Android e mobile security (for developers)

Igor Falcomatà

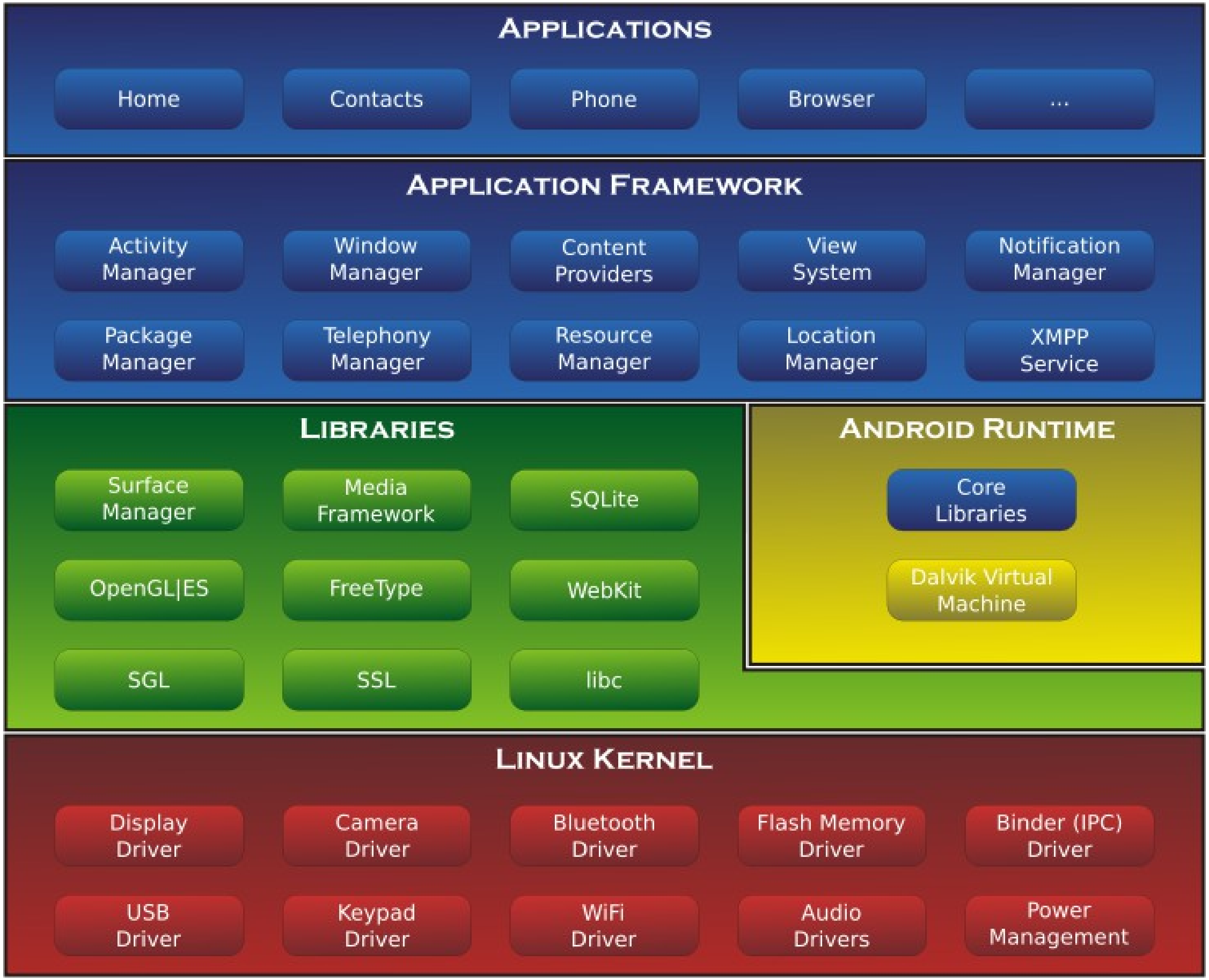
CTO, Enforcer
ifalcomata@enforcer.it

OWASP-Italy Day2012
Rome, 23° November 2012

The OWASP Foundation
http://www.owasp.org

- **attività professionale:**
  - **analisi delle vulnerabilità e penetration testing (~13 anni)**
  - **security consulting**
  - **formazione**
- **altro:**
  - **sikurezza.org**
  - **(F|Er|bz)lug**

free advertising >



Applications

Home | Contacts | Phone | Browser | ...

Application Framework

Activity Manager | Window Manager | Content Providers | View System | Notification Manager

Package Manager | Telephony Manager | Resource Manager | Location Manager | XMPP Service

Libraries

Surface Manager | Media Framework | SQLite

OpenGL|ES | FreeType | WebKit

SGL | SSL | libc

Android Runtime

Core Libraries

Dalvik Virtual Machine

Linux Kernel

Display Driver | Camera Driver | Bluetooth Driver | Flash Memory Driver | Binder (IPC) Driver

USB Driver | Keypad Driver | WiFi Driver | Audio Drivers | Power Management

http://en.wikipedia.org/w/index.php?title=File:Android-System-Architecture.svg

- Architetture: ARM, (MIPS, x86, ..)
- Kernel
  - Kernel Linux 2.6.x (Android 1, 2 e 3.x)
  - Kernel Linux 3.0.x (Android 4.x)
  - componenti e driver standard
  - FS, processi, permessi, processi
  - vulnerabilità standard ;)
- Componenti custom
  - binder, ashmem, pmem, logger, wavelocks, OOM, alarm timers, paranoid network security, gpio, ..
  - android e vendor custom hw driver
  - nuove vulnerabilità da scoprire ;)

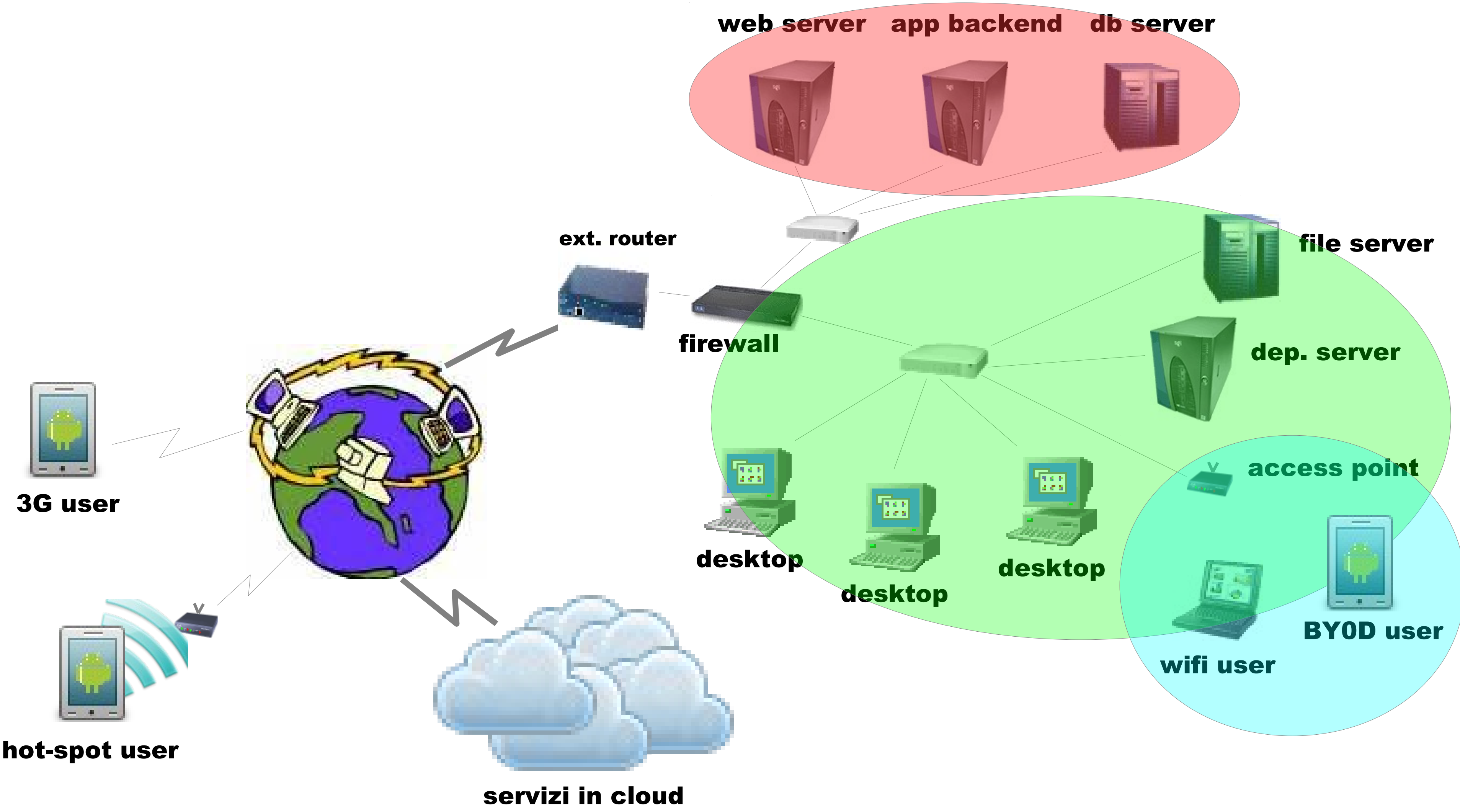
- Sandbox (OS level)
  - sandboxing con uid/gid linux + patch kernel (protected API)
  - 1 processo = 1 applicazione = 1 VM (+ componenti OS)
  - protected API per accesso all'hw: camera, gps, bluetooth, telefonia, SMS/MMS, connessioni di rete)
  - root = root (full access)

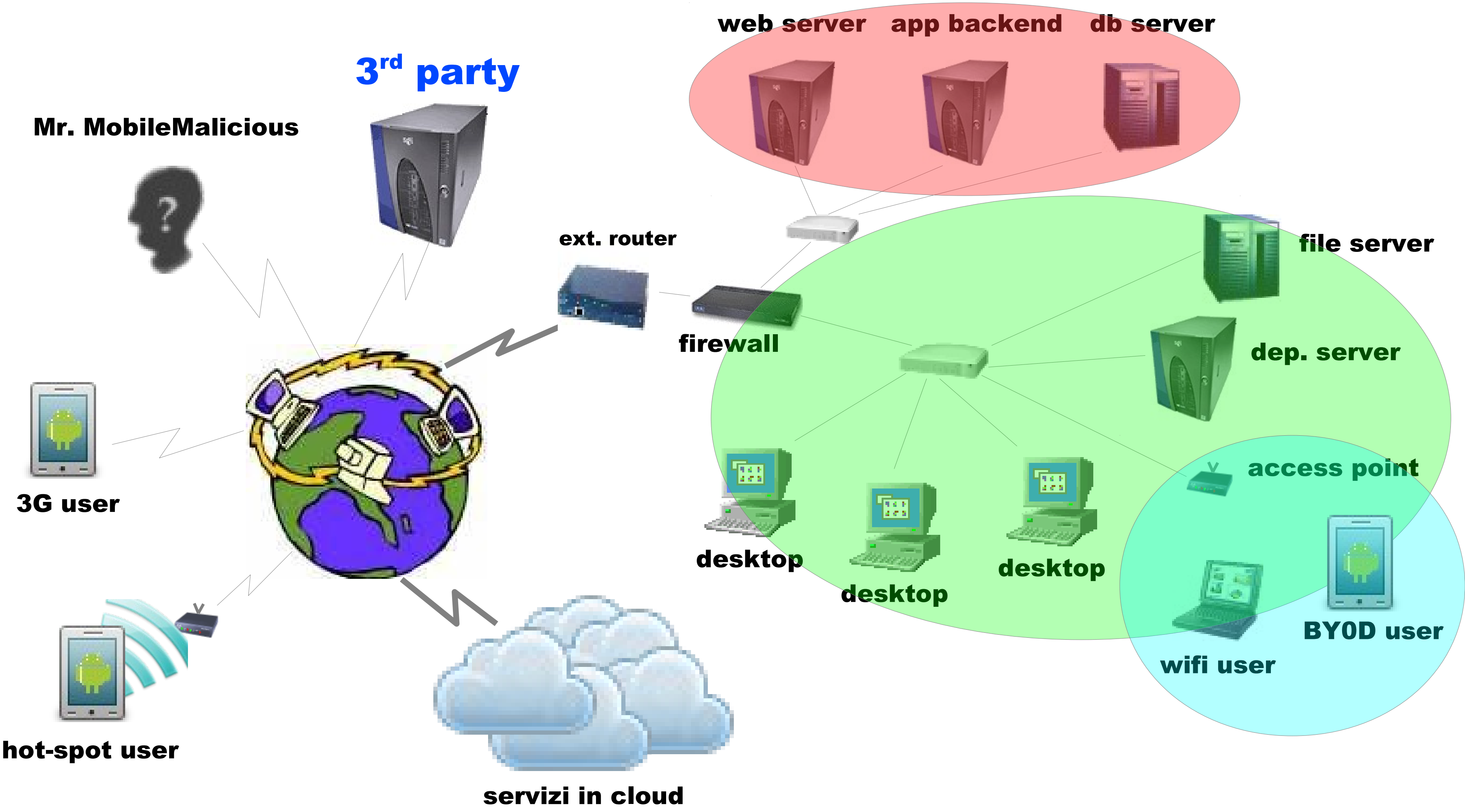
- Librerie
  - bionic libc (!= gnu libc, !posix)
  - udev, WebKit, OpenGL, SQLite, crypto, .. (& bugs)

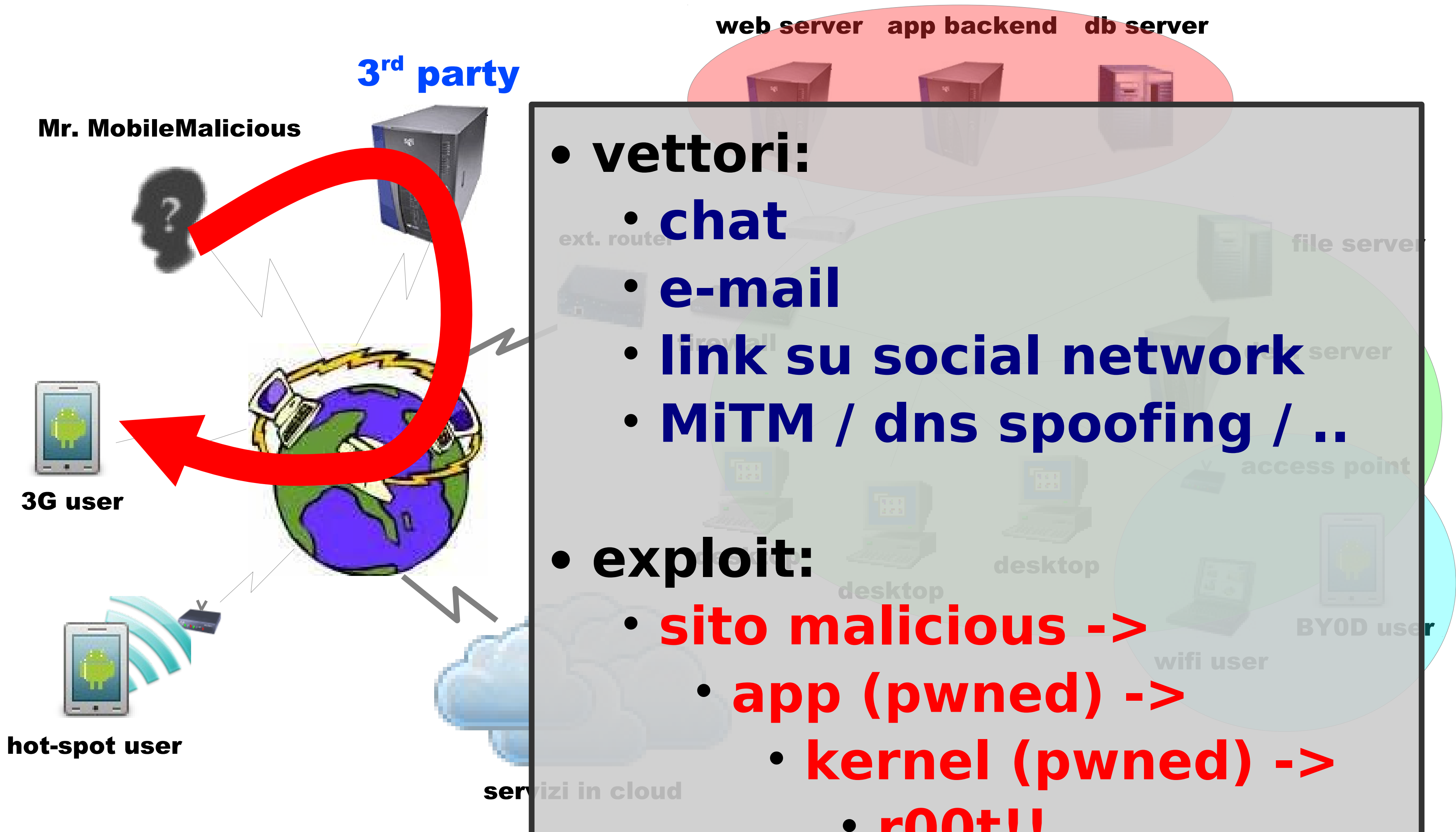
- Dalvik VM (!= JVM)
  - Java Code -> dex bytecode
  - custom Java libraries
  - può lanciare codice nativo (syscall, ioctls, ..) -> kernel

- Sandbox (OS level)
  - sandboxing con uid/gid linux + patch kernel (protected API)
  - 1 processo = 1 applicazione = 1 VM (+ componenti OS)
  - protected API per accedere all'hw (camera, gps, bluetooth, telefonia, SMS/MMS, connessioni di rete)
  - root [illegible]
- Librerie
  - bionic [illegible]
  - udev, WebKit, OpenGL, SQLite, crypto, ... ([illegible])
- Dalvik VM (!= JVM)
  - Java Code -> dex bytecode
  - cust[illegible]
  - può [illegible] codice nativo (syscall, ioctls, ...) [illegible]

