



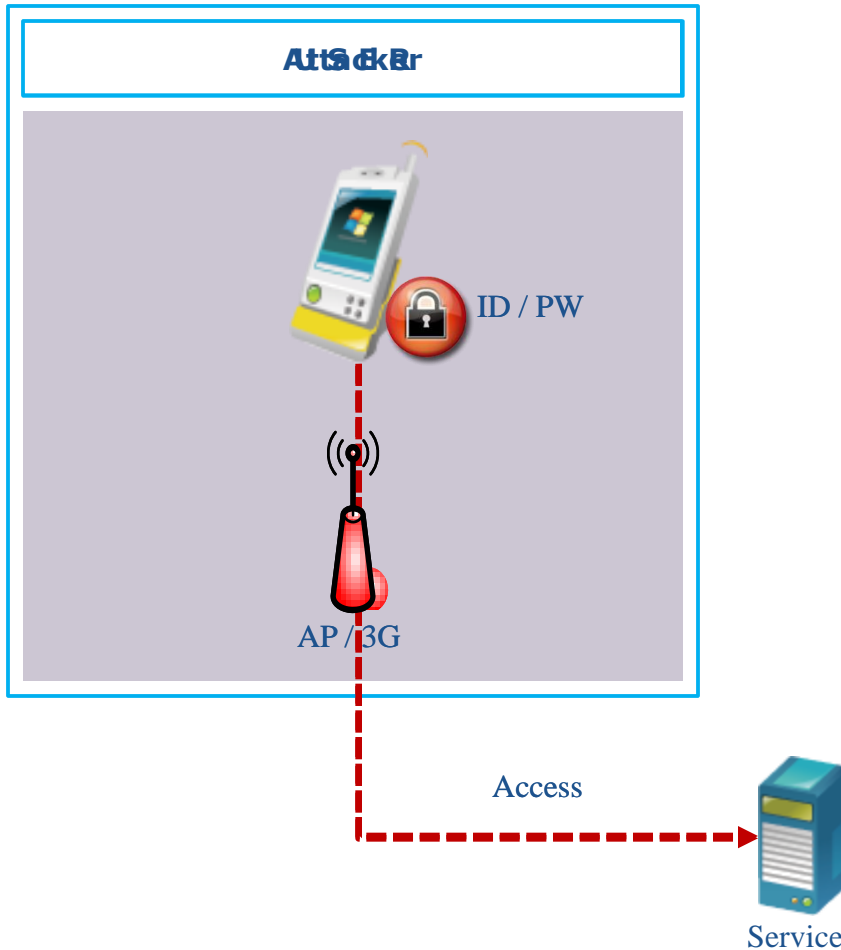
# **Authentication Method for Preventing damages from lost and theft Smartphone**



