

Who's watching your back?

Mobile Application Security Testing

Gursev Kalra
Dec 5, 2009

Agenda

- ▶ Introduction
- ▶ Browser Based Mobile Applications
- ▶ Installable Mobile Applications
- ▶ Intercepting Application Traffic
- ▶ Various Traffic Interception Schemes
- ▶ Mobile Traffic and SSL
- ▶ Conclusion

Introduction

- ▶ Who am I?
 - Senior Security Consultant – Foundstone Professional Services
 - Web Applications, Networks...

Introduction

► Mobile Applications

- Tremendous growth in consumer and business mobile applications
- Many new players
- Security aspects might get overlooked



Browser Based Mobile Applications

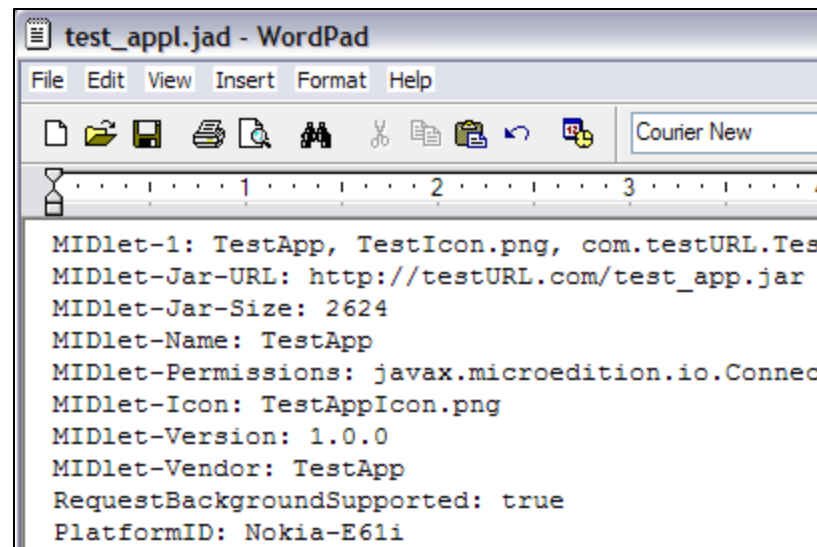
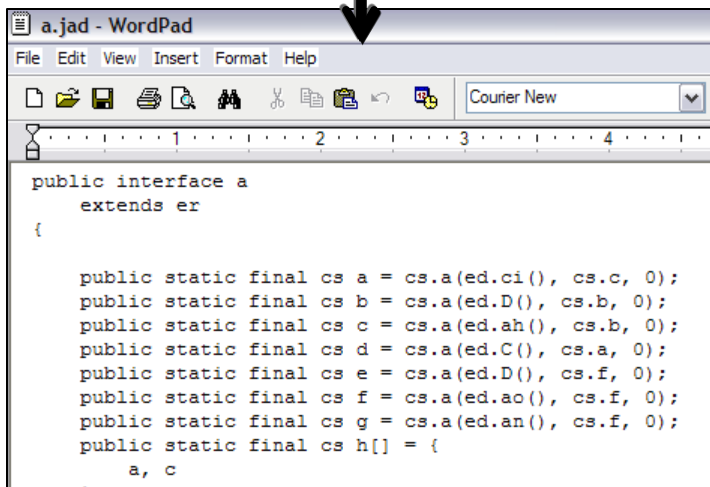
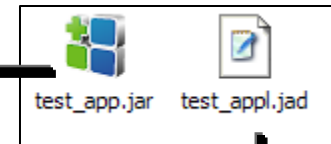
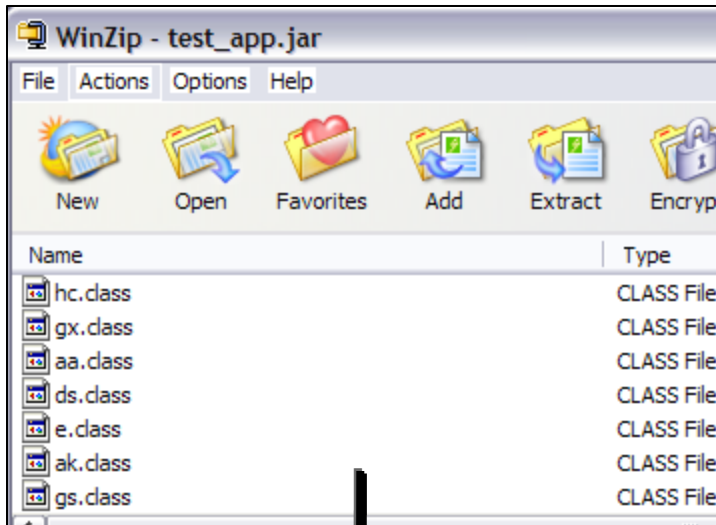
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-application/xaml+xml
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; rv:1.9.1.2pre) Gecko/20090302; .NET CLR 3.5.21022

