Distributing Security-Mediated PKI

Gabriel Vanrenen, Sean Smith, John Marchesini

Presented by: Qingzhao Tan

Outline

- Introduction
- SEM
- Tools
- Design
- Prototype
- Conclusions and future work

Introduction

- Security-mediated approach to PKI – trust and scalability disadvantages
  - Each user depends on a mediator that may go down or become compromised
- Distributing security-mediated PKI
  - Trusted computing platforms / peer-to-peer networks: to create a network of trustworthy mediators and improve availability
  - Threshold cryptography: to build a back-up and migration technique which allows recovery from a mediator crashing while also avoiding having all mediators share all secrets
  - Strong forward secrecy: to mitigate the damage if a crashed mediator actually be compromised

SEM Approach to PKI

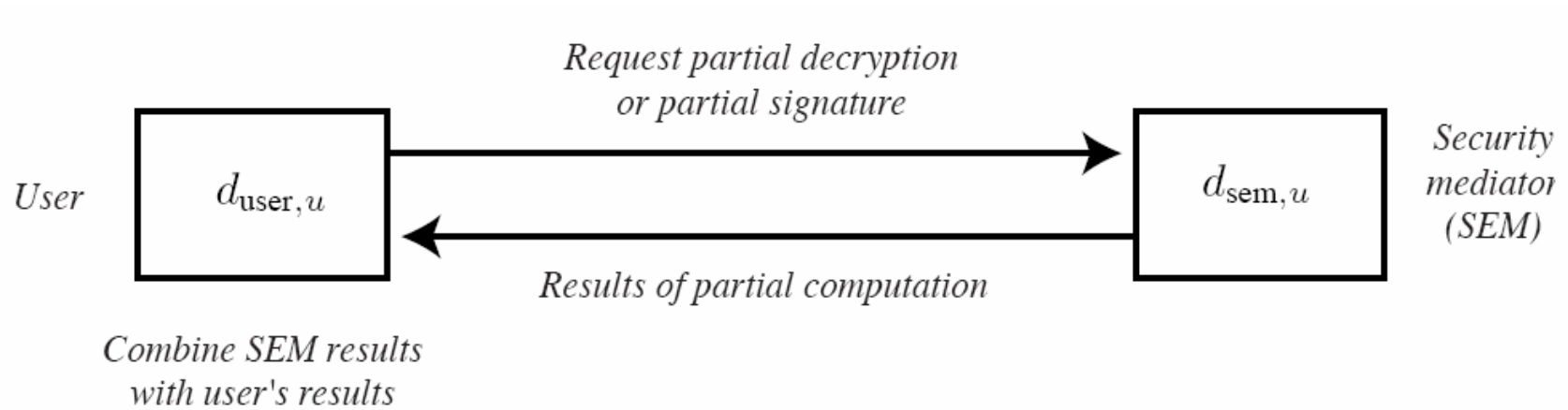
- Motivation: fast and scalable certificate revocation
  - PKI: to create and distribute certificates to relying parties
  - Revoke certificate when certificate is ceased
  - revocation information needs to propagate to relying parties
- SEM: A system that revokes the ability of the keyholder to use a private key, instead of revoking the certificate attesting to the corresponding public key

mRSA – a Variant of RSA

- Standard RSA: for each user
  - A public key (n_u, e_u)
    - n_u : product of two large primes
    - $\gcd(e_u, \varphi(n_u)) = 1$
  - A private key d_u
    - $d_u * e_u = 1 \pmod{\varphi(n_u)}$
- Mediated RSA: for each user
  - A public key (n_u, e_u) – the same as standard RSA
  - A private key – split into two parts
    - $d_{sem,u}$ and $d_{user,u}$ where $d_u = d_{sem,u} + d_{user,u} \pmod{\varphi(n_u)}$

mRSA – a Variant of RSA

- Key setup
  - $d_{sem,u}$ is chosen as a random integer in [0, n_u-1]
  - $d_{user,u}$ is calculated as $d_u = d_{sem,u} + d_{user,u}$
- Private key operations require the participation of both the user and the SEM



SEM Approach to PKI

- Advantages:
  - Compatibility
  - No useful information could be gained by a malicious SEM
  - The compromise of a single SEM does not compromise the secret keys of any users
- Disadvantages:
  - Scalability disadvantages
  - If a user's $d_{sem,u}$ lives on exactly one SEM
    - Temporary denial of service if the network is partitioned
    - Permanent denial of service if the SEM suffers a serious failure
    - Inability to revoke the key pair if an adversary compromises a SEM and learns its secretes

