HNSF
Health Network Security Forum 2017
医疗网络安全论坛

第三届雪野湖医疗网络安全技术论坛

当前全省二级以上医院网络安全工作存在的主要风险和应对建议

山东省信息网络安全协会副会长　　张朝伦

个人简介

公安部网络安全等级保护地方专家组成员

公安部网络安全等级保护高级测评师

公安部网络安全等级保护管理师培训CIIP-T讲师

山东省网络安全等级保护工作协调小组专家组成员

青岛市电子政务与大数据发展委员会网络安全专委会专家

山东省卫健委网络安全专家组成员

中国中医信息研究会信息安全分会副会长

山东省网络安全与信息化技术创新发展联盟理事长

山东省信息网络安全协会副会长

山东国维信息安全培训中心主任

医院网络安全工作现场互动

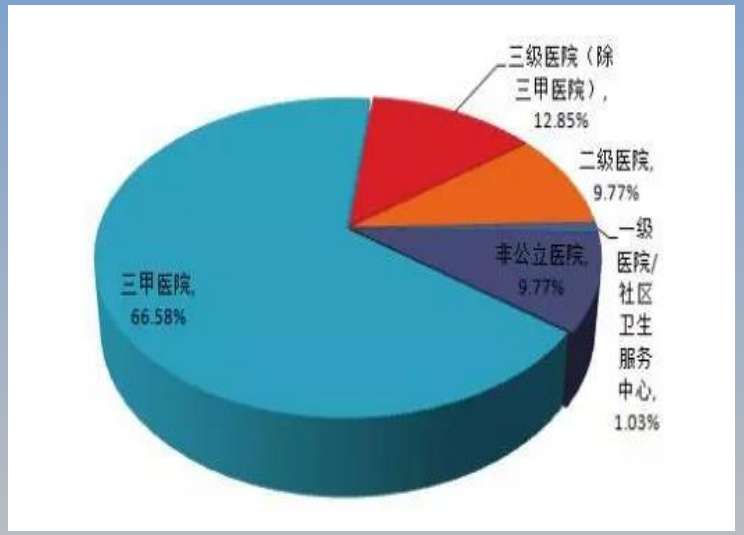
- 1、通过查看网络安全设备日志或日志服务器记录发现了网络攻击事件，并做到对新的攻击提前预警。
- 2、通过数据库审计系统中发现了网络攻击事件，并做到对新的攻击提前预警。
- 3、通过网络安全态势感知系统发现了网络攻击事件，并做到对勒索病毒的提前预警。
- 4、医院信息化人员在医院的地位和待遇大幅提高

