National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

Anonymous Password-Authenticated Key Exchange and Its Application

SeongHan Shin

Security Fundamental Team

ANONYMOUS PASSWORD-AUTHENTICATED KEY EXCHANGE

Anonymity

- User privacy is a big concern
- E.g., net counseling, whistle blowing
- Suppose an attacker who can eavesdrop networks
  - Communication history of access to ftp servers, web-mail servers, Internet banking servers or shopping mall servers
  - It is easy to collect user’s personal information by analyzing the communication history itself
  - These information may reflect user’s life pattern and sometimes can be used for spam mails

Previous Approaches

- The dining cryptographers problem [Cha88]
- Many re-routing protocols
  - Anonymizer (using web proxy server) [Ano]
  - Mix, Mix-nets [Cha81]
  - Onion routing [SGR97]
  - Crowds [RR97]
- Group/ring signatures

Anonymous Authentication

- In this talk,
  - We only consider user anonymity of "Authenticated Key Exchange (AKE)" protocols
  - Both mutual authentication and generation of secure session keys
  - E.g., SSL/TLS, IKE, SIGMA, PAKE
- Why AKE?
  - Bellare et al., [BR95] "...entity authentication is rarely useful in the absence of an associated key distribution*, while key distribution, all by itself, is not only useful, but it is not appreciably more so when an entity authentication occurs along side."

*when using a physically secured communication channel

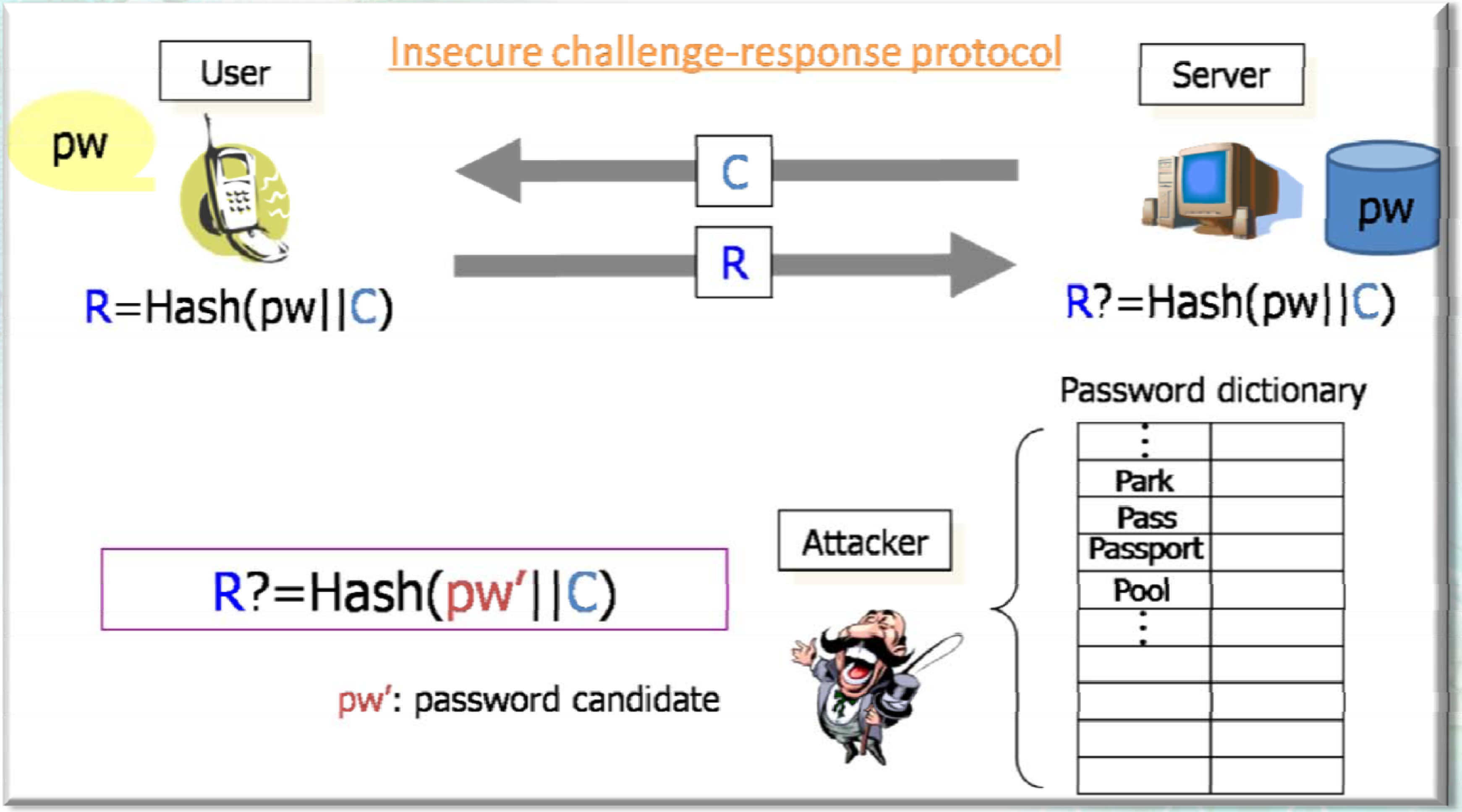
National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

