

Privacy and Security in Wireless Networks (Part II)

Anthony D. Joseph
CS 294-1

Lecture 9
October 25, 2000

Outline

- Scribe?
- Guest Lecture next week: UMTS
 - Papers/schedule will be changed
- D. Samfat, R. Molva, A Method Providing Identity Privacy to Mobile Users during Authentication
- R. Molva, D. Samfat, G. Tsudik, Authentication of Mobile Users
- Y. Frankel et al, Security Issues in a CDPD Wireless Network

October 25, 2000

CS 294-1 Lecture #9

2

Identity Privacy for Mobile Users [Sam95]

- Need for Authentication
 - User roams into foreign domain and requests billable services
 - Foreign network must determine user's authenticity and *solvency*
- Resulting Security Problems, Issues
 - Unauthorized tracking of user's identity, location, and migration
 - Ex: Employee tracked by employer
 - Also, spoofing by malicious foreign networks

October 25, 2000

CS 294-1 Lecture #9

3

Existing Approaches: GSM

- User requests services using International Mobile Subscriber Identifier (IMSI)
 - IMSI transmitted in clear when first authenticating to network
- Network assigns Temporary IMSI (TMSI)
 - Not usually changed afterwards

October 25, 2000

CS 294-1 Lecture #9

4

Existing Approaches: CDPD

- Diffie-Hellman key exchange between user and foreign host
 - Used to create shared secret key for enciphering user's ID
- But, no validation of foreign host before key exchange
 - Intruder may masquerade as foreign host and generate key with user
 - Classic "Man in the middle" attack exposes user's ID
 - Can be used to gain/abuse service later, also DoS

October 25, 2000

CS 294-1 Lecture #9

5

Levels of Identity Privacy

- Goal
 - Single mechanism for keeping identity secret, while providing access control
- Hiding:
 - User identity from eavesdroppers
 - Handled by most solutions, but have to hide successive aliases
 - User identity from foreign authorities
 - Really only need to prove solvency (but, how to handle billing?)
 - Relationship between user and home authority
 - Prevent abuse, identity theft
 - Identity of the home authority from foreign authorities
 - Not possible without third-party authentication server
 - User behavior from home authority
 - Hard, but needed for perfect secrecy

October 25, 2000

CS 294-1 Lecture #9

6

New Authentication Protocol

- Use MIT's Kerberos or IBM's KryptoKnight protocol in home domain
- Use KK protocol when roaming
 - Idea is to never send IMSI in the clear (only an alias)
 - Also change alias frequently so that alias alone does not enable an eavesdropper to follow the user

October 25, 2000

CS 294-1 Lecture #9

7

Protocol Details

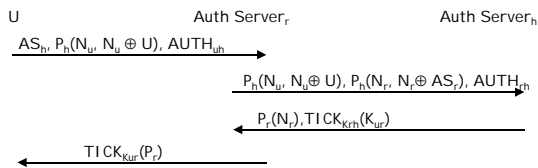
- Symmetric, secret key crypto for "request for authentication" msg
 - $AUTH_{xy}$ (includes N_x, T_x , and sender's id)
 - Nonces and timestamps protect against playback attacks
 - Symmetric \rightarrow need sender's ID in cleartext
- Generate alias using recipient's public key
 - $P_b(N_a, N_a \oplus A)$
 - *One-time, random* alias based on nonce, N_a
 - Only B can identify A
 - Use alias to hide A in $AUTH_{ab}$

October 25, 2000

CS 294-1 Lecture #9

8

Untraceable Authentication Protocol



- $AUTH_{uh} = E_{K_{uh}}(U \oplus E_{K_{uh}}(T_u \oplus E_{K_{uh}}(N_u)))$, N_u, T_u
- Home domain validates:
 - The mobile user to the remote domain
 - The remote domain to the mobile user

October 25, 2000

CS 294-1 Lecture #9

9

Enhancing Anonymity

- Protocol discloses relationship between user and AS_h
 - Violates C3
- Solution
 - User computes alias for AS_h before contacting AS_r

October 25, 2000

CS 294-1 Lecture #9

10

Conclusion

- Important need for identity privacy
 - GSM and CDPD have weaknesses in providing sufficient user anonymity
- Protocol protects identity of user from eavesdroppers and foreign authorities
 - Also provides reverse authentication
- But, significant computational complexity
 - Also, law enforcement issues

October 25, 2000

CS 294-1 Lecture #9

11

Authentication of Mobile Users [MoI94]

- Same authors as first paper
 - Need to establish temporary, authenticated ID when roaming
 - Let's concentrate on the differences
- Design Criteria
 - Focus on maintaining strict separation of security domains
 - Avoid sending domain-specific secret info out of domain
 - Low latency handover between foreign domains
- Transparency to Users
- User Identity Confidentiality
 - Identity and movements of user should be kept secret
- Minimal Overhead
 - Minimize # of msgs sent between home and foreign domains

October 25, 2000

CS 294-1 Lecture #9

12

Existing Approaches

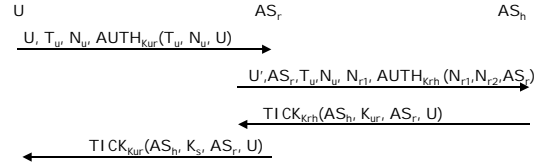
- GSM uses triples for roaming authentication
 - Inefficient BW and home domain resource usage
 - Assumes secure fixed network between MSCs
 - Secret, home grown A5 and A8 algos are bad
- CDPD uses Diffie-Hellman key exchange
 - Uses triples for roaming authentication
 - Assumes fixed network is secure
 - Vulnerable to long-term impersonation