·CHIMA 2019 医院信息安全调查报告

中国医院协会信息专业委员会

CHIMA 2019 医院信息安全调查报告

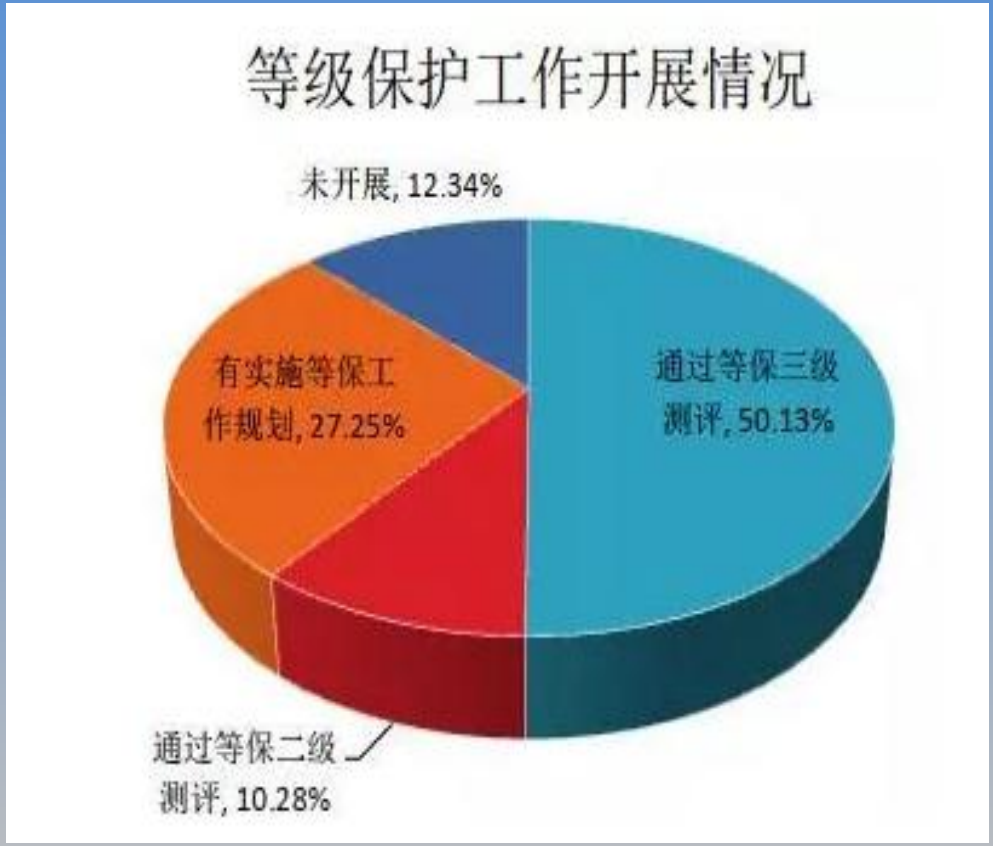
本次调查受访者共计 400 人，以医院信息化工作者为主，占总受访人群的 86.75%。其中，主管信息院领导为 38 人，占比 9.5%；信息部门主管 158 人，占比 39.5%；信息部门员工 144 人，占比 36%。另外，HIT 企业人员占 10%，其他 6%。



在近三年医院信息化建设重点内容的调查排名前三位的是，重点建设患者服务系统（挂号APP、自助机等）的医院为 226 家，占比58.10%，重点建设医院管理系统（HRP、BI、财务系统等）的医院为212 家，占比 54.50%，重点建设 HIS 以外的业务系统（EMR、LIS、PACS、超声等）的医院为 203 家，占比52.19%。

.

至少有一个系统通过等保三级测评的受访医院共计 195 家，占比 50.13%；通过等保二级测评的受访医院共计 40 家，占比 10.28%；有实施等保工作规划的医院有 106 家，占比 27.25%；没有开展等保工作规划的医院有 48 家，占比 12.34%。



在对操作系统级安全措施的调查中发现，上线网络版病毒软件的医院共计 314 家，占比 80.72%；上线桌面管理软件的医院共计 226 家，占比 58.10%；上线软件防火墙的医院共有 194 家，占比 49.87%；未采用任何措施的医院仍有 7 家，占比 1.80%。

在应用系统级安全措施方面，排名前三位的分别是：用户权限控制、多级授权密码以及应用系统级灾难恢复。其中采取用户权限控制的医院共有 330 家，占比 84.83%；采用多级授权密码的医院是 203 家，占比 52.19%；应用系统级灾难恢复的医院共有 198 家，占比 50.90%。

开展数据灾备的医院共有 287 家，占比 73.78%；采取数据离线存储的医院共有 205 家，占比 52.70%；进行数据脱敏的医院共计 143 家，占比 36.76%；未采取数据安全保障措施的医院仍有 13 家，占比 3.34%。

在网络环境中，为防止患者个人隐私数据丢失、篡改、泄露或损坏，医院采取了系列信息安全防范技术措施，包括设置防火墙、安装防病毒软件、配置 VPN 等。在本次调查中，网络安全防范措施排名前三位的分别是：设置了防火墙的医院共有 327 家，占比 84.06%；上线防病毒软件的医院共计 232 家，占比 59.64%；配置 VPN 的医院共有 219 家，占比 56.30%。

