Today

⇒ * Security implementation in AFS

Wednesday

- Wrap up

Friday

- Townhall

Final Exam

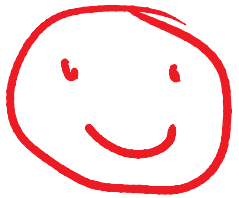
- Wed @ 8 AM (12/9)

C105 Score Card

Spring 2015

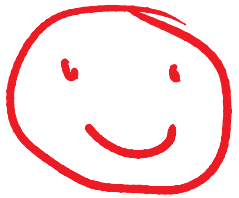
C105 Score Card

Spring 2015 100%.



CIOS Score Card

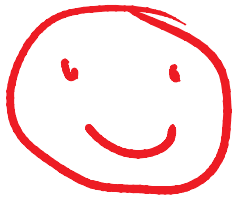
Spring 2015 100%



Fall 2015 33%
(So far)

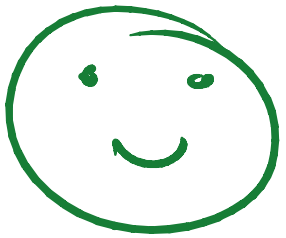
CIOS Score Card

Spring 2015 — 100%



Fall 2015 — 33% (so far)

By next week — 100%



Challenges for Andrew System

Authenticate User

Authenticate Server

Prevent replay attacks

isolate users

Choice in Andrew: private key crypto system
⇒ identity of sender in cleartext

Traditional Unix: username, password
— overuse of Lotk security hole

Dilemma: What to use as identity and Private Key?

Andrew solution

- username and password only for login
- use ephemeral id and keys for subsequent venus-vize communication

Andrew solution

- username and password only for login
- use ephemeral id and keys for subsequent Venus-Vice communication

Three classes of client-server interaction

- login
- RPC session establishment
- file system access during session

Andrew solution

- username and password only for login
- use ephemeral id and keys for subsequent Venus-Vice communication

Three classes of client-server interaction

- login ⇒ username, password
- RPC session establishment
- file system access during session

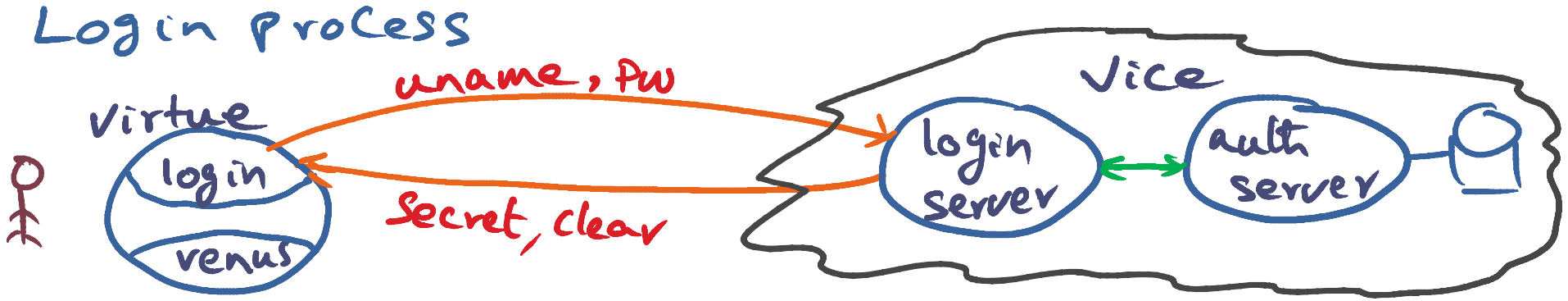
Andrew solution

- username and password only for login
- use ephemeral id and keys for subsequent Venus-Vice communication

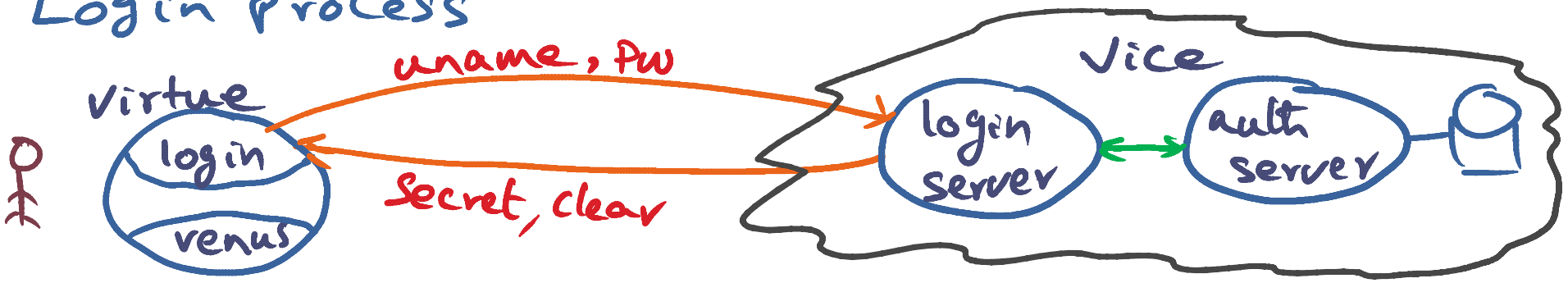
Three classes of client-server interaction

- login ⇒ username, password
- RPC session establishment
- file system access during session

} both use ephemeral id and keys


Login process
Virtue
login
venus
uname, PW
Secret, clear
Vice
login server
auth server

Login process



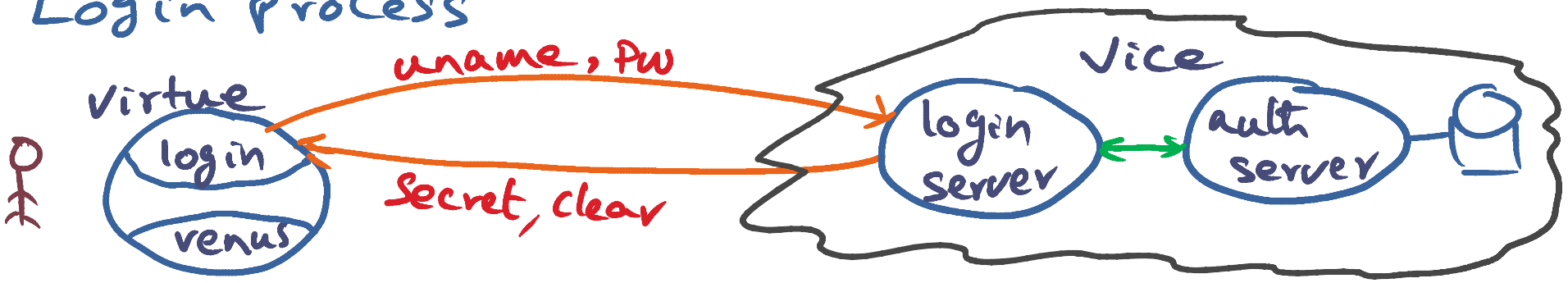
Cleartoken: Data structure

⇒ Extract handshake key client (HKC)

Secrettoken: cleartoken encrypted with key

known only to vice

Login process



Cleartoken: Data structure

⇒ Extract handshake key client (HKC)

Secrettoken: cleartoken encrypted with key

known only to vice

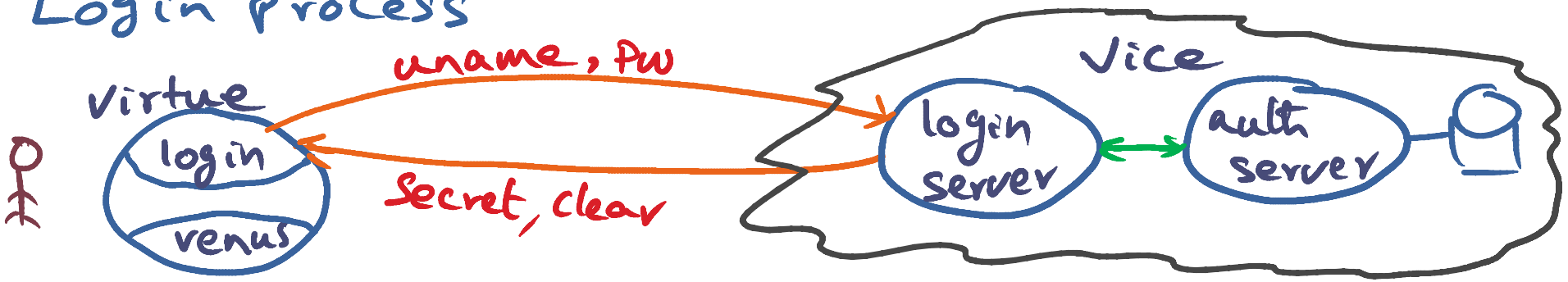
⇒ unique for this login session

⇓

use as ephemeral client-id

for this login session

Login process



Cleartoken: Data structure

⇒ Extract handshake key client (HKC)

