Advanced Lecture on Internet Infrastructure
6. IP Security

Masataka Ohta

mohta@necom830.hpcl.titech.ac.jp

ftp://ftp.hpcl.titech.ac.jp/infra6e.ppt

Better Security

- IPv6 mandates IPsec
  - should be able to disable DoS with IPsec authentication
- IPsec needs cryptographic keys configured
  - not useful for packets from unknown origins

True Security

- end to end security
  - the principle of the Internet or networking in general
- to make all the ends secure
  - there is no royal road
  - there is no magic

End to End Argument in Original Paper by Saltzer et. al.

http://groups.csail.mit.edu/ana/Publications/PubPDFs/End-to-End%20Arguments%20in%20System%20Design.pdf

- The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)

ILOVEYOU

- once famous macro virus
  - attack vulnerability of “intelligent” applications
    - automatically execute programs attached to a mail
- pass all the firewalls at that time and VPNs
- mitigations
  - never use “intelligent” applications and OSes
    - often produced by Microsoft
  - virus checker may be useful to some extent

What is Security?

- secrecy
  - hide information from third parties
  - encryption
- authentication
  - certify permission
- mutually related
  - information for authentication must be secret
  - secret information may be offered to authenticated person

Methods of Encryption

- by shared secret key
  - encrypted text=E(plain text, secret key)
  - plain text=D(encrypted text, secret key)
- by public key
  - encrypted text=E(plain text, public key)
  - plain text=D(encrypted text, secret key (private key))

Methods of Authentication

- use hash function (pseudo random number)
- by shared secret key
  - authentication info=H(plain text, secret key)
- by public key
  - authentication info=A(H(plain text), private key)
  - D(authentication infor, H(plain text), public key)

Weak Security

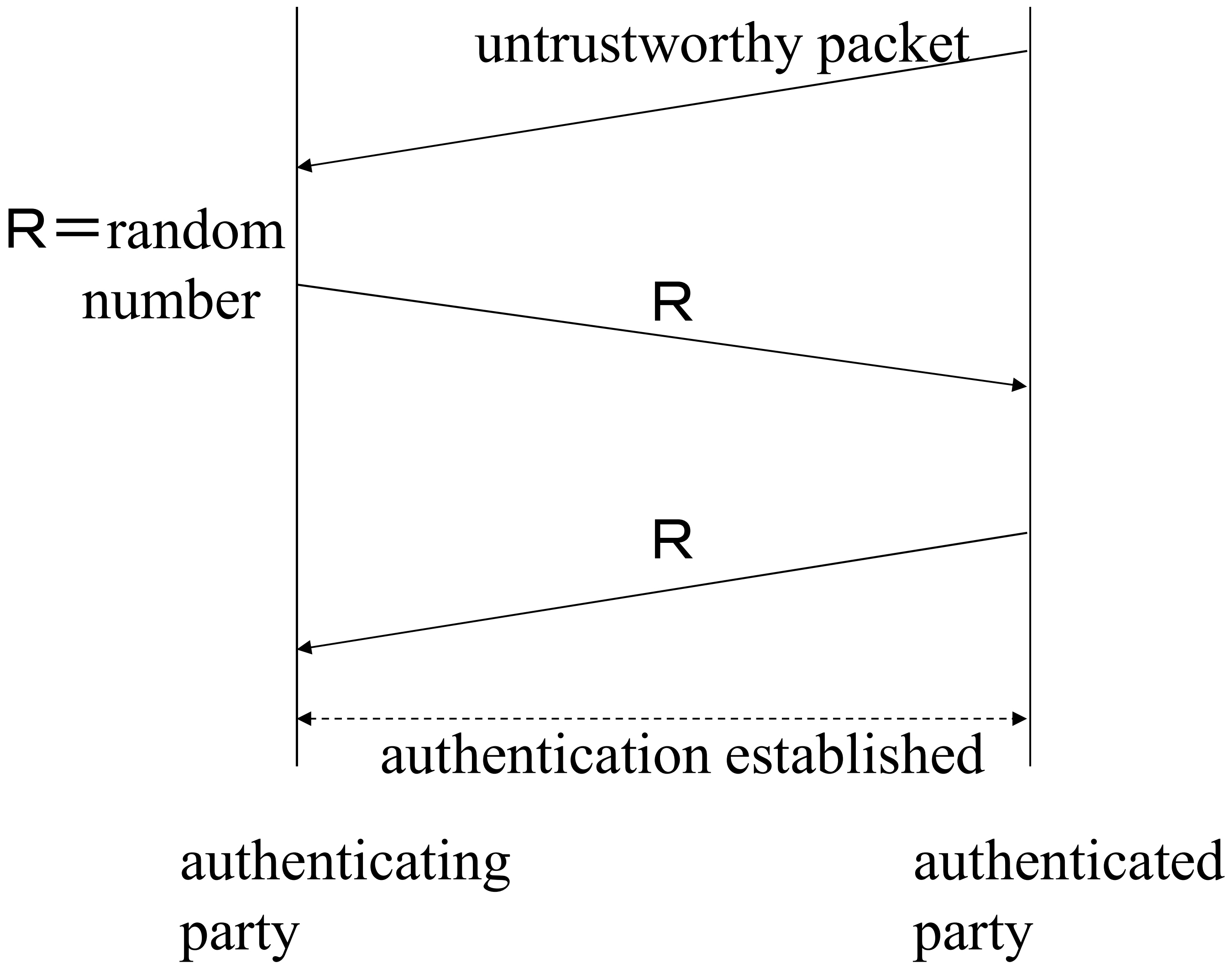
- security relying on infrastructure offered by third parties
  - if ISPs are reliable, packet is delivered to a host with the destination address, without being tapped or modified
  - ISPs may tap or modify packets
- similar to security of phone network
  - telcos may tap or modify conversation
- similar to security of PKI

Security of Phone Network

- assume phone companies are trustworthy
  - call is connected to peer specified by phone number
  - no wiretapping en route
  - can identify peer by phone number
    - rely phone number of peer provided by telco
    - phone number told be peer is not reliable
      - can be confirmed by calling back
- trustworthiness is just an assumption

Weak Security of the Internet

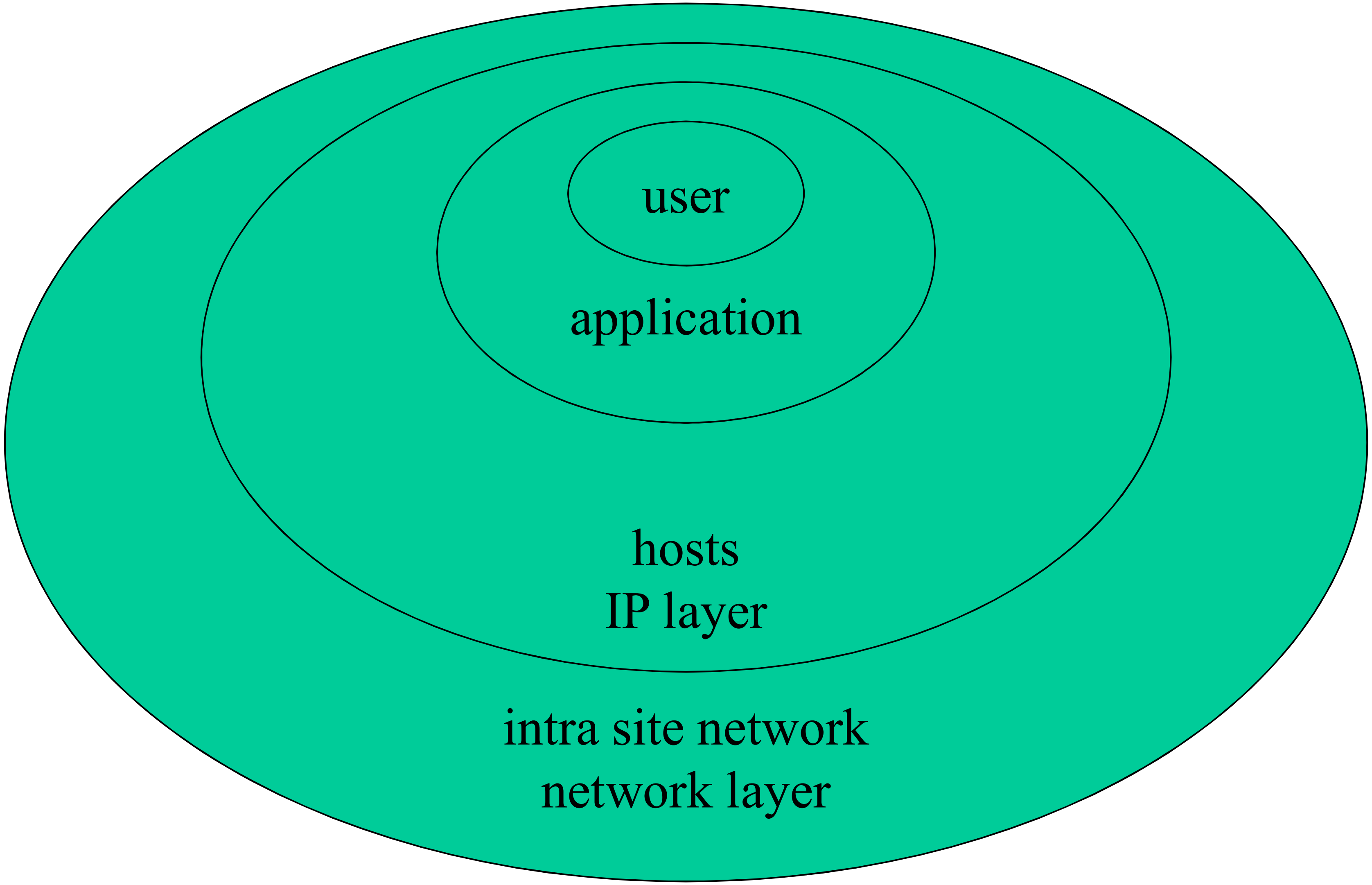
- assume ISPs are trustworthy
  - packet is sent to peer specified by IP address
  - no wiretapping en route
  - can identify peer by IP address
    - source IP address in IP header is not reliable
      - can be confirmed by handshaking (random number sent to peer’s IP address is sent back)
- trustworthiness is just an assumption



