Packet Level Authentication (PLA) Extensions for Host Identity Protocol (HIP)

Dmitrij Lagutin, Dmitrij.Lagutin@hiit.fi

Helsinki Institute for Information Technology HIIT

Aalto University School of Science and Technology

Contents

- Introduction
- Packet Level Authentication (PLA) architecture
- Implementation and Applications of PLA
- PLA and HIP
- Conclusions

Introduction

- Internet is currently very insecure
- Attacks (DDoS, SPAM, etc.) are easy to launch
  - Anyone can freely send data to any destination
- Attacks are difficult to stop and mitigate
  - Firewalls can only block the traffic near the destination
  - Practically impossible to distinguish valid traffic from unwanted one
- Culprits are rarely caught
  - No accountability

Introduction: main security problems

- To protect the network against various attacks both end-to-end and hop-by-hop security solutions are necessary
  - End-to-end solutions protect the communication end points. They are not effective if the underlying network infrastructure is attacked and is unable to deliver packets
  - Example: A server protected by firewall and HIP/IPSec will not able function if a denial-of-service attack chokes ISPs bandwidth
- After the network infrastructure has been protected, end-to-end solutions can secure end-points and services efficiently

Packet Level Authentication (PLA)

- PLA is a novel method for securing the network infrastructure and providing availability on the network layer
- PLA is based on assumption that public key cryptography can be used to digitally sign large dataflows
  - Using new public key cryptography algorithms which allow small key sizes compared to, e.g., RSA
  - Using dedicated ASICs to accelerate cryptographic operations up to a speed of millions of verifications per second