Password-based AKE (1/2)

- Easy-of-use authentication
- Already deployed in practice
- Suitable for ubiquitous communications
- However, it faces some challenges on security
  - Due to a dictionary size of password
  - On-line attacks
    - inevitable but controllable
  - Off-line attacks
    - must be avoided

Password-based AKE (2/2)



Insecure challenge-response protocol

User

pw

Server

pw

C

R

R=Hash(pw||C)

R?=Hash(pw||C)

Password dictionary

⋮	
Park	
Pass	
Passport	
Pool	
⋮	

Attacker

R?=Hash(pw'||C)

pw': password candidate

Password-Authenticated Key Exchange (1/2)

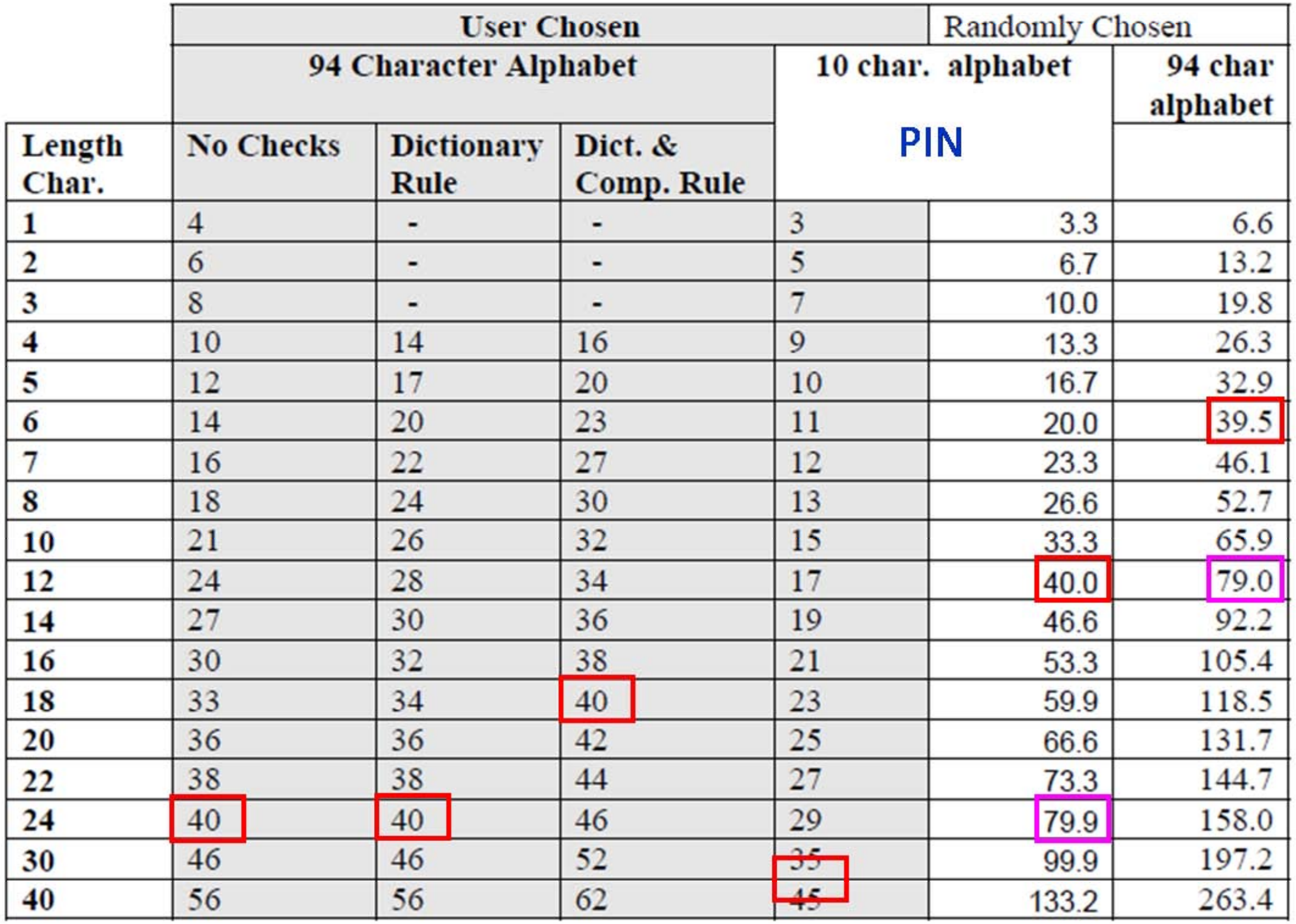
- Secure password-only AKE (called, PAKE)
  - – Without any device and infrastructure
- E.g., EKE, AuthA, SRP, AMP, SNAPI
- In IEEE standardization [P1363.2]
- Security
  - – Against passive attacks
  - – Against active attacks
  - – Against off-line attacks