存在问题

1、不同医院网络安全等级保护工作推进差异较大
2、网络安全专职人员偏少，需加强培训
3、网络安全投入有待增加
4、对网络安全和数据安全重视程度需要普及

·2018年全省卫生健康行业网络安全检查情况的通报

2016-2018年信息化投资总额约为2.44亿元，其中网络安全建设专项资金投入总额约为0.3亿元，约占信息化投资总额的12%；46家医院2016-2018年信息化投资总额约为10亿元，其中网络安全建设专项资金投入总额约为1.69亿元，约占信息化投资总额的16.9%，比以往有较大提高；安全经费占信息化费用比例≥10%的单位数量超过50家。

各市卫生健康委（卫生计生委）中有12市完成网络安全等级测评工作，占全部单位的70%；46家医院中有34家单位完成了网络安全等级保护评测工作，占全部单位的74%。仍有部分单位未按规定完成网络等级保护测评工作。90%以上的单位与评测机构签订安全保密协议。

46家医疗机构L5级、L4级、L3级、L2级、L1级单位数量分别是0家、6家、10家、18家和12家。17市卫生健康委L5级、L4级、L3级、L2级、L1级单位数量分别是0家、2家、3家、8家和4家。

市级卫生健康委（卫生计生委）、二级以上医院、疾控中心、卫生监督所、血液中心网站开展漏洞底监测结果，发现90%以上的网站存在安全隐患，20%以上的网站存在高风险漏洞单位相对集中，90%以上出现漏洞的单位网站的并未作安全加固。

存在问题

1、网络安全责任制仍需进一步落实到位
2、对网络安全的重视程度仍需进一步提高
3、网络安全整改工作需要进一步加大力度落实
4、网络安全管理体系建设亟待进一步完善
5、网络安全专业技术人才队伍建设有待于进一步加强。
6、网络安全资金保障没有形成长效机制。
7、网络安全合规建设亟需加强
8、互联网医疗等新业态网络安全亟须进一步加强

·2018年医院网络安全调研情况

总体情况

- 1、院领导网络安全认识有不同程度提高；
- 2、医院网络安全方面投入不断加大；
- 3、医院信息科技队伍逐步壮大；
- 4、医院网络安全管理制度逐步完善；

存在的主要风险

- **1、源代码漏洞严重。**
- 网站代码、业务系统代码、APP代码等漏洞

- 系统上线前没有经过第三方安全检测、系系统上线后也没有经过检测

敏感信息泄露： 某癫痫病医院APP

com/hxyt/sddxbyy/application/MyApplication.java:538

APP在进行网络请求时，会发送用户的账号，密码到服务器。此处的风险有两处。一是使用了未加密的http链接，因此整个信息传送是明文的，可被轻易地监听。其次是在538行，将提交的信息中的每一个字段都明文打印到了日志里。其他的app通过监听日志就能完整获取app和服务器通信的**每一个细节**。包括525行的用户密码。监听者既可用用户名、密码登录对象的账号

