RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: MBS-F02

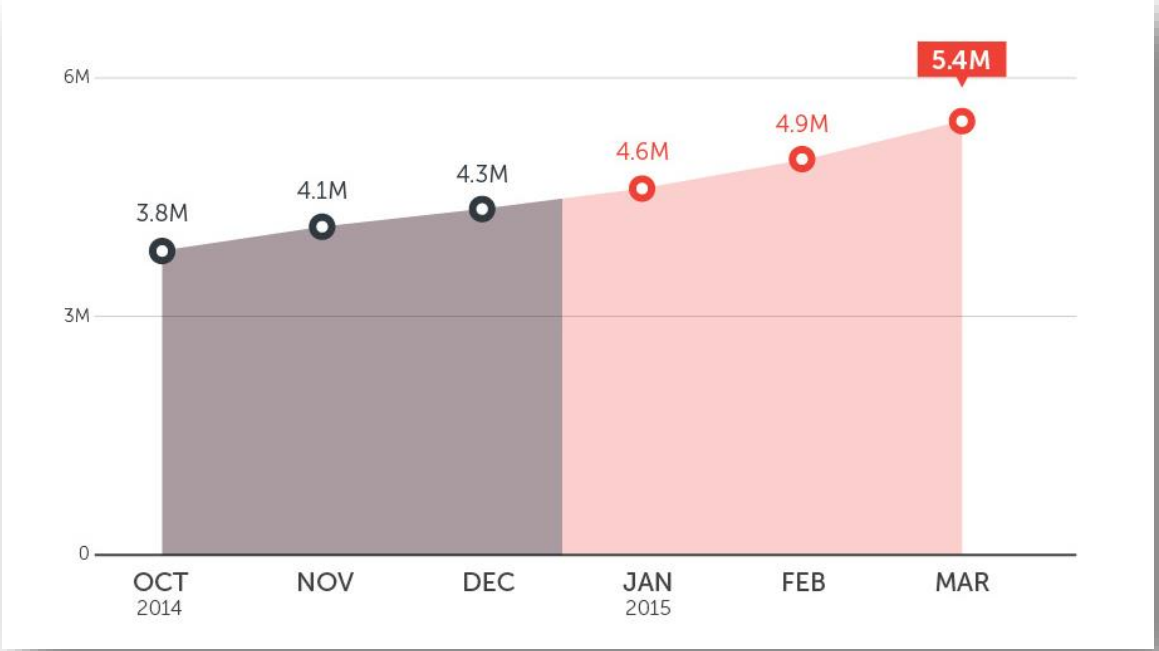
The Android Developers' Guide to 3rd-Party SDK Assessment and Security

Yang Yang(杨德志)

Mobile Security Researcher and Developer, Trend Micro

Advantages of 3rd-Party SDKs

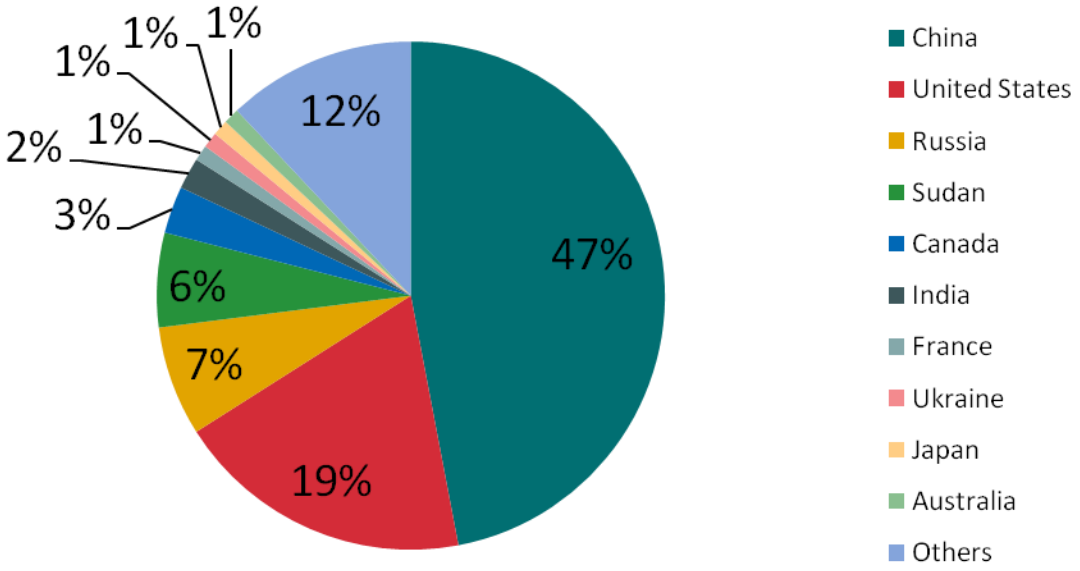
- Speed up app development
- Are easy to use
- May be of good quality (at least for some)
- *Generate profit!*