Password-Authenticated Key Exchange (2/2)

- Overall security depends on the number of on-line attacks
  - Be cautious to choose random-like passwords
  - Be cautious not to register same passwords to many different services
  - Be cautious to change passwords regularly
  - Be cautious not to write down passwords on somewhere

Estimated Password Guessing Entropy

- NIST Special Publication 800-63 [NIST800-63]
  - With one minute lock out for 3 failed trials, it would take about 90 years to carry out $2^{25.5}$ trials.

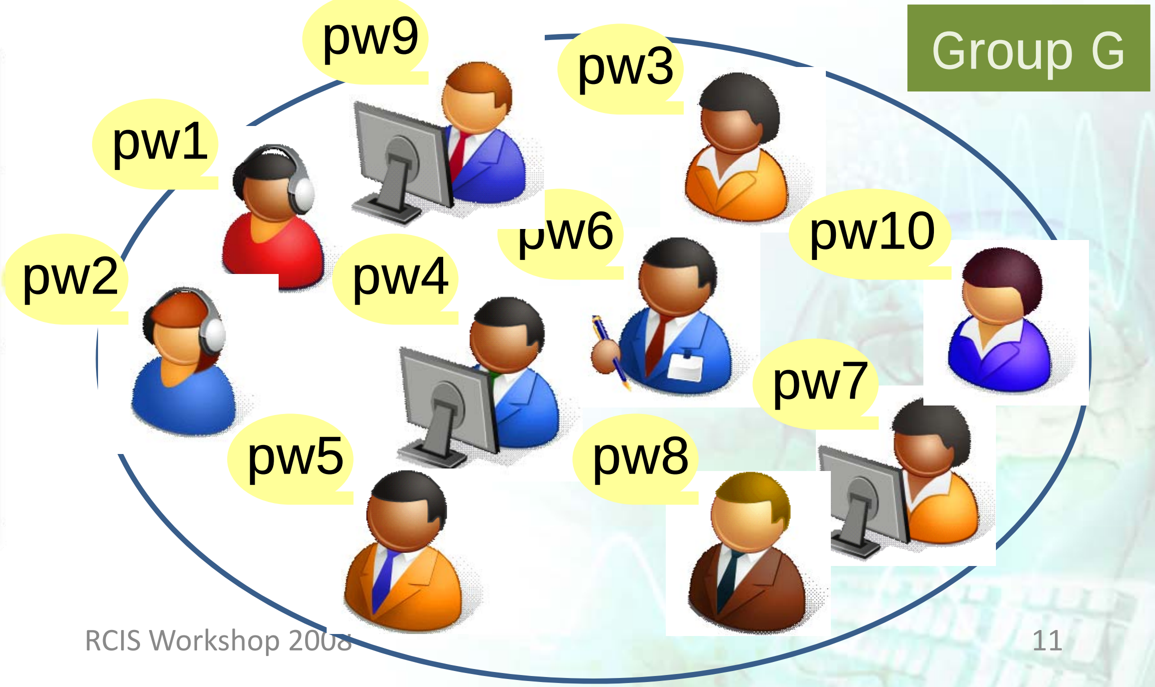