Secrettoken: cleartoken encrypted with key known only to vice

⇒ unique for this login session

⇓

use as ephemeral client-id for this login session

use HKC as private key for establishing a new RPC session

Venus – Vice Communication

Authenticate User

Authenticate Server

Prevent replay attacks

Venus – Vice Communication

Authenticate User

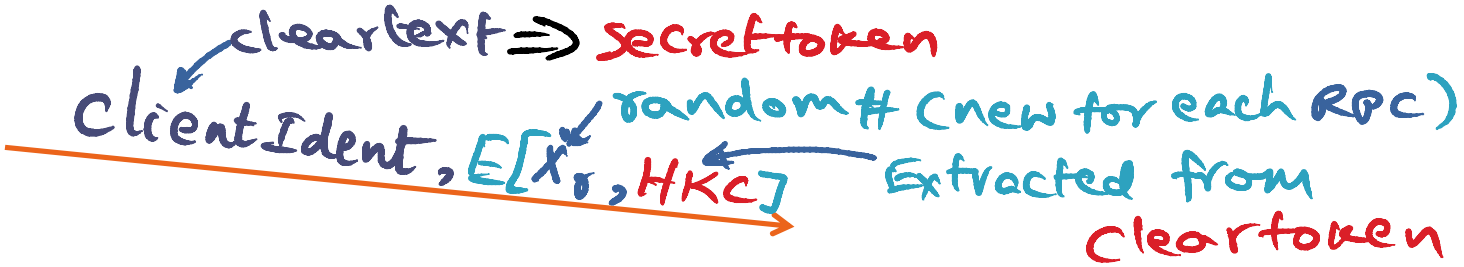
Authenticate Server

Prevent replay attacks

⟹ Bind at Core of this Communication

RPC Session establishment (Bind client-server)

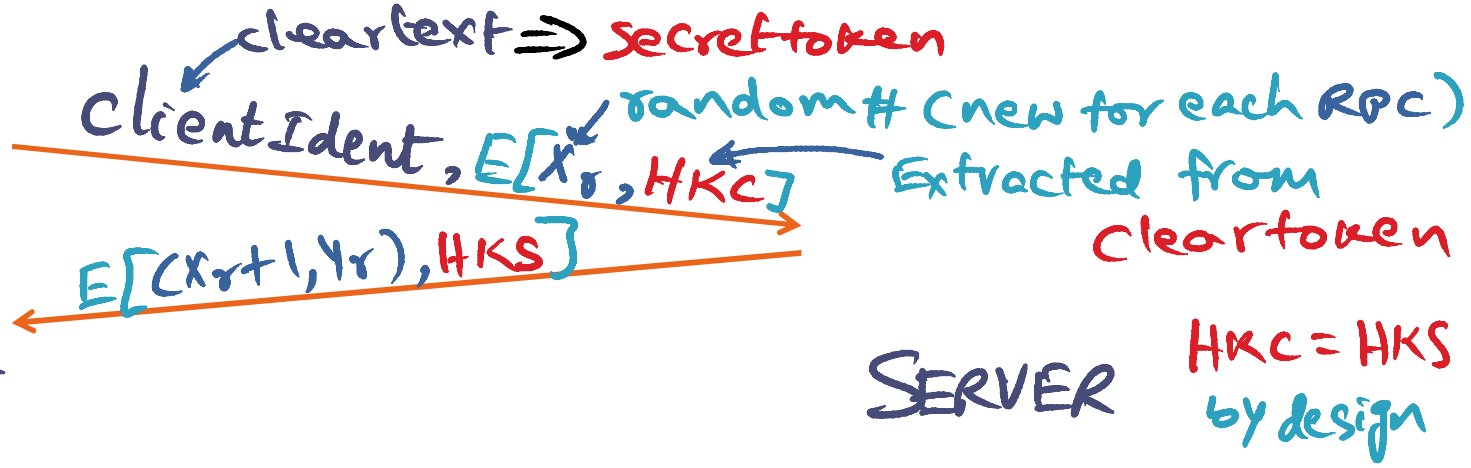
RPC Session establishment (Bind client-server)



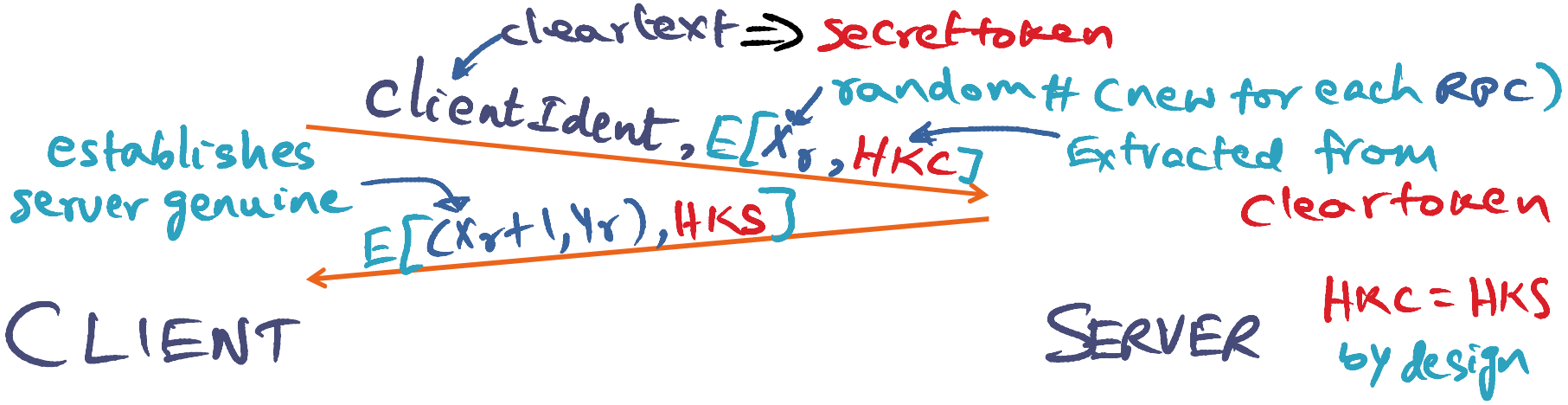
CLIENT

SERVER

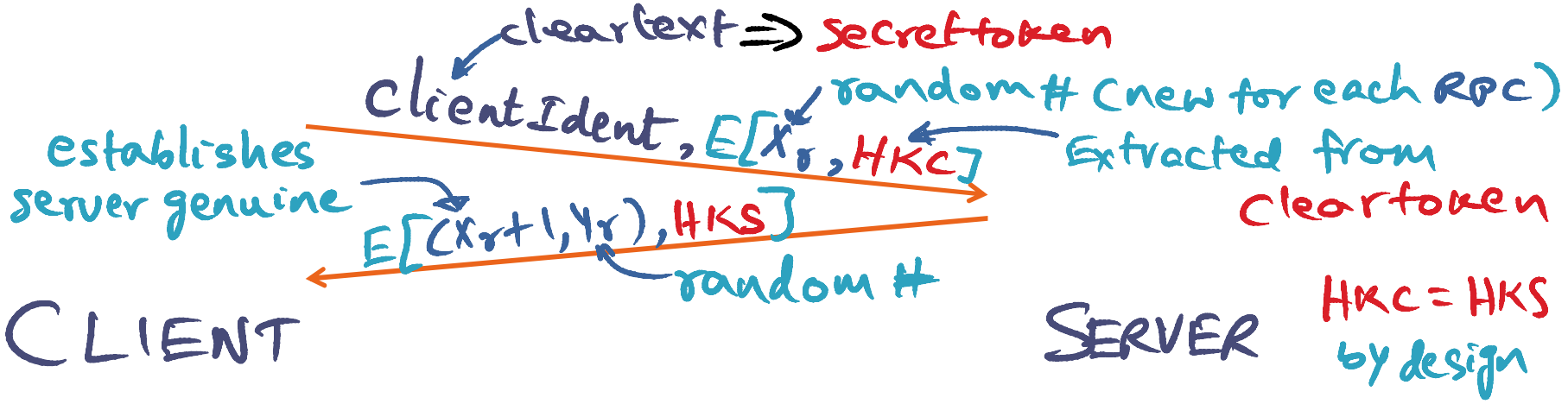
RPC Session establishment (Bind client-server)



