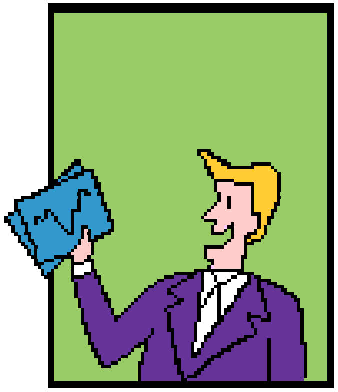
Security in the Ambient Computational Environment

S.Vidyaraman

Thesis defense for the degree of
Master of Science in
Computer Engineering
University of Kansas

August 14th, 2002



Committee:
Dr.Joseph. B Evans (Chair)
Dr.Gary.J Minden
Dr.Arvin Agah

Acknowledgements

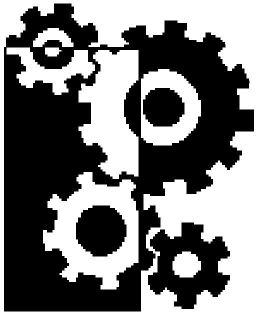
Thanks to the ACE development team and the Management! I have had a wonderful time here at ITTC and KU.

Overview

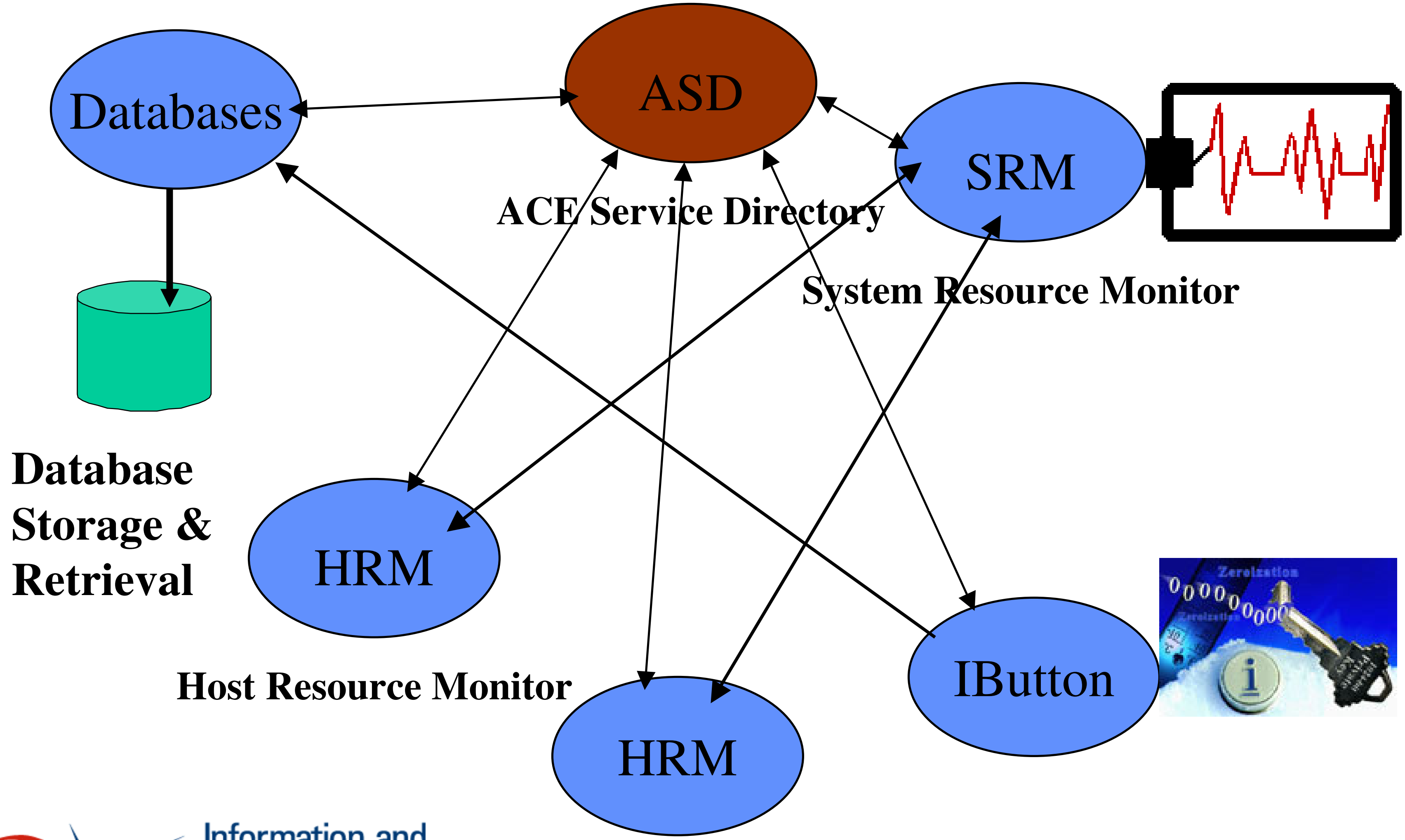
- Background
- Security Issues Addressed
- Security Services Implemented
- Typical Scenarios
- Analysis
- Summary & Future Work
- Q&A

