Ceremony Design and Analysis

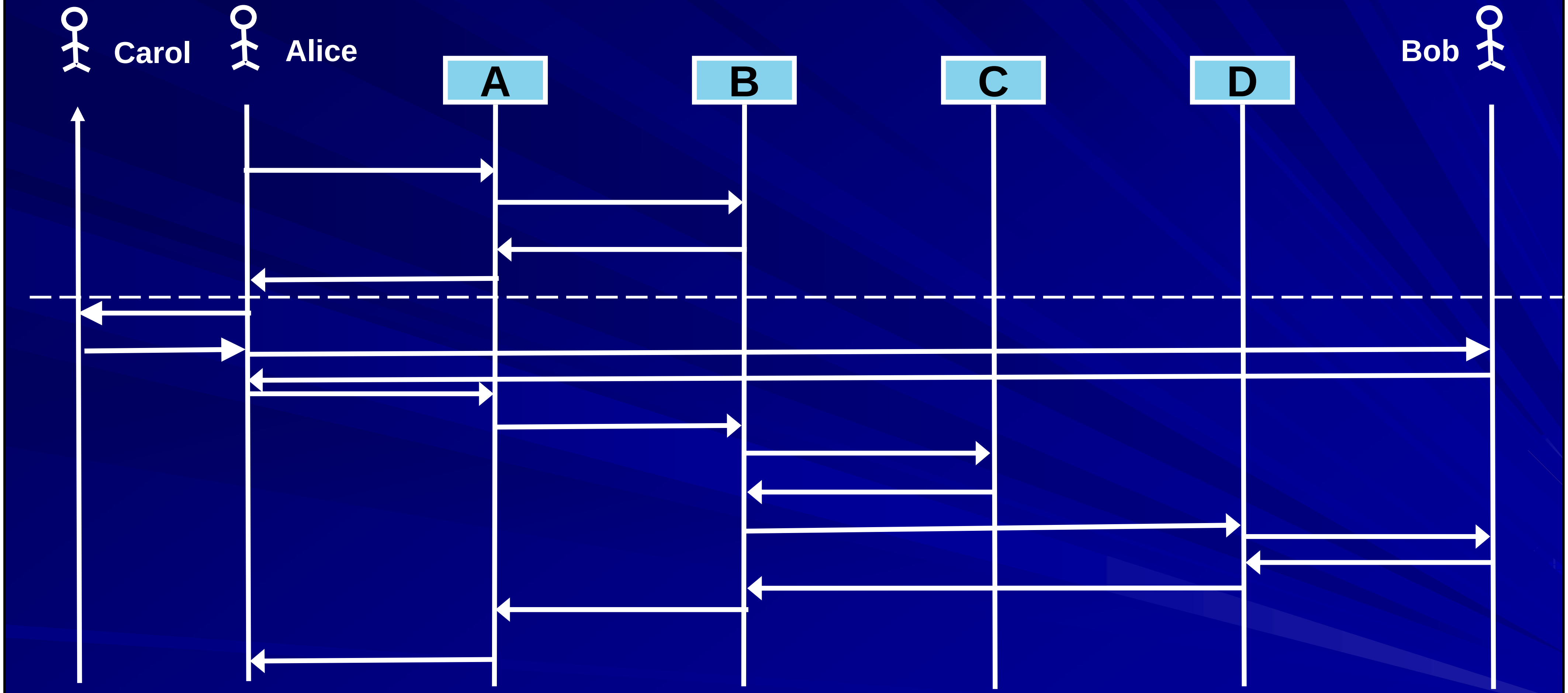
Carl M Ellison
cme@microsoft.com

October 22, 2007

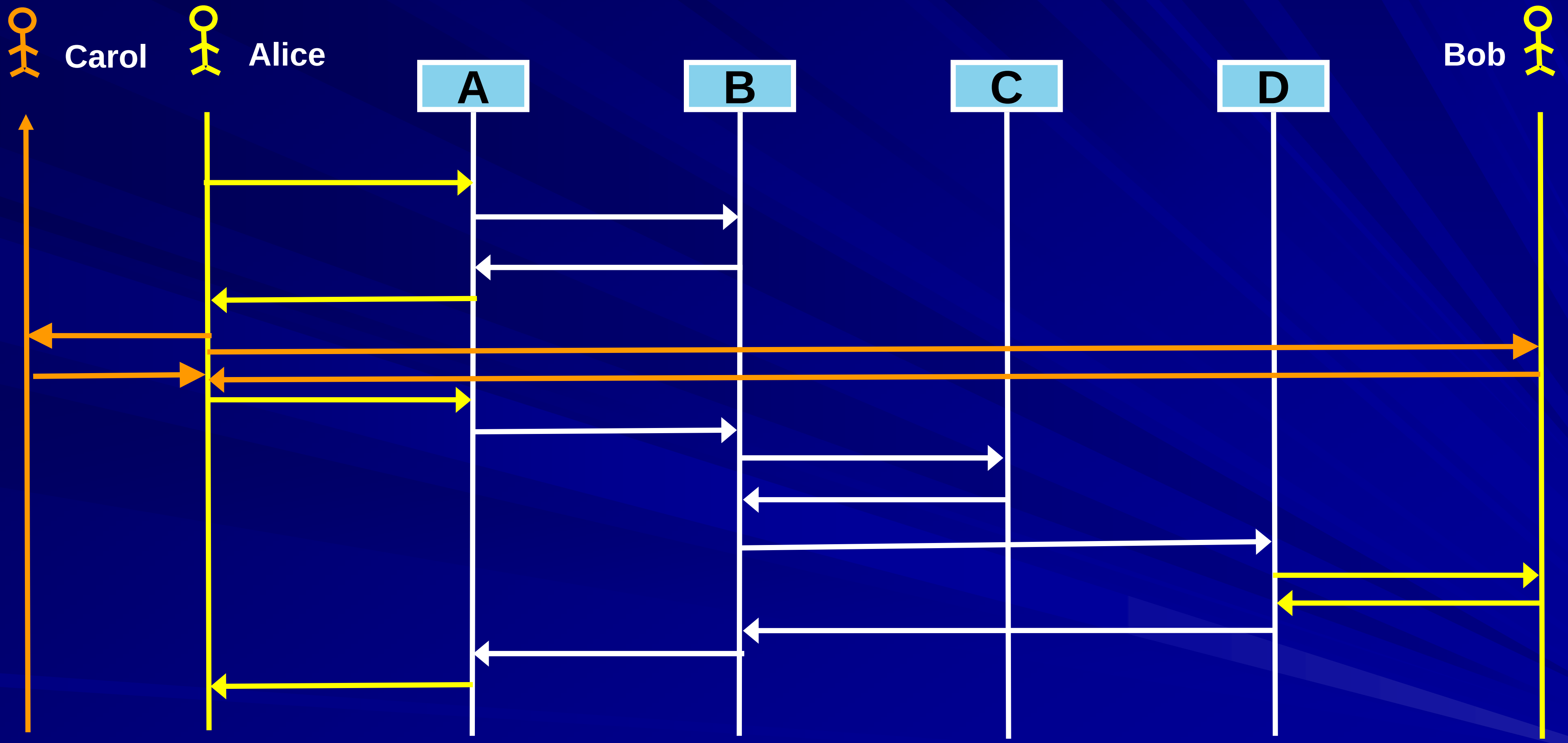
Careful Design

Context

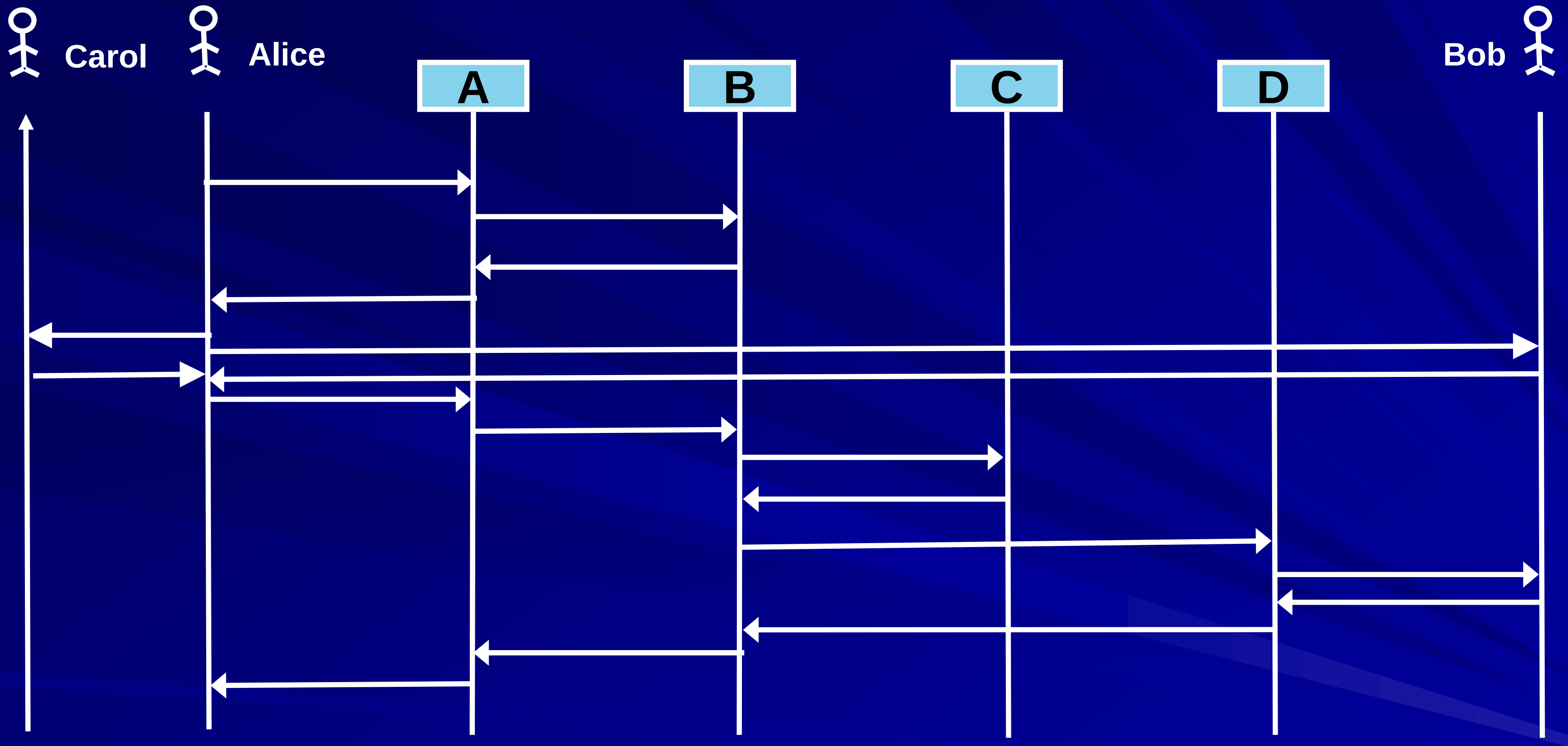
Distributed System



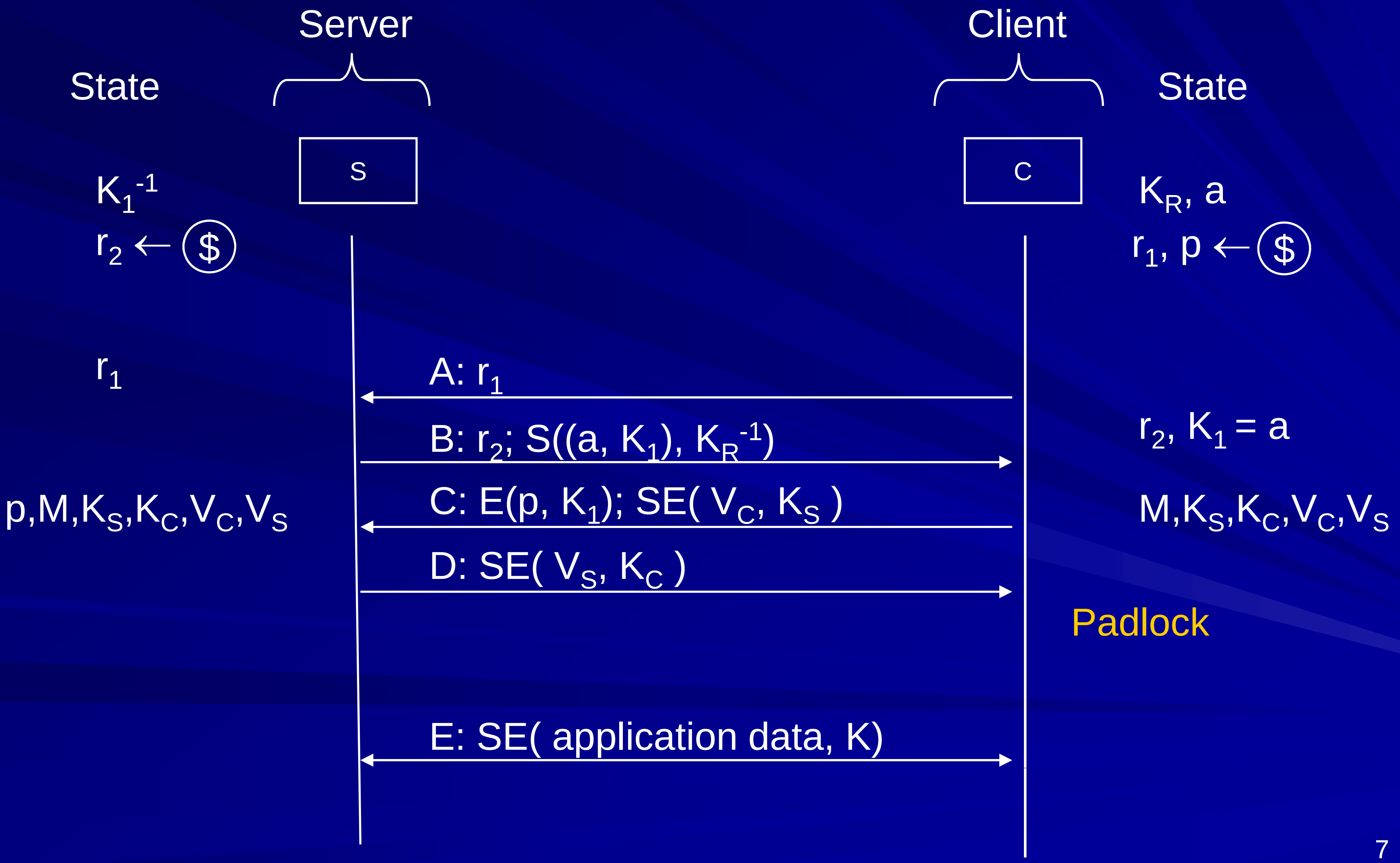
Design Process



The Full System ≡ Ceremony



TLS



Server

Client

State

State

S

C

K_1^{-1}

$r_2 \leftarrow \$$

K_R, a

r_1, p $\leftarrow \$$

r_1

A: r_1

B: r_2; $S((a, K_1), K_R^{-1})$

