

# Mobility and multihoming

## solutions in different layers and security discussion

Christian Dickmann  
mail@christian-dickmann.de

Institute of Informatics  
Georg-August University of Goettingen

Advanced Topics in Computer Networks (ATCN) Seminar  
1. July 2005

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ Internet users change from static workstation users to mobile users
- ▶ i.e. Mobile phone networks turn into IP based networks
- ▶ Devices have multiple internet access technologies
- ▶ Users might move while using the internet causing changes in access points to the internet and switching to different technologies (GRPS, UMTS, WLAN, etc.)
- ▶ Redudancy and loadsharing are additional applications for multiple internet interfaces
- ▶ Handover between access points and access technologies should be invisible to users

## Introduction

## Background

## Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

## Security

SCTP security  
discussion

## Conclusion

## Introduction

## Background

## Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

## Security

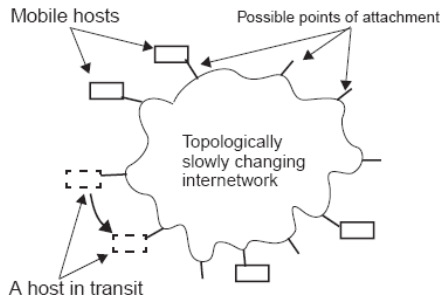
SCTP security  
discussion

## Conclusion

- ▶ Problem
- ▶ Background
  - ▶ What is Mobility?
  - ▶ What is Multihoming?
  - ▶ Abstract problem definition
- ▶ Solutions in different network layers
- ▶ Security considerations
- ▶ Conclusion
- ▶ Open discussion

- ▶ Mobile devices have to face two main scenarios:
  - ▶ Multiple access points to the internet at a time
  - ▶ Moving from one access point to another
- ▶ Many different layers to solve the problem:
  - ▶ Network layer (Internet Protocol)
  - ▶ Intermediate layer between network and transport layer (HIP layer)
  - ▶ Transport layer (UDP, TCP, SCTP, etc.)
  - ▶ Application layer
- ▶ New security threats due to mobility and multihoming
  - ▶ Hijacking attacks
  - ▶ Bombing attacks
  - ▶ Blocking attacks

# What is Mobility?



- ▶ Host changes its access point to the internet
- ▶ The same link layer technology is used for old and new access point
- ▶ The IP address of the host changes

Introduction

Background

Solutions

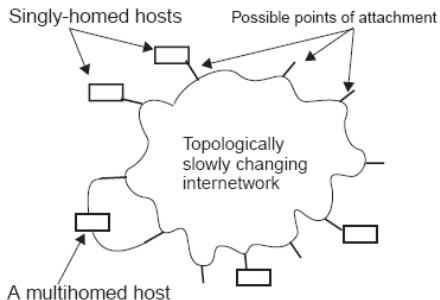
Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

# What is Multihoming?



- ▶ Host has multiple access points to the network at a time
- ▶ Usually different link layer technology is used (i.e. GPRS and WLAN)
- ▶ The host is associated with a set of IP addresses

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ Mobility and multihoming can be abstracted
  - ▶ Mobility means: Host has dynamic address
  - ▶ Multihoming means: Host has a set of addresses

## Solution

- ▶ Associate host with a dynamic set of IP addresses.
- ▶ Solves both, mobility and multihoming

# Which aspects make up a good solution?

- ▶ Users should not notice that there is a problem at all
- ▶ ⇒ Short delays
- ▶ Deployment:
  - ▶ Infrastructure changes should be small
  - ▶ Even important and accepted technologies like IPv6 take decades to deploy
- ▶ The solution should be easy but solving many scenarios
  - ▶ Small group of protocols and applications should be affected
  - ▶ Many applications should profit from the solution
- ▶ It should be possible to perform handovers on a per-connection basis
- ▶ Loadsharing would be an additional interesting feature

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ Problem can be solved in different layers
- ▶ Solutions covered in this talk:
  - ▶ Application layer: general discussion
  - ▶ Transport layer: SCTP
  - ▶ Network layer: Mobile IPv6
  - ▶ Intermediate layer between network and transport layer: HIP
- ▶ Security discussion:
  - ▶ A set of threats is common to all mobility/multihoming scenarios
  - ▶ Security discussion of SCTP

- ▶ Application layer: general discussion
- ▶ Transport layer: SCTP
- ▶ Network layer: Mobile IPv6
- ▶ Intermediate layer between network and transport layer: HIP

- ▶ Mobility support refers to automatically reconnect after a connection is lost
- ▶ Multihoming support means, that the application can choose the outgoing interface
- ▶ Already present in many current applications
- ▶ Very limited
  - ▶ Long delay, so normally user notices reconnect, often not very smooth
  - ▶ One open connection needs to use the same link all of the time, so no load-sharing
  - ▶ Every application has to implement it