Background

- ACE : Ambient Computational Environment
- Its all about reinventing the 4 wheels of the car. But then ……
- Entities in ACE
  - ACE Services
  - ACE Users



ACE Services



Databases

ASD

ACE Service Directory

SRM

System Resource Monitor

Database Storage & Retrieval

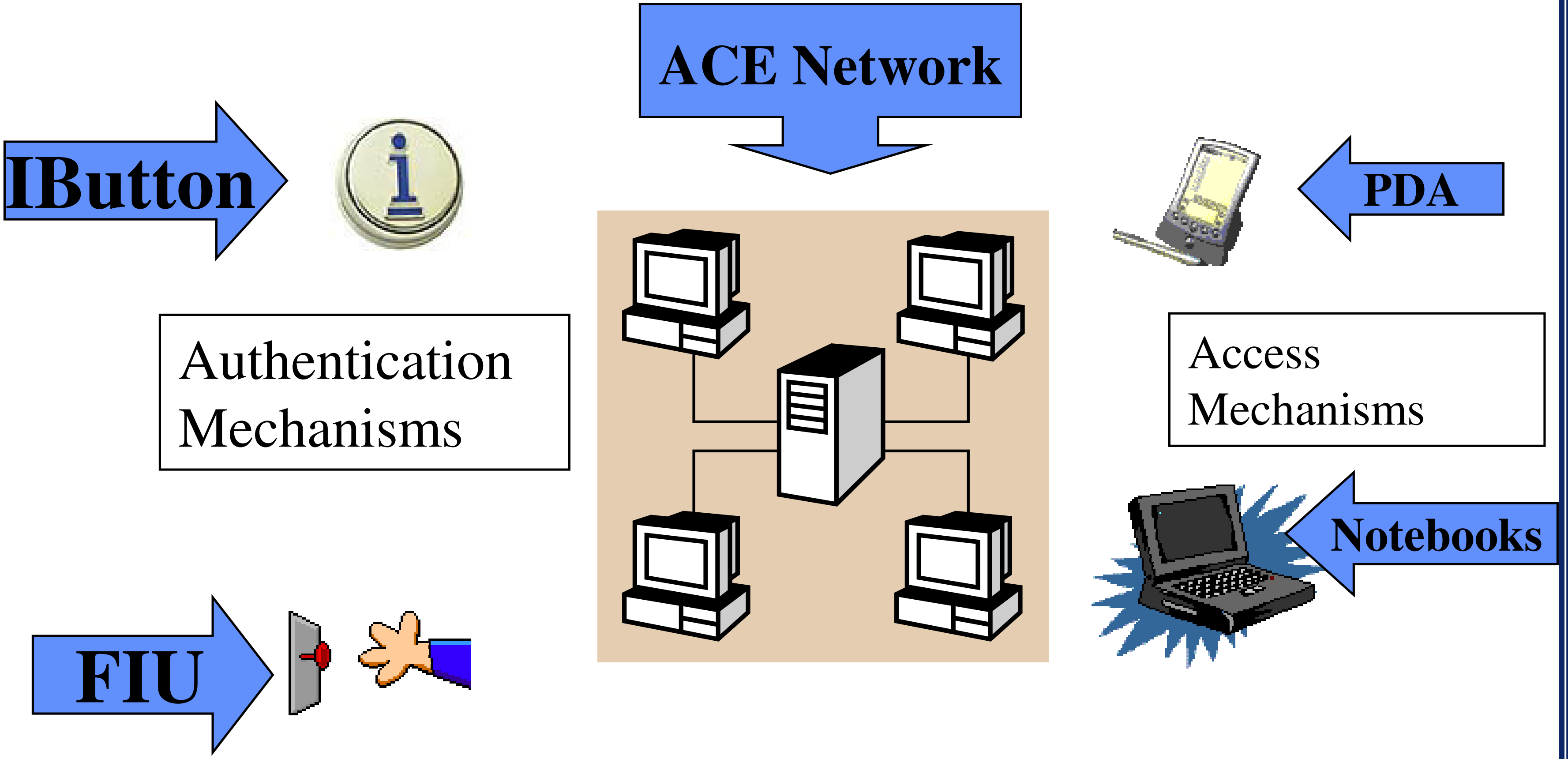
HRM

Host Resource Monitor

HRM

IButton

ACE User



ACE Network

IButton

PDA

Authentication Mechanisms

Access Mechanisms

Notebooks

FIU

Security Issues addressed

- Services communicate within themselves.
  - Network Commands
  - Data Streams (Audio and Video)
- Users
  - Authentication
- The Users Workspace is a VNC Session.
- How do we identify both Users and Services?