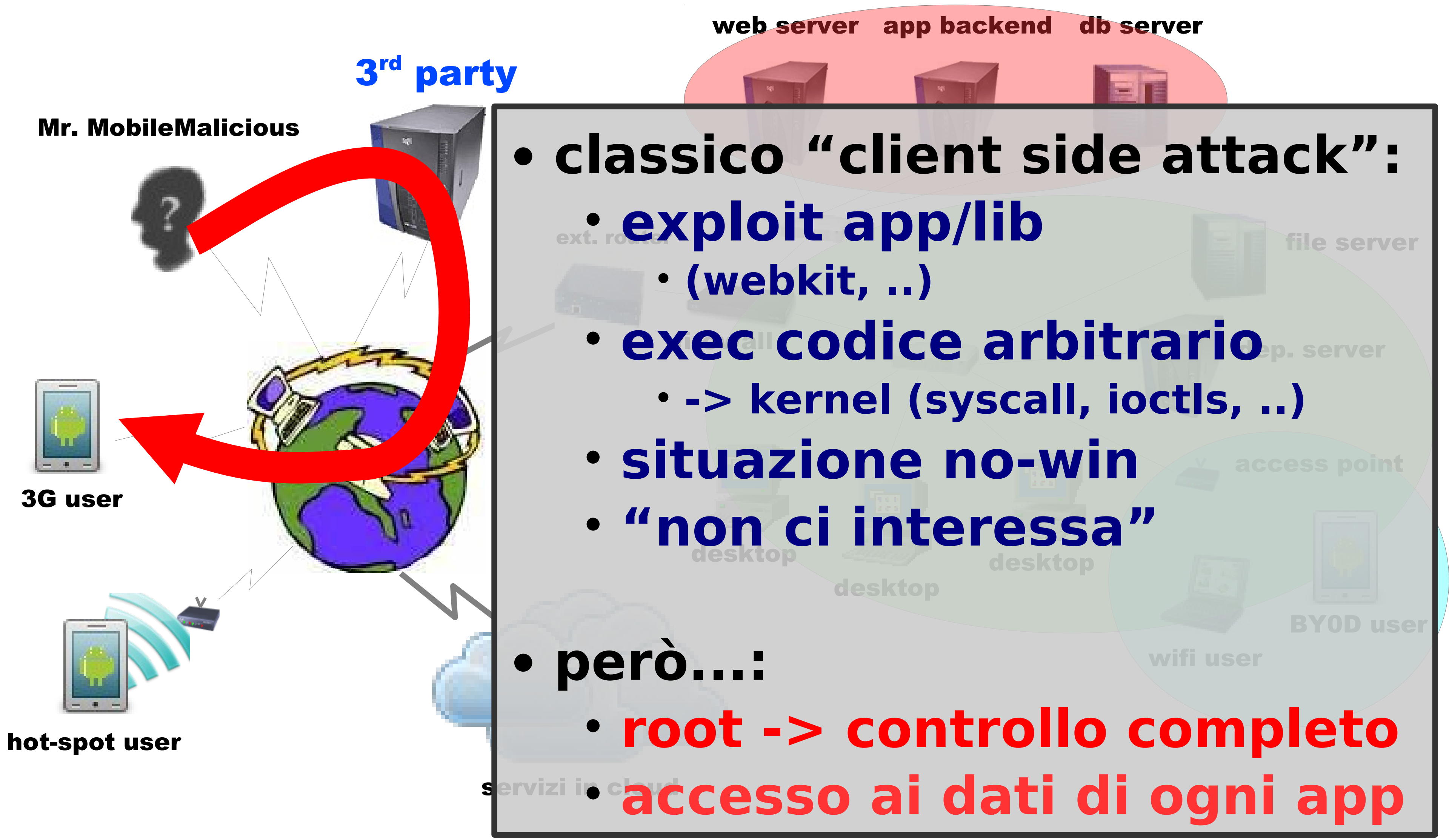
> **“Like all security features, the Application Sandbox is not unbreakable. However, to break out of the Application Sandbox in a properly configured device, one must compromise the security of the the Linux kernel.”**


web server
app backend
db server
ext. router
file server
firewall
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud

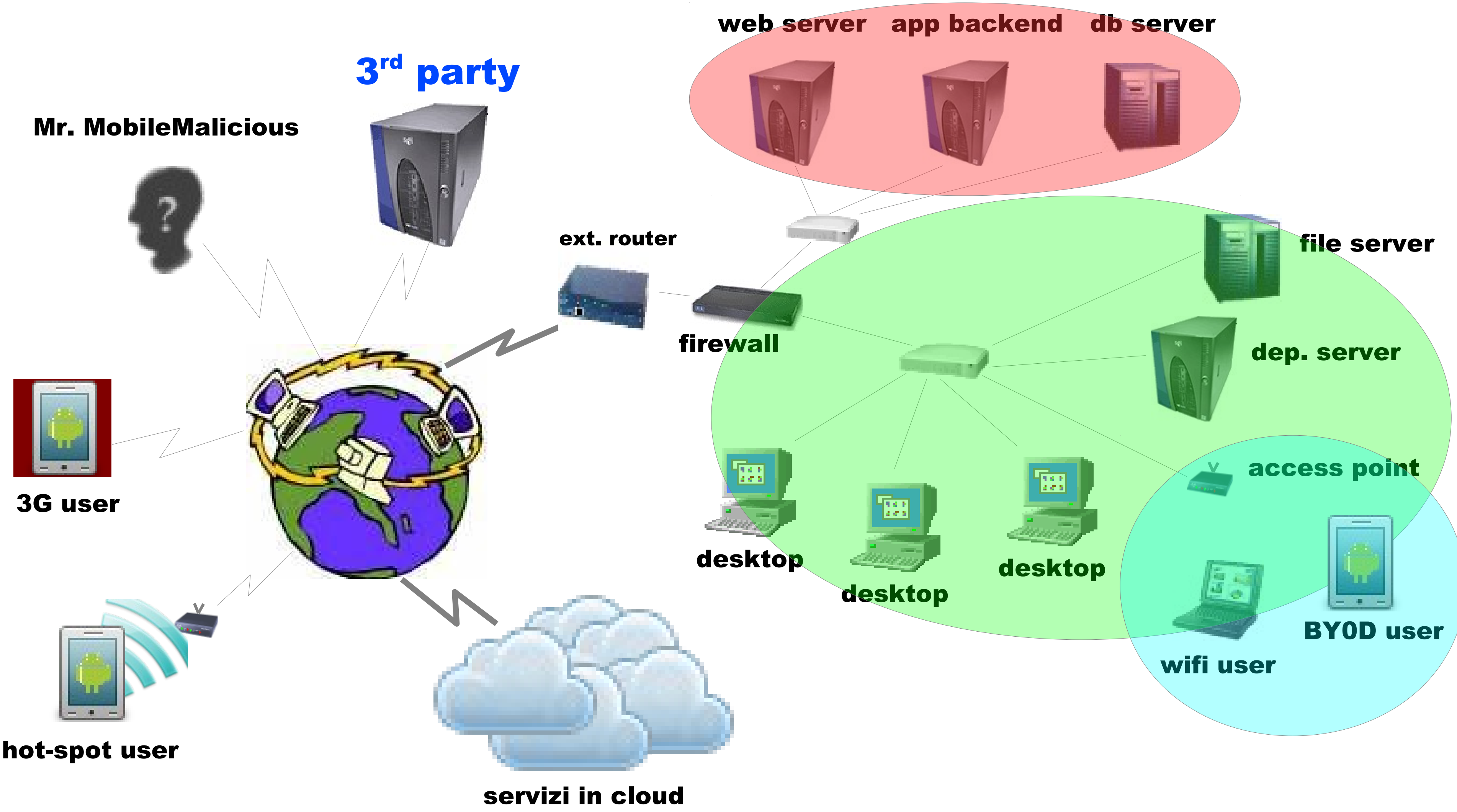

web server
app backend
db server
3rd party
Mr. MobileMalicious
ext. router
file server
firewall
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
hot-spot user
wifi user
servizi in cloud

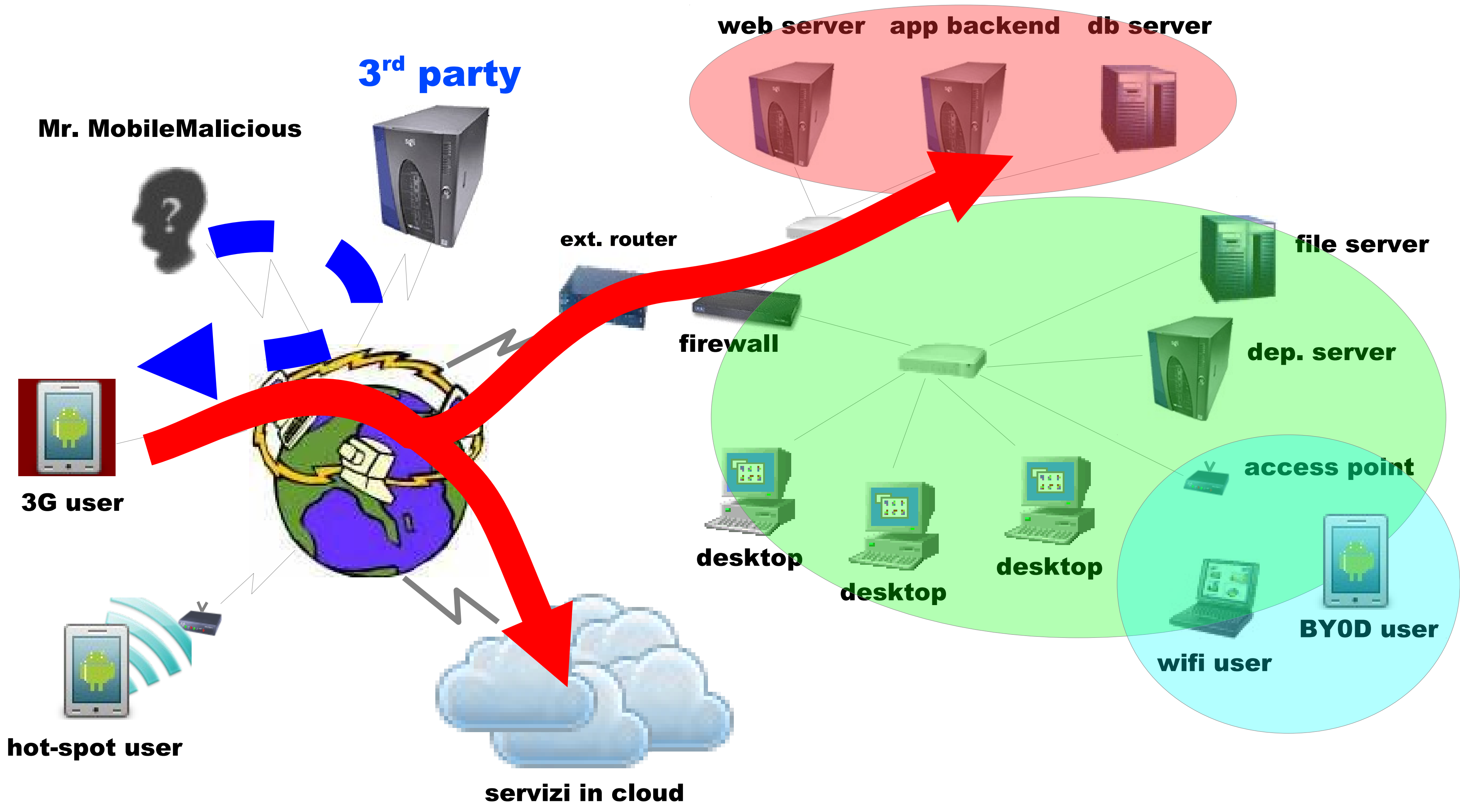


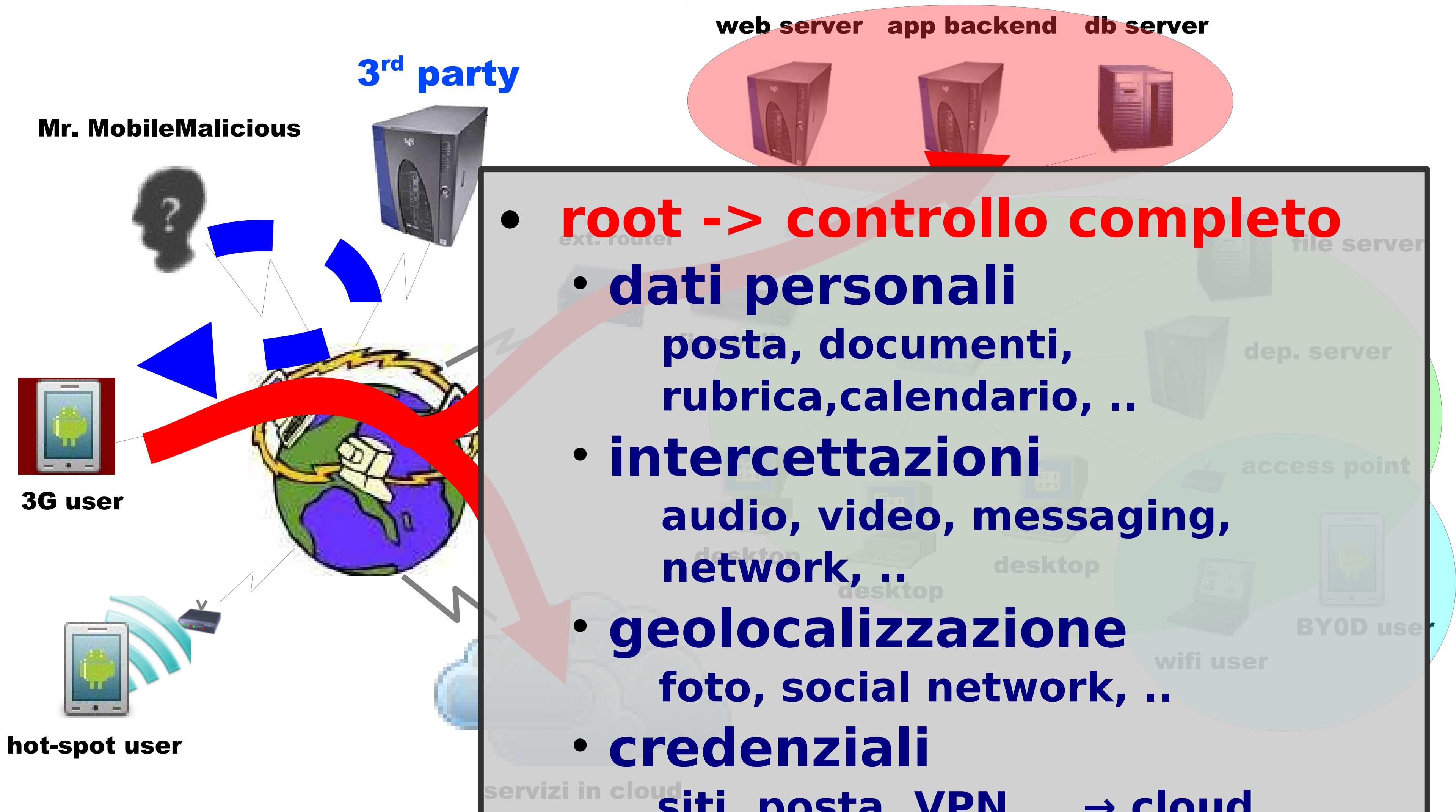
- vettori:
  - chat
  - e-mail
  - link su social network
  - MiTM / dns spoofing / ..
- exploit:
  - sito malicious ->
    - app (pwned) ->
      - kernel (pwned) ->
        - r00t!!



- classico “client side attack”:
  - exploit app/lib
    - (webkit, ..)
  - exec codice arbitrario
    - -> kernel (syscall, ioctls, ..)
  - situazione no-win
  - “non ci interessa”
- però...:
  - root -> controllo completo
  - accesso ai dati di ogni app


web server
app backend
db server
3rd party
Mr. MobileMalicious
ext. router
file server
firewall
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud


web server
app backend
db server
3rd party
Mr. MobileMalicious
ext. router
file server
firewall
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud



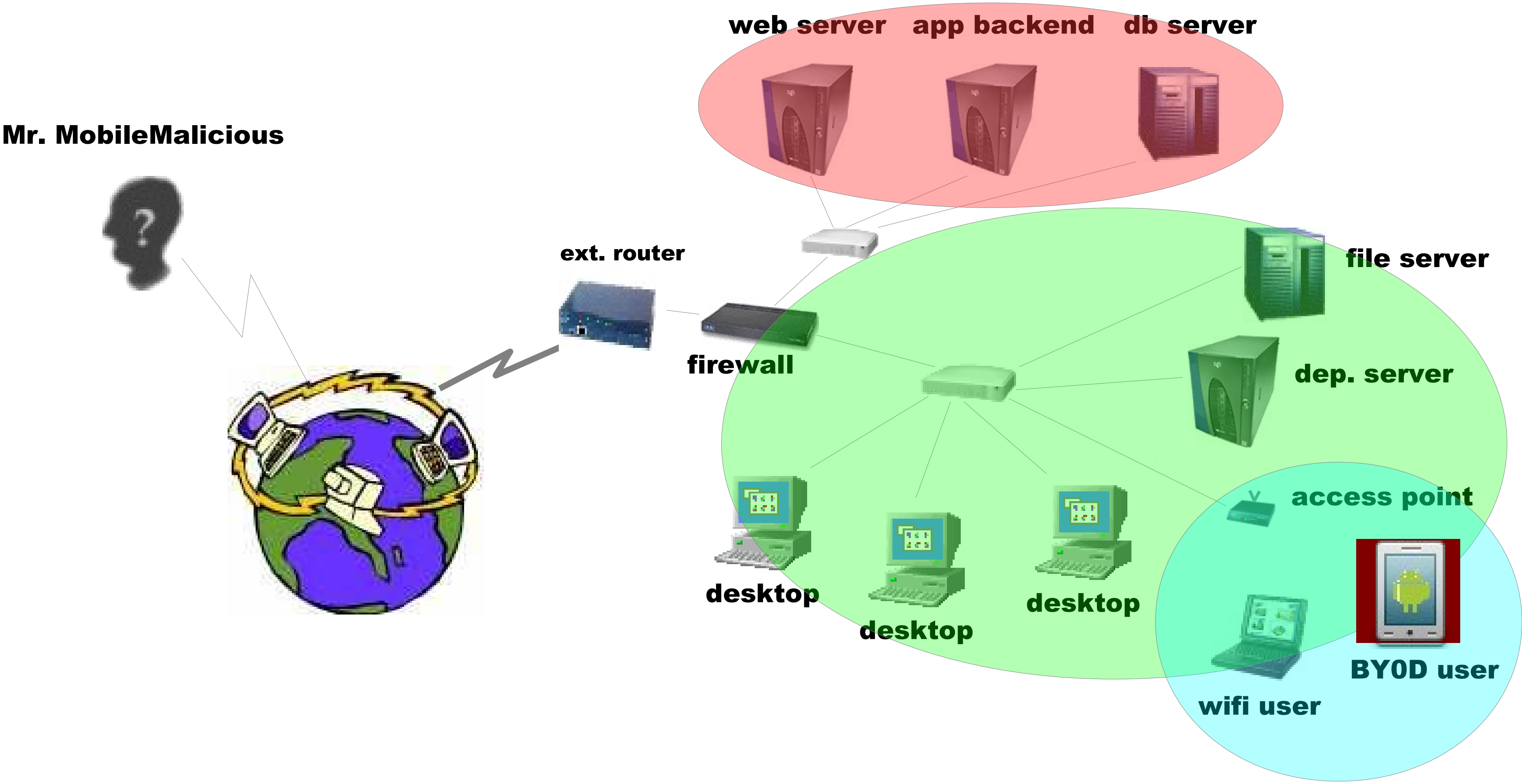
- root -> controllo completo
  - dati personali