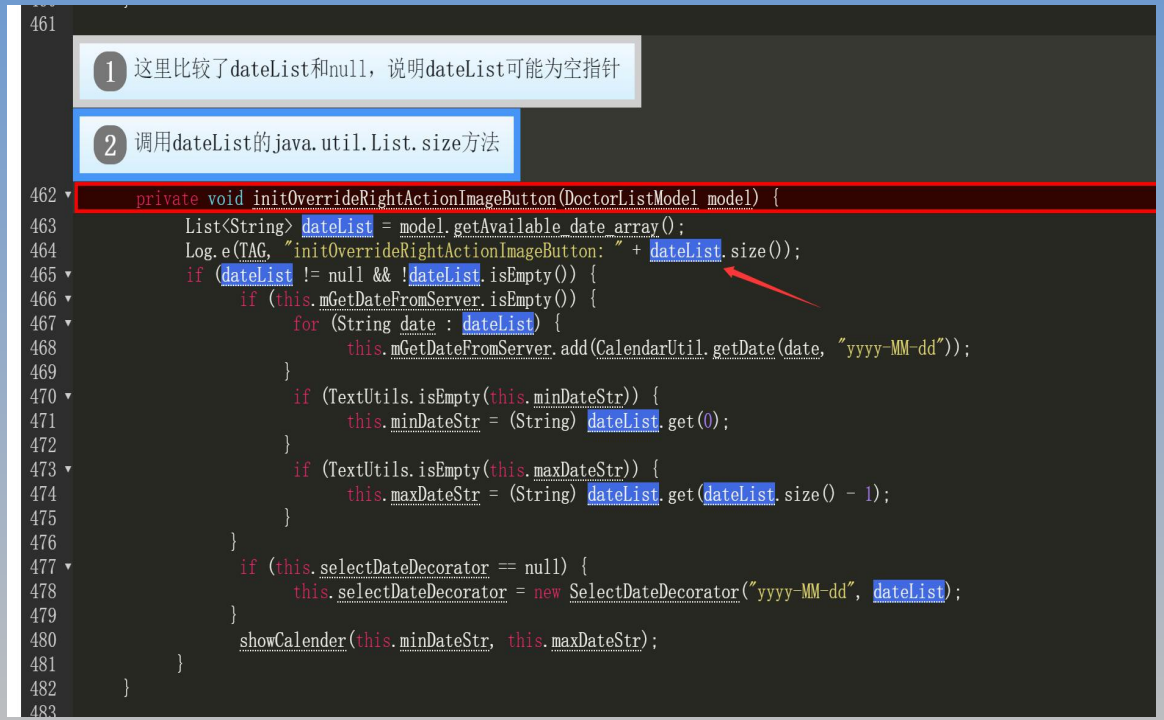
1 "http://kswdx.huixinyt.com/Appntws/PostMsgImg.aspx" may be hard-coded URL, which may incur information leak

```
506             HttpURLConnection conn = (HttpURLConnection) new URL("http://kswdx.huixinyt.com/Appntws/PostMsgImg.aspx").openConnection();
507             conn.setReadTimeout(100000000);
508             conn.setConnectTimeout(100000000);
509             conn.setDoInput(true);
510             conn.setDoOutput(true);
511             conn.setUseCaches(false);
512             conn.setRequestMethod(Constants.HTTP_POST);
513             conn.setRequestProperty("Charset", "utf-8");
514             conn.setRequestProperty("connection", "keep-alive");
515             conn.setRequestProperty(com.baidu.tts.loopj.AsyncHttpClient.HEADER_CONTENT_TYPE, content_type + ";boundary=" + boundary);
516             DataOutputStream dos = new DataOutputStream(conn.getOutputStream());
517             StringBuffer stringBuffer = new StringBuffer();
518             stringBuffer.append(prefix);
519             stringBuffer.append(boundary);
520             stringBuffer.append(end);
521             dos.write(stringBuffer.toString().getBytes());
522             Map<String, String> params = new HashMap();
523             params.put("userId", userId);
524             params.put("content", content);
525             params.put("userPwd", userPwd);
526             for (Entry<String, String> entry : params.entrySet()) {
527                 String map = String.valueOf(entry.getKey());
528                 stringBuffer.append(prefix);
529                 stringBuffer.append(boundary);
530                 stringBuffer.append(end);
531                 stringBuffer.append("Content-Disposition: form-data; name=\"" + map + "\" --");
532                 stringBuffer.append("Content-Type: text/plain; charset=" + CHARSET + end);
533                 stringBuffer.append("Content-Transfer-Encoding: 8bit" + end);
534                 stringBuffer.append(end);
535                 stringBuffer.append((String) entry.getValue());
536                 stringBuffer.append(end);
537             }
538             Log.e("res---sb---", stringBuffer.toString() + "");
539             Log.e("post", "post_running");
```

