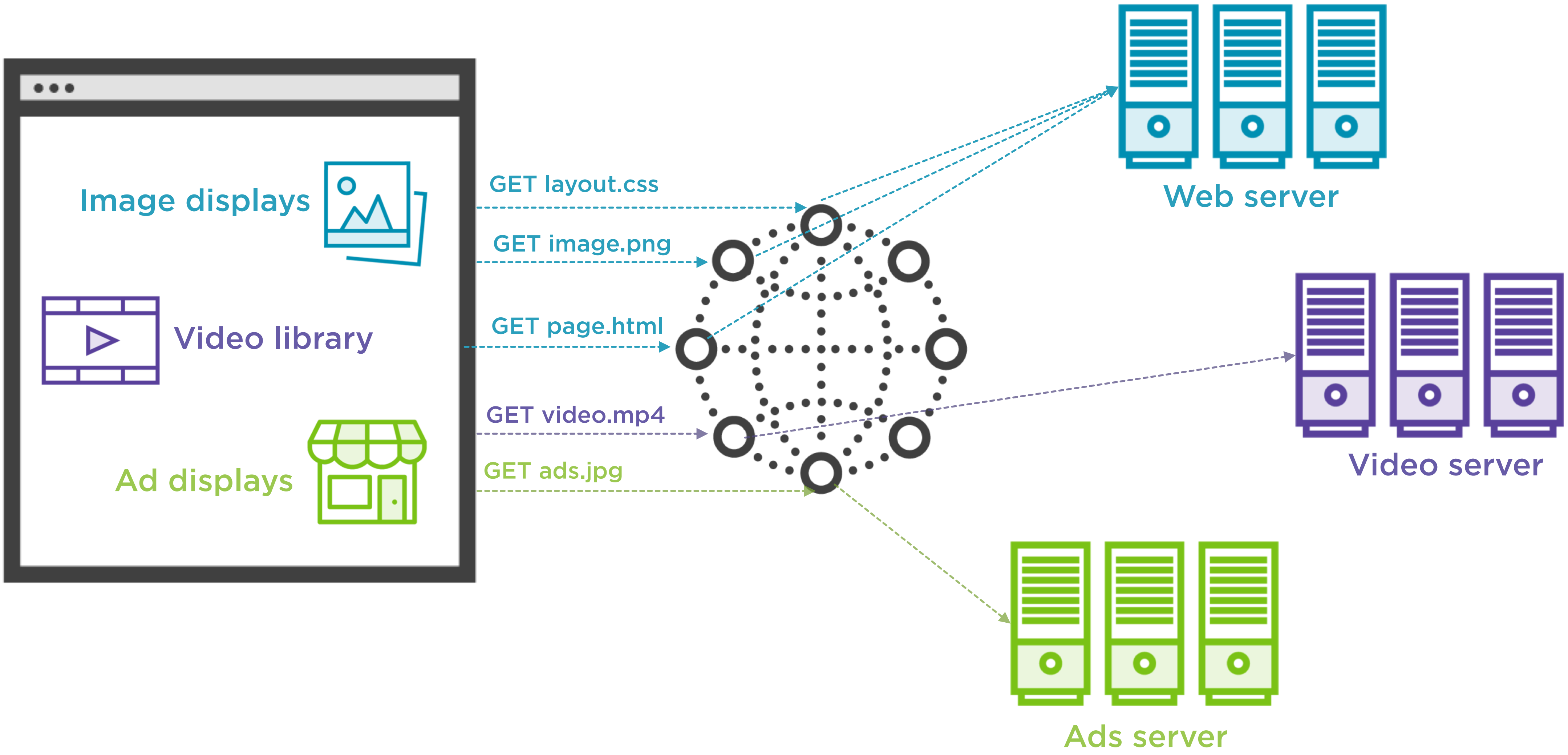
Securing network communication using network security configs

Nitin Singh
MOBILE DEVELOPER

Difference between HTTP and HTTPS Connections

How HTTP Communication Works



Security Risks When Using HTTP

Data passes through untrusted entities like proxy servers, routers

Data can be seen by any of these entities as it is sent in plain text over the network