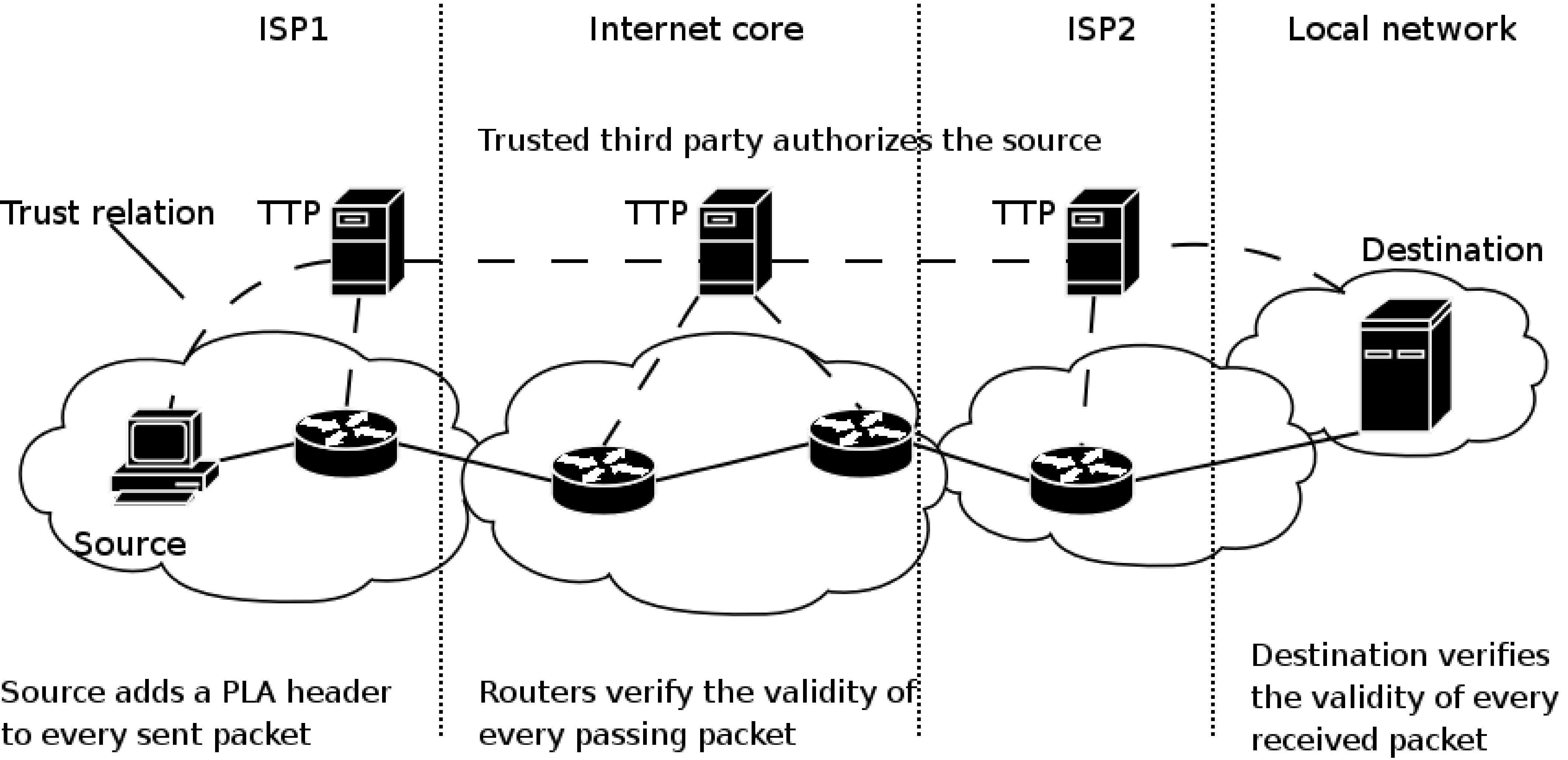
Packet Level Authentication

- Paper currency contains built-in security measures (watermark, hologram), there is no need to contact the bank to verify bill's authenticity
  - Similarly, PLA allows any node to verify authenticity of any packet without having any kind of trust association with the sender of the packet
  - Modified, delayed and duplicated packets can be detected and discarded quickly before they can cause damage or consume resources in the rest of the network
- PLA complements existing security solutions instead of replacing them. PLA can work together with other security solutions like HIP and IPSec

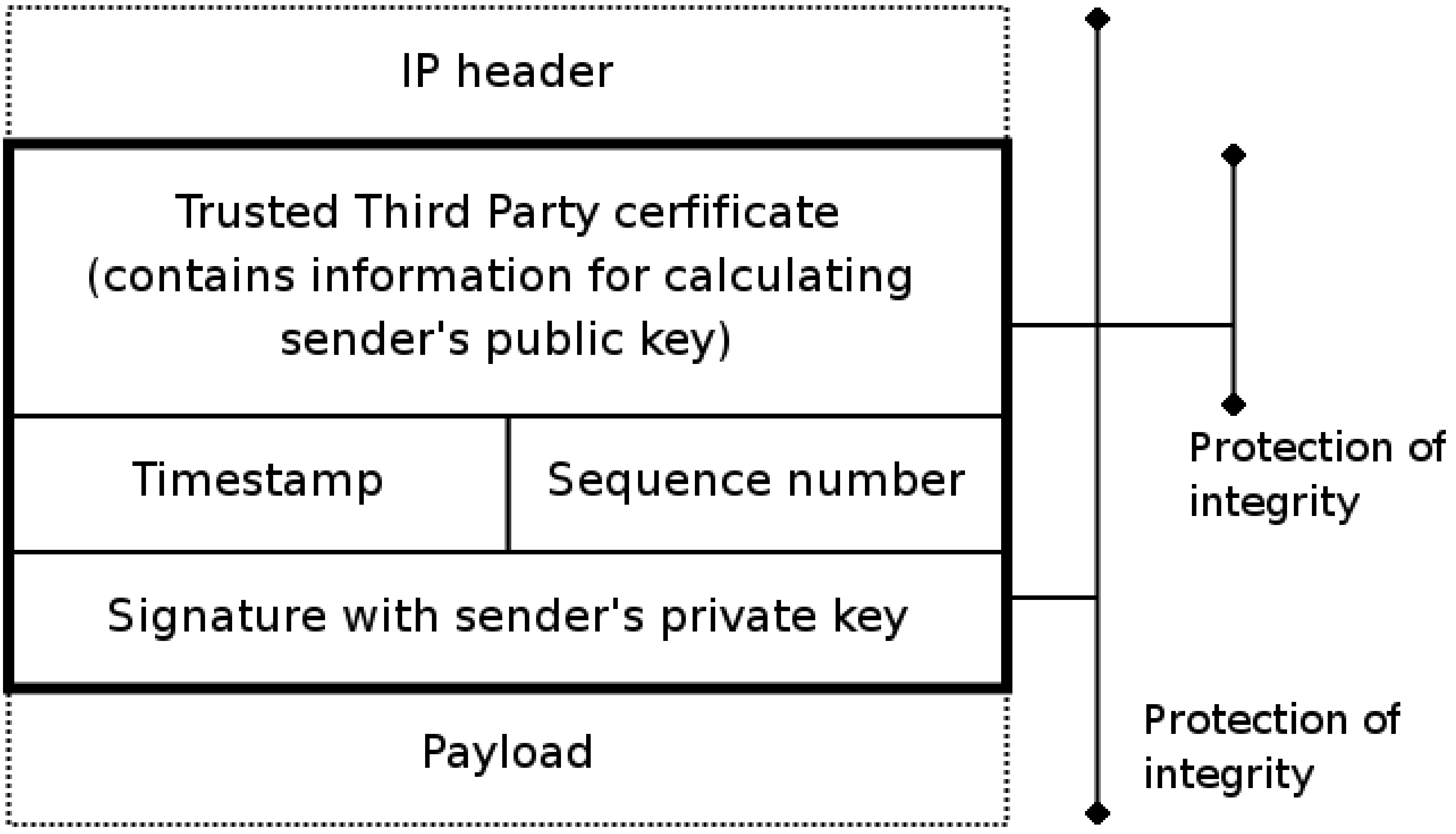
Packet Level Authentication

- PLA offers protection on two layers
- PLA header added to each packet protects the packet through a cryptographic signature => invalid or unwanted traffic can be detected and discarded at the next hop
- Trusted third parties (TTPs) offer a trust management mechanism, they are equivalent of traditional certificate authorities
  - Binds the user's cryptographic identity with a real one => accountability
  - Authorizes the user to use the network => malicious nodes can be removed from the network

