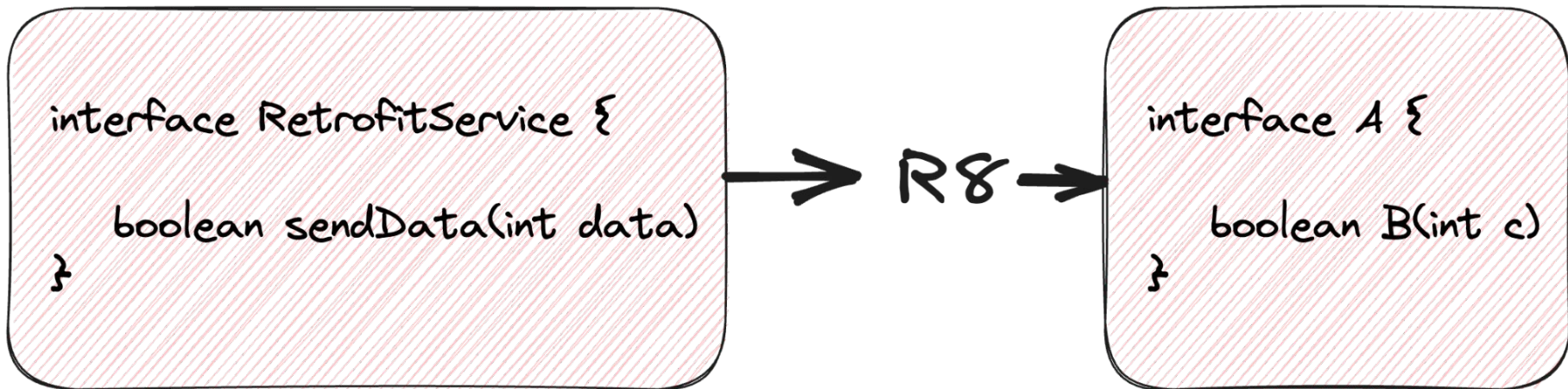
Атака



Java

```
interface RetrofitService {  
    boolean sendData(int data)  
}
```

# Защита

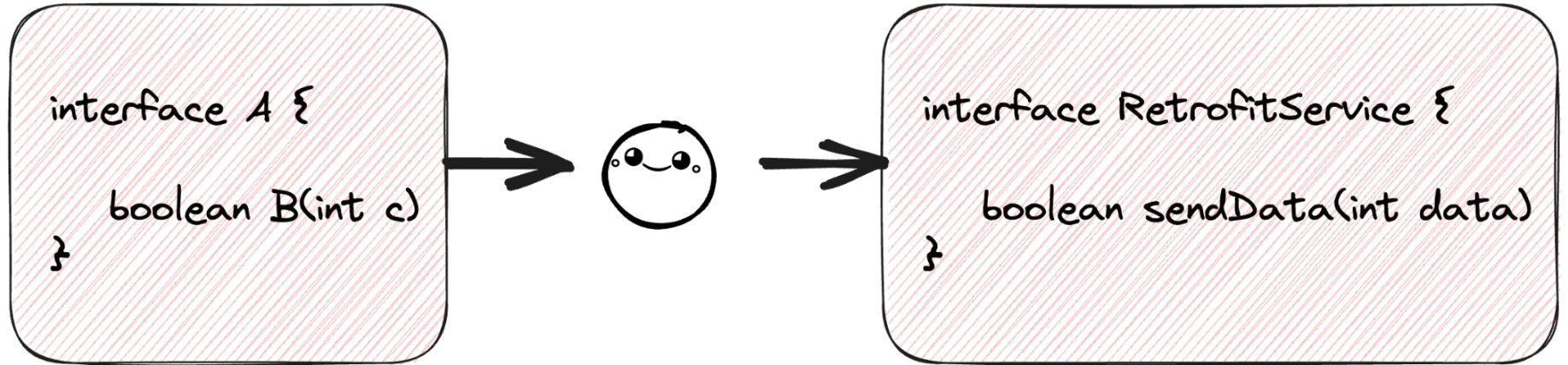




Атака



# Атака. Деобфускация



# Атака. Обфускация. Проверки на null

```
public final void mo12072a(float[] fArr, float[] fArr2) {  
    C1913g.m5240e(fArr, "xValues");  
    C1913g.m5240e(fArr2, "yValues");  
}
```

```
@Serializable  
internal data class M12(  
    @SerializedName("calls")  
    val f124: List<M857g>,  
    @SerializedName("page")  
    val f69: M87t  
)
```

```
private final void m2419U() {  
    C2065g<R> E = this..mo14131I(new C1470c(new C1236m(this)));  
    C2065g<R> n = E.mo14143n(new C1471d(C1232i.f1811e));  
    C1913g.m5239d(n, "addWaterObservable / 2 < it.second }");  
}
```

# Атака. Обфускация. Ошибка и прочее

- Ошибки.
- Ресурсы.
- Захардкоженные строки
- И много-много всего.

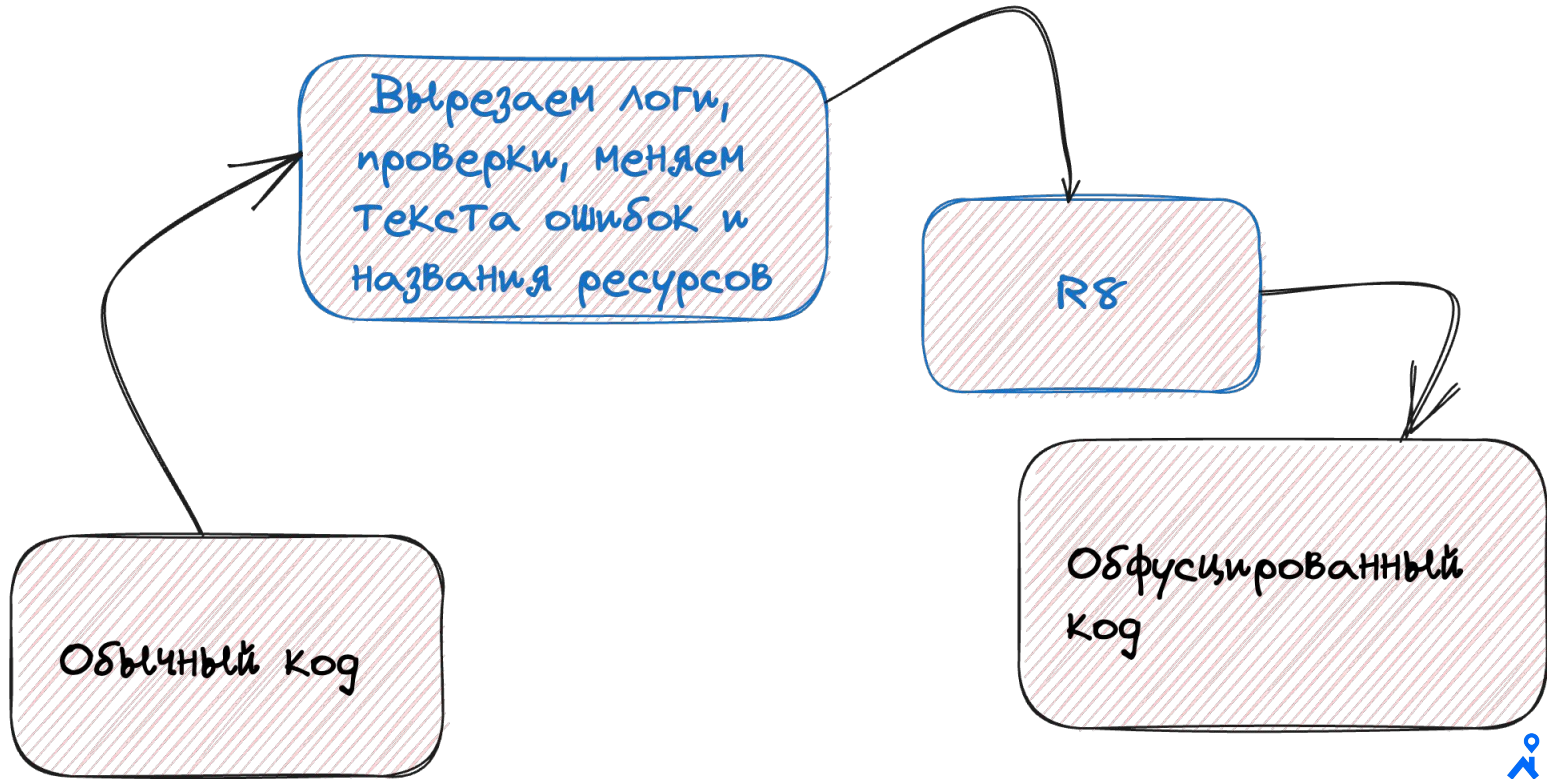


Java

```
interface RetrofitService {  
    boolean sendData(int data)  
}
```

# Защита

# Защита. Обфускация. Улучшаем





JADX WARNING: Code restructure failed:  
missing block: B:7:0x0013, code lost:

# Защита. Обфускация. Проблемы dex2jar. Issues

50

pxb1988 / dex2jar

Search: Type to search

Code Issues 385 Pull requests 6 Actions Projects Wiki Security Insights

**Want to contribute to pxb1988/dex2jar?** Dismiss

If you have a bug or an idea, browse the open issues before opening a new one. You can also take a look at the [Open Source Guide](#).

Filters  Labels 7 Milestones 0 New issue

<input type="radio"/> 385 Open <input checked="" type="radio"/> 169 Closed	Author	Label	Projects	Milestones	Assignee	Sort
<input type="radio"/> <b>Detail Error Information in File .\jioJoin-error.zip Please report this file</b> #588 opened 4 days ago by Bhubonmondal						
<input type="radio"/> <b>READ THIS **BEFORE** CREATING ISSUES!</b> #587 opened 3 weeks ago by ThexXTURBOXx						
<input type="radio"/> <b>java.lang.NullPointerException</b> #583 opened on Jul 1 by mxhui						1
<input type="radio"/> <b>GLITCH: 0003 LBuilder;.testDeadEndTry(l)  not enough space for reading instruction</b> #581 opened on Jun 14 by sendaoYan						2
<input type="radio"/> <b>d2jar error</b> #580 opened on May 22 by code-and-relax						1

sessionKey = asdsfsgfdg

a << 0

s >> 2 << 1

d << 4 >> 3 << 3 + s >> 2 << 3

dsadasffdsf

# Защита. Обфускация. Байтовые сдвиги. Результат <sup>52</sup>

```
/* access modifiers changed from: private */
/* JADX WARNING: Code restructure failed: missing block: B:7:0x0013, code lost:
    if (r4 != 3) goto L_0x0095;
 */
/* renamed from: P */
/* Code decompiled incorrectly, please refer to instructions dump. */
public static final boolean m2414P(com.princeparadoxes.watertracker.presentation.screen.main.MainActivity r3, android.view.View r4,
/*
    java.lang.String r4 = "this$0"
    p087p3.C1913g.m5240e(r3, r4)
    int r4 = r5.getAction()
    r0 = 1
    if (r4 == 0) goto L_0x008f
    r1 = 0
    if (r4 == r0) goto L_0x003e
    r2 = 2
    if (r4 == r2) goto L_0x0017
    r5 = 3
    if (r4 == r5) goto L_0x003e
    goto L_0x0095
L_0x0017:
    android.widget.FrameLayout r4 = r3.m2410L()
    float r4 = r4.getTranslationY()
    float r2 = r5.getY()
    float r4 = r4 + r2
    float r2 = r3.f1802w
    float r4 = r4 - r2
    int r2 = (r4 > r1 ? 1 : (r4 == r1 ? 0 : -1))
    if (r2 >= 0) goto L_0x002c
    goto L_0x002d
```



Атака

# Атака. Обфускация. Enjarify


54

Storyyeller / enjarify Search Type to search

<> Code Issues 6 Pull requests 2 Actions Projects Security Insights






 **enjarify** Public  
forked from [google/enjarify](#)

 Watch 36

 master 2 branches 4 tags

[Go to file](#) [Add file](#) [Code](#)

This branch is [15 commits ahead](#), [2 commits behind](#) google:master. #20

 enjarify	Handle primitive const-class (#12)	7 6364dfb on Mar 7, 2020	 78 commits
 tests	Adjust test2 to pass		7 years ago
 .gitattributes	Add change-detector script		8 years ago
 .gitignore	ignore all output jars		7 years ago