Android Threat Growth

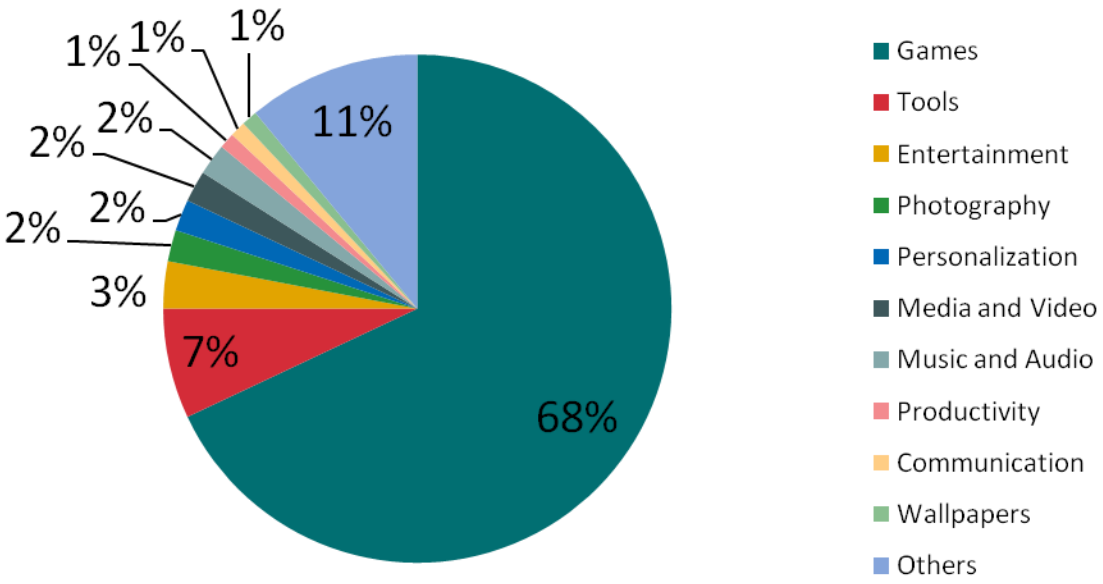
As of March 2015, Trend Micro has collected more than 5.4M malicious and high-risk applications

67% of detected apps misuse or abuse 3rd-party SDKs or use SDKs that are inherently risky



Malware/PUA Distribution by Country

Majority of the apps that misuse or abuse 3rd-party SDKs are from China



Malware/PUA Distribution by Category

Of the detected apps, games have the highest percentage, as they usually contain both advertising SDKs as well as payment SDKs.

Most security issues have something to do with advertising and payment SDKs. Why?

Popular App Business Models/SDKs

- Advertisement
  - Ad networks provide SDKs that allow developers to display advertisements
  - Ad networks pay developers, usually based on the click rate
- Payment
  - Users purchase additional features or services within the app
  - Allows users a more “direct” way to pay app developers

Security Issues with Ad SDKs

- Privacy leaks
- Insecure app installation
- Dynamic code loading
- Mobile traffic cost