	User Chosen				Randomly Chosen	
	94 Character Alphabet			10 char. alphabet		94 char alphabet
Length Char.	No Checks	Dictionary Rule	Dict. & Comp. Rule	PIN		
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

Anonymous PAKE (1/2)

- PAKE does not provide user anonymity!
  - A user should send his/her identity clearly
- Be careful
  - No trusted third party
  - User remembers only passwords

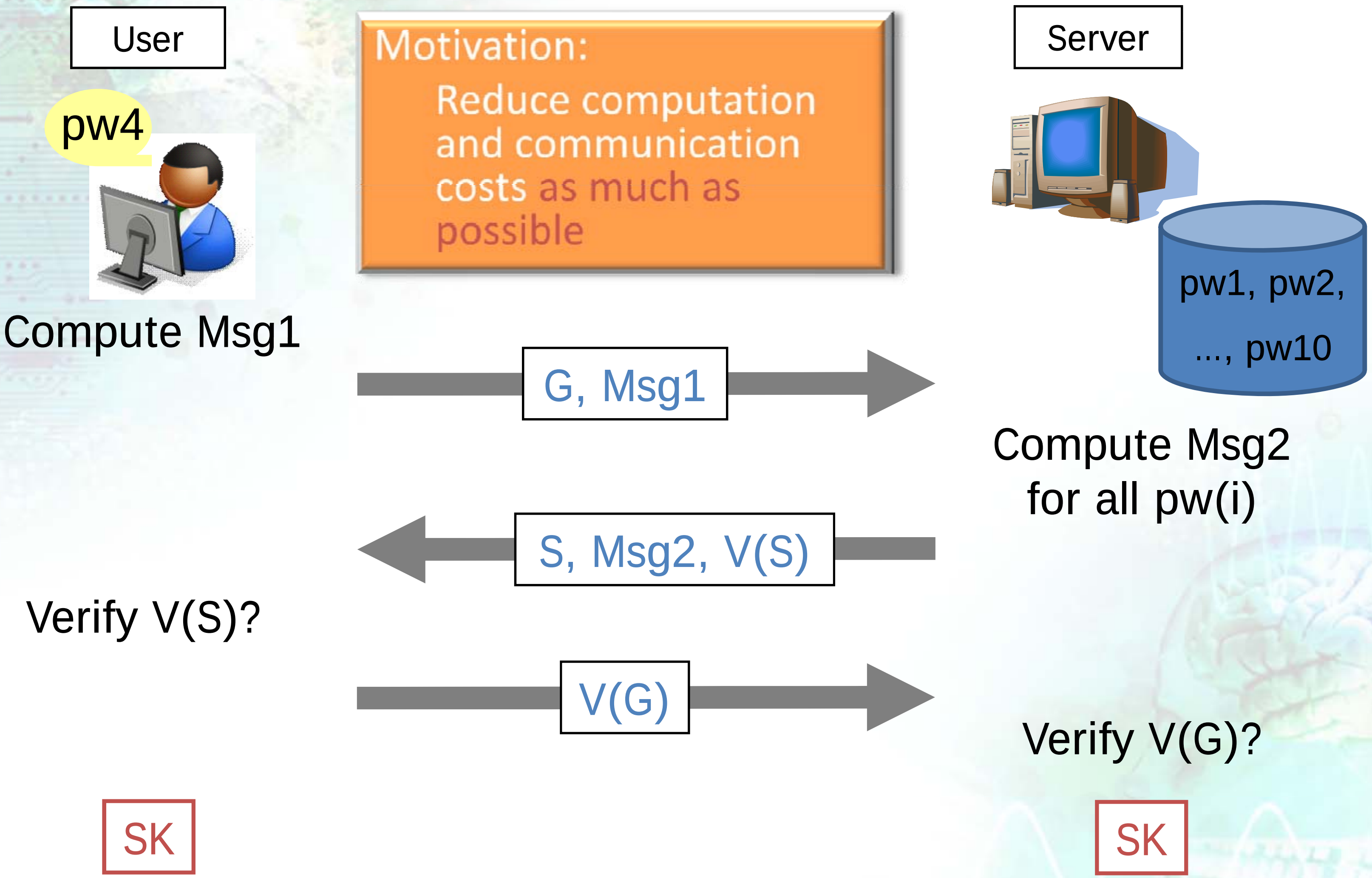
- Simple idea [VYT05]
  - Similar to group authentication
  - A user can blend him/herself to a group



