Usage of Packet Level Authentication (PLA) –technique in securing communication of military-grade networks

prof. Hannu H. Kari, National Defence University, Finland

contact information: Hannu.Kari@mil.fi

While Internet has serious problems in stability and faces many cyber threats, the armed forces are still actively driving to use more and more commercial-of-the-shelf (COTS) –products and Internet technologies also in battlefields. Thus, we foresee that problems in Internet will eventually spread into the military systems as well. As for example, if the infrastructure is paralyzed by flooding or information shortage attacks, the modern end-to-end security solutions are useless.

In our research project, we have defined a SW and HW architecture as well as implemented its proof-of-concept prototype that shows how we can protect our IP based network infrastructures against the adversaries. Especially, we have been interested in providing means to filter away all garbage and process only good packets. The strength of our solution is based on solid, open cryptographic algorithms, not on secret implementations.

Our vision is that we need more protection at the network infrastructure level. Especially, every router shall be capable of detecting whether a received packet is an authentic -- good packet -- that should be forwarded further. To solve this problem, we have proposed a solution in which every IP packet is signed by the original sender using a cryptographically strong digital signature algorithm. The sender includes enough additional information into every packet so that other nodes can verify the integrity, timeliness and uniqueness of the packets without previous communication with the sender. In order to manage additional computational load per packet, we have also developed a HW-accelerator to demonstrate the scalability of the approach.

We believe that our Packet Level Authentication (PLA) –technique will be eventually implemented as an elementary part of every computing device attached in the future society where billions (or trillions) of computer devices are forming a global communication network. Hence, our work shall be used as a foundation for future standardization effort towards global, robust network systems. Our proposed technology is scalable from small scale computers, such as sensors or battery operated hand held device, to large scale core routers. Also, since its original design criteria consisted both military and civilian requirements, the same technological solution can be utilized both in commercial networks as well as in military battlefield.

The PLA technique utilized elliptic curve cryptography (ECC) that has benefits over the traditionally used public key crypto algorithms such as RSA. The key length of ECC public keys are significantly shorter as reasonably good protection is obtained with 233 bit keys, that corresponds the strength of 2048 bit RSA keys. Since the key length is short in ECC, it enables to add those public keys into every IP packet with reasonable overhead. Our proof-of-concept implementation demonstrated that the additional header of PLA is about 150 bytes that generates some 10% additional overhead on average IP packets on Internet –traffic.

Second benefit of the ECC cryptography is the possibility to implement very energy efficient hardware accelerators for calculating digital signatures in large numbers. Our proof-of-concept implementation demonstrated capability to calculate, in order of magnitude, tens of thousands of digital signatures per second. Since the implementation is easy to parallelize, it can be easily scaled up to millions of signatures per second with one single chip. This is enough of digitally verify – one-wire-speed – 10 gigabit per second

optical link traffic practically without any delays. Since the HW implementation is also very energy efficient, digital signature verification consumes far less energy that transmitting a packet wirelessly to next hop on the route. Thus, the PLA solution dramatically reducing power consumption of the wireless network that is infiltrated by adversaries who copy or manipulate legitimates packets that are secured with end to end solutions such as IPsec.

Since every packet has a legitimate owner and the integrity, timeliness and uniqueness of the packet can be verified not only by the final destination of the packet but every single node (router) in the network, the PLA protocol shall change dramatically also the other structures and operations of the network.

One example is given here: Firewalls. As the PLA header consists of both the identity of certifying authority (TTP) and the identity of the sender as well as digital signature over the packet by the original sender, the only thing that a firewall needs to be configured is which TTPs it shall trust. Once a packet arrives to the firewall, it extracts from the packet TTP's identity (its public key), that is used to verify that sender's identity (sender's public key) and is trustworthy at the moment (over validity period). Then, the firewall verifies the packet's integrity and timeliness with the public key of the send. All this can be done without prior knowledge of the sender or without storing anything for the future to be processed with next packets. Thus firewall can operate totally in memoryless mode. If we want to add protection against adversaries that send multiple copies of the same legitimate packet, that can be easily done by a simple state that remembers the last valid sequence number of that sender's PLA header and ignores those packet that have the same or smaller sequence numbers.

Beside of this firewall example, we have envisioned several other application level solutions that are possible both in military and civilian environments.

Keywords: Network infrastructure protection, Wireless communication, Digital signatures, Elliptic curve cryptography, Communication integrity