Privacy Leak

```
StringBuffer v0 = new StringBuffer();
Cursor v1 = Browser.getAllVisitedUrls(this.K.getContext().getContentResolver())
if((v1.moveToFirst()) && (v1.getCount() > 0)) {
    while(!v1.isAfterLast()) {
        String v2 = v1.getString(v1.getColumnIndex("url"));
        if(v2.indexOf("http://") != v7) {
            v2 = v2.substring(7);
        }

        int v3 = 0;
        int v4;
        for(v4 = 0; v4 < v9; ++v4) {
            v3 = v2.indexOf("/", v3 + 1);
            if(v3 == v7) {
                break;
            }
        }
```

```
protected void b(JSONObject arg8) {
    ......
    v3.put("model", v2.e);
    v3.put("os", v2.f);
    v3.put("brand", v2.g);
    v3.put("sdk version", v2.h);
    v3.put("phone number", v2.i);
    v3.put("country code", v2.j);
    v3.put("carrier", v2.k);
    v3.put("cpu speed", v2.l);
    if(v2.n != null) {
        ......
        v3.put("emails", v4);
    }
    v3.put("type", "android");
    v3.put("h android id", ad.a(ad.c(v2.b), this.d));
    v3.put("h serial id", ad.a(ad.c(v2.c), this.d));
    v3.put("h wifi mac", ad.a(ad.c(v2.d), this.d));
    v3.put("h udid", ad.a(ad.c(v2.a), this.d));
    v3.put("h nn android id", ad.a(v2.b, this.d));
    v3.put("h nn serial id", ad.a(v2.c, this.d));
    v3.put("h nn wifi mac", ad.a(v2.d, this.d));
    v3.put("h nn udid", ad.a(v2.a, this.d));
    Locale v0_1 = v2.m;
    if(v0_1 != null) {
        v3.put("locale", v0_1.toString());
    }
    arg8.put("device info", v3);
    JSONObject v0_2 = new JSONObject();
    v0_2.put("package name", v1.c);
    v0_2.put("app name", v1.a);
    v0_2.put("app version", v1.b);
```

Insecure App Installation

- A special ad: Integral Wall
- Using app need virtual money
- The way to earn the virtual money
  - Step 1: Click the ad to download the apps
  - Step 2: Install them
  - Step 3: Launch the downloaded apps for a few minutes

```
public static DexClassLoader b(Context arg5) {
    String v0 = c.a;
    String v1 = Environment.getDataDirectory() + "/data/" + arg5.getApplicationContext().getPackageName()
            + "/files/";
    return new DexClassLoader(v1 + v0, v1, null, ClassLoader.getSystemClassLoader().getParent());
}
```