# Атака. Обфускация. Enjarify

Smali Bytecode

```
.class public class LStartActivity;  
.super Lcom.android.Activity;  
.source "StartActivity.kt"
```

Enjarify

Java

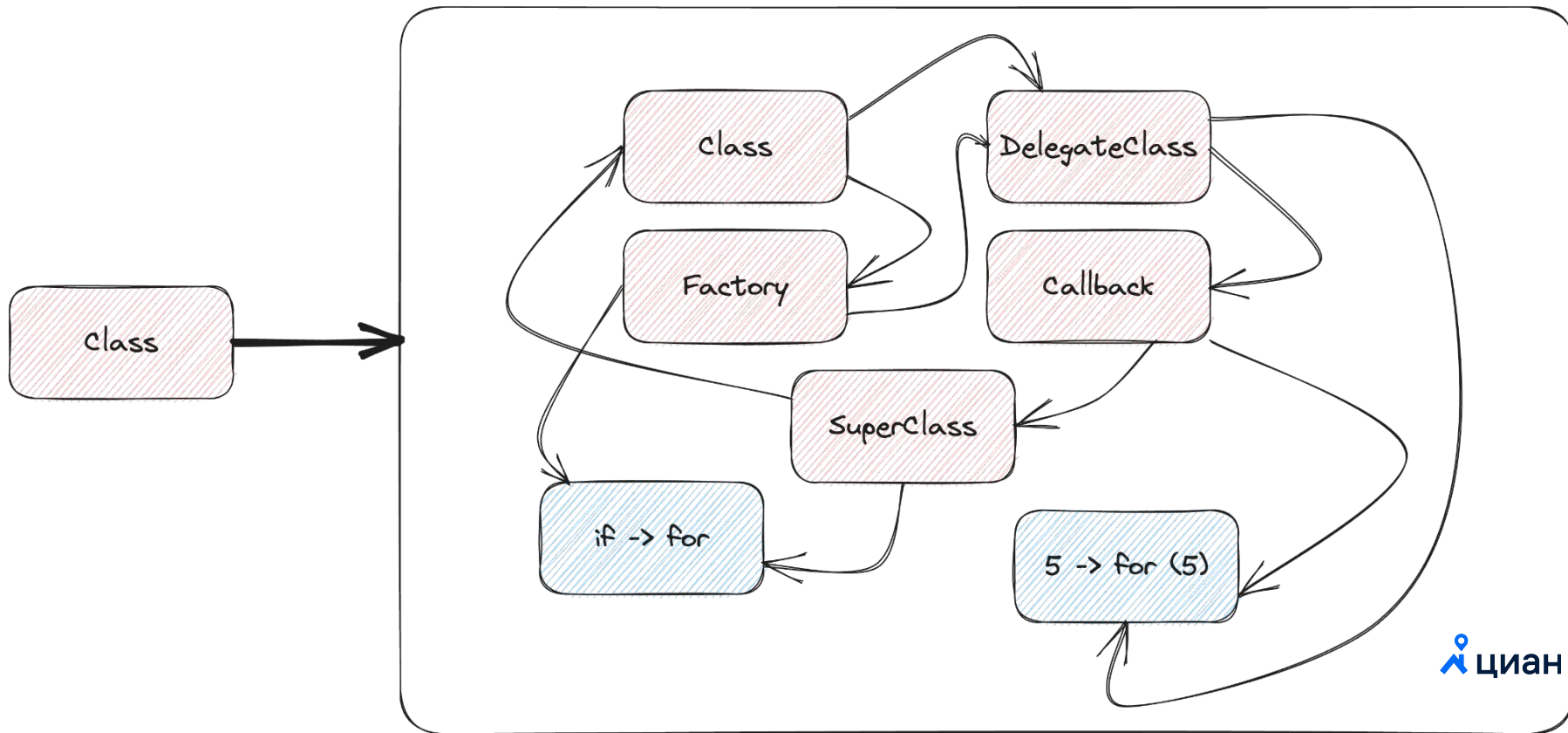
```
class StartActivity extends Activity {  
    void onCreate() {  
        .....  
    }  
}
```

Java

```
interface RetrofitService {  
    boolean sendData(int data)  
}
```



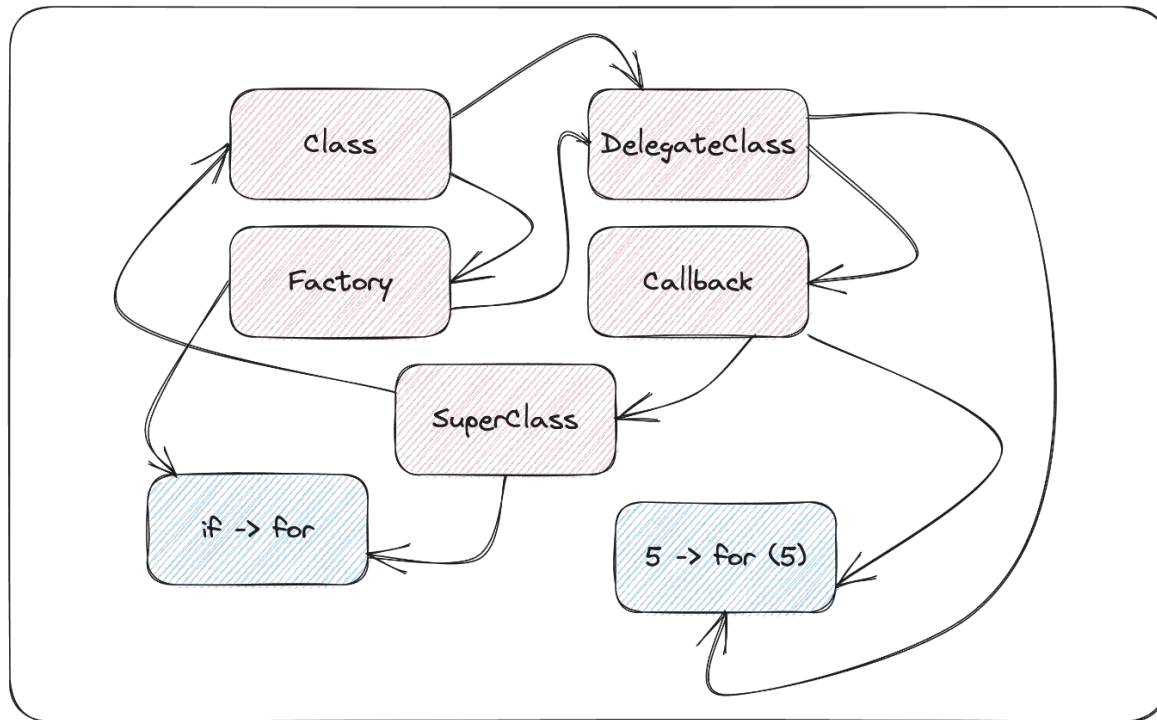
# Защита





Атака

# Атака. Говнокод. Изменение поведения



# Изменение поведения



## Script

```
val i = 12
```

## App

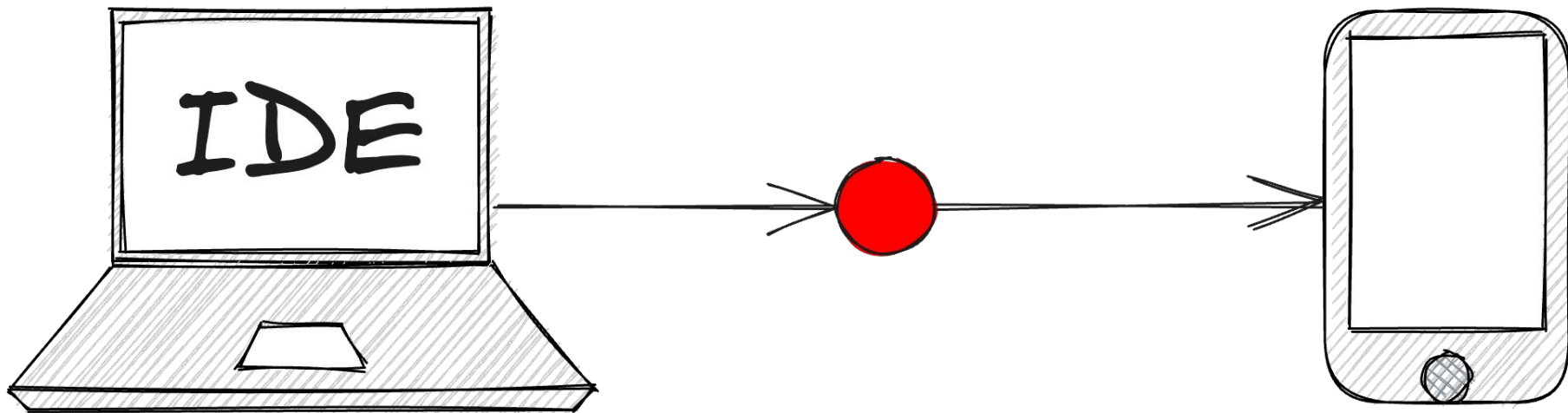
```
val i = 1
```

```
val s = "$i"
```

```
val g = s.size
```

```
println("Size $g")
```

# Изменение поведения. Breakpoint



# Изменение поведения. Breakpoint

```
class TestDebugClass {  
  
    fun number(isOne: Boolean): String {  
        val number = if (isOne) "1" else "2"  
        return number  
    }  
}
```



# Изменение поведения. Breakpoint

Events ~/GlobalEvents

```
1 class TestDebugClass {  
2  
3 fun number(isOne: Boolean): String {  
4     val number :String = if (isOne) "1" else "2"  
5     return number  
}
```

ain  
kotlin

**TestDebugClass.kt:5**

Enabled

Suspend:  All  Thread

Condition:  Kotlin ▾

Log:  "Breakpoint hit" message  Stack trace  Evaluate and log:  Kotlin ▾

Remove once hit

Disable until hitting the following breakpoint:

After hit:  Disable again  Leave enabled

Instance filters:  ▾

Class filters:  ▾

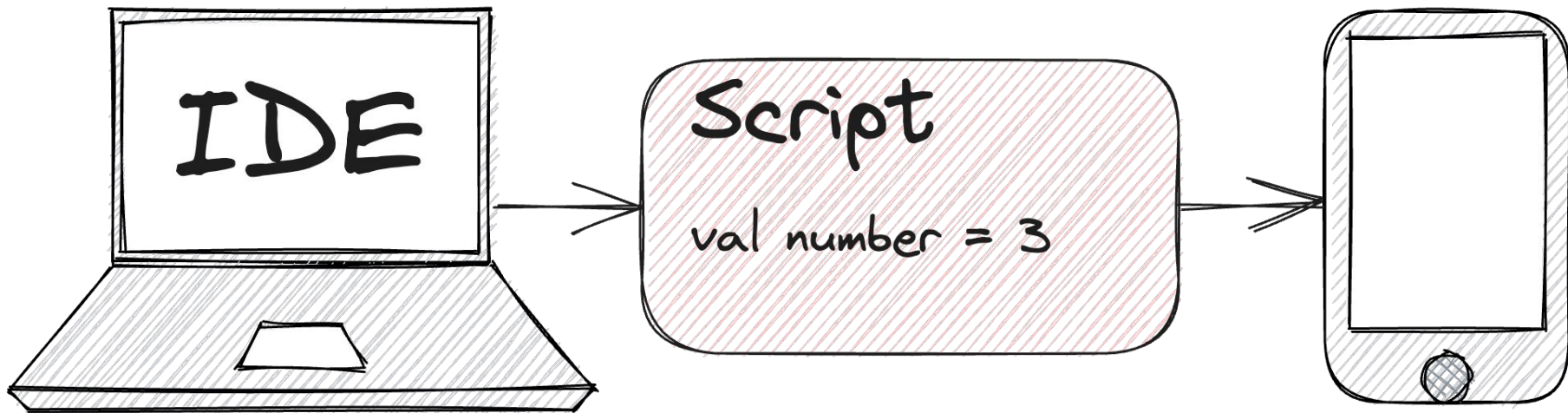
Pass count:

