Distributed Information Processing
26th Lecture

Eom, Hyeonsang (엄현상)
Department of Computer Science & Engineering
Seoul National University

©Copyrights 2010 Eom, Hyeonsang All Rights Reserved
Outline

- Possible Topics for Final Review
  - Information Protection
  - DRM Introduction
- Q&A
Possible Topics for Final

- Chandy’s “Snapshot” Algorithm
- Ordering Events with Vector Clocks
- Balance and Tradeoff among Communication, Processing, and Storage
- Memory Consistency Models
- Memory Coherence
- DSM vs Message Passing
- Lazy Release Consistency
- Location Independence in DFS
- Cache Unit Size in DFS
- Large Cluster vs SM Machines
Possible Topics for Final

- Chord
- Tapestry
- Chord vs Tapestry
- Tapestry Routing & Object Location
- Techniques for Embedded Software
- Embedded Software Issues
- Context
- Security Violation Types
- Security Attack Methods
- Stack and Buffer Overflow
Possible Topics for Final

- ATM PIN Security
- Capability vs Access Control List System
- Protected Subsystems
- Attacks & Countermeasures in WSNs
- Basic Security Concepts
- Symmetric vs Asymmetric Cryptographic Algorithms
- Digital Signatures
- Certificates
- PKI Example
- Security Holes in PKI
Possible Topics for Final

- OMA DRM Example
- Characteristics of Internet Content Delivery Systems
- Ontology
- Ontologies vs XML
- Latency Reduction vs Latency Hiding
- Critical Path Issues
- Bandwidth, Delay, and Loss Adaptation
- Dynamic Adaptation Methods
Review: Information Protection

ATM PIN Security

- Splitting of a Customer’s PIN into Two Parts and Storing Them Separately
  - PIN Offset in the ATM server
  - Natural PIN derived with the PIN key in the PIN machine

CustomerPIN = (?) f(Acct#, PINOffset, PINKey)

Natural PIN Is Not Stored Anywhere in the Entire Process
Review: PKI Example

Basics

- Digital Signature (DS)
  - DS(I, pr) for Information I and a private key pr
- Certificate C (Containing a Public Key and DS)
  - C(pu, pr0) for a public key pu and pr0 from CA

Question

- Is This Secure?
  - A sends B I + DS(I, pr1) + C1(pu1, pr0)
  - B verifies C1(pu1, pr0) by obtaining C0(pu0, pr0) from CA
  - Verification with DS of C1(pu1, pr0), and pu0
  - B verifies DS(I, pr1) with pu1