崩溃闪退类缺陷：某县人民医院APP

com/health/patient/taborder2/HosDepartmentFragment2.java:462行

写APP的时候，总是会对传输的数据做一些判断，进行保护。因为网络可能不稳定，比如拉日期列表的函数，拿到的日期列表就不一定有数据。所以会有一个判断是否为空的保护(第465行)。但是在判断之前，程序员好意地打了一句日志。这句日志没有判空保护。所以实际上如果网络不好，打日志的时候，app就会闪退（第464行红色箭头处）。




```
461
462     private void initOverrideRightActionImageButton(DoctorListModel model) {
463         List<String> dateList = model.getAvailable_date_array();
464         Log.e(TAG, "initOverrideRightActionImageButton: " + dateList.size());
465         if (dateList != null && !dateList.isEmpty()) {
466             if (this.mGetDateFromServer.isEmpty()) {
467                 for (String date : dateList) {
468                     this.mGetDateFromServer.add(CalendarUtil.getDate(date, "yyyy-MM-dd"));
469                 }
470                 if (TextUtils.isEmpty(this.minDateStr)) {
471                     this.minDateStr = (String) dateList.get(0);
472                 }
473                 if (TextUtils.isEmpty(this.maxDateStr)) {
474                     this.maxDateStr = (String) dateList.get(dateList.size() - 1);
475                 }
476             }
477             if (this.selectDateDecorator == null) {
478                 this.selectDateDecorator = new SelectDateDecorator("yyyy-MM-dd", dateList);
479             }
480             showCalender(this.minDateStr, this.maxDateStr);
481         }
482     }
483
```

发现位置：某妇幼保健院APP

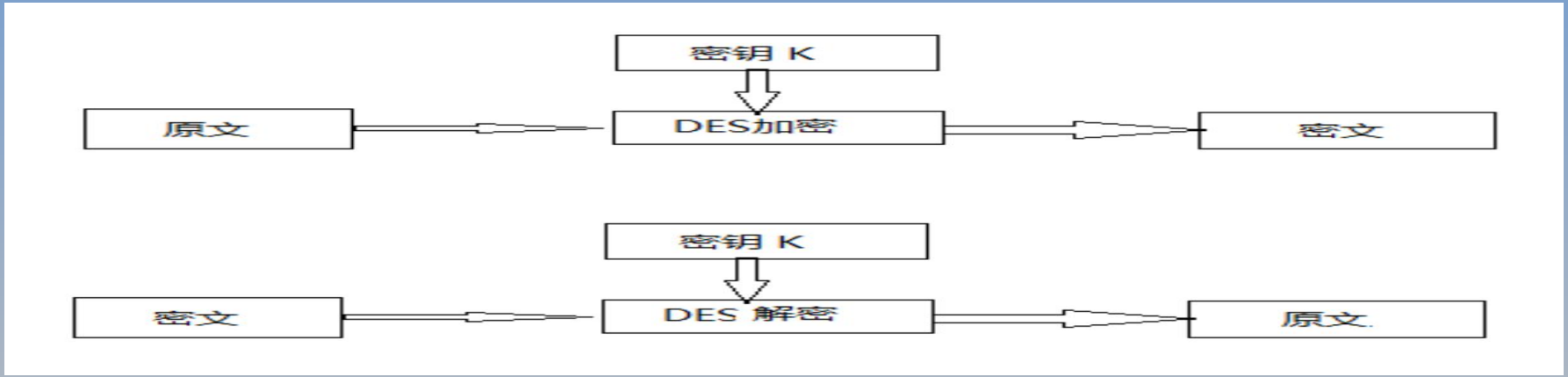
com/rubik/ucmed/rubikwaplink/utils/WebViewUtils.java:113

```
103                 WebViewUtils.c = false;
104                 wapLinkBaseFragment.a();
105                 wapLinkBaseFragment.a(str);
106             }
107
108             public void onPageFinished(WebView webView, String str) {
109                 super.onPageFinished(webView, str);
110                 wapLinkBaseFragment.a(str);
111                 ViewUtils.a(webView, WebViewUtils.c);
112                 ViewUtils.a(view, !WebViewUtils.c);
113                 if (!(wapLinkBaseFragment == null || wapLinkBaseFragment.getActivity().isFinishing())) {
114                     wapLinkBaseFragment.b();
115                 }
116                 wapLinkBaseFragment.d();
117                 wapLinkBaseFragment.b((String) WebViewUtils.b.get(str));
118             }
119
```

