Advances in ad hoc networking: Packet Level Authentication

Dmitrij Lagutin, dlagutin@cc.hut.fi

T-79.5401 Special Course in Mobility Management: Ad hoc networks, 2.5.2007

Contents

- Introduction
- Packet Level Authentication
- Implementation of Packet Level Authentication
- Applications of Packet Level Authentication
- Conclusions

Introduction

- The Internet was designed to survive a nuclear war, but it was not designed to be secure against internal attacks
  - As a result, the Internet infrastructure is very vulnerable to different kinds of attacks
- Distributed denial of service attacks are easy to launch against nodes of Internet
- Packets that are moving through Internet can be easily forged, duplicated or delayed

Introduction

- These kind of attacks consume network's resources and they are dangerous especially in wireless and ad hoc networks since such networks have very limited resources
- Most current security solutions like IPSec concentrate on end-to-end security
  - They do not protect underlying Internet infrastructure, only the endpoints of the connection will notice if packets have been modified
  - They are useless if the Internet infrastructure is attacked and as result it is unable to deliver packets to destination

Packet Level Authentication

- A Packet Level Authentication (PLA) is a novel solution to protect IP networks against different kinds of attacks
- The aim of the PLA is to make it possible to verify authenticity of packets without having any kind of contact with the sender of the packet
- Analogy: Money, sales clerk can verify authenticity of the Euro note without having a contact with the bank that has issued the note. It is enough to check security measures in the note like watermark, hologram, metal string etc.

Packet Level Authentication

- Design goals of the PLA include
  - Validation of packets
    - Modification detection
    - Duplicate detection
    - Delay detection
  - Survivable in dynamic and hostile environment
  - Ability to add new nodes to the network and remove compromised nodes from the network
  - Scalability
  - Minimum traffic overhead
  - Minimum trust between nodes

Packet Level Authentication

- The idea of the PLA is that every node in the network, e.g. a router, can detect forged, duplicated and delayed packets immediately and discard them
- The PLA allows attacks to be stopped quickly, before they consume a large amount of network resources and before they inflict a significant damage
- The PLA utilizes public key cryptography and it introduces additional header on top of standard IPv6 header
  - Elliptic curve cryptography (ECC) is used because it has very compact keys. 160 bit ECC key that is used with the PLA is as strong as 1024 bit RSA key.

PLA: Header

- The PLA header includes:
  - The public key of the sender
  - A certificate where the Trusted Third Party (TTP) authorizes the sender. A TTP could be for example an operator. This guarantees that the sender is a trusted entity.
  - A time stamp to detect delayed packets
  - A monotonically increasing sequence number to make detection of duplicated packets possible
  - The cryptographic signature over the whole packet with sender's private key, this guarantees that forged packets will be easily detected because forgery breaks the signature

PLA: Trusted Third Parties

- The aim of the TTP is to authorize nodes that are sending PLA packets. If the node is hostile, TTP will not grant the node a new certificate, and without a proper certificate from TTP, node cannot communicate using the PLA
- The node that is checking packets must also to be able to check wherever the TTP that has authorized the sender can be trusted
  - If the packet has a correct signature, correct TTP certificate and the TTP can be trusted, then the packet is authentic and it has been sent by a legitimate node

Software implementation

- Experimental PLA implementation exists for Linux
  - The implementation consists of a Linux kernel module and userspace applications
  - Source code is available from: http://www.tcs.hut.fi/Software/PLA/new/Download.shtml
  - Handling cryptographic operations with general purpose CPU is quite slow. Round trip time through of PLA packets two PLA enabled routers (2GHz Athlon64 PCs) is about 60ms.
  - In the future, hardware acceleration can be used to increase performance of cryptographic operations

Hardware acceleration for cryptographic operations

- Field Programmable Gate Array (FPGA) chip can be used for increasing the performance of cryptographic operations like signing packets and verifications of signatures
- FPGAs produce very large performance improvement in specialized tasks compared to general purpose processors
- Various hardware implementations of elliptic curve cryptography have produced a good performance and energy efficiency

Hardware acceleration for cryptographic operations

- Preliminary results achieved in the PLA project with the FPGA accelerator are encouraging
- With Altera Stratix II FPGA chip it is possible to achieve about 165000 ECC verifications per second
  - With 150MHz clock speed and 19 computational blocks
- Assuming 5kbit payload per packet, this equals to 840Mbps of traffic
  - With maximum data payload (about 10kbit per packet) this equals to 1.68Gbps of traffic
  - Thus the scalability of the PLA is good as long as dedicated hardware acceleration is used to handle cryptographic operations

Applications of PLA

- The PLA has been designed for protecting IP network from attacks, however the PLA can also be utilized for other tasks
- The sequence number that is present in the PLA header can be used by operators for per packet billing
  - A monotonically increasing sequence number together with sender's signature provide a proof that the sender has sent the packet
  - A sequence number could be increased by the size of packet, this would allow billing based on the amount of data that the sender has sent

