HackCon

The Norwegian cyber security conference

Oslo, Feb' 2016

The Age of Mobile Application Insecurities

Aditya Modha

Lucideus Tech Pvt. Ltd.

Who am I

Security Analyst

Infosec Trainer

I blog at oldmanlab.blogspot.com

I tweet at @oldmanlab

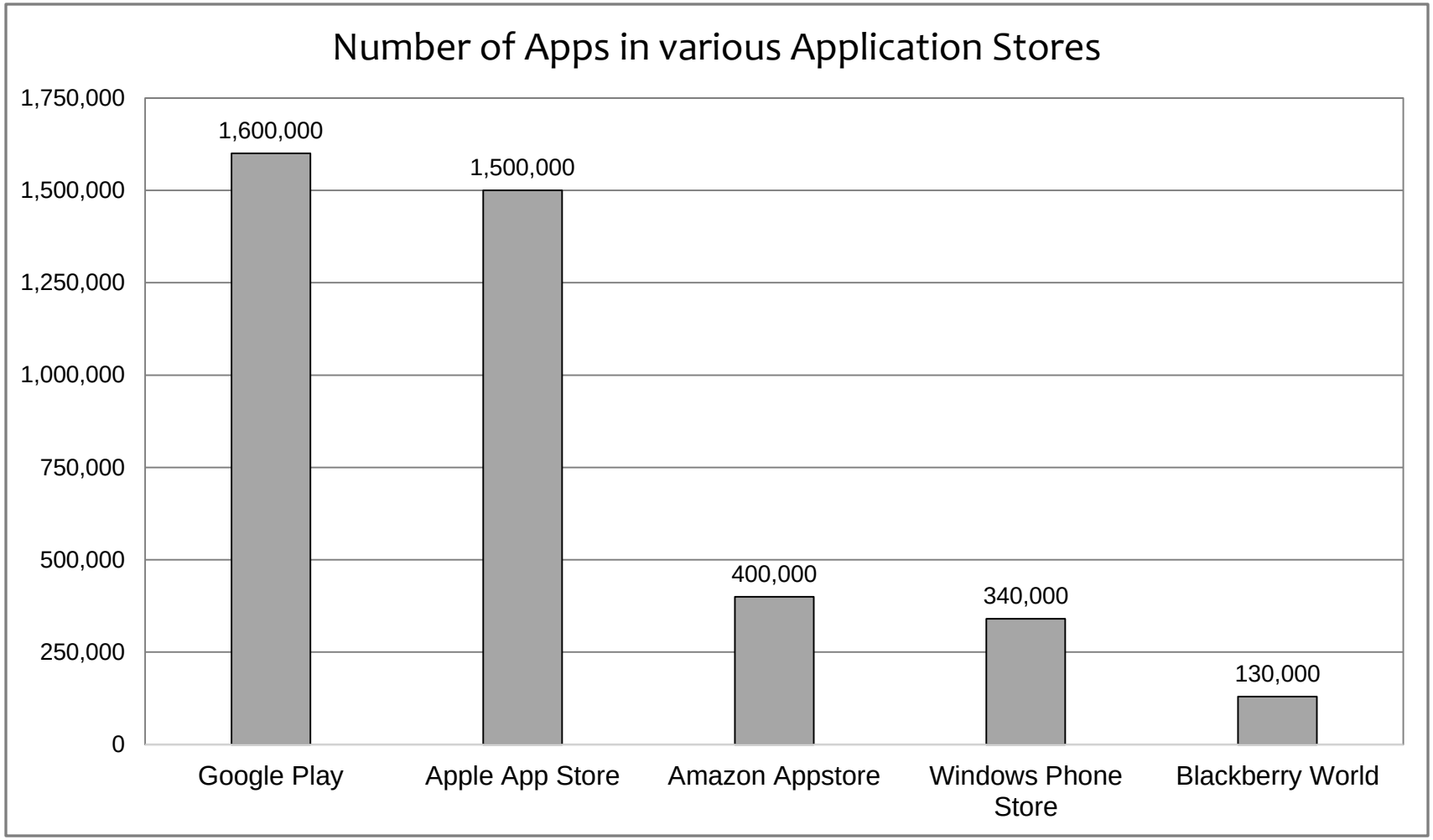
What is this talk all about