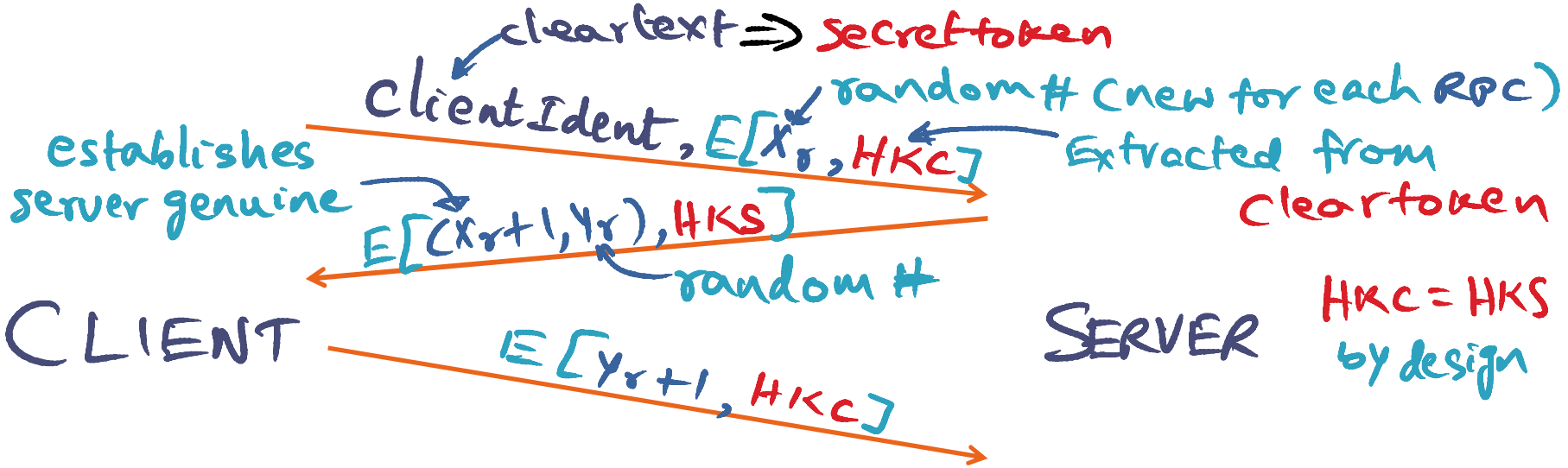
RPC Session establishment (Bind client-server)



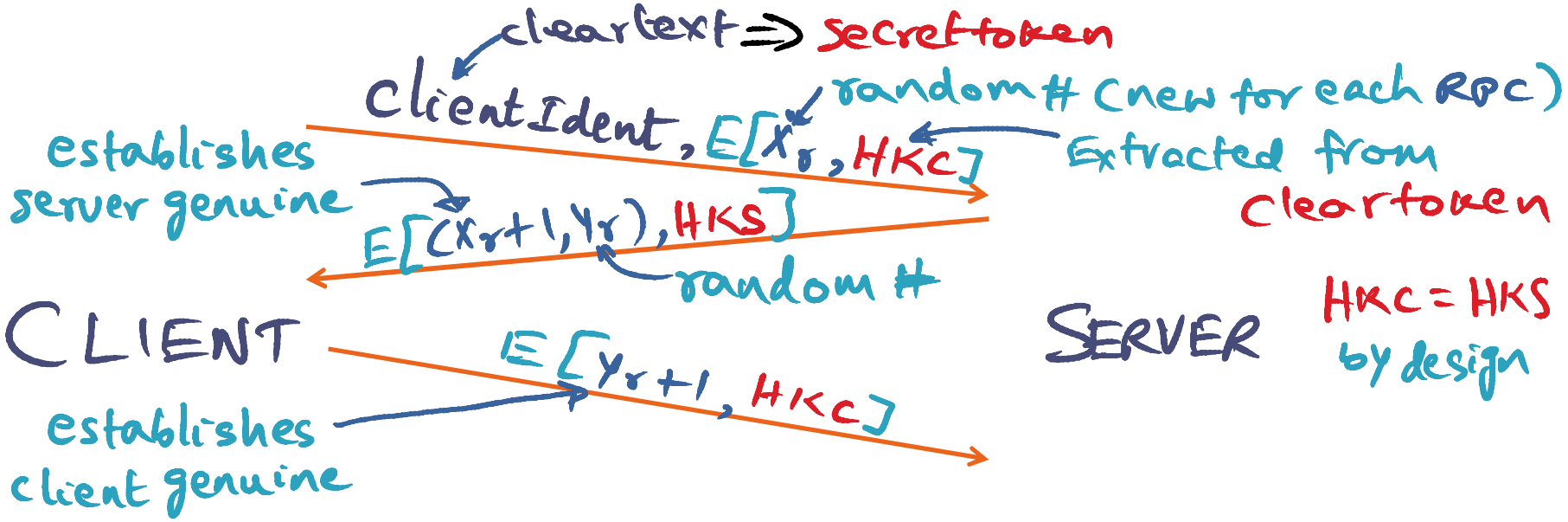
RPC Session establishment (Bind client-server)



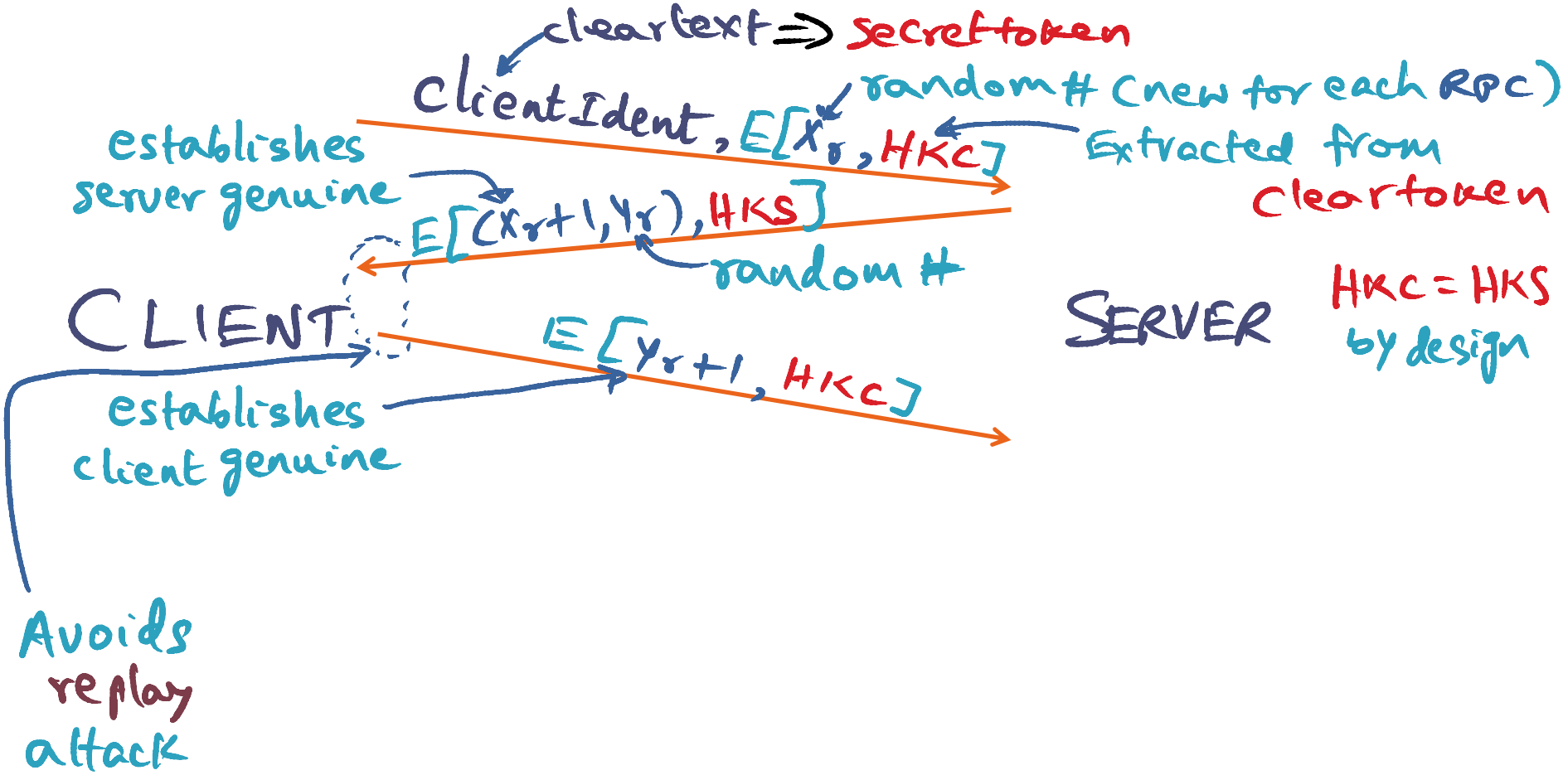
RPC Session establishment (Bind client-server)