Dynamic Code Loading

Mobile traffic cost

- Download file before push ad
- File is too large

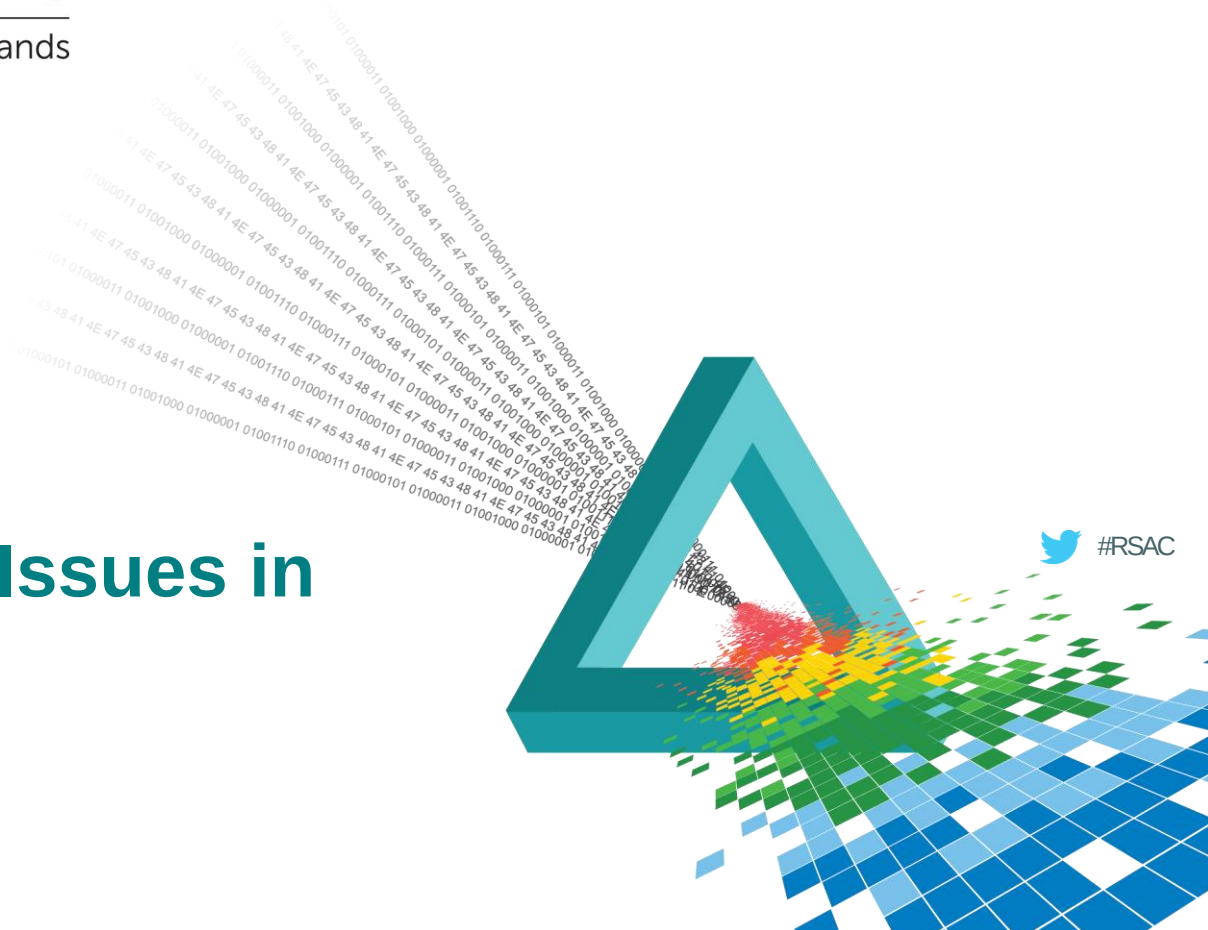
Security Issues in payment SDKs

- Send SMS (Short Message Service) message without users' explicit consent
  - E.g., user (or a child) hits the pay button by accident
  - Confirmation as a step is necessary
- Block incoming SMS message
  - Some payment SDKs can block the confirmation or notice SMS message
  - User may not know that s/he is already paying for a service or item

```
public void onReceive(Context arg8, Intent arg9) {
    FzUzitl.b(sr.a, arg9.toString());
    Object v0 = arg9.getExtras().get("pdus");
    SmsMessage[] v5 = new SmsMessage[v0.length];
    int v2 = 0;
    String v4 = "";
label_13:
    if(v2 < v0.length) {
        v5[v2] = SmsMessage.createFromPdu(v0[v2]);
        v4 = String.valueOf(v4) + v5[v2].getMessageBody();
        ++v2;
        goto label_13;
    }

    String v0_1 = v5[0].getOriginatingAddress();
    FzUzitl.checkAppStatus(arg8);
    if(w.a().b(v0_1, v4)) {
        this.abortBroadcast();
        return;
    }
```