Vulnerabilities in Mobile Applications

Failed or Inadequate Patches

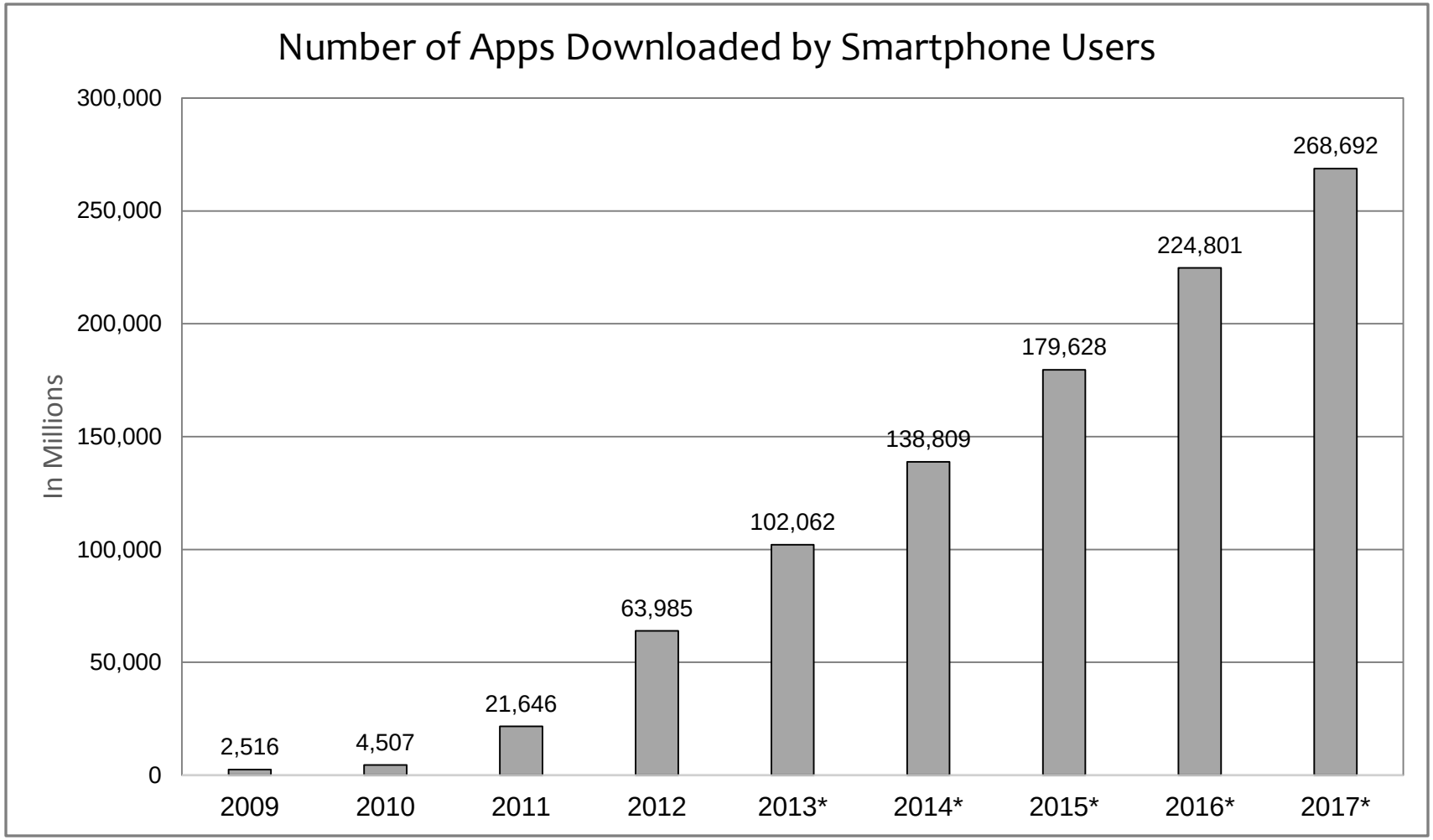
Some Numbers

Why this talk



source: www.statista.com

Why this talk

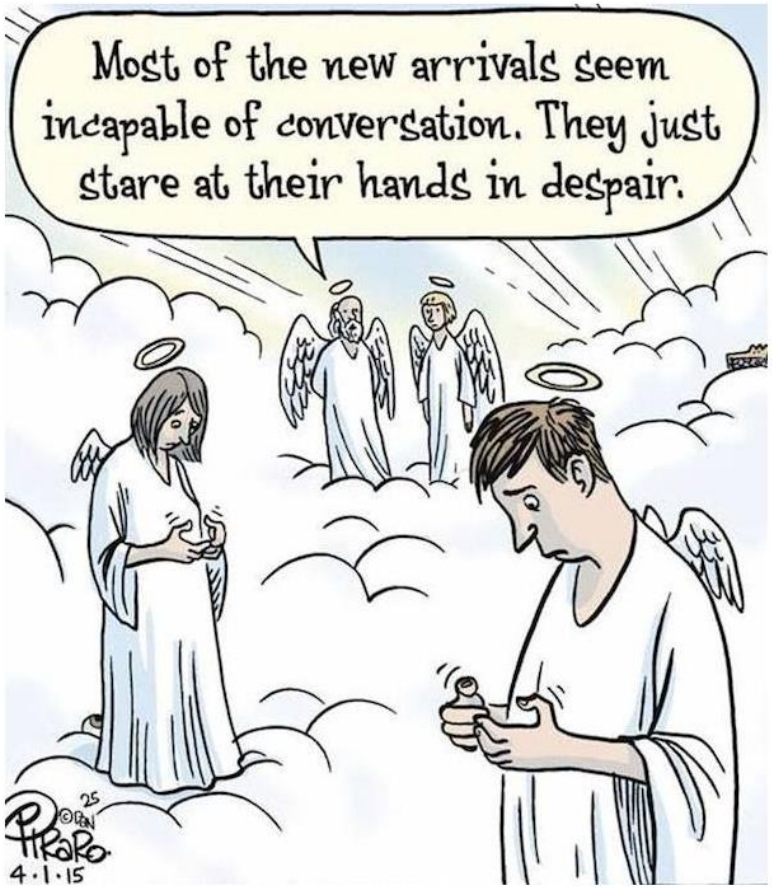


source: www.statista.com

Lucideus Tech Pvt. Ltd.

Why this talk

- The number of Android vulnerabilities has increased 188% compared to 2011.
- The number of iOS vulnerabilities has increased 262% compared to 2011.
- 31% of the Google Play apps that have more than 50,000 downloads contain remote exploitable vulnerabilities.
- Gartner says more than 75% of Mobile Applications will fail basic security tests through 2015.



