Intrusion Fault-Tolerance using Threshold Cryptography

Rahim Sewani
Sarvjeet Singh
Abhilasha Bhargav

Outline

- Introduction
- Motivation
- Threshold Cryptography Basics
- Threshold Cryptography Functionality
- Library Demo
- Analysis
- Achievements

Introduction

- *Goal* – To develop an intrusion fault-tolerant group communication system using threshold cryptography to exchange messages
- TCP-IP supports point to point communication
- Need multi-point to multi-point communication – “Group Communication”

Motivation

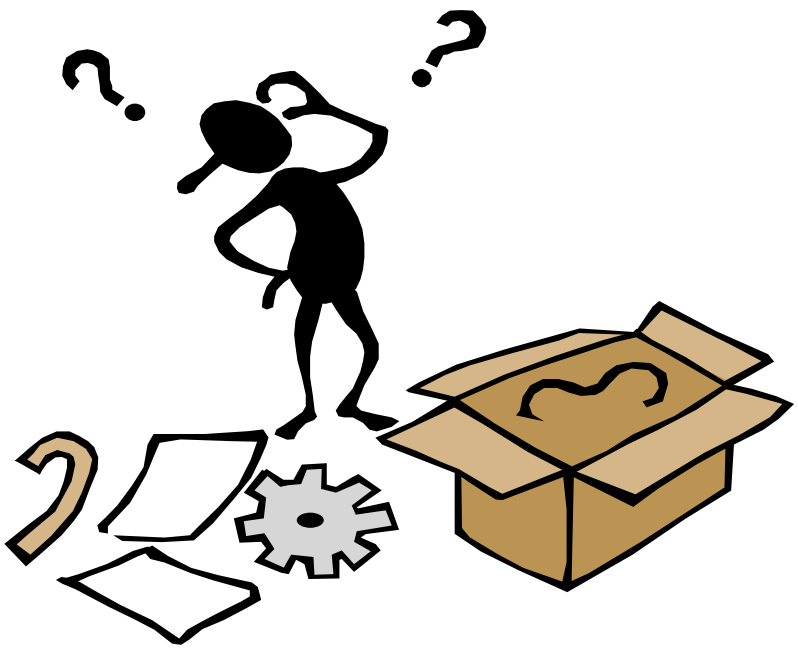
- *Spread* – Provides group communication with reliability and availability in presence of network partitions or component failures
- Server:
  - Receives, processes and forwards messages
  - Needs location of all potential spread servers
  - Exchanges messages to generate a consistent view of the system
- Client:
  - The group members that communicate with the server to send and receive messages

Motivation…

- How to achieve authenticated group communication in Spread?
- Adversary tries to disrupt the consistent view of the system
- Two extremes of agreement
  - Trust everyone
  - Trust no one
- Servers can trust their own subnet
- Servers trust a threshold of servers belonging to another subnet
- Proposed Solution: Integrating *Threshold Signature Library* into the servers