    posta, documenti, rubrica,calendario, ..
  - intercettazioni

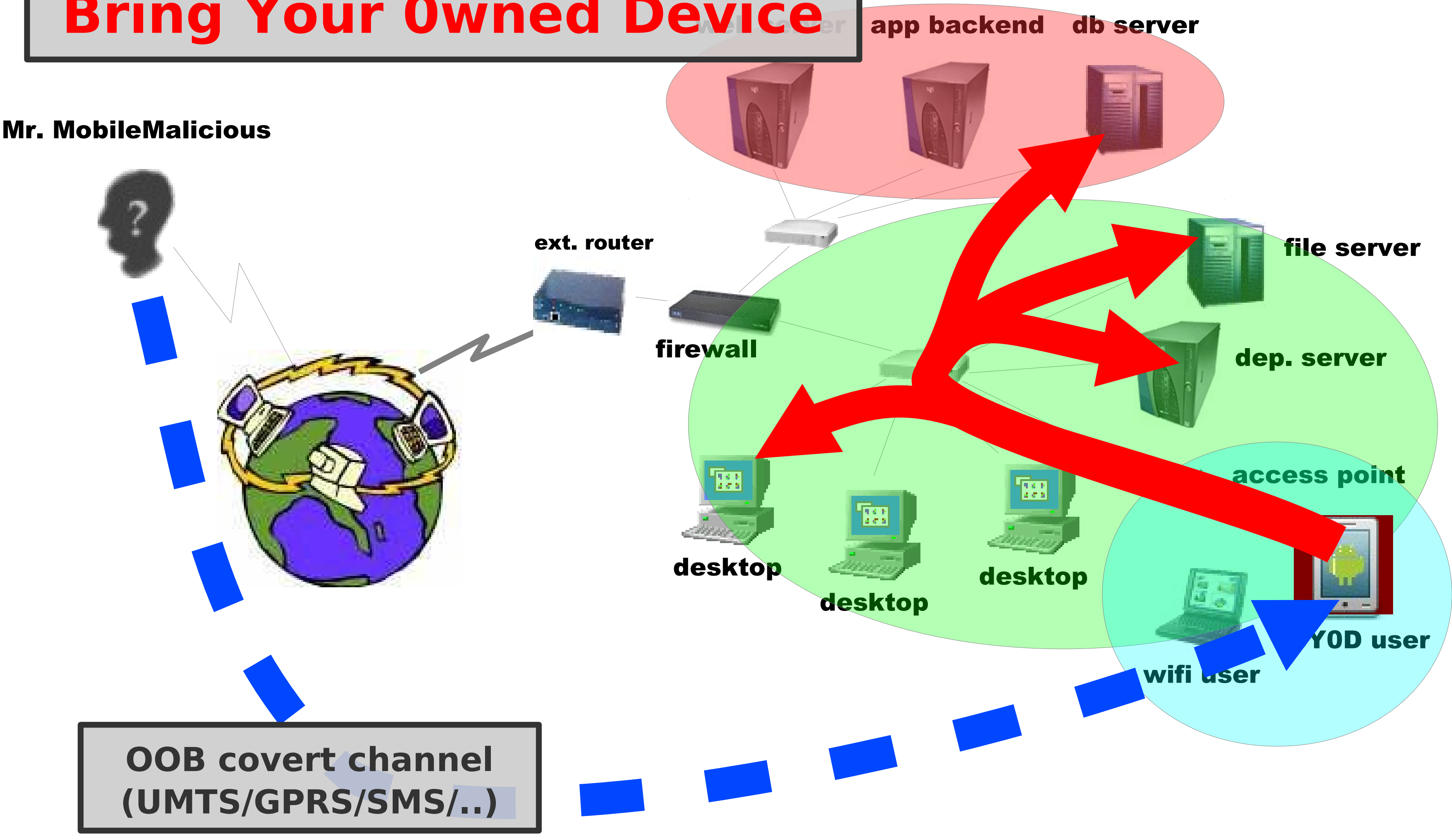
    audio, video, messaging, network, ..
  - geolocalizzazione

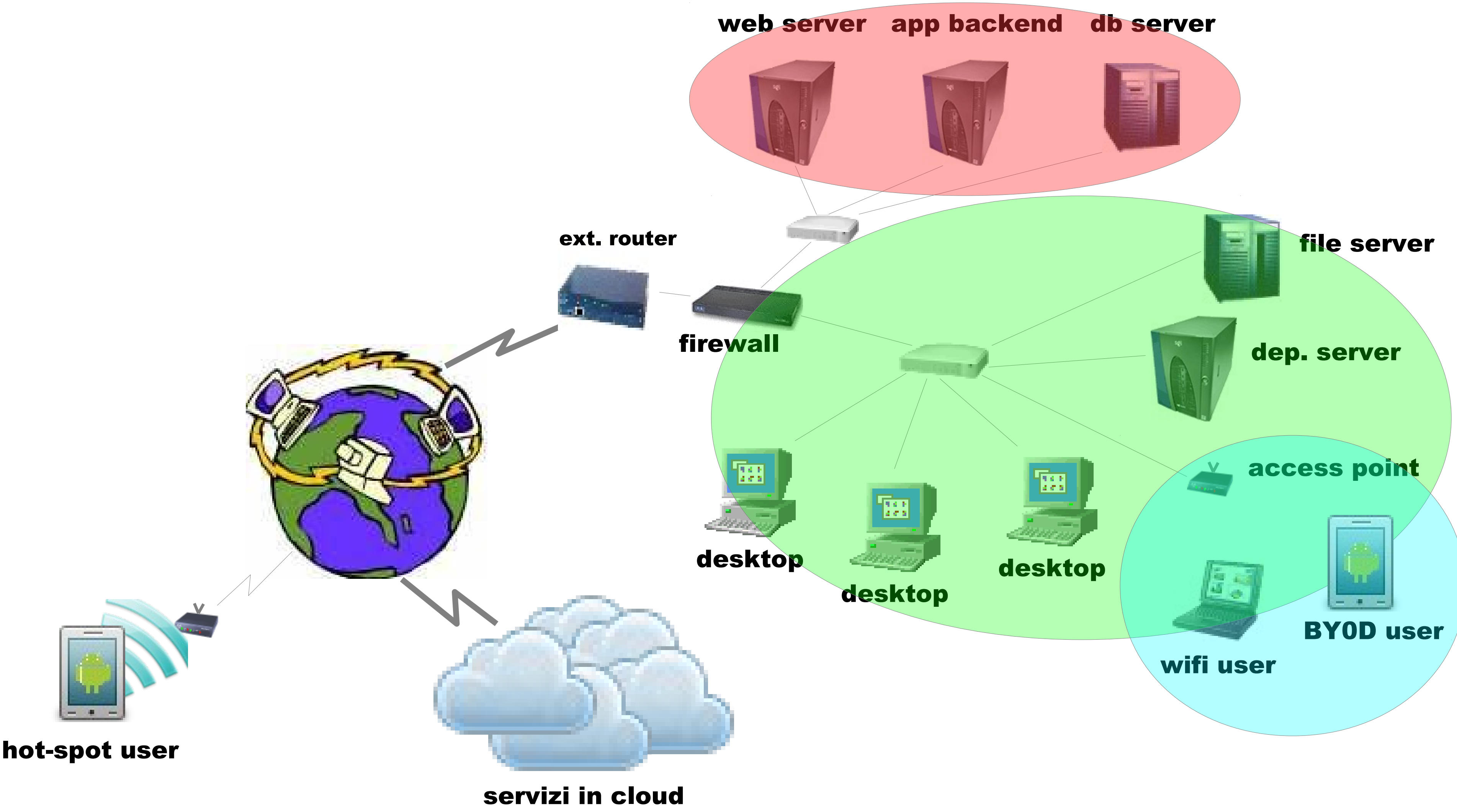
    foto, social network, ..
  - credenziali

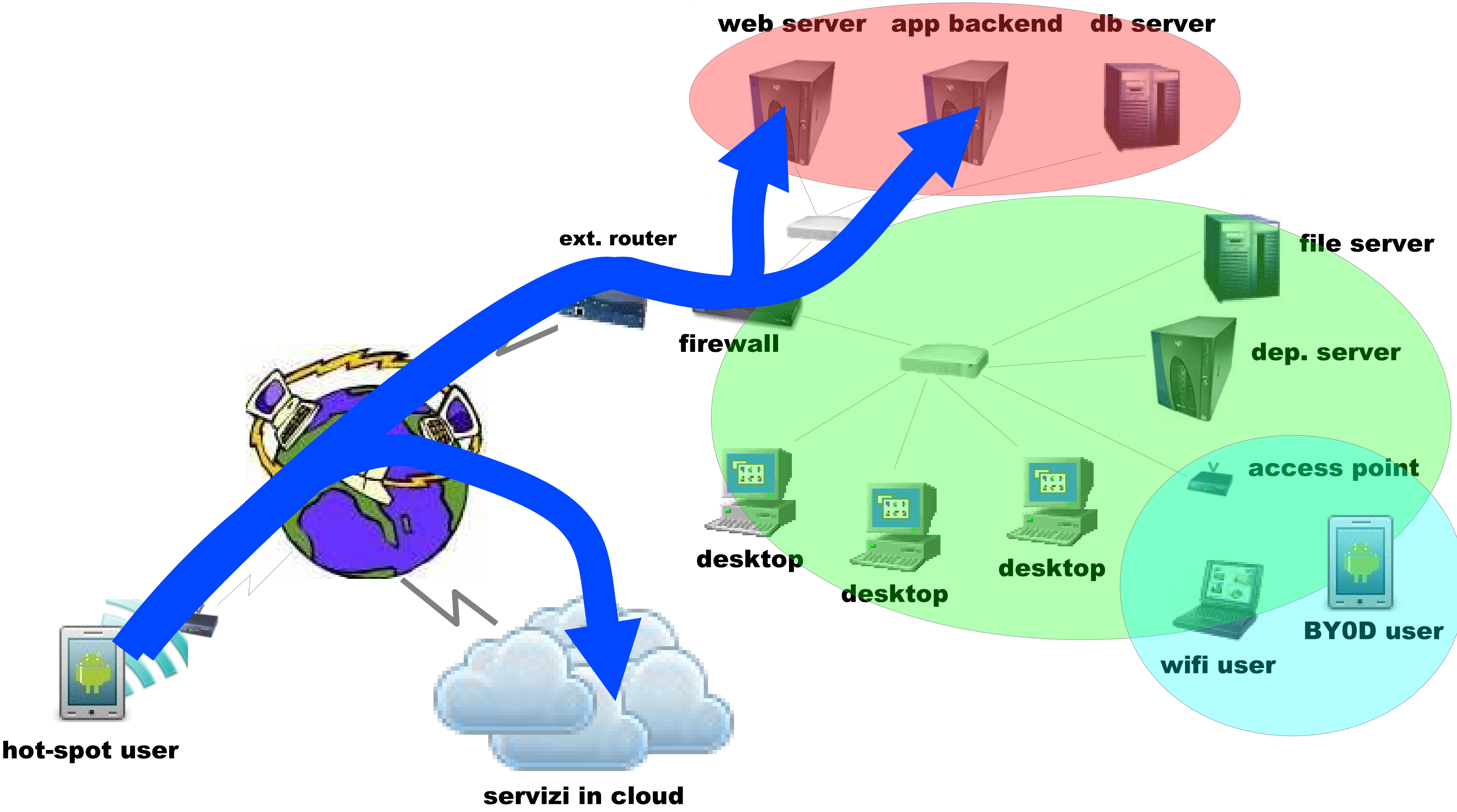
    siti, posta, VPN, .. → cloud storage

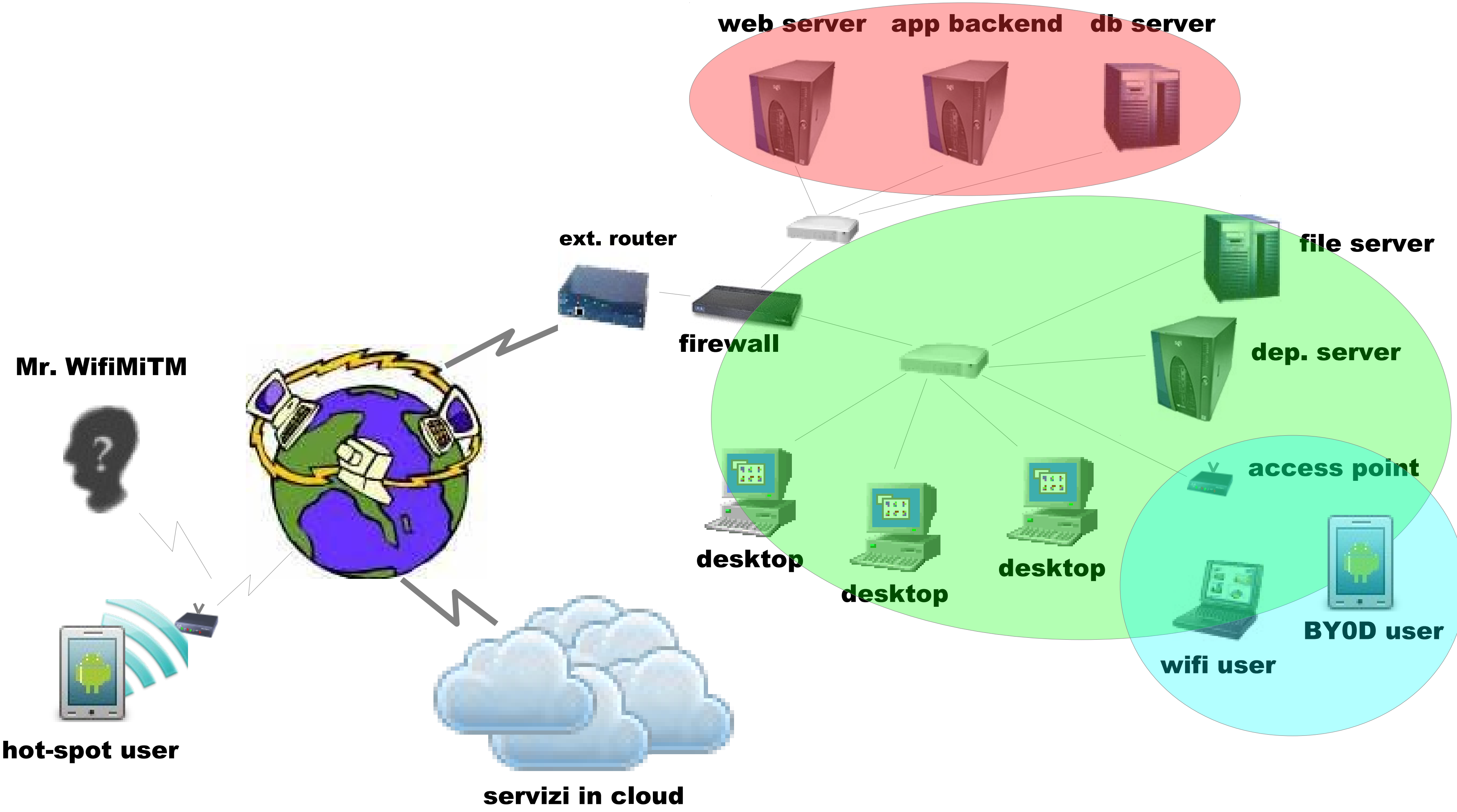

web server
app backend
db server
Mr. MobileMalicious
ext. router
file server
firewall
dep. server
access point
desktop
desktop
desktop
BY0D user
wifi user