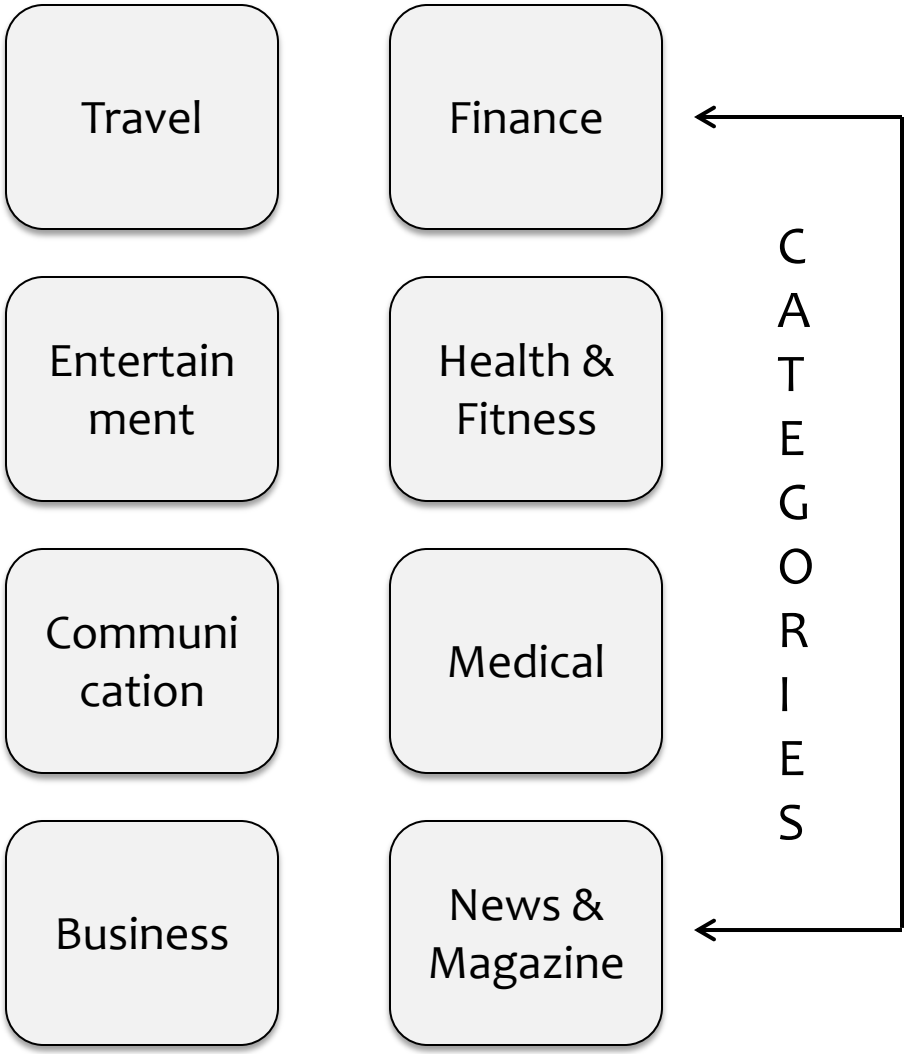
https://www.fireeye.com/blog/executive-perspective/2015/02/state_of_mobile_secu.html

Common Vulnerabilities

OWASP TOP 10 Mobile Risks

- M1 – Weak Server Side Controls ✗
- M2 – Insecure Data Storage ✓
- M3 – Insufficient Transport Layer Protection ✓
- M4 – Unintended Data Leakage ✓
- M5 – Poor Authorization and Authentication ✓
- M6 – Broken Cryptography ✓
- M7 – Client Side Injection ✗
- M8 – Security Decisions Via Untrusted Input ✓
- M9 – Improper Session Handling ✗
- M10 – Lack of Binary Protections ✓