Accept: text/html,application/xhtml+xml,application/xml;q=0.9;q=0.7,*/*;q=0.5
Accept-Charset: iso-8859-1;q=0.5;q=0.7,*/*;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en;q=1.0,en-us;q=0.5,ms;q=0.5
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-us) AppleWebKit/413 (KHTML, like Gecko) Safari/413 es611

Accept: text/html,application/xhtml+xml,application/xml;q=0.9;q=0.7,*/*;q=0.5
Accept-Charset: iso-8859-1;q=0.5;q=0.7,*/*;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en;q=1.0,en-us;q=0.5,ms;q=0.5
Cookie:
Cookie2:
User-Agent: Mozilla/5.0 (SymbianOS/9.3; U; Symbian; en-us) AppleWebKit/532.0 (KHTML, like Gecko) Safari/532.0

User-Agent: Mozilla/5.0 (Windows; U; windows NT 5.1; en-US; rv:1.8.1.20) Gecko/20080702 Firefox/1.9.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9;text/plain;q=0.8,image/jpeg,*/*;q=0.5

Installable Mobile Applications



Intercepting Application Traffic for Nokia S40 Series Phones

- Set up a custom web proxy and obtain its IP and port
- Edit the configuration WML and change proxy IP and port to the custom web proxy
- Compile WML to a provisioning (WBXML) file
- Transfer the new settings to S40 mobile phone
- Activate custom settings and access the Internet using new settings

Intercepting Application Traffic for Nokia S60 Series Phones

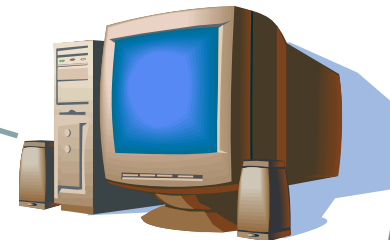
- Set up a custom web proxy and obtain its IP and port
- Create duplicate of existing Access Point settings
- For the copy created, change the proxy IP and port to the custom proxy
- Access Internet using custom proxy settings

Proxy With Public IP Address

- Phone with Application
- Access Point: Service provider default settings
- Proxy Server Address: W1.X2.Y3.Z4 (Public IP)
- Port Number: 8888



- Public IP: W1.X2.Y3.Z4
- Paros/Fiddler/Burp/Charles: Web Proxy running on port 8888



W1.X2.Y3.Z4

Proxy On WLAN

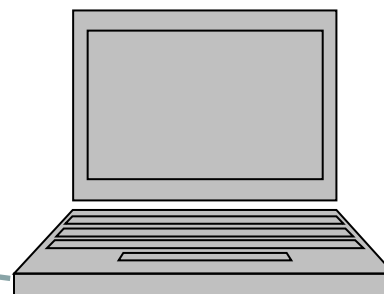
- Phone with Application
- WLAN Netw. Name: PenTest
- WLAN Mode: WPA2
- Proxy Server Address: 192.168.30.102
- Port Number: 8888



