CERIAS

The Center for Education and Research in Information Assurance and Security

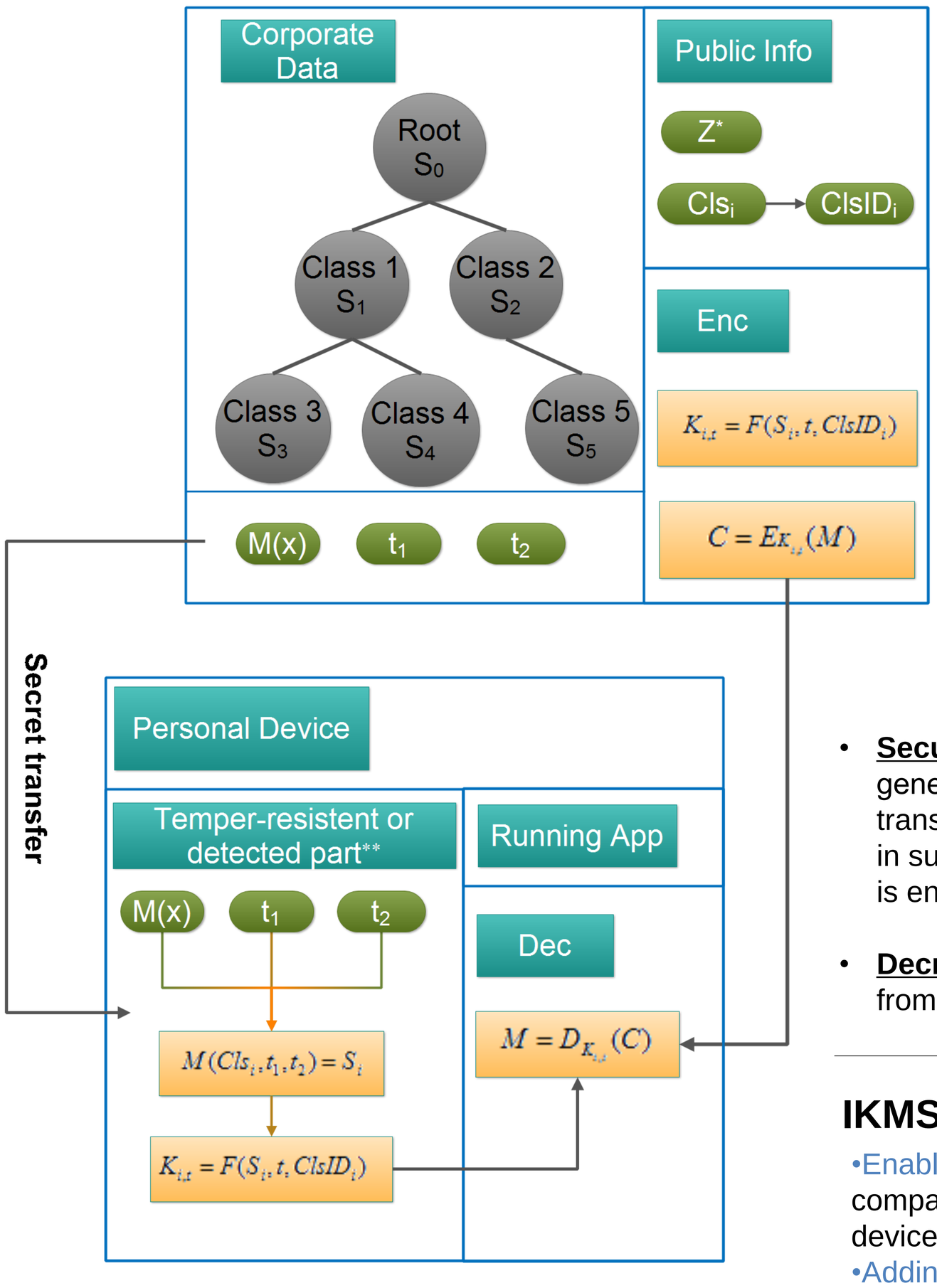
A Key Management Scheme in BYOD Environment

Di Xie, Baijian Yang

Purdue University

Overview

Bring-Your-Own-Device (BYOD) refers to an IT policy that encourages and allows employees to use their personal devices to access privileged corporate network resources. Current BYOD practices are not sufficient to provide both flexible and secure access to data stored on personal devices and are likely to cause privacy infringement issues and incur high management cost. This research presents an Innovative Key Management Scheme (IKMS) approach that employs a hierarchical and time-bounded key management system to battle the security and privacy issues in BYOD deployment.



* Z is the time period of key refreshment. From an initial time point t=0, all seeds assigned to classes are used till t=Z. After that, seeds will be refreshed. t_1 and t_2 are the beginning and ending time point of a clearance. $0 \leqq t_1 \leqq t_2 \leqq Z$.
** Tamper-resistant or detected part is believed that no tamper can be applied or any tamper can be detected in the first time through 24/7 monitoring.

Current BYOD Mechanism Deficiencies for stored data

- Solidified access policies
- High potential of privacy infringement
- High management cost

Basic IKMS Operations

- **Encrypting data based on class**: Divide corporate data into classes with different security privileges in a organized hierarchy. Each class is assigned a seed S_i. Any data to be stored on employees' devices will be encrypted by key $K_{i,t}$. $K_{i,t}$ is generated from seed S_i, timestamp t, and class ID $ClsID_i$. The accessiblity of the stored data is therefore equate to the capability of attaining key $K_{i,t}$. A device has no access to S_i.

- **Secure Transfer of clearance**: A clearance M(X) will be generated based on users' privileges and will be securely transferred and stored on the device. Clearance M(X) is designed in such a way that it can be used to reconstruct key $K_{i,t}$ that a user is entitled to have access during time period (t_1,t_2)

- **Decrypting data on device**: Mobile Apps use the key generated from clearance M(X) to decrypt data.

IKMS Contributions

- Enable flexible corporate access control by making corporate company participating in the process of data access on a personal device.
- Adding another layer of data protection by providing hierarchical data storage and time-bounded data accessibility
- Avoid privacy infringement by monitoring key usages rather than monitoring user data, user behaviors, or device opeartions
- Minimize management costs by providing a cross-platform IKMS.

Security analysis