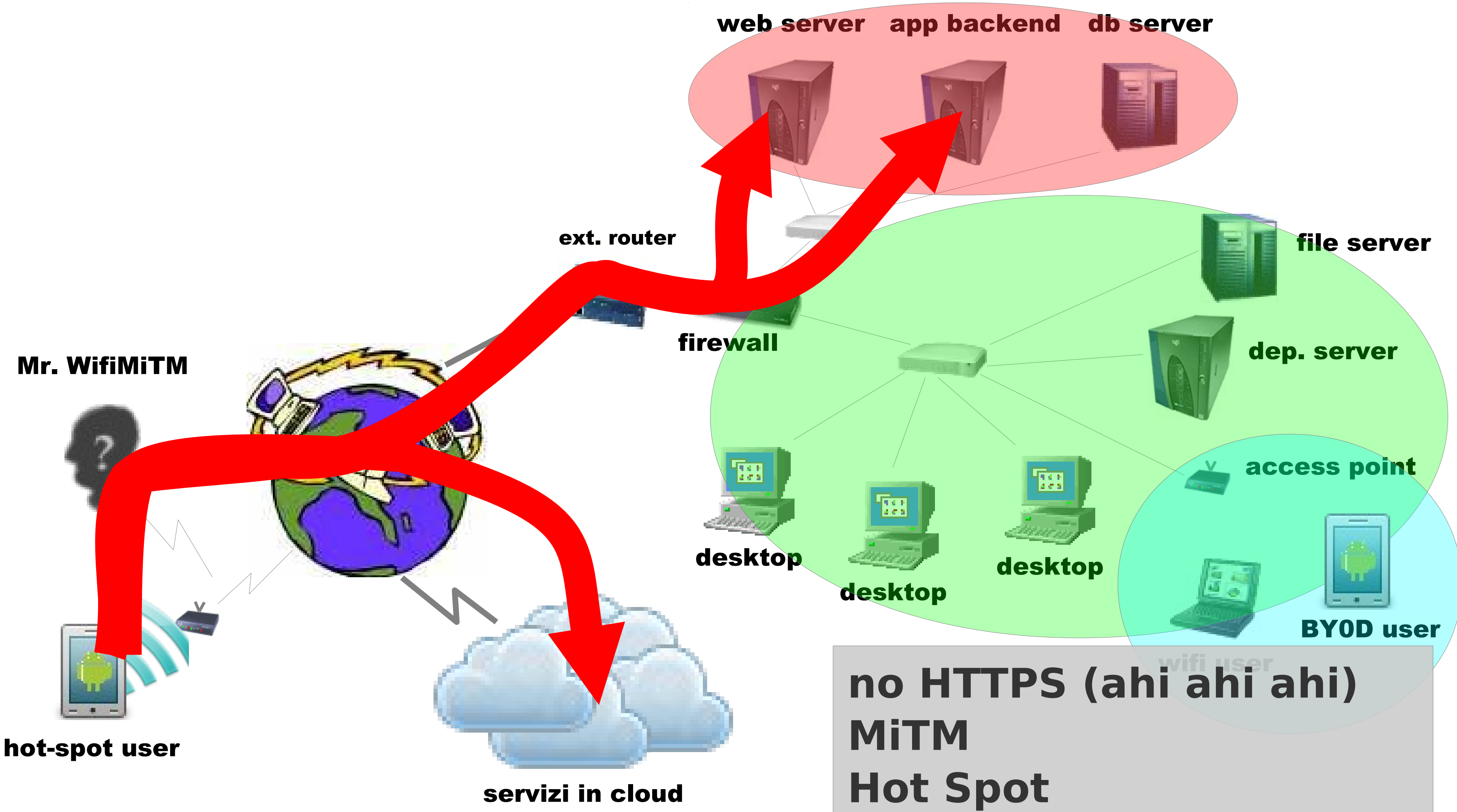
Bring Your 0wned Device



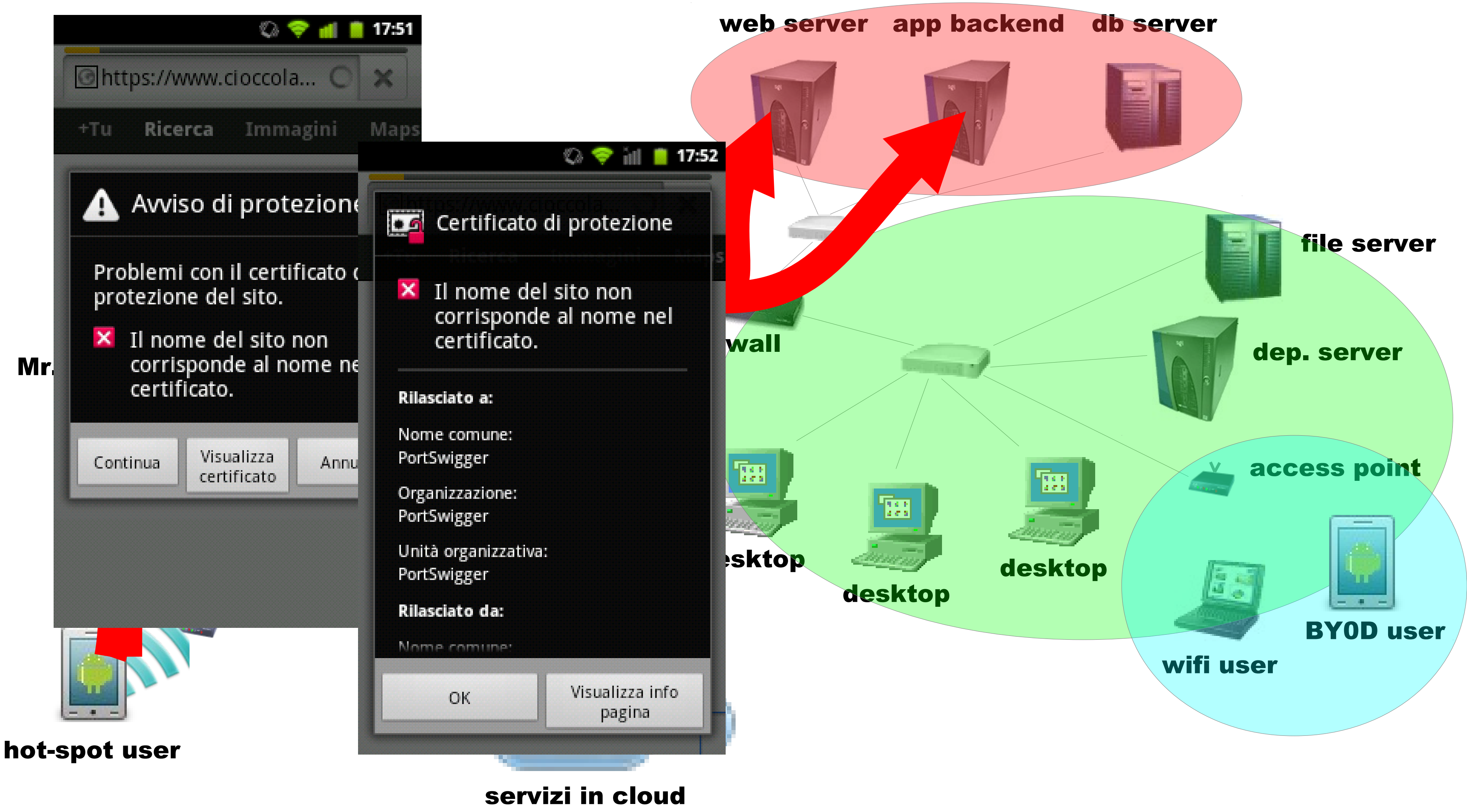

web server
app backend
db server
ext. router
firewall
file server
dep. server
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud


web server
app backend
db server
ext. router
file server
firewall
dep. server
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud


web server
app backend
db server
ext. router
file server
firewall
dep. server
Mr. WifiMiTM
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud



no HTTPS (ahi ahi ahi)
MiTM
Hot Spot
Rogue APs



17:51

https://www.cioccola...

+Tu Ricerca Immagini Maps

Avviso di protezione

Problemi con il certificato d
protezione del sito.

☒ Il nome del sito non corrisponde al nome ne certificato.

Continua

Visualizza certificato

Annu

17:52

Certificato di protezione

☒ Il nome del sito non corrisponde al nome nel certificato.

Rilasciato a:

Nome comune:
PortSwigger

Organizzazione:
PortSwigger

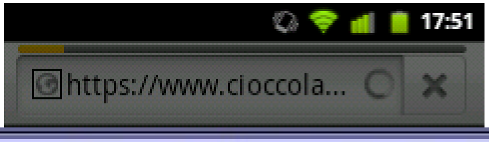
Unità organizzativa:
PortSwigger

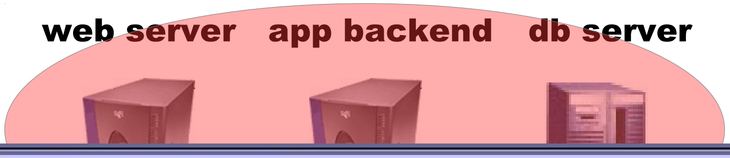
Rilasciato da:

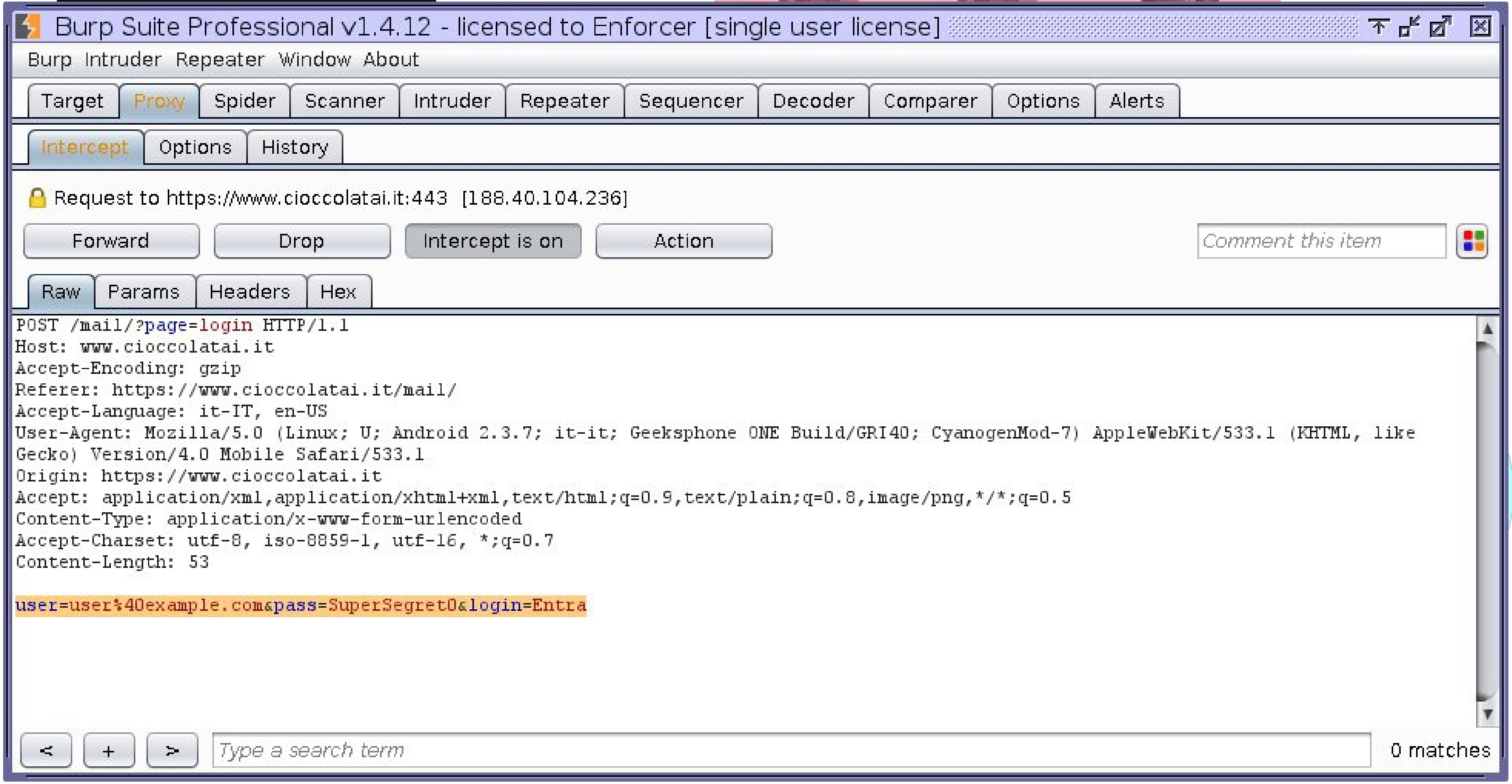
Nome comune:

OK

Visualizza info pagina

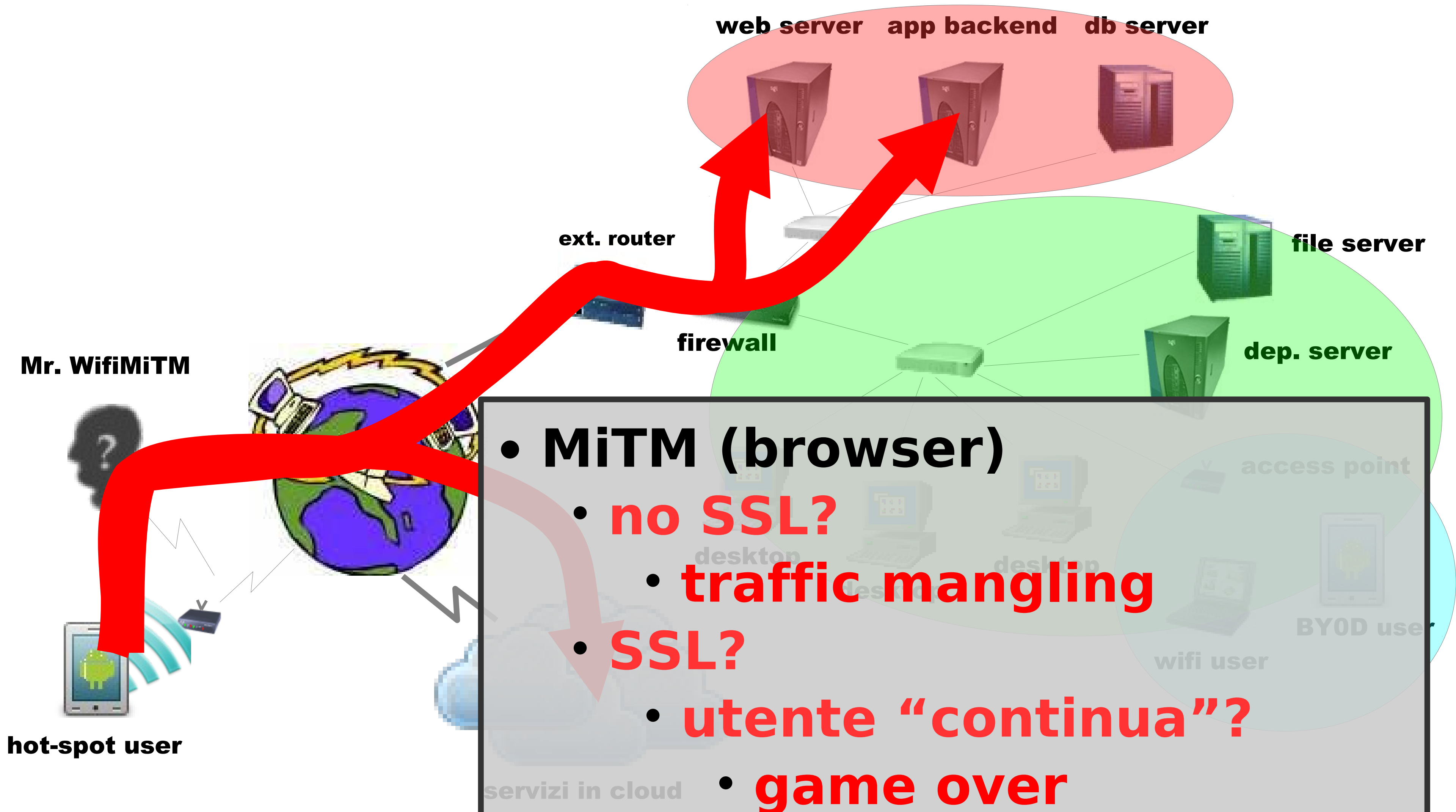




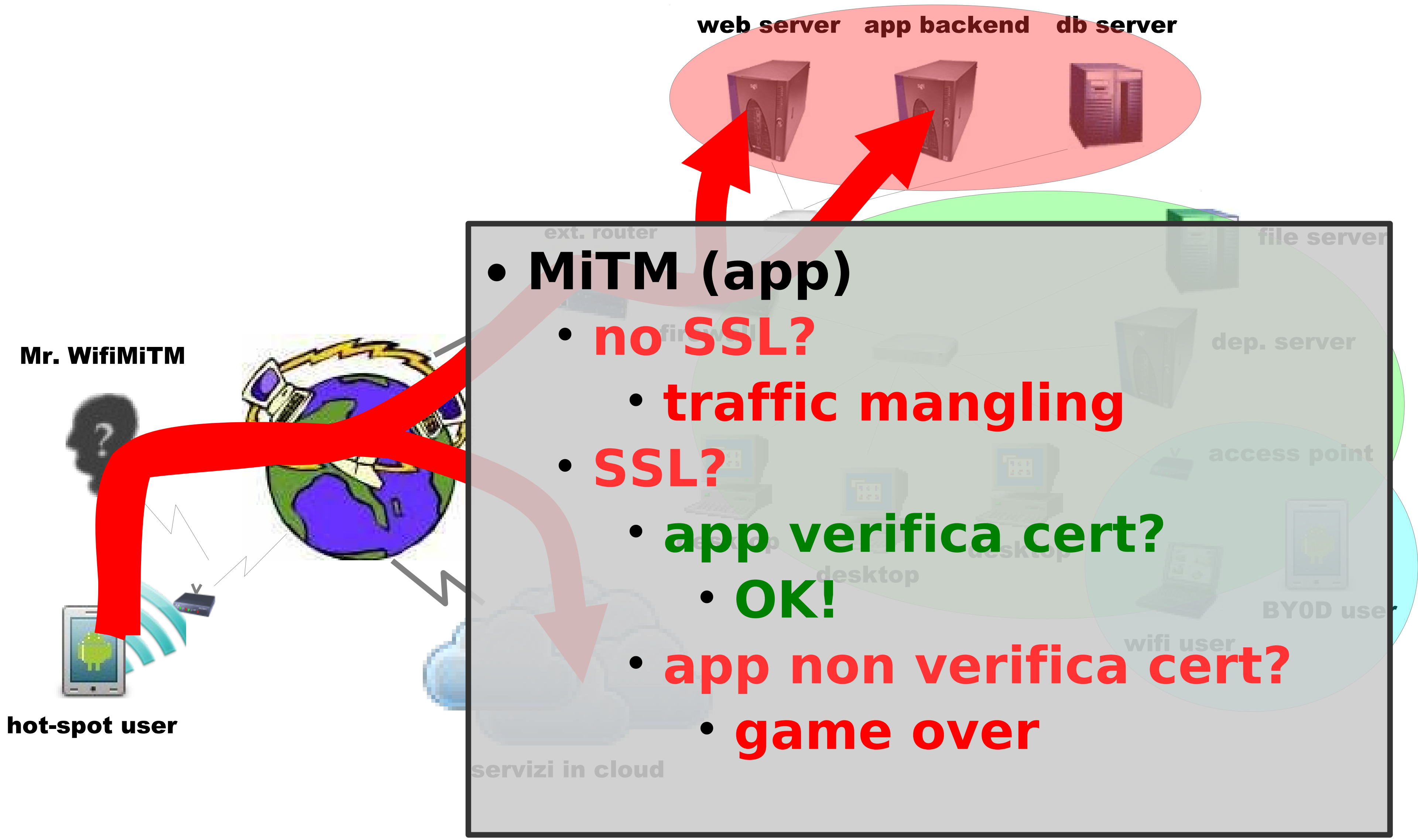

Burp Suite Professional v1.4.12 - licensed to Enforcer [single user license]
Burp Intruder Repeater Window About
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept Options History
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
<
+
>
Type a search term
0 matches

Request to https://www.cioccolatai.it:443 [188.40.104.236]