Tools

- Trusted computing platforms
- P2P networking
- Threshold cryptography
- Strong forward security

Trusted Computing Platforms

- Goal: to trust a SEM to use and delete each user's $d_{sem,u}$ when appropriate, and not transmit it further
- Basic requirements:
  - A general-purpose computing environment
  - Cryptographic protections
  - High-assurance protection against physical attacks
  - An outbound authentication scheme
- Trusted Computing Platforms: Gives a safe and confidential environment in remote environments

P2P networking

- Goal: to make it easy for users to find SEMs and this functionality is persisted despite failures and malicious attacks
- P2P networking: decentralization
  - Communication does not rely on a central entity
  - Each entity either tries to satisfy a request itself or forwards it to its neighbors.

Threshold Cryptography

- Goal: to distribute critical secrets across multiple SEMs
- Threshold cryptography:
  - Given a secret y and parameters t < k
  - Construct a degree t polynomial that goes through the point (0,y)
  - Choose k points on this polynomial as shares of y
  - Any t shares suffices to reconstruct the polynomial and hence y
  - Few than t shares give no information

Strong Forward Security

- Goal: to mitigate the damage of potential exposure
- Strong forward security
  - Divide time into a sequence of clock periods
  - Use a cryptographic system such that even if the private key for a given period is exposed, use of the private key in previous or future sessions is still secure

Design – Architecture

- Architecture:
  - Network of server nodes
  - Software to allow for the distribution of SEM approach
- Network:
  - SEMs – distributed trustworthy islands
  - Each island can house resources that enable it carry out services
  - Users can authenticate islands; islands can authenticate each other
  - Use P2P technique to route the request and responds

Design – Migration

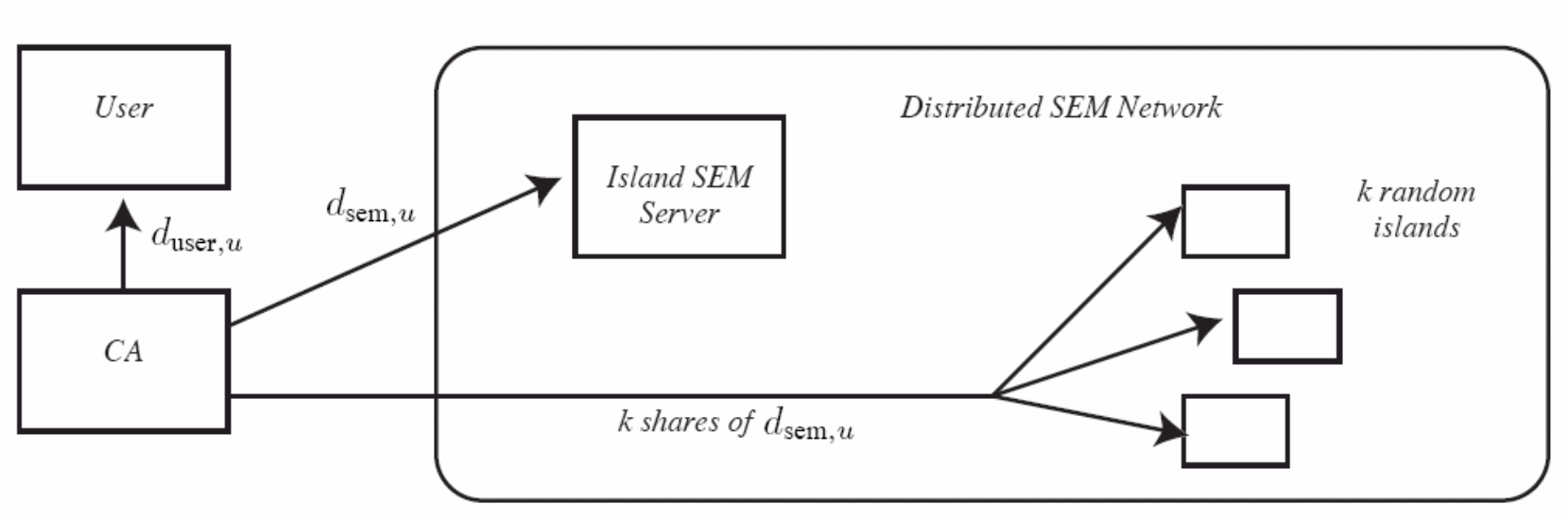
- Aims:
  - A secure way to avoid replication
  - To update the secret held by an island and migrate it to another one
- Secret initialization:
  - Create a secret x and transmit it to an island L
  - Split x into k shares
  - Transmit each share of x to a different island
- When L is unavailable – redirect the requester to another island M

