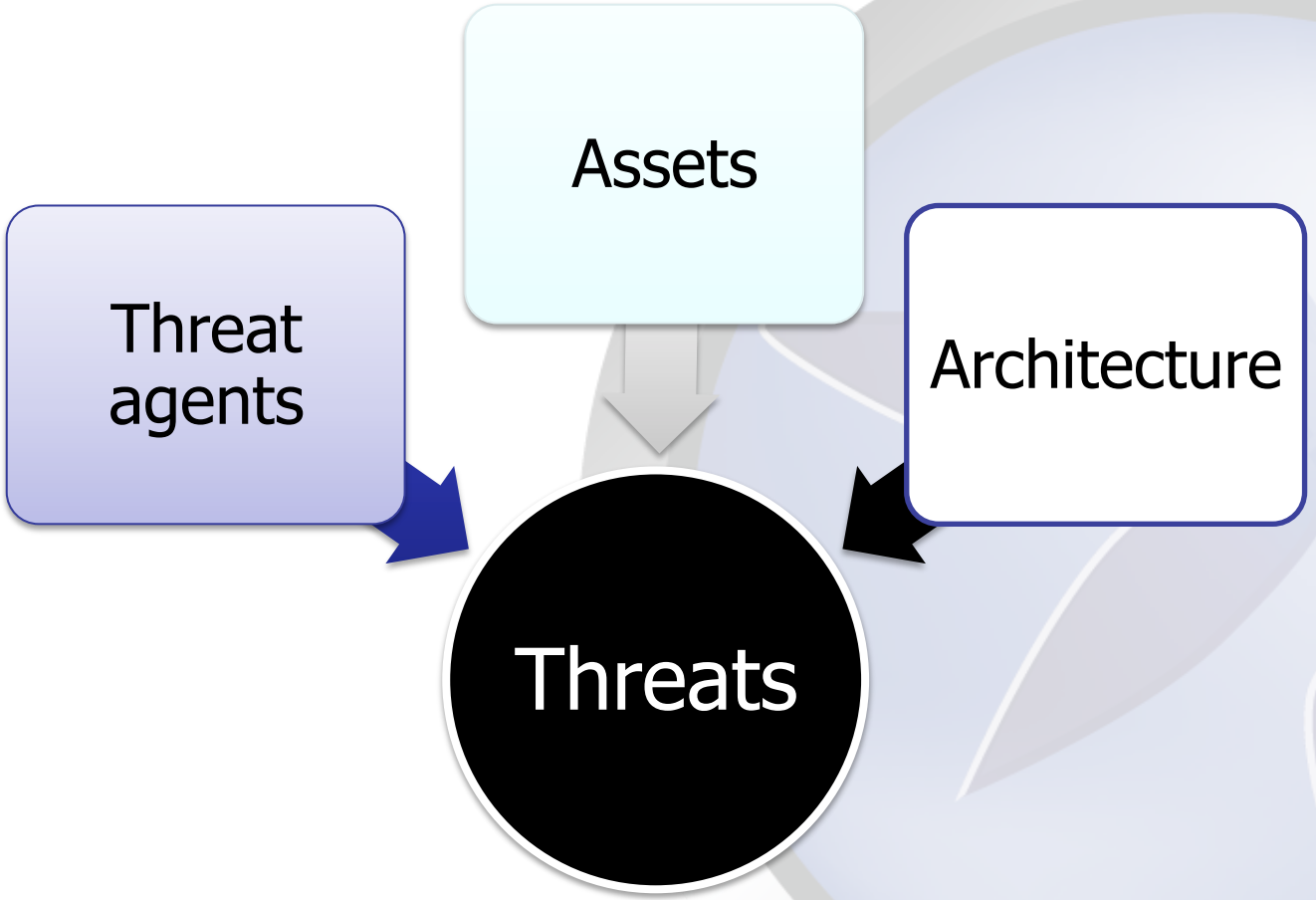
Mobile Application Threat Analysis

Ari Kesäniemi
Nixu

Threat Modeling



Thought Process for Discovering Threats

1. “What do we want to protect and why?”
2. “Where could the attack happen?”
3. “What could go wrong?”
4. “Do we have appropriate protection?”
5. “What is the risk we accept?”