Data can be modified before returning to the client by any of these entities

The Solution

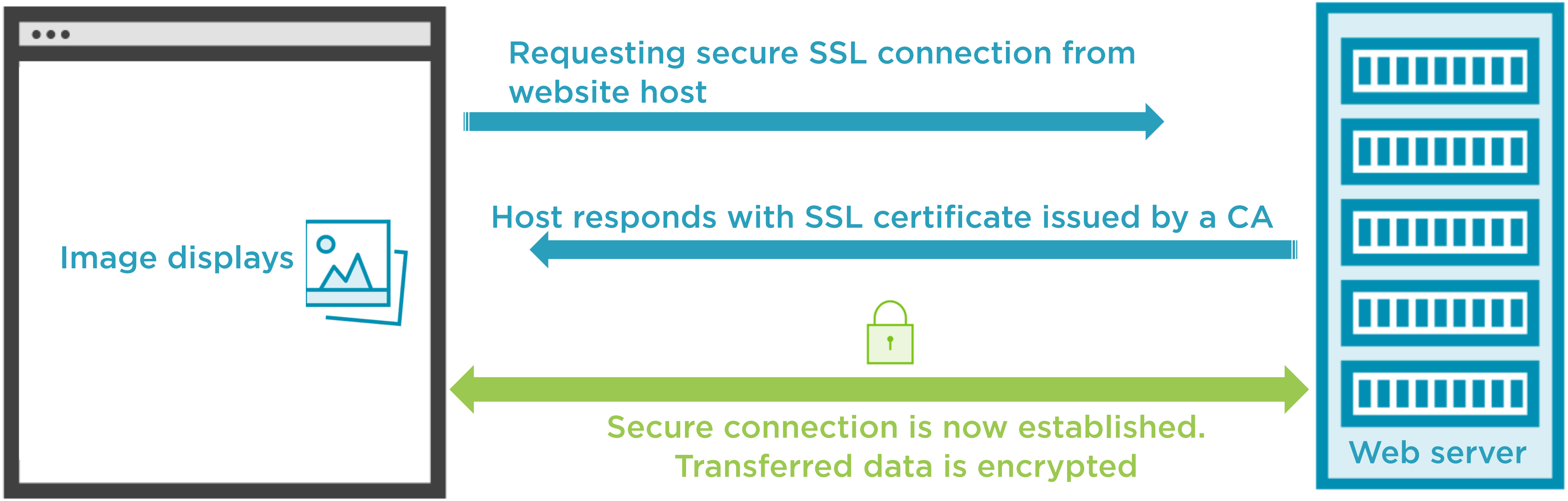
Use HTTPS requests instead of HTTP requests

HTTPS = HTTP + TLS

All data sent over network is encrypted

Integrity checks are done on data before accepting it

How HTTPS Communication Works



Requesting secure SSL connection from website host

Host responds with SSL certificate issued by a CA

Secure connection is now established. Transferred data is encrypted

How to Migrate to HTTPS in Your App

Ensure your web server has a TLS certificate issued by a well-known CA

Use ‘HttpsURLConnection’ instead of ‘HttpURLConnection’

Ensure all end-points used by the app have the https:// protocol

Starting with Android P all HTTP traffic is blocked by default.

Demo

Contact application

See how data sent using HTTP requests can easily be read by a proxy server

Migrate requests to HTTPS and examine if security issues are fixed

Network Security Configuration

The purpose of Network configs is to allow apps to modify their network security settings safely via a config file without modifying app code

Key Capabilities Supported by Network Configuration

1 Cleartext Traffic Optout

2 Debug-only Overrides

3 Custom Trust Anchors

4 Certificate Pinning

```
<manifest ... >
  <application android:networkSecurityConfig="@xml/network_security_config">
    ...
  </application>
</manifest>
```

How to Add a Network Configuration File

- **Specified in AndroidManifest.xml**
- **networkSecurityConfig attribute on <application> tag is used**

```
<network-security-config>
    <base-config>
        ...
    </base-config>


        <domain-config>
        ...
    </domain-config>


        <debug-overrides>
        ...
    </debug-overrides>
</network-security-config>
```

- ◂ Config applicable to all requests
- ◂ Config applicable to requests for a particular domain
- ◂ Config applicable when debuggable is true

‘network-security-config’ Tag

1 Always the root tag

2 Can have 0 or 1 <base-config>, <debug-overrides> tag

3 Can have multiple <domain-config> tags

‘base-config’ Tag

1 Values to be used for all requests except those overridden by <domain-tag>

2 Control cleartext traffic using cleartextTrafficPermitted attribute

3 Can contain 1 or more <trust-anchors> tags

‘domain-config’ Tag

1 Values to be used for domains specified by the <domain> sub-tags

2 Control cleartext traffic using cleartextTrafficPermitted attribute

3 In case of conflict between <domain-config> tags the closest match is used

```
<base-config cleartextTrafficPermitted="false">
    ...
</base-config>
```

