

The First International ICST Conference on Security and Privacy
in Mobile Information and Communication Systems



Impersonation Attacks on a Mobile Security Protocol for End-to-End Communications

Reiner Dojen, Vladimir Pasca, Tom
Coffey

Data Communications Security Laboratory,
Department of Electronic & Computer Engineering
University of Limerick, Ireland



Overview of Presentation

- ◆ Introduction to Security Protocols
- ◆ The LYH Mobile End-to-End Authentication and Secrecy Protocol
- ◆ Forging Certificates for the LYH Protocol
- ◆ Attacks to Impersonate a Mobile Users
- ◆ Attacks to Impersonate a Base Stations
- ◆ Fixing the LYH Protocol
- ◆ Conclusions

Security Protocols

- ◆ Protocols based on cryptographic system – usually running over insecure channels
- ◆ Provide: confidentiality, integrity, authentication, non-repudiation etc





Attacks on Security Protocols

- ◆ Attacks: Replay, Parallel Session, Type Flaw, Impersonation, etc.
- ◆ “Attacker never play by the rules”





Attacks on Security Protocols

- ◆ Attacks: Replay, Parallel Session, Type Flaw, Impersonation, etc.
- ◆ “Attacker never play by the rules”





Attacks on Security Protocols

- ◆ Attacks: Replay, Parallel Session, Type Flaw, Impersonation, etc.
- ◆ “Attacker never play by the rules”





Attacks on Security Protocols

- ◆ Attacks: Replay, Parallel Session, Type Flaw, Impersonation, etc.
- ◆ “Attacker never play by the rules”





The LYH Mobile End-to-End Authentication and Secrecy Protocol

- ◆ Proposed by Lee, Yang and Hwang in 2003
- ◆ Aims to provide end-to-end authentication between mobile users connected via series of base stations
- ◆ Mobile Users trust Base Stations
- ◆ Authentication based on signed certificates
- ◆ Session key selected by Base Station is distributed
- ◆ Three Phases: Certification, Authentication, Communication



Certification Phase

- ◆ Signature scheme has 3 parameters:
 - p : randomly selected large prime
 - q : large prime factor of $p-1$
 - g : equals $m^{(p-1)/q}$ for some m satisfying $1 < m < p-1$ and $m^{(p-1)/q} > 1$
- ◆ Principals select their own private key x randomly and generate public key $y = g^x$
- ◆ Certification Authority's (CA) public key securely distributed to all principals
- ◆ Principals send their public key to CA for signature