authentication of IP address with weak security

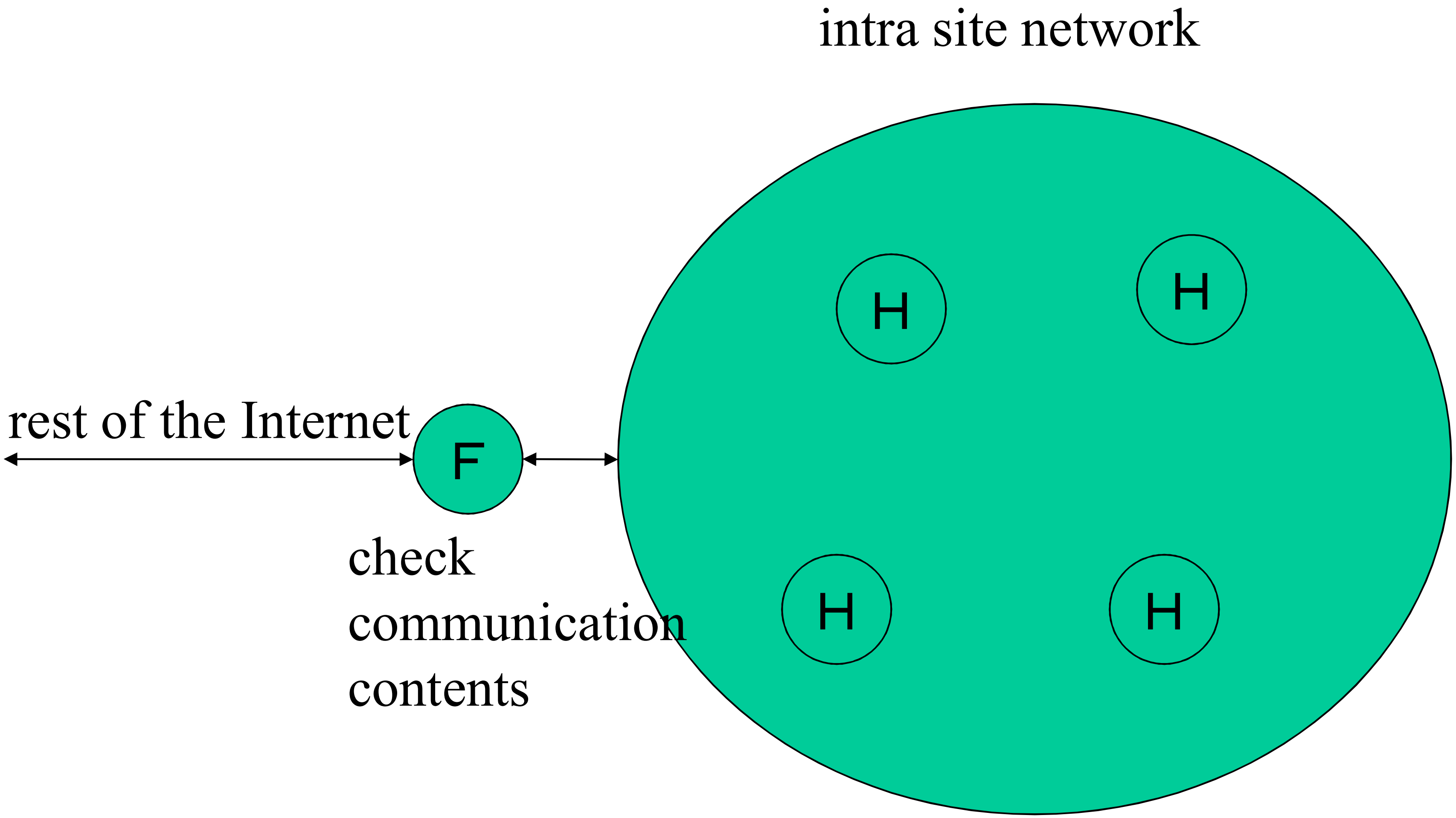
Purpose of Security

- offer security to every user of every application


user
application
hosts
IP layer
intra site network
network layer

How to Offer Security

- Firewall?
  - protect some part of network from the rest
  - security only at network layer
  - does not offer true security (similar to cold medicine only to relief simptom of cold)
    - if each hosts are secure, we don’t need firewalls
    - firewalls can not know all the vulnerabilities of all the applications
      - known vulnerabilities should be mitigated by developpers of applications (the end to end principle)



intra site network

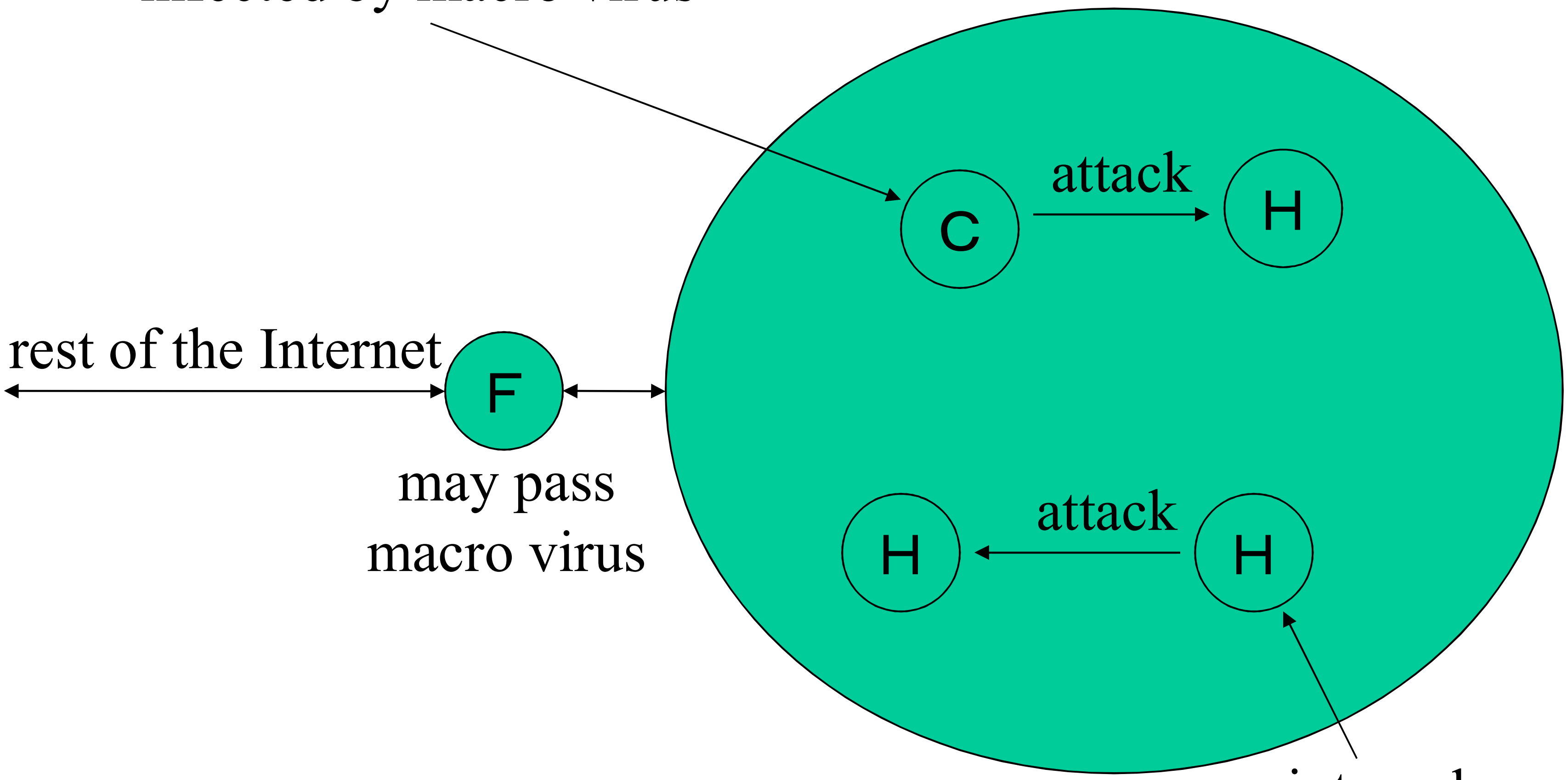
rest of the Internet

check
communication
contents

meaning of firewalls

intra site network

infected by macro virus



C

attack

H

rest of the Internet

F

may pass
macro virus

H

attack

H

internal
bad guy

meaninglessness of firewalls

Toward True Security

- every user should be security aware
- every application should be secured
- every hosts should be secured
  - be careful, if you share a host with others

Implementing True? (Cryptographic) Security

- by sharing secret key
  - somehow share secret key between related parties
  - N^2 keys necessary for N parties
- by public key
  - each has secret private key and publish corresponding public key
  - only N keys necessary for N parties (scalability!)?