Security Services Implemented

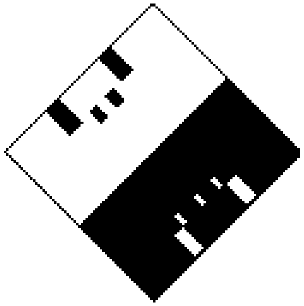
- Remote Connection Manager
- Certificate Authority
- Certificate Distribution System
- Key Manager

Security Services Implemented

- Remote Connection Manager
  - Functionality
  - DH Key Establishment
  - SPEKE Protocol
- Certificate Authority
- Certificate Distribution System
- Key Manager

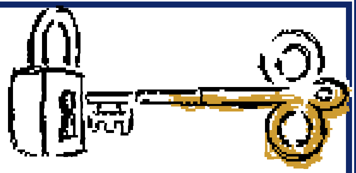
Remote Connection Manager

- Gateway to the ACE Domain from Outside
- Functions:
  - Authenticate the user
  - Establish a shared session key



- At present, it implements the SPEKE protocol
  - A Variant of the Diffie-Hellman Key establishment
  - One of the ***strong*** authentication mechanisms with (even) weak passwords
  - Minimum (3) number of passes
  - Protects against dictionary attacks

Diffie-Hellman Key Establishment



- Session Key Establishment
- Assumes 2 known values
- Offers No Authentication

	Alice		**Bob**
A prime number p and a generator g are known to Alice and Bob			
	Picks a secret number R_A		**Picks a secret number R_B**
Key Set up	**$Q_A = g^{(R_A)} \bmod p$**	→	
		←	**$Q_B=g^{(R_B)} \bmod p$**
	$K = Q_B^{(R_A)} \bmod p$		**$K=Q_A^{(R_B)} \bmod p$**

SPEKE Protocol

Secure

Password-authenticated

Exponential

Key

Exchange

The generator g is now the squared hash of the password S

	Alice		Bob
	All operations are mod p		
	$Q_A = S^{(2\,R_A)}$	→	
Key Exchange		←	$Q_B = S^{(2\,R_B)}$
	$K = Q_B^{(2\,R_A)}$		$K = Q_A^{(2\,R_B)}$
	Abort if K< 2		**Abort if K< 2**
		←	$V_1 = h(h(K))$
Verification	$V_2 = h(K)$	→	
	Abort if V_1 **!= h(h(K))**		**Abort if** V_2 **!= h(K)**

Security Services Implemented

- Remote Connection Manager

- Public Key Infrastructure (PKI based Services)
  - Certificate Authority
  - Certificate Distribution System

- Key Manager

Certificate Authority

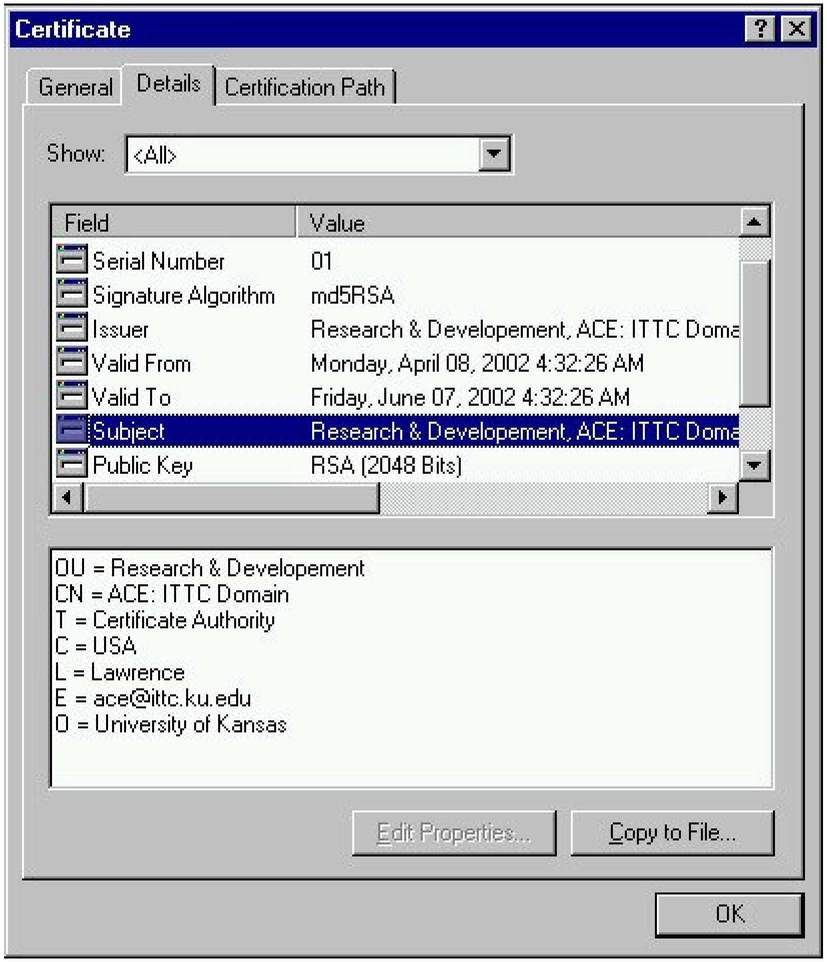
- Provides identification to users and daemons
- Issues X509 digital certificates to users & daemons
- Revokes the user / daemon certificate when necessary
  - Creates a CRL for all the certificates revoked
- Notifies the issued & Revoked Certificates to the Certificate Distribution Daemon

