SECURING MEDICAL RECORDS ON SMART PHONES

Ryan Gardner, Sujata Garera, Matthew Pagan
Matthew Green, Aviel Rubin

Security and Privacy in Medical and Home-Care Systems [ACM CCS 2009]

- Mehool Intwala

Storage Options

- Paper based records of doctor visits
  - Gets piled up over time
  - Messy / Unorganized
- Online: Google Health & Microsoft HealthVault
  - Needs internet access
- Why not portable devices such as smart phones?

Why Smart phones ?

- Always by your side 24 x 7
- Goes with you Anywhere and Everywhere
- No overhead of carrying additional device
- Always at your finger tips

ADVANTAGES

- User can view his own records anytime
- Medical emergencies
  - No need to go around collecting the medical files
- Brutal Accidents
  - Medical information available to the Emergency Medical Technicians

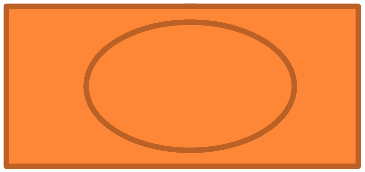
ADVERSARIAL MODEL

- Online Adversary :
  - Interfaces with the phone through normal OS and applications
  - Person who takes the phones, tries to view private information & returns before the owner notices

- Offline Adversary :
  - Has read access to all components of a phone
  - Can read phone's raw memory and storage