r_2, $K_1 = a$

C: $E(p, K_1)$; $SE(V_C, K_S)$

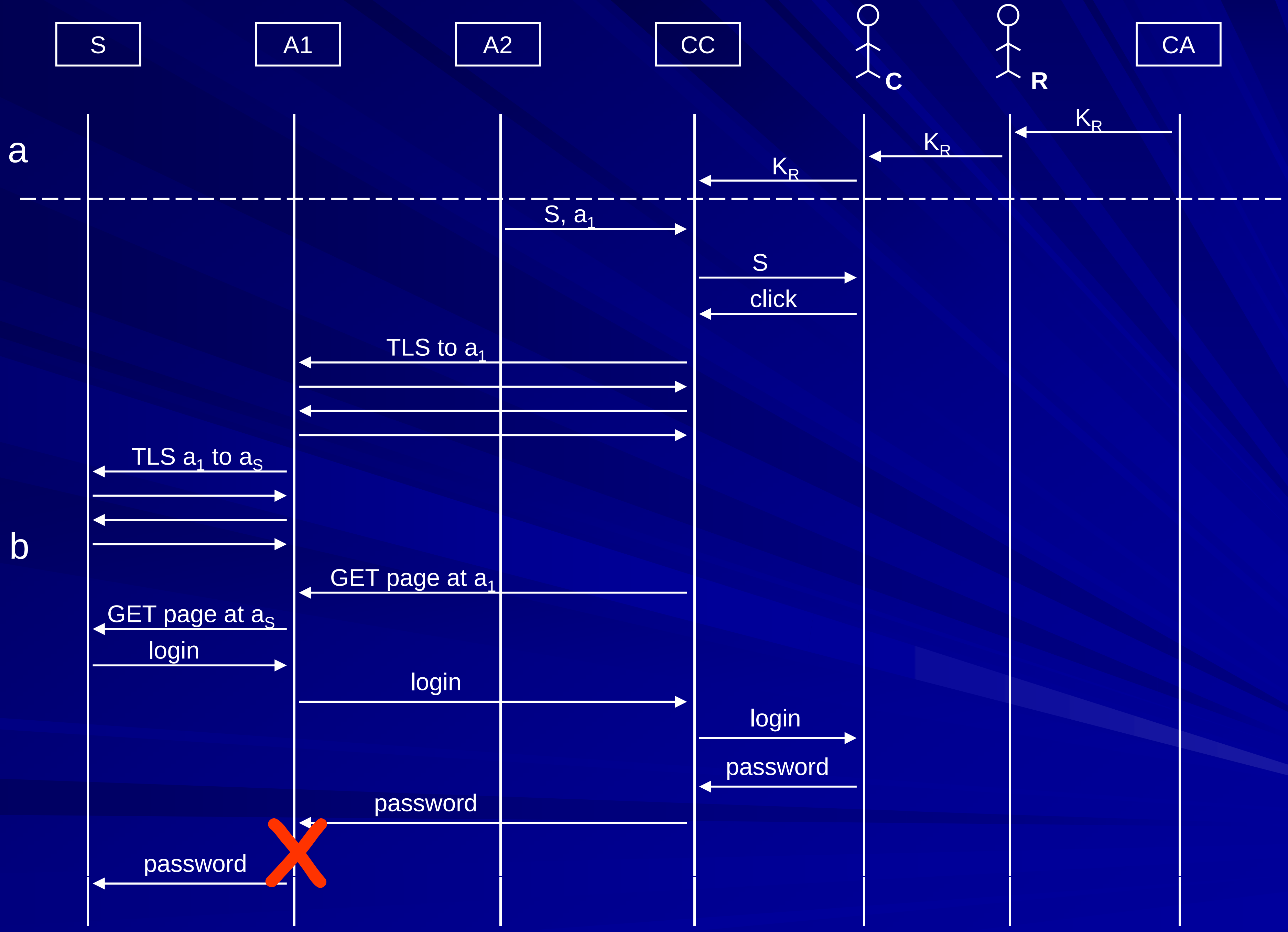
p, M, K_S, K_C, V_C, V_S

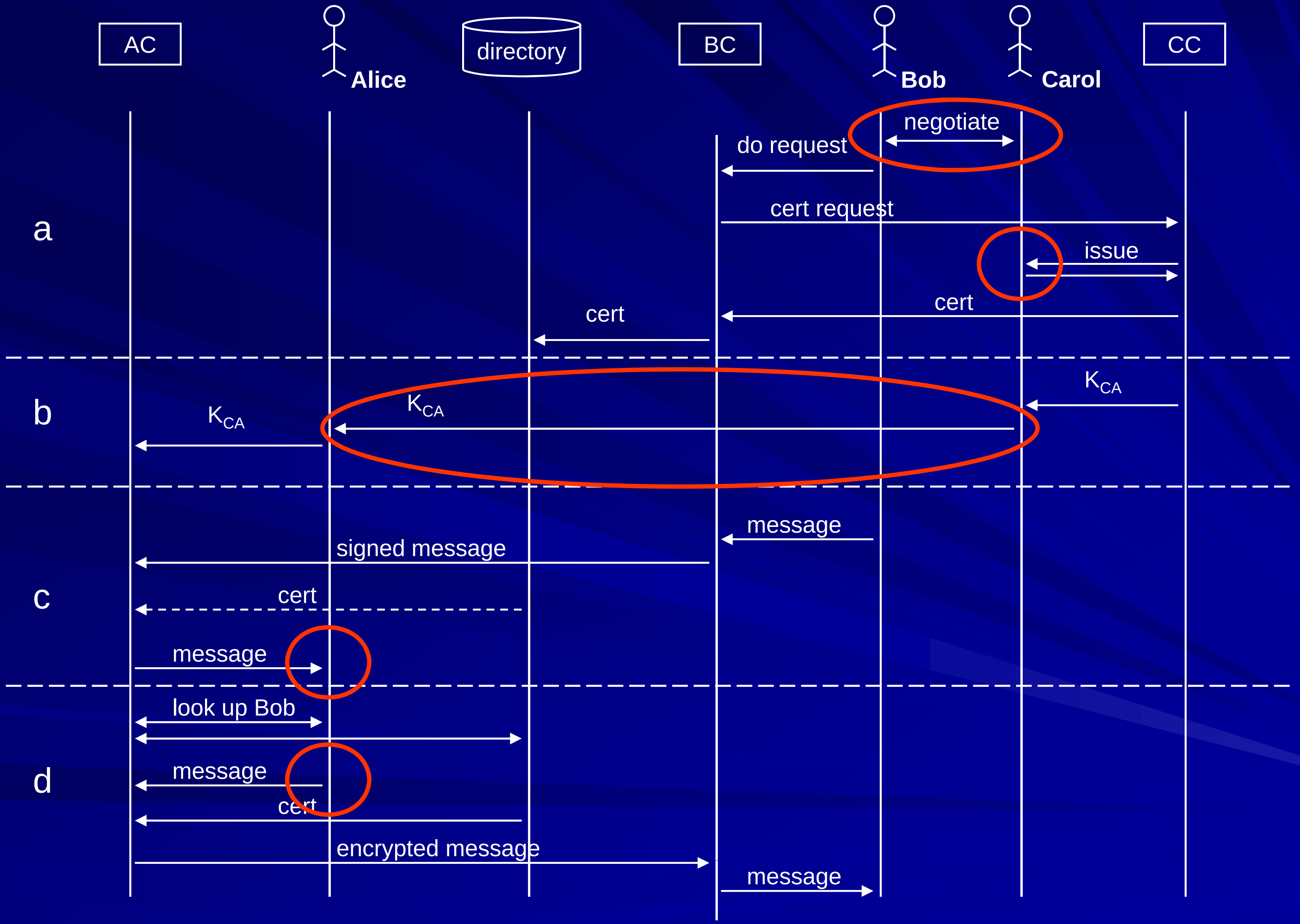
M, K_S, K_C, V_C, V_S

D: $SE(V_S, K_C)$

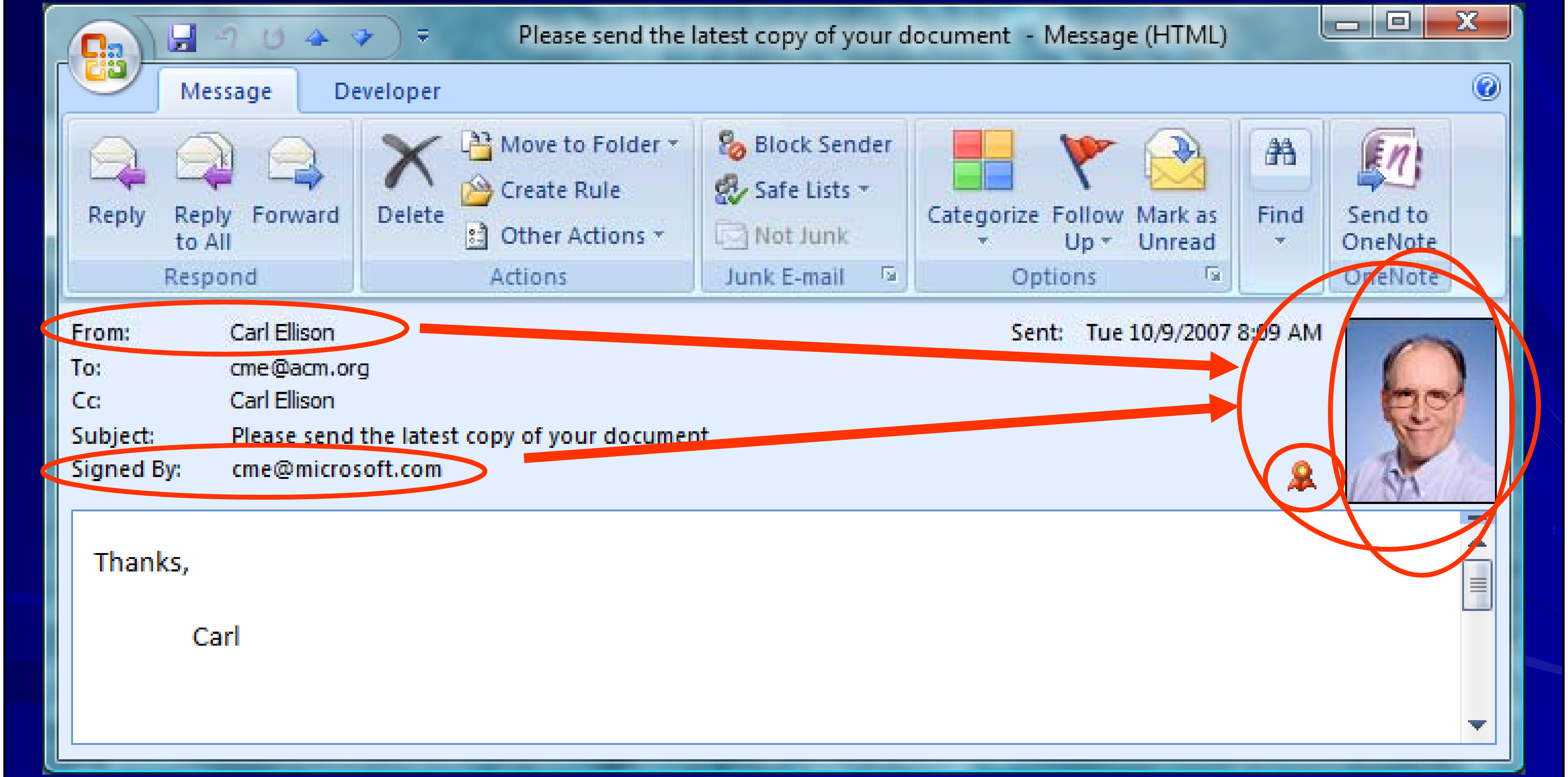
Padlock

E: SE(application data, K)


S
A1
A2
CC
C
R
CA
a
K_R
K_R
K_R
S, a_1
S
click
TLS to a_1
TLS a_1 to a_S
b
GET page at a_1
GET page at a_S
login
login
login
password
password
password


AC
Alice
directory
BC
Bob
Carol