Principle of Public Key

- computation of private key from public key is practically impossible
  - based on factorization or discrete logarithm with large prime numbers
- encryption/decryption/authentication with private/public key is relatively easy
  - modulo exponentials of integers represented by several hundreds of bits
  - in practice, public keys are used only initially to share shared secret session keys (>N^2 keys)

Public Key and CA (Certificate Authority)

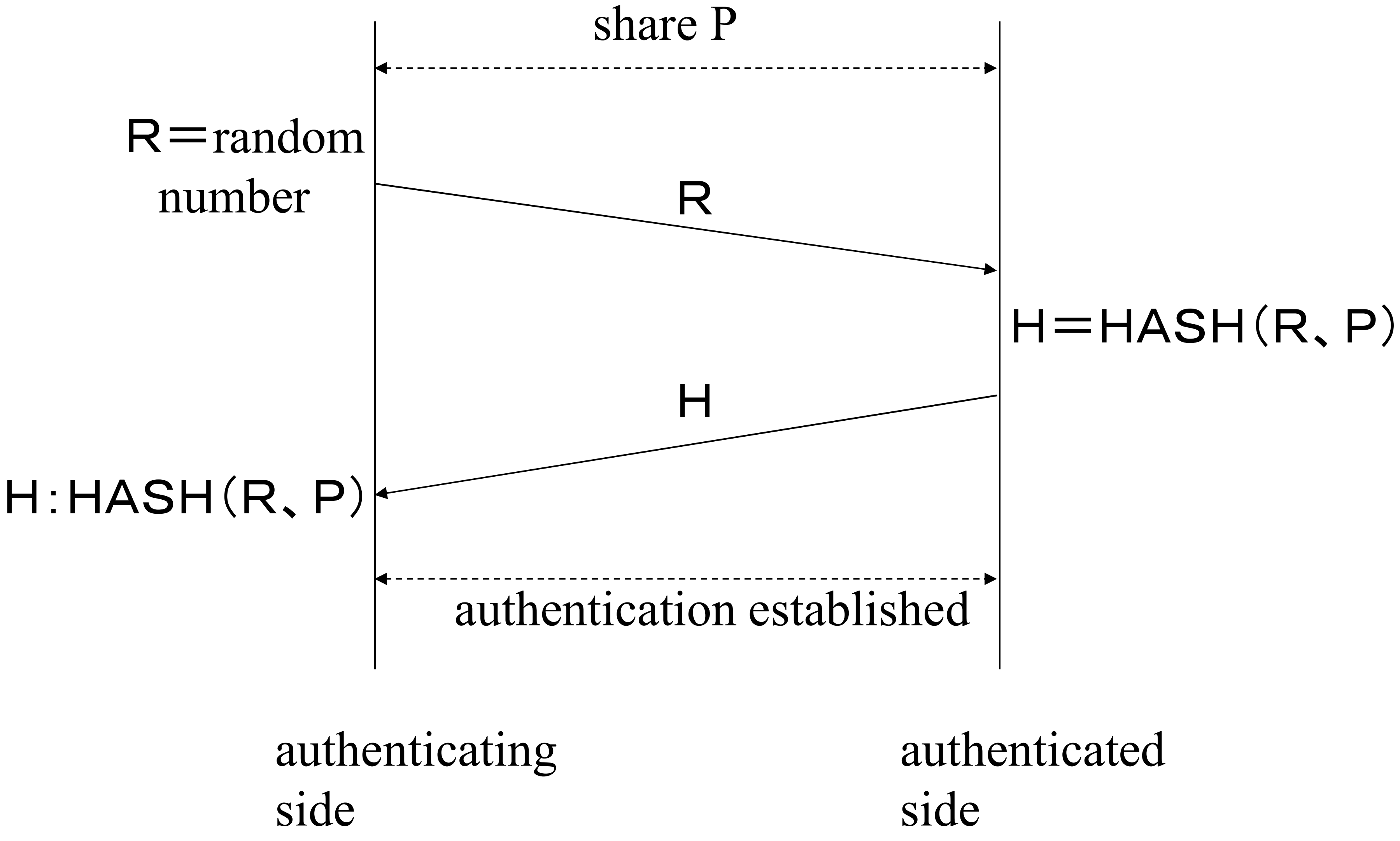
- how can we reliably know public key of peer?
  - authentication on the key is necessary
- have a CA and share its public key
  - CA authenticate public keys of other organizations
  - hierarchy of CA is possible
    - not very useful unless CA hierarchy follows actual social hierarchy

Example of Secrecy for Authentication

- plain text password
  - if communication is tapped
    - password is stolen
  - plain text password cannot be used over leaky communication channels
    - one time password, etc.

Safe Password

- Chap (Challenge Handshake Authentication Protocol)
  - generate hash of password and random number sent from peer
  - send the hash to peer
- one time password
  - use same password only once
  - large number of passwords are shared in advance



