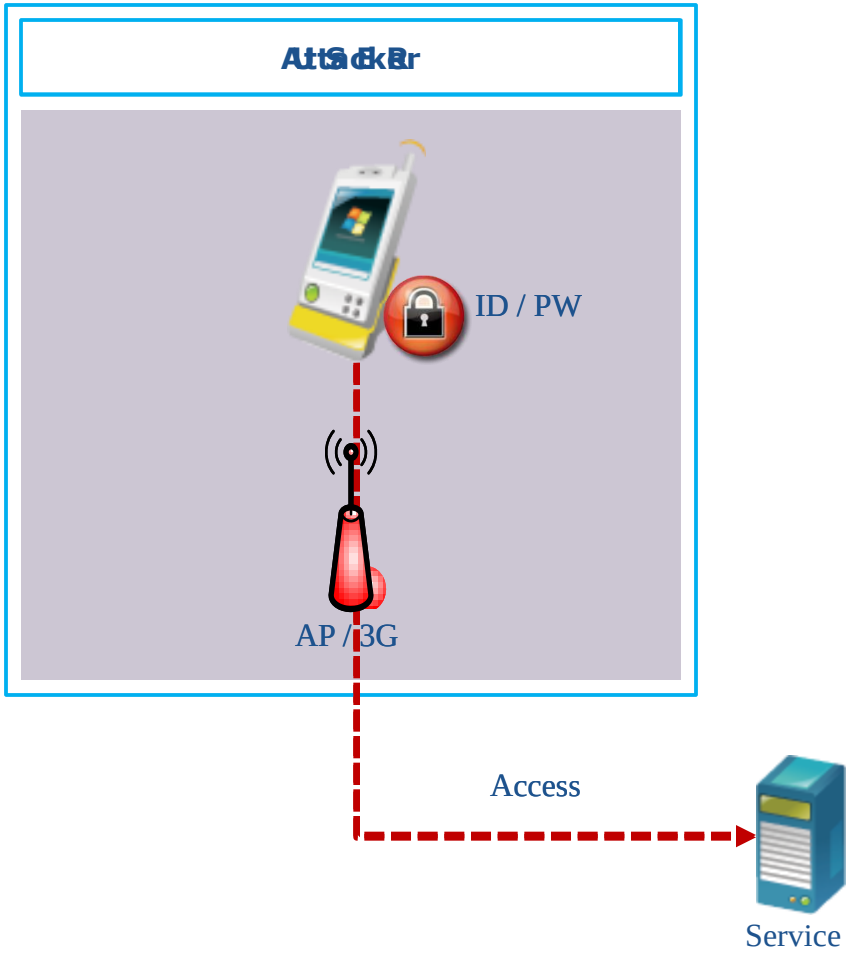
Authentication Method for Preventing damages from lost and theft Smartphone