Caller filters:  ▾

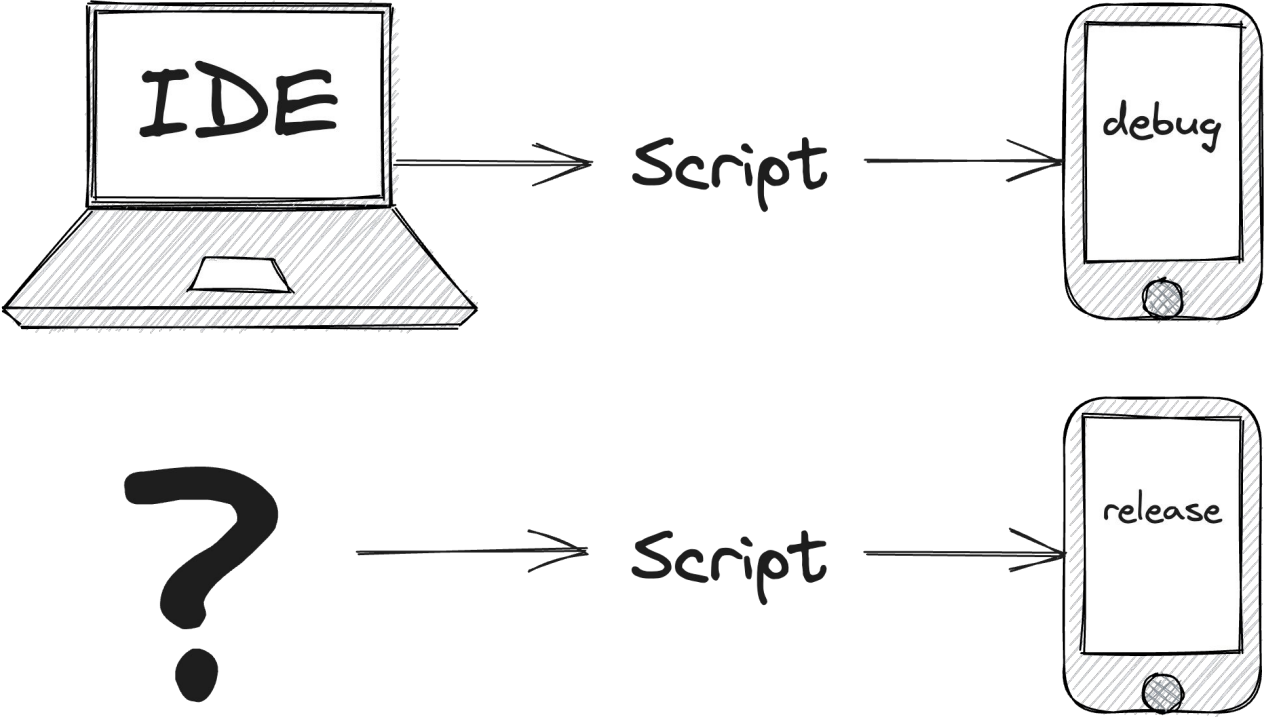
More (⇧F8) Done

ne/bin/java ...

# Изменение поведения. Breakpoint

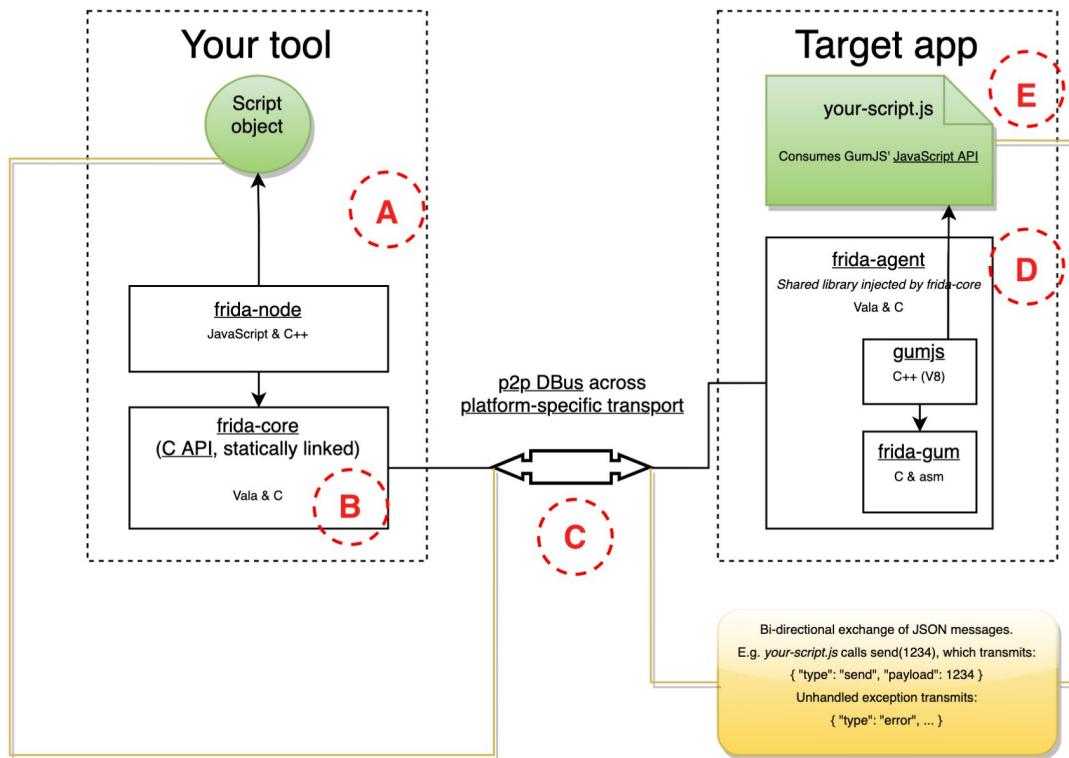


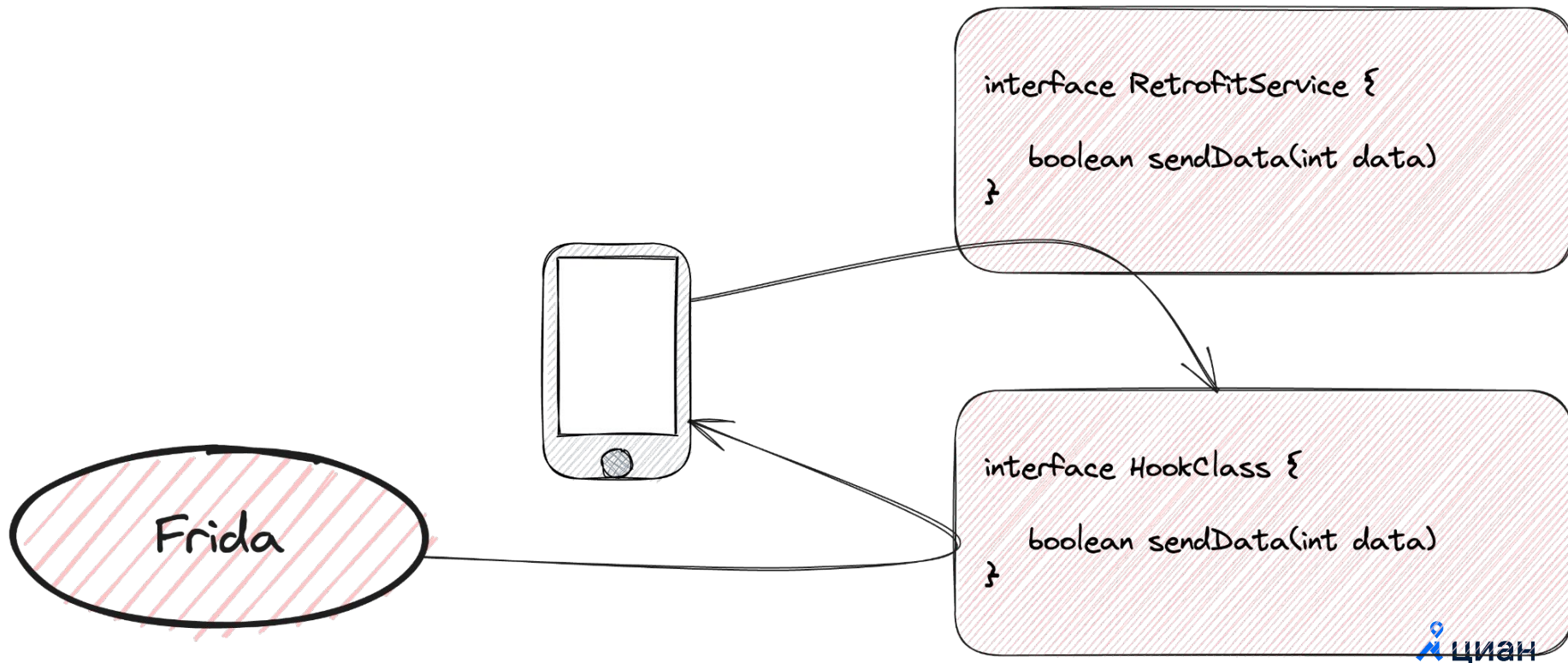
# Debug vs Release



FRYIDA

# Frida. Архитектура





# Frida. Пример. Переопределяем клик

```
Java.perform(() => {  
  const MainActivity = Java.use('ru.cian.MainActivity');  
  
  const onClick = MainActivity.onClick;  
  onClick.implementation = function (view) {  
    onClick.call(this, view);  
    // Показываем Toast  
  };  
});
```

# Frida. Пример. Переопределяем локацию

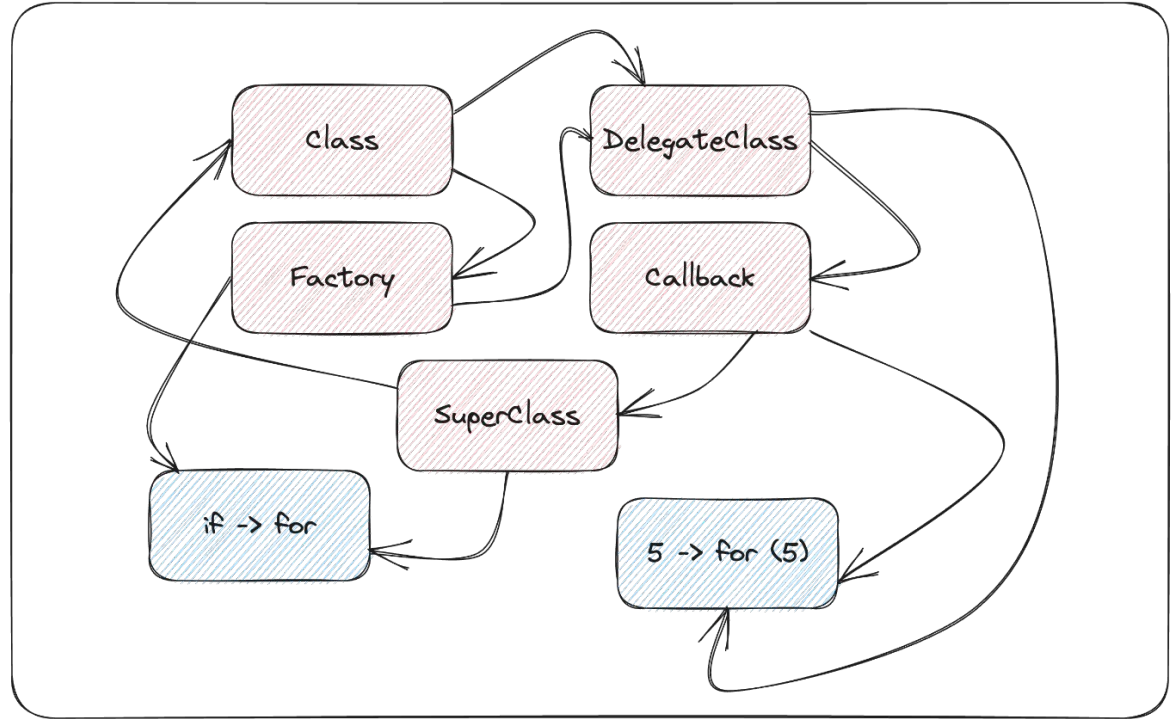
```
Java.perform(() => {  
    var Location = Java.use('android.location.Location');  
    Location.getLatitude.implementation = function() {  
        return LATITUDE;  
    }  
    Location.getLongitude.implementation = function() {  
        return LONGITUDE;  
    }  
})
```