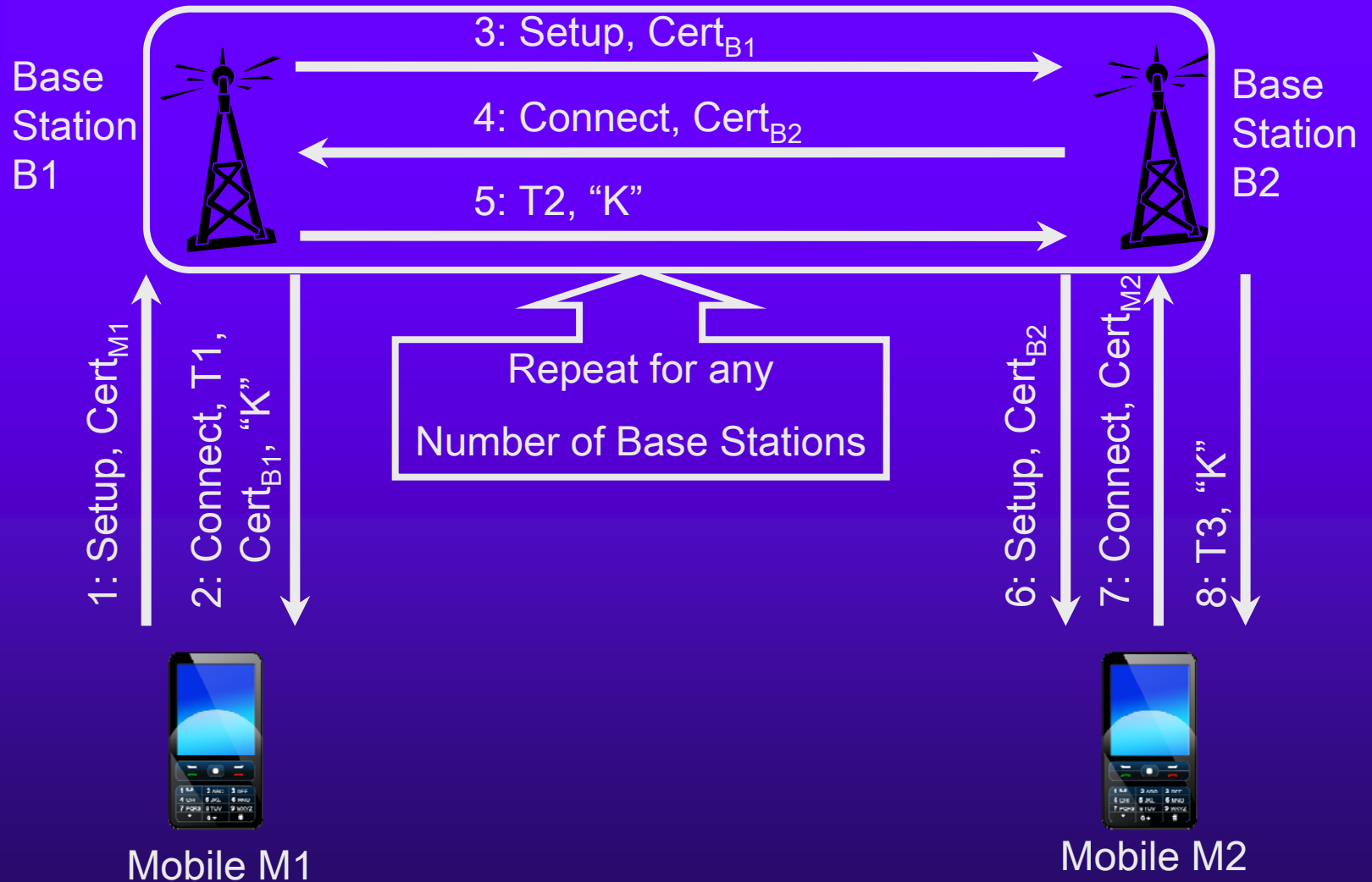


Validity of CA's Signature

- ◆ Signature on message M consist of triple (M, s, t) :
 - M : message itself
 - s : random signature component,
 $s = g^r \text{ mod } p$, for random r
 - t : message dependant component,
 $t = -s - h(M)x_{CA}^{-1} r \text{ mod } p$
- ◆ Signature is valid if:
$$y_{CA}^{s+t} s^{h(M)} \text{ mod } p = 1 \text{ mod } p$$



Authentication Phase





Communication Phase

- ◆ After successful authentication phase, mobile users employ session key K for communication
- ◆ No direct authentication $M1 \leftrightarrow M2$
- ◆ Authentication only to “direct partner”
- ◆ Both mobile users (and all involved base stations) possess session key K
- ◆ No other principal has key K (?)



Forging Signatures of CA

- ◆ Signature (M, s, t) , where
$$s = g^r \text{ mod } p$$
$$t = -s - h(M)x_{CA}^{-1} r \text{ mod } p$$
- ◆ Attacker selects $r = x_{CA}$, consequently
$$s = y_{CA} (= g^{x_{CA}} = g^r) \text{ mod } p$$
$$t = -s - h(M) \text{ (as } x_{CA}^{-1}x_{CA} = 1) \text{ mod } p$$
- ◆ Can create signatures on arbitrary messages, including bogus certificates

Impersonating Mobile Users M1

Base
Station
B1

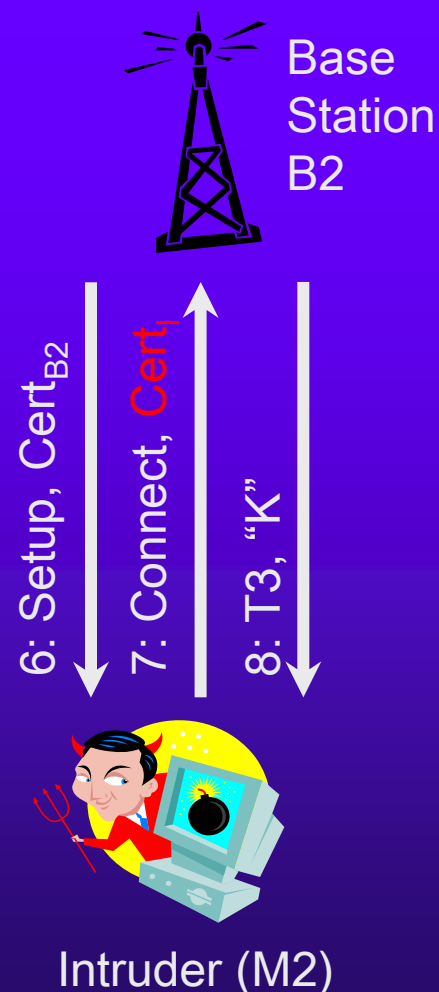


Intruder (M1)