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

INTRODUCTION

Security Threats



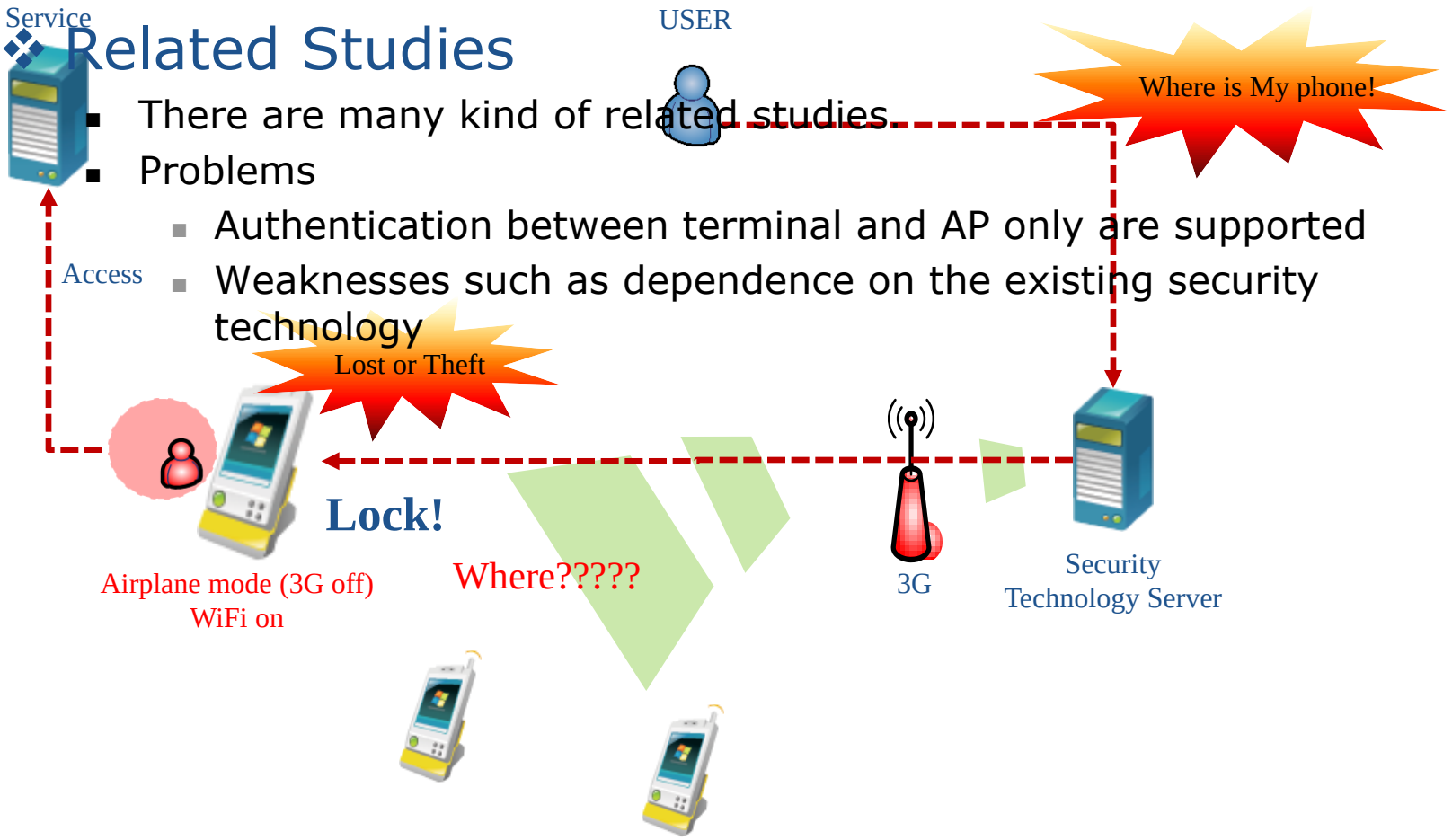
- Brazil scoring 75% on phone/data loss and 82% on abuse under disguised identity, and Russia scoring 68% on phone/data loss and 82% on abuse under disguised identity

nvdark@gmail.com

Related existing studies for Smartphon loss an Prevention

Related Studies

- There are many kind of related studies.
- Problems
  - Authentication between terminal and AP only are supported
  - Weaknesses such as dependence on the existing security technology