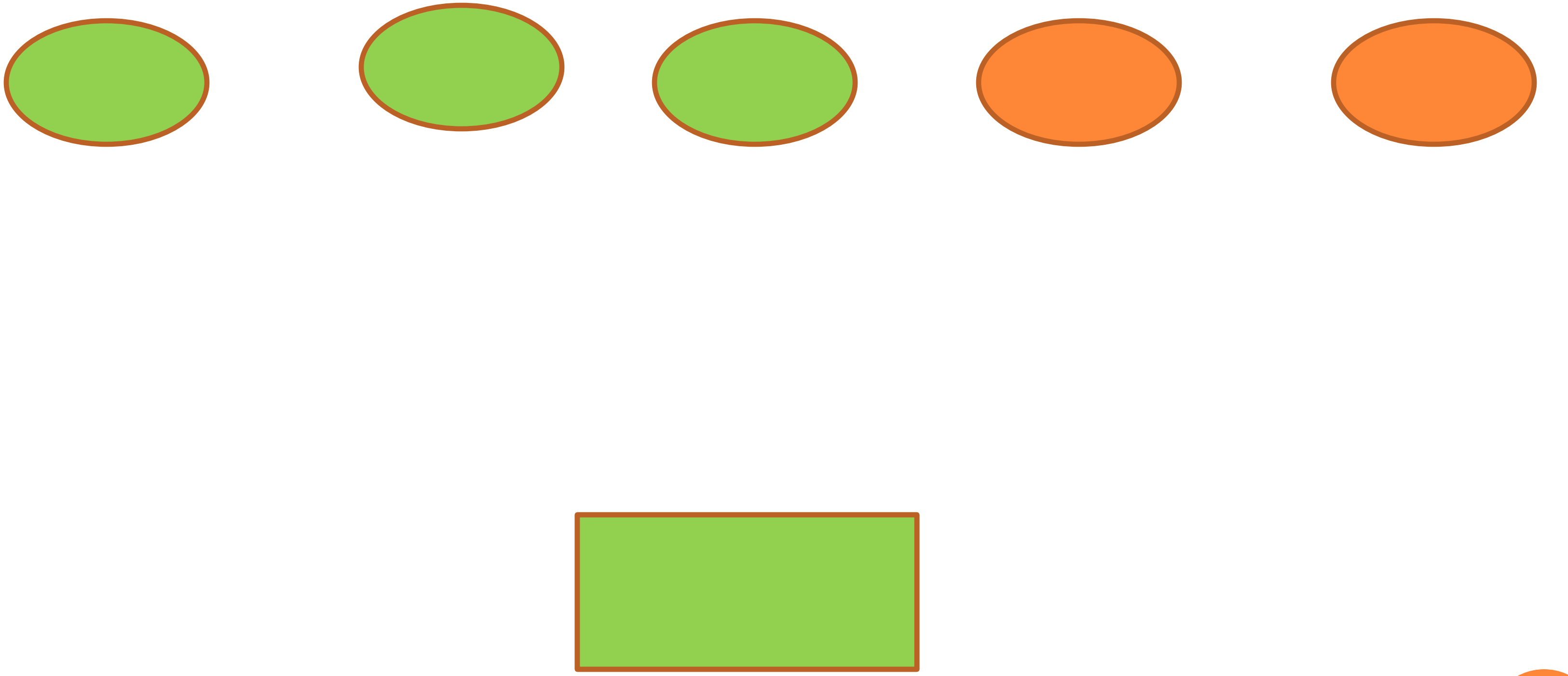
Secret Sharing Scheme

- N = 5   K = 3



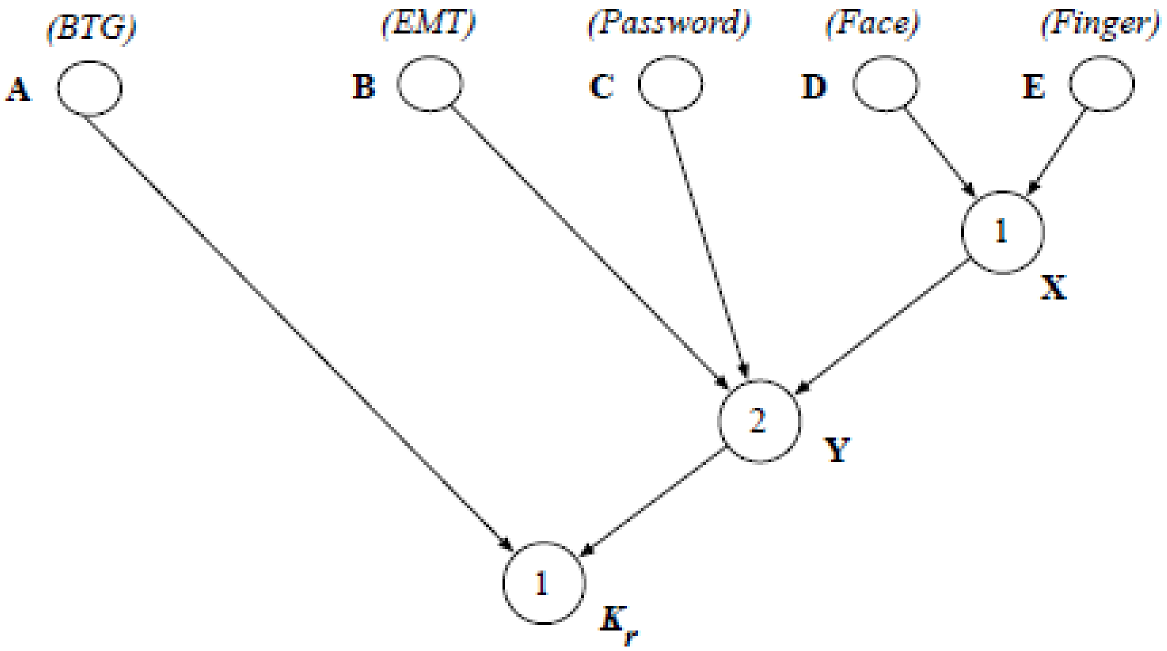
Secret Sharing Scheme

- N = 5 K = 3



Proposed architecture

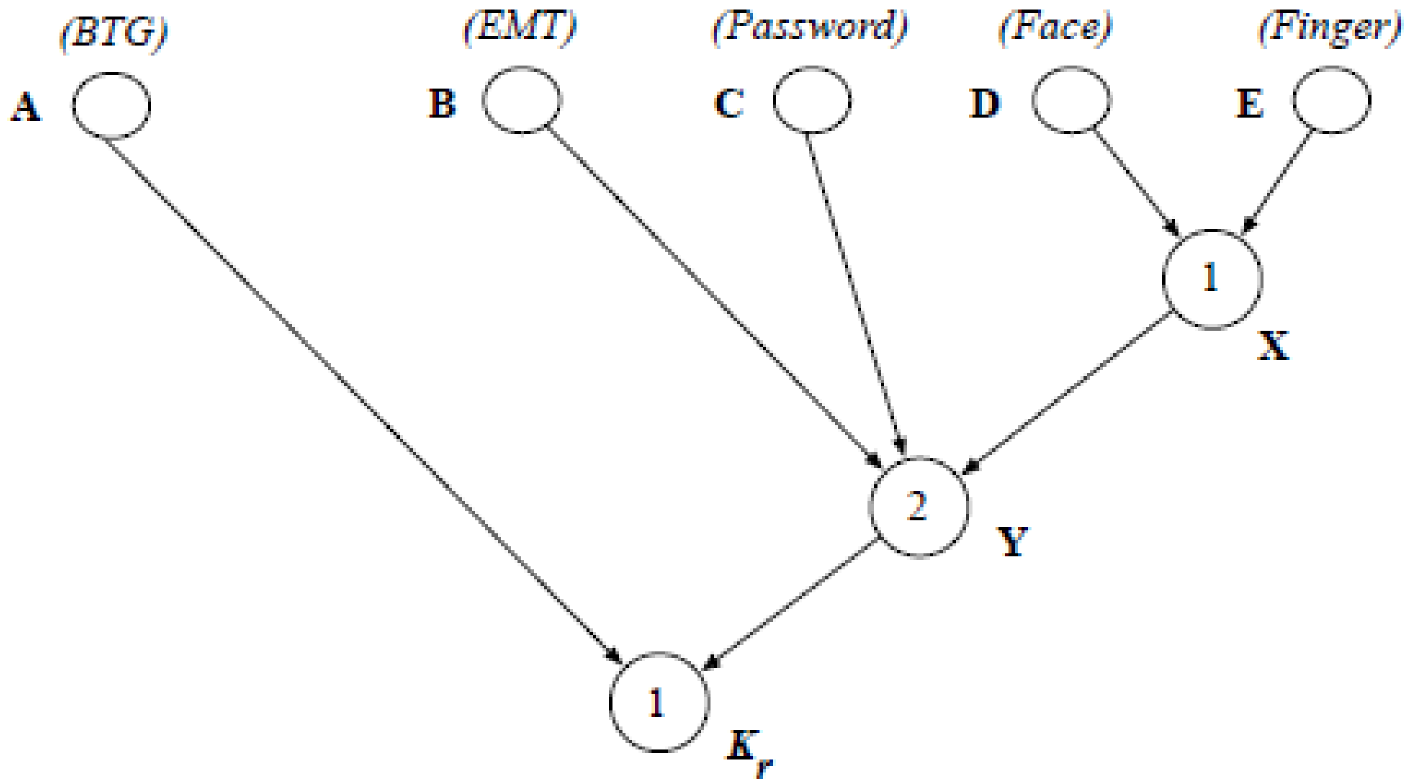
- Secret Sharing Scheme



Share Management

- Finger : Accessible with the owner’s fingerprints
- Face : Accessible with the owner’s face
- EMT : Share available to the EMT
- Password : Accessible with the owner’s password
- BTG (Break-The-Glass) : can be obtained by a special authorization process

Architecture revisited



Discussion

Drawbacks :

- Biometrics ??
- EMT Share losses ??
- Active v/s Passive ??

Thank You