Certificate Distribution System

- Function: To distribute all valid user / daemon certificates
- Answers queries from ACE services regarding validity of certificates
- Publishes the list of valid certificates and the Certificate Revocation List (CRL) on a publicly accessible LDAP service

ACE Root Certificate

- Same Issuer and Subject
- Essentially a self signed Certificate
- Signature Algorithm: md5withRSA
- Thumbprint Algorithm: sha1

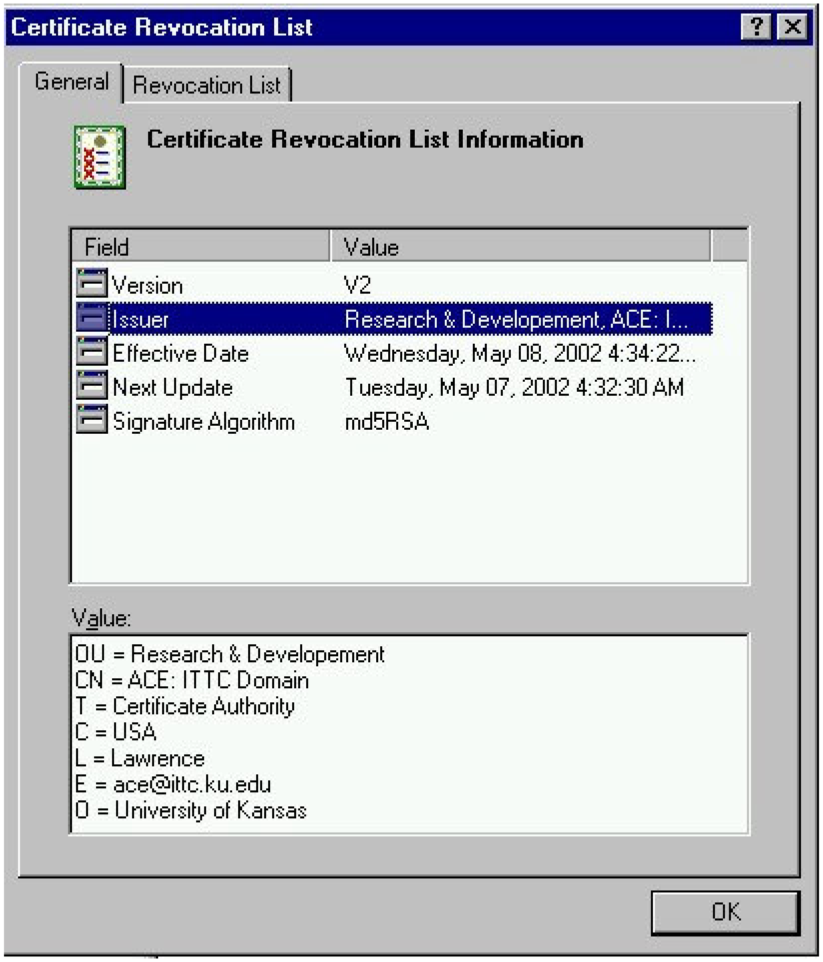


Show: <All>

Field	Value
Serial Number	01
Signature Algorithm	md5RSA
Issuer	Research & Developement, ACE: ITTC Doma
Valid From	Monday, April 08, 2002 4:32:26 AM
Valid To	Friday, June 07, 2002 4:32:26 AM
Subject	Research & Developement, ACE: ITTC Doma
Public Key	RSA (2048 Bits)

OU = Research & Developement
CN = ACE: ITTC Domain
T = Certificate Authority
C = USA
L = Lawrence
E = ace@ittc.ku.edu
O = University of Kansas