CC
a
negotiate
do request
cert request
issue
cert
cert
b
K_{CA}
K_{CA}
K_{CA}
c
message
signed message
cert
message
d
look up Bob
message
cert
encrypted message
message

Signed E-mail Message



From: Carl Ellison

Sent: Tue 10/9/2007 8:09 AM

To: cme@acm.org

Cc: Carl Ellison

Subject: Please send the latest copy of your document

Signed By: cme@microsoft.com

Thanks,

Carl

UI Design

- UI designers tend to concentrate on beauty and special effects.
- Protocol designers, system programmers and especially cryptographers tend to be very poor UI designers.
  - A sensible company won’t trust them with the paint brush.
- For ceremonies, UI ***must be*** part of the design and analysis.
- So, we need an interdisciplinary team for UI.

Characteristics of Ceremonies

- Ceremonies cover the ***whole*** design
  - – nothing important is out-of-band
    - UI, workflow, key management, provisioning, …
- All protocol analysis techniques apply
  - – security, performance, fault-tolerance, deadlock, race, realizability, formal methods…
- Human node modeling ≠ usability study
  - – correctness >> appeal, enjoyment
  - – learn the human state machine empirically

Node Model

- State
- State machine
- Events (timer, desire, …)
- Input messages
- Output messages
- Memory
  - Tamper resistance
  - Secrets

Meaningful IDs

- A ***meaningful ID for user X*** is one that calls to user X’s mind the correct identified entity.
- If you use IDs and want correct ceremony behavior, they must be meaningful IDs.
- A global ID is almost never meaningful.
- Meaningful IDs are probably held in a personal dictionary, built by that user and translating from/to a global ID.

Better Ceremony Designs

- Physical key metaphor
  - – Bank crypto module key management
  - – STU-III ignition key
  - – USB devices for machine introduction
- Meaningless values
  - – Clipper phone verification (AuthN by voice)
  - – UPnP™ Security Ceremonies

Conclusions

- Ceremonies cover the whole design.
- All protocol analysis techniques work on ceremonies.
- The design is yours, but you are given the human nodes. You must learn their programming – or design around them.
- The field is wide open for both invention and analysis.

Q & A

- For more details, see:
- http://eprint.iacr.org/2007/399

Microsoft®

Your potential. Our passion.™

© 2007 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.