**SoonChunHyang Univ., Korea  
Kihun, Jang  
Penetration Test Team  
nvdark@gmail.com**

# INTRODUCTION

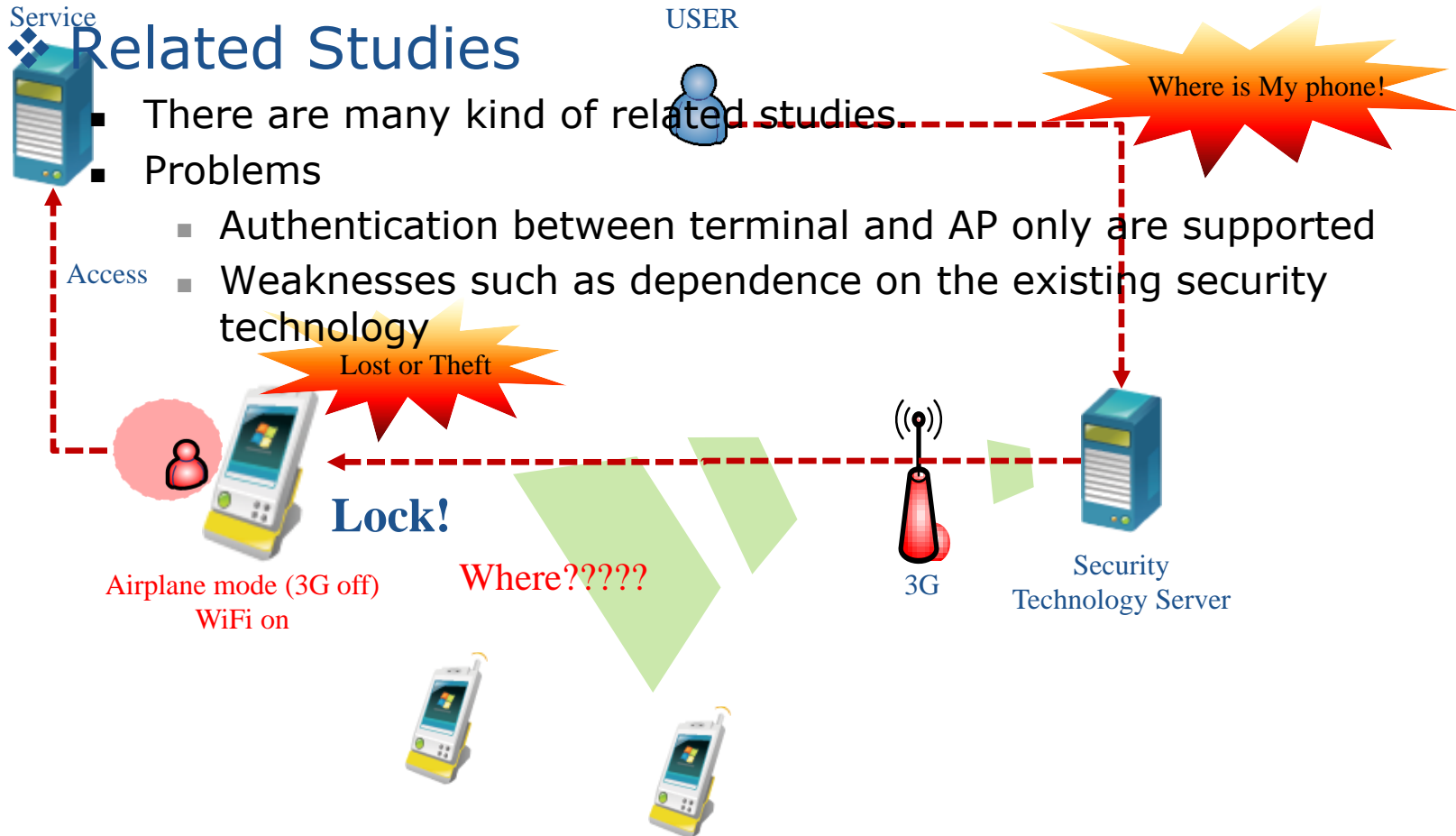
## Security Threats



- ❖ Brazil scoring 75% on phone/data loss and 82% on abuse under disguised identity, and Russia scoring 68% on phone/data loss and 82% on abuse under disguised identity

# Related existing studies for Smartphone loss an Prevention

## Security Threats



# Proposed Authentication Techniques

## Authentication Protocol

```
//Client
  send MN,DSC

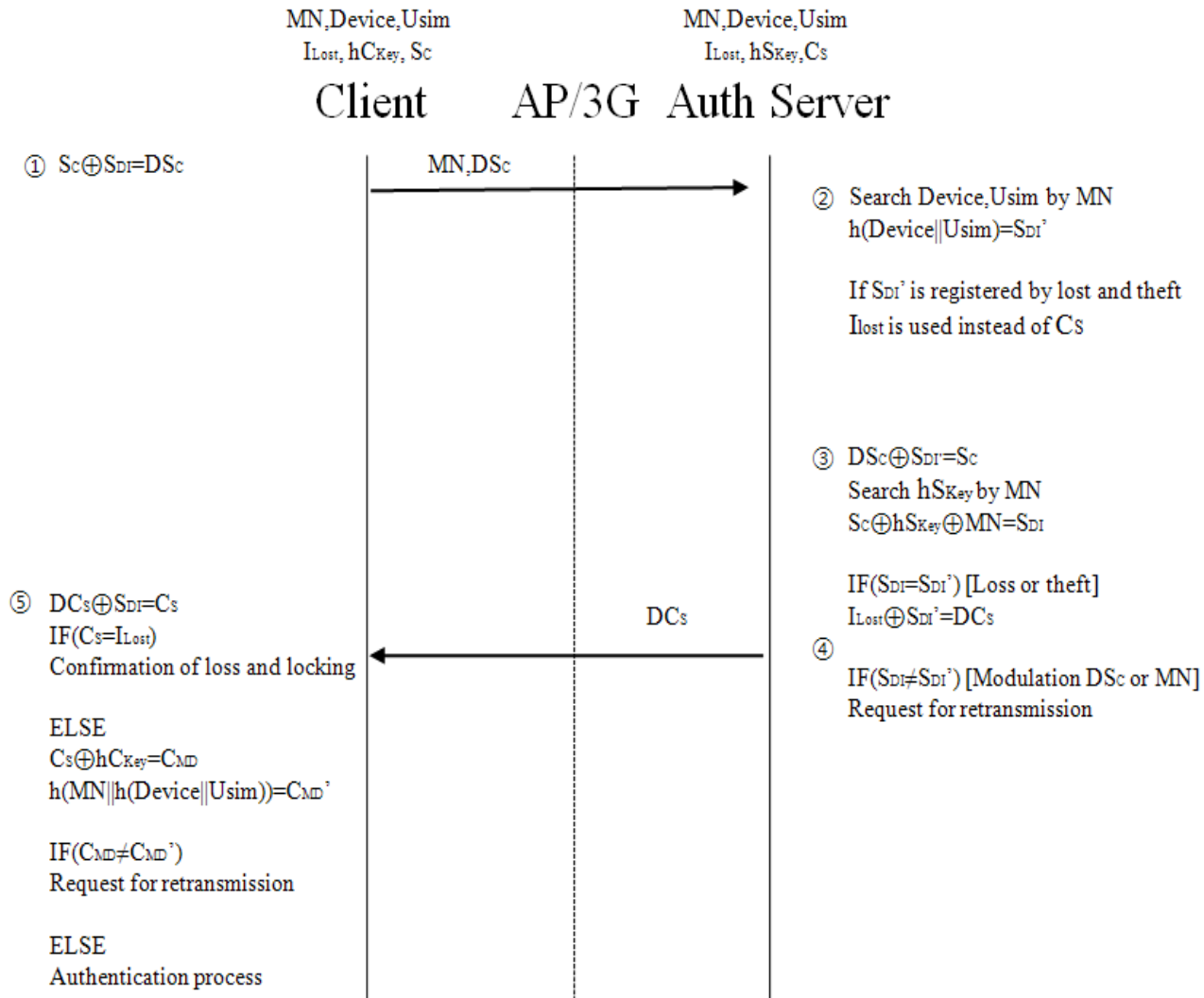
//Server
  receive MN,DSC
  calculate SDI from DSC,MN
  IF(SDI==SDI'){
    IF(loss or theft){
      Generation DCS using Ilost
    }
    ELSE{
      Generation DCS
    }
  }
  ELSE{
    failed
  }
  send DCS|

//Client
  receive DCS
  calculate Ilost from DCS
  IF(Ilost==Ilost'){
    Lock Mobile phone
  }
  IF ELSE(CMD==CMD'){
    Generation New SC, CS(Server)
    Internet Access
  }
  ELSE{
    failed
  }
}
```