Motivation…

- Did not find any open source Threshold Signatures toolkit



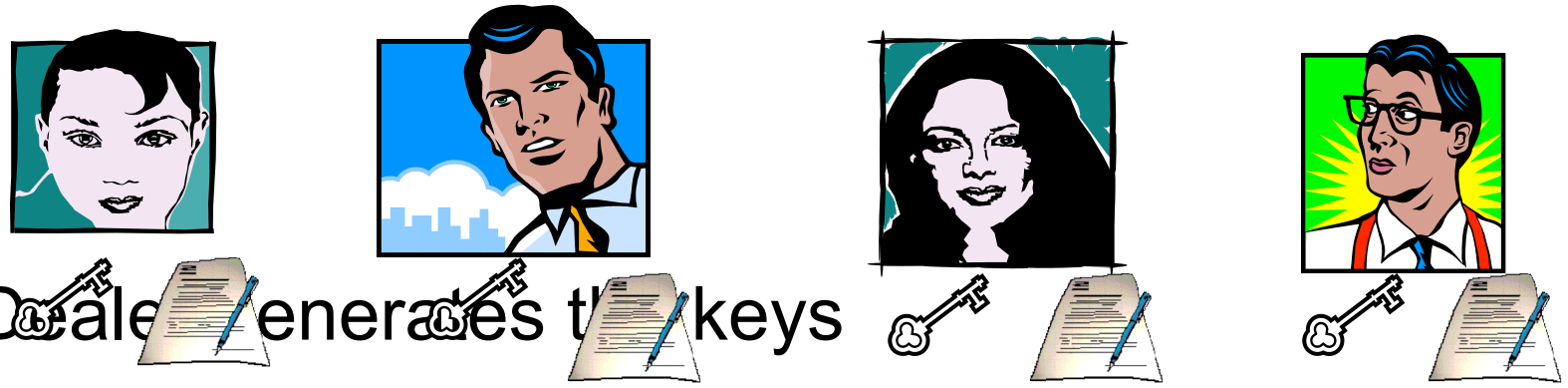
RSA Basics

- Public key = (n,e) ; Secret Key = d
- Signature: $S = M^d \bmod n$
- Verification: $S^e \bmod n = M$?

- Threshold RSA distributes secret amongst all members

Threshold Cryptography

- Allows n parties to share the ability of performing a cryptographic operation (e.g. creating a digital signature)
- Any t parties (t < n) can perform this operation jointly
- Infeasible for any t -1 parties (or less) to do so, even by collusion
- The secret cannot be recovered by any subset of parties

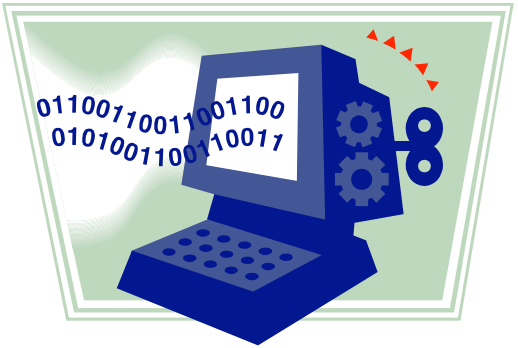


- Dealer generates the keys
- Dealer distributes the keys and send it to the members
- Member signs the message and sends it to the combiner
- Combiner combines the signatures to get a signed message
- Message is broadcast to members