Anonymous PAKE (2/2)

- Anonymous PAKE [VYT05]
  - Combined with OT (Oblivious Transfer)
    - OT for user anonymity
  - Honest-but-curious setting
  - User anonymity against outsider
  - User anonymity against passive server
  - Its threshold construction
    - Based on Shamir's SSS (Secret Sharing Scheme)
    - However, turned out insecure against off-line attacks [SKI07]

How Does It Work?



User

pw4

Compute Msg1

Motivation:

Reduce computation and communication costs as much as possible

Server

pw1, pw2, ..., pw10

G, Msg1

Compute Msg2 for all pw(i)

S, Msg2, V(S)

Verify V(S)?

V(G)

Verify V(G)?

SK

SK

Efficient Anonymous PAKE (EAP)

- Efficient Anonymous PAKE [SKI07]
  - Main idea: construct without OT part
  - Efficiency gain where n is the number of users
    - # of modular exp. on user side is reduced to 3 from 6
    - # of modular exp. on server side is reduced to n+1 from 4n+2
    - Comm. bandwidth is reduced to ((n+2)|hash|+2|p|) from ((n+2)|hash|+(n+2)|p|)
  - Honest-but-curious setting
  - Security
    - Semantic security of session keys
    - User anonymity against outsider
    - User anonymity against passive server
  - Its secure threshold construction

