Lecture 17 (Trusted Computing)

1 Some Issues

1. Digital Rights Management
2. Robust Security

2 Trusted Computing

1. Isolation from regular OS
2. Hardware based security guarantees
3. Reconfigurability

2.1 Implications

1. Enhanced confidence in device security
2. Ensures that device performs the way it is supposed to
3. Recovery after a potential compromise
4. Secure storage

3 Trusted Execution Environment OS

1. Apple
   - iOS Secure Enclave
   - separate processor
2. Google
   - Trusty
   - ARM/Intel (Intel's is called Software Guard eXtension - SGX)
3. Linaro
   - OPTEE
   - Arm TrustZone
4. Qualcomm
   - QTEE
   - ARM TrustZone
5. Samsung

- TEEgris
- ARM TrustZone

4 ARM TEE Architecture

1. Two worlds exist
   - Non-Secure World
     a. Untrusted apps
     b. Embedded OS
   - Secure World
     a. Trusted apps
     b. Trusted OS
2. Protected H/W resources are accessible only by Secure World

5 Remote Attestation

1. Integrity check in non-secure world checks integrity of application
2. It is a part of the kernel to ensure correctness
3. The problem of security reduces to verifying integrity of kernel
4. Remote server interacts with secure world for this
5. To solve issue with kernel updates, the *gold hash* is stored at the remote location