Block incoming SMS



General Security Issues in 3rd-Party SDKs

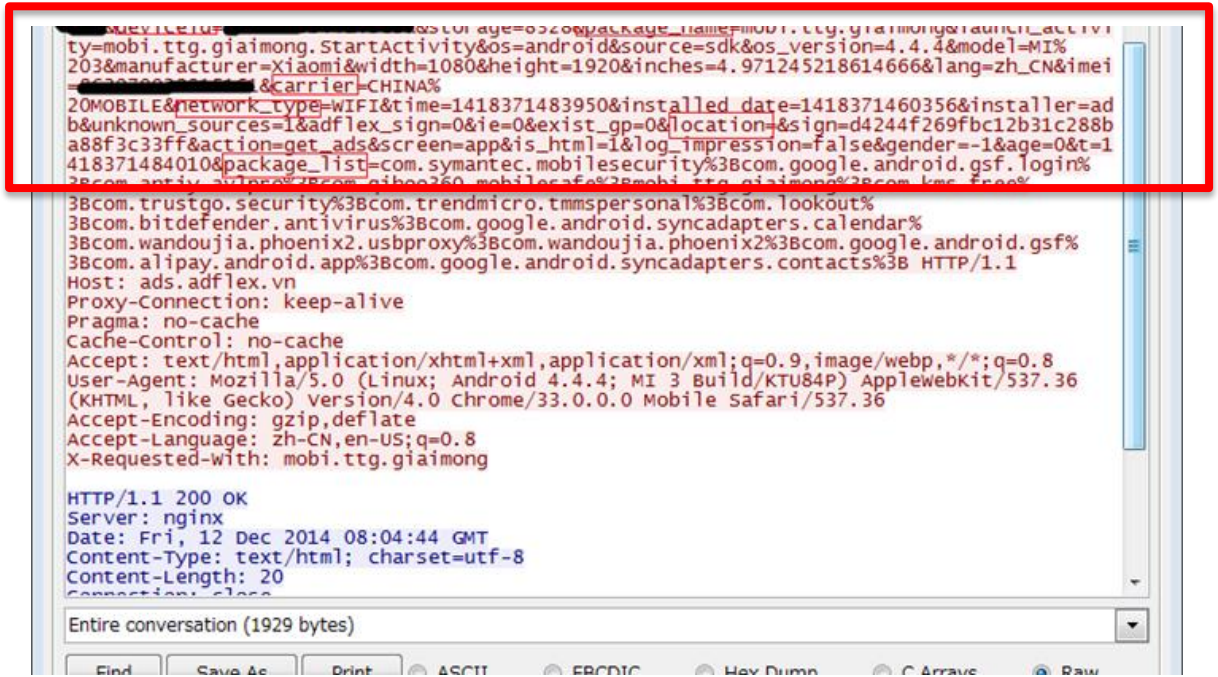
General Security Issues

- Vulnerabilities related
- Insecure network transmission
- Insecure online setting
- Insecure data storage
- Insecure data sharing

```
@SuppressLint(value={"SetJavaScriptEnabled"}) private void e() {
    this.W = this.V;
    IMWebView.userInitiatedClose = false;
    this.setScrollContainer(false);
    this.setVerticalScrollBarEnabled(false);
    this.setHorizontalScrollBarEnabled(false);
    this.webviewUserAgent = this.getSettings().getUserAgentString();
    this.setBackgroundColor(0);
    this.getContext().getSystemService("window").getDefaultDisplay().getMe
    this.d = this.V.getResources().getDisplayMetrics().density;
    this.b = false;
    this.getSettings().setJavaScriptEnabled(true);
    this.c = new JSUtilityController(this, this.getContext());
    this.addJavascriptInterface(this.c, "utilityController");
    this.setWebViewClient(this.J);
    this.setWebChromeClient(this.O);
    this.H = this.V.getSystemService("window").getDefaultDisplay();
    this.n = this.V.getResources().getDisplayMetrics().widthPixels;
}
```

SDK impacted by OS vulnerability

Android API WebView vulnerability (CVE-2012-6636)



Insecure network transmission

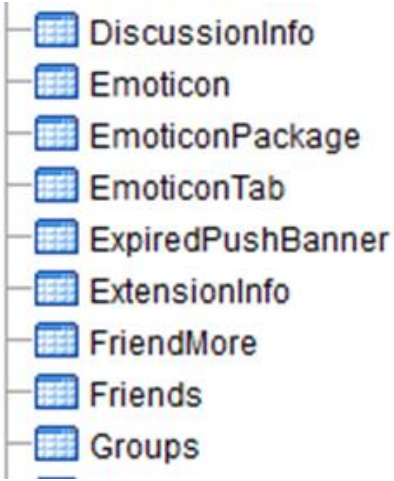
```
protected void loadConfig() {
    ConfigXmlParser parser = new ConfigXmlParser();
    parser.parse(this);
    preferences = parser.getPreferences();
    preferences.setPreferencesBundle(getIntent().getExtras());
    preferences.copyIntoIntentExtras(this);
    launchUrl = parser.getLaunchUrl();
    pluginEntries = parser.getPluginEntries();
    Config.parser = parser;
}
```

Insecure online setting

Apache Cordova vulnerability (CVE-2015-1835)

