

TAMZ II

Android platform libraries

- System C
- Graphics
- Surface manager
- Audio manager

Android application framework

- Package
- Window
- View system
- Resource
- Activity
- Content

Art

- Replaced Davig since 5.0

Android bootup

- Boot ROM
- Bootloader - Memories, verification, security
- Kernel - Interrupt controllers, cahces and scheduling
- Init process - Mounts file system, launch processes

Application Internals

Types of apps

- Foreground
 - Visible on screen
- Background
 - Restricted since 8.0
- Widget & shortcuts
 - Entry points
- Multi-window & multi-resume
 - Active side by side (tablets, multiscreens)

App components

- Activity
 - Primary for user interaction
 - Presentation layer
 - Each activity start stops the previous and save in stack

- Responsible for saving its own state
- onCreate - Must have, calls when creating
- onPause - System calls when user leaves activity
- onStart, onResume, onRestart, onStop, onDestroy
- Service
 - Code running in background
 - Independent of any activity
- Content provider
 - Store and share data
 - Accessible by multiple apps
- Broadcast receiver
 - Responds to system-wide broadcast
 - Subscriber in publish/subscribe pattern (as observer)
- Widget
 - Visual components
 - Notifications

Navigation

- Task
 - Collection of activities
- Backstack
- Suspending & resuming activities

Priorities

- All apps remain running until the system needs memory
- Killing apps based on priority
- With same priority, kills process with longest lower priority history
- Active process
 - Foreground
- Visible process
 - Visible, not active
- Started service
 - Should continue without visible interface
- Background process
 - Without running service
- Empty process

On config change, Android kills Activity and restarts it. Automatically saves the state Views with UID

Intents

- Describing action (e.g. Send a message)
- Intent object - Bundle of information
- Passive data structure, holding abstract description of operation to be performed
- Operations, events

- Sends asy messages
 - Communicate between activities, components...
 - Explicit
 - Names the component
 - Implicit
 - Asks system to perform service without telling which class should do this service
 - Android tries to find Activity that matches, this is called **Intent resolution**
 - Based on the **Intent** and **Intent filters**
 - Intent filters specified in AndroidManifest.xml
 - Action
 - Data
 - Category
- ```

Intent inte = new Intent();
inte.setAction(Intent.ACTION_SEND);
inte.setType("plain/text");
startActivity(inte);

```

## Intents objects

- Name (opt)
- Action
  - String naming the action
- Data
  - Uri of data and MIME type
- Category
- Extras
  - Key-values pairs
- Flags

## App manifest

- Defines structure, Intent filters and permissions
- uses-sdk define min and max SDK
- uses-configuration specify supported devices
- uses-feature specify hardware features and min version of OpenGL
- supports-screens specify which screens you can and can't use
  - smallScreens
  - normalScreens
  - largeScreens
  - anyDensity
- You must include all activities
- **Launch methods**
  - standard - new Activity launched and added to backstack
  - singleTop - if Activity instance exists on top, Android routes to the instance instead of creating new
  - singleTask - new Activity is created in new task, if task already exists, routes to the task instead

- singleInstance - same as singleTask, except the Activity is always single and only member of its task

## Resources

- **Non-source** code entity
- Layout
- Strings
- Images
- Menus
- Animations
- Located in `/res`
- **R class** - automaticaly generated. Cotains references for each resource
- `package.resource_type.resource_name`
- Code: `R.string.hello`
- XML: `@string/hello`
- Default
  - Should be used regardless of config
- Alternative
  - Designed for specific config

## Assets

- To store **any** kind of data

## Basic UI

- View
  - any view have UID
- ViewGroup - View that holds other views

## Jetpack compose

- Composable functions
- Faster iteration
- Eliminates boilerplate (XML + findViewById)
- Easier testing
- @Composable - tells the compiler this is gonna be UI

## Callbacks

- onClick()
- onLongClick()
- onFocusChange()
- onKey()
- onTouch()
- ...

## States

- Local state - Hold by one composable
- Hoisted state - Moved into shared parent component

## Layout

- Container - Layout Manager
- Constrain
  - Created manually in code or XML
- Linear
  - Horizontally/Vertically
- Relative
  - Lays widgets based on relations
- Table
  - Grid base on specification
- ScrollView
- Nesting composable
  - Column, row, box, spacer...

