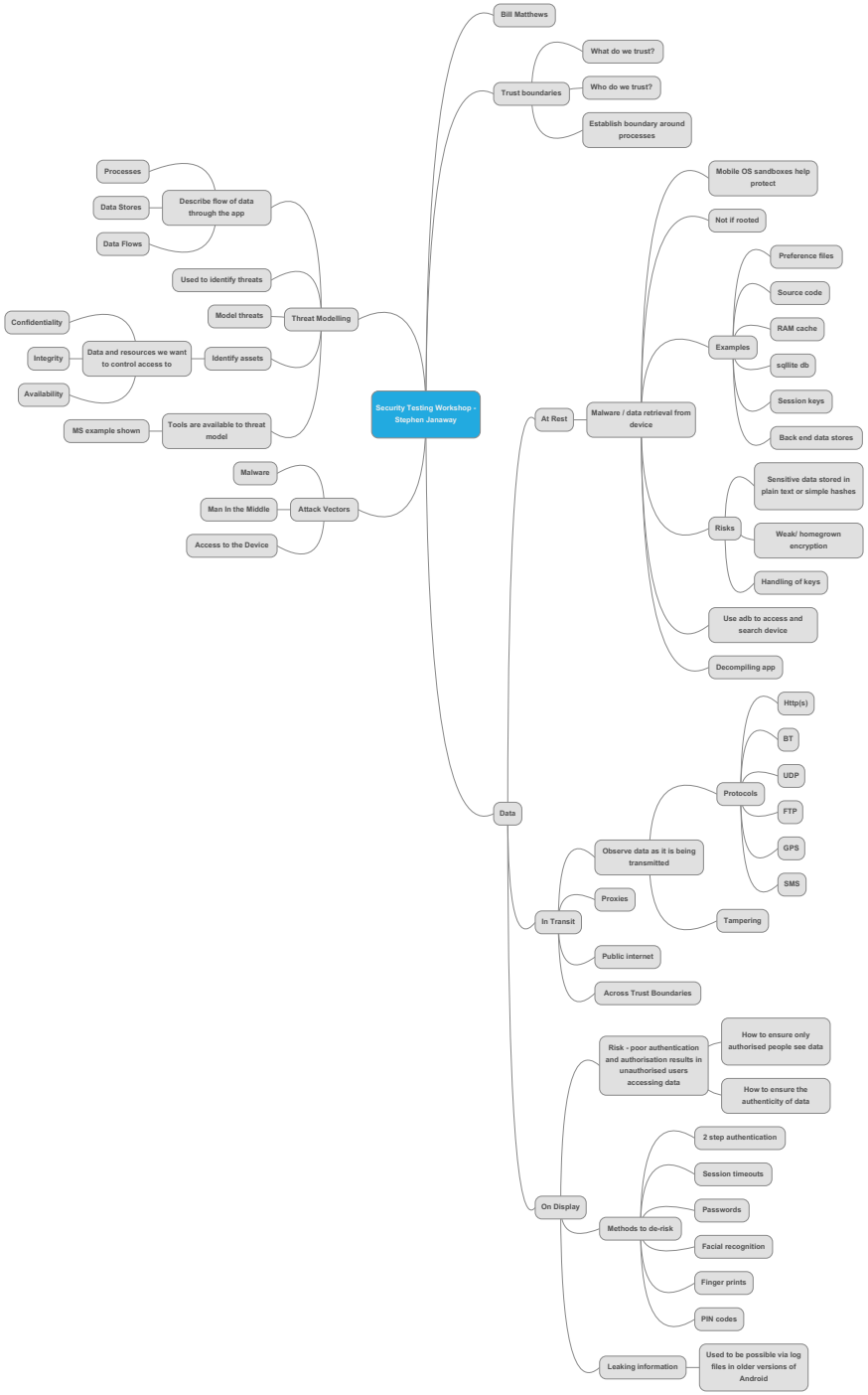
Security Testing Workshop - Stephen Janaway
Bill Matthews
Trust boundaries
What do we trust?
Who do we trust?
Establish boundary around processes
Threat Modelling
Describe flow of data through the app
Processes
Data Stores
Data Flows
Used to identify threats
Model threats
Identify assets
Data and resources we want to control access to
Confidentiality
Integrity
Availability
Tools are available to threat model
MS example shown
Attack Vectors
Malware
Man In the Middle
Access to the Device
Data
At Rest
Malware / data retrieval from device
Mobile OS sandboxes help protect
Not if rooted
Examples
Preference files
Source code
RAM cache
sqllite db
Session keys
Back end data stores
Risks
Sensitive data stored in plain text or simple hashes
Weak/ homegrown encryption
Handling of keys
Use adb to access and search device
Decompiling app
In Transit
Observe data as it is being transmitted
Protocols
Http(s)
BT
UDP
FTP
GPS
SMS
Tampering
Proxies
Public internet
Across Trust Boundaries
On Display
Risk - poor authentication and authorisation results in unauthorised users accessing data
How to ensure only authorised people see data
How to ensure the authenticity of data
Methods to de-risk
2 step authentication
Session timeouts
Passwords
Facial recognition
Finger prints
PIN codes
Leaking information
Used to be possible via log files in older versions of Android