硬编码密码：某医院APP

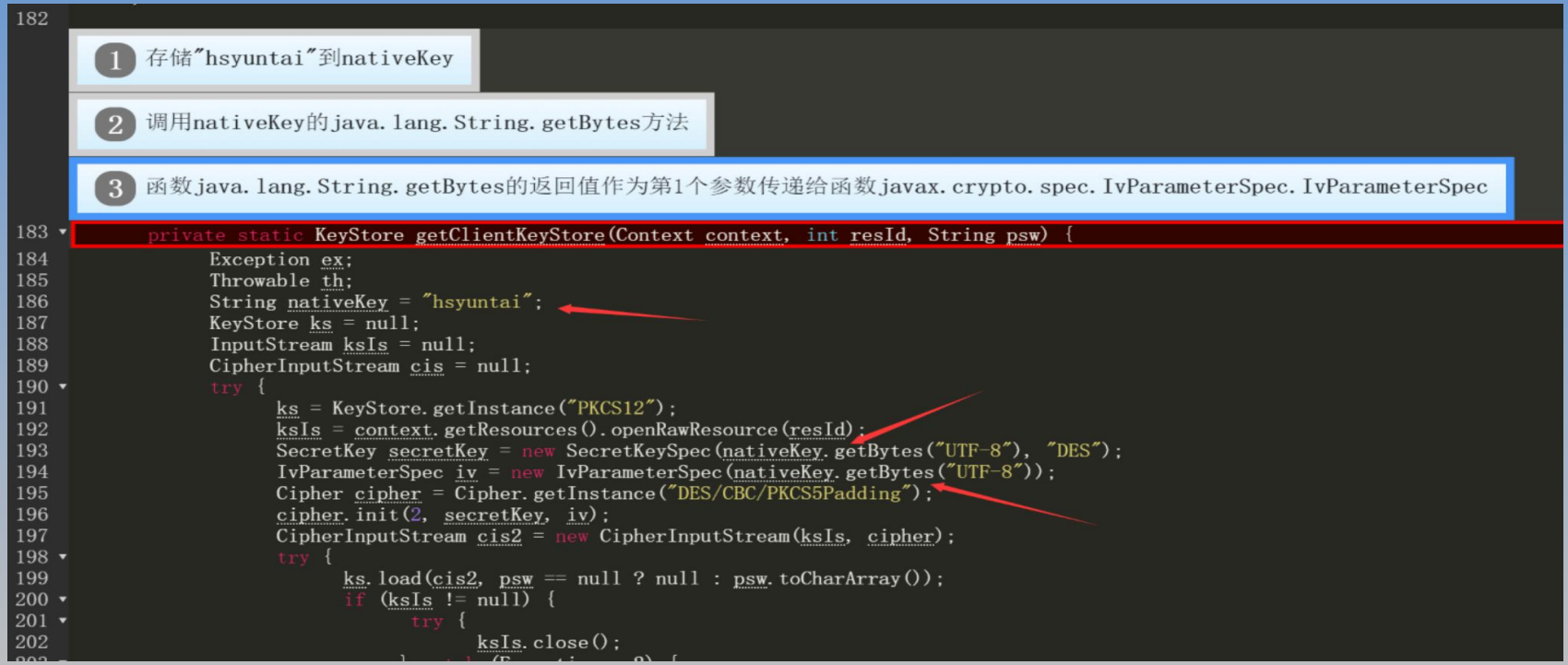
com/hundsun/net/factory/HundsunSSLSocketFactory.java:183

此处使用了DES加密，DES是一种对称加密手段，双方通过相同的密码加密文本，这样信息被拦截或窃听时就不会暴露。



同时，为了防止撞库攻击（通过加密后的文本推断原文），DES加密会使用一个IV向量，使得每次生成的密文都不同。前提条件是，IV初始化向量使用安全的随机数生成器，随机生成。