1. “What do we want to protect and why?”

- What are the *assets* worth protecting?
- What would be the business impact if compromised?

- Data
- Money, privacy, credentials
- Transactions and processes
- IPR, innovations, algorithms
- Reputation, customer experience
- Resources

Thought Process for Discovering Threats

1. “What do we want to protect and why?”
2. “Where could the attack happen?”
3. “What could go wrong?”
4. “Do we have appropriate protection?”
5. “What is the risk we accept?”

2. “Where could the attack happen?”

- What is the *attack surface?*

- Local storage? (Including logs, caches etc)
- Connection to back end server?
- Connection to third party services?
- Malicious user?
- Web browsing and content handlers?
- Exposed API or RPC?
- Third party components part of the application?

Thought Process for Discovering Threats

1. "What do we want to protect and why?"
2. "Where could the attack happen?"
3. "What could go wrong?"
4. "Do we have appropriate protection?"
5. "What is the risk we accept?"

3. “What could go wrong?”

- What are the most feasible attack scenarios?

- How each of the assets (from step 1) could be compromised
  - Considering confidentiality, integrity, availability and non-repudiation for information assets?
  - Considering STRIDE* for processes and data flows?
  - Considering attack surfaces (from step 2)?
  - Considering the system as a whole?

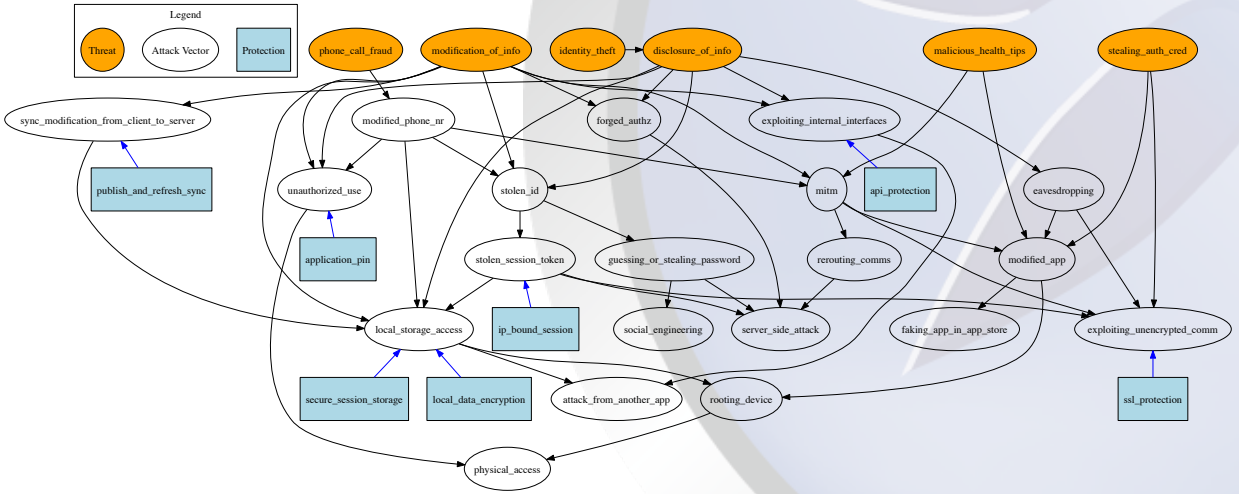
* STRIDE = **S**poofing / **T**ampering / **R**epudiation / **I**nformation disclosure / **D**enial of service / **E**levation of privilege