Threshold Signature Library Demo

Threshold Cryptography Implementation

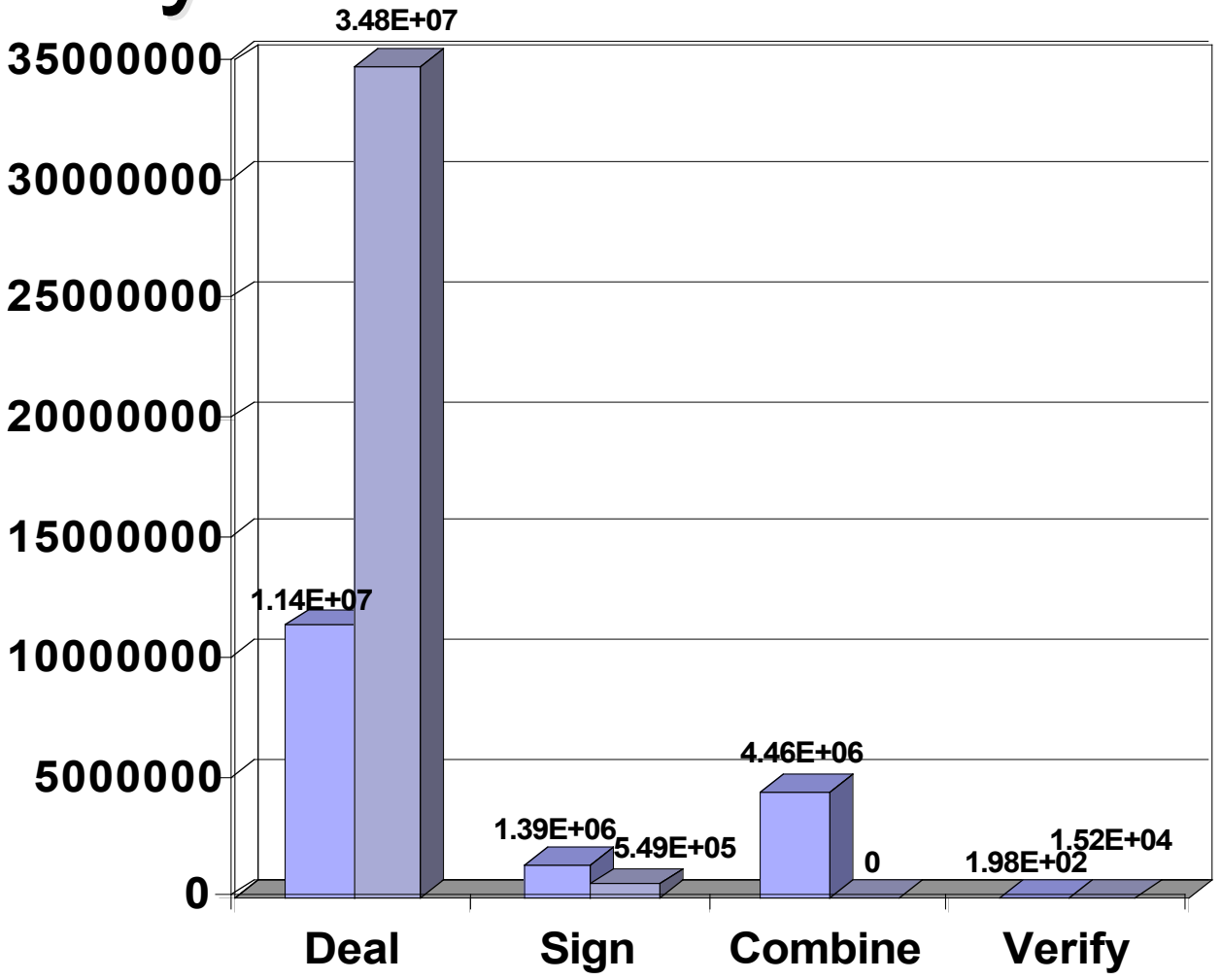
- Implemented signature protocol as described in Victor Shoup “Practical Threshold Signature” paper
- Uses OpenSSL Crypto library
- Generic
  - No assumption about the underlying platform
  - No assumption about the underlying communication mechanism
- Open Source



Analysis of TC-RSA with RSA

	TC-RSA	RSA
Size of the signature	O(1)	O(k) k = Threshold
Generate Ind. Signatures	O(k)	O(k)
Merging Signatures	O(k)	0 (N/A)
Signature Verification	O(1)	O(k)

Analysis of TC-RSA with RSA



Y-Axis: Number of Micro seconds

X-Axis: Function

TC-RSA (1024)
RSA (1024)

N = 100

K = 67

Analysis of TC-RSA with RSA

- Setup cost (PKI):

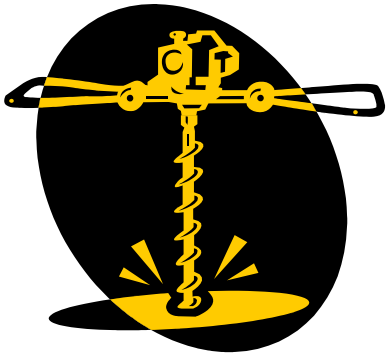
TC-RSA	RSA
Requires one certificate for the public key per group	Requires n certificates for all group members

Accomplished Work

- Researching and understanding current state of work in group communication protocols and threshold cryptography
- Understanding the Spread architecture and the interaction between its modules
- Implementing and testing the Threshold Cryptography library
- Threat and run time and complexity analysis of threshold signatures

Future Work

- Integrating the threshold signatures in the Spread communication system
- Testing and analyzing the performance of the code implemented



Questions

Acknowledgement

Professor Cristina Nita-Rotaru and CS590D students for insight and helpful suggestions