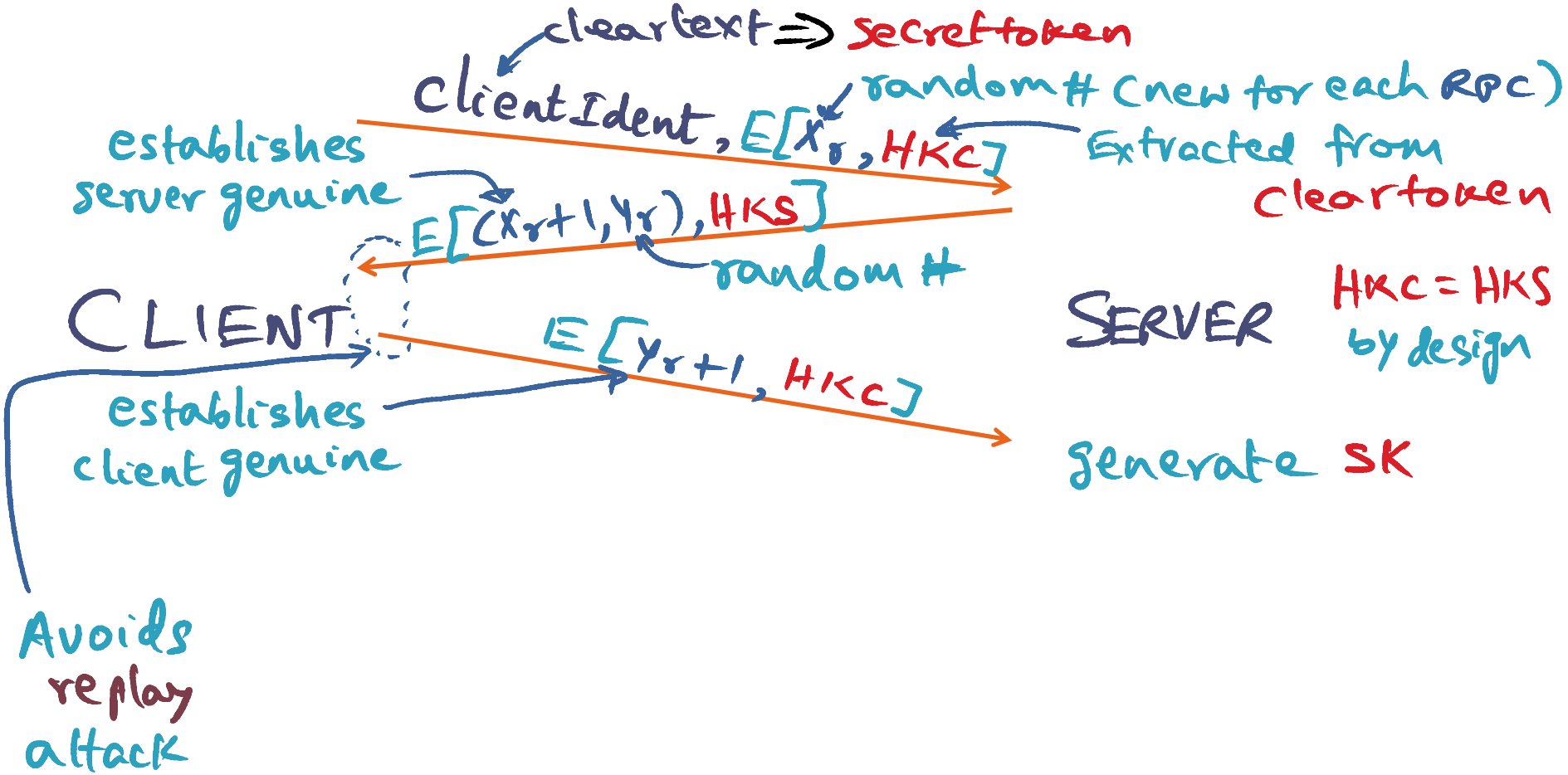
RPC Session establishment (Bind client-server)



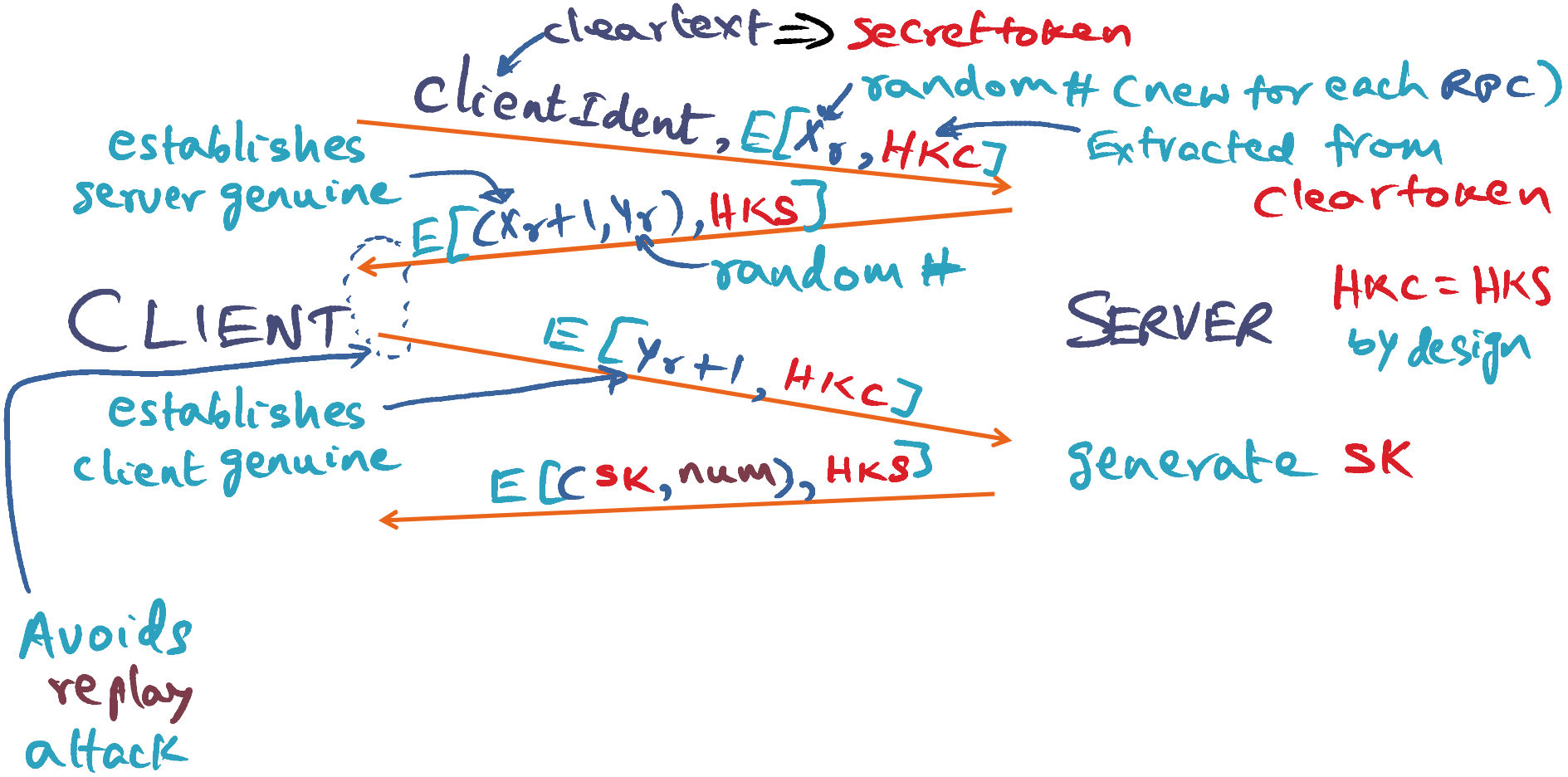
RPC Session establishment (Bind client-server)



