

Adaptive Security Support in Future Internet through Class of Security Level

2008.06.20.

Jongho Park

Computer Networks and Security Laboratory
Electrical Engineering and Computer Science
Seoul National University



Contents

- Introduction
- Class of Security Level
 - Overview
 - Quantification of Security Features
 - Routing Path Setup
- Conclusion



Introduction

- Future Internet
 - Robust and Available
 - Inherently secure
 - Anonymous and private
 - Accountable when necessary

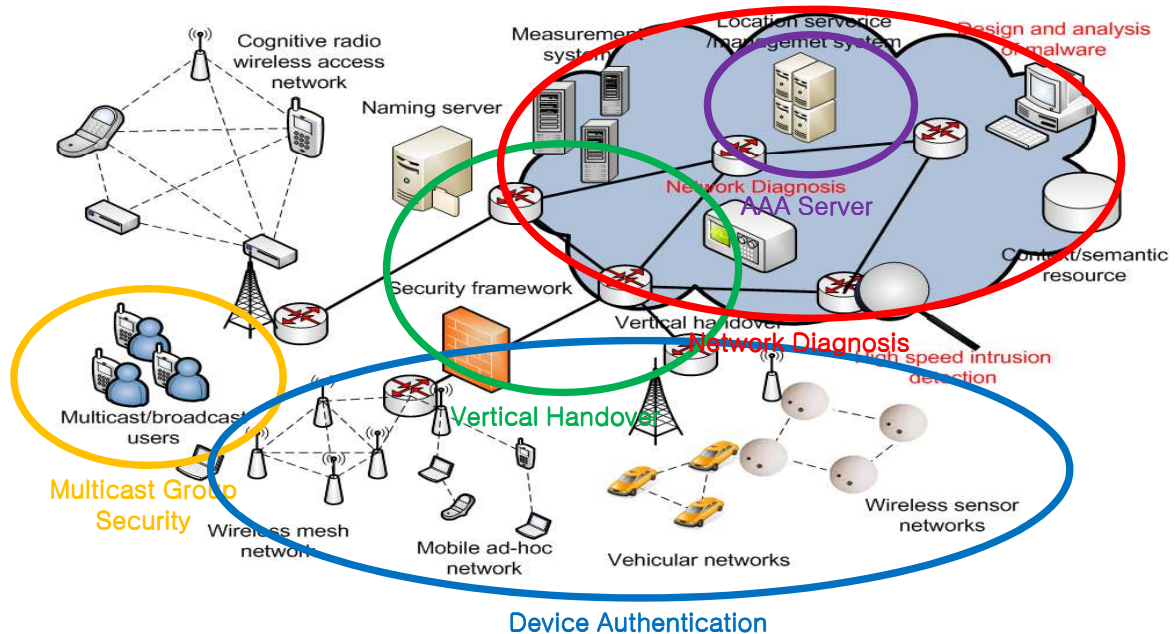


Introduction

- Future Internet Security
 - User-centric security
 - Multimedia : Multicast group security
 - Internet of Services → Internet of Things
 - Device authentication
 - Privacy
 - Heterogeneous Network
 - Secure Handover
 - Authentication (Location of AAA Server)
 - Unified Network Diagnosis

Introduction

■ Future Internet Security



Motivation

- Inherent security features needed
 - Inherently secure network
 - Widespread of Security Critical Service
 - E-commerce, E-Business, Online banking, video on demand, etc.
 - Various User's needs on security
 - User-centric security service
 - Limited network capability
- ➔ to provide different security service a user by user

Class of Security Level

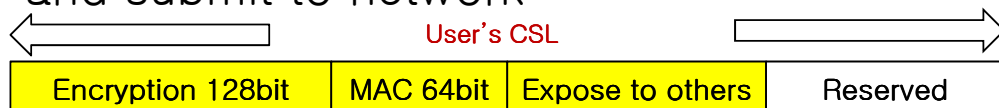
■ Overview

- CSL : to provide security services in the network layer
 - Quantification of security features
 - Confidentiality, Integrity, Authenticity, Privacy Guarantee
 - Routing path setup using CSL
 - Network CSL : capability of network to support user's wanted CSL.
 - User's CSL : CSL value that user want to be served from network

Class of Security Level

■ Procedure

1. A user selects security features to be served and submit to network



2. Decide whether network can support user's selection
 1. Network can provide user's CSL
 - ➔ judges the possible paths to the destination
 2. Network can't provide user's CSL
 - ➔ suggest the other possible candidate path with less security level



Quantification of Security Features

■ Steps

- Measure the degree of safety for embodiment of security features
 - Security algorithms, key length, time spent to break the encrypted message
- Measure the resources needed to implement the security algorithms
 - Computation power, memory space, link's bandwidth
- Calculation of relative importance of security features
 - To express different security features as the same units