ACE Certificate Revocation List

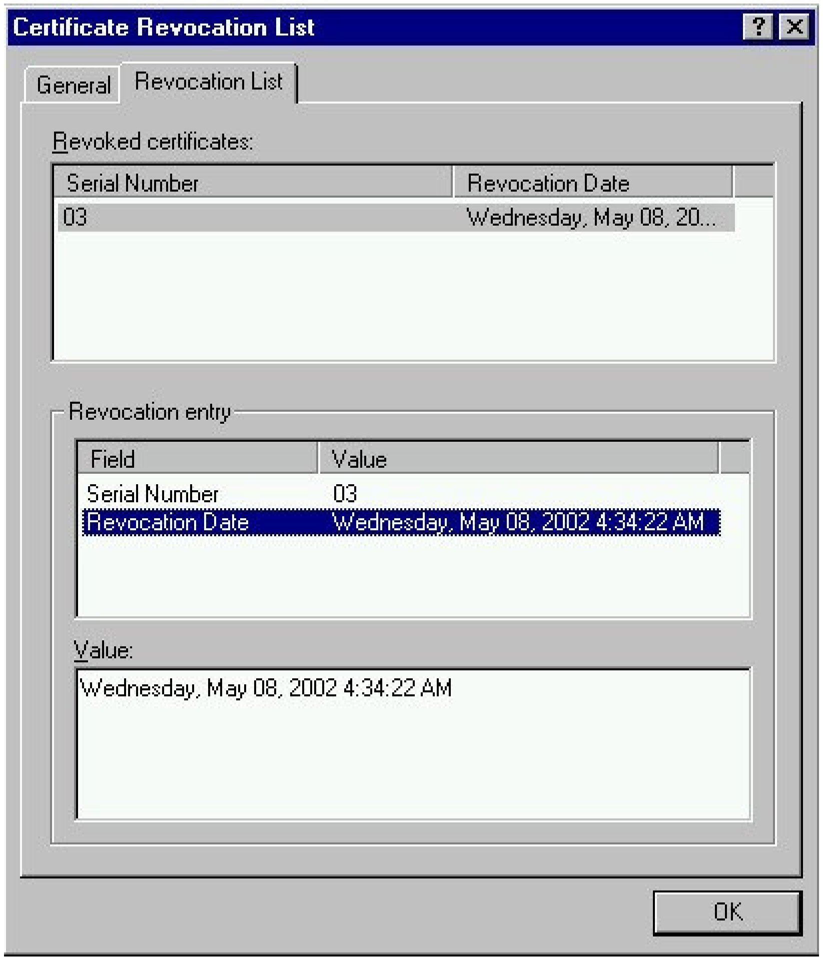


Certificate Revocation List Information

Field	Value
Version	V2
Issuer	Research & Developement, ACE: I...
Effective Date	Wednesday, May 08, 2002 4:34:22...
Next Update	Tuesday, May 07, 2002 4:32:30 AM
Signature Algorithm	md5RSA

Value:

OU = Research & Developement
CN = ACE: ITTC Domain
T = Certificate Authority
C = USA
L = Lawrence
E = ace@ittc.ku.edu
O = University of Kansas



Revoked certificates:

Serial Number	Revocation Date
03	Wednesday, May 08, 20...

Revocation entry

Field	Value
Serial Number	03
Revocation Date	Wednesday, May 08, 2002 4:34:22 AM

Value:

Wednesday, May 08, 2002 4:34:22 AM

Security Services Implemented

- Remote Connection Manager
- Certificate Authority
- Certificate Distribution System
- Key Manager