Introduction

Background

Solutions

**Application layer**

Transport layer

Network layer

Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ Stream Control Transmission Protocol (RFC 2960)
- ▶ Features similar to TCP, but datagram oriented
- ▶ In TCP a connection is given by 4-tupel (Source-IP, Source-Port, Dest-IP, Dest-Port)
- ▶ SCTP associates a host with a set of IP addresses
- ▶ SCTP identifies a connection by (Source-IP-1, ..., Source-IP-N, Source-Port, Dest-IP-1, ..., Dest-IP-M, Dest-Port)
- ▶ Originally just to solve address failures
- ▶ Upcoming extension 'SCTP Dynamic Address Reconfiguration' (draft-ietf-tsvwg-addip-sctp-12)

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ Advantages of the solution:
  - ▶ Short delay
  - ▶ User does not notice a handover
  - ▶ No change to existing Internet infrastructure needed
  - ▶ Load-sharing can be done, cause SCTP accepts messages from all associated addresses
  - ▶ Deployment easy for new applications
  - ▶ Handover can be done per connection
- ▶ Disadvantages of the solution:
  - ▶ Old applications like HTTP or others depending on TCP/UDP do not profit

- ▶ Mobile IPv6 is specified in RFC 3775
- ▶ Three involved entities:
  - ▶ Mobile node (MN)
  - ▶ Correspondant node (CN): The communication partner
  - ▶ Home agent (HA): Forwarding agent with fixed address
- ▶ The HA is always informed by the MN about its current location
- ▶ The CN communicates with the MN which redirects the data to the HA
- ▶ The MN sends its traffic through the HA too
- ▶ There is a route optimiation to inform the CN about the real address of the MN to communicate directly

Introduction

Background

Solutions

Application layer

Transport layer

**Network layer**

Layer 3.5

Security

SCTP security

discussion

Conclusion

- ▶ Advantages of the solution:
  - ▶ User does not notice the handover
  - ▶ All applications profit from the solution
- ▶ Disadvantages of the solution:
  - ▶ All nodes need to support Mobile IPv6 (and IPv6 at all)
  - ▶ Handover can't be done for single connections
  - ▶ No real multihoming solution

# Interim result and what's now?

- ▶ No layer seems to fit all the needs
- ▶ Can multihoming even be solved in network layer at all?
  - ▶ In the network layer a messages needs a well defined topological destination
  - ▶ So multihoming can not be solved in this layer!
- ▶ But mobility and multihoming can't be solved in the transport layer in a way, where all applications make use of it
- ▶ The solution might be an intermediate layer between the network layer and the transport layer

Introduction

Background

Solutions

Application layer

Transport layer

Network layer

Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ In TCP/IP architecture IP addresses serve two purposes
  - ▶ Topological location needed for routing
  - ▶ Host identity
- ▶ Traditionally hosts did not move, so they had a fixed IP address
- ▶ This statement does not hold anymore!

## Solution

- ▶ Host Identity is assigned to every host
- ▶ Host Identity maps to a dynamic set of IP addresses
- ▶ This mapping can be seen as Layer 3.5

Introduction

Background

Solutions

Application layer

Transport layer

Network layer

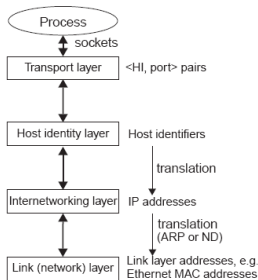
Layer 3.5

Security

SCTP security  
discussion

Conclusion

# Layer 3.5 - HIP



- ▶ New Host Identity layer
- ▶ Upper layers (TCP, etc.) operate with HI instead of IP addresses
- ▶ For outgoing messages one of the assigned IP addresses is chosen
- ▶ Incoming messages to/from different IP addresses can be collected for one transport layer connection

Introduction

Background

Solutions

Application layer

Transport layer

Network layer

**Layer 3.5**

Security

SCTP security

discussion

Conclusion

- ▶ Advantages of the solution:
  - ▶ User does not notice a handover
  - ▶ Handover can be done per connection
  - ▶ Load-sharing can be done
  - ▶ All applications and transport layer protocols profit
- ▶ Disadvantages of the solution:
  - ▶ Big infrastructure changes, makes deployment very difficult

## Note

Deployment can be improved by using

- ▶ Cryptographically Generated Addresses (CGA)
- ▶ Forwarding agents

Introduction

Background

Solutions

Application layer

Transport layer

Network layer

Layer 3.5

Security

SCTP security  
discussion

Conclusion

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

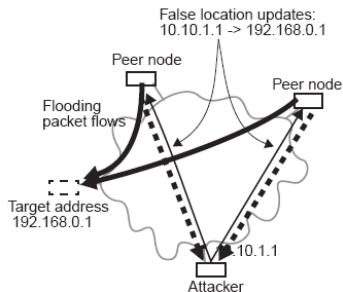
- ▶ We saw solutions in different layers
- ▶ No security considerations so far
- ▶ Next part of the talk:
  - ▶ Common threats to mobility and multihoming solutions
  - ▶ Security considerations for SCTP

## Main problems

- ▶ No validation in place to check if IP address is really owned by a host
- ▶ Address ownership even may change during a connection
  
- ▶ These main problems result in two general attack scenarios



# Common threats - Bombing attack



- ▶ Bombing attack
  - ▶ Attacker tries to bomb a server, resulting in a Denial-of-Service attack
  - ▶ The attacker connects to a large number of hosts
  - ▶ The attacker claims his new address is the one owned by the attacked server