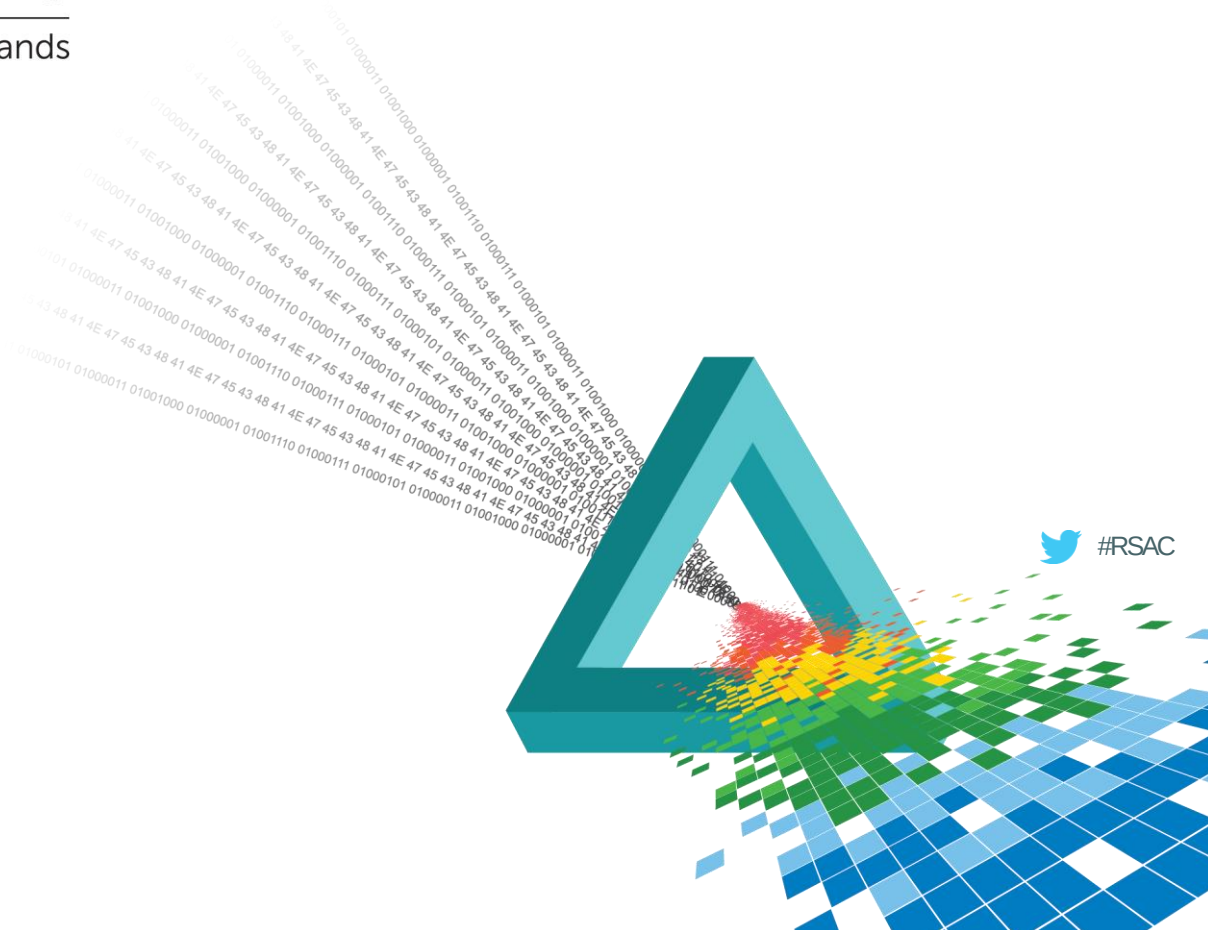
Insecure data storage

- Insecure database
- Insecure sdcard storage



Insecure data sharing

- Android Content Provider
- Share your data with enough limitation



Best Practices

For SDK Developers and Providers

- Provide clear end-user license agreements (EULAs)
- Make the SDK document as clear as possible

  eg: https://developers.google.com/admob/android/quick-start
- Limit collection user information
- Add more limitations for exported interface
- Pay attention to vulnerabilities; provide updated SDKs as necessary
- Online control SDK logic is not recommended