share P

R＝random number

R

H＝HASH（R、P）

H

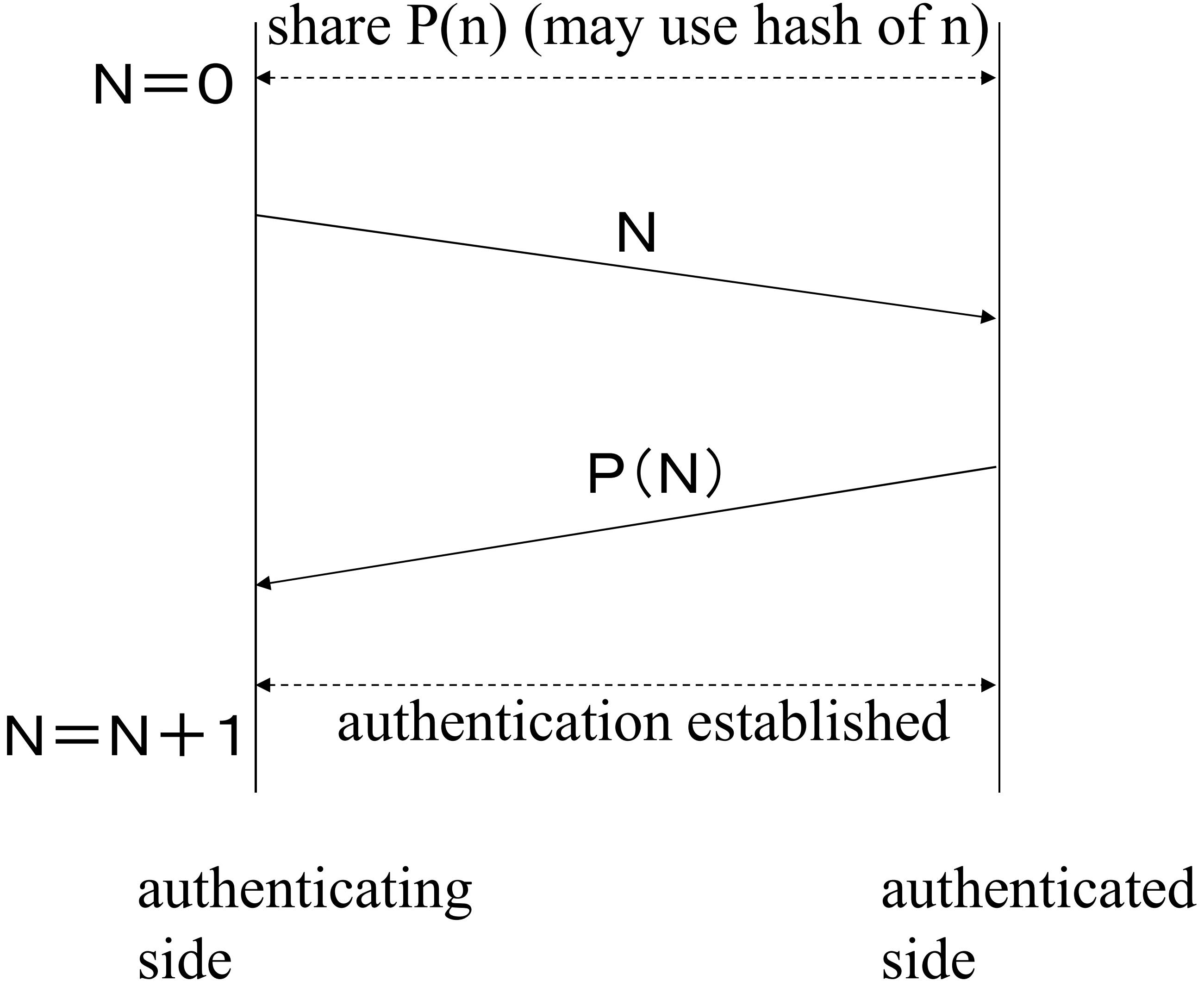
H：HASH（R、P）

authentication established

authenticating side

authenticated side

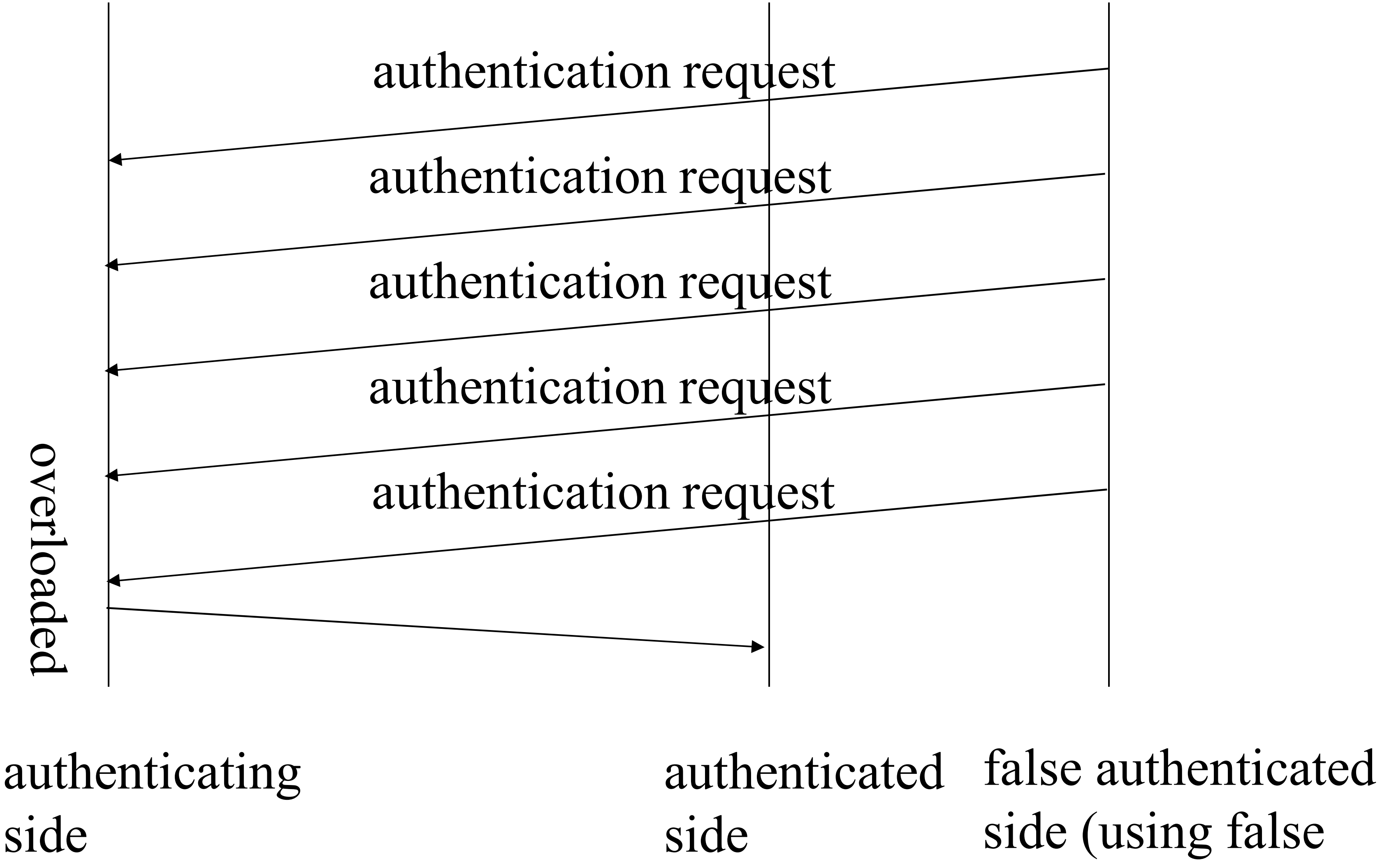
mechanism of CHAP (P does not appear on communication channel



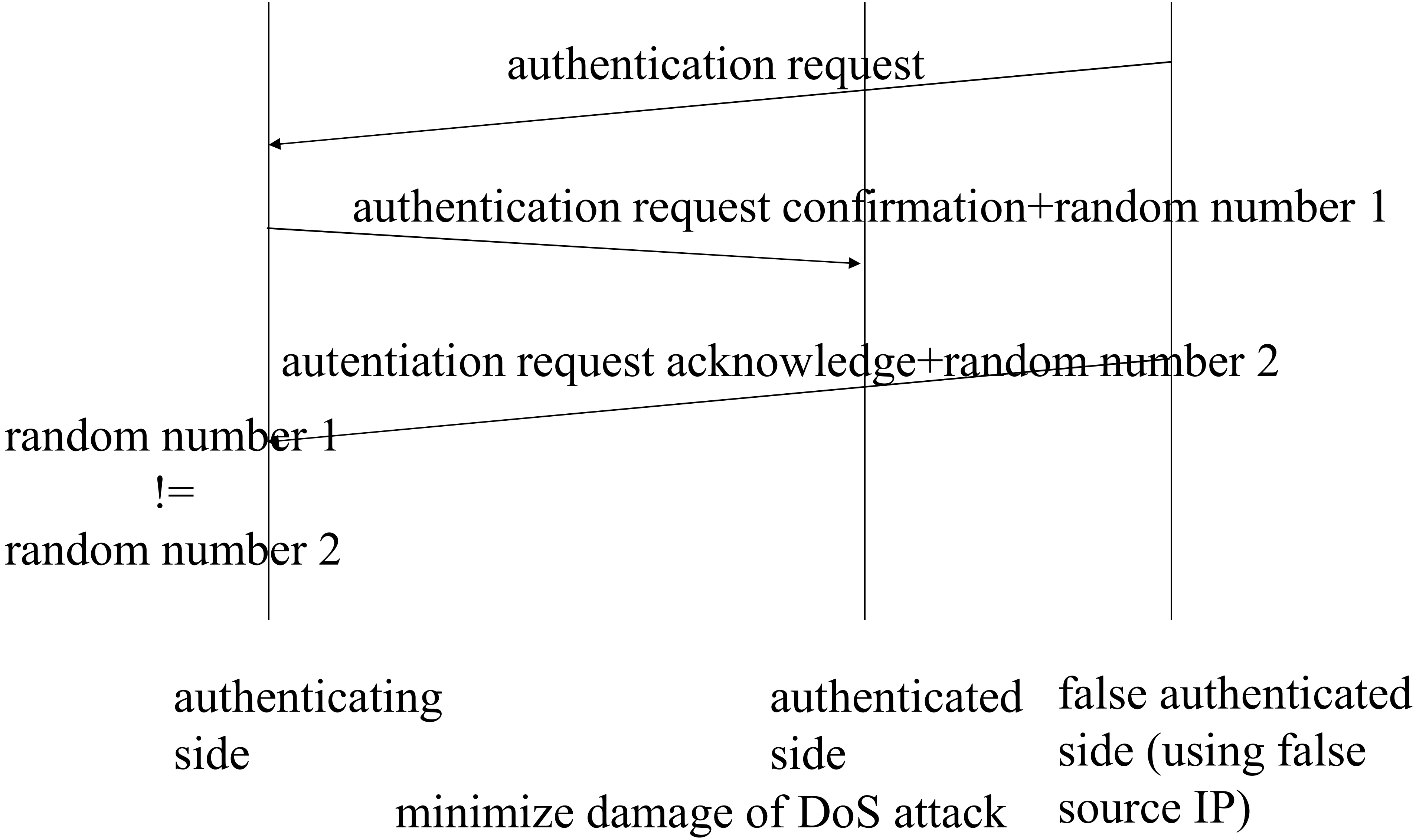
mechanism of one time password
same P(n) is used only once

DoS (Denial of Service)

- attack to increase load by meaningless data
- prevention is basically impossible
  - sophisticated (thus, high load) authentication is easy victim of DoS
- possible to locate the attacker
  - before high load authentication, 3 way handshake relying on weak security should be performed



example of DoS attack


authentication request
authentication request confirmation+random number 1
autentiation request acknowledge+random number 2
random number 1
!=
random number 2
authenticating side
authenticated side
false authenticated side (using false source IP)

minimize damage of DoS attack

VPN (Virtual Private Network)

- technology to construct private network over the Internet
  - for better (?) security
- meaningful if totally private network is constructed
  - better than buying service from telco (inexpensive)
  - not very meaningful, if e-mail is reachable from the Internet

Security of Internet Protocol Suites

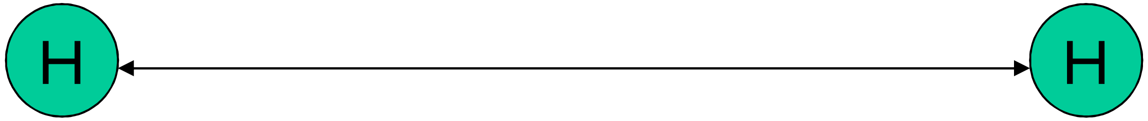
- each protocol has its own security
  - eg: password of ftp
- need a unified mechanism?
  - IPsec

IPsec (rfc2401)

- standard format (AH as IPv6 extension header) for transport/application layer (distinguished by SPI)
- by shared secret key
- authentication (AH, ESP) and encryption (ESP)
- how can keys shared
  - ISAKMP? IKE? DNSSEC?
- transport mode and tunnel mode

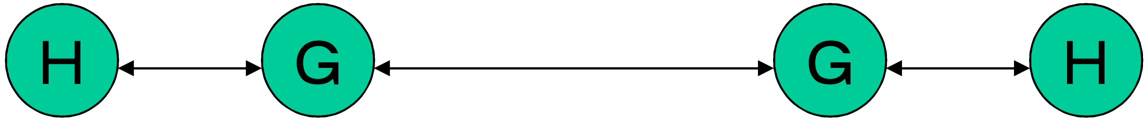
Transport Mode

- used directly between hosts
- straight forward end to end security



Tunnel Mode

- used between security gateways
  - for VPN?
- not end to end, not for Internet



SA (Security Association)

- connection for security
  - may not have 1:1 correspondence with transport connection
  - algorithms for authentication and encryption different SA by SA
- unidirectional
- identified by SPI, destination address and AH/ESP

AH (Authentication Header) (rfc2402)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   |  Payload Len  |          RESERVED             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Security Parameters Index (SPI)               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Sequence Number Field                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                Authentication Data (variable)                 |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fields of AH

- SPI
  - identify SA with destination IP
- Sequence Number
  - prevent replay attack
- Authentication Data
  - hash of authenticated data and shared secret key

ESP (Encrypted Security Payload) (rfc2406)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ----
|               Security Parameters Index (SPI)                 | ^Auth.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|                      Sequence Number                          | |erage
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ | ----
|                    Payload Data* (variable)                   | |   ^
~                                                               ~ |   |
|                                                               | |Conf.
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |Cov-
|               |     Padding (0-255 bytes)                     | |erage*
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |   |
|                               |  Pad Length   | Next Header   | v   v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ ------
|                 Authentication Data (variable)                |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Methods of Encryption

- by shared secret key
  - encrypted text=E(plain text, secret key)
  - plain text=D(encrypted text, secret key)
- by public key
  - encrypted text=E(plain text, public key)
  - plain text=D(encrypted text, secret key (private key))

Implementing True? (Cryptographic) Security

- by sharing secret key
  - somehow share secret key between related parties
  - N^2 keys necessary for N parties
- by public key
  - each has secret private key and publish corresponding public key
  - only N keys necessary for N parties (scalability!)?