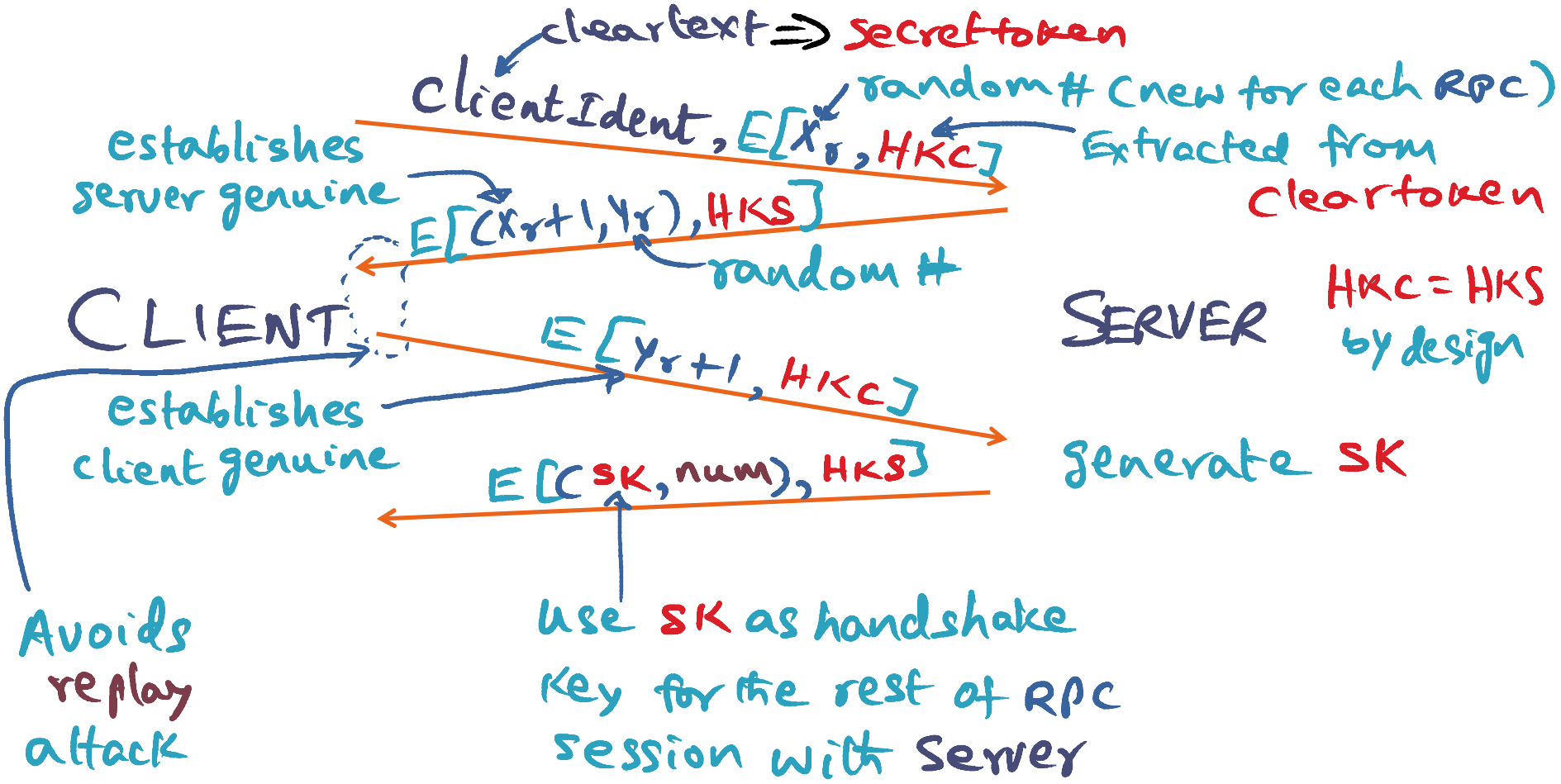
RPC Session establishment (Bind client-server)



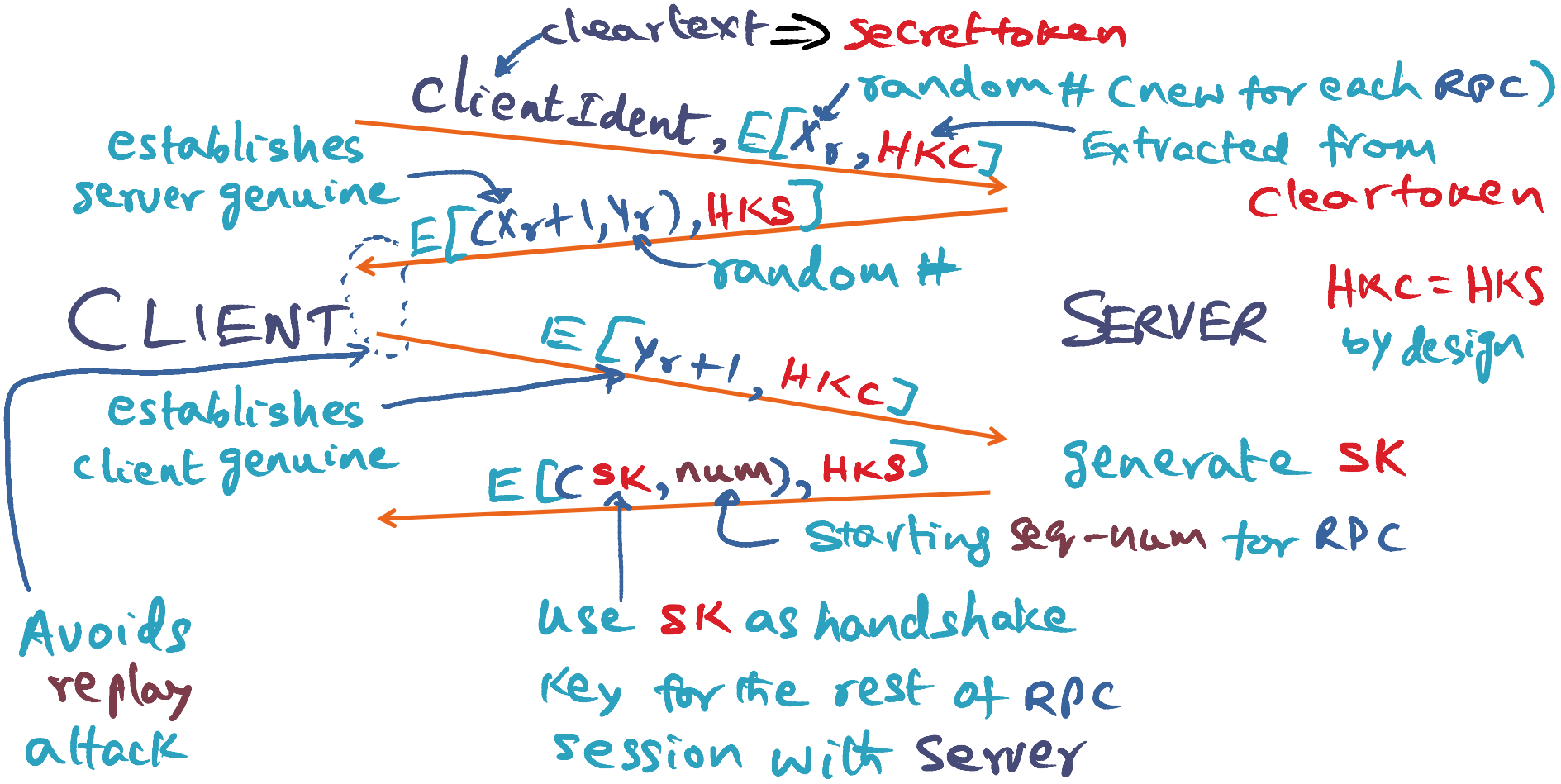
RPC Session establishment (Bind client-server)