## Fragments

- Behavior or a portion of UI
- Life cycle
  - Resumed - Visible
  - Paused - Another activity has focus
  - Stopped - Not visible
- States
  - onAttach
  - onCreate
  - onCreateView
  - onActivityCreated
  - onDestroyView
  - onDestroy
  - onDetach

## Menus

- Options
- Contextual
- Contextual action bar
- Popup menu

## Data storage

- Shared preferences
  - Stored in key-value pair
  - `getSharedPreferences()`

- `getPreferences()`
- `putString(), getBoolean()`...
- `.commit` to save
- Internal storage
  - Private storage on device memory
  - uses `FileOutputStream`
- External storage
  - Non-private for large datasets
- SQLite
- Network connection
- Content provider

## Transactions

- ACID
  - Atomicity - Performed all or nothing
  - Consistency - When completed, data must be consistent
  - Isolation - Modifications must be isolated between transactions
  - Durability - After completion, effects are permanently in place. Persists even with sysfail

## Game development

- Delta time - Time since the last frame update
- Game loop - Root of the game graph. Children get called once per frame
- Android game development kit
  - C/C++ core, performance tuning, high-performance audio
- Android game development extension
  - For VS Code development
- Android GPU Inspector
  - Graphic tool, tracking and analysis of individual frames

## Inputs

- Polling
  - `while(!button.pressed){}`
- Event-based handling
  - `button.setOnClickListener(){}`
- Events
  - Touch down / drag / up
  - Key down / up
  - Accelerometer

## Rendering

- 2D
  - Canvas (CPU)
  - SurfaceView (CPU)
  - OpenGL/Vulkan (GPU)

- Jetpack Compose (GPU)
- 3D
  - OpenGL/Vulcan (GPU)
- onDraw() - Calls drawing
- invalidate() - Calls redraw

## Image

| PNG                             | JPG                      |
|---------------------------------|--------------------------|
| Dosent loose data at compresion | Loose data at compresion |
| Compresion ration ~2.7:1        | Compresion ration 10:1   |
| Higer size                      | Lower size               |

- WebP
  - Better. lower size, loosless compresion

## Android 2D Graphics

- Drawable
  - `android.graphics.drawable`
    - ShapeDrawable
    - BitmapDrawable
    - PictureDrawable
    - LayerDrawable
    - NinePatchDrawable
      - Stretchable bitmap
      - PNG that includes extra 1-pixel-wide border
      - Extension .9.png
  - `android.view.animation`

## Audio & Video

- Built-in encoderrs/decoders
- Core media formats

## Network connectivity

- Data sync
- Fetching resources
- Real-time updates
- Multi-device, peer sharing
- Cloud

## Types

- Network

- Bluetooth
  - NFC (Near field communication)
  - USB
- 

- Must set permissions
  - <uses-permission android:name="android.permission.INTERNET" />
  - <uses-permission android:name="android.permission.ACCESS\_NETWORK\_STATE" />
- **Network reachability ≠ Actual internet access**
- Connectivity Manager
  - Gives state of network
  - Notify changes
- Network info
  - Describe network interface status

## Sockets

- `Socket client = new Socket("hostname", portNumber);`
- **UDP**
  - Packet for real time streaming
  - Doesn't matter if damaged packet could be corrected or retransmitted
  - Connectionless
- **STUN**
  - Internet standards-track suite of methods
  - Used in NAT Traversal
  - Allows operation through NAT (Network address translator)

## HTTP & REST APIs

- HTTP methods
  - GET, POST, PUT, DELETE, PATCH
  - Request / Response -> Status codes (2xx, 4xx, 5xx)
  - Headers, query parameters, path parameters, body (JSON, XML, binary)

## Asy patterns

- *Bad*

## Http clients

- OkHttp
  - Connection pooling, transparent GZIP compression, HTTP/2 multiplexing.
- Retrofit
  - Defines connection as interface
  - Generate implementation
- Ktor client
  - Multiplatform
- Volley

- Automatic scheduling of network requests
- Multiple concurrent network connections

## APIs Patterns

- REST API
- WebSocket
  - Persistent full-duplex communication over single TCP
- Server sent event (SSE)
  - One way channel: server -> client
- GraphQL
- gRPC
  - Uses protocol buffers

## BaaS (Backend as a Service)

- Firebase
  - Google
- AWS
  - Amazon Web Service
- Supabase
- Google cloud

## Data conversion

- Big Endian
  - >ARMv3
  - More natural
- Little Endian
  - <ARMv3, x86
  - Easier to place values

## Security

- Use TLS / HTTPS, avoid clear-text
- Validate certificates
- Auth tokens (JWT, OAuth2)
- Dont leak data *duh*

## Connectivity

### USB

- UsbManager
  - Entry point for managing
- UsbDevice
  - Represent USB device
- UsbInterface

- Functional group within device (e.g. printer interface)
- UsbEndpoint
  - Communication port (IN/OUT)
- UsbDeviceConnection
  - Channel with transfers
    - Control
    - Bulk
    - Interrupt
    - Isochronous

## WiFi

- Throttling
  - Each foreground app can scan four times in 2 minutes
  - All background apps combined can scan once per 30 minutes
- Wifi direct
  - Connection between device via wifi without the need for access point