PKI (Public Key Infrastruture)

- false public key makes public key insecure
  - N^2 transactions necessary to receive public key of peers directly (securely) between N parties
- instead, rely on CA (certificate authority)
  - CA authenticate public keys of all the parties
  - all the parties have public key of CA
    - only N transactions with CA necessary for N parties
  - CAs have hierarchy for better scalability
    - all the parties have public key of root CA

ISKMP (Internet Security Association and Key Management Protocol) (rfc2408)

- framework for key sharing
- based on public key infrastructure
- manage SA
- generate key
- protection against DoS
- protection against replay attacks

IKE (The Internet Key Exchange) (rfc2409)

- actual protocol for key sharing
- based on public key infrastructure
- manage SA
- generate key
- protection against DoS
- protection against replay attacks

Secure DNS (rfc2535)

- make DNS truly secure
  - plain DNS is very weakly secure
    - 16 bit ID to match request and reply
- zone tree structure becomes PKI tree structure
  - public key of root zone is shared by all
  - public key of child zone is authenticated by secret key of parent zone, recuresively

Current Status of IPsec (failed except for VPN)

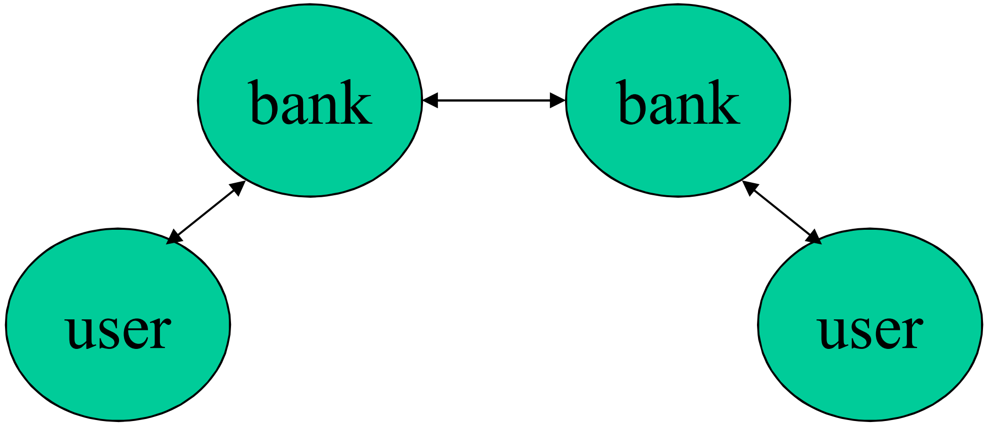
- ESP should be enough and AH is unnecessary?
- key sharing by manual configuration
  - ISKAMP too complicated
  - DNSSEC too complicated
    - worse, was so poorly designed by a person without much knowledge on delicacy of DNS (authority relationships involving NS, glue A and CNAME)
- each protocol has its own security

Is PKI Really Secure?

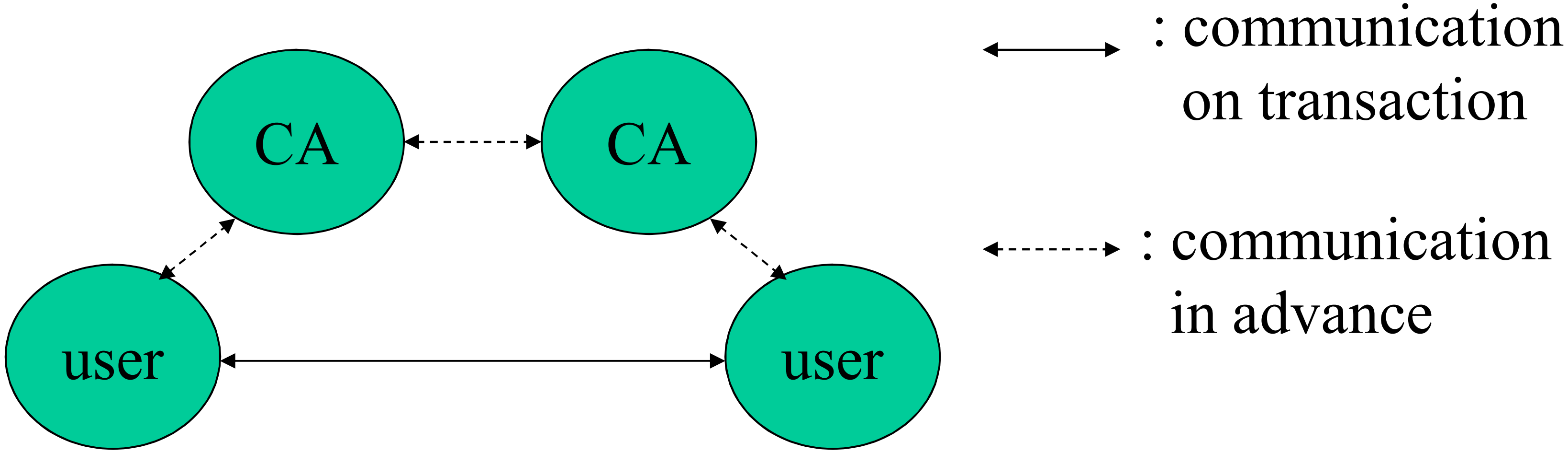
- the number of shared key is not a problem
- similar hierarchy of KDC (key distiribution center) with shared secret key possible
  - though communication with KDC is necessary
    - for every transaction
      - communication is, anyway, necessary for any transaction over the Internet
      - communication is free over the Internet
- who operate CA reliably?
  - if ISPs are not reliable, can we rely CAs?

Considering Electric Settlement

- communication delay & error inevitable
  - distributed “exactly once” is impossible
  - reliable intermediate entity (bank) is necessary to prevent unpayment or double payment
- communication with banks necessary on every transaction
- if PKI without communication is used
  - no one can be responsible for accident
  - PKI is as useful as deposite balance certificate

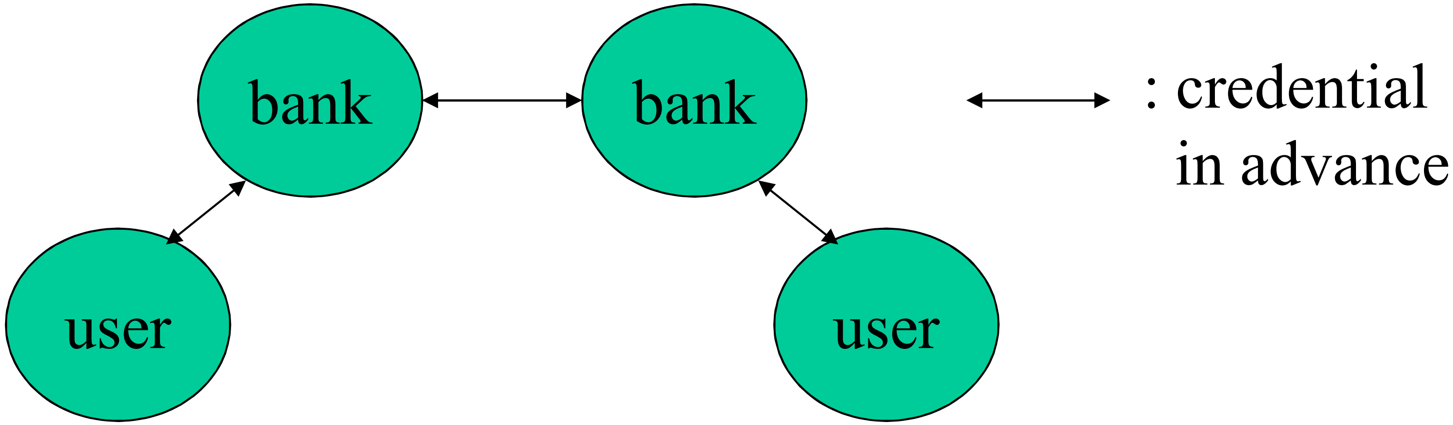


settlement through banks

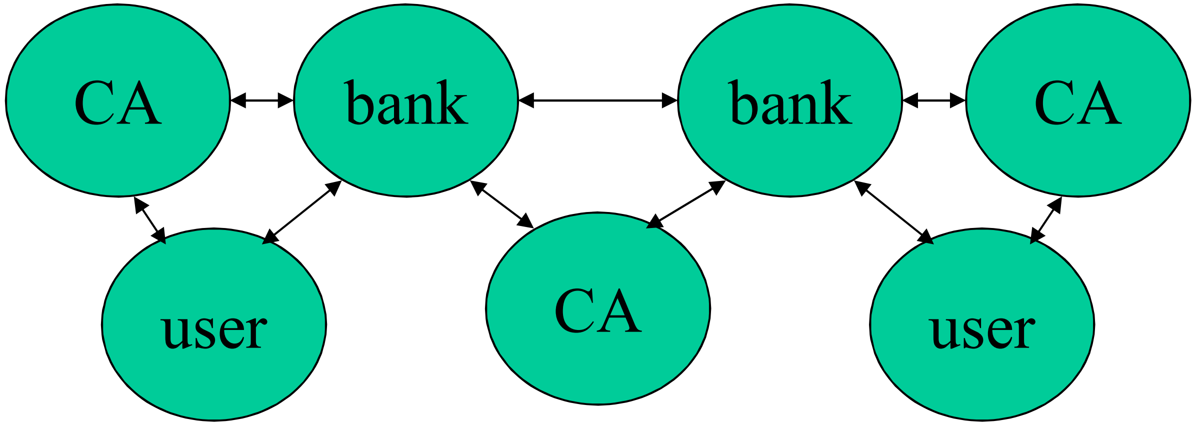


settlement through CAs

how electric settlement works


bank
bank
user
user
: credential in advance

settlement through banks (based on credential in advance)


CA
bank
bank
CA
user
CA
user

settlement through banks and CAs (lots of unnecessary credentials)

use both banks and CAs?