Атака

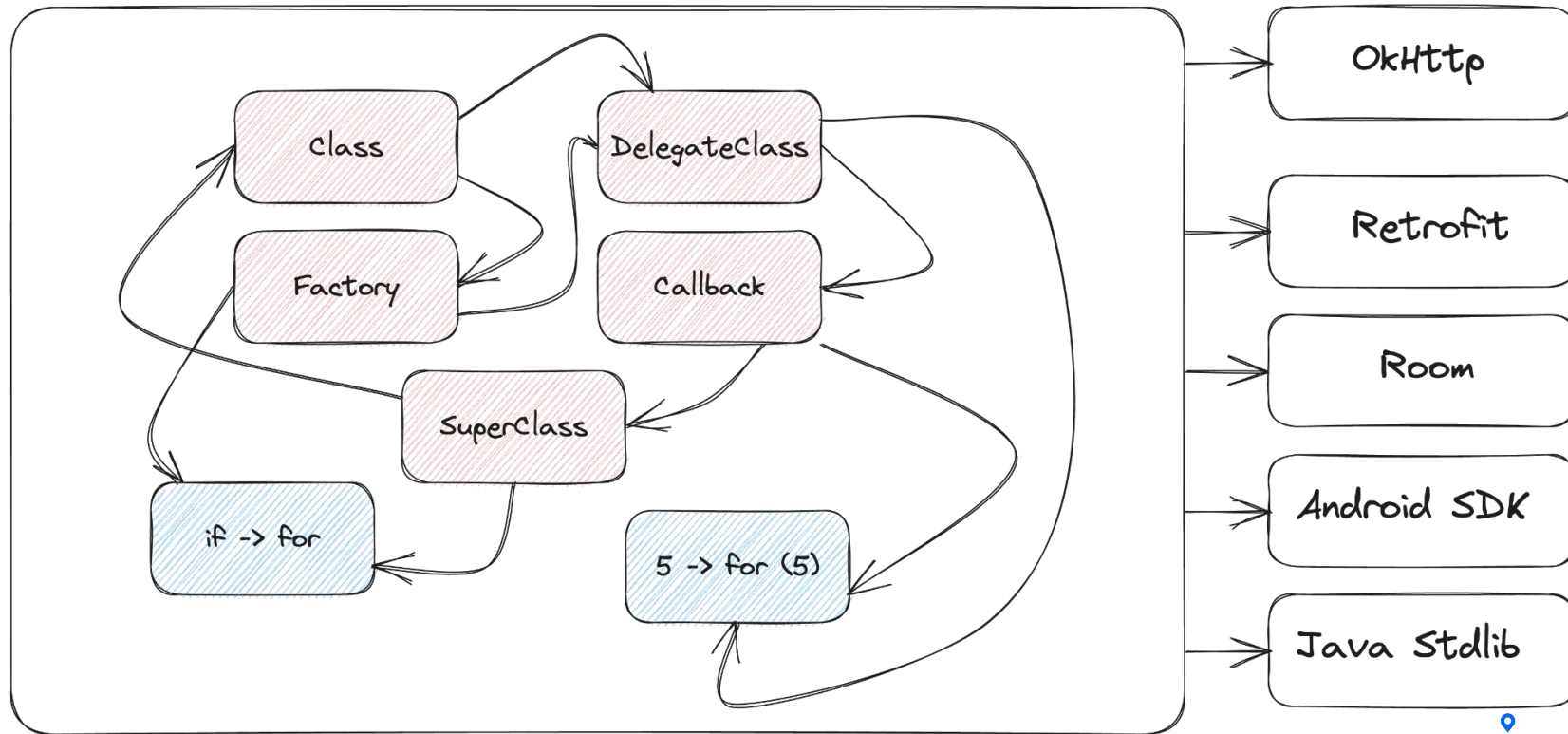
# Атака. Говнокод



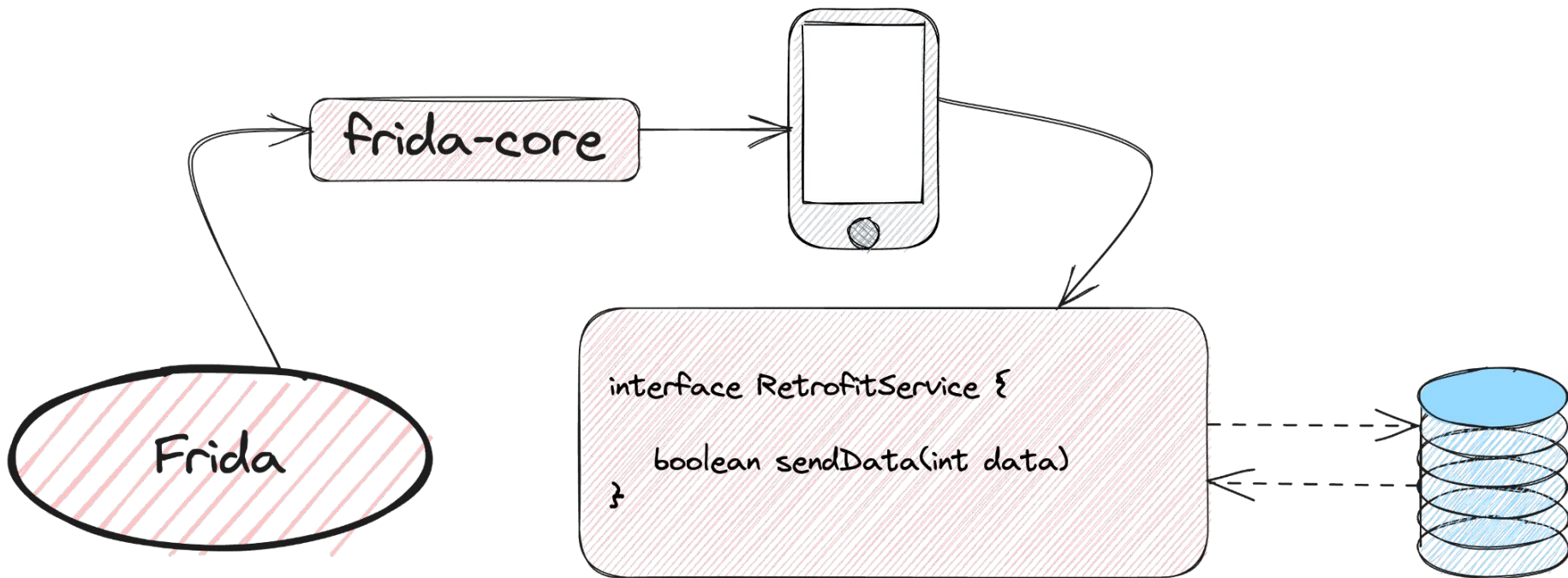
# Атака. Говнокод. Stacktrace

```
Java.perform(() => {  
    var log = Java.use("android.util.Log"),  
    var exception = Java.use("java.lang.Exception");  
    console.log(log.getStackTraceString( exception.$new()));  
})
```

# Атака. Говнокод. Стандартные библиотеки

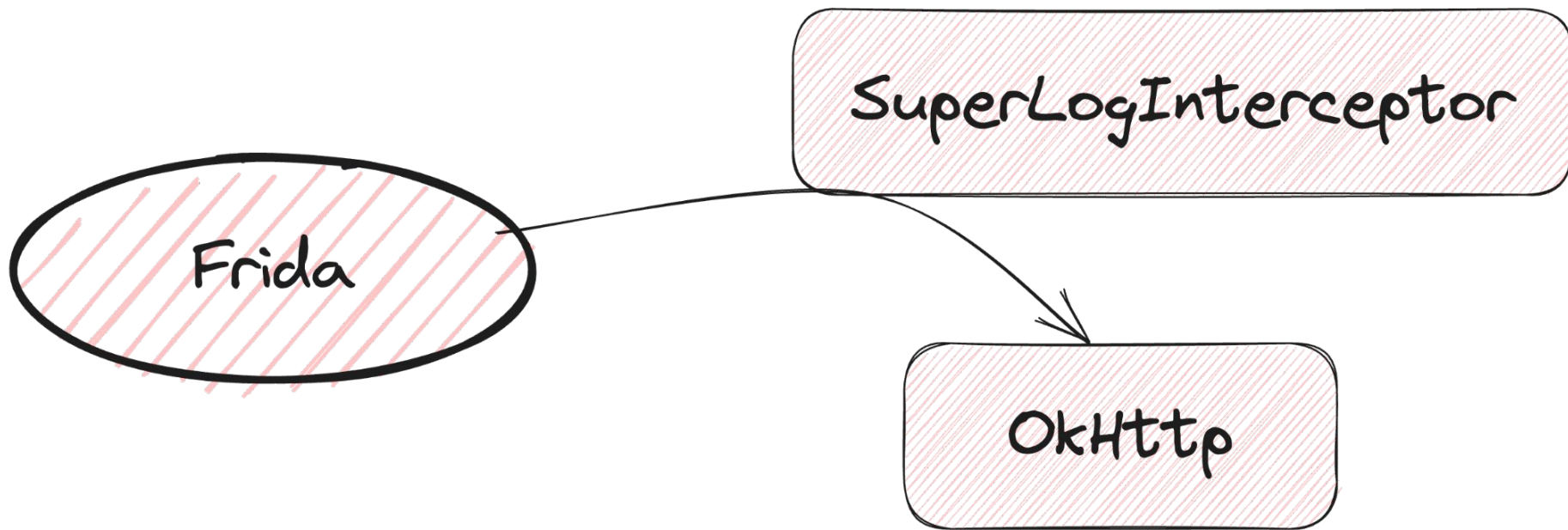


# Атака. Frida. Внедряем скрипт



# Атака. Frida. Внедряем свои логи в OkHttp

78



# Атака. Frida. Доверяем всем сертификатам

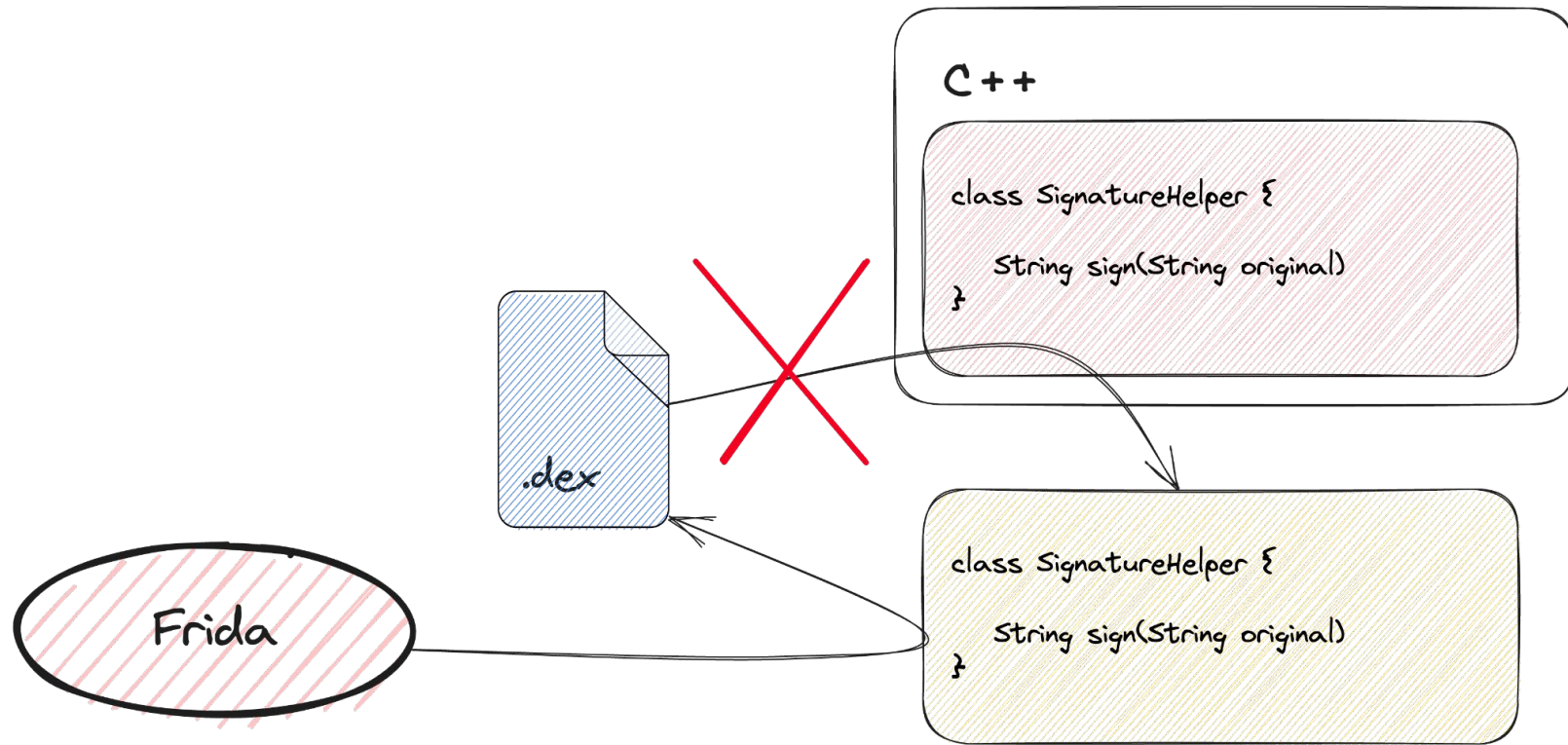
```
Java.perform(() => {  
  
    var array_list = Java.use("java.util.ArrayList");  
    var ApiClient = Java.use('com.android.org.conscrypt.TrustManagerImpl');  
  
    ApiClient.checkTrustedRecursive.implementation = function(a1, a2, a3, a4, a5, a6) {  
        var trusted = array_list.$new();  
        return trusted;  
    }  
  
});
```

