

Privacy and Security in Wireless Networks (Part I)

Anthony D. Joseph
CS 294-1

Lecture 8
October 18, 2000

Outline

- Scribe?
- Mid-project checkpoints around Thanksgiving week
- PCS papers
 - Brookson, C. GSM security: a description of the reasons for security and the techniques. IEE Colloquium on 'Security and Cryptography Applications to Radio Systems', June '94.
 - D. Brown, Techniques for privacy and authentication in Personal Communication Systems. IEEE Personal Communications, August '95.
 - Ross Anderson, GSM hack -- operator flunks the challenge. Personal communications in RI SKS DIGEST 19.48, Nov '97.
- Wireless Networking paper
 - A. Aziz and W. Diffie, Privacy and Authentication for Wireless Local Area Networks. IEEE Personal Communications, First Quarter 1994, p. 25-31.

October 18, 2000

CS 294-1 Lecture #8

2

Security In Wired Telephony

- Anonymity
 - Not possible, can block Caller ID, but not Automatic Number Identification (800, 911)
- Authentication
 - Based upon "wire," ANI info
- Signaling protection
 - Requires physical access to wire or SS7 network
 - Can't spoof ANI (sort of)
- User Data Protection
 - Requires physical access to wire

October 18, 2000

CS 294-1 Lecture #8

3

Security in Analog Cellular

- Anonymity
 - None, IMSI transmitted in the clear
- Authentication
 - IMSI sent in the clear on signaling channel
- Signaling protection
 - None, vulnerable to cloning, interception
 - Highway overpass sniffers
 - Simple split channel authentication solution
 - IMSI on signaling channel, PIN on voice channel
- User Data Protection
 - None, famous interception cases
 - Added simple, slow hopping

October 18, 2000

CS 294-1 Lecture #8

4

Desired Security Attributes

- Anonymity
 - Protect users from identification
- Authentication and Key Agreement
 - Secure, reliable authentication of users
 - Generation of session key for signaling and data
- Signaling protection
 - Secure signaling, protected from interception
- User Data Protection
 - Protect privacy of conversations
 - Except for Lawful Interception?
 - Must be very efficient and low cost (power & \$\$)

October 18, 2000

CS 294-1 Lecture #8

5

Security in GSM [Brookson94]

- Goals
 - Strong authentication and privacy of users
 - Protect operator against fraud
 - Make radio path *as secure as* the wired path!
 - Issue bills to right people, protect services
 - Protect operators from one another
- Minimal cost
 - Low delay in call setup or later communication
 - Low bandwidth overhead
 - Low complexity
 - Low cost

October 18, 2000

CS 294-1 Lecture #8

6

GSM Security Issues

- Have to account for environment
- Need secure procedures for
 - Generation and exchange of keys
 - Exchange of information between operators
 - Confidentiality of algorithms (!)
 - Security through obscurity (not a good idea)
- Biggest threat is employees and other systems
 - Leaked keys, insecure billing, corruption

October 18, 2000

CS 294-1 Lecture #8

7

GSM Functions

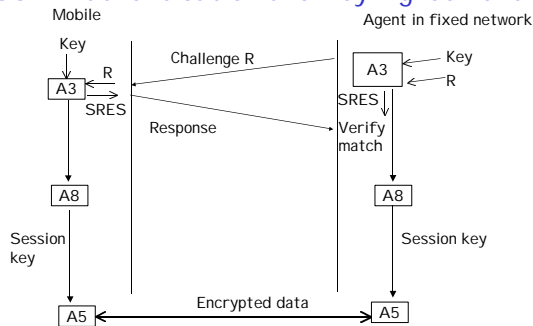
- Anonymity
 - End users use real IMSI to obtain a temp IMSI
 - All subsequent operations use the temp IMSI
- Authentication and Key Agreement
 - Challenge response mechanism
 - A3 algorithm is used to compute Response from Challenge using a shared, secret key

October 18, 2000

CS 294-1 Lecture #8

8

GSM Authentication and Key Agreement



October 18, 2000

CS 294-1 Lecture #8

9

GSM Functions (cont'd)

- Signaling protection
 - Sensitive information (telephone numbers) transmitted in call setup after encrypted channel has been established
- User data protection
 - All data protected using A5 series algorithm
 - Efficient, low cost symmetric key algorithm

October 18, 2000

CS 294-1 Lecture #8

10

GSM Security Implementation



- A3 implemented within a Smart Card
 - "Tamper proof" smart card containing the key
- A5 is in the data path and must be fast (in the phone hardware)
 - Implemented in low cost, custom ASICs for speed
 - A5/1 is "strong" encryption
 - Weaker A5/2 for "export"-level encryption

October 18, 2000

CS 294-1 Lecture #8

11

GSM Roaming Support

- Home network sends 1 to 5 triples: *<Challenge, Response, Session Key>*
- Why not exchange secret key?
- "Trust, but verify!"
 - Protects home network from rogue operator
 - One tuple required every x minutes or for each call
 - Or operator with bad security, employees, ...