在此处，有两个误用，一是把对称加密的密钥”hsyuntai”直接写在代码中。在193行作为密钥直接使用。第二个误用是在第194行将密钥同时用于IV初始化向量。大大降低了通信的安全性。




```
182
183     private static KeyStore getClientKeyStore(Context context, int resId, String psw) {
184         Exception ex;
185         Throwable th;
186         String nativeKey = "hsyuntai";
187         KeyStore ks = null;
188         InputStream ksIs = null;
189         CipherInputStream cis = null;
190         try {
191             ks = KeyStore.getInstance("PKCS12");
192             ksIs = context.getResources().openRawResource(resId);
193             SecretKey secretKey = new SecretKeySpec(nativeKey.getBytes("UTF-8"), "DES");
194             IvParameterSpec iv = new IvParameterSpec(nativeKey.getBytes("UTF-8"));
195             Cipher cipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
196             cipher.init(2, secretKey, iv);
197             CipherInputStream cis2 = new CipherInputStream(ksIs, cipher);
198             try {
199                 ks.load(cis2, psw == null ? null : psw.toCharArray());
200                 if (ksIs != null) {
201                     try {
202                         ksIs.close();
```

某县人民医院APP
com/yht/util/Des3Util.java:17

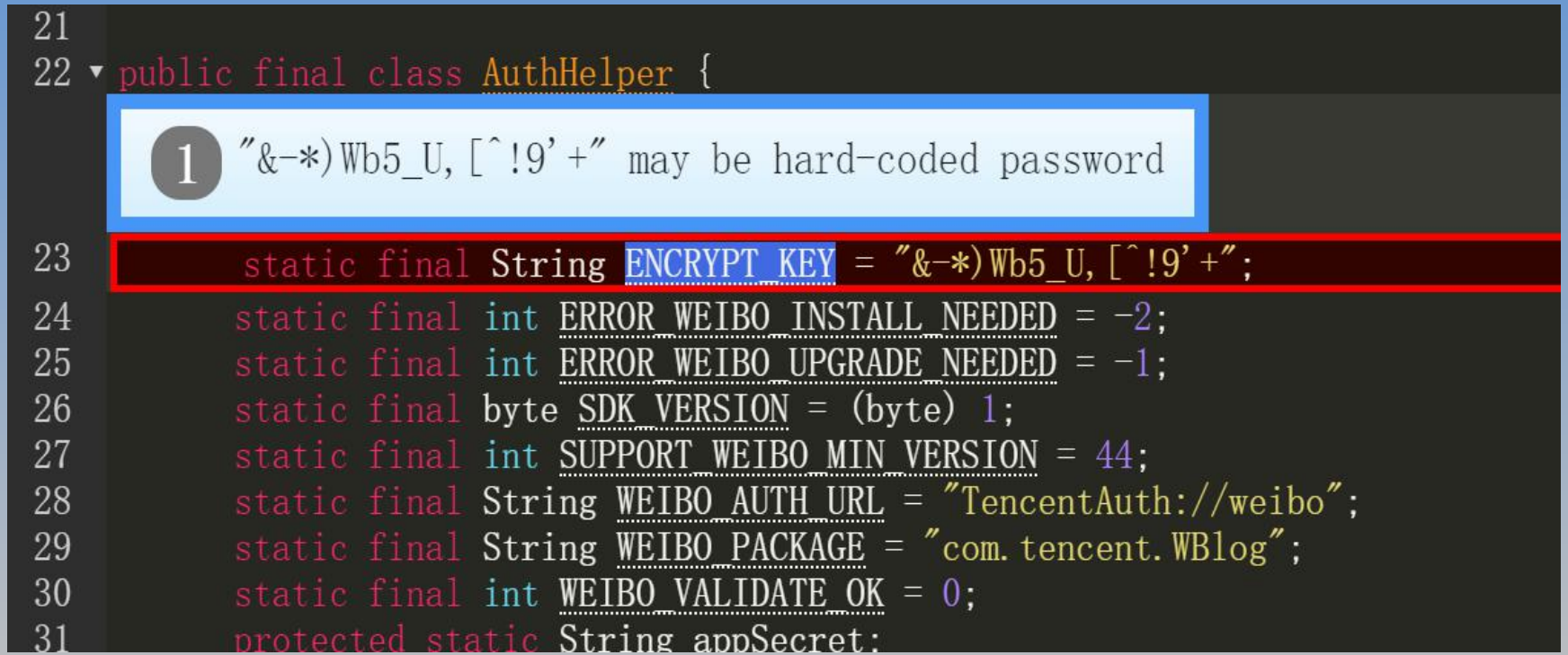
```
17      public static String encode(String plainText, Context context) {
18          try {
19              Key desKey = SecretKeyFactory.getInstance("DES").generateSecret(new
    DESKeySpec(SSLSocketFactoryMaker.hex2byte(context.getString(R.string.des_key))));
20              Cipher cipher = Cipher.getInstance(TRANSFORMATION);
21              cipher.init(1, desKey);
22              return Base64.encodeToString(cipher.doFinal(plainText.getBytes(encoding)), 2);
23          } catch (Exception e) {
24              Log.d("Des", e.toString());
25              return "";
26          }
27      }
28  }
29
```