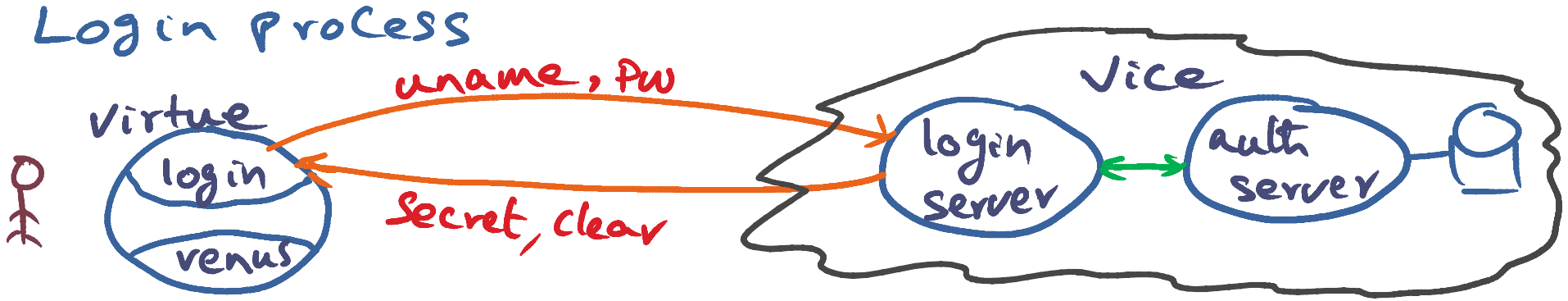


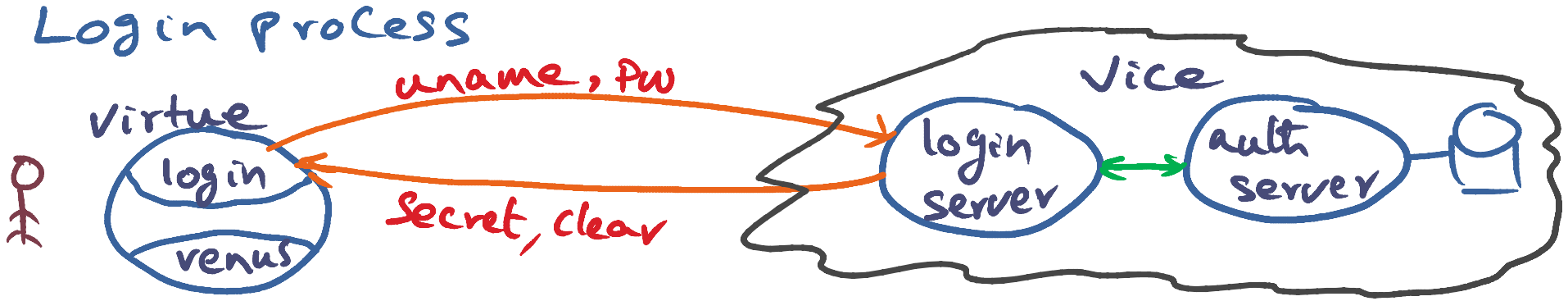
RPC Session establishment (Bind client-server)



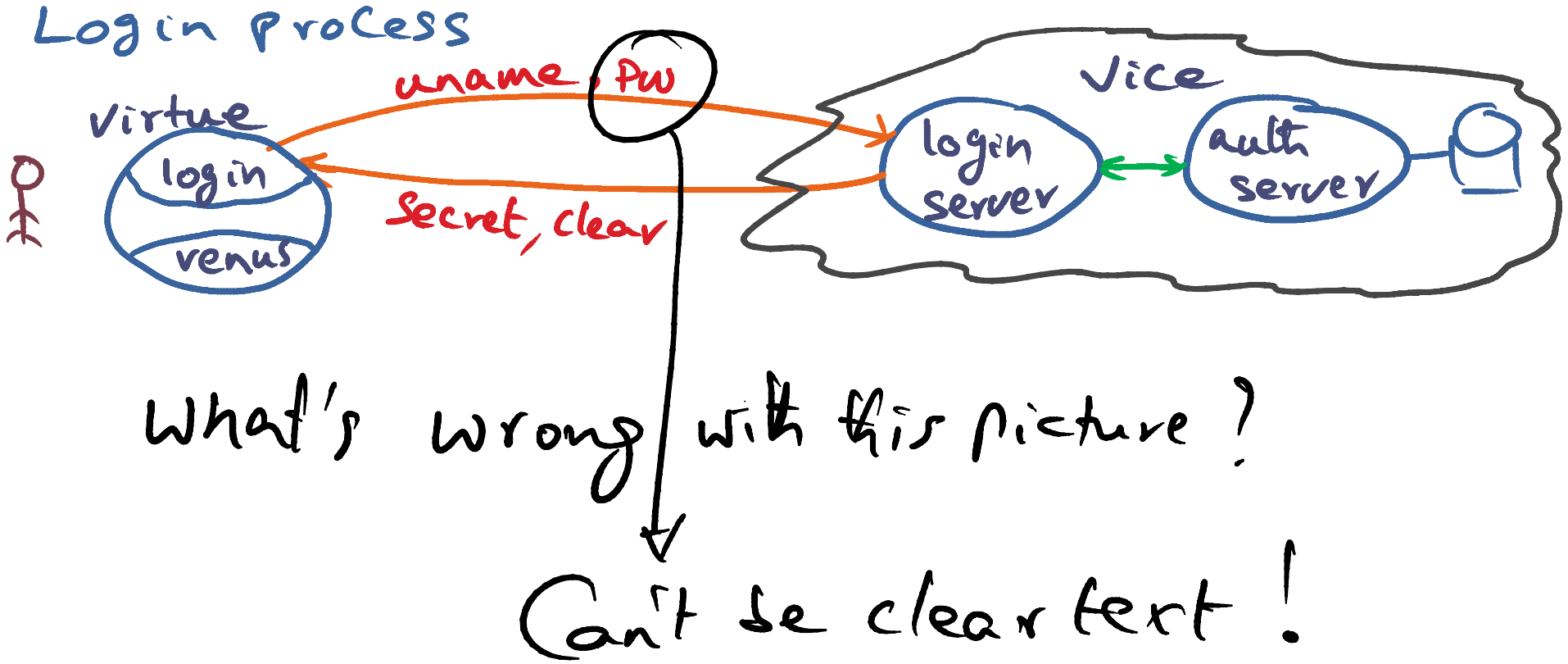
RPC Session establishment (Bind client-server)




Login process
Virtue
login
venus
uname, PW
Secret, clear
Vice
login server
auth server



What's wrong with this picture?


Login process
uname, PW
Virtue
login
venus
Secret, clear
Vice
login server
auth server
What's wrong with this picture?
Can't be clear text!

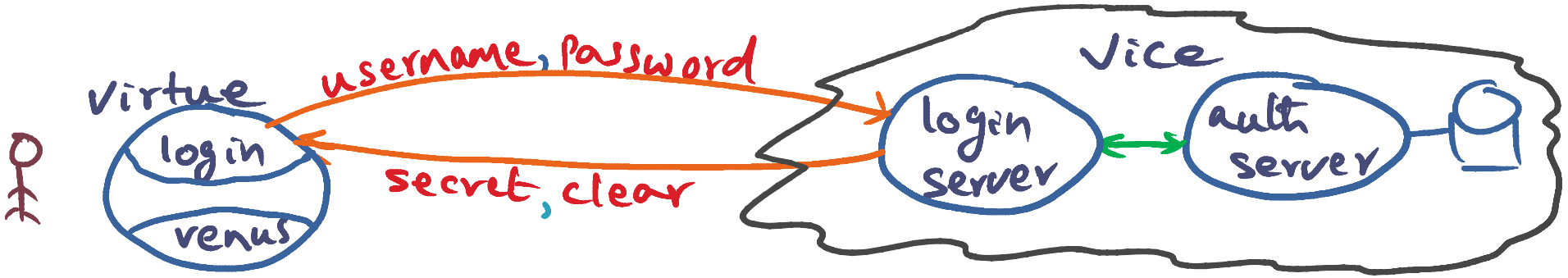
Login is a special case of Bind

- Password used as HKC
- username used for ClientIdent

Login is a special case of Bind

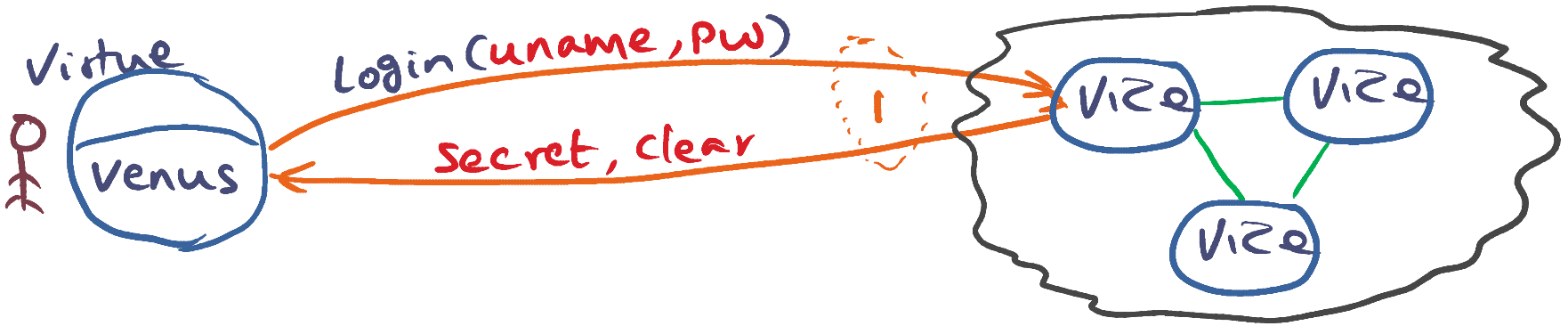
- Password used as HKC
- username used for ClientIdent
- get back two tokens