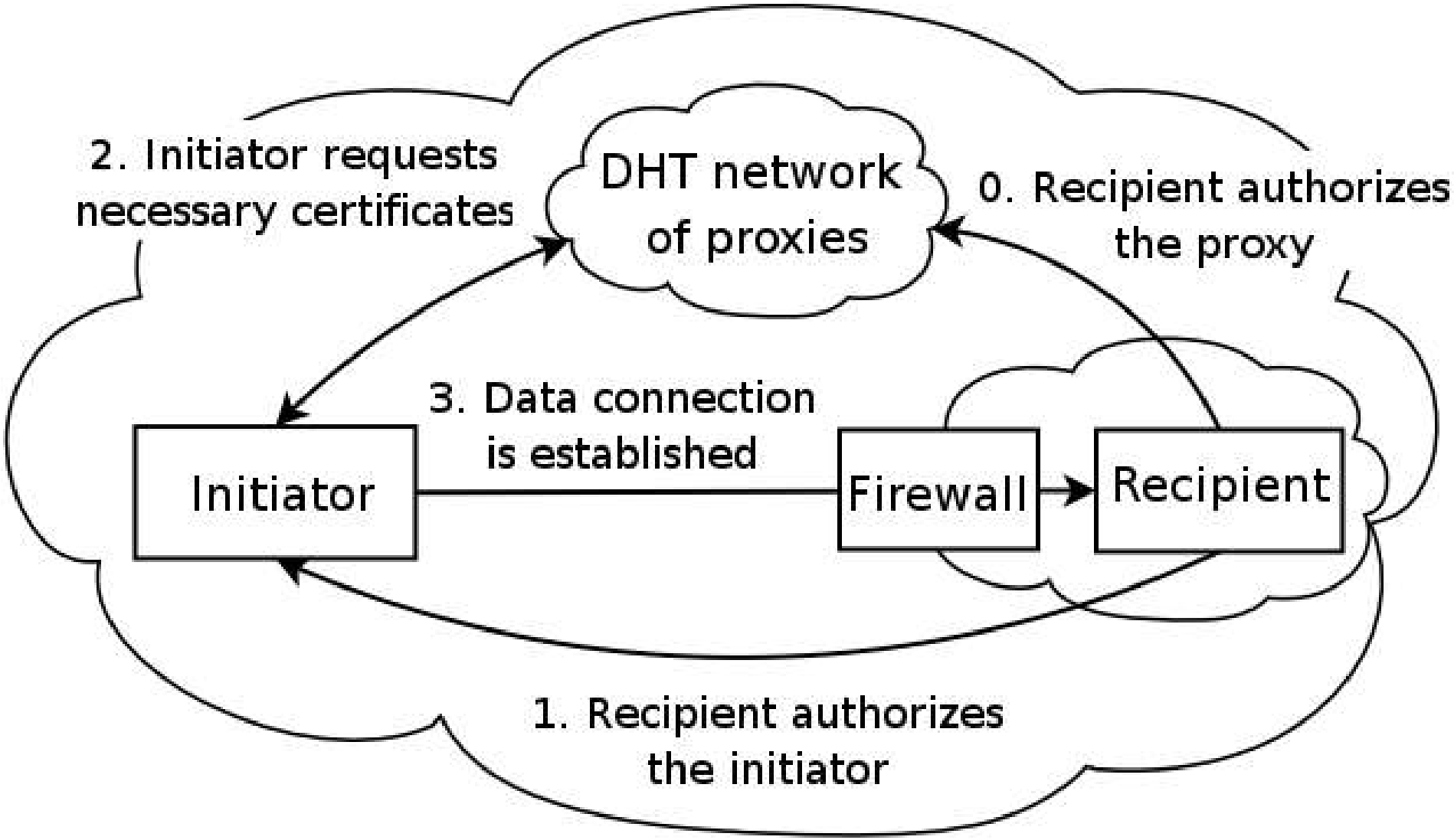
Applications of PLA: Controlling incoming connections

- Traditionally the initiator of the connection controls it, however this can cause problems
  - The recipient of the connection may use a mobile access network with a limited bandwidth and may even have to pay for all incoming traffic
  - The recipient is busy and does not want to receive unnecessary connections
- Limiting the incoming connections would also make much harder to initiate denial of service attacks against the recipient or the recipient's network

Applications of PLA: Controlling incoming connections

- New policy: All incoming connections are denied before they reach the recipient, only explicitly allowed connections will go through
- Implementation using certificates:
  - The recipient authorizes certain parties to create incoming connections to itself using certificates.
  - The firewall in recipient's network blocks unauthorized connections before they reach the recipient.
- The PLA is necessary to ensure that the data is really sent by a certified party

Controlling incoming connections: Example



Applications of PLA: Controlling incoming connections

- Proxy
  - The recipient trusts in proxy and the proxy can give certificates to other trusted parties for making incoming connections to the recipient
  - The proxy also keeps track of the recipient's IP address if the recipient is changing networks
  - In order to eliminate a single point of failure, proxies form a Distributed Hast Table (DHT) network

Applications of PLA: Controlling incoming connections

- Firewall
  - Is located in the recipient's access network
  - Takes notice of certificates that are passing through it
  - Blocks all connections to the network unless the recipient is a valid entity within the network and the incoming connection has been explicitly allowed via certificates. Public key in PLA header of the packet must match with the public key of the certificate that is given in step 1.

Applications of PLA: Ad hoc networks

- Ad hoc networks are severely limited by resources like energy and bandwidth
- Various attacks against ad hoc networks can consume significant amount of network's resources and thus make the network unusable or decrease the lifetime of the network
- PLA requires more processing power, however since PLA allows attacks to be stopped quickly, it can prolong lifetime of the network in situations where the network is frequently attacked

Conclusions

- Current Internet infrastructure has not been designed with security in mind
- The aim of the PLA is to allow for every node to detect forged, duplicated and delayed packets, thus possible attacks can be stopped quickly
- The PLA does not produce high computational overhead if a hardware acceleration is used for cryptographic calculations
  - Small key size of ECC limits bandwidth overhead
- The PLA can be utilized also for other tasks like billing of controlling incoming connections