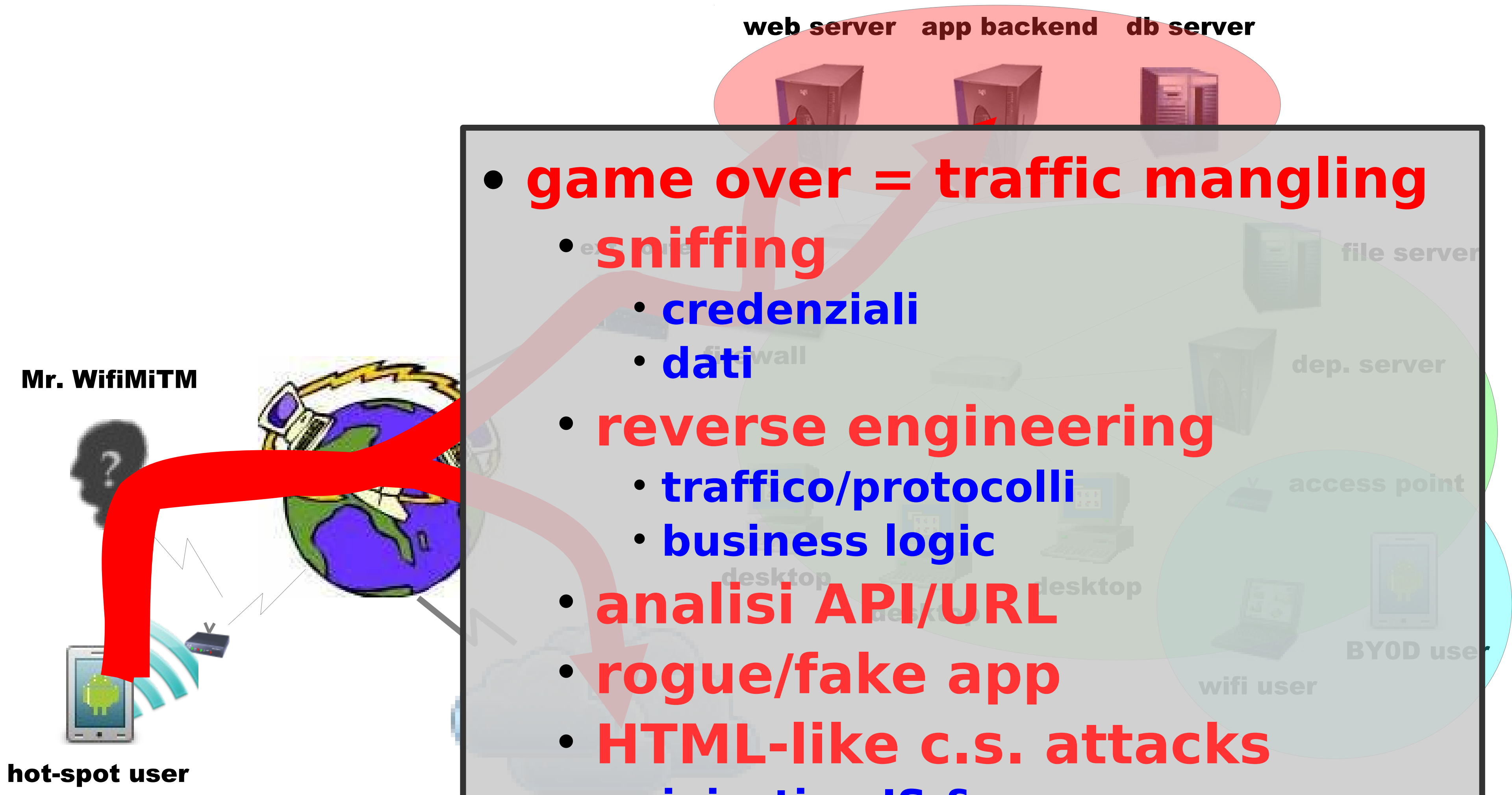
```
POST /mail/?page=login HTTP/1.1
Host: www.cioccolatai.it
Accept-Encoding: gzip
Referer: https://www.cioccolatai.it/mail/
Accept-Language: it-IT, en-US
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; it-it; Geeksphone ONE Build/GRI40; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1
Origin: https://www.cioccolatai.it
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Content-Type: application/x-www-form-urlencoded
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Content-Length: 53

user=user%40example.com&pass=SuperSegret0&login=Entra
```



- MiTM (browser)
  - no SSL?
    - traffic mangling
  - SSL?
    - utente “continua”?
      - game over

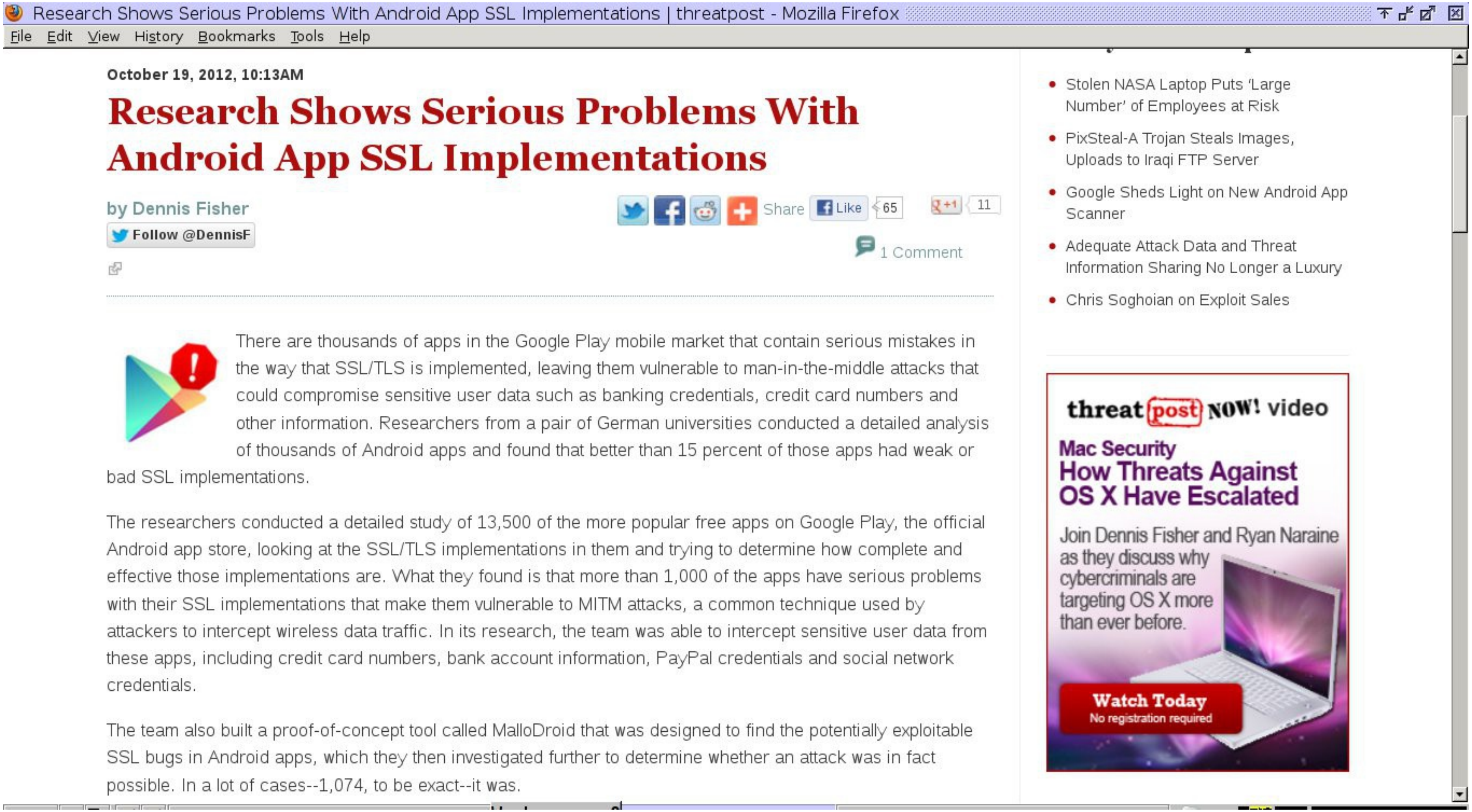


- MiTM (app)
  - no SSL?
    - traffic mangling
  - SSL?
    - app verifica cert?
      - OK!
    - app non verifica cert?
      - game over



- **game over = traffic mangling**
  - **sniffing**
    - **credenziali**
    - **dati**
  - **reverse engineering**
    - **traffico/protocolli**
    - **business logic**
  - **analisi API/URL**
  - **rogue/fake app**
  - **HTML-like c.s. attacks**
    - **injection JS & co.**
    - **client side injection**

https://threatpost.com/en_us/blogs/research-shows-serious-problems-android-app-ssl-implementations-101912


Research Shows Serious Problems With Android App SSL Implementations | threatpost - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Share
Like
65
+1
11
Follow @DennisF
1 Comment

October 19, 2012, 10:13AM

Research Shows Serious Problems With Android App SSL Implementations

by Dennis Fisher

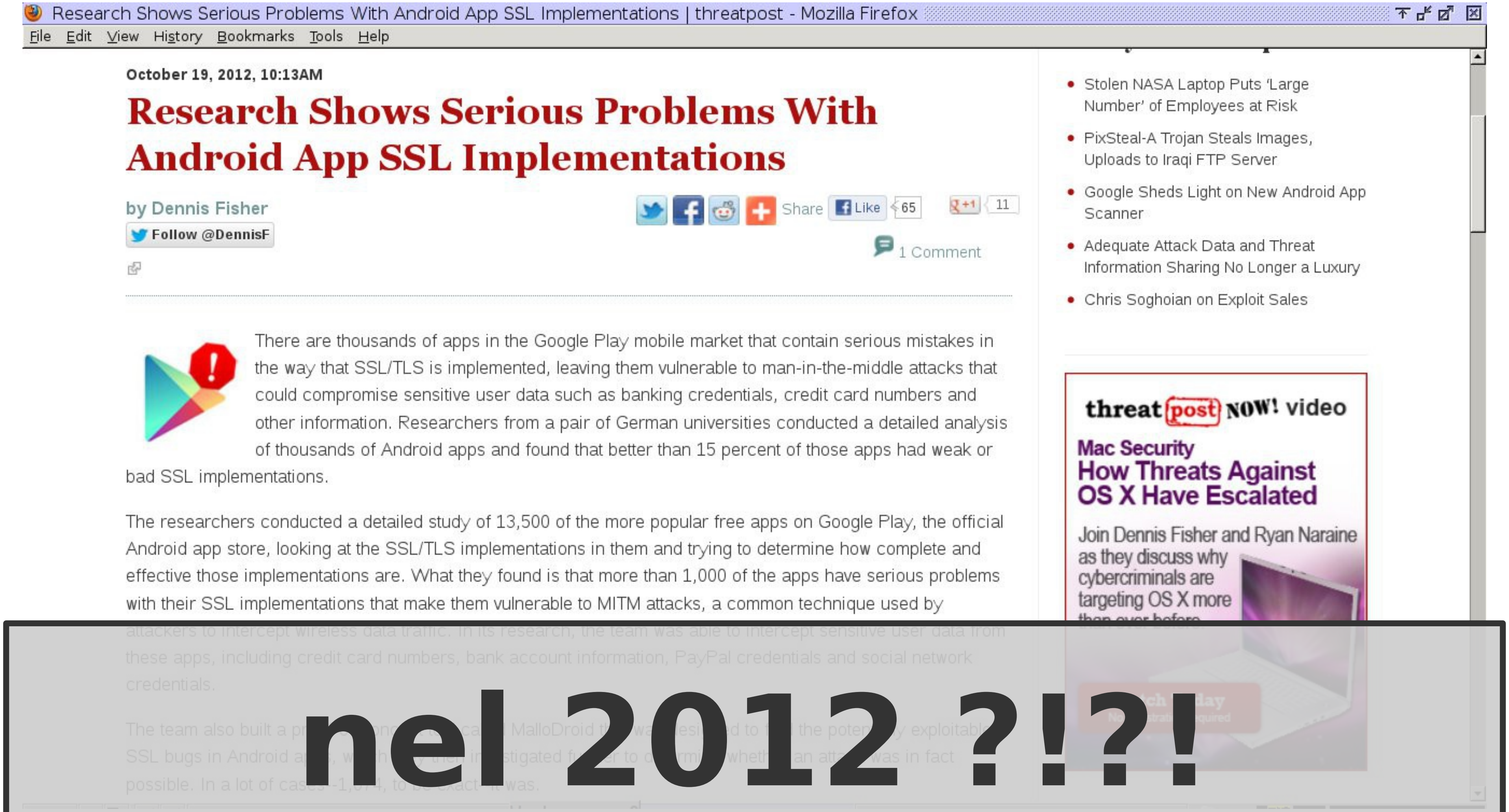
There are thousands of apps in the Google Play mobile market that contain serious mistakes in the way that SSL/TLS is implemented, leaving them vulnerable to man-in-the-middle attacks that could compromise sensitive user data such as banking credentials, credit card numbers and other information. Researchers from a pair of German universities conducted a detailed analysis of thousands of Android apps and found that better than 15 percent of those apps had weak or bad SSL implementations.

The researchers conducted a detailed study of 13,500 of the more popular free apps on Google Play, the official Android app store, looking at the SSL/TLS implementations in them and trying to determine how complete and effective those implementations are. What they found is that more than 1,000 of the apps have serious problems with their SSL implementations that make them vulnerable to MITM attacks, a common technique used by attackers to intercept wireless data traffic. In its research, the team was able to intercept sensitive user data from these apps, including credit card numbers, bank account information, PayPal credentials and social network credentials.

The team also built a proof-of-concept tool called MalloDroid that was designed to find the potentially exploitable SSL bugs in Android apps, which they then investigated further to determine whether an attack was in fact possible. In a lot of cases--1,074, to be exact--it was.

- Stolen NASA Laptop Puts ‘Large Number’ of Employees at Risk
- PixSteal-A Trojan Steals Images, Uploads to Iraqi FTP Server
- Google Sheds Light on New Android App Scanner
- Adequate Attack Data and Threat Information Sharing No Longer a Luxury
- Chris Soghoian on Exploit Sales

https://threatpost.com/en_us/blogs/research-shows-serious-problems-android-app-ssl-implementations-101912


Research Shows Serious Problems With Android App SSL Implementations | threatpost - Mozilla Firefox
File Edit View History Bookmarks Tools Help

October 19, 2012, 10:13AM

Research Shows Serious Problems With Android App SSL Implementations

by Dennis Fisher

Follow @DennisF
Share
Like 65
+1 11
1 Comment

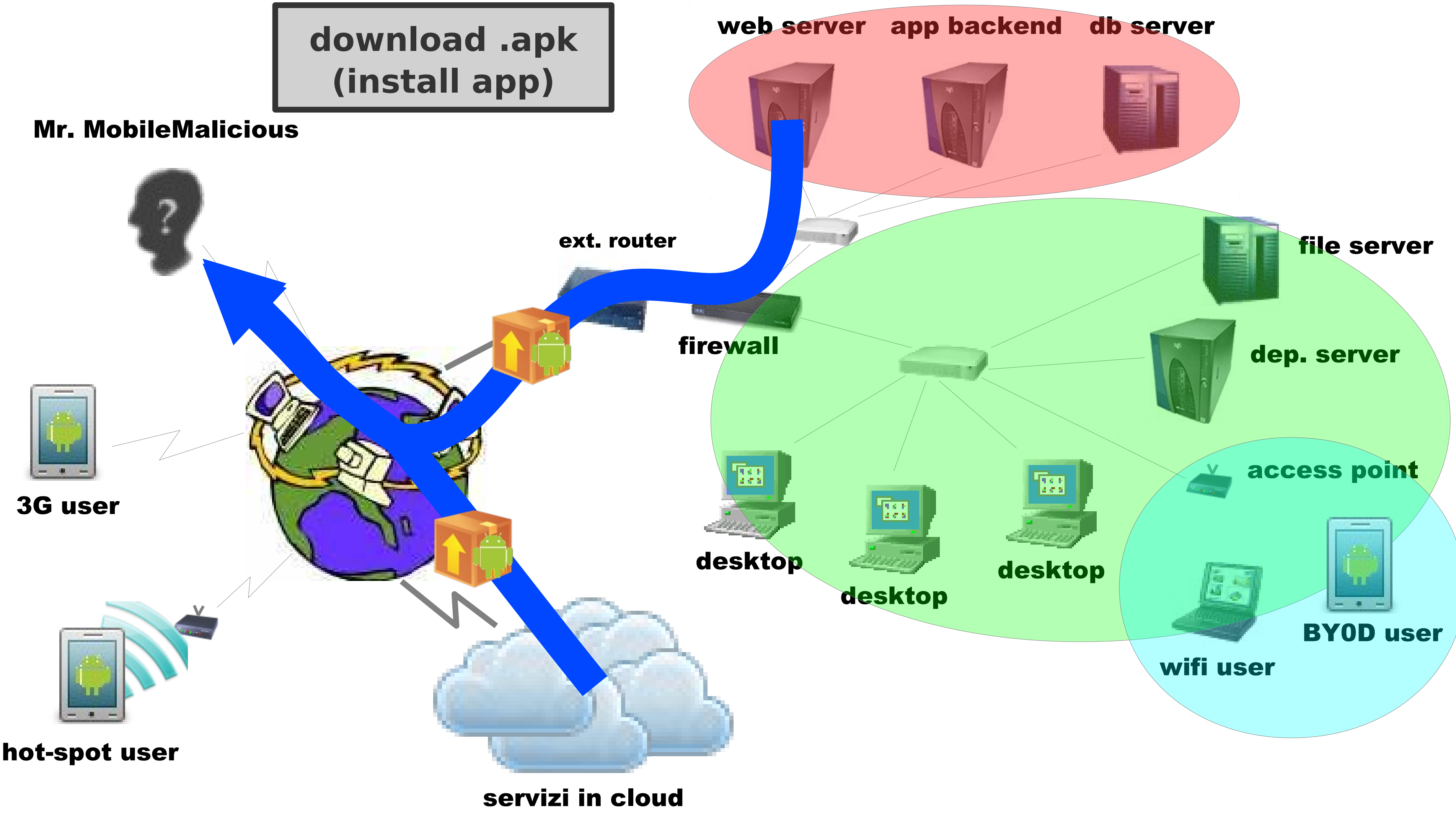
There are thousands of apps in the Google Play mobile market that contain serious mistakes in the way that SSL/TLS is implemented, leaving them vulnerable to man-in-the-middle attacks that could compromise sensitive user data such as banking credentials, credit card numbers and other information. Researchers from a pair of German universities conducted a detailed analysis of thousands of Android apps and found that better than 15 percent of those apps had weak or bad SSL implementations.