Key Manager

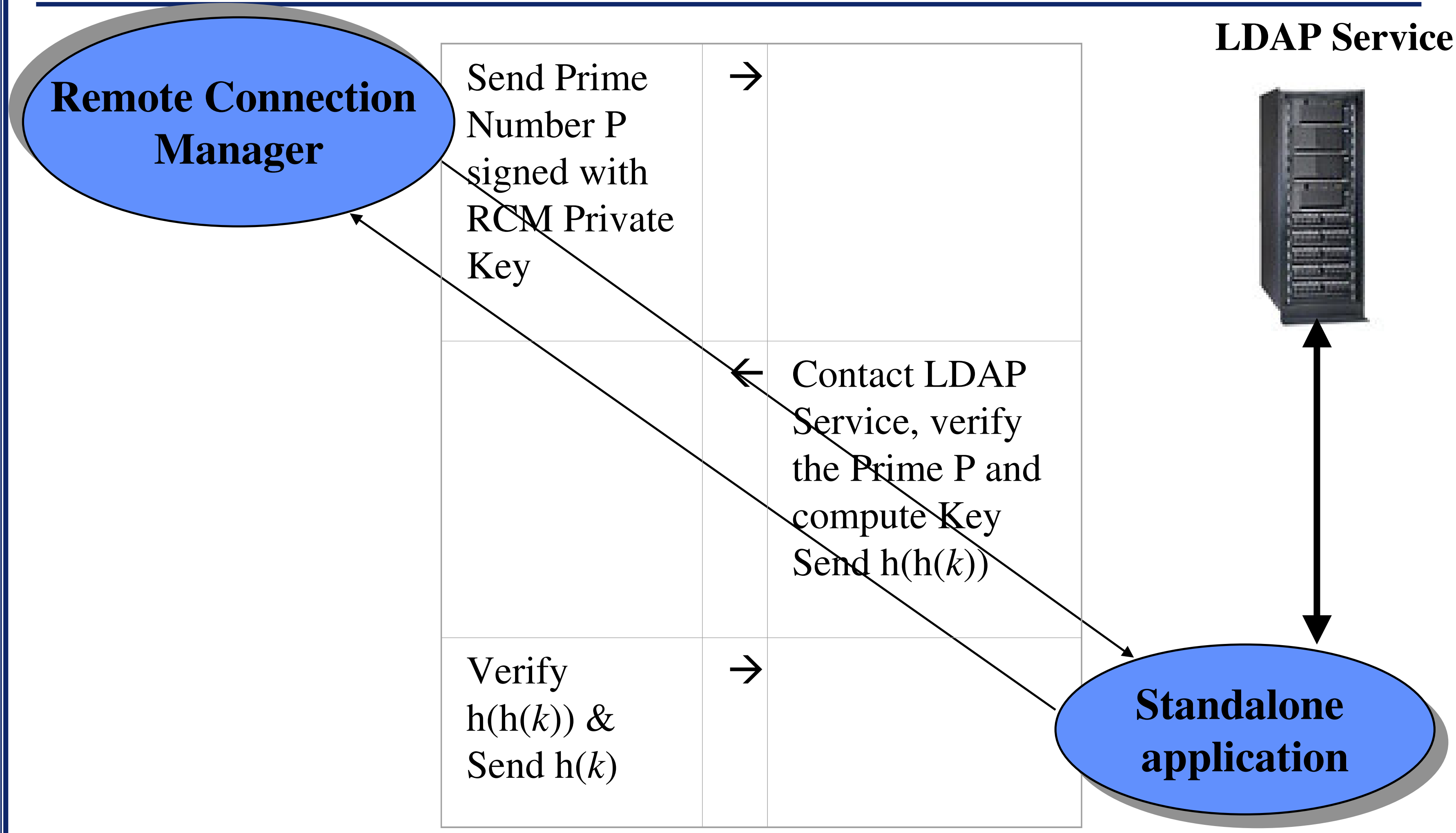
- Service that issues cryptographic keys to services
- Supports of a wide variety of cryptographic algorithms
- Keys may be used as:
  - One time session
  - Conference
- All issued keys are stored in a PBE encrypted keystore