# Защита

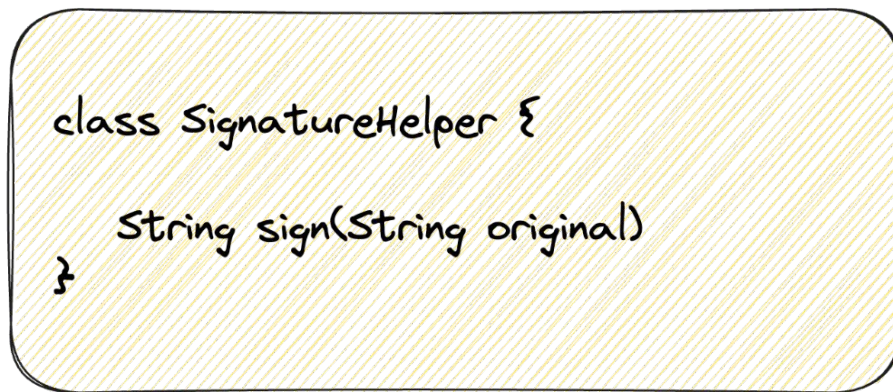


# C++

The background features a solid blue color with several overlapping, semi-transparent spheres and ovals in shades of purple and light blue. These shapes are arranged in a way that creates a sense of depth and movement, with some appearing to be in the foreground and others receding into the background.



1234



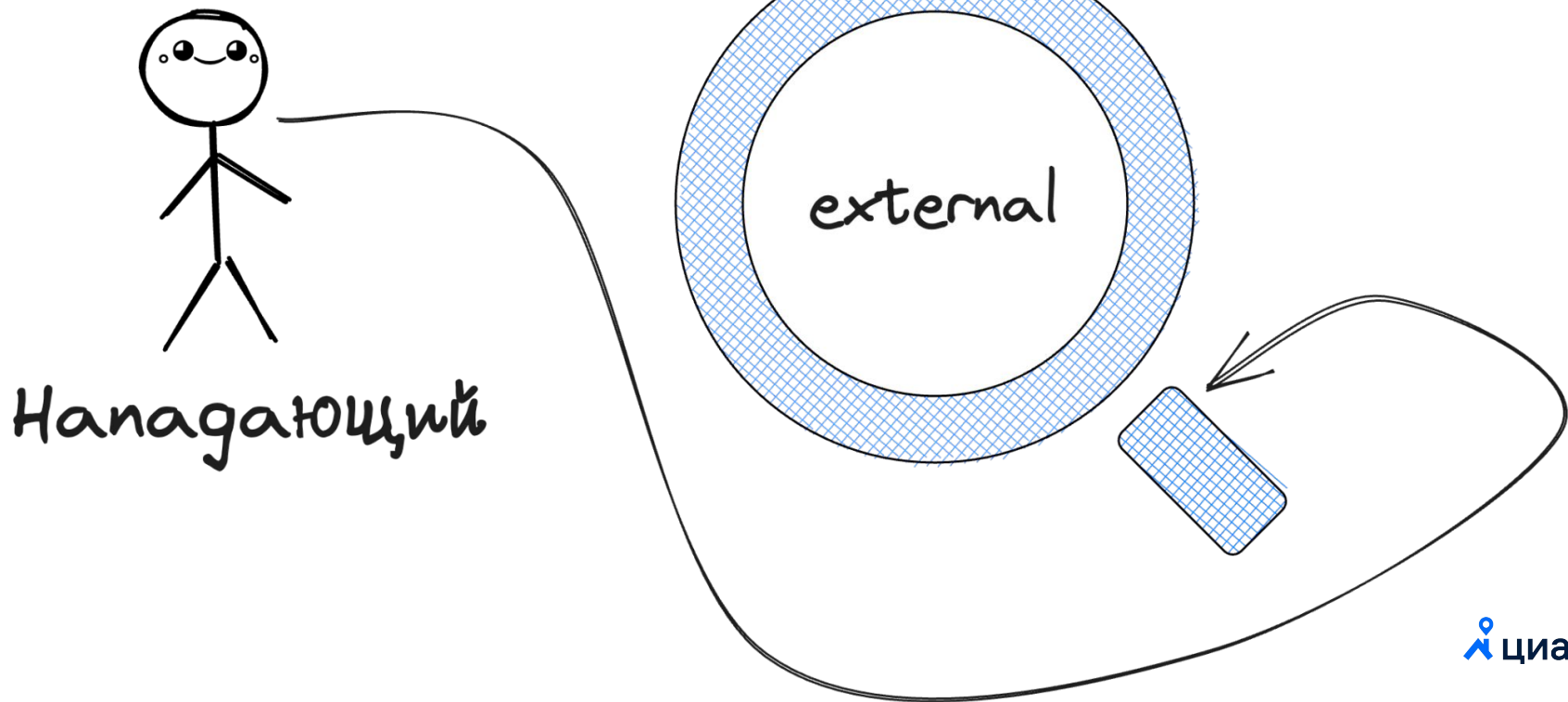
2345

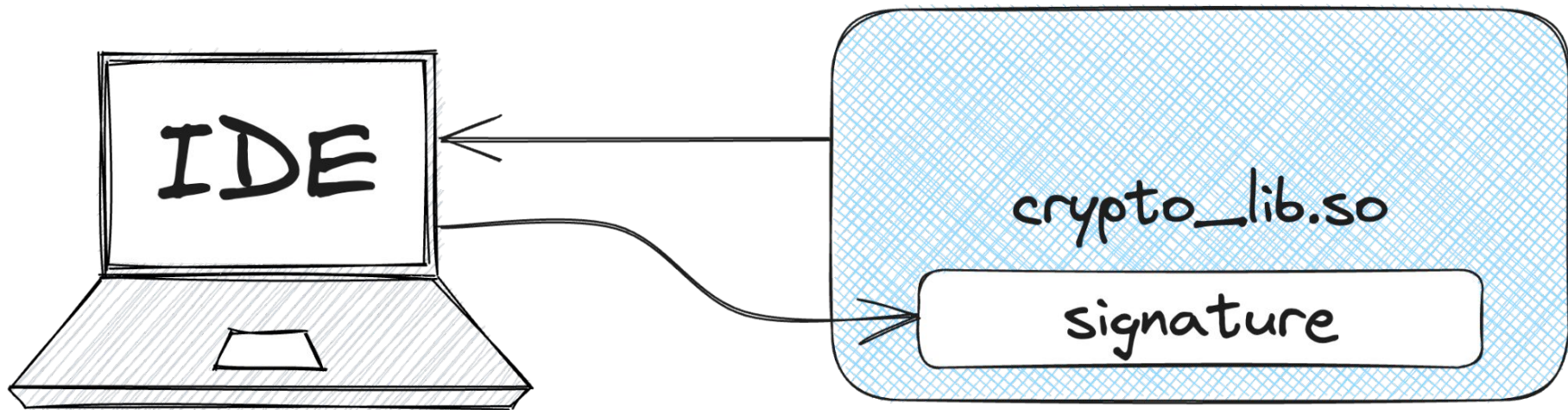
```
std::string SignatureHelper::createSignature(std::string inputString) {  
    std::string outputString = std::string();  
    for (int i = 0; i < inputString.size(); i++) {  
        outputString[i] = inputString[i] + 1;  
    }  
    return outputString;  
}
```

```
Java_com_princeparadoxes_myapplication_MainActivity_signature(  
    JNIEnv* env,  
    jobject jobj,  
    jstring inputString) {  
  
    jboolean isCopy;  
    const char *stdString = (env)->GetStringUTFChars(inputString, &isCopy);  
  
    SignatureHelper helper = SignatureHelper();  
    std::string signature = helper.createSignature(stdString);  
  
    return env->NewStringUTF(signature.c_str());  
}
```



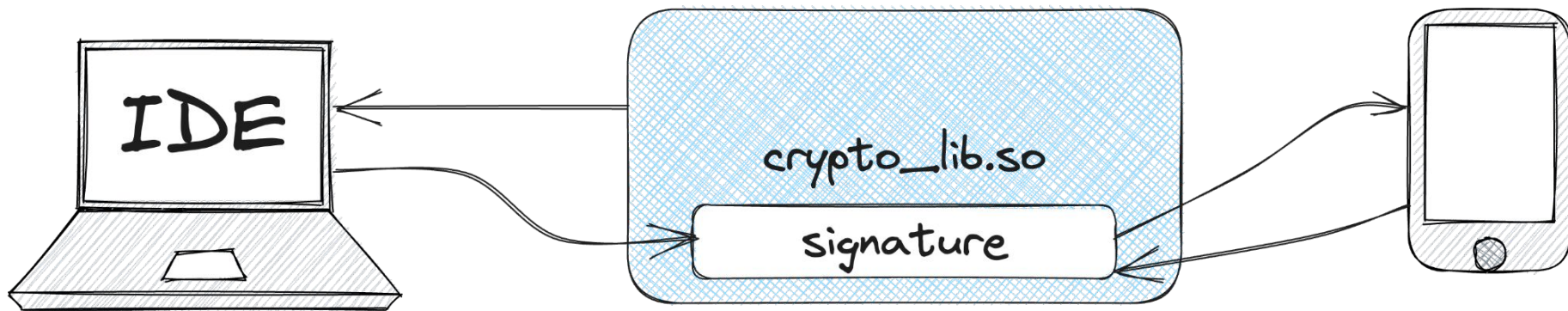
Атака







# Защита



1234



```
class SignatureHelper {  
    String sign(String original)  
}
```



PQRS

```
std::string SignatureHelper::createSignature(std::string inputString) {  
    std::string outputString = std::string();  
    for (int i = 0; i < inputString.size(); i++) {  
        outputString[i] = inputString[i] +  
            android_get_device_api_level();  
    }  
    return outputString;  
}
```



Атака

```
0101 1010 0011  
1100 1010 0100  
1001 0110 1001  
0101 1010 0011  
1100 1010 0100  
1001 0110 1001
```

Decompile

C++



# C++. Декомпиляция. Результат

96

```
push    rbp
mov     rbp, rsp
sub     rsp, 60h
mov     rax, rdx
mov     [rbp+shift], rdi
mov     [rbp+var_11], 0
mov     rdi, [rbp+var_38] ; this
call   __ZN15SignatureHelper8getShiftEv
mov     ecx, eax
mov     [rbp+var_2C], ecx
jmp     $+5
```