这里就能从apk中提取des密钥。

```
587    <string name="deleting">正在删除...</string>
588    <string name="department_description">科室介绍</string>
589    <string name="department_doctors">科室名医</string>
590    <string name="department_label">科室: %1$s</string>
591    <string name="deposit_record_title">押金记录</string>
592    <string name="des_key">543141324f33473455354b3645374a38493931</string>
593    <string name="description_add_ask_bottom">非工作时段，无法保证回复时间，请您耐心等待</string>
594    <string name="description_add_ask_top">医生利用休息时间接诊，预计30分钟得到回复</string>
595    <string name="description_item_ask">全员医生可见，响应速度超乎想象</string>
596    <string name="description_item_search_doctor">有熟悉医生，戳这里，直接咨询</string>
```

发现位置：某妇幼保健院APP

com/tencent/weibo/sdk/android/component/sso/AuthHelper.java:23



发现位置：某妇幼保健院APP

com/rubik/waplink/updata/UpdataConstant.java:14

```
14      public static final String c = "ZW5sNWVWOWhibVJ5YjJsaw==";
15      public static final String d = "1";
16      public static final String e = "4";
17      public static final String f = "api.edition";
18      public static final String g = "";
19      public static final String h = "";
20      private static String i = "downApp";
21      private static String j = "downAppStoreDir";
22      private static File k = null;
23
24      public static JSONObject a(Context context) {
25          JSONObject jSONObject;
26          JSONException e;
27          AppWapLinkConfig a = AppWapLinkConfig.a();
28          try {
29              jSONObject = new JSONObject();
30              try {
31                  jSONObject.put("app_id", b);
32                  jSONObject.put("app_key", c);
33                  jSONObject.put(HttpConstants.f, "1");
34                  jSONObject.put(HttpConfig.h, "4");
35                  jSONObject.put("api_name", f);
36                  jSONObject.put("client_mobile", "");
```

发现位置：某癫痫病医院APP

com/hxyt/sddxbyy/application/MyApplication.java:135

```
131
132     public void onCreate() {
133         mInstance = this;
134         this.mLocationClient = new LocationClient(this);
135         this.mLocationClient.setAK("WNpmy1RYFG7KSgGh9Hg8uOdj");
136         this.mLocationClient.registerLocationListener(this.myListener);
137         this.mGeofenceClient = new GeofenceClient(this);
138         super.onCreate();
139         JPushInterface.setDebugMode(true);
140         JPushInterface.init(this);
141         handlerThread = new HandlerThread("Application");
142         handlerThread.start();
143         initContext();
144         initFolder();
145         initImageLoder();
```

- **2、第三方服务行为不可控**
- 人员、工具、程序、流程、协议　审计
- 自己的安全过度依赖第三方

- **3、安全设备策略配置不到位**

- 防火墙、入侵检测、数据库审计、WAF
- 检查更新不及时

- **4、访问权限设定不科学**
- 内部人员、服务人员、检查人员、产品厂厂商
- 没有遵循最小原则、超级管理员人数太多

- **5、应急处置准备不足**

- 方案不适用，应急演练走过场，没有支援组织，缺少专家指导、缺少事件沟通上报机制


医院网络安全工作建议

当务之急

- 1、组织第三方代码安全检测、漏洞检测（验收、评估）
- 2、加强第三方服务管理（准入、考核、审计）
- 3、加强科技人员岗位能力培训（专职网络安全管理员培训）
- 4、加强专家队伍建设（落实百人专家计划）

- **联系方式：**
- 张朝伦　18753145711
- 微信：sdic00