Typical Scenarios

- Remote Authentication

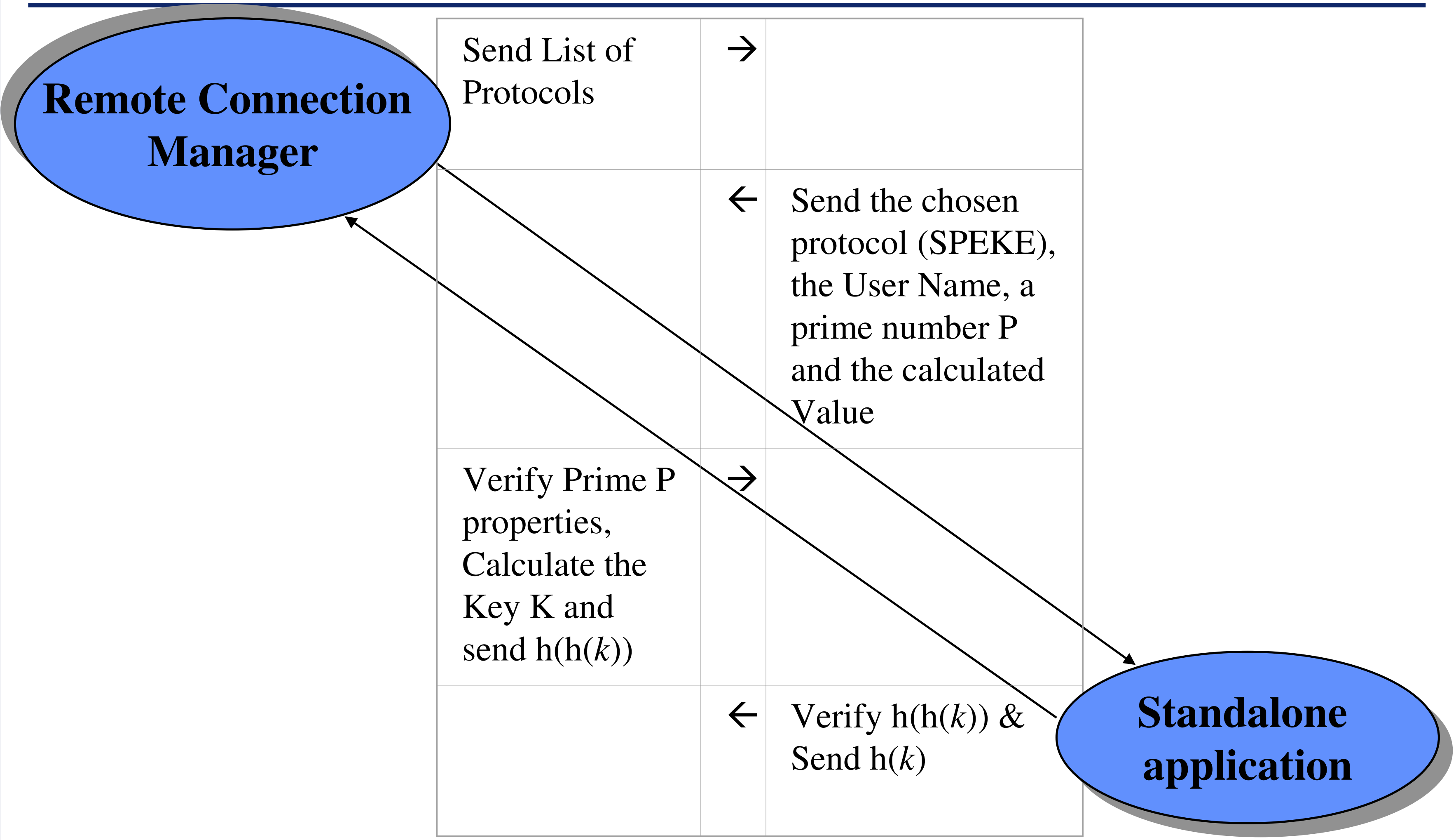
- Certification Process

Possible Remote Authentication Procedure



Send Prime Number P signed with RCM Private Key	→	
	←	Contact LDAP Service, verify the Prime P and compute Key Send h(h(*k*))
Verify h(h(*k*)) & Send h(*k*)	→	