# C++. Декомпиляция. Цикл

```
mov     eax, [rbp+var_28]
add     eax, 1
mov     [rbp+var_28], eax
jmp     loc_203B3
```

# C++. Декомпиляция. Цикл

```
; this  
]  
]  
ax  
basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEE4sizeEv ; std::__ndk1::basic_string<char,std::__ndk1::char_traits<char>,std::__ndk1::allocator<char>>::size(void)  
]
```

```
loc_20424:  
mov [rbp+var_11], 1  
test [rbp+var_11], 1  
inz loc_20438
```

```
mov rdi, [rbp+var_50] ; this  
movsxd rsi, [rbp+var_28] ; __pos  
call _ZNSt6__ndk112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEixEm ; std::__ndk1::basic_string<char,std::__ndk1::char_traits<char>,std::__ndk1::allocator<char>>::operator[](ulong)  
mov rdi, [rbp+var_48] ; this  
movsx eax, byte ptr [rax]  
add eax, [rbp+1]  
mov [rbp+var_59], al  
movsxd rsi, [rbp+var_28] ; __pos  
call _ZNSt6__ndk112basic_stringIcNS_11char_traitsIcEENS_9allocatorIcEEEixEm ; std::__ndk1::basic_string<char,std::__ndk1::char_traits<char>,std::__ndk1::allocator<char>>::operator[](ulong)  
mov cl, [rbp+var_59]  
mov [rax], cl  
mov eax, [rbp+var_28]  
add eax, 1  
mov [rbp+var_28], eax  
jmp loc_20383
```

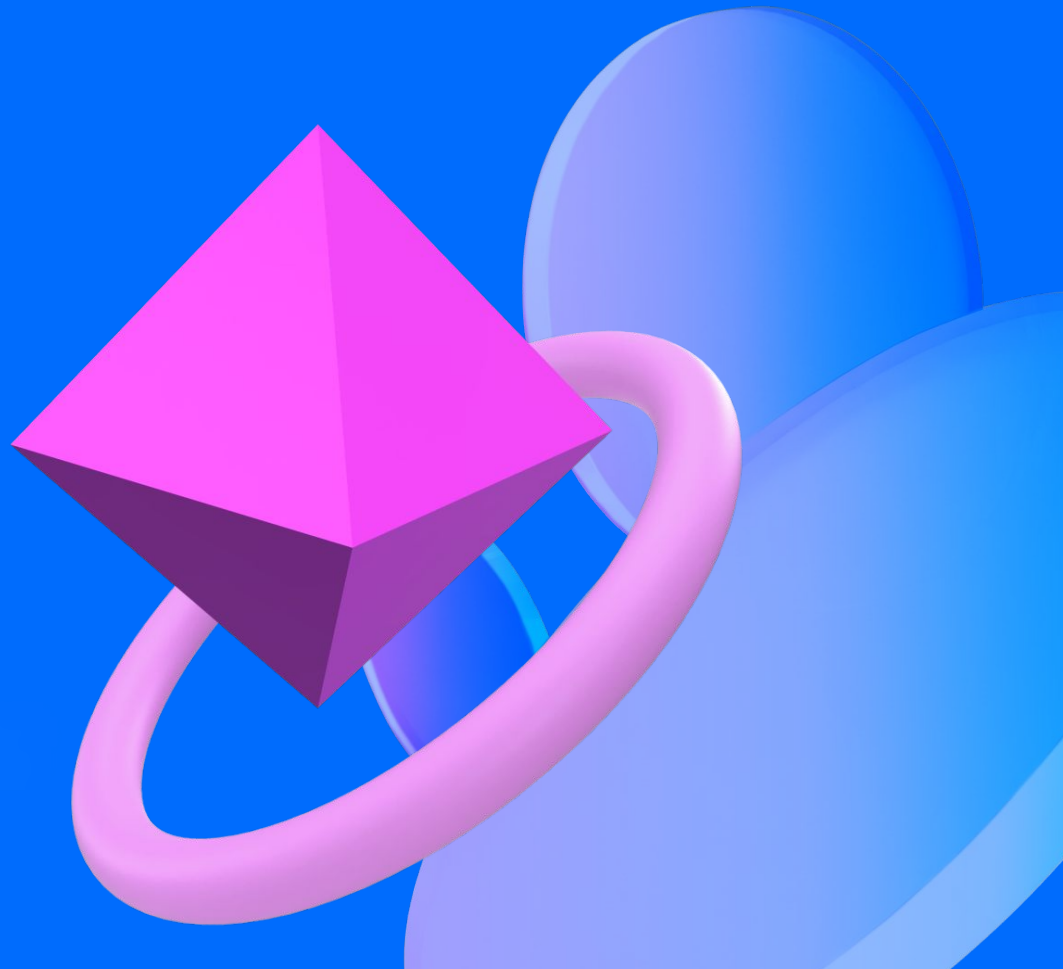
```
; std::__ndk1::basic_string<char,std::__ndk1::char_traits<char>,std::__ndk1::allocator<char>>::~basic_string()
```

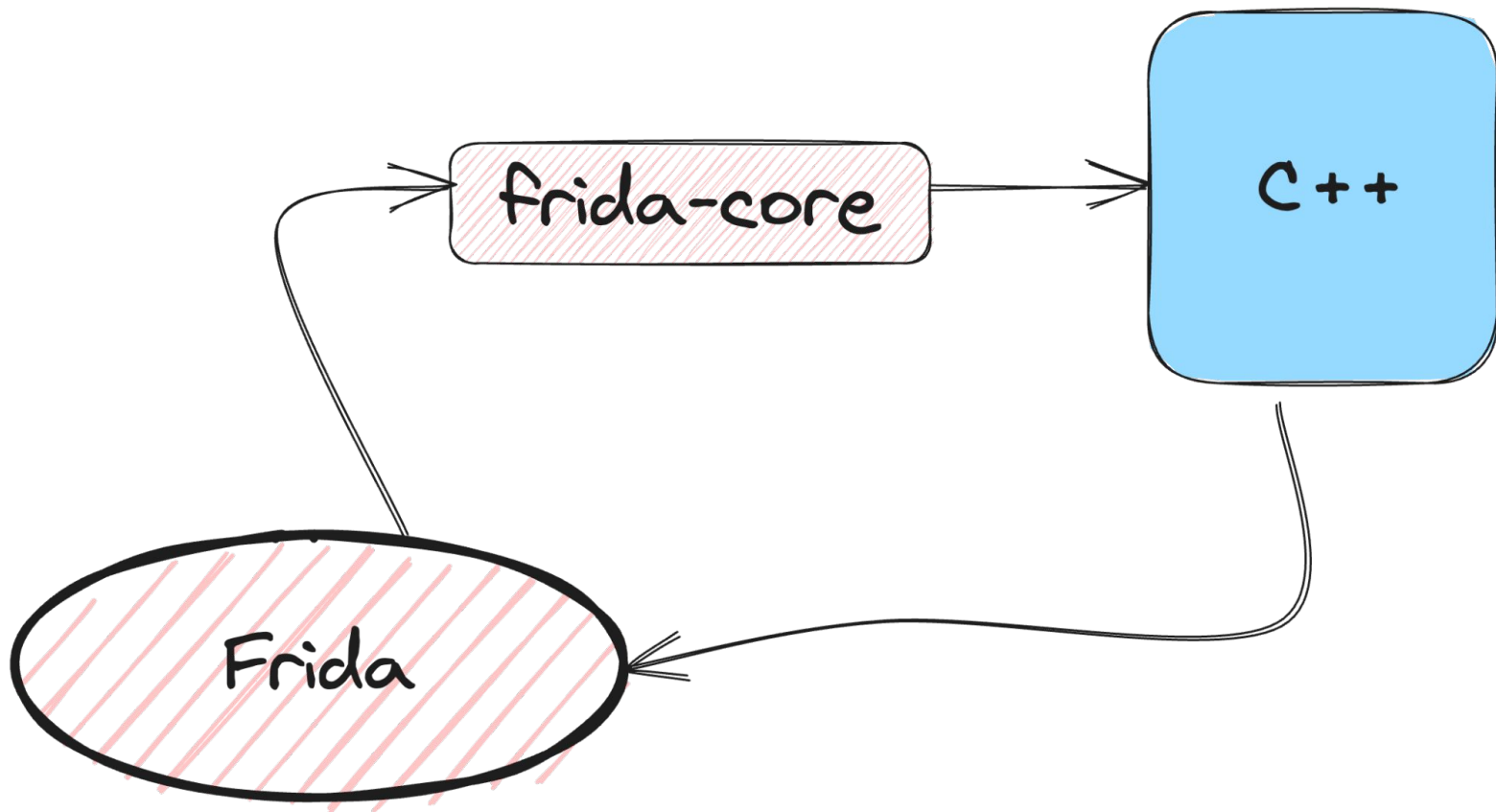
```
loc_20438:  
mov rax, [rbp+var_40]  
add rsp, 60h  
pop rbp  
ret
```

# C++. Декомпиляция. getShift

```
push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     [rbp+var_8], rdi
call  _ZL28android_get_device_api_levelv
mov     [rbp+var_C], eax
mov     eax, [rbp+var_C]
add     rsp, 10h
pop     rbp
retn
```

# Поведение



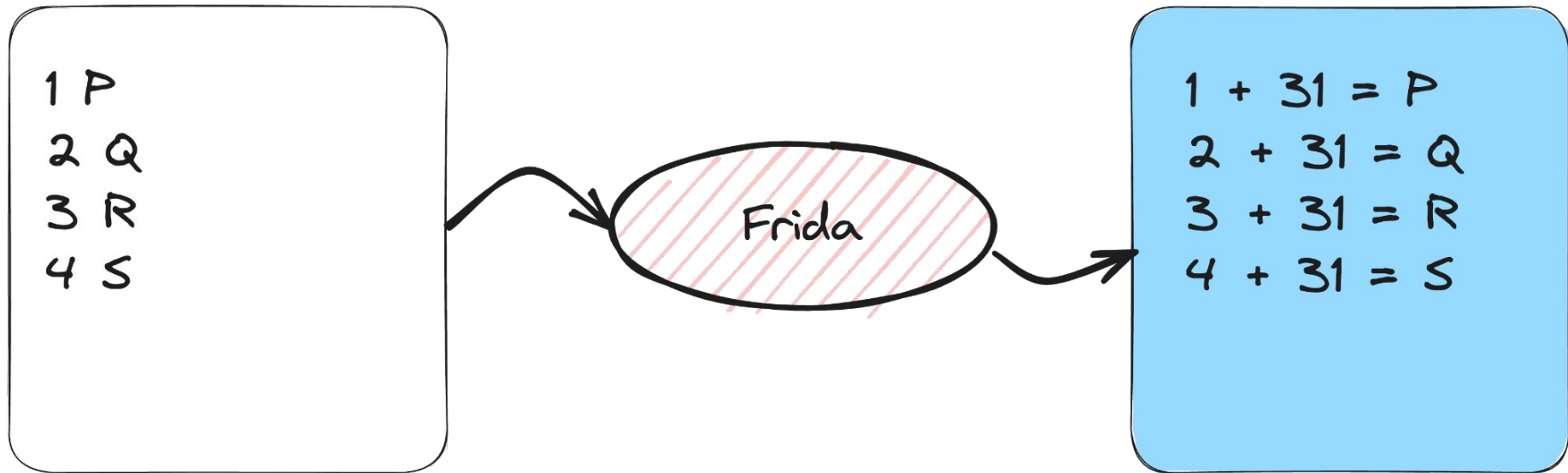


# C++. Frida. Атака на строки

```
function hook(name, count) {
  Interceptor.attach(Module.findExportByName(«libc.so», name), {
    onEnter: function(args) {
      let bt = DebugSymbol.fromAddress(
        Thread.backtrace(this.context, Backtracer.ACCURATE)[0]);
      let arg = [];
      for (var i = 0; i < count; i++){
        try {
          arg.push(Memory.readCString(args[i]));
        } catch (e) {}
      }
      if (bt.moduleName.indexOf(«crypto_lib.so») !== -1) {
        console.log(name + '(»' + arg.join('», «') + '») ' + bt);
      }
    }
  });
}
```

