Next Generation Wireless IP Networking Applications

IPSec's growing importance in ensuring security and reliability in new networks

By Asaf Shen, Discretix Inc.

Internet Protocol Security (IPSec) provides security at the network layer of the protocol stack. By using IPSec, protection is offered to all IP packets regardless of the protocols and applications running in the upper layers of the protocol stack. IPSec provides a comprehensive security framework including access control, integrity (for connectionless traffic), authentication of data origin and more.

IPSec is used to secure communications over networks that are vulnerable to attacks (e.g. the Internet). It is also used to provide organizations with a mechanism to grant access to remote workers. The protocol has also been extended to cater for mobility, ensuring that the associated IP addresses can change while the user is on the move. This allows a VPN client to retain its connection to the gateway, even when the user is mobile.

Ubiquitous internet connectivity, combined with the wider deployment of wireless access networks, means that network-related technologies are no longer confined to traditional networking equipment (e.g. routers and switches). IP-based networks are penetrating new markets such as smart metering, automobiles, industrial controls, wearable computing and more. As the role of security and reliability in these networks is critical, IPSec's importance is growing rapidly.

IPSec is a mature protocol that is implemented in many of today's IP networks. The adoption of IP networking into new emerging markets will lead to the use of IPSec in addressing security requirements of new applications as well. This article will provide a brief overview of how smart networks and vehicular communications utilize IPSec. The article will also discuss the implication of new radio access networks on traditional IPSec implementation.

New wireless markets for IPSec

Smart Grids, Vehicular Communication and Wireless Devices
For many years public utilities delivered services in a reliable, low-cost manner. However, existing infrastructure must be upgraded to meet growing capacity demands and the latest requirements such as environmental safety.

Smart grids are defined as a means to "deliver electricity from suppliers to consumers using digital technology to control appliances at consumer's homes to save energy, reduce cost and increase reliability and transparency. Smart grids must address these requirements while working over different physical layers (wireless, wireline and powerline), supporting multiple applications (advanced

metering and distribution automation) and maintaining a high level of security. Given these requirements, it should not come as any surprise that smart grid equipment vendors are basing their networks on standard Internet Protocol (IP) technologies and are using IPSec for security.

An IP-based smart grid with security enables the use of application layer communication protocols such as Session Initiation Protocol (SIP). SIP is a natural choice for smart grid control because of its maturity, reliability and scalability all of which support the necessary network topology (i.e. amongst devices and between devices and operating centers/back offices). SIP is not at all dependent on the form of data exchanged by the communicating devices and can therefore allow the use of device-specific data exchange protocols. In addition, SIP is already complaint with many of the requirements emanating out of smart grid standards development organizations. SIP's utilization of the IPsec underlying security protocol allows features such as identification of devices, data confidentiality, integrity and prevention of network intrusion.

A lesser known requirement for smart grids is the support for Plug-in Electric Vehicles (PEV). These vehicles which at different times can be charging from the grid (the user is debited) or providing energy to it (the user is credited) require complex metering. This metering must also be mobile as the PEV can be connected to the grid in different locations.

Vehicular communications and in particular, the market for intelligent transportation systems (ITS) are another new market where IPSec is gaining traction. Together with other security protocols, IPSec is deployed for network level security. ITS can support commerce for toll roads, filling stations and parking facilities. ITS can also be used for fleet management, navigation services, in-vehicle internet connectivity, safety and more. In order to support all of these wireless applications, security must be in place. Security is needed to provide authentication, integrity verification and confidentiality of information within the ITS framework. Without security, altered functionality of ITS applications can cause disastrous consequences.

As far as mobile phones are concerned, IPSec is deployed for applications such as mobile VPN access. IPSec requires a significant amount of processing per packet. It has a fixed processing component which is independent of packet length and a varying component which is linearly related to the packet length and takes care of cryptography. Historically, the IPSec protocol was software implemented, with a tolerable load on the device processor due to relatively low throughput. However, the implementation methods of IPSec in mobile devices are shifting towards hardware-based implementations and are driven by several factors:

Hardware-based IPSec Acceleration

Acceleration of IPSec processing can be based on hardware cryptographic engines (with no notion of the IP packet) or a "lookaside" engine offloading more of the packet processing from the host in a power-efficient way. The processing is

offloaded from the host processor by using dedicated hardware. Any hardware implementation should be highly-configurable and capable of dealing with a variety of interfaces and cryptographic algorithms.

The host processor performs some pre-processing over the packet (inbound or outbound) and then directs the "lookaside" engine to process the packet. Low-latency packet streams must be handled in a dedicated queue with a higher priority. The offload engine obtains the relevant Security Association (SA) parameters per packet and configures the HW accordingly. The packet is then streamed in through the HW that takes care of header/trailer processing and the relevant cryptography (exact packet manipulation depends on direction, IPSec protocol, algorithms selection etc.). The resulting packet is then sent to the memory location determined by the host.

Conclusion

Ubiquitous connectivity is driving network-related technologies into new markets. As the role of security and reliability in these networks is critical, IPSec's importance is growing rapidly. Smart grids for example, which deliver electricity to consumers, use digital technology to control appliances and utilize resources more efficiently. These grids which connect over various physical layers are required to support multiple applications and maintain a high level of security. These requirements have lead smart grid equipment vendors to base their networks on standard IP technologies and use IPSec for security. Historically IPSec was implemented in software, however as the bandwidth requirement increases and IPSec is deployed on new classes of devices, the implementation methods is shifting towards hardware. Acceleration of IPSec processing can be based on hardware cryptographic engines or a "lookaside" engine offloading more of the packet processing from the host in a power-efficient way.

Asaf Shen is director of product marketing for Discretix Inc., www.discretix.com [1], 408-969-9991.

Source URL (retrieved on *12/19/2013 - 1:27am*):
http://www.wirelessdesignmag.com/articles/2010/02/next-generation-wireless-ip-networking-applications?qt-most_popular=0

Links:
[1] http://www.discretix.com