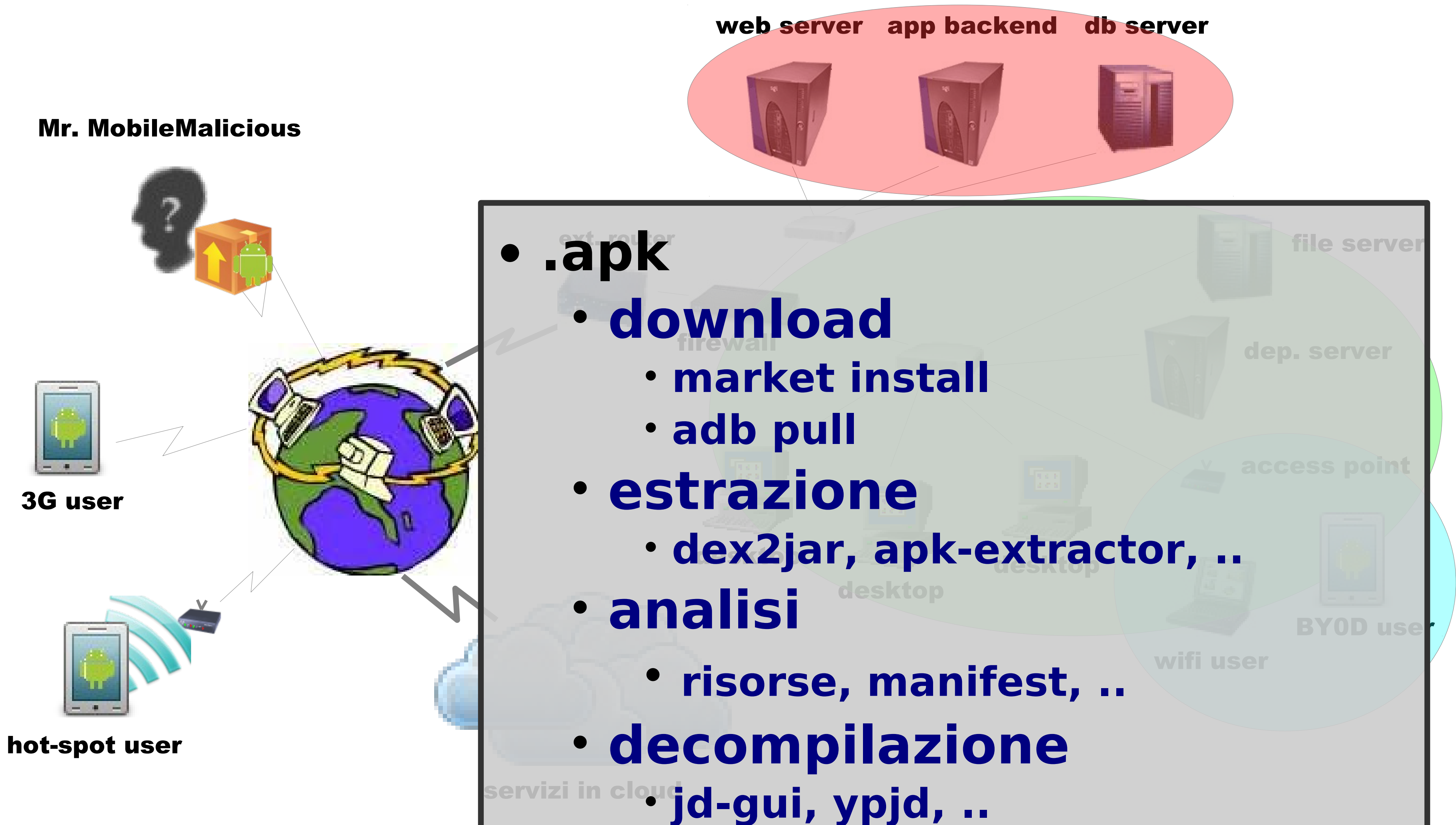
The researchers conducted a detailed study of 13,500 of the more popular free apps on Google Play, the official Android app store, looking at the SSL/TLS implementations in them and trying to determine how complete and effective those implementations are. What they found is that more than 1,000 of the apps have serious problems with their SSL implementations that make them vulnerable to MITM attacks, a common technique used by attackers to intercept wireless data traffic. In its research, the team was able to intercept sensitive user data from these apps, including credit card numbers, bank account information, PayPal credentials and social network credentials.

The team also built a proof-of-concept tool called MalloDroid that was designed to find the potentially exploitable SSL bugs in Android apps, which they then investigated further to confirm whether an attack was in fact possible. In a lot of cases--1,074, to be exact--it was.

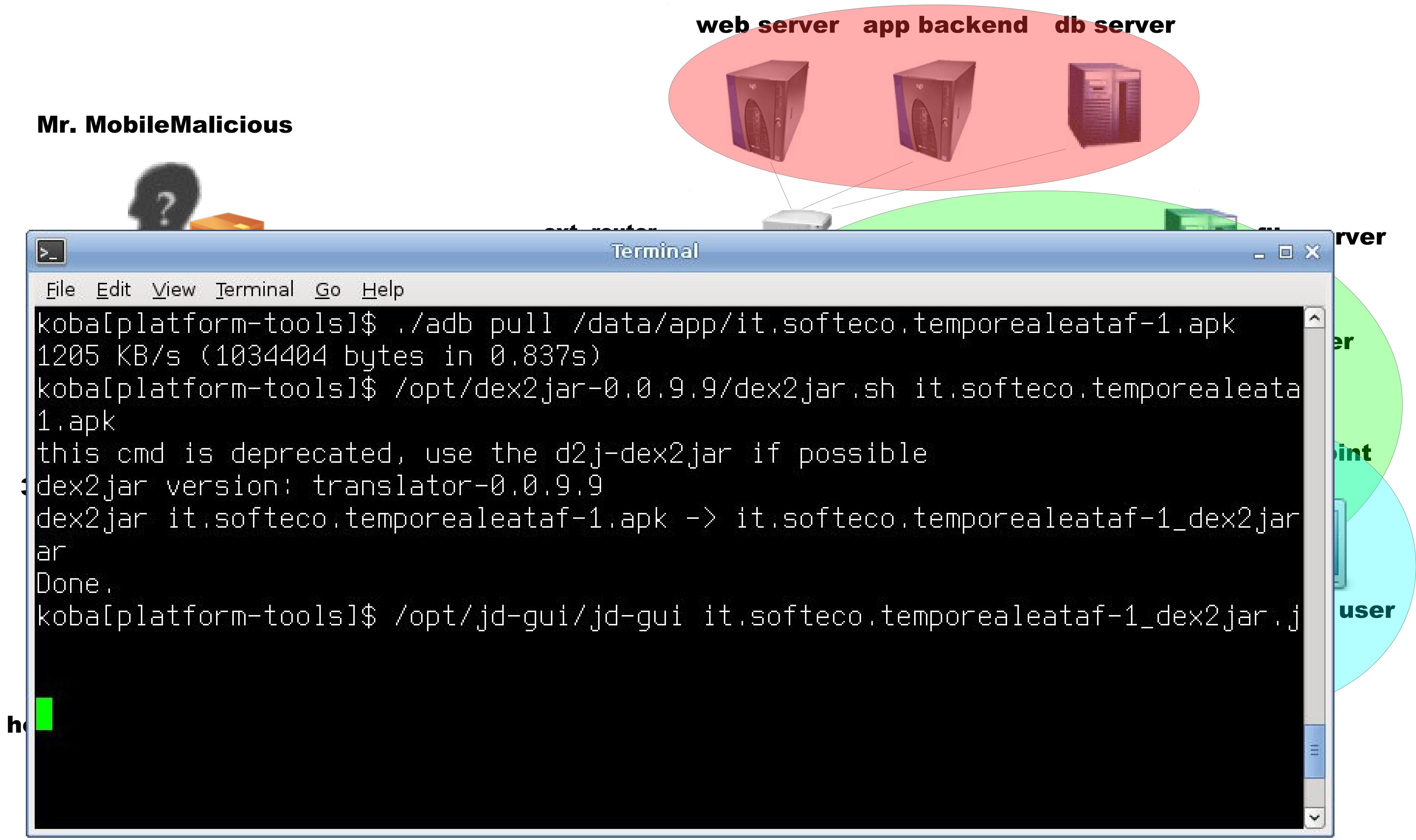
- Stolen NASA Laptop Puts 'Large Number' of Employees at Risk
- PixSteal-A Trojan Steals Images, Uploads to Iraqi FTP Server
- Google Sheds Light on New Android App Scanner
- Adequate Attack Data and Threat Information Sharing No Longer a Luxury
- Chris Soghoian on Exploit Sales

nel 2012 ?!?!


download .apk
(install app)
Mr. MobileMalicious
web server
app backend
db server
ext. router
firewall
file server
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud

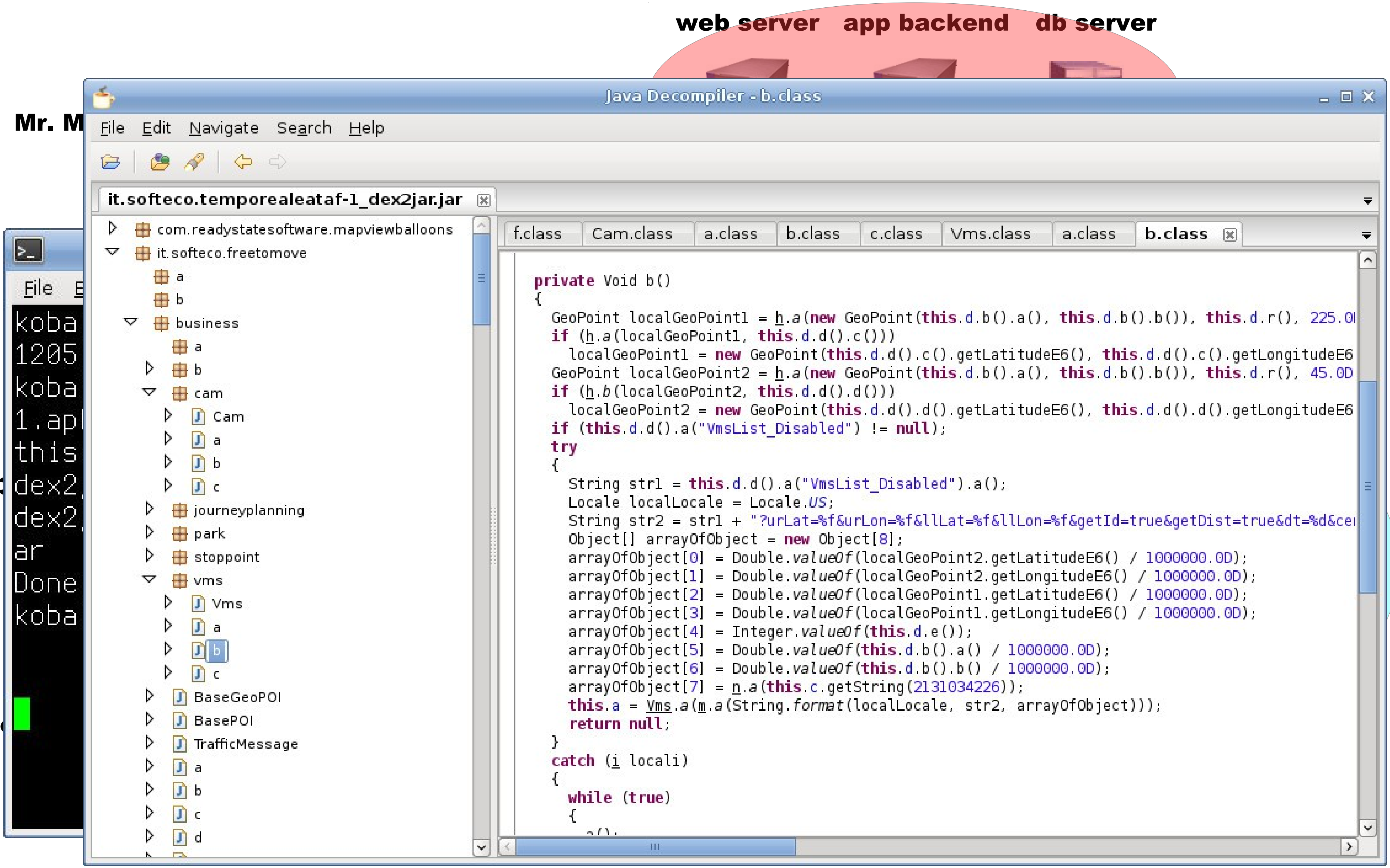


- .apk
  - download
    - market install
    - adb pull
  - estrazione
    - dex2jar, apk-extractor, ..
  - analisi
    - risorse, manifest, ..
  - decompilazione
    - jd-gui, ypjd, ..



```
koba[platform-tools]$ ./adb pull /data/app/it.softeco.temporealeataf-1.apk
1205 KB/s (1034404 bytes in 0.837s)
koba[platform-tools]$ /opt/dex2jar-0.0.9.9/dex2jar.sh it.softeco.temporealeata
1.apk
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.9
dex2jar it.softeco.temporealeataf-1.apk -> it.softeco.temporealeataf-1_dex2jar
ar
Done.
koba[platform-tools]$ /opt/jd-gui/jd-gui it.softeco.temporealeataf-1_dex2jar.j
```

Mr. M



```
File E
koba
1205
koba
1.apl
this
dex2
dex2
ar
Done
koba
```

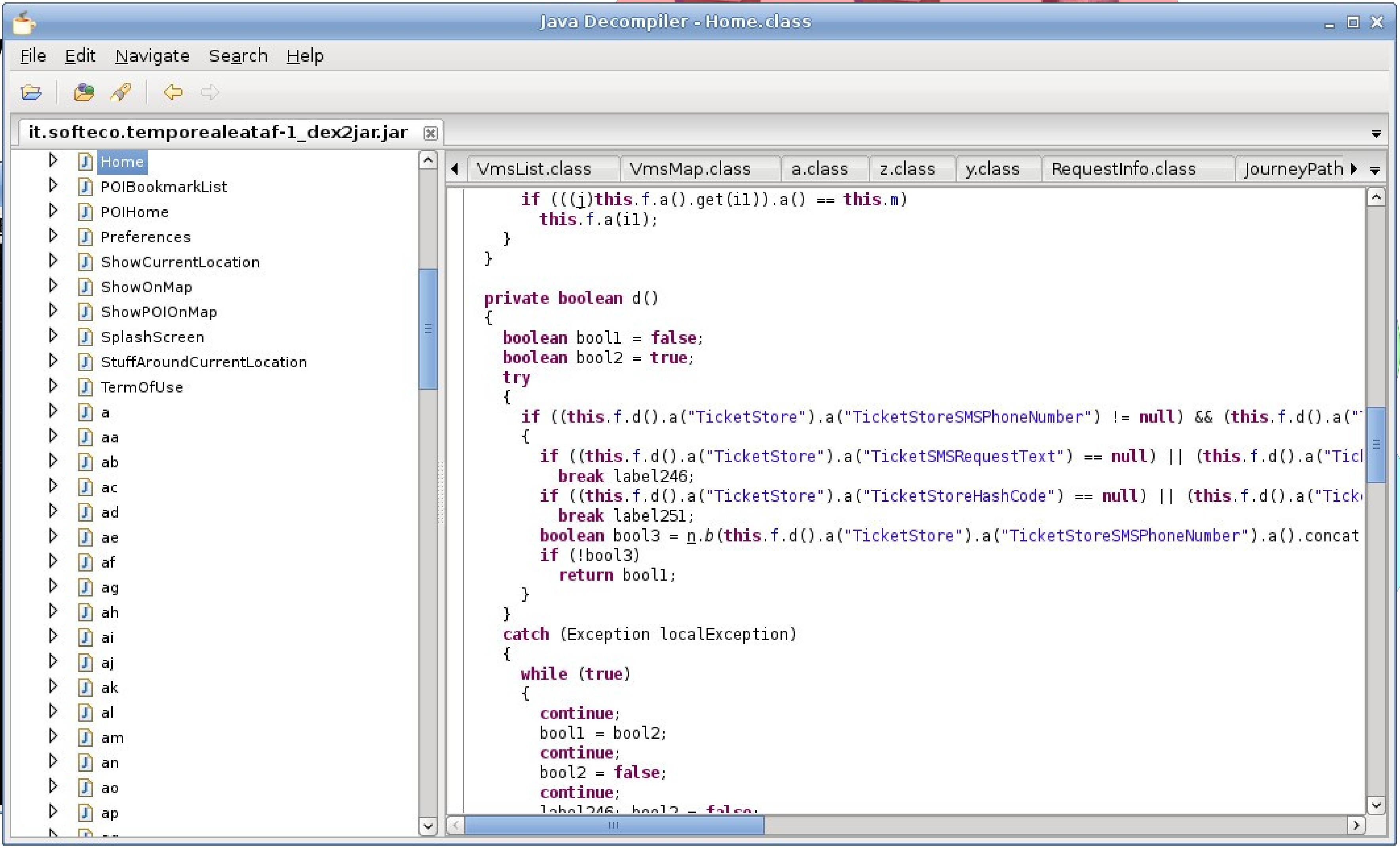
```
private Void b()
{
  GeoPoint localGeoPoint1 = h.a(new GeoPoint(this.d.b().a(), this.d.b().b()), this.d.r(), 225.0D
  if (h.a(localGeoPoint1, this.d.d().c()))
    localGeoPoint1 = new GeoPoint(this.d.d().c().getLatitudeE6(), this.d.d().c().getLongitudeE6
  GeoPoint localGeoPoint2 = h.a(new GeoPoint(this.d.b().a(), this.d.b().b()), this.d.r(), 45.0D
  if (h.b(localGeoPoint2, this.d.d().d()))
    localGeoPoint2 = new GeoPoint(this.d.d().d().getLatitudeE6(), this.d.d().d().getLongitudeE6
  if (this.d.d().a("VmsList_Disabled") != null);
  try
  {
    String str1 = this.d.d().a("VmsList_Disabled").a();
    Locale localLocale = Locale.US;
    String str2 = str1 + "?urLat=%f&urLon=%f&llLat=%f&llLon=%f&getId=true&getDist=true&dt=%d&ce
    Object[] arrayOfObject = new Object[8];
    arrayOfObject[0] = Double.valueOf(localGeoPoint2.getLatitudeE6() / 1000000.0D);
    arrayOfObject[1] = Double.valueOf(localGeoPoint2.getLongitudeE6() / 1000000.0D);
    arrayOfObject[2] = Double.valueOf(localGeoPoint1.getLatitudeE6() / 1000000.0D);
    arrayOfObject[3] = Double.valueOf(localGeoPoint1.getLongitudeE6() / 1000000.0D);
    arrayOfObject[4] = Integer.valueOf(this.d.e());
    arrayOfObject[5] = Double.valueOf(this.d.b().a() / 1000000.0D);
    arrayOfObject[6] = Double.valueOf(this.d.b().b() / 1000000.0D);
    arrayOfObject[7] = n.a(this.c.getString(2131034226));
    this.a = Vms.a(m.a(String.format(localLocale, str2, arrayOfObject)));
    return null;
  }
  catch (i locali)
  {
    while (true)
    {
      a();
```