Opt-out of Cleartext Traffic

Useful for apps targeting below API level 27 as the default is to allow cleartext traffic

Prevents accidentally allowing cleartext traffic due to URL changes by external systems like the server

‘domain’ Tag

1 Used as a sub-tag for <domain-config> to specify domains to apply the configuration to

2 <domain includeSubdomains=″true″>example.com</domain>

3 includeSubdomains attribute is used to indicate if subdomains of the domain specified should used same configuration

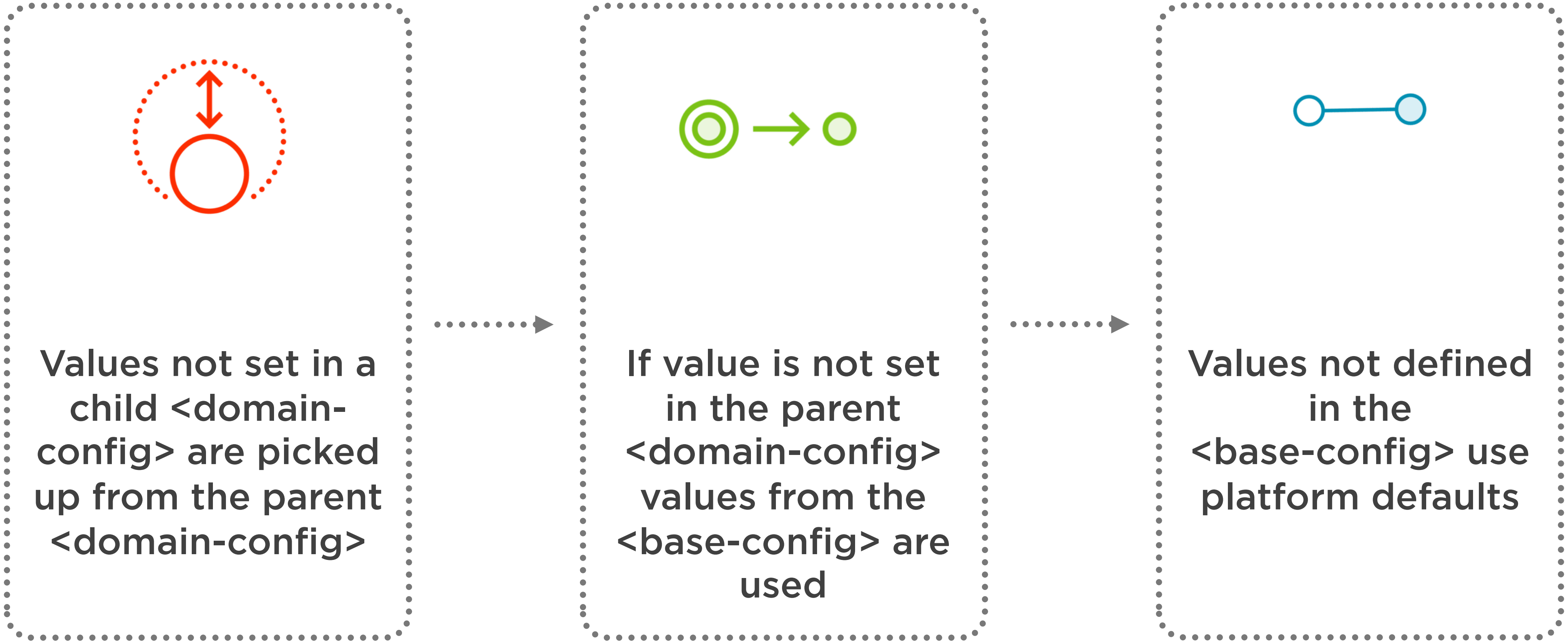
‘debug-overrides’ Tag

1 Used only when android:debuggable is true

2 Can have 1 or more <trust-anchors> tags

3 Avoids conditional code that can lead to app shipping with wrong set of trusted CAs or wrong network configuration

Configuration Inheritance Behavior



Values not set in a child <domain-config> are picked up from the parent <domain-config>

If value is not set in the parent <domain-config> values from the <base-config> are used

Values not defined in the <base-config> use platform defaults

Demo

Contact application

Setup network configuration such that cleartext traffic is allowed only for certain domains

Summary

How HTTP communication works

Security risks in HTTP requests

How HTTPS solves the security issues with HTTP

How to migrate your app to HTTPS

Key capabilities of Android’s network security configuration

Understanding how to create network configurations

The various tags involved in a network configuration and how they interact with each other

What’s next

Securing Network Communication Using Certificate Authorities and Certificate Pinning

Thank you