Weak Security

- security relying on infrastructure offered by third parties
  - if ISPs are reliable, packet is delivered to a host with the destination address, without being tapped or modified
  - ISPs may tap or modify packets
- similar to security of phone network
  - telcos may tap or modify conversation
- similar to security of PKI

PKI is only Weakly Secure

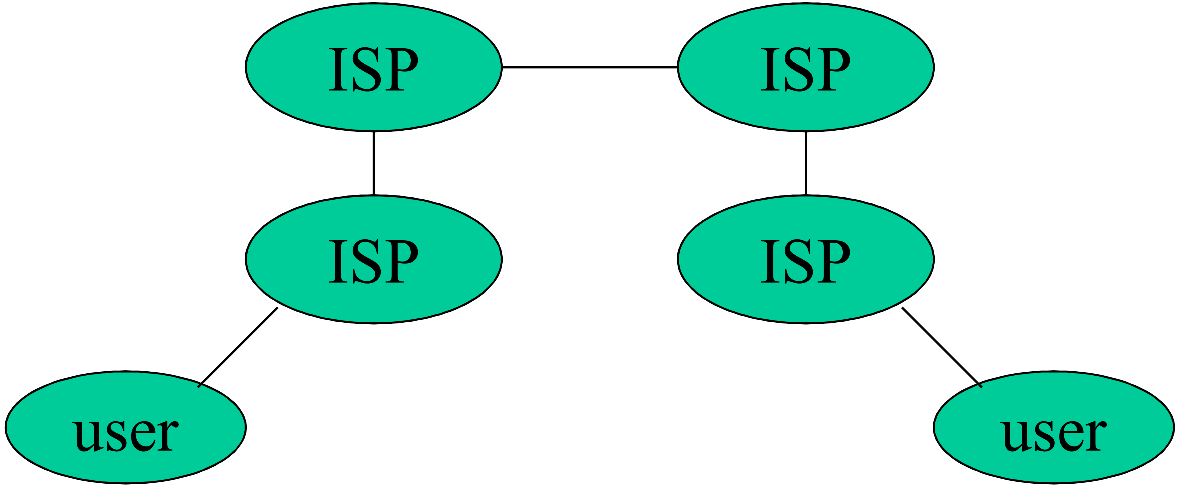
- security relying on infrastructure (PKI) offered by third parties
  - if CAs are reliable, public key of peer certificated by CAs is reliable
  - if CA forges certificate, no security
- there is no cryptographic security
  - PKI assumes CAs are TTP (trusted third party)
    - why not assume ISPs are TTP?

DH (Diffie-Hellman) Key Exchange

- modular computation with large *p*
- share *m* and each generate random number (*a* and *b*)
- exchange *m*^*a* and *m*^*b* (may be tapped)
  - practically impossible to compute *a* from *m*^*a* (discrete logarithm)
- (*m*^*a*)^*b*= (*m*^ *b*)^*a* is shared secret
- not secure
  - against active MitM (man in the middle) attack

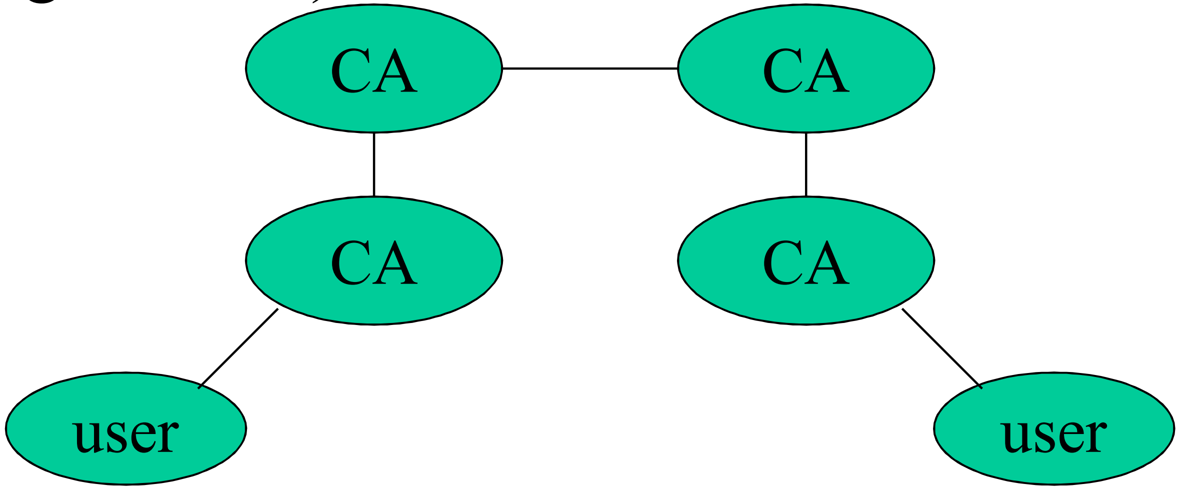
MitM (Man in the Middle) Attack

- tapping, dropping and modification by intermediate ISPs
  - makes plain text password and DH insecure
  - if ISPs are reliable, no further security necessary



MitM (Man in the Middle) Attack on PKI

- forged certificate by intermediate CAs
  - CA and ISPs should be equally reliable
  - if CA is insecure, no cryptographic security (diginotar!!!)



To Prevent MitM Attack

- don’t rely on third parties
  - relying on third parties is against E2E principle
- only use ISPs and CAs operated by the first or second parties
  - CAs need direct (E2E) key sharing between first and second parties
    - if N:N, N^2 sharing
      - no point to use public key

Is Public Key Cryptography Useful?

- PKI is not very useful
- public key is slow to compute and, maybe, unsafe
  - may be able to compute private key
- credential to non-consumable credit?
  - the credit may be converted to consumable one
- may be useful to authenticate broadcast contents?

Credit and End to End Principle

- cryptography is a tool to carry credit
- credit is formed by direct communication
  - secrete key may be shared at the same time
  - CAs do not offer credit
  - CAs are intermediate intelligent entities and is useless
- the E2E security needs direct credit information and key sharing between related parties

Wrap-up

- the Internet is as secure as phone network
- E2E security is the true security
  - secure hosts and applications
- IPsec (AH, ESP)
  - standard format for security?
- DNSSEC
  - useful?
- PKI is against E2E principle, which is why it is very complicated but insecure

Meaninglessness of PKI for Authentication on Consumable Credit

Major Problems of PKI

- PKI cannot be used to guarantee remaining credit
  - remaining credit must be checked on every transaction
    - no better than shared secrete
- PKI is insecure if intermediate CA is not reliable
- PK structure may be useful for some purpose
  - general purpose PKI is impossible

Classic Fraud by Check Book

- receive check book by depositing money to bank
- using the check book, repeat the following
  - purchase (inexpensive) goods
  - sell the goods to secondhand dealers
- escape before being caught
- success if total resold money exceeds deposit

Protection from Classic Fraud by Check Book

- tentative relief (increase cost of crime)
  - don’t issue check book lightly (Japan)
  - request ID at secondhand dealers
- fundamental relief (limit profit of crime)
  - finite number of checks in a check book
  - shops take the risk
    - when purchasing (expensive) goods, shops ask bank account balance of customer

Classic Fraud by Credit Card

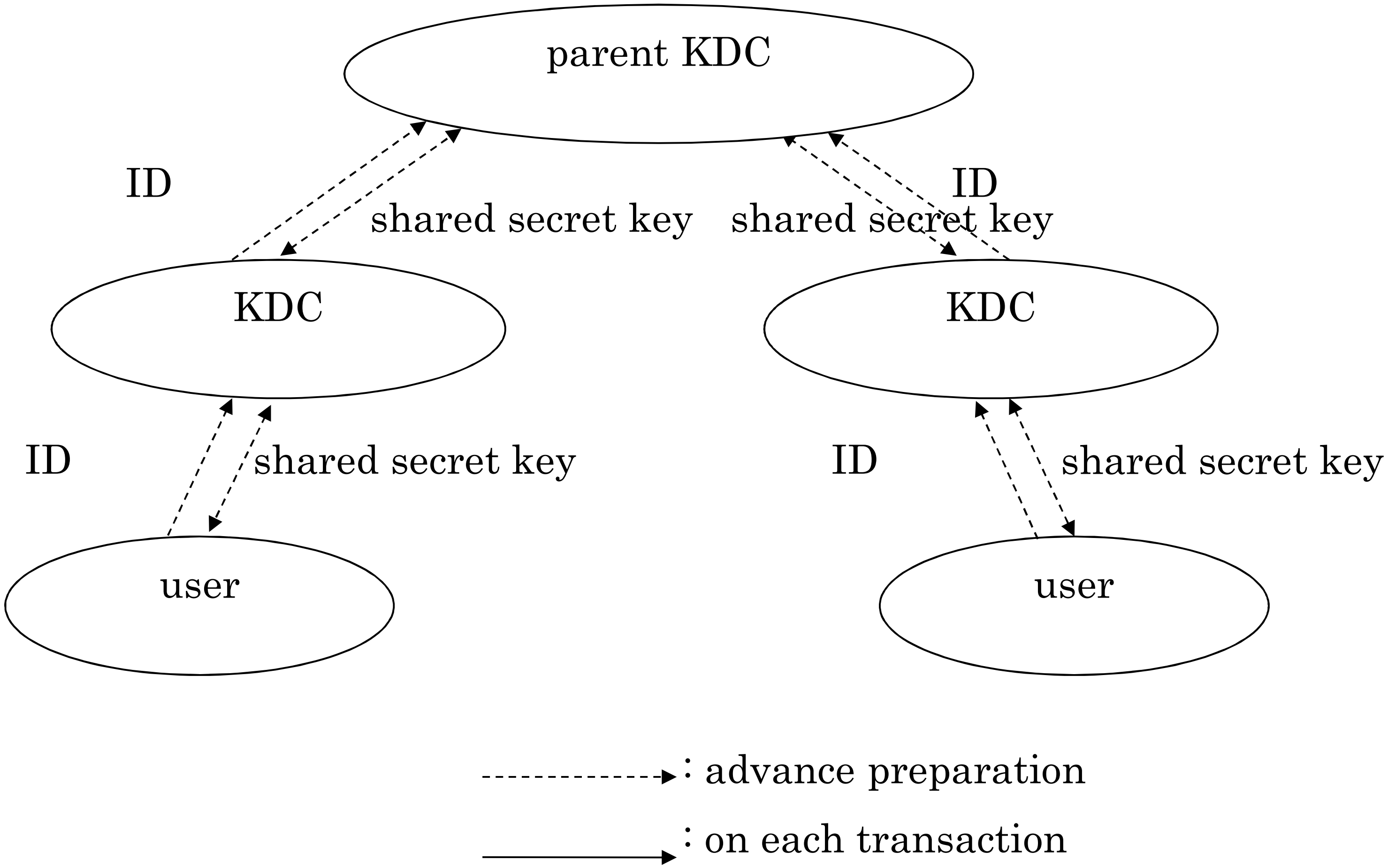
- get a credit card
- using the card, repeat the following
  - purchase (inexpensive) goods
  - sell the goods to secondhand dealers
- escape before being caught
- success if total resold money exceeds cost of getting credit card