h

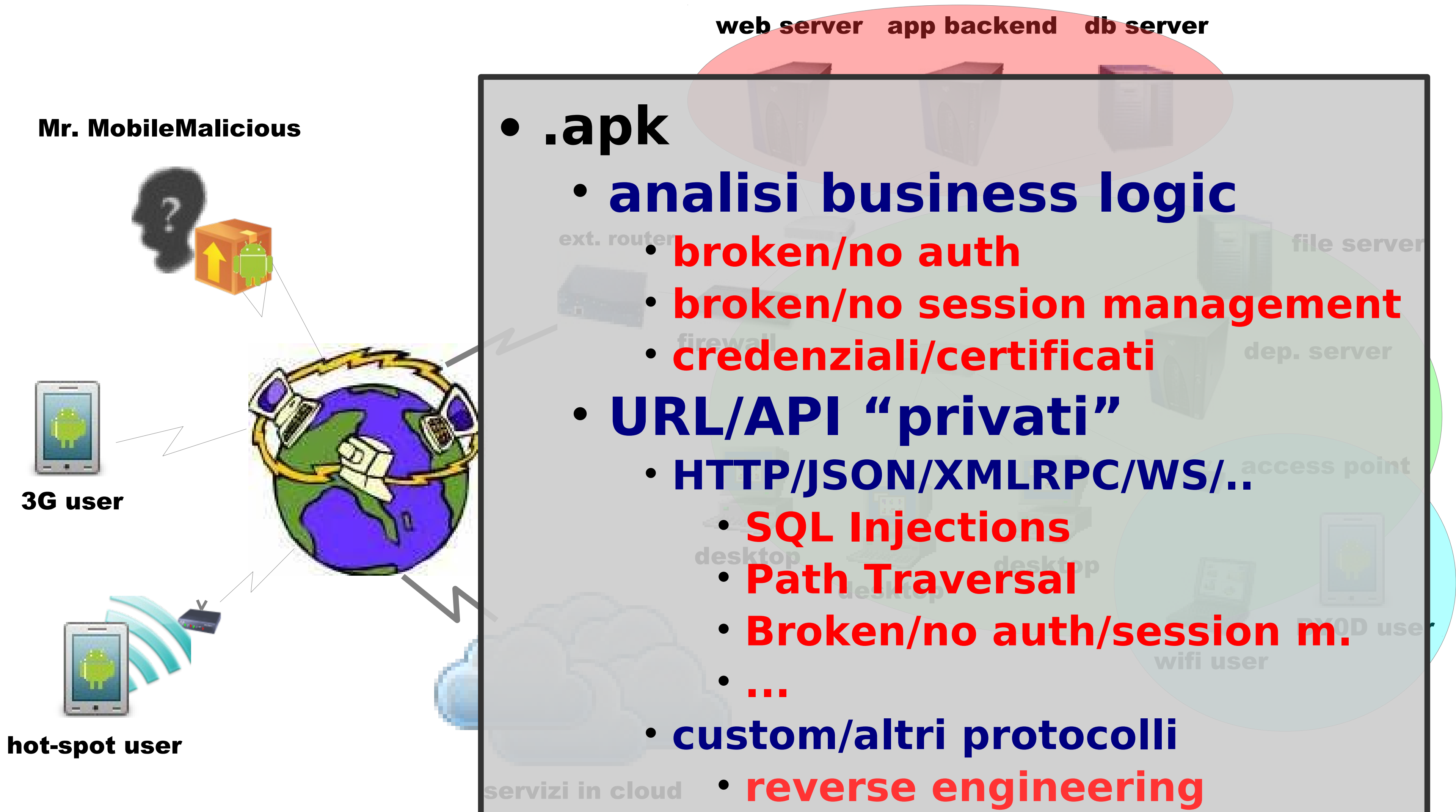
Mr. M

```
koba
1205
koba
1.ap
this
dex2
dex2
ar
Done
koba
```

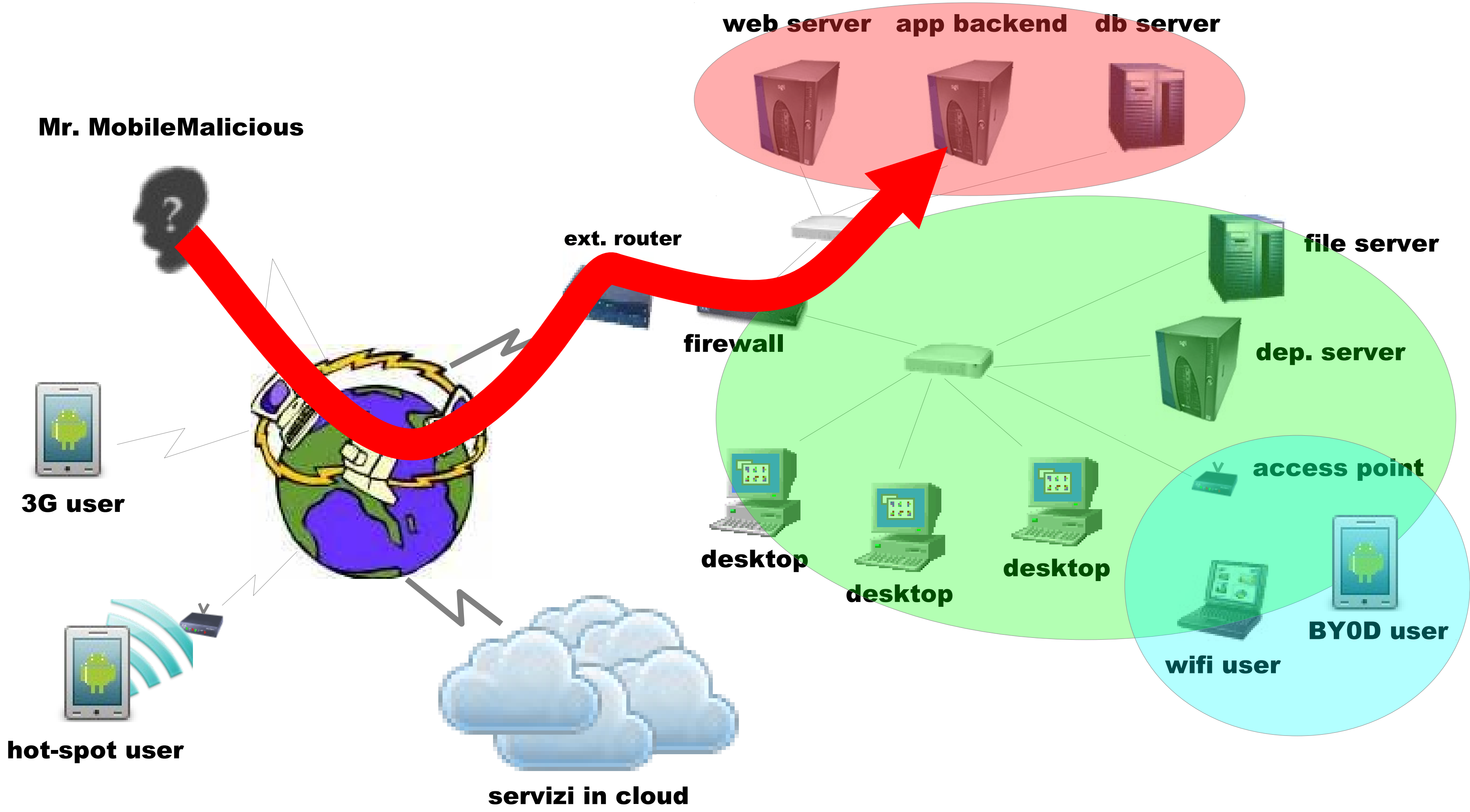
h

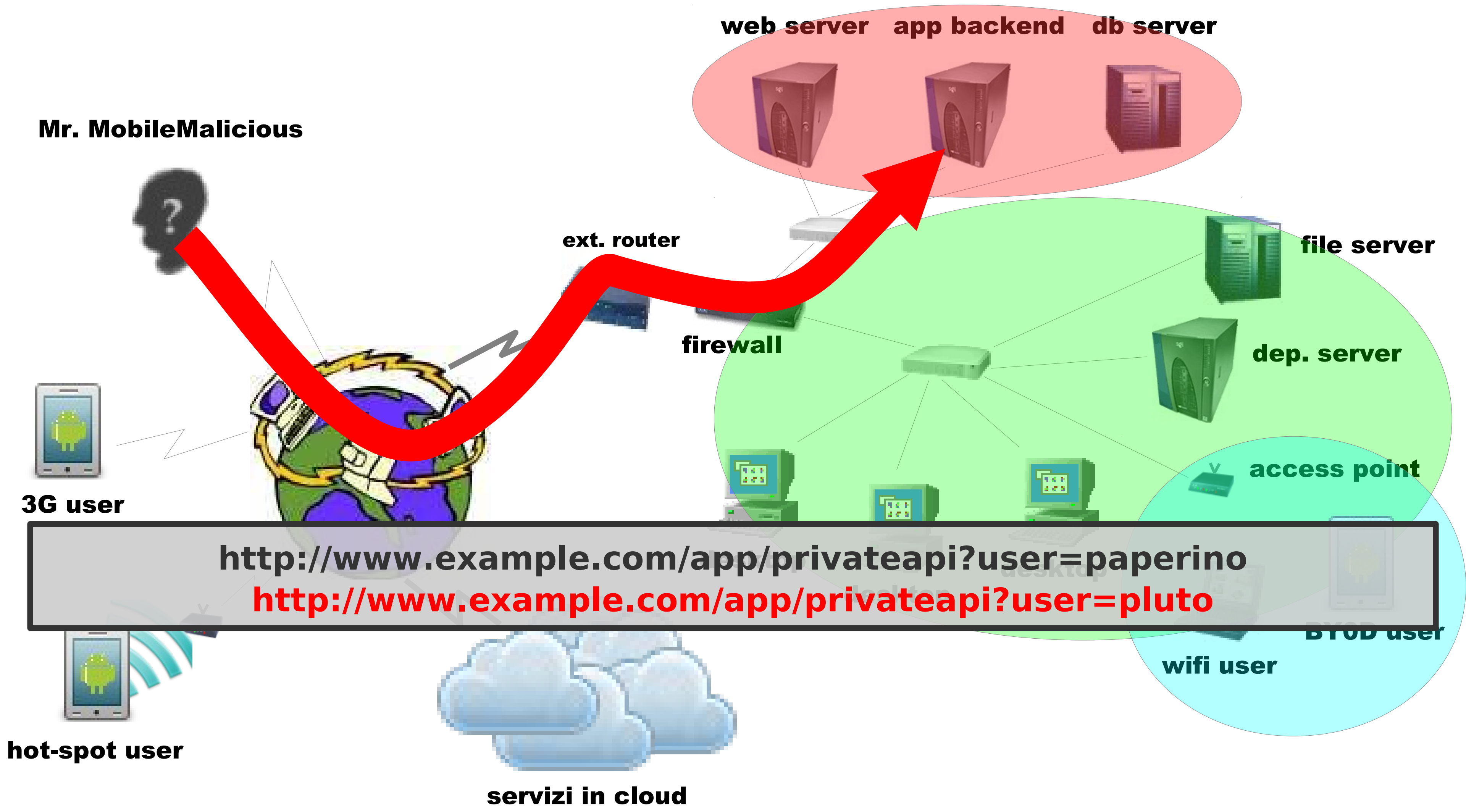


```
      if (((j)this.f.a().get(i1)).a() == this.m)
        this.f.a(i1);
    }
  }

  private boolean d()
  {
    boolean bool1 = false;
    boolean bool2 = true;
    try
    {
      if ((this.f.d().a("TicketStore").a("TicketStoreSMSPhoneNumber") != null) && (this.f.d().a("
      {
        if ((this.f.d().a("TicketStore").a("TicketSMSRequestText") == null) || (this.f.d().a("Ticl
          break label246;
        if ((this.f.d().a("TicketStore").a("TicketStoreHashCode") == null) || (this.f.d().a("Ticke
          break label251;
        boolean bool3 = n.b(this.f.d().a("TicketStore").a("TicketStoreSMSPhoneNumber").a().concat
        if (!bool3)
          return bool1;
      }
    }
    catch (Exception localException)
    {
      while (true)
      {
        continue;
        bool1 = bool2;
        continue;
        bool2 = false;
        continue;
        label246: bool2 = false;
```



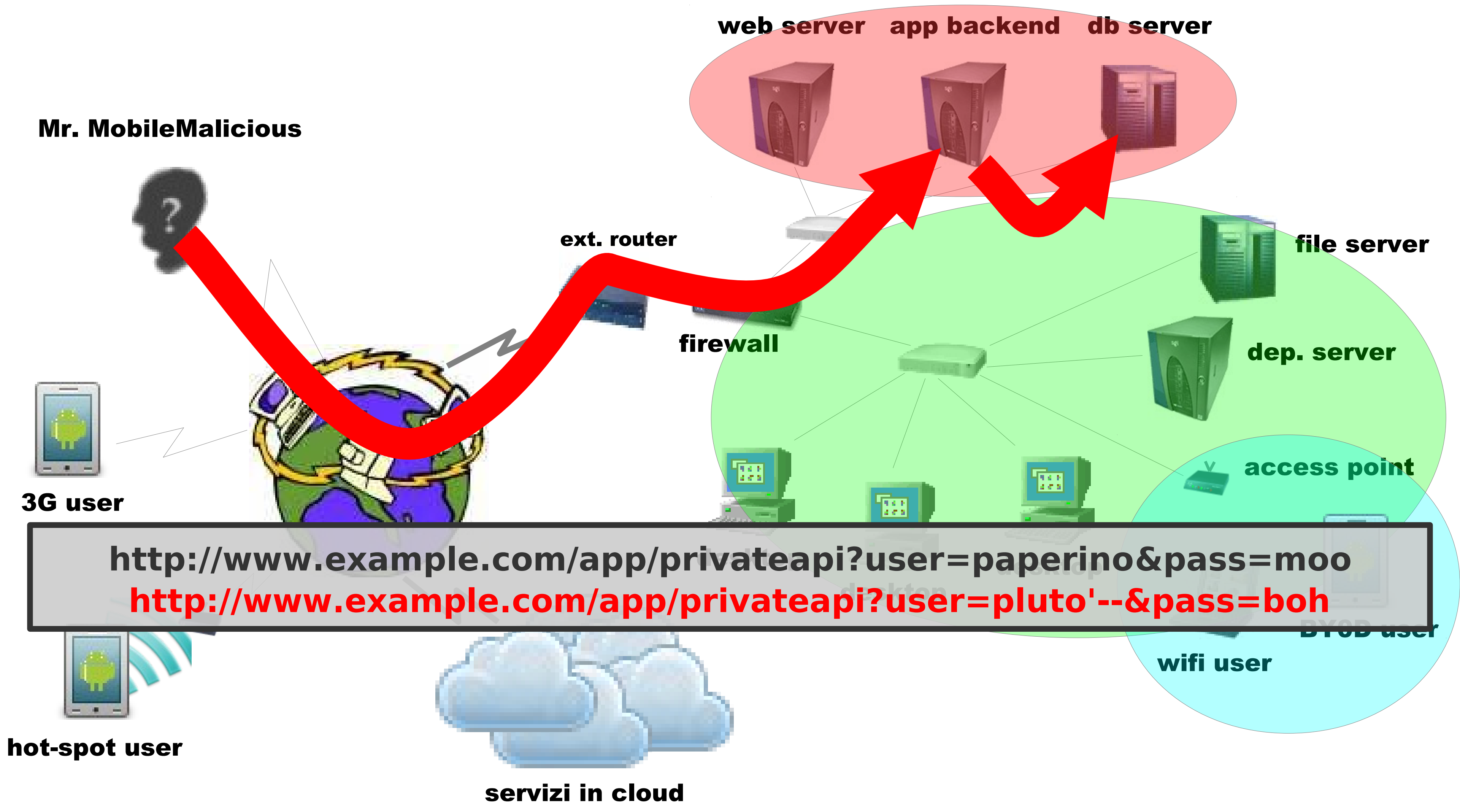
- .apk
  - analisi business logic
    - broken/no auth
    - broken/no session management
    - credenziali/certificati
  - URL/API “privati”
    - HTTP/JSON/XMLRPC/WS/..
      - SQL Injections
      - Path Traversal
      - Broken/no auth/session m.
      - ...
    - custom/altri protocolli
      - reverse engineering
      - vedi sopra


web server
app backend
db server
Mr. MobileMalicious
ext. router
file server
firewall
dep. server
3G user
access point
desktop
desktop
desktop
BY0D user
wifi user
hot-spot user
servizi in cloud



http://www.example.com/app/privateapi?user=paperino

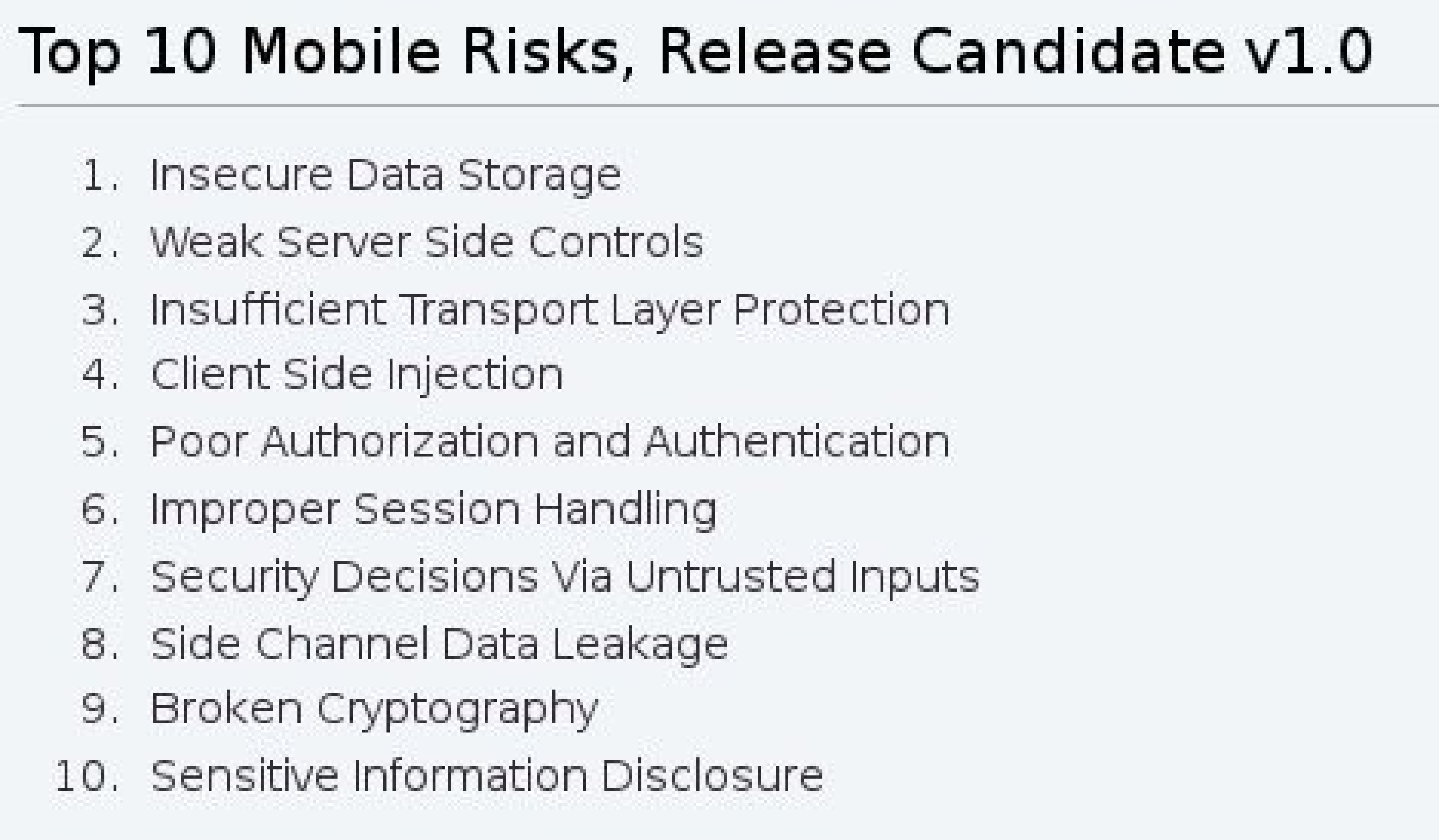
http://www.example.com/app/privateapi?user=pluto