## Bluetooth (Modrý zub 🌐)

| Class | Range |
|-------|-------|
| 1     | 100m  |
| 2     | 10m   |
| 3     | 1m    |

- Permissions
  - BLUETOOTH - To connect
  - BLUETOOTH\_ADMIN - To discover and pair
- BLE (Bluetooth Low Energy)
  - Short data bursts
  - Low energy footprint
  - For smartwatches, fit trackers, medical devices
  - GATT Client - Android app
  - GATT Server - Device, peripheral

## Printing protocols

- ESC/POS
  - For small thermal receipt printers
  - Series of ESCs for text, QR codes...
- ZPL/CPCL (Zebra)
  - mobile label printers
- PCL/PostScript
  - Common office printers
- IPP/LPR/Raw (port 9100)
  - Network protocols

# Barcodes, NFC, RFID

## AIDC (Automatic Identification and Data Capture)

- Barcode / QR code
  - UPC, EAN, Code39
  - QR up to 2953 bytes or 7089 numeric
- RFID (Radio-Frequency identification)
- NFC (Near field communication)
  - Subset of RFID
  - NDEF Message
  - 1 to many Records
  - HCE (Host card emulation) - Emulating contactless pay card
    - NFC Application Protocol Data Unit (APDU)

# Locations and Sensors

## **GPS ≠ GNSS**

- GNSS - Global navigation satellite system
  - Global umbrella term
  - GPS - U.S. Global positioning system
  - Galileo
  - GLONASS
  - BeiDou
  - QZSS
- Multi-constellation GNSS since API 24+
  - Availability
  - Accuracy
  - Time To First Fix

## Augmentation and Correction Systems

- SBAS (Satellite base augmentation system)
- RTK (Real time kinematic)
  - GPS correction
  - Centimeters accuracy
  - Used in drones, autonomous driving
- PPP (Precise point positioning)

## Location

- Fused location provider
  - Google location API
  - Permissions
    - ACCESS\_COARSE\_LOCATION
    - ACCESS\_FINE\_LOCATION
    - ACCESS\_BACKGROUND\_LOCATION

- GPS Module
  - Uses trilateration
- WiFi Module
- Combine with BLE or UWB (Ultra wide modulation)
- Sensors
  - `Android.hardware`
  - Motion, environmental, position
  - Continuous, on-change, one-shot
  - Accelerometer, gyroscope, camera, microphone...
- Update Interval
  - `setInterval()`
  - `setPriority`
    - PRIORITY\_BALANCED\_POWER\_ACCURACY
    - PRIORITY\_HIGH\_ACCURACY
    - PRIORITY\_LOW\_POWER
    - PRIORITY\_NO\_POWER

## Activity

- Activity Recognition API
  - Detects walking, running, still, in-vehicle, cycling
  - Low power
- Awareness API
  - Combines location, time, headphones, weather, activity
  - Contextual triggers -> `when outdoor then tracker`

## Maps

- Google maps
  - Jetpack Compose Maps SDK
- Alternatives
  - Mapbox
  - OSM Droid
  - MapTiler SDK
- WMS (Web map service)
  - Server returns raster or vectors
  - Response -> Rendered map image (PNG/JPEG)

## Sensor hub --- THE Hub

\*wink\*

- Cluster of connected sensor chips

## Cryptography

- Study of mathematical techniques related to aspects of information security ☺

## Goals

- Confidentiality - Only intended recipient can read the data
- Data integrity - Data cannot be modified without detection
- Authentication - Verifying the identity of the user or server
- Availability - Accessible when needed
- Non-repudiation - A sender cannot deny having sent a message
- Forward secrecy - Past comms stay confidential even if future keys are compromised

## Evaluation criteria

- Level of security
- Functionality
- Methods of operation
- Performance
- Ease of implementation

## Terms

- Plaintext - Message in natural format
- Ciphertext - Message altered to be unreadable by anyone except recipients
- Key - Sequence that controls the operation and behavior of algorithm
- Keyspace - Total number of possible values of keys in crypto algorithm
- Cryptosystem - Algorithm, key and functions

## Implementation

- `javax.crypto`
  - Classes and interfaces
  - Cipher - Class used to encrypt and decrypt data
    - Provider based
    - Static factory method `getInstance()`
    - Argument is three part name of desired encryption. e.g. "`DES/CBC/PKCS5Padding`"
  - KeyMint - Standardized HAL for key operations, os-level storage description
- Key agreement
  - Each party calls `init()` and supplies Key object
  - After Key exchange, calls `doPhase()`
  - `doPhase()` returns intermediate Key object, and these keys are passed into `doPhase()` again
  - After that, each party calls `generateSecret()`, that returns SecretKey object for the named algorithm
  - Key material remains **non-exportable**
  - If device support TEE (trusted execution environment), key material is there