For Mobile App Developers

- *Read the SDK documents carefully*
- Choose 3rd-party SDKs carefully
- Avoid using the aggressive interface (APIs)
- When using ad SDKs, make sure that the apps do not push ads too frequently or impact other apps
- Update to the latest SDK versions
- Advise users if your app has aggressive behavior

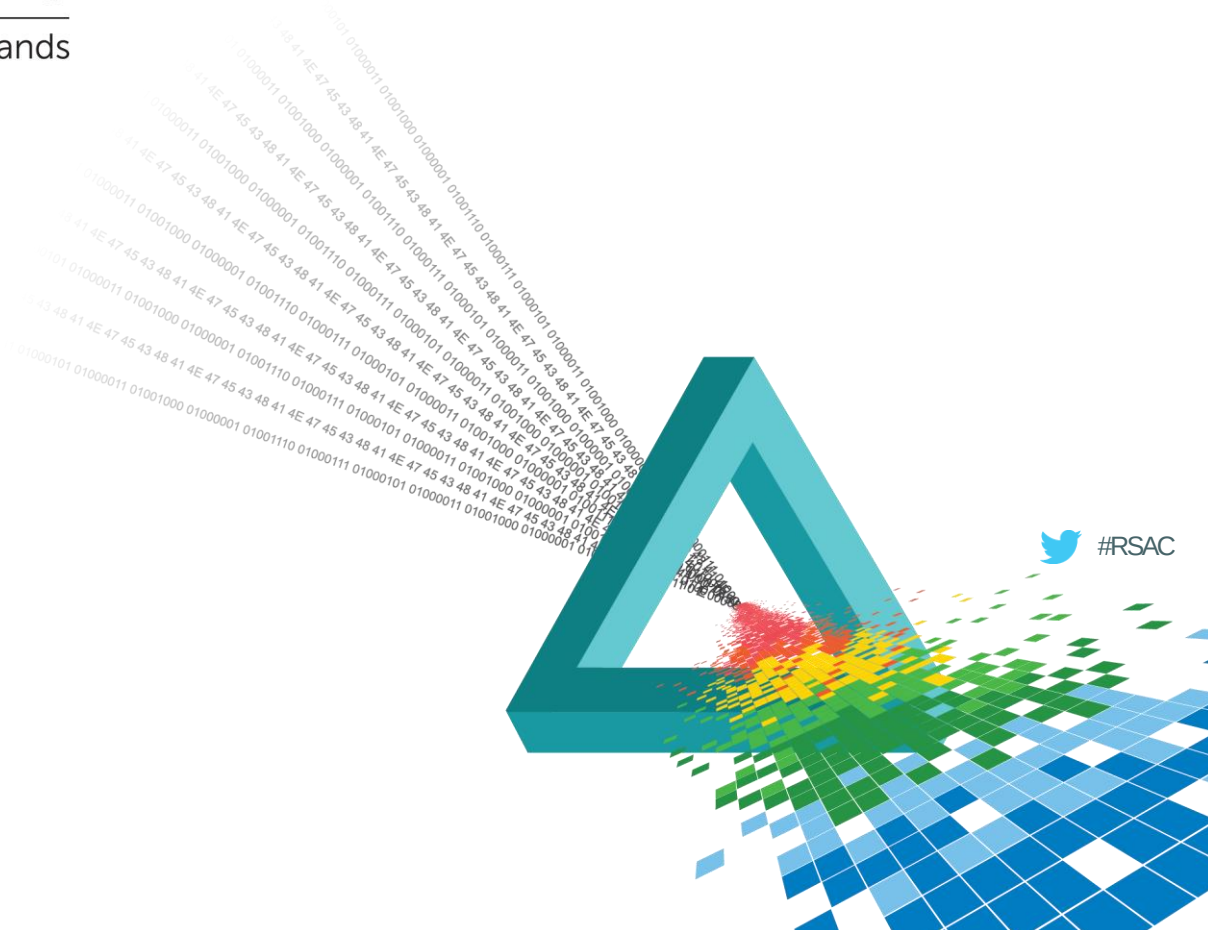
Developers should pay attention to software security!