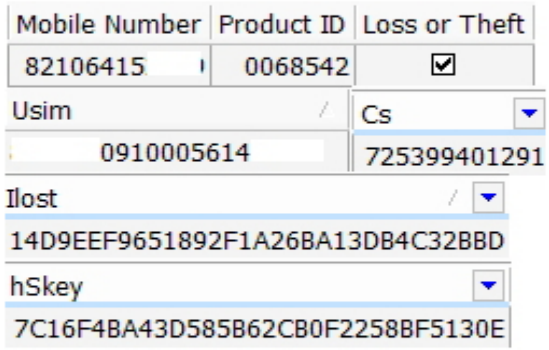


nvdark@gmail.com

Proposed Authentication Techniques

Authentication Protocol

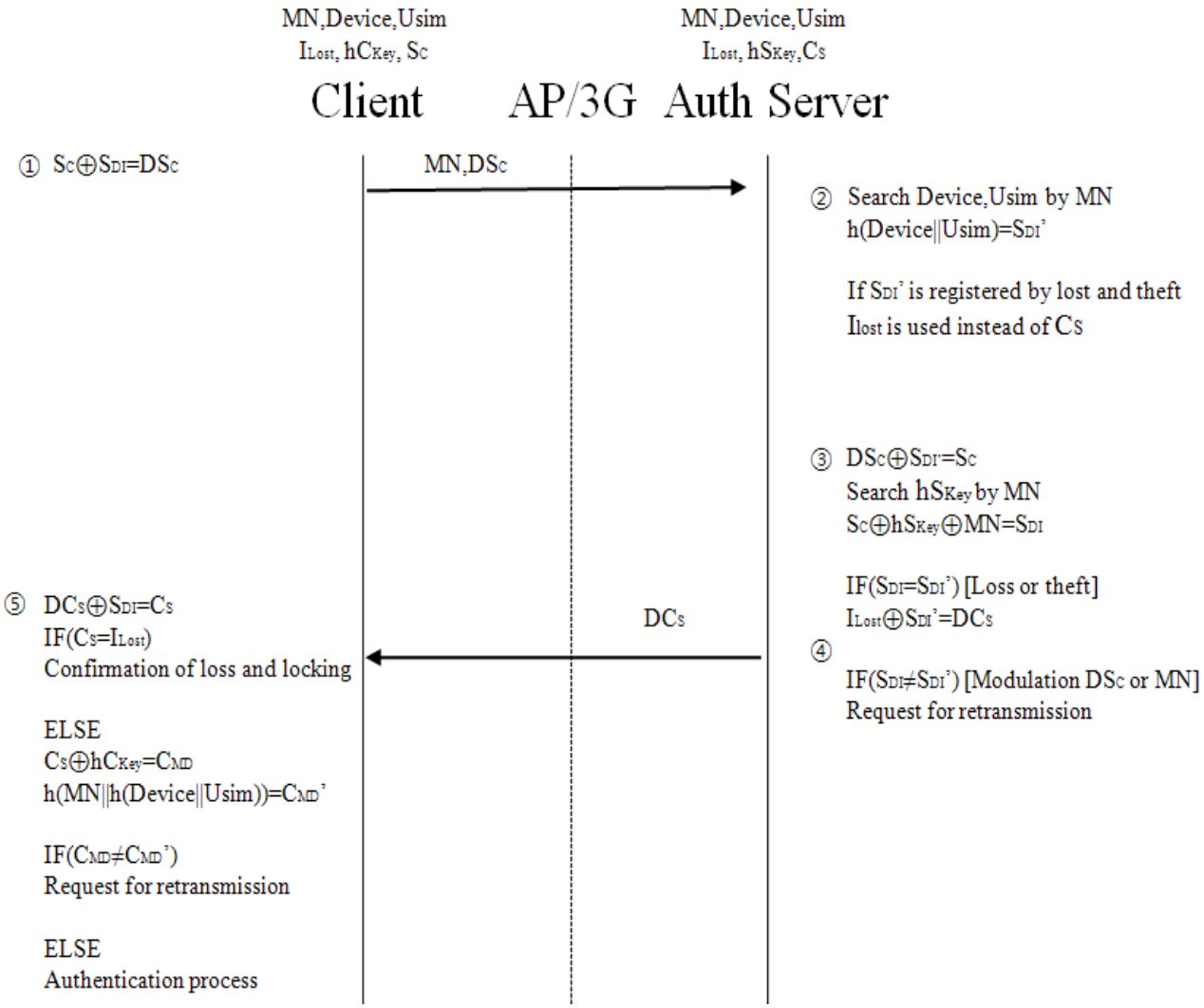
```
//Client
        send MN,DSC

//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
        }
```