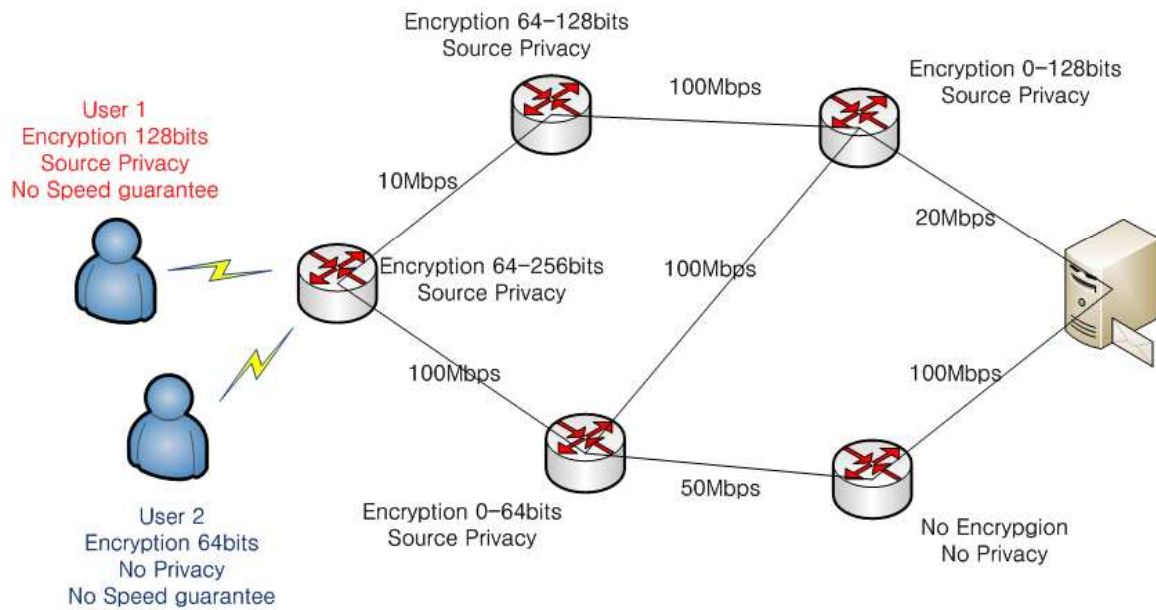


Routing Path setup

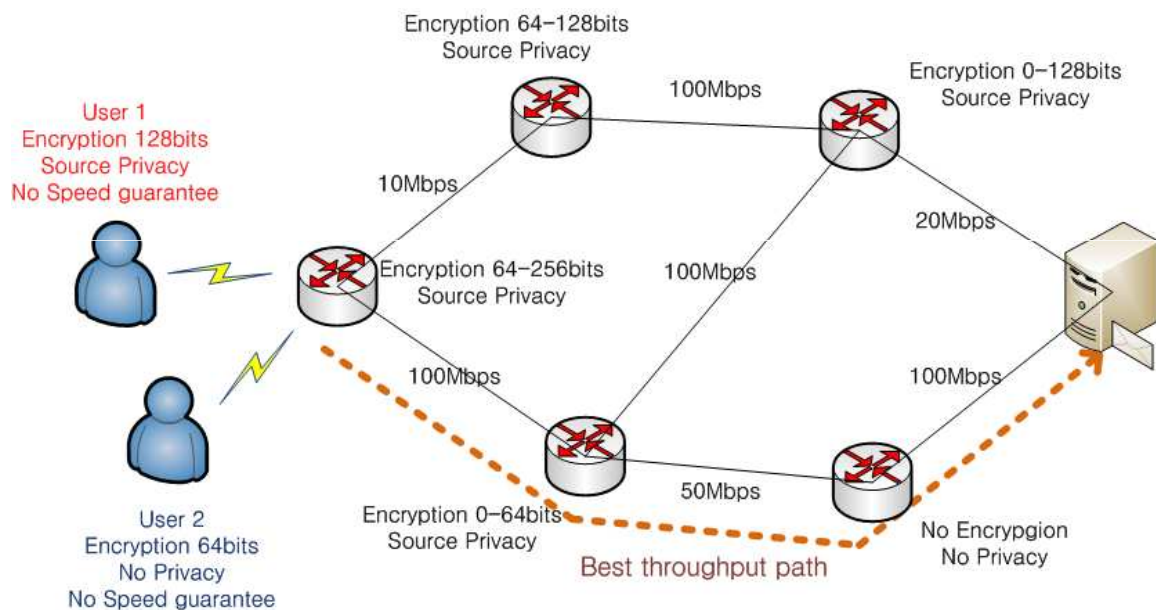
■ Procedures

- Determine whether the network can satisfy the user's security requirement(CSL) or not
 - Supportable security algorithms, key length, extra resources, bandwidth
- Transfer the network's status to the other networks
 - Availability of security algorithms and the resources