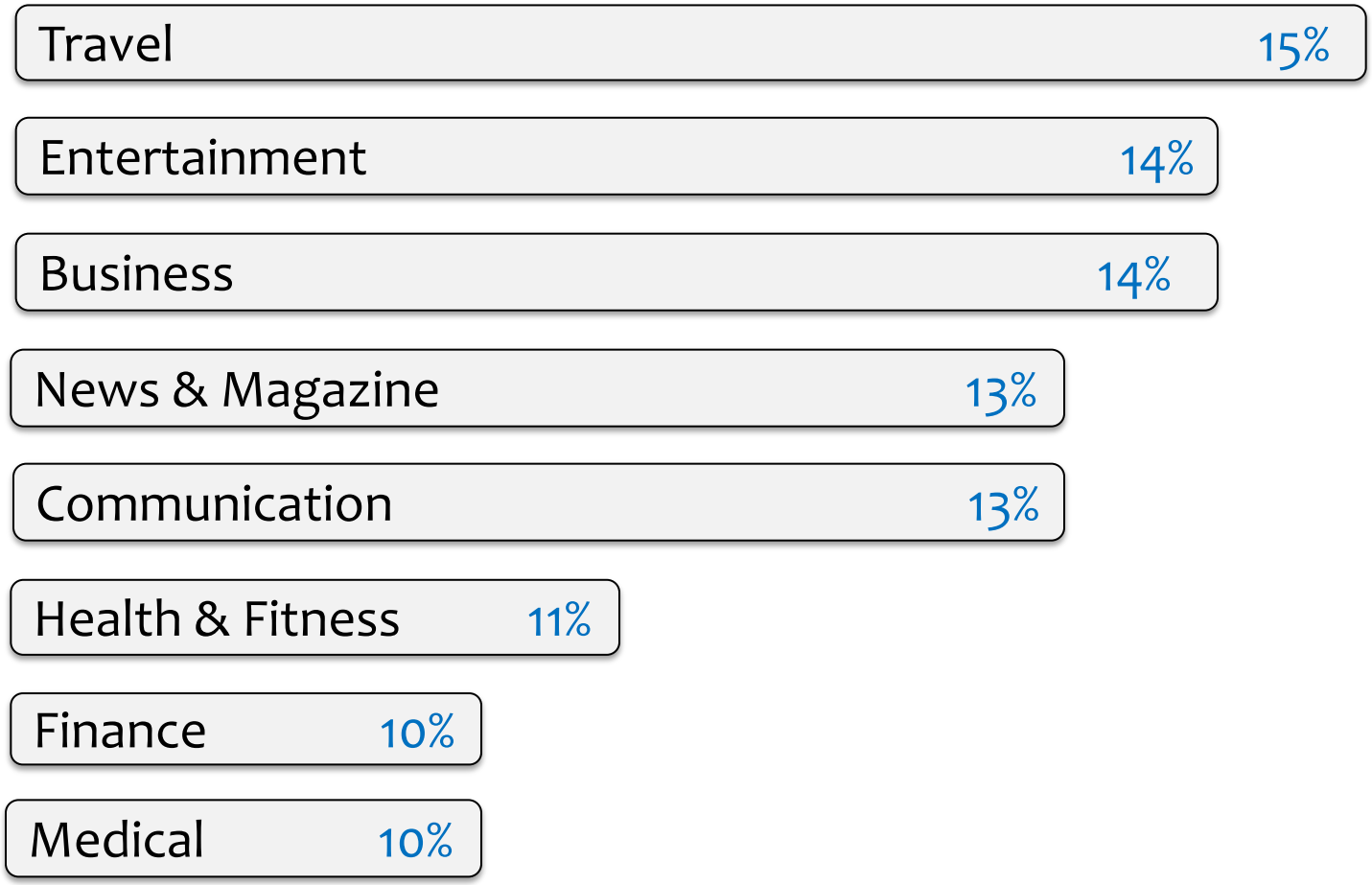
Total Reviewed Applications



- 25 Apps in each category
- Apps of the Android and iOS platform
- Total 8 categories

25 x 8 x 2 = 400 Apps

Apps Category v/s Vulnerability %



Lucideus Tech Pvt. Ltd.

Top Vulnerabilities

Un-Obfuscated Code	55%
Insecure (Weak) Algorithm	46%
Local PII Storage	24%
Credentials over HTTP	17%
Insecure SSL Verification	4%
Local Password Storage	4%
Local Authentication	2%
Hardcode Encryption Key	2%

% of total apps

Exhibits

Cleartext credential transmission

Burp Suite Free Edition v1.6

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options | Alerts

Intercept | HTTP history | WebSockets history | Options

Request to http://[redacted]:80[redacted]

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
GET
/[redacted].html?&username=aditya.m@lucideustech.com&password=supersecretpasswors&ca
[redacted] HTTP/1.1
Host: [redacted]
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
Cookie: JSESSIONID=8838112CA61F4BF0E989957FFA6C15F5[redacted]
Connection: keep-alive
Accept-Language: en;q=1, ar;q=0.9, fr;q=0.8, de;q=0.7, ja;q=0.6, nl;q=0.5
User-Agent: [redacted] (iPhone; iOS 7.1.2; Scale/2.00)
```

? < + > 0 matches

Un-obfuscated Code