October 18, 2000

CS 294-1 Lecture #8

12

GSM Issues

- A3 standard has been compromised
 - Leaked by accident, vulnerabilities exposed
 - Can extract key from a SIM → cloning possible
- A5 standard has also been leaked
 - Can change A3 for a service provider, but not A5
- Protocol vulnerabilities
 - Standard supports non-encrypted channel
 - Could be used by rogue BTS to spoof access
 - No authentication of BTS → Mobile

October 18, 2000

CS 294-1 Lecture #8

13

GSM Hack [Anderson '97]

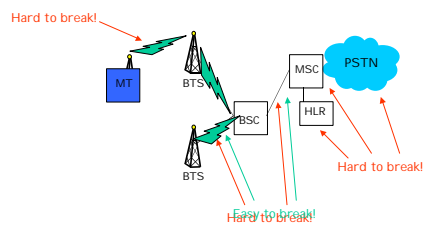
- Operator proposes silly challenge
 - Break my network for money!
- Cambridge University research group
 - Found nifty solution for problem!
 - Remember early comment about threats
- Go after the easy part, not the hard part
 - Break the network, not the link

October 18, 2000

CS 294-1 Lecture #8

14

GSM Hack



October 18, 2000

CS 294-1 Lecture #8

15

GSM Hack

- Equipment
 - About \$20,000 worth of equipment to intercept authentication information on links between MSC ↔ BSC or BSC ↔ BTS
- Operator Response
 - What challenge?
- PacBell's "can't be cloned" slogan for GSM
 - Didn't last long...
- Solutions?

October 18, 2000

CS 294-1 Lecture #8

16

5-minute Break

October 18, 2000

CS 294-1 Lecture #8

17

Wireless LANs [Aziz, Diffie '94]

- Security in wireless harder since physical protection is impossible!
 - Easy to eavesdrop on wireless networks
- Wireless security choices
 - Link-level security
 - Deploy in islands, minimal changes
 - What about intermediate links?
 - Machine-machine authentication, can't authenticate end users
 - End-to-end security
 - Can mutually authenticate end users

October 18, 2000

CS 294-1 Lecture #8

18

E2E Public/Shared Key Authentication and Communication

- Public key cryptography
 - Use to authenticate BTS and mobile
 - Use to establish session key
- Shared key cryptography
 - *Efficient* privacy while exchanging data
 - Algorithm to use is *negotiated*
- Variant of Diffie-Hellman
 - Minimize expensive private key operations (symmetric DES operations)

October 18, 2000

CS 294-1 Lecture #8

19

Protocol Steps: Mobile to Base

- Mobile sends a signed certificate from CA
 - Contains binding from station name to public key, signed by CA (Certifying Authority)
 - Assumes certificate was received by mobile over an authenticated channel with a CA
- Also includes in the message to the Base
 - A random 128-bit challenge value (CH1)
 - A list of available shared key methods
 - Ex: FEAL-32, DES, IDEA, Blowfish, 3DES, ...
 - Other details (e.g., desired key lengths)

October 18, 2000

CS 294-1 Lecture #8

20

Protocol Steps: Base to Mobile

- Base verifies certificate
- Base sends a signed certificate
 - $E(\text{Pub_Mobile}, \text{RN1})$
- Includes in the message
 - List of chosen shared key methods
 - $\text{Sig}(\text{encrypted RN1}, \text{chosen methods}, \text{CH1}, \text{original list of methods})$
- Mobile can verify
 - Validity of Base certificate
 - Its message was not tampered or replayed
 - Ex: Weaker list of SKCs
 - Avoids 1 private key op at mobile (signing 1st message)

October 18, 2000

CS 294-1 Lecture #8

21

Protocol Steps

- Mobile to Base
 - $E(\text{Pub_Base}, \text{RN2})$
 - $\text{Sig}(\text{encrypted RN2}, \text{encrypted RN1 from base})$
- Now, have a shared secret:
 - (RN1 XOR RN2)
 - Uses 2 pieces of information instead of 1
 - Why?
- Limits damage from lost mobile key
 - Can't intercept previous traffic w/o both base and mobile's private keys

October 18, 2000

CS 294-1 Lecture #8

22

Efficiency

- Computationally expensive portion of public key crypto systems are the private key operations
- Mobile does two private key operations
 - To decrypt RN1 from message #2
 - To sign message #3
- Base does two private key operations
 - To sign message #2
 - To decrypt RN2 from message #3