Example PLA architecture



PLA Header



IP header
Trusted Third Party cerfificate
(contains information for calculating
sender's public key)
Timestamp
Sequence number
Signature with sender's private key
Payload
Protection of
integrity
Protection of
integrity

PLA Header

- Signature by sender's private key together with a sender's public key are used to check authenticity of the packet
- Trusted third party (TTP) certificate authorizes the sender
- Timestamp is used to detect delayed packets which may be a sign of a replay attack
- Monotonically increasing sequence number is used to detect duplicated packets

PLA implementation and cryptographic solutions

- PLA software implementation exists for Linux and FreeBSD
- Elliptic curve cryptography (ECC) is used due to its compact keys. A 163-bit ECC key that is used with PLA is as strong as a 1024-bit RSA key
  - The total size of the PLA header is about 1000 bits
- Simulations have shown that an unoptimized 90nm ASIC based on the FPGA could verify about 4Gbps of traffic
  - Performance can be further improved by using optimized ASICs manufactured on a modern manufacturing process, jumbo frames, or not verifying every packet at every node
  - Therefore, with a hardware acceleration PLA is scalable to 40Gbps and future 100Gbps interfaces

Applications of PLA

- Strong security mechanisms offered by PLA can also be utilized for other tasks, for example:
  - Using PLA, it is possible to built a system where incoming connections are blocked by default unless explicitly allowed
  - The sequence number that is present in the PLA header can be used for per packet or per bandwidth billing
  - TTP certificate mechanism can also be used for user authentication (i.e., wireless LAN authentication) and roaming

Deployment and other issues

- PLA uses standard IP header extension mechanisms, therefore it is compatible with standard IP networks, and can be deployed gradually
  - Packet verification at each node is not compulsory
  - Initially, PLA can be used to build a "control plane" to the Internet. TTP certificate mechanism can be used to distinguish various types of traffic
- Reasonable privacy can be maintained by using multiple cryptographic identities that act as a pseudonyms
  - Wrongdoers will be caught using the TTP mechanism, but in a normal situation users will be anonymous to the network

PLA and HIP

- PLA and HIP complement each other
  - PLA: hop-by-hop integrity protection, authorization
  - HIP: confidentiality, end-to-end security
- PLA does not need a key exchange, or complex signaling
  - First sent message already authenticates the sender
- Potential initial use cases:
  - HICCUPS-like VoIP scenario
  - User authentication during, e.g., handovers
  - DDoS protection in middleboxes
  - Mobile and ad-hoc networks with dynamic topology

PLA-HIP Header

- For simplicity, PLA's trusted third party (TTP) mechanism was omitted from the initial PLA-HIP proposal
- The PLA-HIP packet basically contains the host identity, signature, timestamp and a sequence number:

  IP (HIP (HOST_ID, PLA_HIP, HIP_SIGNATURE) PAYLOAD)

  – Where the PLA_HIP is a new parameter containing the timestamp and sequence number
  – Any cryptographic algorithm may be used for signatures. However, ECC is by far the most bandwidth-efficient solution.

PLA-HIP: Packet Processing

- To fully verify the packet, timestamp, sequence number, and signature must be checked.
  - It is not compulsory to always perform these checks, and the order of verifications may differ

```
   (In)          +----------------+          OK
 -------------> |Verify timestamp| -----------------------+
                +----------------+                         |
                        |                                  |
                        | Fail                             |
                        |                                  |
                        v                                  v
                  /-----------\      Fail      +----------------------+
                  |Drop packet| <------------ |Verify sequence number|
                  \-----------/                +----------------------+
                        ^                                  |
                        |                                  |  OK
                        | Fail                             |
                        |                                  |
          OK    +----------------+                         |
 <------------- |Verify signature|-------------------------+
   (Out)        +----------------+
```

Conclusions

- PLA is novel way to secure the network infrastructure, it gives to every node the ability to verify independently the authenticity of every packet
- PLA can also be used for other tasks, such as secure billing and authentication
- PLA is scalable for high speed networks and low power devices as long as dedicated hardware is used for accelerating cryptographic operations
- PLA with HIP fit well together, since their security properties complement each other

References

- General PLA architecture: http://www.tcs.hut.fi/Software/PLA/new/doc/Lagutin-Redesigning%20Internet-The%20Packet%20Level%20Authentication%20architecture.pdf
- Using PLA to control incoming connections http://www.springerlink.com/content/51h06845116j0167
- Energy efficiency of PLA in wireless networks: http://www.springerlink.com/content/y60115lmu6374157/
- Securing media independent handovers with PLA: http://doi.ieeecomputersociety.org/10.1109/WiMob.2009.50
- PLA for HIP draft: http://tools.ietf.org/html/draft-lagutin-hip-pla