Design – Migration

- General migration scheme
  - Connects to L but fails
  - Connects to M
  - Shareholders of secret x are contacted and this x is updated
  - Strong forward security results in M storing the updated secret
  - Migration is complete and M can fulfill the request
- Benefits
  - Uninterrupted service
  - Secure service after Node Compromise
  - Rare use of distributed computation
- Other caveats
  - If L is compromised
  - If M is compromised
  - If shareholders of x are compromised

SEM Operations

- Key generation:
  - Split into two parts: $d_{sem,u}$ and $d_{user,u}$
  - Share $d_{sem,u}$ to k islands

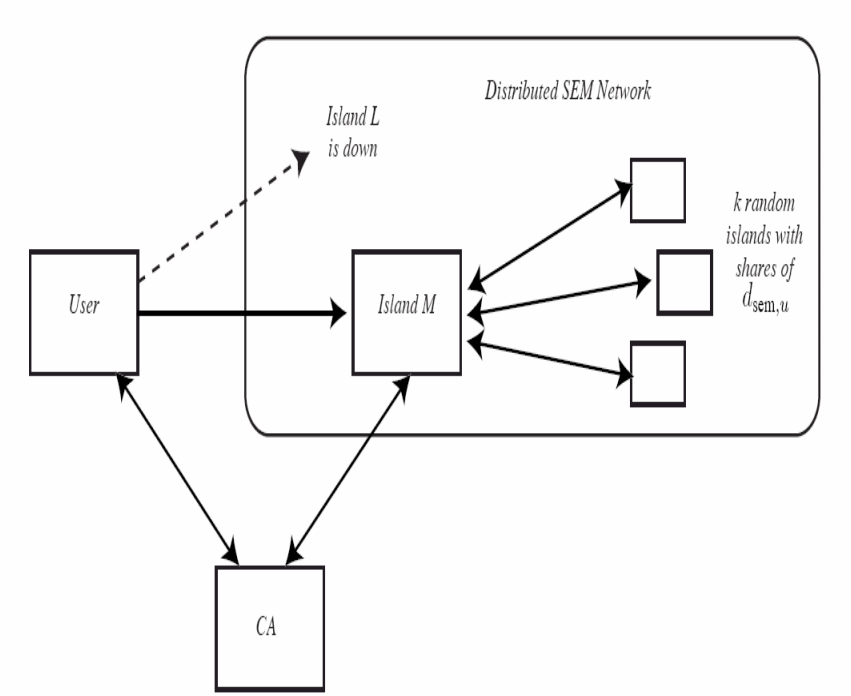


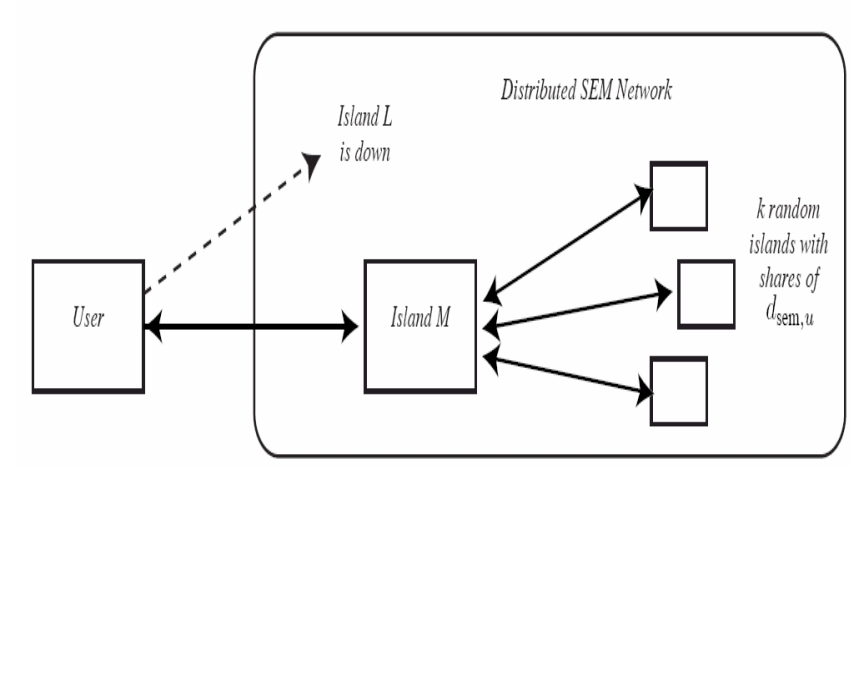
SEM Operations

- Revocation
  - If the island that holds $d_{sem,u}$ and revocation information for a user u goes down
  - During revocation, have the shareholders, original island update the revocation status for that key pair

SEM migration

- L is not available for the request
  - Contacts the SEM network and selected M
  - Using a CA / no CA





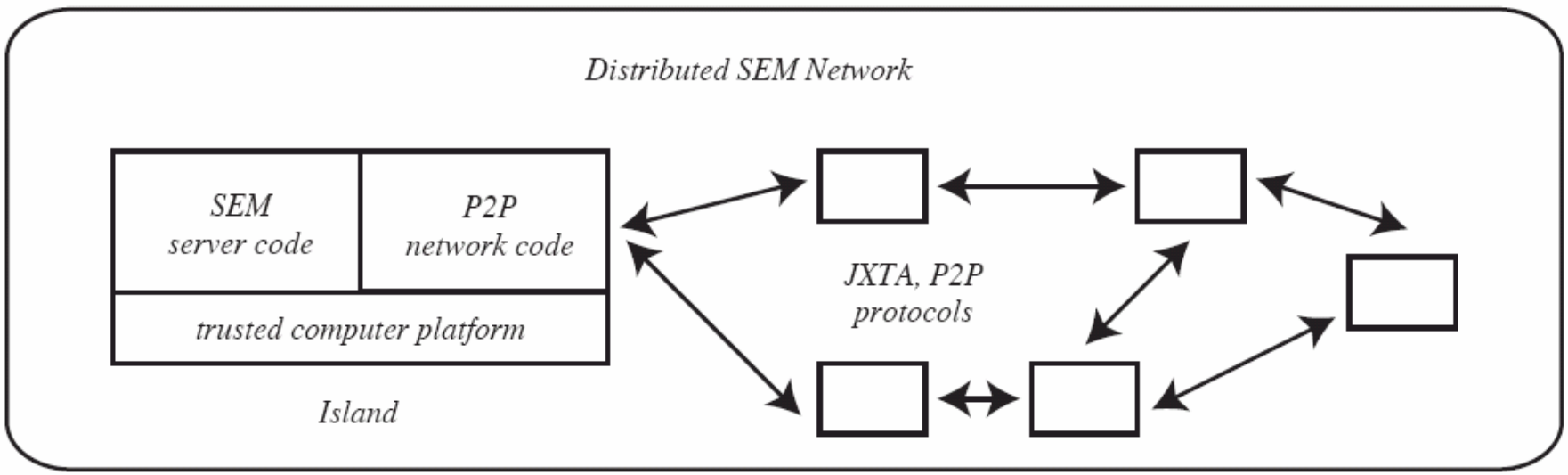
SEM migration

- Renewing user key pairs
  - Regenerate user's private key during regeneration of $d_{sem,u}$
- Recovery: when an island goes down
  - Delete all of the key halves
  - Poll the other islands to determine which $d_{sem,u}$ halves have migrated away from it

Network Trust Model

- Island
  - The primary parties requiring use of the network
  - Join the network normally and become full members of it
- Certificate authorities
  - Connect to an island server that provides an interface to the rest of the network
  - Connect directly to the P2P network but with limited capabilities
- Users
  - Do not connect directly to the P2P network
  - Communicate with an island that provides indirect access to the services available on the network

Prototype


Distributed SEM Network
SEM
server code
P2P
network code
trusted computer platform
Island
JXTA, P2P
protocols

Conclusions and future work

- Summary: to distribute SEM by using a network that combines the benefits of trusted computing platforms and peer-to-peer networking, and provides efficient and uninterrupted access to private data stored on a trusted third party, even in the event of occasional server compromise
- Future work
  - Further performance testing and tuning
  - To explore other applications