PISA -
P2P Internet Sharing Architecture
draft-heer-hip-midauth-00.txt

Tobias Heer
Distributed Systems Group
Chair of Computer Science IV
RWTH Aachen University
http://ds.cs.rwth-aachen.de
OECD Broadband Statistics (December 2006)

- In OECD countries:
  - 197.000.000 broadband subscribers
  - Finland, Denmark, Norway, Korea, etc.:
    - More than 26 broadband subscribers per 100 inhabitants

- Access technologies:
  - DSL: 62%
  - Cable modem: 29%
  - FTTH/FTTB: 7%
  - Other (Satellite, fixed wireless...): 2%
Ubiquitous Wired vs. Scarce Wireless Internet

- Publicly accessible Wi-Fi access points
  - Only in selected areas (airports, hotels, ...)
    - High density of users expected
  - At high prices
    - Mostly for busyness users

- Users start to share their Wi-Fi with others
Work Published So Far


- Tunneling as basic building block
- Utilize router at mobile user’s home
- Goal: increased security
One Problem: Security

- Web-based authentication
  - Easy to trick inexperienced users (MITM)

- Unencrypted public Wi-Fi
  - Eavesdropping

- No continuous authentication
  - Only initial authentication is "secure"
  - IP address is a very weak identifier
  - Impersonation

- Responsibility issue
  - Illegal actions relate to AP owner
  - Result of weak authentication

192.168.0.1
(authenticated as Bob)

80.21.12.1
requested illegal content

It wasn't me! It was Bob!

192.168.0.1

It wasn't me!
It was Bob!
Wi-Fi Sharing and HIP

- HIP is just one possible solution...  
  ... but matches the requirements nicely:

- Support for strong authentication
  - Public keys as host identities

- End-to-end security
  - No eavesdropping anymore
  - No MITM attacks

- Support for mobility
  - Transport layer is happy

- Authentication without passwords
  - Better support for key-less and screen-less devices
PISA – Mode 1:
Use User’s Home Router as Traffic Relay

- Users use their routers at home to relay traffic
  - Illegal actions point to the HR

- Cryptographic identities
  - Allow verifying the ID of the HR

- Community certificates
  - HR membership
  - Decentralized access control

- Encrypted tunnel
  - No eavesdropping from
    - Other users
    - AP owners (MITM)
  - HIP association
PISA – Mode 2: Direct Internet Access

- Mode 2 is used when...
  - HR is down
  - Larger bandwidth / low latency is required

- Home router issues digitally signed token
  - AR can verify relationship
  - HR can issue several tokens (reseller)
  - Mobile client can stay anonymous

- AR logs actions of mobile user
  - Cryptographic logging

- Illegal actions relate to AR
  - AR can prove that HR is responsible
HIP Authentication on Middleboxes

1.) Authentic Base EXchange:

2.) Replay:
draft-heer-hip-middle-auth

- **Scope (not restricted to PISA)**
  - MB that authenticate packets/hosts "on the fly"
  - No explicit registration
  - No explicit middlebox detection

- **Examples for middleboxes**
  - Firewalls
  - Rate-limiting MB
  - Accounting, logging

- **Support for authentication by MB during**
  - BEX
  - Mobility signaling
Authentication Mechanism

- Let MB „participate“ in BEX, UPDATE
- MB injects parameters to HIP control packets
- Challenge - response
  - Pretty much like ECHO_REQUEST / RESPONSE
- ECHO_REQUEST_M, ECHO_RESPONSE_M
  - Middlebox adds ER_M parameter to control packet
  - Receiving host echoes parameter in signed part of response packet
- DoS protection for middleboxes
  - Puzzle mechanism
New Parameters

- **ECHO_REQUEST_M**
  - Identical to ECHO_REQUEST
  - In unsigned part of packet (65332)
  - SHOULD be small (< 32 bytes)

- **ECHO_RESPONSE_M**
  - Identical to ECHO_RESPONSE_SIGNED
  - In signed part of packet (962)
New Parameters (cont’d)

- **PUZZLE_M**
  - Similar to PUZZLE
  - Larger opaque data field (6 bytes vs. 2 bytes)
  - In unsigned part of packet (65334)

- **SOLUTION_M**
  - Similar to SOLUTION
  - Larger opaque data field (6 bytes)
  - In signed part of packet (322)
Authentication: BEX

I1

R1 + EQ1_M

Add request

Verify response, add request

I2 + {ER1_M}

Verify response

R2 + {ER2_M}

I1

R1

I2 + {ER1_M} + EQ2_M

R2 + {ER2_M}
Authentication: UPDATE

M2

U1
U2 + {ER1_M} + EQ2_M
U3 + {ER2_M}
U4 + {ER3_M}

U1 + EQ1
U2 + {ER1_M}
I2 + {ER2_M}

M2

U2 + {ER1_M} + EQ2'_M
U3 + {ER2'_M}
U4 + {ER3_M}

Wrong!
OK!
OK!

OK!
I2 + {ER2'_M} + EQ3_M
U4 + {ER3_M}
Parameter Handling

- Middleboxes
  - MUST preserve order of parameters
  - MUST add further parameters after present ones
  - Helps host to determine location of MB

- End-hosts
  - MUST preserve order when copying to response
  - Sign packet
  - Helps MB to find parameter
Missing HOST_ID

- Problem: no HOST_ID in UPDATE packet
  - But: MB must figure out PKs
  - Request from URL
    - Slow (1 RTT)
    - Insecure (resource exhaustion, reflection, amplification)

- Solution: send HOST_ID in UPDATEs
  - Carrying ECHO_RESPONSE_M
  - Carrying SOLUTION_M

- BUT: larger packets
Middlebox Policies - Why so many MAYs and SHOULDs?

- Not part of the draft
- Intentionally kept open
- Possible outcomes of failed auth
  - No service
  - Degraded service
  - No better service
  - No difference

- We don’t want to tell people what to do with their middleboxes.
Open Issues

- Number of PUZZLE_M and ECHO_REQUEST_M per packet
  - Huge NAT / firewall cascades (requiring authentication each)
  - DoS Attack (Middlebox adds numerous parameters)

- Problem we should handle?
  - Is it likely to have deep cascades?
  - Wouldn’t it be easier to drop packets?
Open Issues (cont’d)

- Size of S’_M / E’_RESPONSE_M exceeds response packet size
  - Send two responses with parameters in reverse order.
  - First clears way for second one.
Conclusion

- **PISA offers**
  - Secure Internet connection sharing
  - Authentication by middleboxes
  - Support for roaming / mobility
  - Support for display- and key-less devices

- **draft-heer-hip-middle-auth**
  - Prevent replay attacks
  - Use BEX and UPDATE to authenticate communicating peers
  - Enables secure access control without explicit registration
  - Protection from DoS
  - Is this useful for the RG?