EAP-SIM Security Analysis

Mobility Solutions

Keyspace and Mutual Authentication Weaknesses

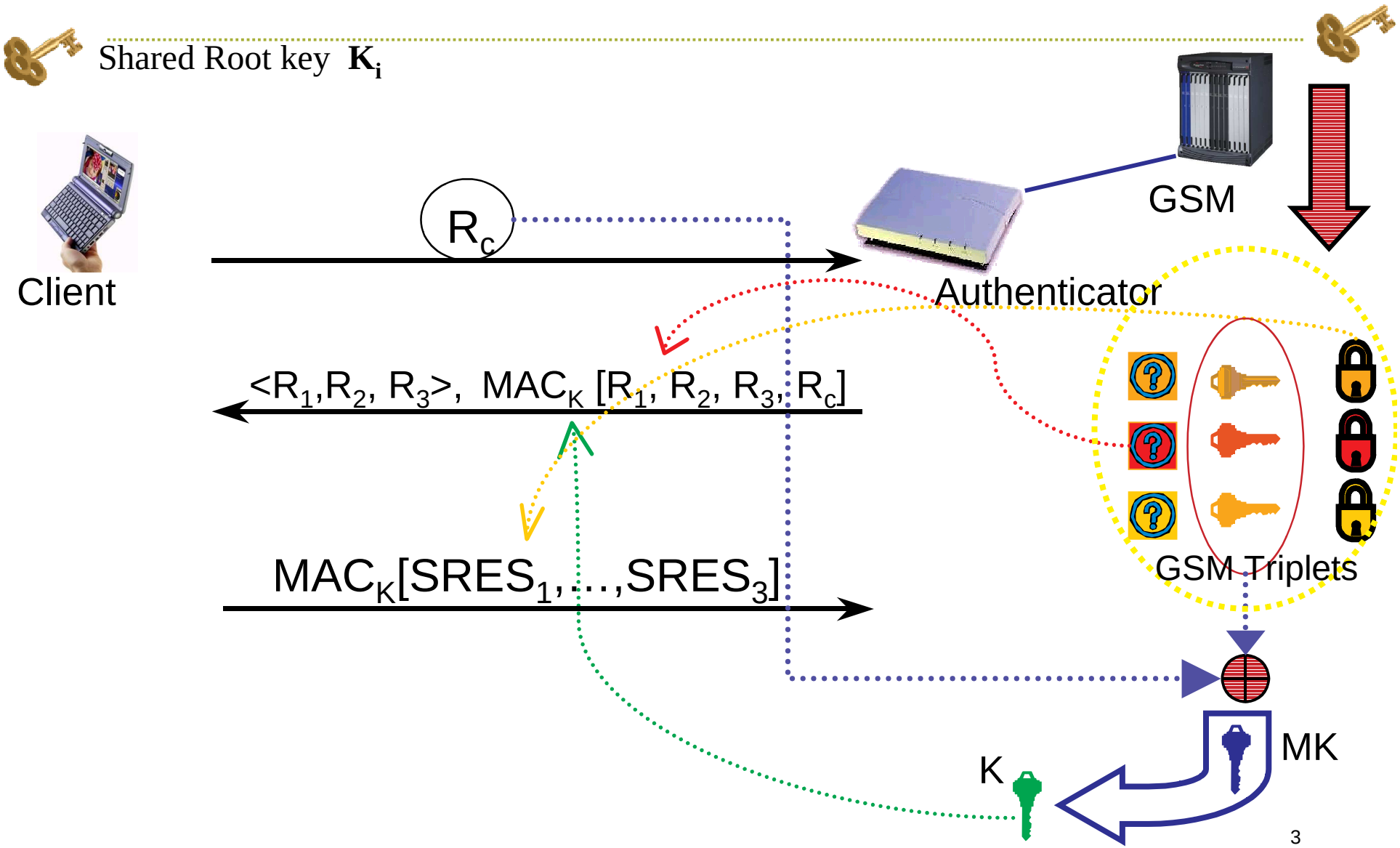
Uri Blumenthal (analysis done by Sarvar Patel)
Member of Technical Staff

Lucent Technologies
Bell Labs Innovations

EAP-SIM Draft and its Security Claims

- Current EAP-SIM provides interoperability with GSM 2G cellular
- Current EAP-SIM claims to provide 128-bit security
  - Two 64-bit attacks are described
- Current EAP-SIM claims to be a Mutually Authenticated Protocol with Session Independence.
  - Session independence at the triplet level cannot be achieved

EAP-SIM Cryptographic Essentials



Attack 1 – bring strength down to 64-bits

- Impersonator chooses R and guesses corresponding K_c
  - *Probability of success* 2^{-64} **not** 2^{-128}
  - Now attacker knows appropriate K_c for the R
- Impersonator sends <R R R> to the victim
  - Attacker makes all the triplets equal
  - Thus attacker knows K_c for all R's
- Attacker creates Master Key MK and completes protocol

- Solution 1: Enforce the check on R's in the protocol
  - **Client** must ensure that all received R's are different, or reject
- Solution 2: Include SRES into key derivation input for MK
  - Gives 96-bit strength in total (even for one triplet)

Attack 2 - brute-force the 64-bit key

- Condition: network uses N=1 and then moves to N=3
  - Attacker observes the exchanges of single triplets
  - The network later switches to multiple triplets
- Attacker brute-forces 3 keys of 64-bit when N=1
  - Each Kc recovery requires 2^{64} operations
  - Verification: compare responses – calculated with observed
- Now attacker can impersonate the network for N=3
  - Send <R_1, R_2, R_3, MAC> to the victim (since $Kc_{1,2,3}$ are known)
  - Complete the protocol
- Solution 1: never allow using single triplet
- Solution 2: include SRES to key derivation input for MK

Lack of session independence

- If Kc values for three triplets are compromised, then attacker can impersonate the network forever
- Reason: Rc is not included in the Kc derivation
  - GSM specific: triplets are usually pre-computed by Network
  - GSM does not offer mutual authentication
- Assumption *"But Kc will never get exposed!"*
  - If such were true, there would be no need to ever generate new triplets
  - Kc in GSM designed to be used for one session only!
  - Solution: none

Conclusions

- Current EAP-SIM does **not** provide 128-bit security
  - Two successful 64-bit attacks were described
  - Solutions – minor improvements to the protocol (not currently incorporated)
- Lack of session independence on triplet level
  - Can’t be practically solved