```
public void verifyOTP(String paramString)
{
  try
  {
    this.alertDialog = ErrorsScreen.showCustomProgressDialog(this.mActivity, "Verifying OTP...");
    Type localType = new TypeToken()
    {
    }
    .getType();
    VolleyNetworkRequest localVolleyNetworkRequest = new VolleyNetworkRequest(this.mActivity, this,
    HashMap localHashMap = new HashMap();
    localHashMap.put([redacted]SharedPreferences.getCandidateId(this.mActivity));
    localHashMap.put("auth_code", paramString);
    localVolleyNetworkRequest.setUsePostMethod(localHashMap);
    localVolleyNetworkRequest.execute("verifyOTP");
    return;
  }
  catch (Exception localException)
  {
    localException.printStackTrace();
  }
}
```

OTP code in HTTP response

POST request to http:/[redacted]

Previous | Next | Action

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Thu, 18 Feb 2016 00:49:34 GMT
Server: Apache
X-Powered-By: PHP/5.5.9
Vary: Accept-Encoding
Content-Length: 209
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

{"RESPONSE":{"STATUS":"SUCCESS","GLUSRID":"","OTP":"717197",[redacted],"MES
SAGE":"OTP SENT","autoLogin":0},"CODE":"200","ERROR":"","Execution":"0.1275
seconds","unique_id":"56c5151e814fa"}
```

Defeats 2-Factor Authentication

? | < | + | > | 0 matches

cert — -bash — 67×16


```
12|0|????
13|0|????
14|0|{"RESPONSE":{"STATUS":"SUCCESS","GLUSRID":"","OTP":"717197","M
I[redacted]","MESSAGE":"OTP SENT","autoLogin":0},"
CODE":"200","ERROR":"","Execution":"0.1275 seconds","unique_id":"56
c5151e814fa"}
15|0|{"RESPONSE":{"STATUS":"SUCCESS","GLUSRID":"","MESSAGE":"USER N
OT VERIFIED"},"CODE":"200","ERROR":"","unique_id":"56c51564ddd24"}
16|0|{"RESPONSE":{"LoginCookie":{"admsales":"0","":null,"au":"98b48
c8e226720b62e45e8af0795a23b","admln":"0","name":"Aditya","id":"2690
7482","mail":"aditya.m@lucideustech.com","[redacted]986","utyp":"
F"},"DataCookie":{"ph1":"","int":"na","cn":"[redacted]es","
imurl":"","ct":"","ln":"","ad":"","phcc":"971","iso":"AE","admln":"
0","url":"","co":"","fn":"Aditya","ph2":"","cd":"18\/FEB\/2016","ph
ac":"","[redacted]986","mb2":"","glid":"26907482","st":"","utyp":
"F","zp":"","em":"aditya.m@lucideustech.com","ctid":"","nm":"Aditya
```

Local password store in plaintext

Downloads — adb shell — 89×12

```
oldmanlab:Downloads oldmanlab$ adb shell
root@android:/ # cd /data/data/com.[redacted]t/shared_prefs
root@android:/data/data/com.[redacted]t/shared_prefs # ls -la
-rw-rw---- u0_a52   u0_a52      749 2016-02-18 00:29 MapViewInitializerPreferences.xml
-rw-rw---- u0_a52   u0_a52     2341 2016-02-18 00:29 MyPref.xml
-rwxrwxrwx u0_a52   u0_a52      221 2016-02-18 00:24 com.[redacted].xml
m.[redacted].xml
<string name="username">aditya.m@lucideustech.com</string>
<string name="password">mysupersecret</string>
<boolean name="isAccountVerified" value="true">
<string name="Token">7e0fed77-0223-5e60-9201-c8673898606a</string>
root@android:/data/data/com.[redacted]t/shared_prefs #
```

```
"original-purchase-date-pst" = "2012-07-12 05:54:35 America/Los_Angeles";
"purchase-date-ms" = "1342097675882";
"original-transaction-id" = "170000029449420";
"bvrs" = "1.4";
"app-item-id" = "450542233";
"transaction-id" = "170000029449420";
"quantity" = "1";
"original-purchase-date-ms" = "1342097675882";
"item-id" = "534185042";
"version-external-identifier" = "9051236";
"product-id" = "com.zeptolab.ctrbonus.superpower1";
"purchase-date" = "2012-07-12 12:54:35 Etc/GMT";
"original-purchase-date" = "2012-07-12 12:54:35 Etc/GMT";
"bid" = "com.zeptolab.ctrexperiments";
"purchase-date-pst" = "2012-07-12 05:54:35 America/Los_Angeles";
```