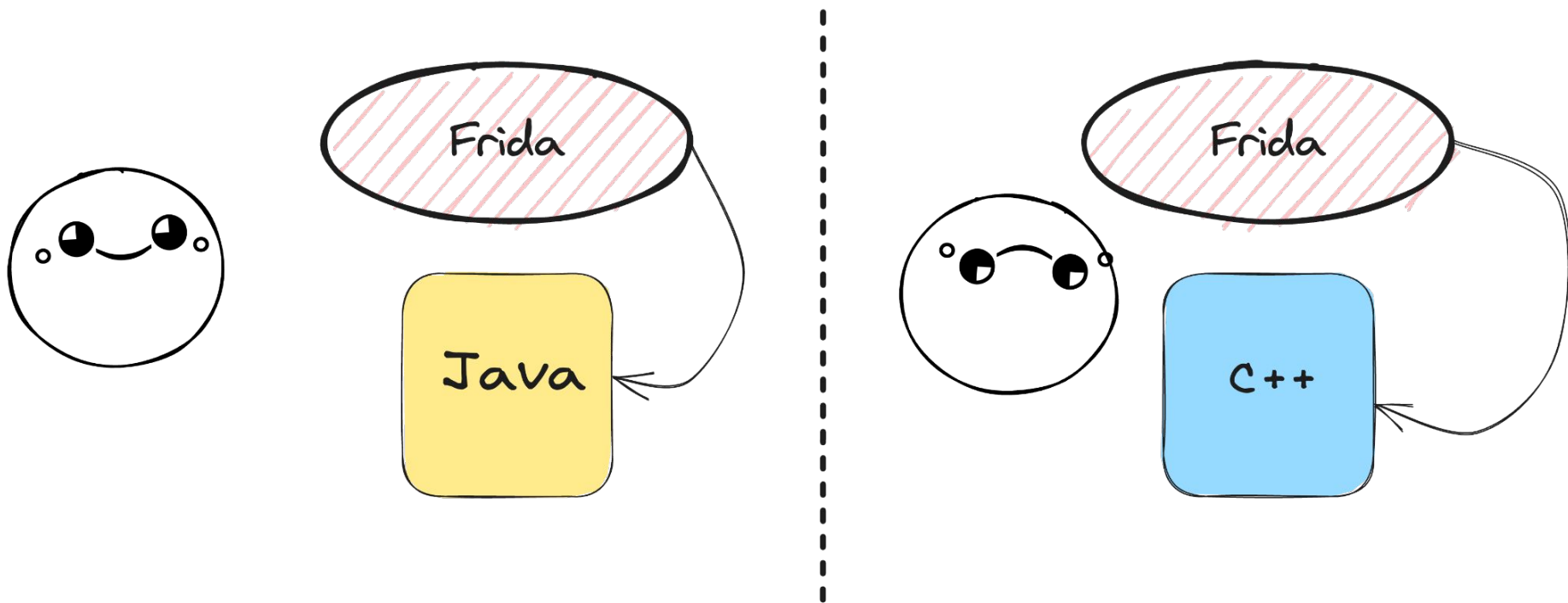
# C++. Frida. Атака на строки

```
function makeHooks() {  
    hook(«strcmp», 2);  
    hook(«strncmp», 2);  
    hook(«strncpy», 2);  
    hook(«strcat», 2);  
    hook(«strchr», 1);  
    hook(«strcpy», 2);  
    hook(«strlen», 1);  
    hook(«strrchr», 1);  
}
```