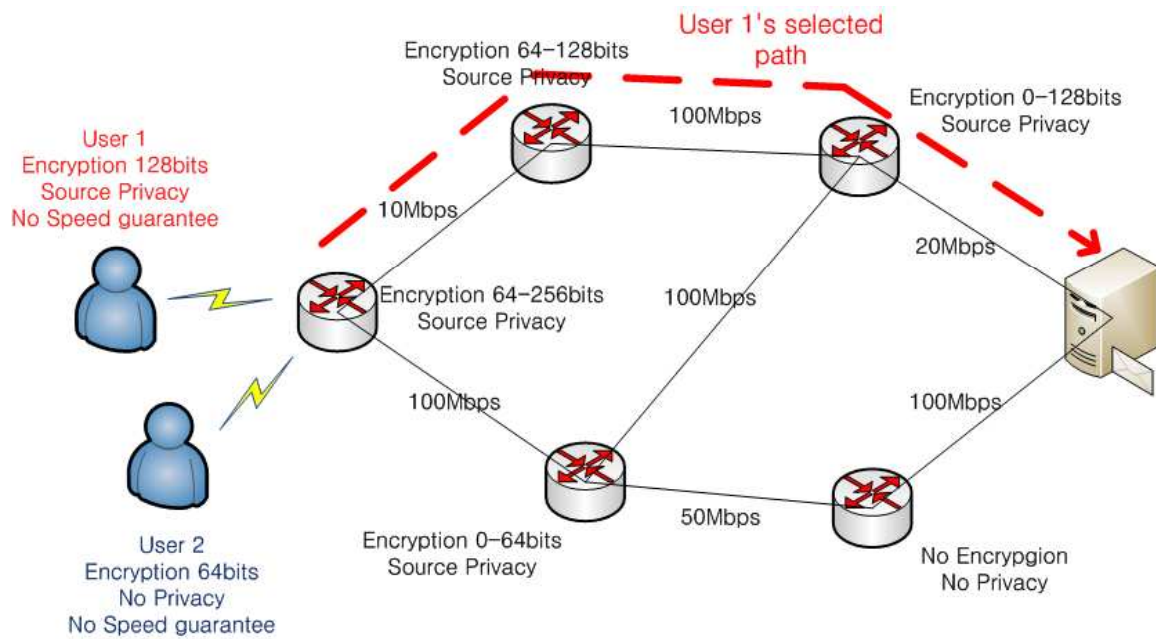
Routing Path setup



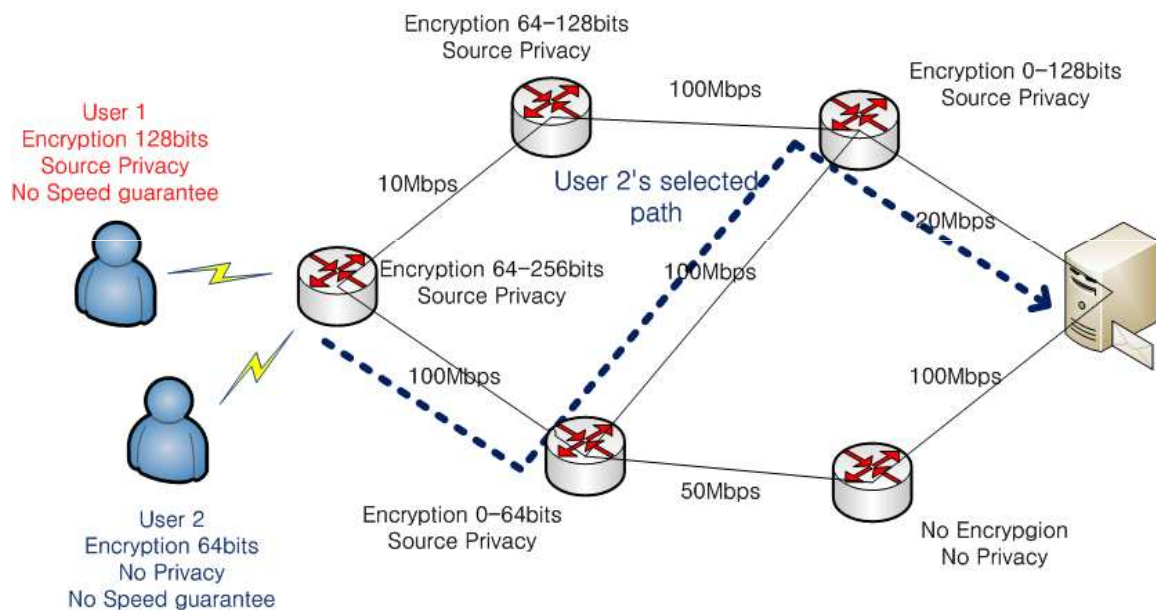
Routing Path setup



Routing Path setup



Routing Path setup





Conclusion

- Proposed Concept of Class of Security Level
 - Quantification of security features
 - Routing path setup

- Future work
 - Detailed algorithms
 - Quantification, Routing
 - Availability support method