Mobile Number	Product ID	Loss or Theft
82106415	0068542	<input checked="" type="checkbox"/>
Usim /		Cs
0910005614		725399401291
Ilost /		
14D9EEF9651892F1A26BA13DB4C32BBD		
hSkey		
7C16F4BA43D585B62CB0F2258BF5130E		

# Proposed Authentication Techniques

## Loss and theft verifying process



# Proposed Authentication Techniques

## Analysis of safety

Offset	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017
SEARCH	31	46	41	32													

Offset	-007	-006	-005	-004	-003	-002	-001	000	+001	+002	+003	+004	+005	+006	+007
MODIFY								12	34	56	78				

검색의 최대 길이: 패킷내 적용 개수: 1

검색 범위: Winsock 1.1

- Send
- SendTo
- Recv

필터 이름: 1

바꾸기를 시작할 위치:

- 패킷의 처음부터 바꿈
- 검색한 곳을 기준으로 바꿈

☆이후 적용 안 함

- 패킷의 활동 여부
- 패킷 전송 안 함

검색 위치:

- 패킷의 처음부터
- 패킷내 어디든지

1 :10101 8 RecvFrom

0000 31 46 41 32 35 41 46 36

1 :10101 8 RecvFrom

0000 12 34 56 78 35 41 46 36

Trace

- auth protocol test ARP Spoof
- auth protocol test ARP Spoof C to S
- auth protocol test ARP Spoof S to C

Sender IP: 192.168.123.196

Target IP: 192.168.123.254

Sender Mac: 40fc899c13fa

Target Mac: 001cc0393dba

Checked

DataChange Option

- CheckTCP
- CheckUDP
- WriteTrace

530733814 123456 Change Data

- ❖ Simple program using proposed protocol for testing
- ❖ WPE PRO MULTI and SnoopSpy is used for test tool
  - Monitoring and Attack on Frequency Modulation
  - Replay Attack
  - Spoofing Attack
  - Substitution Attack





# CONCLUSIONS

- ❖ Expected that the proposed method may be used in accessing the Internet through other wireless Internet network
- ❖ Expected effects from the proposed method include the inability on the part of the third party that has picked up a lost or stolen smart phone to use services requiring the Internet by using account information stored on the lost phone, and the capability of the smart phone to prevent subsequent illegitimate use of identity and the likelihood of information leaking out.
- ❖ However, in order to preclude the third party from using services through the wireless Internet before declaration of loss and theft is received, further study should be explored especially for the process of user authentication in the future.



Thank you