  SecretToken } encrypted with
  ClearToken } Password

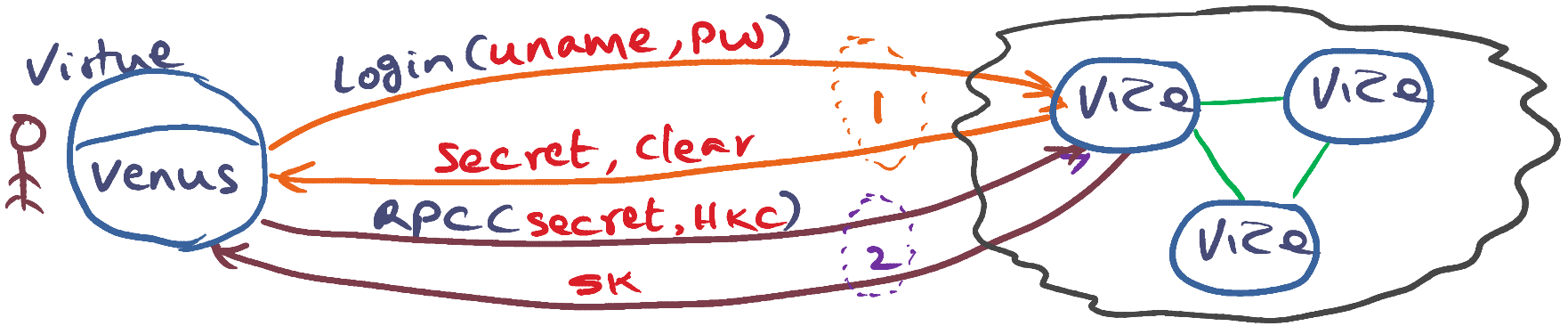


- tokens kept by venus for this login session

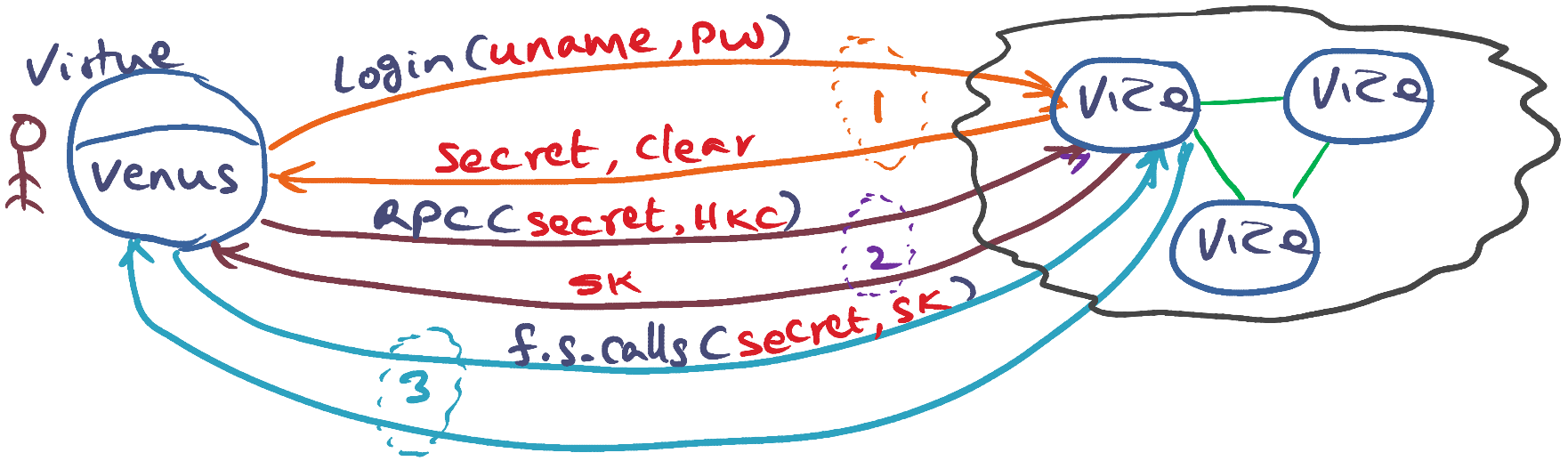
Putting it all together



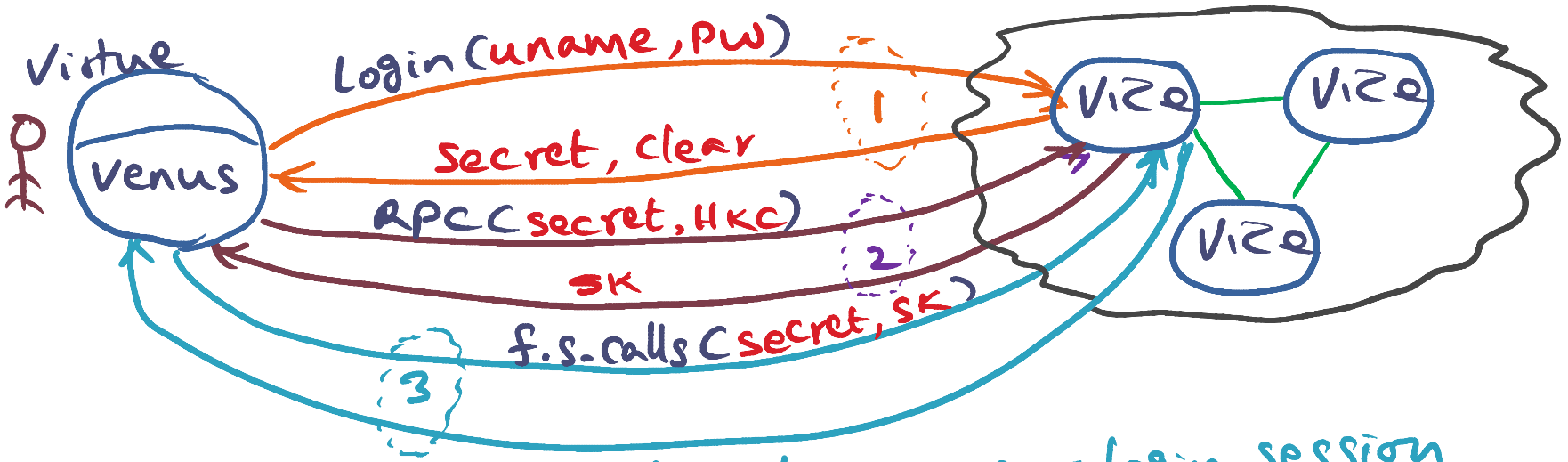
Putting it all together



Putting it all together

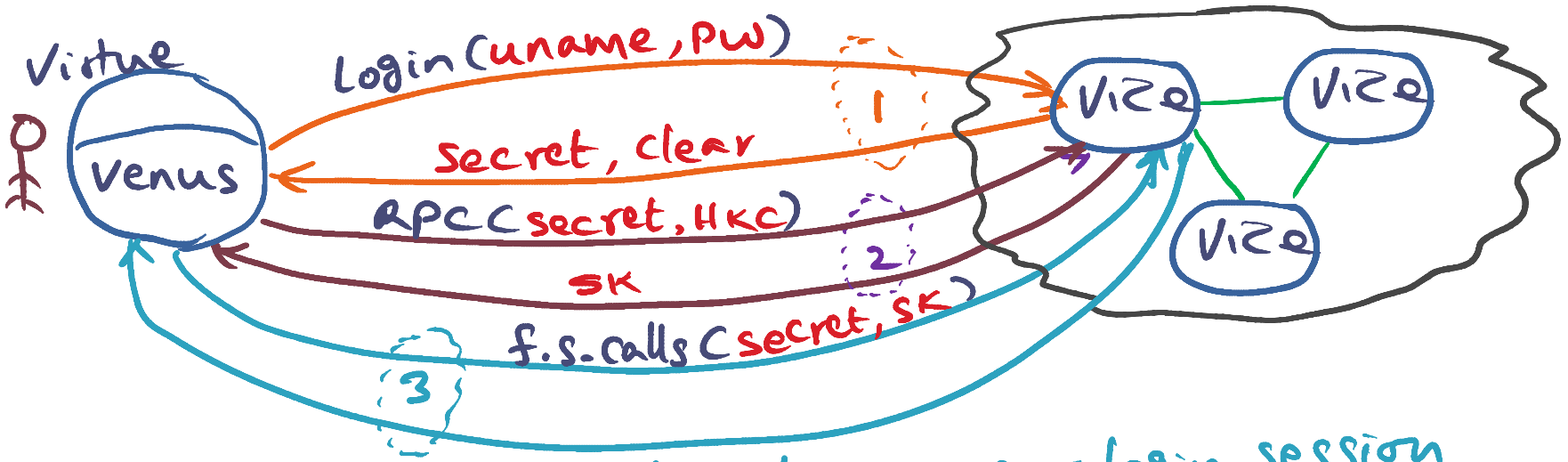


Putting it all together



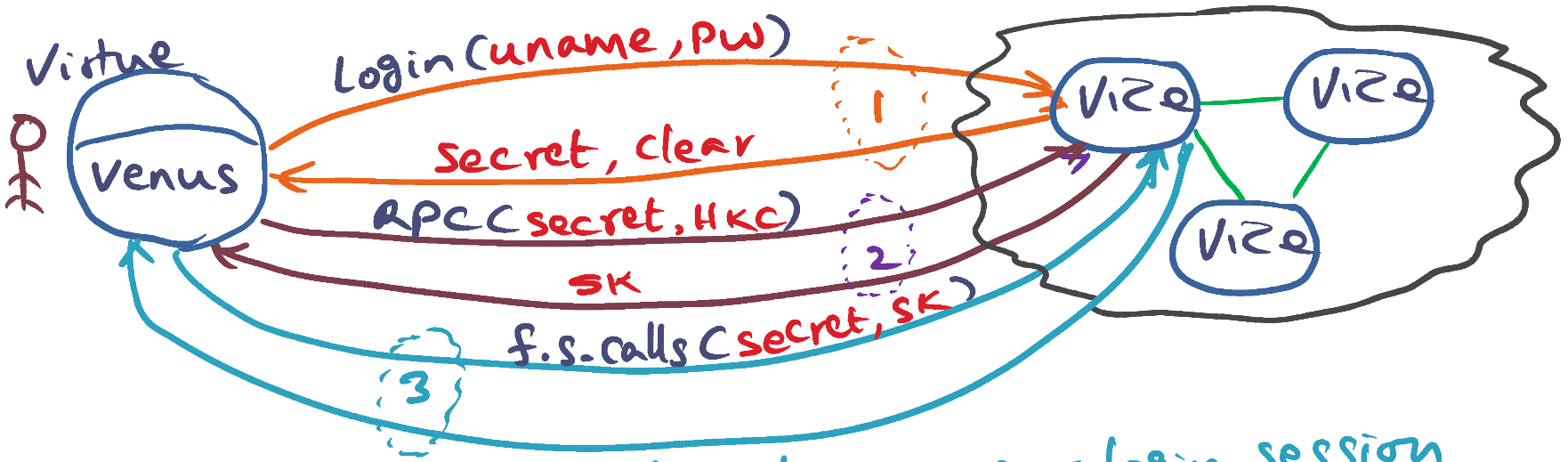
– (uname, PW) exposed only once per login session

Putting it all together



- (uname, PW) exposed only once per login session
- HKC used only for a new RPC session

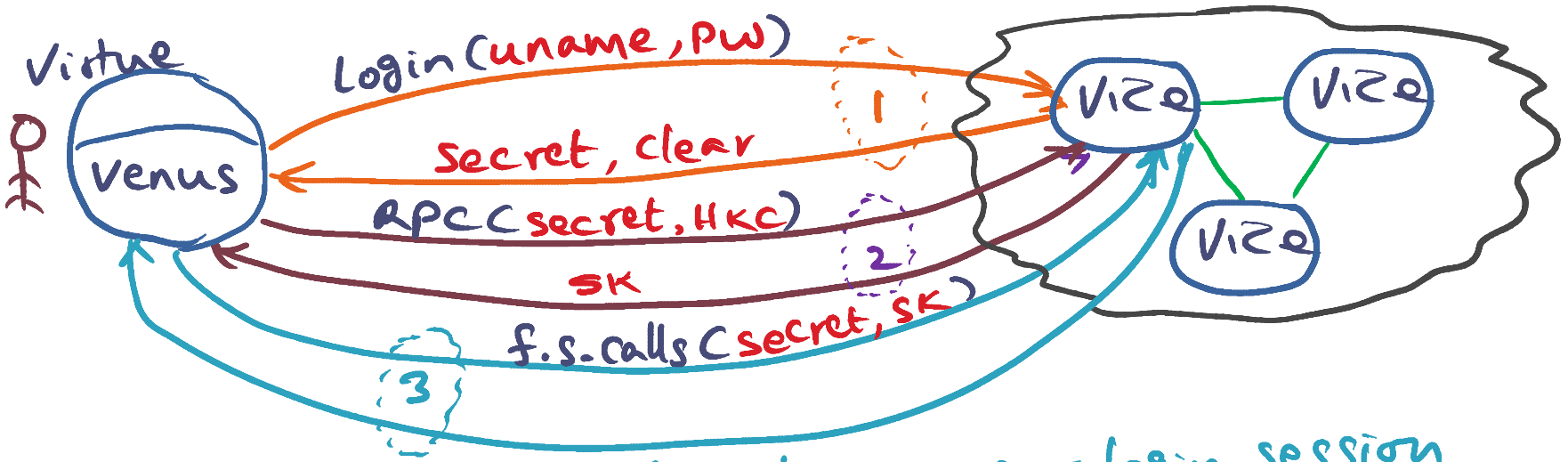
Putting it all together



- (uname, PW) exposed only once per login session
- HKC used only for a new RPC session

duration of login session validity

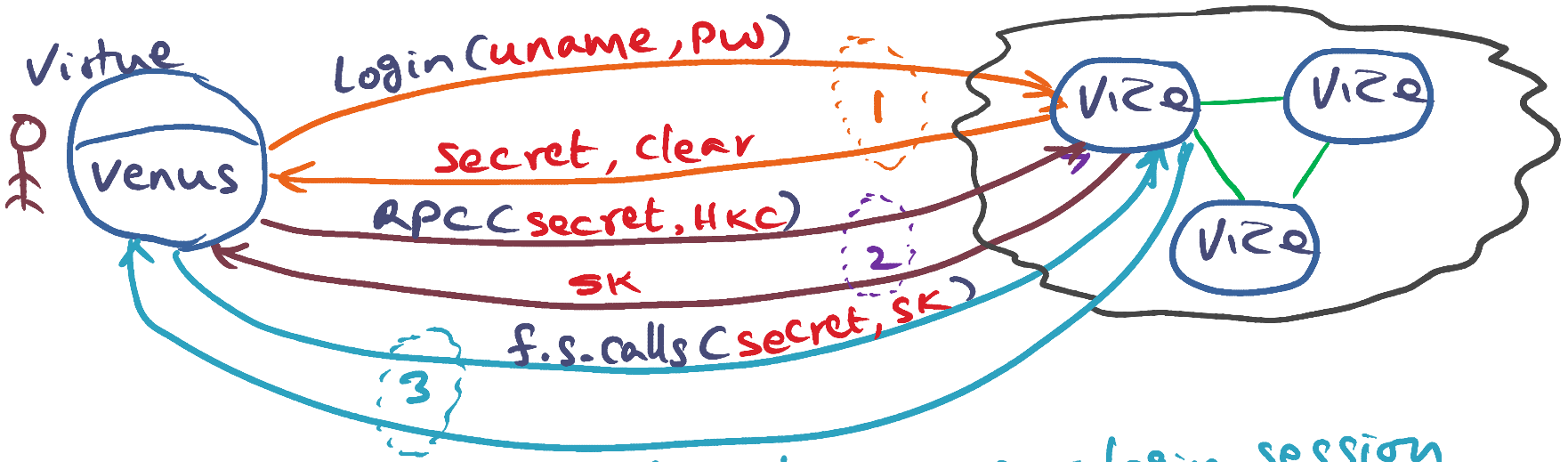
Putting it all together



- (uname, PW) exposed only once per login session
- HKC used only for a new RPC session
- SK for all Rpc calls to file System

↳ duration of login session validity

Putting it all together



- (uname, PW) exposed only once per login session
- HKC used only for a new RPC session
- SK for all Rpc calls to file System
  - → duration of RPC session validity

→ duration of login session validity

Group Activity : AFS security Report Card

Mutual Suspicion

☐ yes ☐ NO

Protection from System for Users

☐ yes ☐ NO

Confinement of resource usage

☐ yes ☐ NO

Authentication

☐ yes ☐ NO

Server integrity

☐ yes ☐ NO

AFS security Report Card

Mutual suspicion
- [x] yes
- [ ] NO

} yes from fellow users

Protection from system for users
- [ ] yes
- [x] NO

} gotta trust!

Confinement of resource usage
- [ ] yes
- [x] NO

} NW BW DOS attacks

Authentication
- [x] yes
- [ ] NO

} validation of client-server

Server integrity
- [ ] yes
- [x] NO

} Physical + social moves

Another group Activity

Features of AFS Compared to Vanilla NFS ??

Key takeaways

- Andrew file system has features that extend the vanilla privilege levels provided by the Unix file system semantics.
- Further it also introduces the notion of audit trail for system administrators modifying the system.
- OS designers we can take the "best solution" that is out there for information security and implement a secure and usable distributed system.
- benchmark solution against the design principles laid out by Saltzer for information security