Thought Process for Discovering Threats

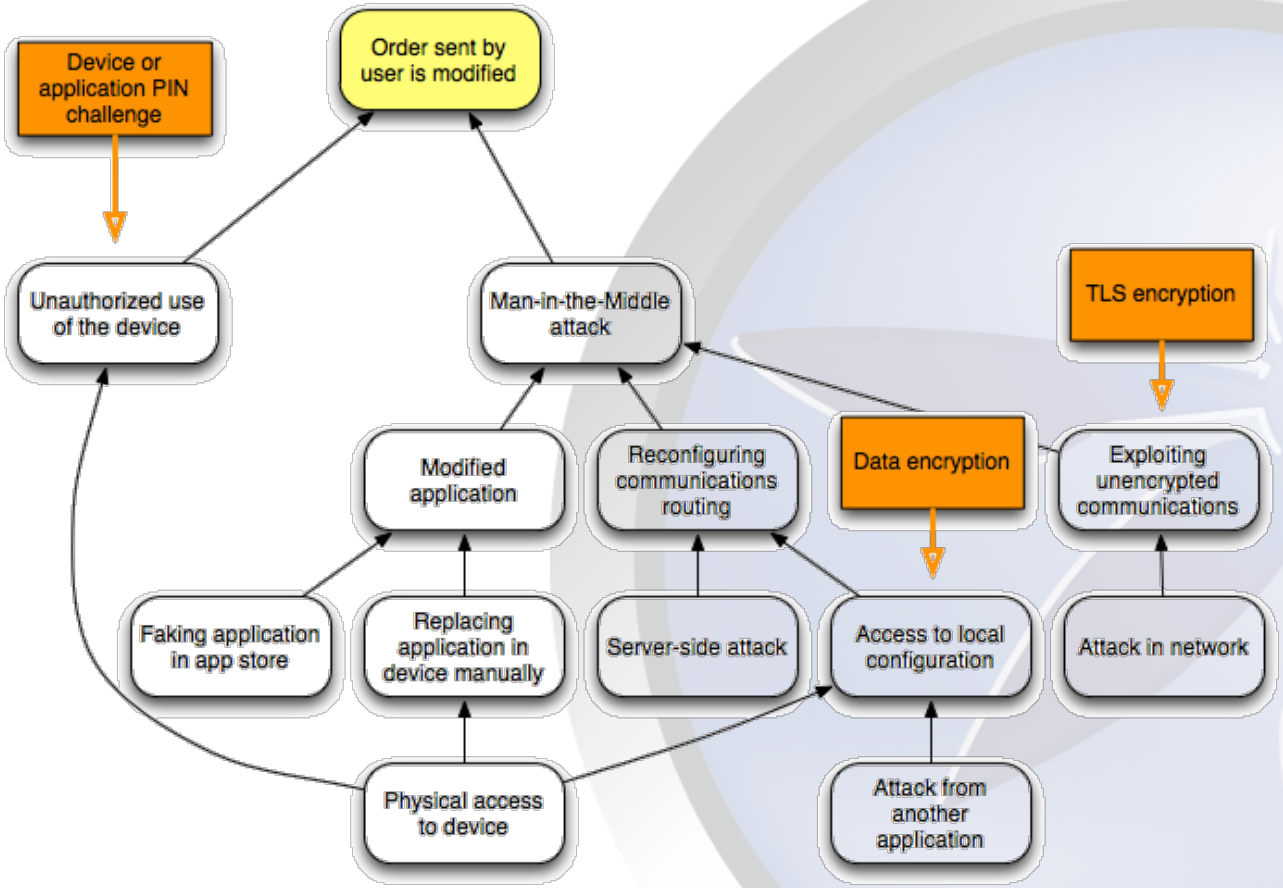
1. "What do we want to protect and why?"
2. "Where could the attack happen?"
3. "What could go wrong?"
4. "Do we have appropriate protection?"
5. "What is the risk we accept?"

4. “Do we have appropriate protection?”