Remote Authentication Process

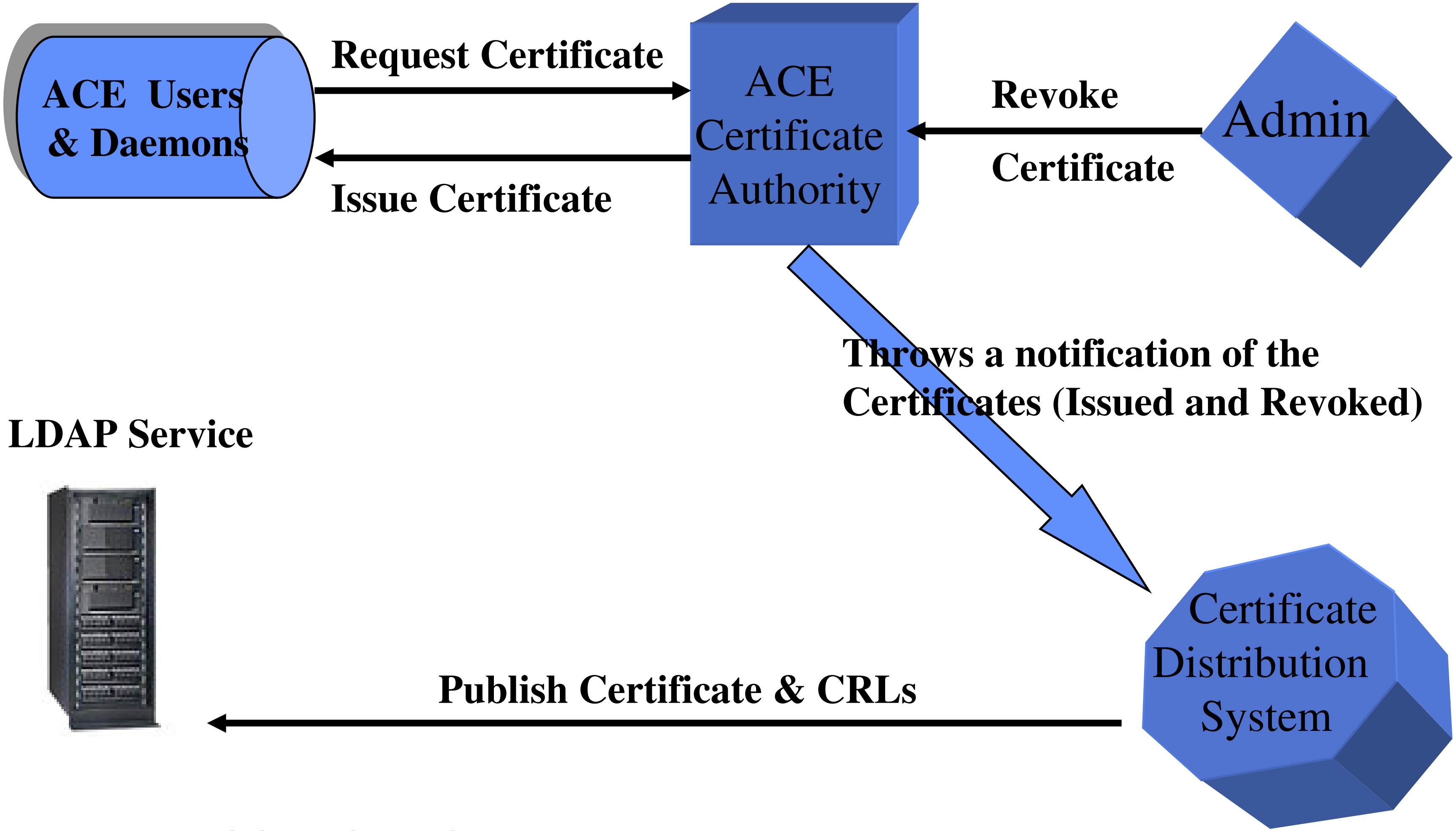


Remote Connection Manager

Standalone application

Send List of Protocols	→	
	←	Send the chosen protocol (SPEKE), the User Name, a prime number P and the calculated Value
Verify Prime P properties, Calculate the Key K and send h(h(*k*))	→	
	←	Verify h(h(*k*)) & Send h(*k*)

Certification Process


ACE Users & Daemons
Request Certificate
Issue Certificate
ACE Certificate Authority
Revoke
Certificate
Admin
Throws a notification of the Certificates (Issued and Revoked)
LDAP Service
Publish Certificate & CRLs
Certificate Distribution System

Analysis

1. What problem are we trying to solve?
   - User and Daemon identification
   - User Authentication (Remote)
   - Secure Communications
2. How effective is the proposed solution?
   - X509 Digital Certificates
   - Password / IButton ID / Fingerprint ID
   - Standard encryption

Analysis

3. What new problems have been added?

- Addition overhead of managing a limited PKI
- Additional vulnerability to social engineering problems
  - Passwords can be changed once a compromise is detected
  - Not true with IButton and Fingerprint data

- Extraneous issues!
  - Java
  - API calls & Key lengths

Summary

- The following services have been prototyped in this thesis
  - A Rudimentary Key Manager
  - A Certificate Authority
  - A Certificate Distribution System
  - A Remote Connection Manager
- But then …….Security is a process, not a product.

Future Work

- Implement a (m,l)- threshold b-secure t-group key distribution scheme
  - Number of centers: *m*
  - Minimum number of centers required: *l*
  - *(l-1)* center & *b* user compromise doesn’t compromise the system
- Better storage system for CA Keys and Certificates

Questions ?

X.509 Digital Certificate Fields

Certificate field	Description
Version	The X.509 version number.
Serial number	The unique serial number that the issuing certification authority assigns to the certificate. The serial number is unique for all certificates issued by a given certification authority.
Signature algorithm	The hash algorithm that the certification authority uses to digitally sign the certificate.
Issuer	Information regarding the certification authority that issued the certificate.
Subject	The name of the individual or certification authority to which (whom) the certificate is issued. This may be a full name and e-mail name or some other personal identifier.
Public key	The public key type and length associated with the certificate.
Thumbprint algorithm	The hash algorithm that generates a digest of data (or thumbprint) for digital signatures
Thumbprint	The digest (or thumbprint) of the certificate data.

SPEKE Vs DH-EKE

Constraint	Prevents Attack by:	Applies to
modulus p is huge	discrete log attack	D S
test Q_x != 0, when un-encrypted	forcing K=0	D S
p-1 has large prime factor q	Pohlig-Hellman log computation	D S
encrypted Q_x randomly padded.	leakage from $E_S(Q_x)$	D
base is primitive root of p	partition attack on $E_S(Q_x)$	D
base is a generator of q	partition attack on Q_x	S
base = S_x mod p	password-in-exponent attack	S
first receiver of verification of K must encrypt Q_x	finding password S using chosen R_x, Q_x, $E_K(x)$ and password dictionary	D
use one-way hash of K	narrowing attacks	D S
high bits of p must be 1	partition attack on $E_K(Q_x)$	D
Receiver of clear Q_x abort if K is small order. or Encrypt Q_A, $Q_{B.}$	subgroup confinement of K	D
Abort if K has small order	subgroup confinement of K	S

Navigation

- ACE Entities
  - Services
  - Users
- Services
  - Remote Connection Manager
  - Certificate Authority
    - Certificate
    - Certificate Revocation List
  - Certificate Distribution System
  - Key Manager
- SPEKE
- Diffie-Hellman
- Scenarios
  - Remote Authentication
  - Certification
- Analysis
- Distributed Key Manager