nvdark@gmail.com

Proposed Authentication Techniques

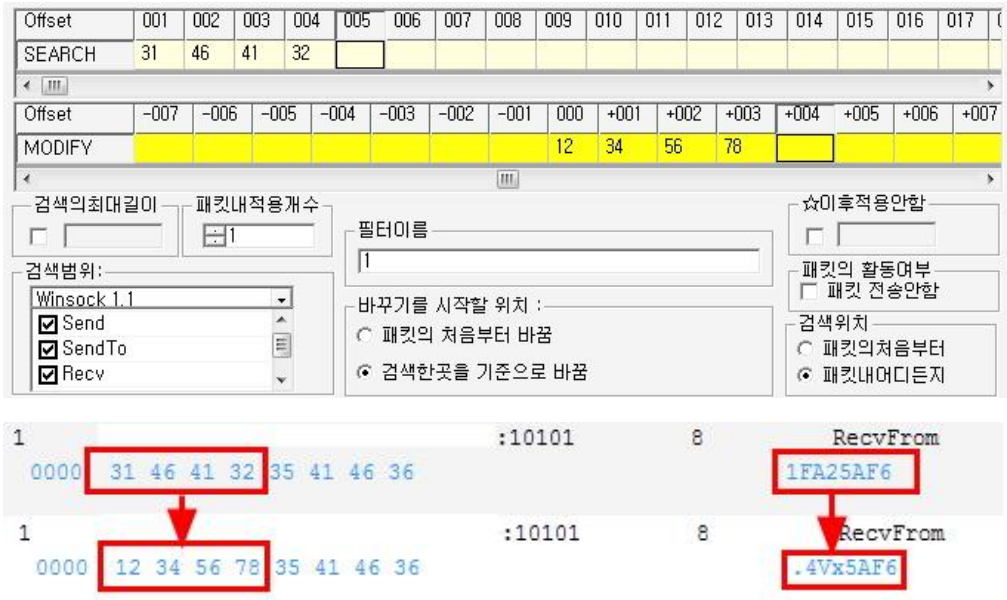
Loss and theft verifying process

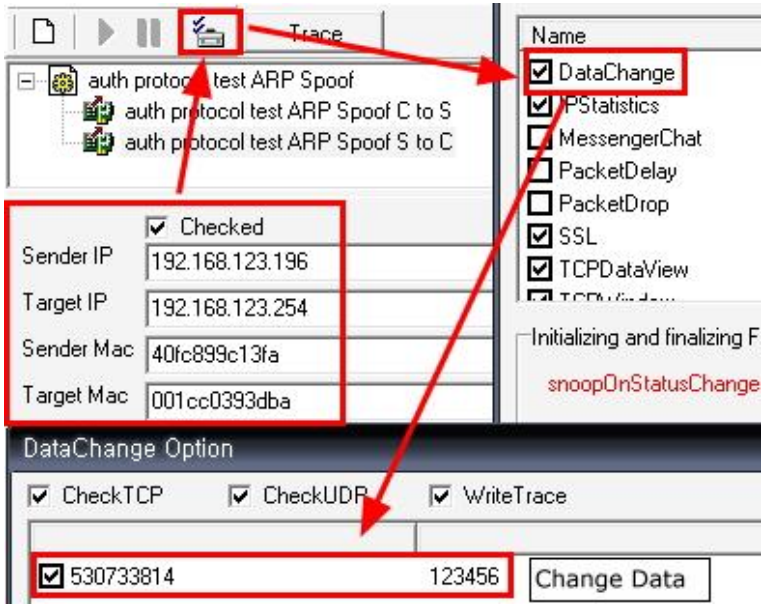


nvdark@gmail.com

Proposed Authentication Techniques

Analysis of safety





- 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

nvdark@gmail.com

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.

nvdark@gmail.com

Thank you

nvdark@gmail.com