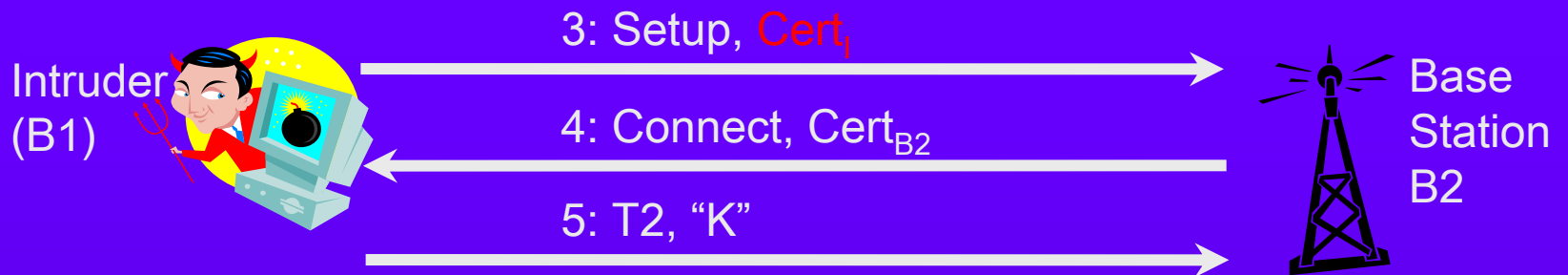
- ◆ Intruder creates bogus certificate $Cert_I$
- ◆ Initiates protocol as M1, replacing $Cert_{M1}$ with $Cert_I$
- ◆ Attacker knows key K

Impersonating Mobile Users M2

- ◆ Intruder creates bogus certificate $Cert_I$
- ◆ Intercepts messages from B2 to M2
- ◆ Responds protocol as M2, replacing $Cert_{M2}$ with $Cert_I$
- ◆ Attacker knows key K



Impersonating Base Station B1

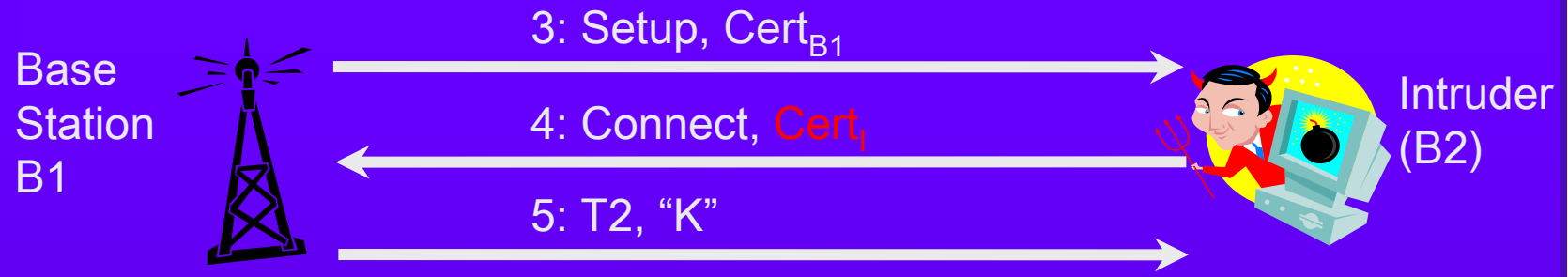


Mobile M1

- ◆ Intruder creates bogus certificate $Cert_I$
- ◆ Intercepts messages from M1 to B1
- ◆ Continues protocol as B1, replacing $Cert_{B1}$ with $Cert_I$
- ◆ Attacker selects key K



Impersonating Base Station B2



- ◆ Intruder creates bogus certificate $Cert_I$
- ◆ Intercepts messages from B1 to B2
- ◆ Continues protocol as B2, replacing $Cert_{B2}$ with $Cert_I$
- ◆ Attacker knows key K



Mobile M2



Fixing the Protocol

- ◆ Algebraic simplifications allow to break signature scheme
- ◆ Elgammal signature scheme similar, but no (known) weaknesses
- ◆ Signature (M, s, t) , where
$$s = g^r \text{ mod } p$$
$$t = r^{-1} (h(M) - x_{CA}s) \text{ mod } p$$
- ◆ Signature is valid if:
$$g^{h(M)} \text{ mod } p = y_{CA}^s s^t \text{ mod } p$$

Conclusions

- ◆ LYH protocol aims to provide end-to-end authentication
- ◆ Algebraic simplifications allow creation of bogus signatures (certificates)
- ◆ Intruder can impersonate any principal (mobile user or base station)
- ◆ Proposed to use Elgammal signature scheme to fix protocol