October 18, 2000

CS 294-1 Lecture #8

23

Access Control

- The 3-way protocol only authenticates endpoints (mobile and base)
- Still need access control
 - Could be simple ACL

October 18, 2000

CS 294-1 Lecture #8

24

Data Transport

- Use additive shared key-based stream cipher
 - Break stream into packets for transport
- Each side has a synchronized pseudorandom stream
 - Generates key for enciphering and deciphering of each packet
- Issues:
 - Packet reordering and corruption
 - Periodic re-keying of cipher key

October 18, 2000

CS 294-1 Lecture #8

25

Data Packet Reordering

- How to deal with possible reordering of data stream?
 - Additive stream ciphers must stay in sync with pseudorandom streams on each side
- Solution:
 - 64-bit message ID field in the clear in each packet

October 18, 2000

CS 294-1 Lecture #8

26

Data Stream Integrity

- How to verify stream has not been tampered with or corrupted?
- Add 32-bit checksum
 - Encrypted as part of each packet
 - Provides integrity checking, not replay protection
- IP can replay packets anyway, so have to catch at higher layers

October 18, 2000

CS 294-1 Lecture #8

27

Changing Cipher Key

- Periodic change is important
 - In case, key is broken, limits exposure
- Change protocol based on R1 and R2
 - Need both to break
- Nice scheme avoids sequence numbers
 - Hard to maintain/store

October 18, 2000

CS 294-1 Lecture #8

28

Privacy and Authentication for PCS [Brown '95]

- Authentication and Key Agreement (AKA)
- Generalize AD '94 to *3-phase security model*
 1. Provisioning, obtain a "bonafide" (credentials) from a trusted server (*a la CA-signed certificate*)
 2. Establish credibility with local service provider and transfer credentials to the provider (proxy)
 3. Establish a shared secret
 - Challenge/response (e.g., GSM)
 - Public key-based certificates (e.g., Aziz-Diffie)

October 18, 2000

CS 294-1 Lecture #8

29

Secret Key Systems: Provisioning

- GSM uses smart card
 - Contains subscriber information and secret key
 - Tamperproof (sort of)
 - Secret key *never* leaves home network
 - Phones are interchangeable
- IS-41
 - Shop manually enters subscriber info
 - User manually enters shared secret, "A-key"
 - Sent by alternate means, why?
 - A-key *never* leaves home network
 - Shared Secret Data (SSD) derived using over-the-air protocol in home network

October 18, 2000

CS 294-1 Lecture #8

30

SKS: Roaming Access Control

- Goal
 - Provide just enough info to authenticate mobile
 - Prevent impersonation by VLR
- Two SKS Solutions
 - Share secret information
 - Share results of secret information (the computation)
- GSM keeps user ID confidential: TMSI

October 18, 2000

CS 294-1 Lecture #8

31

SKS: Roaming Access Control

- GSM
 - HLR gives visited network small # of tuples
 - (RAND, SRES, Kc) [can use alternative to A3 & A8]
 - Must consume tuples at some rate/min or 1 per call
 - Interception → only temporary impersonation
- IS-41
 - HLR gives the SSD to VLR
 - Interception → long-term impersonation!
 - Avoid problem by using a call count to detect cloning
 - Only works if the user uses their phone, otherwise clones work (casual users very vulnerable)
 - Periodic global challenge broadcast
 - Reduce signaling overhead

October 18, 2000

CS 294-1 Lecture #8

32

Public Key System Thoughts

- Future PCS systems would use public key based authentication
- Higher network bandwidth
 - Needed to send larger keys/digests
- More powerful processors
- Asymmetric decomposition of cryptographic functions
 - More work in network, less in mobile

October 18, 2000

CS 294-1 Lecture #8

33

PKS: Benefits

- Eliminates network ↔ network secret exchanges
 - Credentials validated using CA
 - But, still have to validate user profile
- Private keys are never distributed outside the source
- True anonymity
 - Avoids need for TMSI s
- Mutual validation of network and mobile

October 18, 2000

CS 294-1 Lecture #8

34

PKS: Reality

- Network signaling bandwidth constrained
 - Bandwidth is a valuable resource
- Cheap processors aren't very powerful
 - Transmeta changes this assumption
 - But, waste power on authentication?
- No true global distributed, hierarchical certificate authority yet
 - How to setup third-party trust relationships

October 18, 2000

CS 294-1 Lecture #8

35

Summary

- Authentication is a complex process
 - Mutual verification is desirable, but not always achievable
- Network to network roaming is more complex
 - Limited trust → limit vulnerability
- SKS approaches dominate
 - But, PKS approaches are interesting
- Continues next week...

October 18, 2000

CS 294-1 Lecture #8

36