http://www.example.com/app/privateapi?user=paperino&pass=moo

http://www.example.com/app/privateapi?user=pluto'--&pass=boh

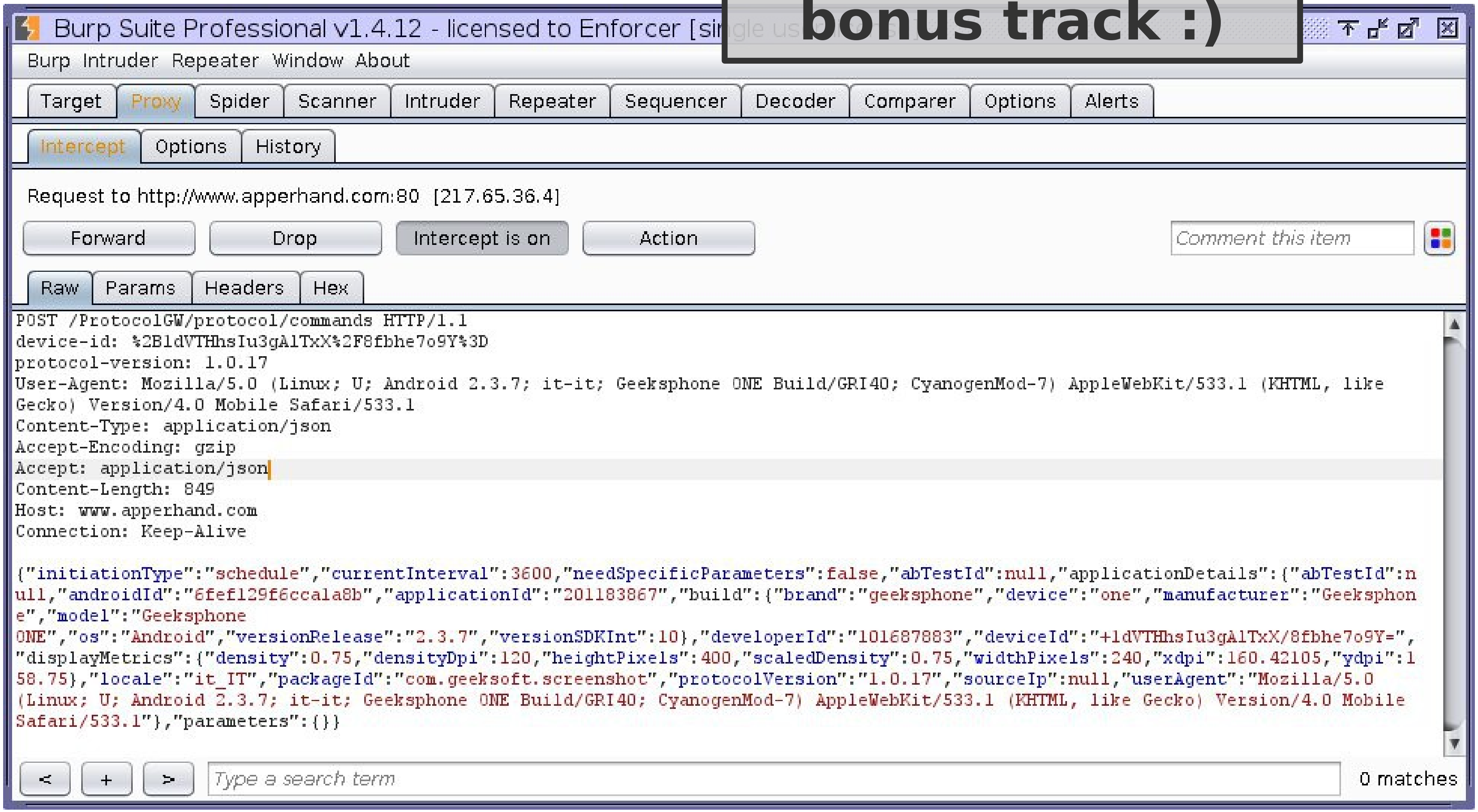
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks



Top 10 Mobile Risks, Release Candidate v1.0

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

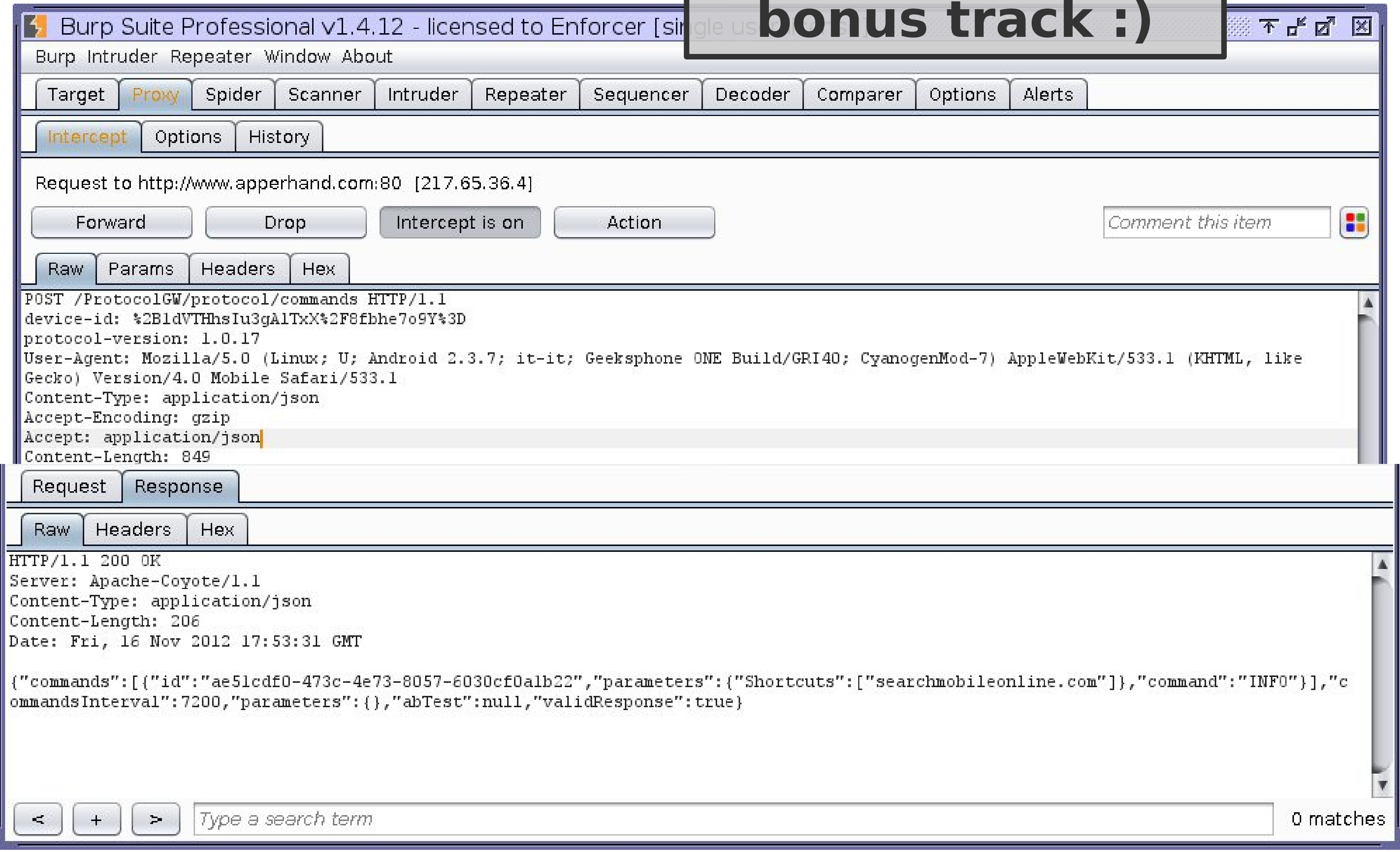
bonus track :)



Request to http://www.apperhand.com:80 [217.65.36.4]

```
POST /ProtocolGW/protocol/commands HTTP/1.1
device-id: %2B1dVTHhsIu3gAlTxX%2F8fbhe7o9Y%3D
protocol-version: 1.0.17
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; it-it; Geeksphone ONE Build/GRI40; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1
Content-Type: application/json
Accept-Encoding: gzip
Accept: application/json
Content-Length: 849
Host: www.apperhand.com
Connection: Keep-Alive

{"initiationType":"schedule","currentInterval":3600,"needSpecificParameters":false,"abTestId":null,"applicationDetails":{"abTestId":n
ull,"androidId":"6fef129f6ccala8b","applicationId":"201183867","build":{"brand":"geeksphone","device":"one","manufacturer":"Geeksphon
e","model":"Geeksphone
ONE","os":"Android","versionRelease":"2.3.7","versionSDKInt":10},"developerId":"101687883","deviceId":"+1dVTHhsIu3gAlTxX/8fbhe7o9Y=",
"displayMetrics":{"density":0.75,"densityDpi":120,"heightPixels":400,"scaledDensity":0.75,"widthPixels":240,"xdpi":160.42105,"ydpi":1
58.75},"locale":"it_IT","packageId":"com.geeksoft.screenshot","protocolVersion":"1.0.17","sourceIp":null,"userAgent":"Mozilla/5.0
(Linux; U; Android 2.3.7; it-it; Geeksphone ONE Build/GRI40; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile
Safari/533.1"},"parameters":{}}
```

bonus track :)

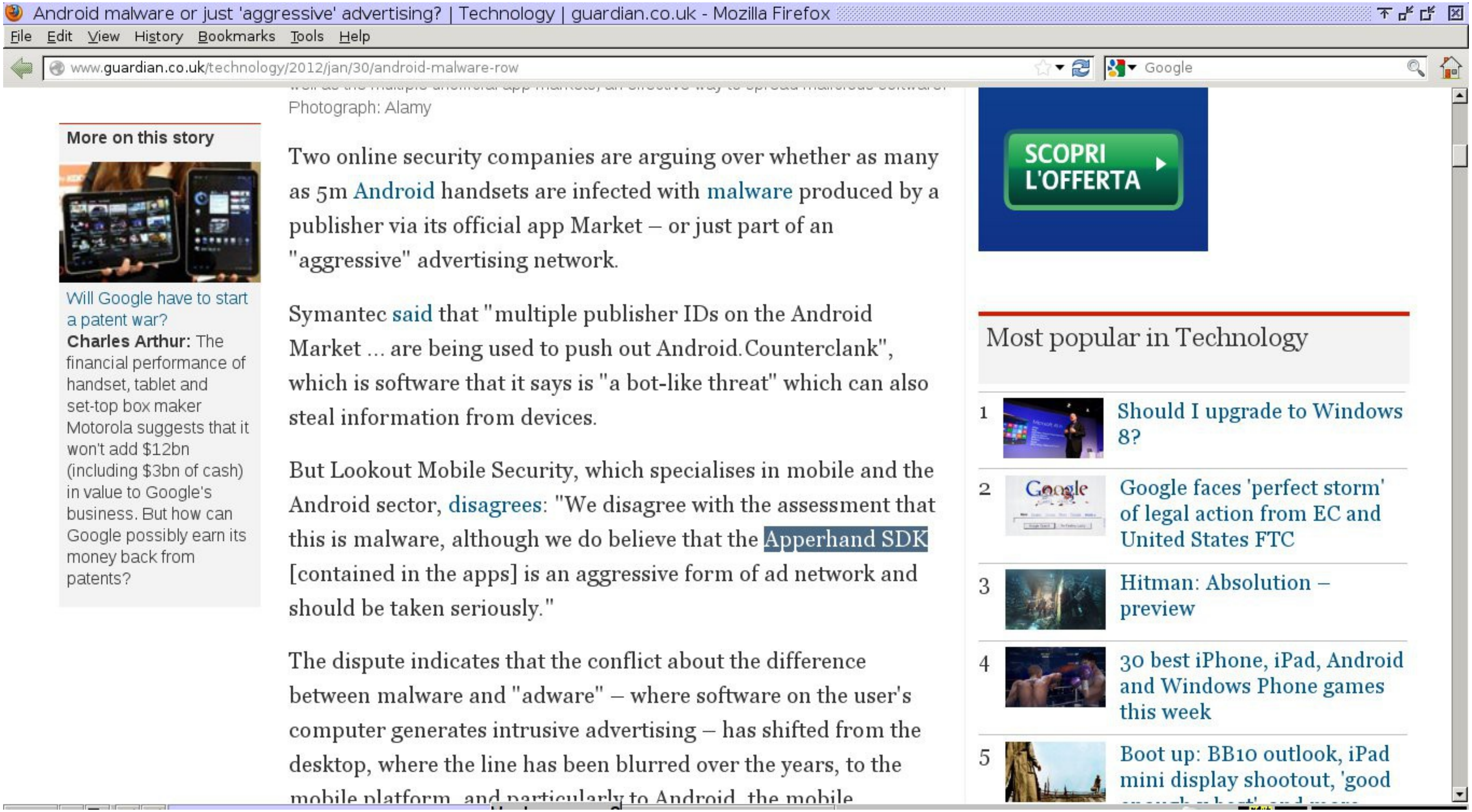

Burp Suite Professional v1.4.12 - licensed to Enforcer [single us
Burp Intruder Repeater Window About
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept Options History
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Request Response
Raw Headers Hex
< + >
Type a search term
0 matches

Request to http://www.apperhand.com:80 [217.65.36.4]

```
POST /ProtocolGW/protocol/commands HTTP/1.1
device-id: %2B1dVTHhsIu3gAlTxX%2F8fbhe7o9Y%3D
protocol-version: 1.0.17
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; it-it; Geeksphone ONE Build/GRI40; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1
Content-Type: application/json
Accept-Encoding: gzip
Accept: application/json
Content-Length: 849
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 206
Date: Fri, 16 Nov 2012 17:53:31 GMT

{"commands":[{"id":"ae51cdf0-473c-4e73-8057-6030cf0a1b22","parameters":{"Shortcuts":["searchmobileonline.com"]},"command":"INFO"}],"c
ommandsInterval":7200,"parameters":{},"abTest":null,"validResponse":true}
```

http://www.guardian.co.uk/technology/2012/jan/30/android-malware-row


Android malware or just 'aggressive' advertising? | Technology | guardian.co.uk - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.guardian.co.uk/technology/2012/jan/30/android-malware-row
Google

well as the multiple unofficial app markets, an effective way to spread malicious software.
Photograph: Alamy

Two online security companies are arguing over whether as many as 5m Android handsets are infected with malware produced by a publisher via its official app Market – or just part of an "aggressive" advertising network.

Symantec said that "multiple publisher IDs on the Android Market ... are being used to push out Android.Counterclank", which is software that it says is "a bot-like threat" which can also steal information from devices.

But Lookout Mobile Security, which specialises in mobile and the Android sector, disagrees: "We disagree with the assessment that this is malware, although we do believe that the Apperhand SDK [contained in the apps] is an aggressive form of ad network and should be taken seriously."

The dispute indicates that the conflict about the difference between malware and "adware" – where software on the user's computer generates intrusive advertising – has shifted from the desktop, where the line has been blurred over the years, to the mobile platform, and particularly to Android, the mobile

More on this story

Will Google have to start a patent war?
Charles Arthur: The financial performance of handset, tablet and set-top box maker Motorola suggests that it won't add $12bn (including $3bn of cash) in value to Google's business. But how can Google possibly earn its money back from patents?

Most popular in Technology

1 Should I upgrade to Windows 8?

2 Google faces 'perfect storm' of legal action from EC and United States FTC

3 Hitman: Absolution – preview

4 30 best iPhone, iPad, Android and Windows Phone games this week

5 Boot up: BB10 outlook, iPad mini display shootout, 'good

- diffusione e “geopardizzazione” (AUGH!)
- sorgenti (AOSP), docs, SDK, NDK, emulatore, ..
- .apk → decompilazione, reversing, debug
- aggiornamenti OS, app e market alternativi
- permessi delle applicazioni “delegati” agli utenti
- Linux Kernel, ~ Linux userspace e librerie (e bug)
- exploit mitigation techniques (fail) (< 2.3, < 4.0.3)
- OOB “covert” channel (umts/gprs, SMS, ..)
- territori poco explorati: OS/lib custom, hw driver

- **dati personali (posta, documenti, rubrica, calendario, ..)**
- **intercettazioni (audio, video, messaging, network, ..)**
- **geolocalizzazione (foto, social network, ..)**
- **credenziali (siti, posta, VPN, ..) → cloud storage**
- **HTML-like client side attacks**
- **EvilApp want to eat your soul.. Install? YES!!!**
- **BY0D (Bring Your 0wned Device)**
- **banking OTP ($$)**
- **NFC ($$)**

- **url e web-services “privati”**
- **business logic esposta (client-side)**
- **-> device -> credenziali -> back-end**
- **-> device -> storage -> back-end**
- **credenziali e certificati hard-coded (.apk)**
- **no/lazy input validation**
- **no/broken authentication & session management**
- **the good ole web security vulns**

Android e mobile security (for developers)

Igor Falcomatà

CTO, Enforcer
ifalcomata@enforcer.it

OWASP-Italy Day2012
Rome, 23° November 2012

Domande?

The OWASP Foundation
http://www.owasp.org

Webografia vedi: http://www.enforcer.it/dl/android_security_smau2012.pdf