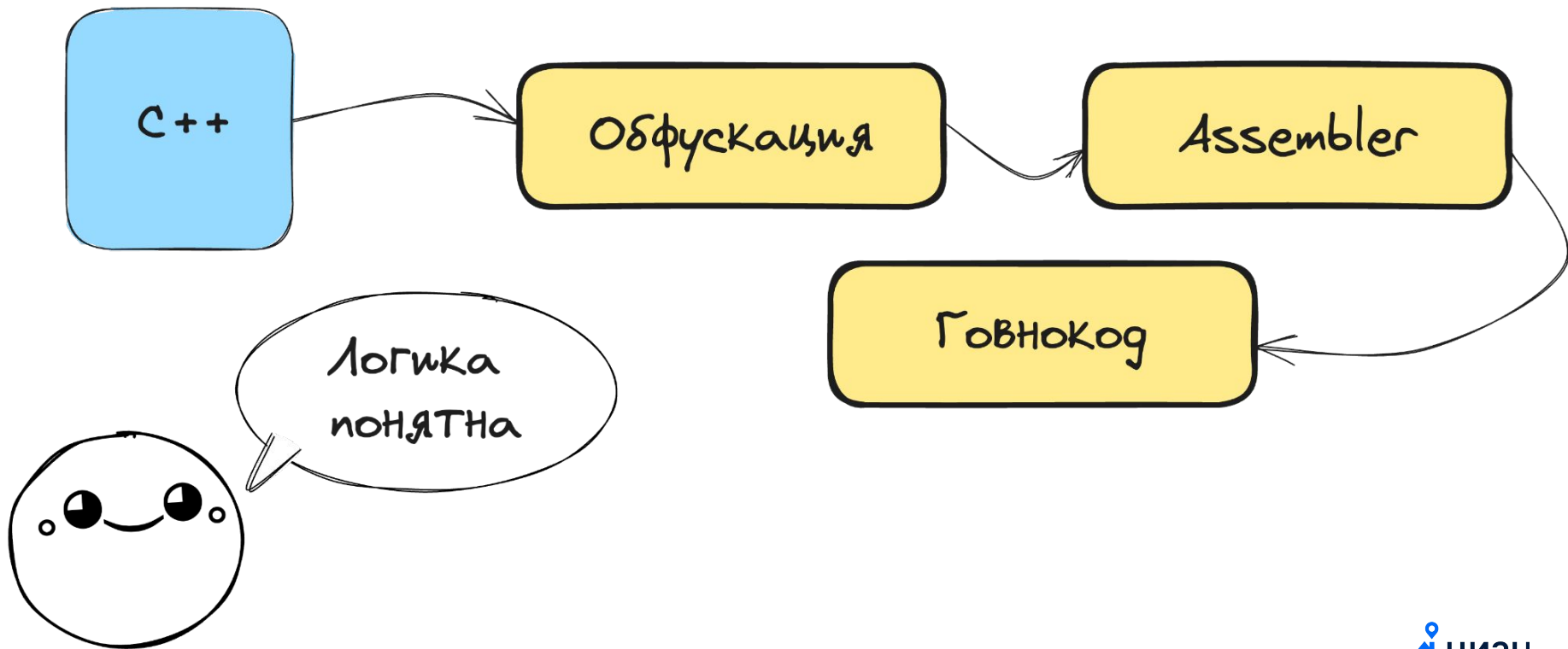




# C++. Frida. Выглядит сильно сложнее



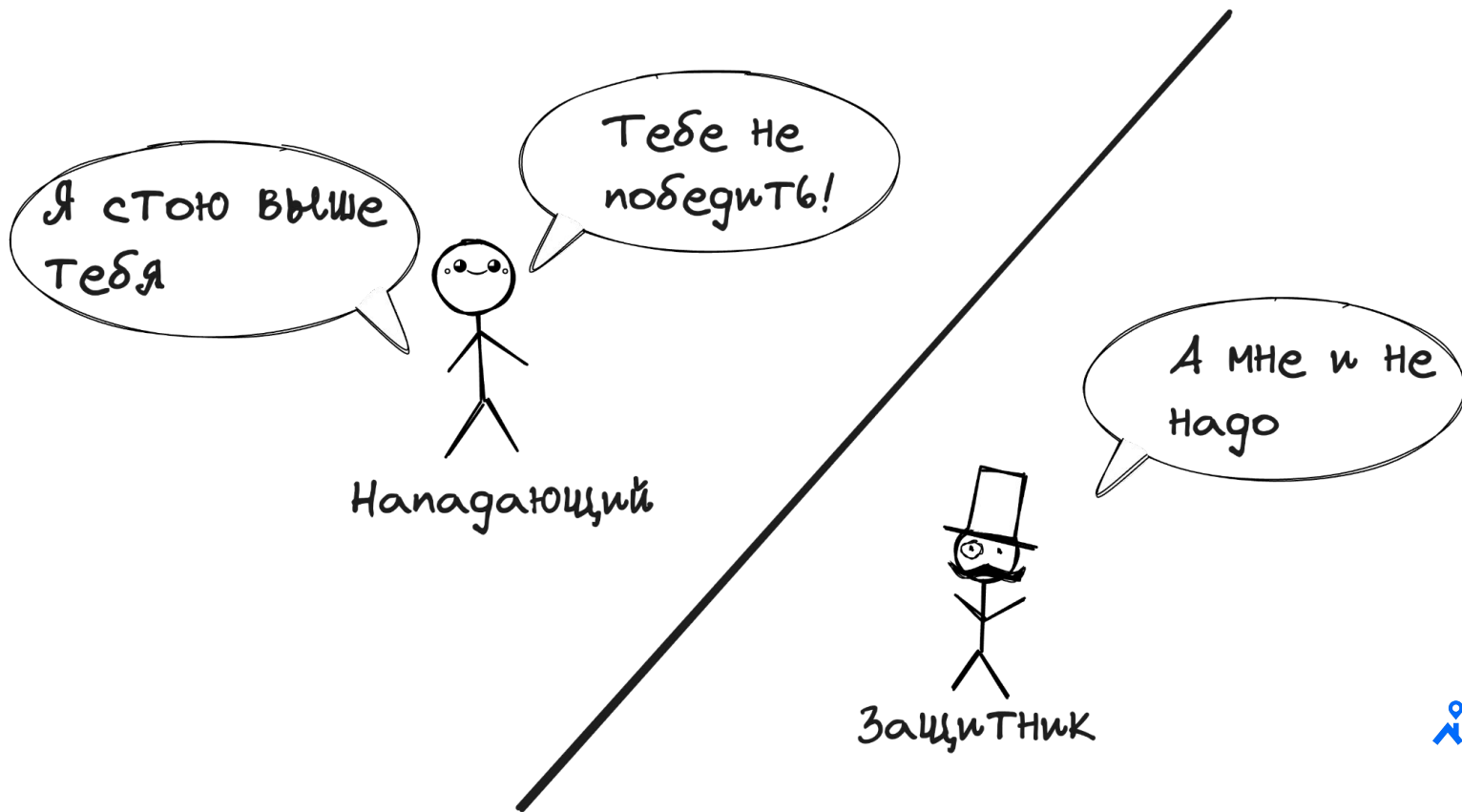
# C++. Можно идти дальше



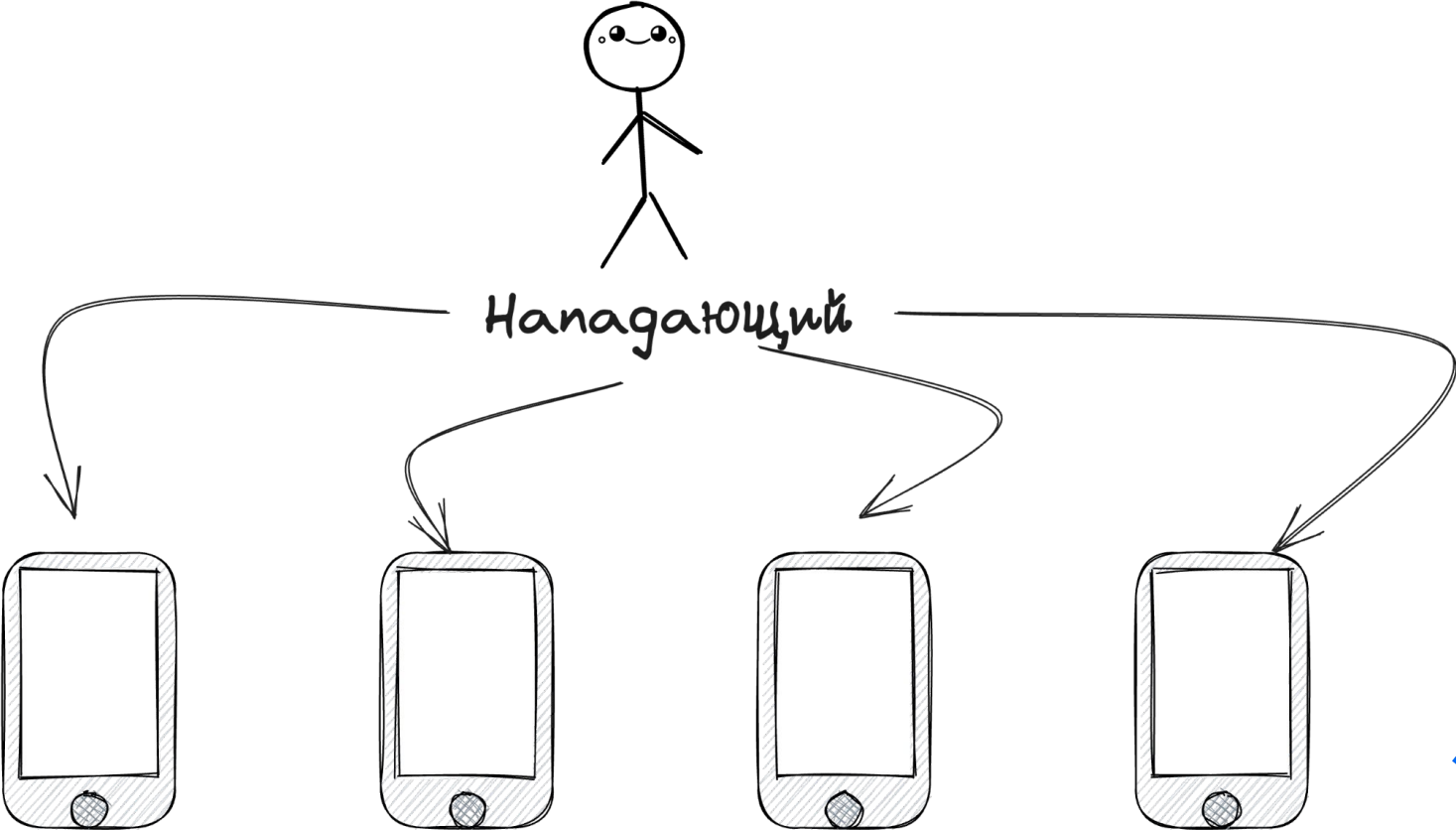
# Заключение



# Приложение не защитить



# Но стоит пытаться. Редко атакуют только вас

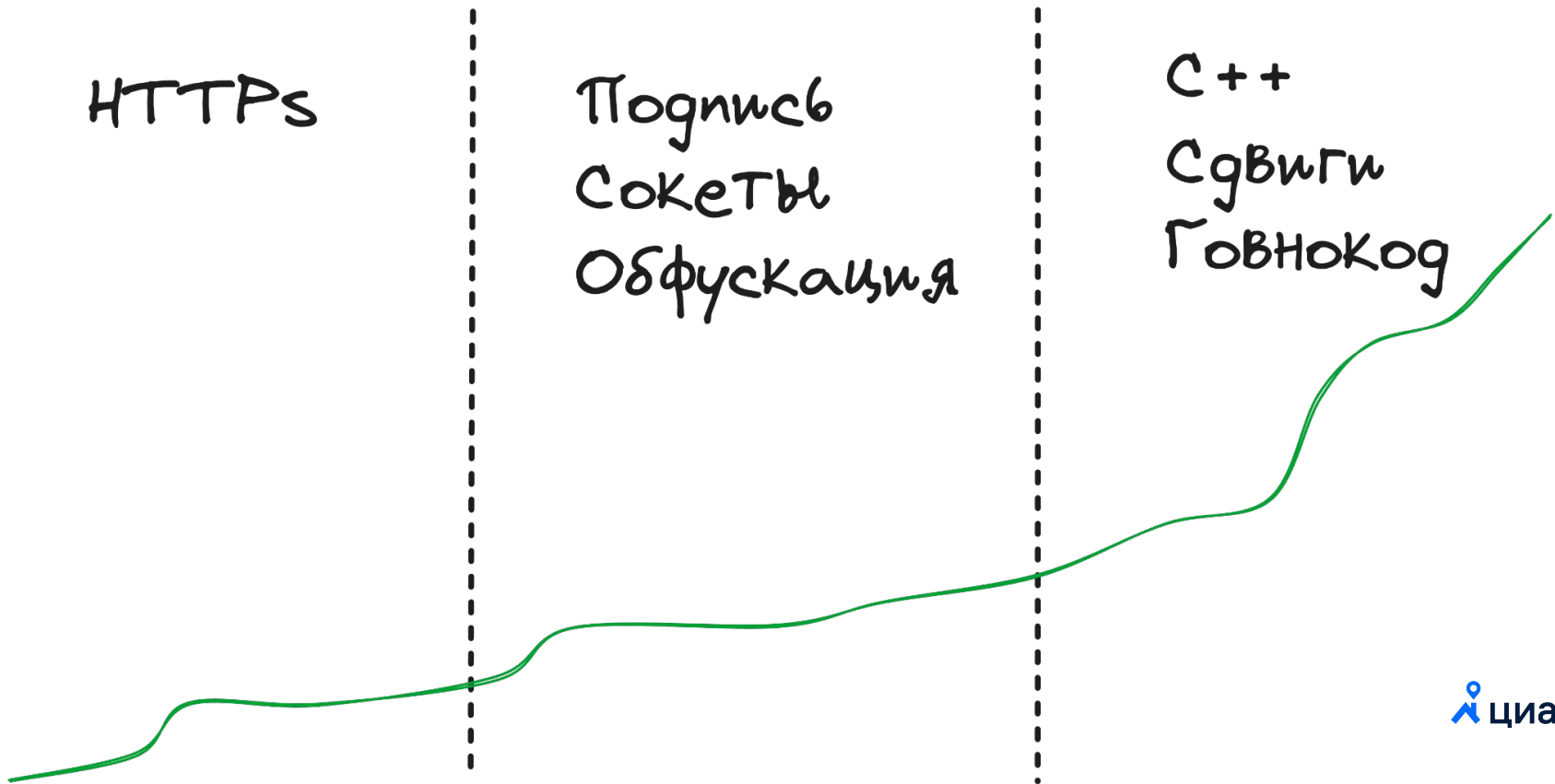


# Уровни защиты

HTTPS

Подпись  
Сокеты  
Обфускация

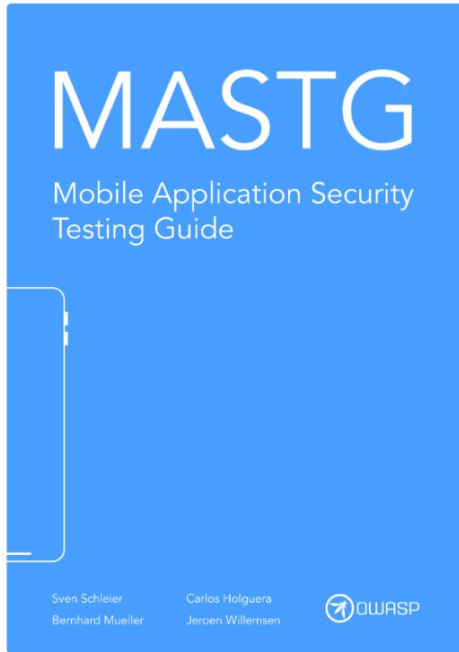
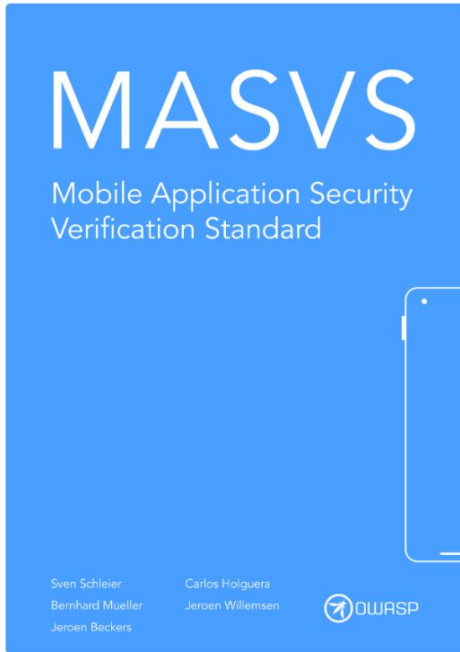
C++  
Сдвиги  
Говнокод



## OWASP MASVS

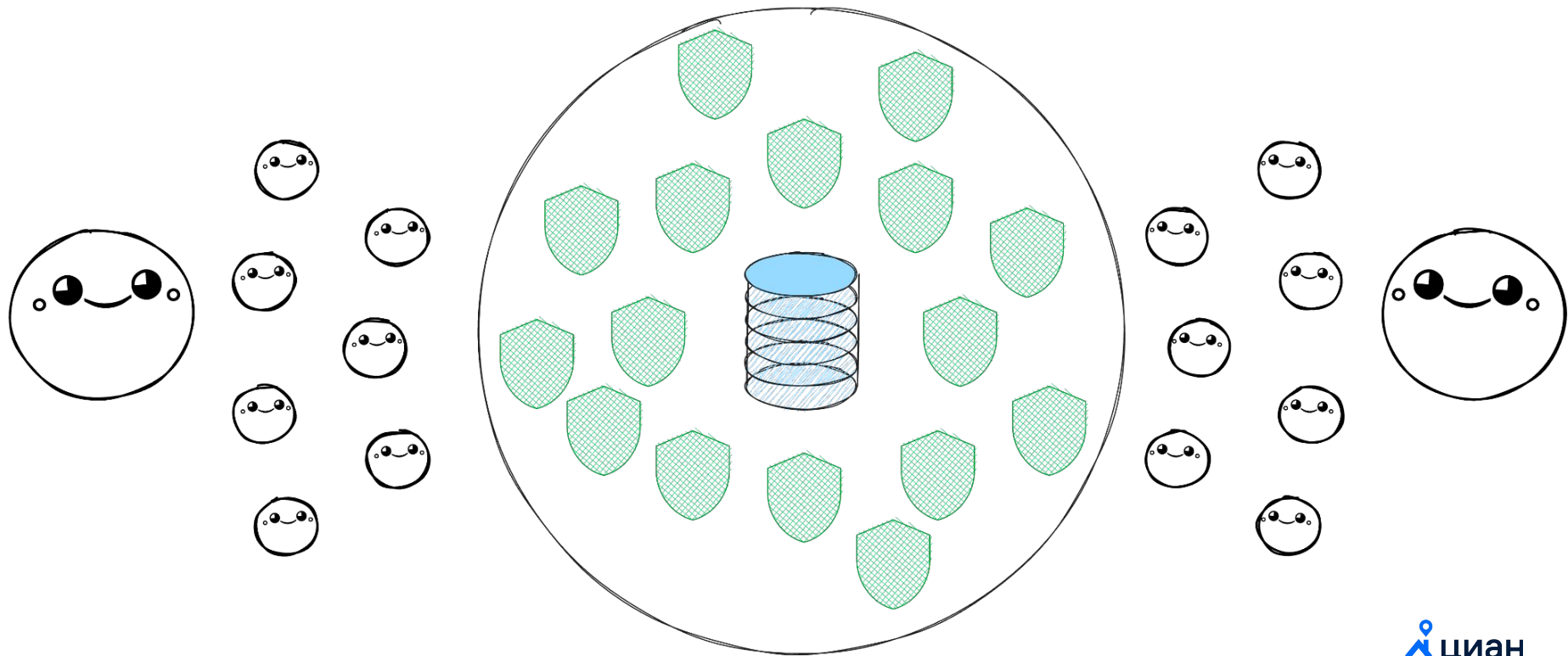
## OWASP MASTG

## OWASP MAS Checklist



MASVS-ID	Platform	Description	L1	L2	R	Status
<b>MASVS-STORAGE-1</b>		<b>The app securely stores sensitive data.</b>				
	android	<a href="#">Testing the Device-AccessSecurity.Policy</a>				Fail
	android	<a href="#">Testing Local Storage for Sensitive Data</a>				Pass
	ios	<a href="#">Testing Local Data Storage</a>				N/A
<b>MASVS-STORAGE-2</b>		<b>The app prevents leakage of sensitive data.</b>				
	android	<a href="#">Testing Logs for Sensitive Data</a>				Fail
	android	<a href="#">Determining Whether the Keyboard Cache is Disabled for Text Input Fields</a>				
	android	<a href="#">Testing Backups for Sensitive Data</a>				

# Основа защиты на backend





# Всё!



@princeparadoxes