## Hardware security

- TEE (Trusted Execution Environment)
  - Stores private keys
  - Resistant to rooting, tampering

- Code isolated from OS
- StrongBox security chip
  - Separated hardware
  - Pixel and high-end Samsungs
- Titan M / M2
  - Secure boot, key attestation
  - Verified boot enforcement

## Symmetric & Asymmetric Algorithms

- **Symmetric**
  - One key
  - Cipher and decipher
  - Stream cipher
    - Encrypt single digits
  - Block cipher
    - Encrypt blocks of data
  - Serpent, Twofish, AES, Blowfish, CAST5
  - Ceasar cipher
    - Replacing each letter with one, three places further
  - Kama-sutra cipher, Pigpen cipher, Playfair cipher, Rail fence cipher
- **Asymmetric**
  - Two keys
    - Private key
      - Known only by one person/device
    - Public key
      - Known publicly
    - Diffie-Hellman Key Exchange, ElGamal, elliptic curves
- **Hybrid**
  - Asymmetric distributes symmetric key (known as session key)
  - Symmetric provides bulk encryption
- Modern use
  - Symmetric
    - AES-GCM
    - ChaCha20-Poly1305
  - Asymmetric
    - X25519
    - Ed25519
    - RSA-2048
  - Hashing
    - SHA-256/512
    - PBKDF2
    - bcrypt

## TEA (Tiny Encryption Algorithm)

- *Bad*

- 64-bit blocks
- 128-bit key

## AES (Advanced Encryption Standard)

- *Good*
- 128-bit blocks
- 128,192 ,256-bit keys
- 10, 12, 14 rounds
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey

## Modes & Paddings

- **Modes** - Describe how to repeatedly apply cipher
- **Padding** - Block ciphers works on fixed size, so it *fills* the block if message is short

## Modes of operations

- ECB (Electronic codeblock)
- CBC (Cipher block chaining)
- GCM (Galois/Counter mode)

## DES (Data encryption standard)

- *Bad*
- 56-bit key
- 64-bit blocks
- Unsecure

## FBE (File Based encryption)

- Splits storage into
    - Device encrypted storage
      - Accesible before unlock
      - Alarm, messages (on locked screen)
    - Credential encrypted storage
      - After unlock
      - Bound to user Pin/Biometrics...
- 
- For random use `SecureRandom().nextBytes(bytes)`

## Reverse engineering protection

- **APK** - Instalable package
- **AAB** - Android app bundle

- Base APK - Functionality
- Configuration APK - Config based on size, language...
- Dynamic Feature APK - Opt modules
- Developer send AAB -> Google play generate APK for users
  - Harder to obtain original code from GPlay

## Smali

- Assembly language for Dalvik VM
  - Register-based VM
- baksmali - disassembler

## Jadx

- High-quality java & kotlin decompiler
- Integrated smali
- Cross-references
- "Show used resources" view

- 
- Many apps move logic to C/C++ -> harder to reverse
  - Heap dump - Snapshot of all the objects in memory
  - Code protectors
    - Packers, optimizers, protectors
    - Proguard, Dexguard, Allatori

## Monetization

### Google play

- \$25 USD registration fee
- Živnostenský list 1000,- Kč
- VAT Registration free
- Developer program standard
  - 15% service fee >\$1M
  - 30% service fee <\$1M
- Subscriptions
  - 15% from day one
- Media experience program
  - Video, music, books
  - Fees as low as 10%
- EU DMS (Digital Market Acts)
  - Fee reduction to 12%/27%

### Five Ps

- Product
- Price

- Place
- Promotion
- People

## Pay models

- In-app purchases
- Subscriptions
- Advertising
- Hybrid monetization
- Paid apps
- Licensing technology
- Ai-powered add-ons
  - Credit based usage
- B2B & SaaS mobile clients

## Metrics

- LTV - Lifetime value
- ARPU - Average revenue per user
- ARPPU - Average revenue per paying user
- Churn rate - % of users who stopped using the app

## Advertising based revenue

- Banner ads
- Interstitial ads
  - Deliver ad at the end of the flow (e.g. level completion)
- Native ads
  - Integratet seamlessly into app (e.g. instagram feed ad)
- Affiliate ads
  - Advertising product/app/service through my app
- Reward ads
  - Watch ad for extra life

## Freemium

- Basic functionality for free
- Charge for additional feature
- (e.g McAfee: Basic functionality like downloading viruses free. Actually blocking viruses behind paywall)

## In-app purchasing

- Models
  - One time purchase
  - Micro transactions
  - Subscriptions
  - Shopping other products

## Data monetization

- Selling user data
- Heavily restricted

## Android piracy

- **Lucky patcher mentioned** ❤
- Server-side validation
- Dynamic assets delivery