Numerical Comparison

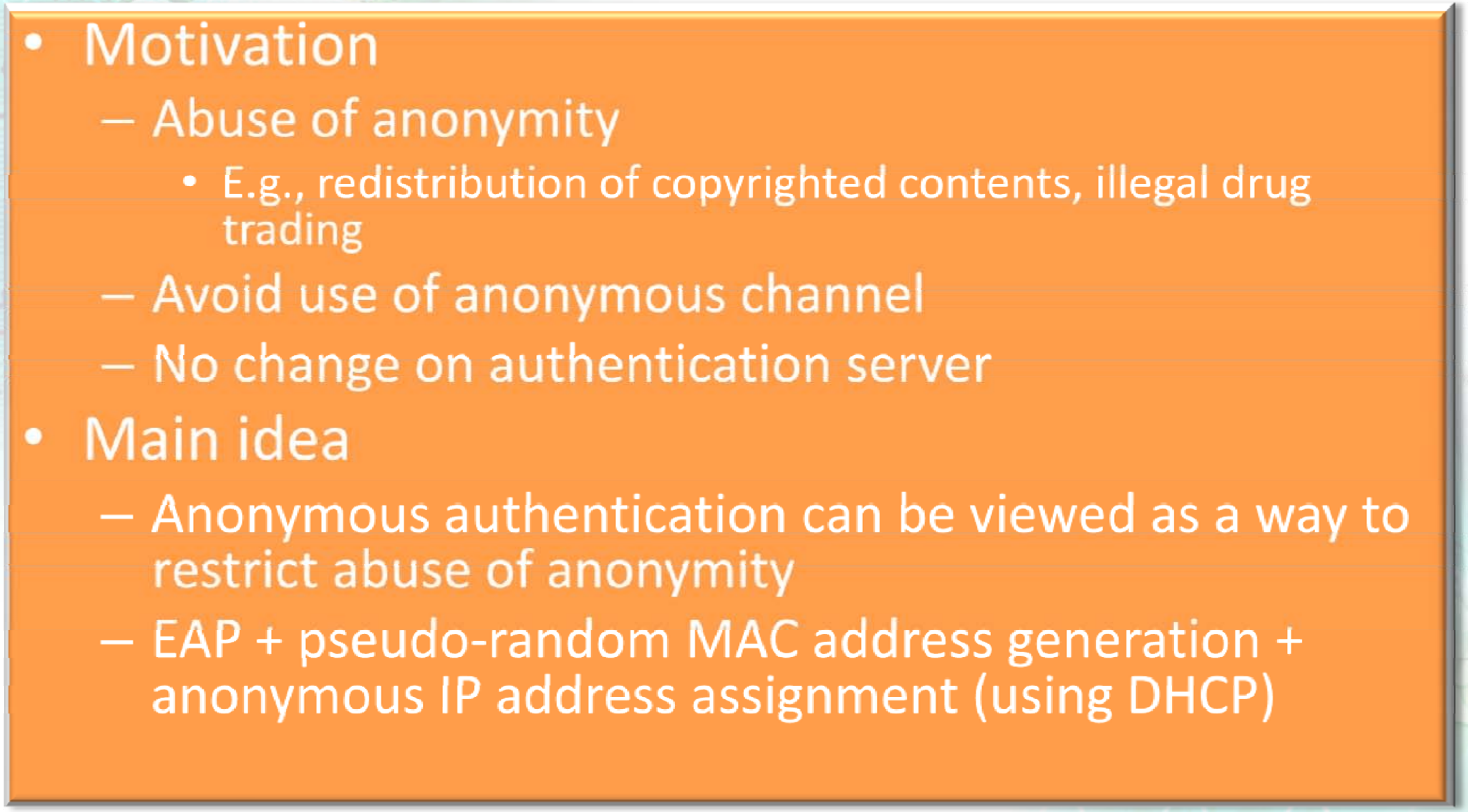
- Parameter setting
  - # of users: 10
  - |ID|=48 bits
  - |p|=1024 bits
  - |hash|=160 bits

Protocols	# of modular exp. on user side	# of modular exp. on server side	Communication bandwidth
[VYT05]	6 (4)	42 (31)	1842 bytes
EAP	3 (2)	11 (10)	562 bytes

  - Numbers in the parentheses are the remaining # of modular exp. after excluding those that are pre-computable
  - The bigger # of users is, the more efficiency gain is

APPLICATION TO IP-BASED WIRELESS NETWORKS [FSKI07]