Protection from Classic Fraud by Credit Card

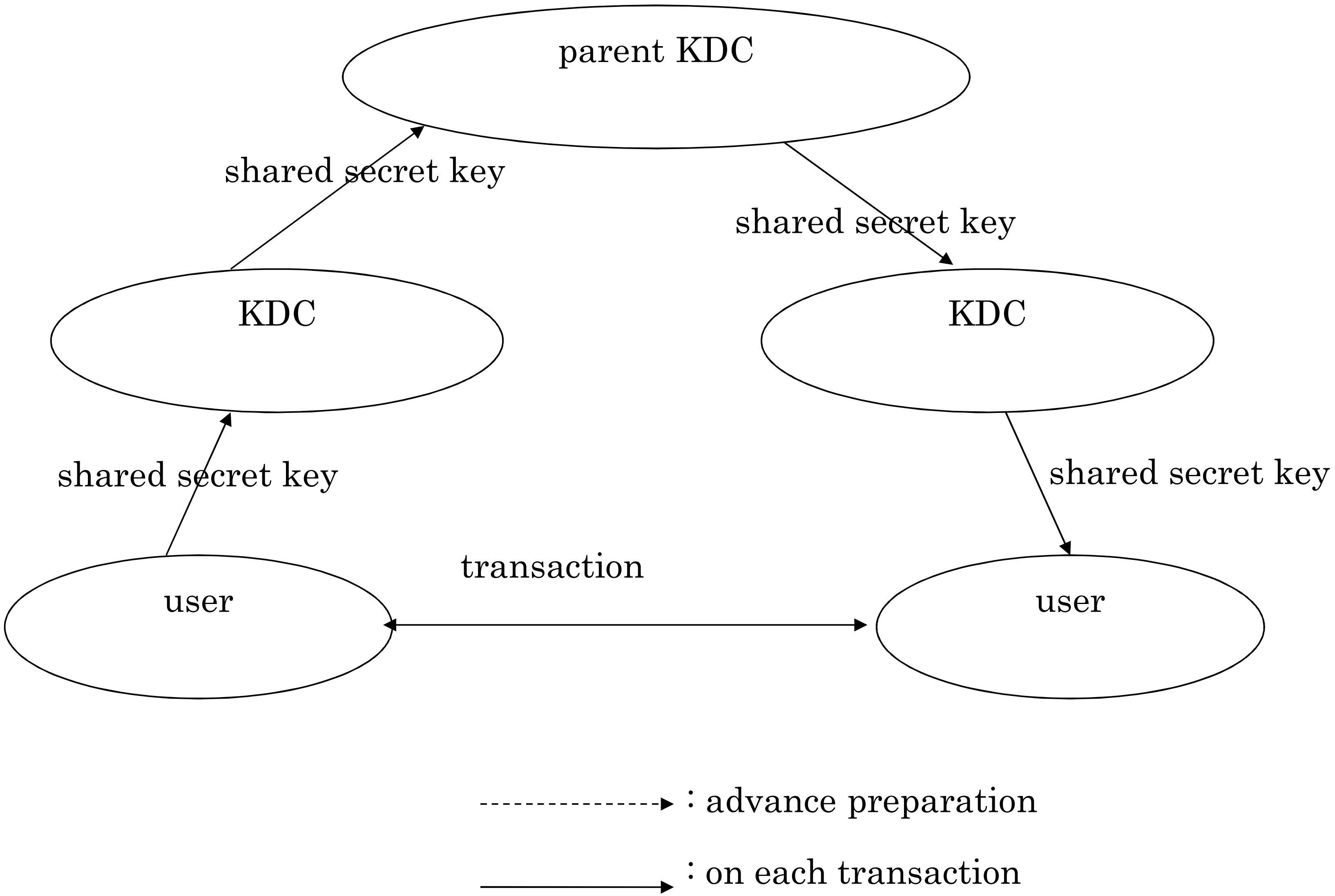
- tentative relief (increase cost of crime)
  - request ID when issuing credit card
  - request ID at secondhand dealers
  - only one card is issued
- fundamental relief (limit profit of crime)
  - shops take the risk
    - when purchasing (expensive) goods, shops confirm credit card issuers remaining credit of customer
      - credit card was not accepted for small amount of purchase
      - confirmation maybe omitted for goods difficult to be resold (fresh food etc.)

Shared Key Cryptography

- related parties “safely” share secret key
- for direct mutual authenticaton between N parties
  - *N**(*N*-1)/2 keys must be shared in advance
  - not practical for large *N*
- if *N* parties share KDC (Key Distribution Center)
  - only *N* key shared by parties and KDC is necessary in advance
  - on transactions, session key is shared through KDC
- KDCs may have hierarchy



shared secret key and KDC (advance preparation)



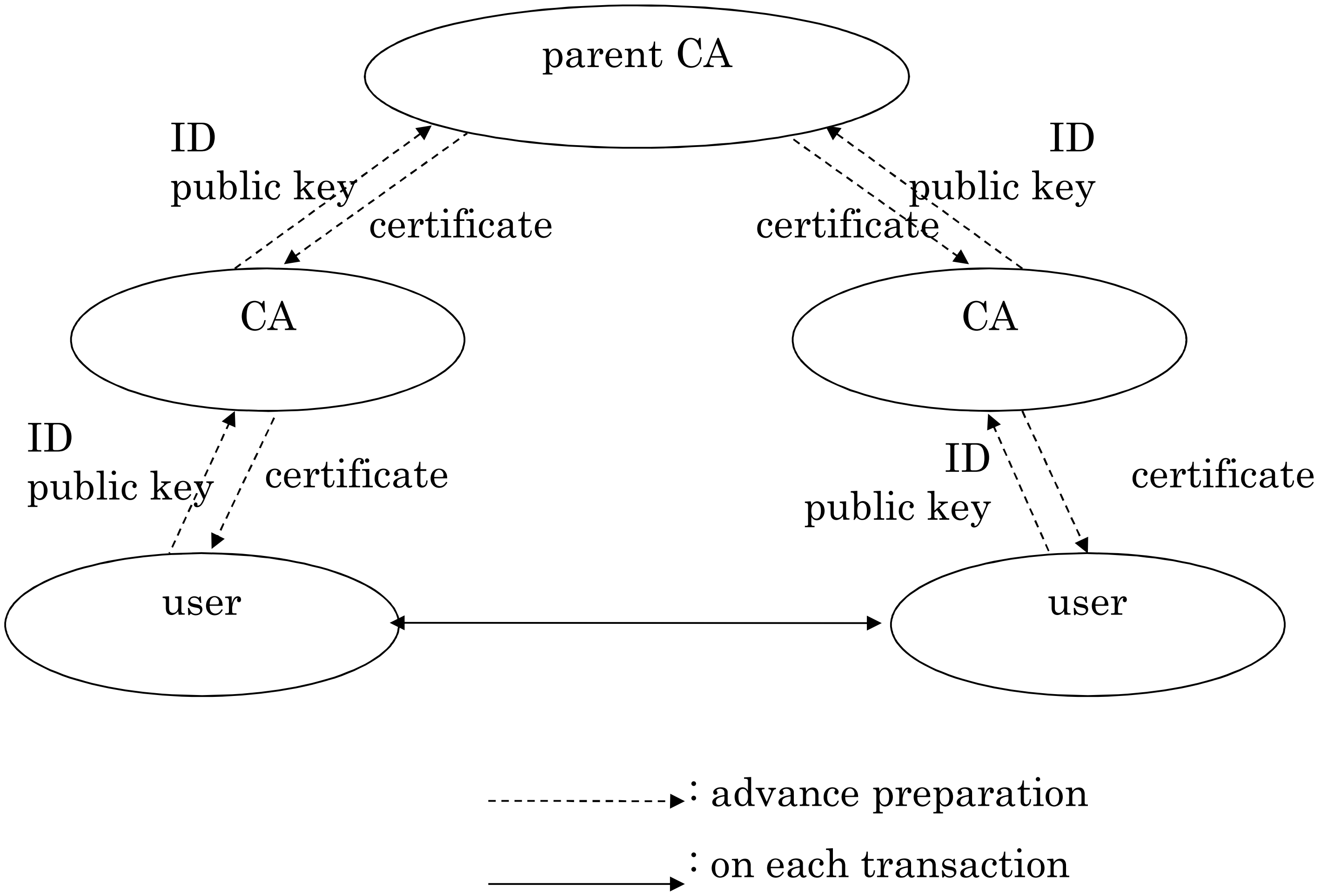
shared secret key and KDC

Public Key Cryptography (1)