# Common threats - General solution approach

- ▶ The main problem is to verify that a address is really owned by a mobile node
- ▶ Cryptographically generated addresses (RFC 3972) are a generic solution
- ▶ Originally proposed as CAM (Child-proof authentication mechanism) for Mobile IPv6 Binding Updates
- ▶ Every host has one or more Public-Key-Pairs.
- ▶ An IPv6 address consists of 64 bit network prefix and 64 bit host identifier.
- ▶ In CGAs the 64 bits are a hash of the public key

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

- ▶ How do CGAs help? A simple example:
- ▶ During connection setup Public-Keys are exchanged
- ▶ Later new address signaling message is signed with private key
- ▶ Receiver checks signed message and new address to verify the identity

## Note

- ▶ No Key-Exchange infrastructure needed!
- ▶ There are more (sophisticated) applications for CGAs!

Introduction

Background

Solutions

Application layer  
Transport layer  
Network layer  
Layer 3.5

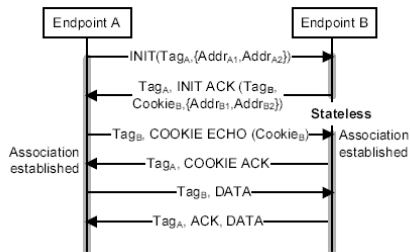
Security

SCTP security  
discussion

Conclusion

- ▶ Both presented attack scenarios are applicable for SCTP too
- ▶ The following security issues have already been addressed, but the lessons learned are important for future transport protocol design
- ▶ The following SCTP discussion will consist of two parts:
  - ▶ Background about SCTP
  - ▶ How this behaviour can be exploited for attacks

# SCTP background



- ▶ 4-way handshake
- ▶ No state in server until third message
- ▶ Verification tags to prevent spoofing ( $TAG_A$ ,  $TAG_B$ )
- ▶ Cookie to prevent DoS
- ▶ Cookie contains verification tags for rare situations

Introduction

Background

Solutions

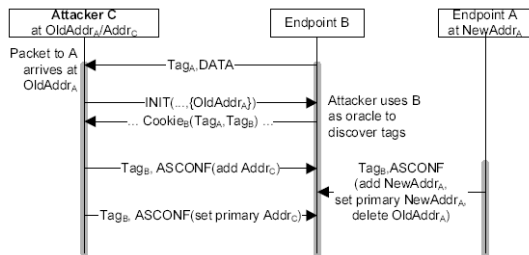
Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

# SCTP security - Association hijacking



- ▶ Endpoint A moves to new address *NewAddr<sub>A</sub>*
- ▶ Attacker C owns old addr. of A *OldAddr<sub>A</sub>* and *Addr<sub>C</sub>*
- ▶ B sends packet to *OldAddr<sub>A</sub>*, C uses INIT mechanism to learn verification tags
- ▶ C claims *Addr<sub>C</sub>* is new addr. of A before A informs about its true new address
- ▶ C sets *Addr<sub>C</sub>* as the main address

Introduction

Background

Solutions

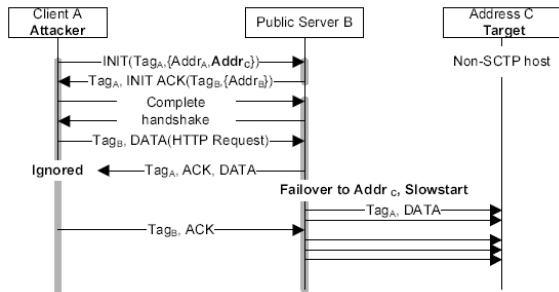
Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

# SCTP security - Bombing attack



- ▶ Attacker connects to Server B with two addresses (its own and the attack target)
- ▶ Attacker starts downloading large file
- ▶ Attacker ignores ACKs, failover to attack target
- ▶ Attacker sends ACKs to increase sending rate

Introduction

Background

Solutions

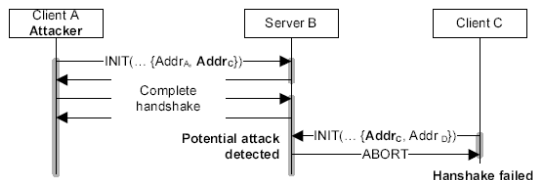
Application layer  
Transport layer  
Network layer  
Layer 3.5

Security

SCTP security  
discussion

Conclusion

# SCTP security - Address squatting (blocking)



- ▶ Attacker connects to Server B with two addresses (its own and the attack target)
- ▶ Attacker uses the Client-Port Client C will be using later
- ▶ Client C tries to connect to B
- ▶ A possible attack is detected and connect fails

- ▶ Problem
  - ▶ Host has dynamic address (Mobility)
  - ▶ Host has a set of addresses (Multihoming)
- ▶ Solutions
  - ▶ Solutions in every layer, but nothing fits really well
  - ▶ New layer 3.5 to solve the problem
- ▶ Security
  - ▶ New threats due to new freedom to move

Thanks for your attention!

- ▶ Open discussion