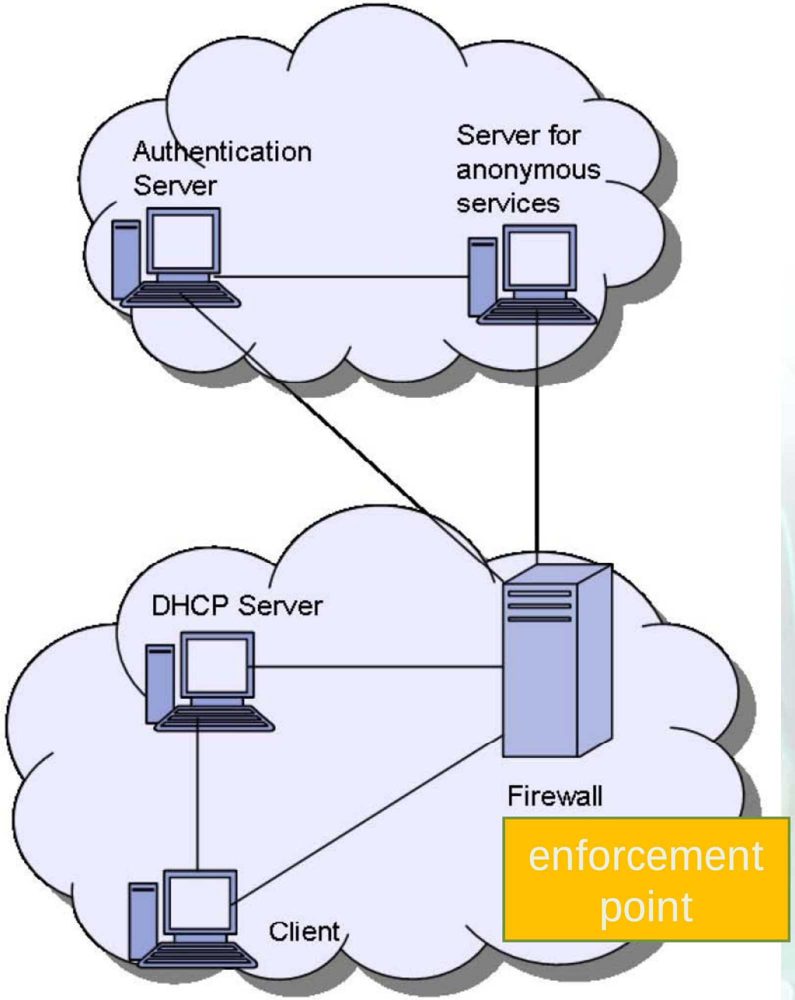
Motivation



- Motivation
  - Abuse of anonymity
    - E.g., redistribution of copyrighted contents, illegal drug trading
  - Avoid use of anonymous channel
  - No change on authentication server
- Main idea
  - Anonymous authentication can be viewed as a way to restrict abuse of anonymity
  - EAP + pseudo-random MAC address generation + anonymous IP address assignment (using DHCP)

Architecture

- Pre-established security association
  - Authentication server and firewall
  - DHCP server and firewall
- Anonymity at link and network layer
  - Pseudo-random 48-bits MAC address
- DHCP (IPv4)
  - Automatic allocation of permanent IP address
  - Dynamic allocation of IP address for temporal use
  - Manual allocation of IP address assigned by network administrator
  - Controlled vs. uncontrolled assignment
    - Exclusively dedicated to anonymous communications



enforcement point

Contributions

- Propose solutions for scenarios
  - In case of controlled IP address assignment
  - In case of uncontrolled IP address assignment
- Possible use
  - Provide user anonymity over wireless hotspots (e.g., Wifi, Wimax)

National Institute of Advanced Industrial Science and Technology
AIST

References (1/2)

Research Center for Information Security

[Ano] Anonymizer, http://www.anonymizer.com/

[BR95] M. Bellare and P. Rogaway, “Provably-Secure Session Key Distribution: The Three Party Case”, STOC’95

[Cha81] D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, 1981

[Cha88] D. Chaum, “The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”, Journal of Cryptology, 1988

[FSKI07] H. Fathi, S. H. Shin, K. Kobara, and H. Imai, “Purpose-restricted Anonymous IPv6 Communications with Scalable Application Servers”, WPMC 2007 (A full version is in submission)

[NIST800-63] NIST, “Information Security: Electronic Authentication Guildline”, Special Publication 800-63, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

References (2/2)

[P1363.2] IEEE P1363.2: Password-Based Public-Key Cryptography, available at http://grouper.ieee.org/groups/1363/passwdPK/index.html

[RR97] M. K. Reiter and A. D. Rubin, “Crowds: Anonymity for Web Transactions”, ACM Transactions on Information and System Security, 1997

[SGR97] P. Syverson, D. Goldschlag, and M. Reed, “Anonymous Connections and Onion Routing”, IEEE Symposium on Security and Privacy, 1997

[SKI07] S. H. Shin, K. Kobara, and H. Imai, “A Secure Threshold Anonymous Password-Authenticated Key Exchange Protocol”, IWSEC 2007

[VYT05] D. Q. Viet, A. Yamamura, and H. Tanaka, “Anonymous Password-based Authenticated Key Exchange”, Indocrypt 2005

SeongHan Shin

E-mail: seonghan.shin@aist.go.jp

THANK YOU FOR YOUR ATTENTION!