cert — -bash — 67×7


```
DER":"Start [redacted]"},"lastVersionTime":"Wed Feb 17 2016 16
:03:28 GMT-0800 (PST)","iso":"AE","country":"[redacted]",
"mobi[redacted]986","email":"aditya.m@lucideustech.com","name":"Ad
itya ","gluserid":"26907482","islogin":"yes","mcatData":{"updated":
false,"mcatId":[]},"UserLocPref":"CITY"}
sqlite> packet_write_wait: Connection to 10.10.2.161: Broken pipe
oldmanlab:cert oldmanlab$
```

Insecure SSL verification

Untitled - Notepad

File Edit Format View Help

```
public MySSLSocketFactory(KeyStore truststore) throws NoSuchAlgorithmException, KeyManagementException,
KeyStoreException, UnrecoverableKeyException
{
        super(truststore);

        TrustManager tm = new X509TrustManager()
  {

        public X509Certificate[] getAcceptedIssuers()
        {
                return null;
        }
  };

        sslContext.init(null, new TrustManager[] { tm }, null);
}


KeyStore trustStore = KeyStore.getInstance(KeyStore.getDefaultType());
trustStore.load(null, null);

MySSLSocketFactory sf = new MySSLSocketFactory(trustStore);
sf.setHostnameVerifier(SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
```