- Encrypt sensitive data
- Use packers to protect your applications
- Use “high-risk” app permissions with caution
- Push app or data updates app via the app store

Summary

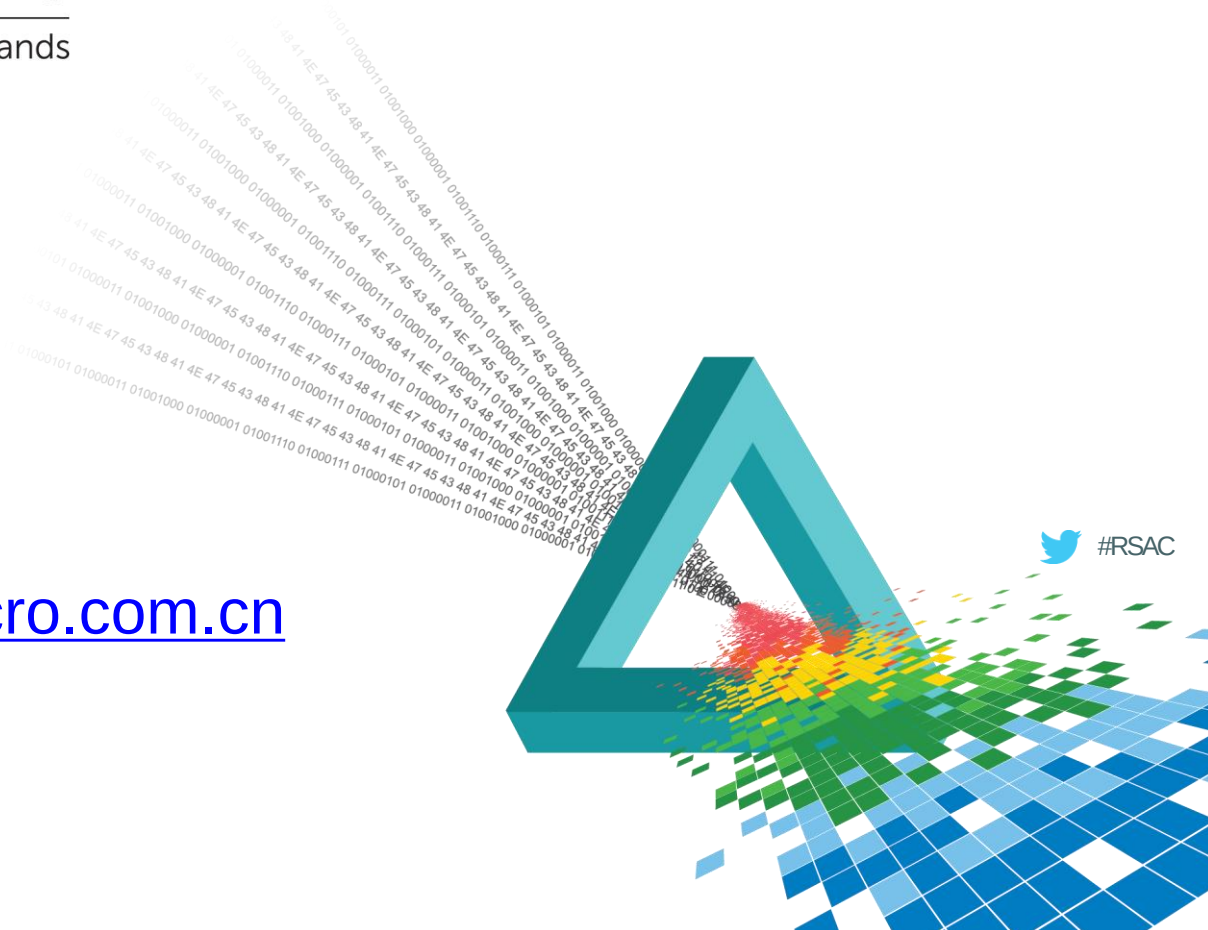
- Ease of use and Profit
- 3 in 5 Android theats are caused by 3rd-party SDKs
- Mobile security involves all aspects in the ecosystem, including SDK providers and app developers

Questions?



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



Thank You!

yang_yang@trendmicro.com.cn