October 25, 2000

CS 294-1 Lecture #9

13

New Authentication Protocol



- Fairly similar to the last paper
- Possibility for decryption of user authentication request, $AUTH_{K_{ur}}(T_w, N_w, U)$ if keys are weak
 - AS_h substitutes nonce, N_{r2} , for user request
 - Use shared key between home and foreign domains
- Useful because mobile may not sufficient CPU power for sophisticated encryption / decryption

October 25, 2000

CS 294-1 Lecture #9

14

Wireless/Cellular Considerations

- Need fast handoff when user crosses foreign domains
 - Have former domain forward a short-term ticket
 - Cut latency by avoiding contacting home domain
- User enters foreign domain B from foreign domain A
 - AS_a forwards AS_b a ticket containing session key, K_s before contacting AS_h
 - AS_b can authenticate U immediately with K_s
 - For any following contact with AS_b , U must be authenticated

October 25, 2000

CS 294-1 Lecture #9

15

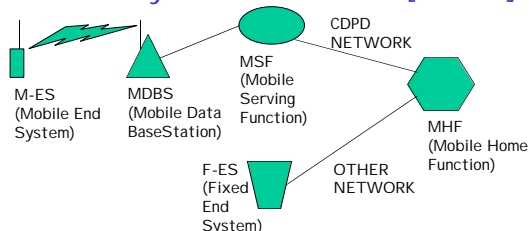
5-minute Break

October 25, 2000

CS 294-1 Lecture #9

16

Security Issues in CDPD [Fra95]



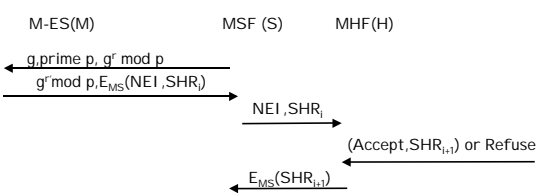
- CDPD architecture
 - Sending digital data on top of idle voice channels
 - Providing Internet connectivity

October 25, 2000

CS 294-1 Lecture #9

17

Current Authentication Protocols



- Initialization
 - H issues Network Equipment ID upon user receiving mobile Shared History Record (SHR)

October 25, 2000

CS 294-1 Lecture #9

18

Interceptor Attack

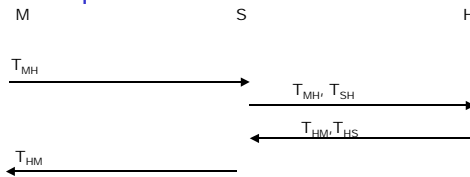
- Interceptor masquerades as S during Diffie-Hellman key exchange
 - M will disclose NEI and SHR to intruder
- Intruder can use SHR to:
 - Obtain service billable to M
 - Prevent M from receiving updated SHR
 - Leads to M being denied service later due to incorrect SHR

October 25, 2000

CS 294-1 Lecture #9

19

Requirements for New Protocol



- Solution:
 - Establish bilateral trust between all network components
 - Authenticating foreign agent is useful when foreign agent charges exorbitant fees for service: home agent can deny authentication to such foreign agents

October 25, 2000

CS 294-1 Lecture #9

20

Potential Faults

- The authors point out possible faults:
 - If verification by the Home Agent fails, there is no way to tell whether the guilty party is a masquerading M or a masquerading S
 - If the verification by S fails, the system could potentially go into an endless repetition of the authentication procedure.

October 25, 2000

CS 294-1 Lecture #9

21

Summary

- What are the requirements of a Mobile Network?
- In AMPS networks, roaming users had to manually request a temporary phone number in the foreign domain to receive (make) phone calls
- Today, calls are automatically forwarded to foreign domains
 - Significant security requirements

October 25, 2000

CS 294-1 Lecture #9

22

Security Requirements

- The link between domains must be secure
- Roaming anonymity should be provided
- Need to protect the secret key of the mobile
 - IS41 approach: punch special code into the handset
 - GSM approach: SIM card contains all the information
 - Not completely secure
- System should limit handoff latency (to scale)
 - Should avoid contacting home for each foreign handoff
- Should be able to verify foreign agents
 - Diffie-Hellman doesn't validate foreign agent

October 25, 2000

CS 294-1 Lecture #9

23

Security Requirements

- Need to limit frequency and quantity of control msgs
- Must be robust against Denial of Service attacks
 - PCS CDMA vulnerability: call count
 - CDPD: Shared History Record
- Secure, private location monitoring?
 - Sometimes, need to pinpoint the location of a mobile call
 - Critical in emergency situations like a 911 call (will be law)
 - But, who gets access to such information?

October 25, 2000

CS 294-1 Lecture #9

24

Detailed Message Exchange

- (T1) $T_{MH} = \langle R_{MH}, T'_{MH} = A_{MH}(S_{MH}, R_{MH}, ID_S - \text{"response"}) \rangle$
- (T2) $T_{SH} = \langle T_{MH}, R_{SH}, T'_{SH} = A_{SH}(T'_{MH}, R_{SH}, ID_M - \text{"relay"}) \rangle$
- (T3) $T_{HS} = \langle S'_{HM}, T'_{HM} = A_{HM}(R_{MH}, S_{HM}, ID_S - \text{"refresh"}), T'_{HS} = A_{HS}(R_{SH}, T'_{HM}, ID_M - \text{"accept"}), \text{"accept"} \rangle$
- (T4) $T_{HM} = \langle S'_{HM}, T'_{HM} = A_{HM}(R_{MH}, S'_{HM}, ID_H - \text{"refresh"}), \text{"refresh"} \rangle$

October 25, 2000

CS 294-1 Lecture #9

25