- each party have secret key
  - its public key is “safely” shared by all parties
- for direct mutual authenticaton between *N* parties
  - only *N* keys may be shared in advance
  - for sharing public keys “safely”
    - *N* keys must be transferred “safely” *N**(*N*-1) times in advance
      - or, keys may be broadcast “safely” *N* times
  - not practical for large *N*

Public Key Cryptography (2)

- if *N* parties share CA (Certificate Authority)
  - only *N* key shared by parties and CA is necessary in advance
  - on transactions, secret shared session key is "safely" shared with certified public keys
    - no interventions by CAs necessary
- CAs may have hierarchy



public key cryptography and CA

Fraud on Credit Balance Certified by Public Key

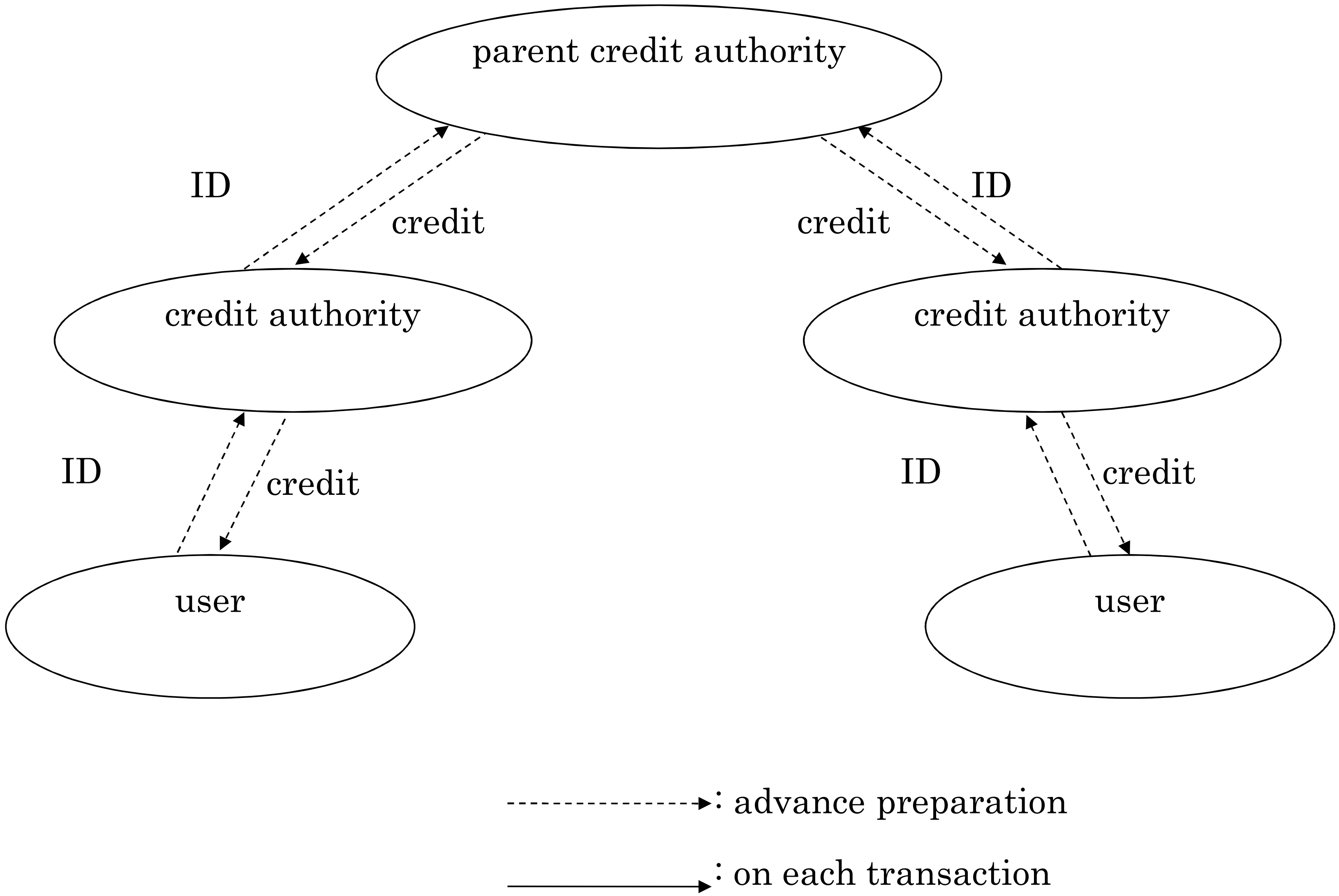
- receive certificate on credit balance
- using the certificate, repeat the following
  - purchase (inexpensive) goods (electrically)
  - sell the goods to secondhand dealers (electrically)
- escape before being caught
- success if total resold money exceeds cost to get the certificate

Properties on Fraud on Credit Balance Certified by Public Key

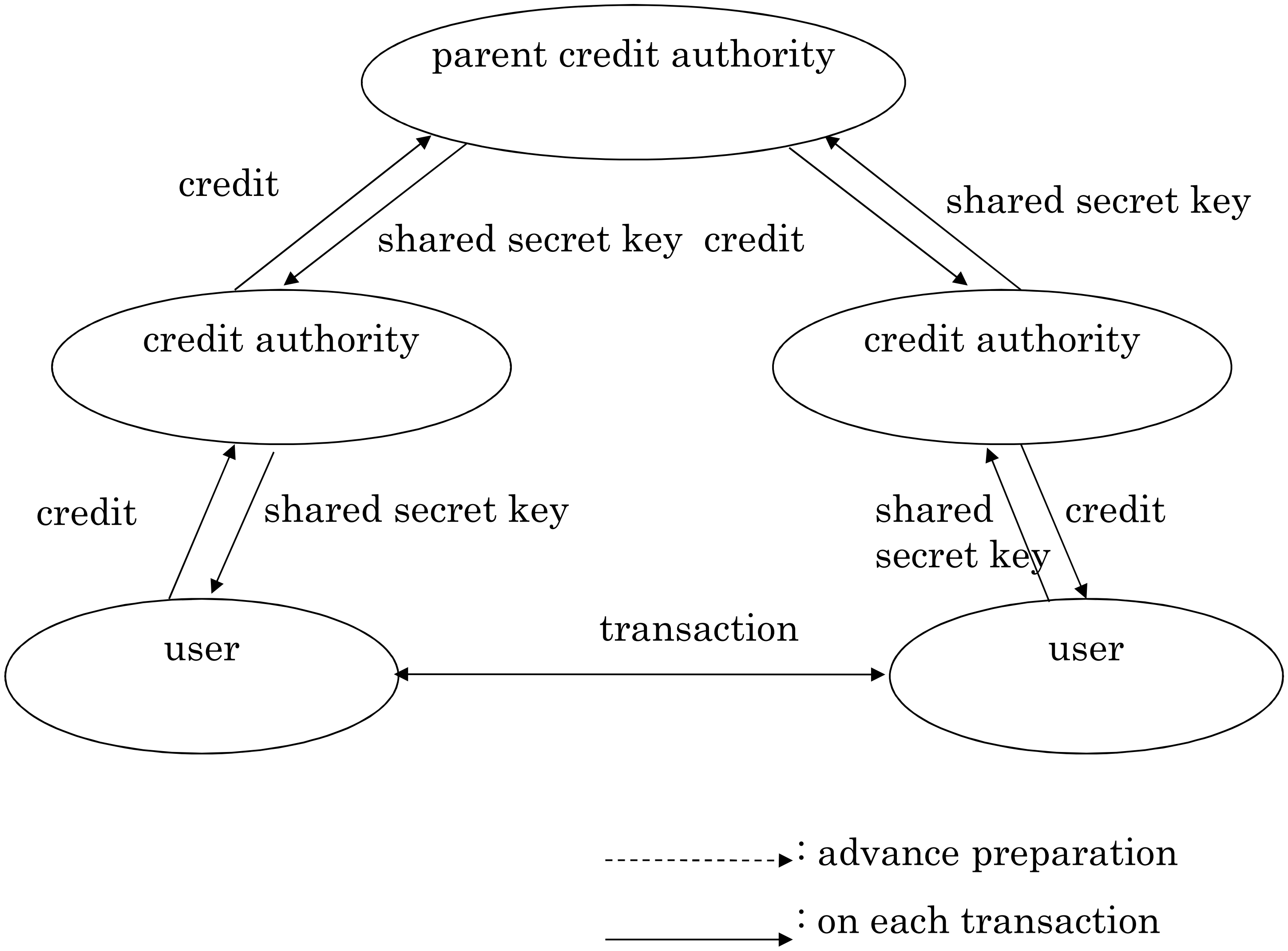
- unlimited # of copies of certificate exist
- transaction is electric
- # of transaction is almost unlimited
- 1000 $1M transaction/s for 1000s from 1000 locations means total amount of $1P
  - 1000 $1000 transaction/s for 1000s from 1000 locations means total amount of $1T
    - revocation by CRL (certificate revocation list) is too late (usually needs weeks or days)

Protection from Fraud on Credit Balance Certified by Public Key

- tentative relief (increase cost of crime)
  - request ID when issuing certificate
  - request ID at secondhand dealers?
    - even though customers are certified by PKI?
- fundamental relief (limit profit of crime)
  - “shops take the risk” is insufficient
  - need “credit authority” to maintain credit balance in real time
    - (however small amount transaction), shops must ask credit authority the current balance



credit balance and credit authority



credit balance and credit authority

Credit Authority and Cryptography

- fraud is impossible, if communication between credit authorities is reliable
  - credit authority act as CA/KDC
    - additional CA/KDC meaningless
    - leakage of secret key from credit authority can be disaster
- communication with credit authority is necessary for each transaction
  - shared key cryptography is enough
- credit authorities are just banks
  - PKI is meaningless on consumable credit