192.168.30.101

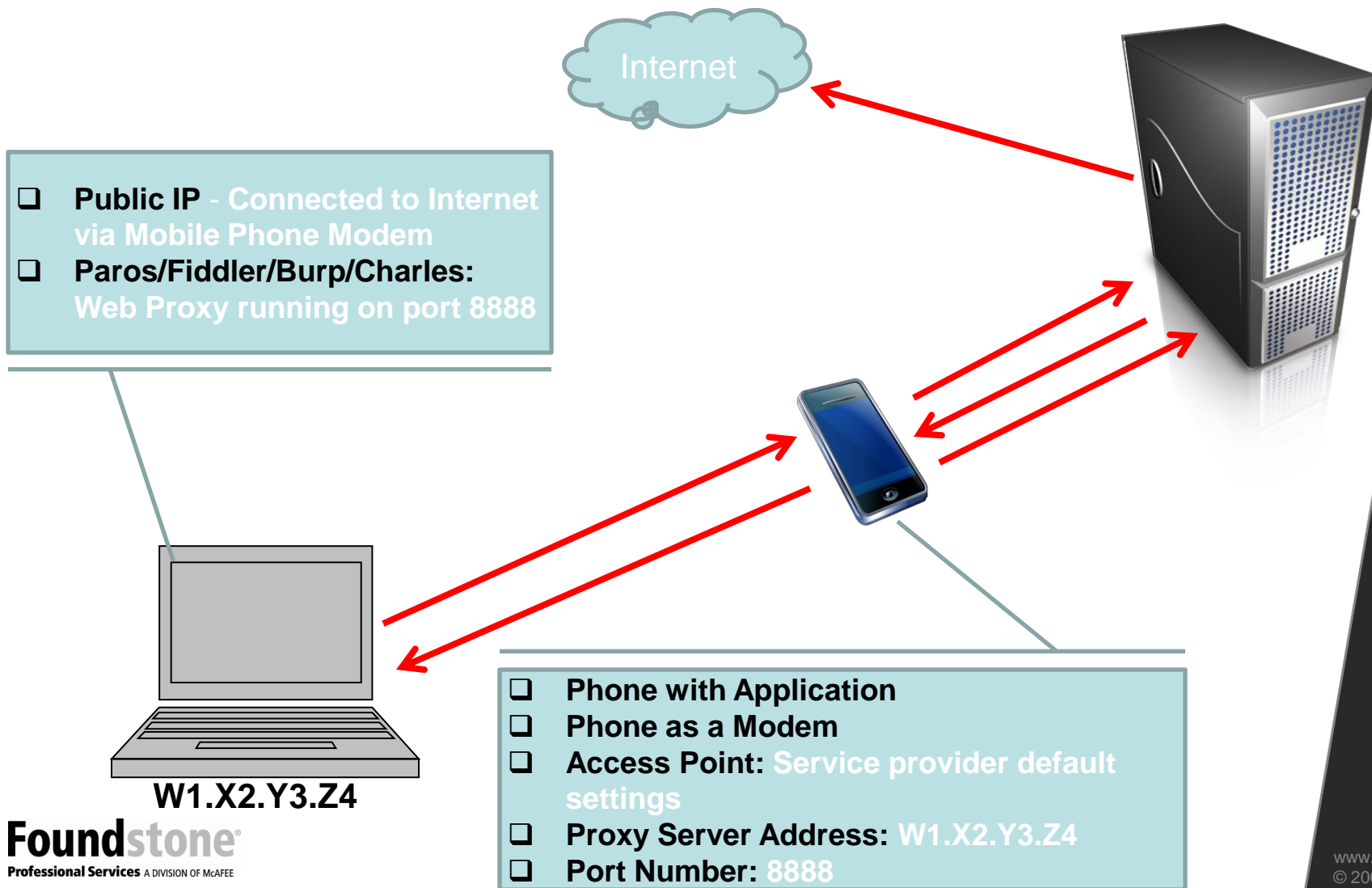


- Paros/Fiddler/Burp/Charles:
Web Proxy running on port
8888



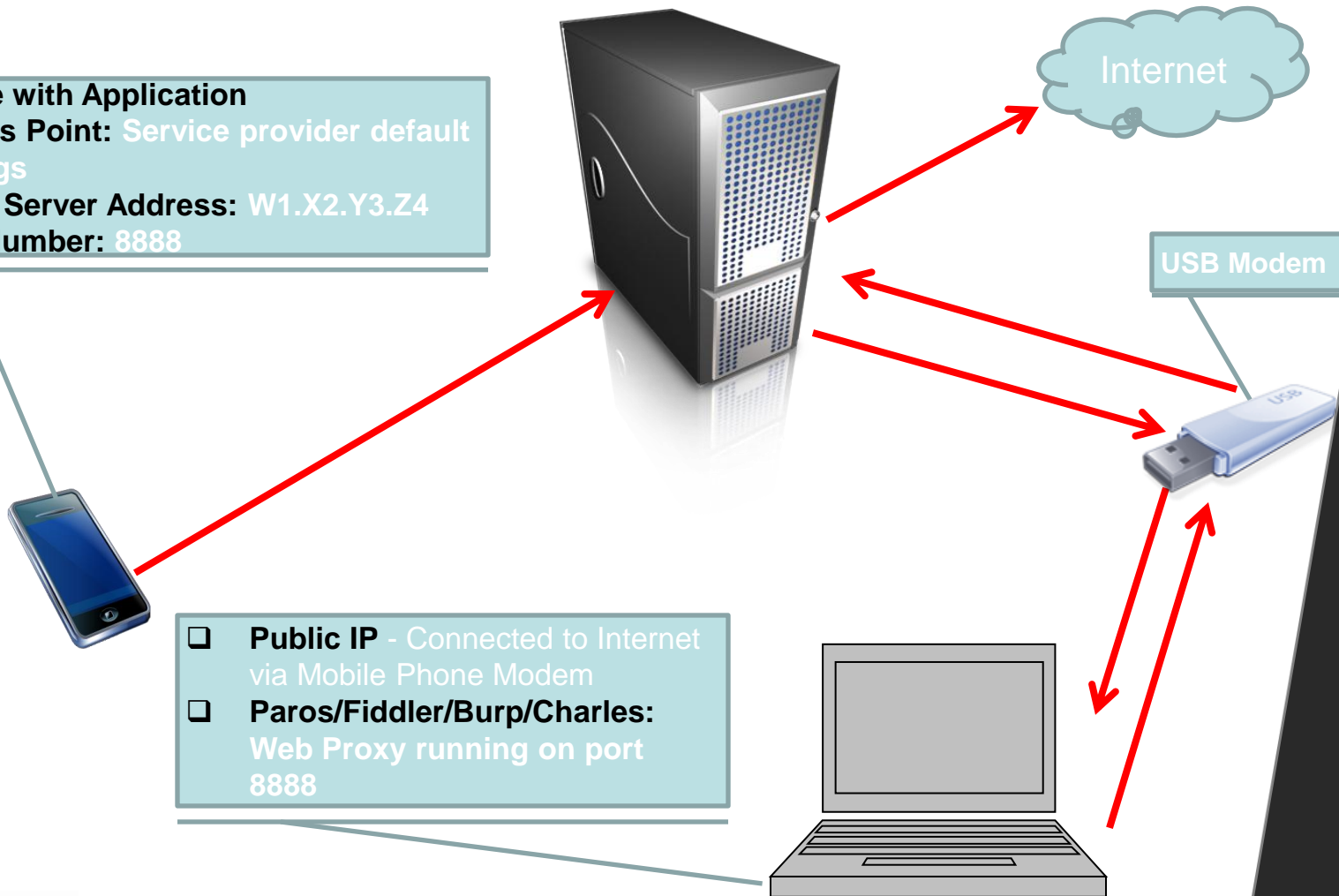
192.168.30.102

Proxy With One Phone



Proxy With External Internet Connection

- Phone with Application
- Access Point: Service provider default settings
- Proxy Server Address: W1.X2.Y3.Z4
- Port Number: 8888



- Public IP - Connected to Internet via Mobile Phone Modem
- Paros/Fiddler/Burp/Charles: Web Proxy running on port 8888

Mobile Traffic Interception and SSL

- Export your web proxy's certificate in DER format
- Copy the certificate file to a web server
- Set the MIME type of the directory to which the certificate is copied to `application/x-x509-ca-cert`
- Use the mobile web browser to browse to the certificate file
- Import the certificate when prompted
- Delete the un-trusted certificate after testing

Conclusion

- ▶ Mobile applications extend traditional network boundaries and introduce new avenues of attack
- ▶ They often have access to sensitive business and personal information
- ▶ They are constantly challenging and extending their reach
- ▶ **Security is critical and should be part of SDLC!!**





Thank You

Gursev Kalra
gursev(dot)kalra(at)foundstone(dot)com