- Consider each scenario individually
- Is there a best practice protection mechanism? Is it implemented in the system?
- Build an attack tree when necessary



Attack Tree


Device or application PIN challenge
Order sent by user is modified
Unauthorized use of the device
Man-in-the-Middle attack
TLS encryption
Modified application
Reconfiguring communications routing
Data encryption
Exploiting unencrypted communications
Faking application in app store
Replacing application in device manually
Server-side attack
Access to local configuration
Attack in network
Physical access to device
Attack from another application

OWASP Top Ten Mobile Risks (DRAFT)

1. Insecure or unnecessary client-side data storage
2. Lack of data protection in transit
3. Personal data leakage
4. Failure to protect resources with strong authentication
5. Failure to implement least privilege authorization policy
6. Client-side injection
7. Client-side DOS
8. Malicious third-party code
9. Client-side buffer overflow
10. Failure to apply server-side controls

… and:

- Abuse of client side paid resources
- Failure to properly handle inbound SMS messages
- Failure to properly handle outbound SMS messages
- Malicious / fake applications from app store
- Ability of one application to view data or communicate with other applications
- Switching networks during a transaction
- Failure to protect sensitive data at rest
- Failure to disable insecure platform features in application (caching of keystrokes, screen data)

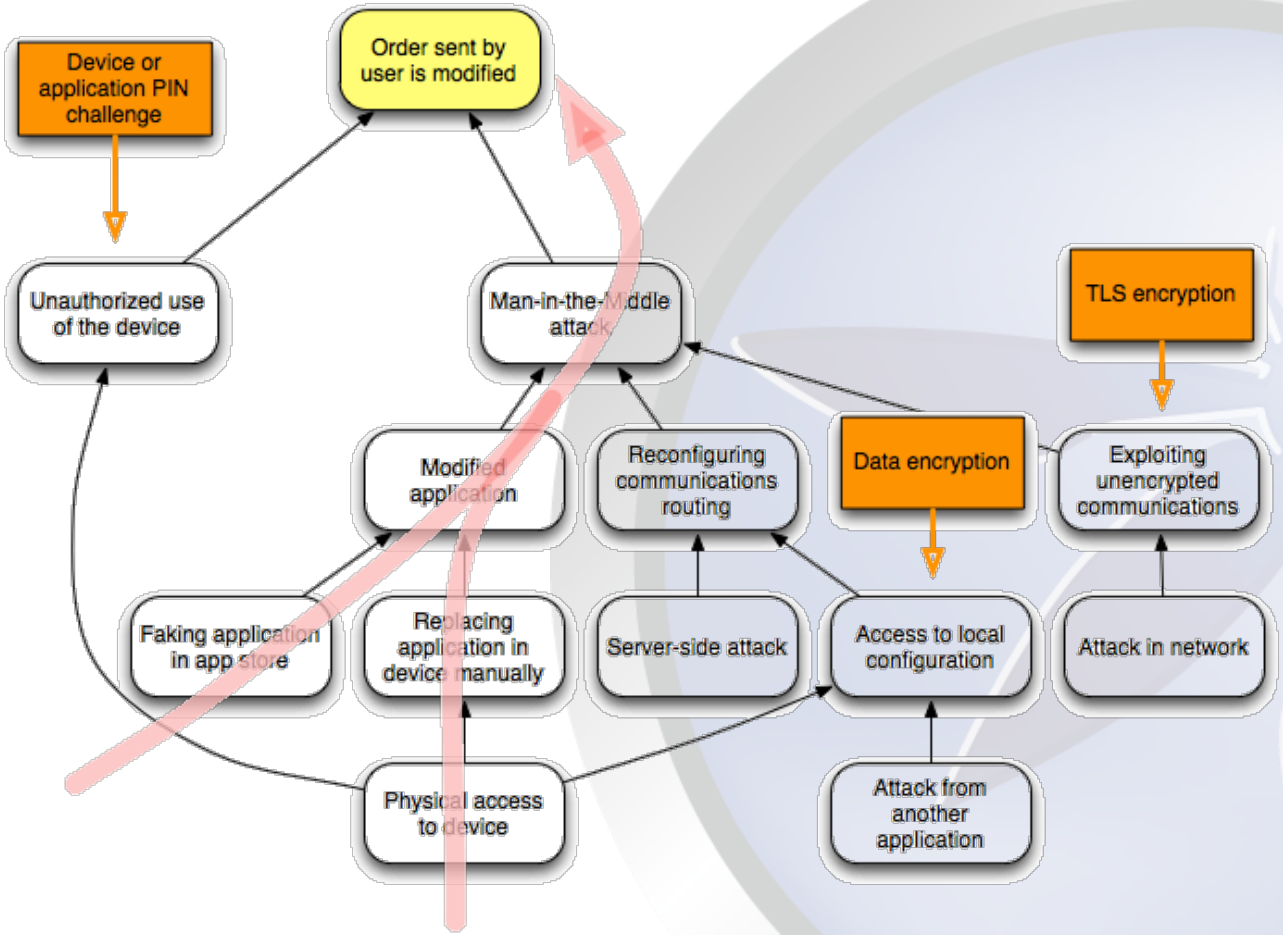
Thought Process for Discovering Threats

1. "What do we want to protect and why?"
2. "Where could the attack happen?"
3. "What could go wrong?"
4. "Do we have appropriate protection?"
5. "What is the risk we accept?"

5. “What is the risk we accept?”

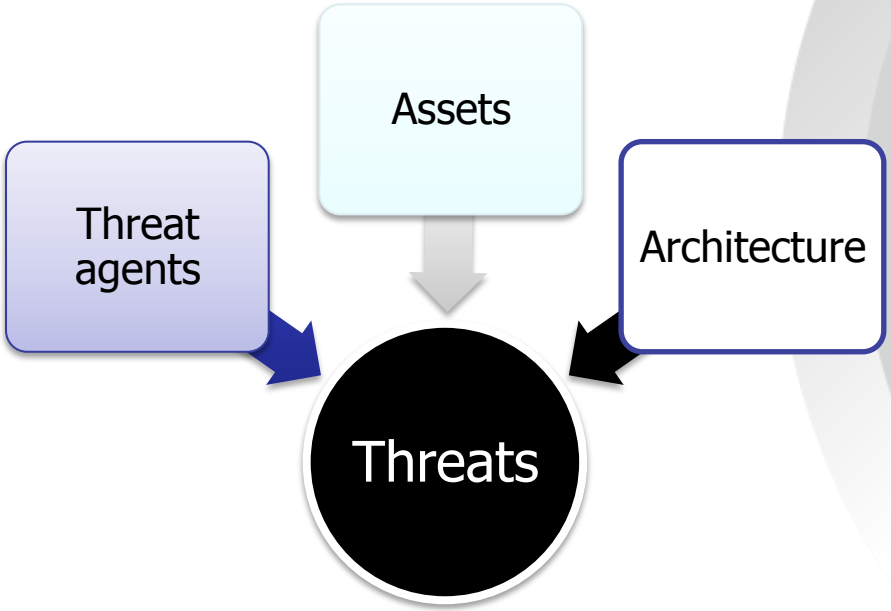
- What are the *residual risks* that can be accepted?
- Not every scenario is worth protecting
- For scenarios not having good protection, consider DREAD:
  - Damage
  - Reproducibility
  - Exploitability
  - Affected users
  - Discoverability
- Is there a known threat agent motivated to perform an attack?

Attack Tree


Device or application PIN challenge
Order sent by user is modified
Unauthorized use of the device
Man-in-the-Middle attack
TLS encryption
Modified application
Reconfiguring communications routing
Data encryption
Exploiting unencrypted communications
Faking application in app store
Replacing application in device manually
Server-side attack
Access to local configuration
Attack in network
Physical access to device
Attack from another application

Summary & Conclusion

1. "What do we want to protect and why?"
2. "Where could the attack happen?"
3. "What could go wrong?"
4. "Do we have appropriate protection?"
5. "What is the risk we accept?"



Questions?

Resources:

- OWASP Mobile Security Project
- ENISA: Top Ten Smartphone Risks
- Microsoft: STRIDE, DREAD