Demo

Common Best Practices Followed

18%

SSL Pinning

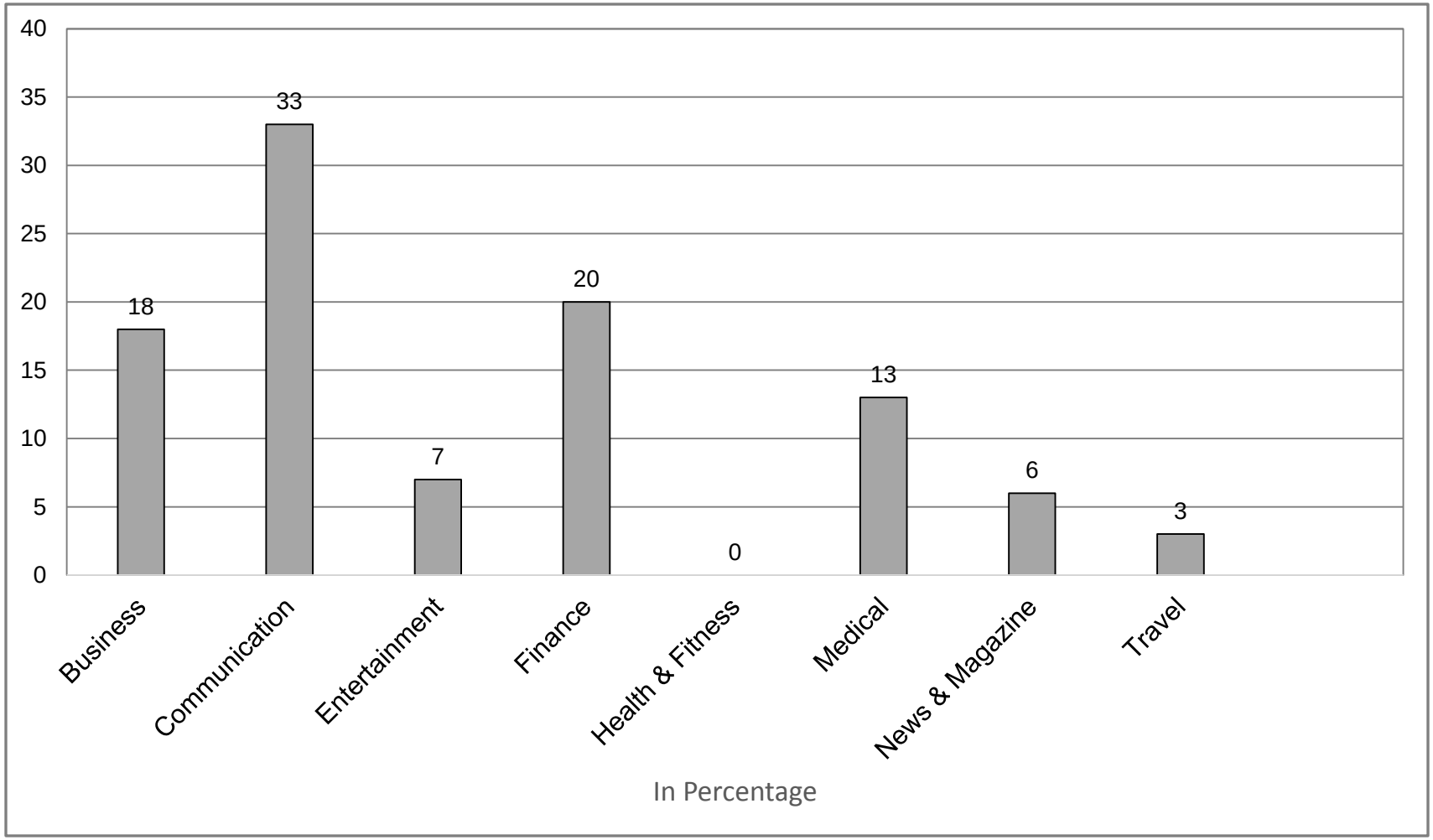
15%

Encrypted Parameters

2%

Binary Protection

Security Best Practitioner



Inadequate or Failed Patches

```
GET
/[redacted]?CustomerId=9210133
HTTP/1.1
authenticationToken: ef6639[redacted]f5e97
Authorization: 71681fe9-9d09-4e01-9e2c-7591821e0bd8
zD3IzZiJzPbmG[redacted]r
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; HTC Desire
526GPLUS dual sim Build/KOT49H)
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
```

Developers prevent access control issues by encrypting the value of key identifier parameter

```
GET
[redacted]customerid=vSW1Q75rdDJN%2BBik
QNvc9g%3D%3D HTTP/1.1
Authorization: 00191690-b0e4-4ff6-aedb-1a32b96080ab
MvAR1tIFP5HvdDjTJ%[redacted]
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2;
google_sdk Build/JB_MR1.1)
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
```

Inadequate or Failed Patches

And then they store the encryption key, hardcoded, in the application code

```
try
{
  c = new SecretKeySpec(paramArrayOfByte1, "AES");
  e = new IvParameterSpec(paramArrayOfByte2);
  d = Cipher.getInstance("AES/CBC/PKCS5Padding");
  return;
}
catch (NoSuchAlgorithmException localNoSuchAlgorithmException)
{
  throw new CipherException();
}
catch (NoSuchPaddingException localNoSuchPaddingException)
{
  label34: break label34;
}
```

```
import java.io.UnsupportedEncodingException;

public class a
{
  private static String a = b.a("PSVJQRk9QTEpNVU1DWUZCRVFGV1VVT0ZOV1RRU1NaWQ=");
  private static String b = b.a("WVdsRkxWRVpaVUZOYVdsaA==");
  private static SecretKeySpec c;
  private static Cipher d;
  private static IvParameterSpec e;

  public static String a(String paramString)
  {
    try
    {
      a(a.getBytes("UTF-8"), b.getBytes("UTF-8"));
      String str = b.a(a(1).doFinal(paramString.getBytes("UTF-8")));
```

Questions?

Thank You