T-110.6220 Special course in network security
Exercise 3, 24-25 November 2008

1. Download the Proverif protocol analyzer. A model of the Denning-Sacco protocol is included in with the analyzer. Run the analyzer (*analyzer.exe*) on the model and try to fix the protocol, and model, by yourself. Compare your solution and model with the corrected version that is also included with the analyzer.

   Sources: http://www.proverif.ens.fr/

2. RFC 4301 assumes that the SPD is decorrelated, i.e., that no two rows (policies) have overlapping selectors. The assumption simplifies the standard specification because the order of rows in the SDP does not matter.
   (a) Decorrelate the SPD of an IPsec gateway below (3 first entries only, not the default DISCARD rule). Why do you think IPsec implementations don't actually decorrelate policies?

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.0/24	500	*	500	BYPASS	IKE
*	1.2.3.0/24	*	2.3.4.10	*	PROTECT: ESP tunnel to 2.3.4.1, authentication and encryption	Branch office server
*	1.2.3.0/24	*	2.3.4.0/24	*	PROTECT: ESP tunnel to 2.3.4.1, authentication only	Branch office subnet
*	*	*	*	*	DISCARD	Default

   (b) Note the "populate from packet" flag on some of the selectors in the policy below. The flag indicates that a separate SA should be created for each value of that selector. How do the flags change the effect of the policy?

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
*	1.2.3.101	*	2.3.4.0/24 populate from packet	*	PROTECT: ESP tunnel to 2.3.4.1, authentication and encryption	
*	1.2.3.101	*	1.2.3.0/24 populate from packet	*	PROTECT: ESP, transport mode, authentication only	
*	*	*	*	*	DISCARD	Default

   (c) Remember that the selector values used to create the SA are copied from the SPD into the SAD. Some IPsec implementations do this by setting a pointer from the SA to the SPD row that was used for creating it. What can go wrong in these implementations? (Hint: Consider both policy examples above for two different problems.)

   Sources: http://www.ietf.org/rfc/rfc4301.txt

3. IKEv2 is specified in RFC 4306. Find the answers to the following questions:

   (a) The IKE protocol is typically implemented in a users-space service (daemon). The IKE service creates one IKE SA with each peer host, which it stores itself. It also creates one or more child SAs, i.e. IPsec SAs, which are stores in the SAD in the OS kernel. What information is stored in the IKE SA? How does IKEv2 generate the shared encryption and authentication keys (keying material) needed by the child SAs?

   (c) IPsec is often used for a VPN connection from a client computer that is roaming in the Internet to a *remote access server*, which allows it to connect to an intranet. IPsec ESP is used in tunnel mode. The outer IP header contains the client address in the access network while the inner IP header contains the intranet addresses of the client and its peer in the intranet. Thus, some kind of mechanism is needed for assigning an intranet IP address to the client. How does IPv2 help with the address assignment?

   Sources: http://www.ietf.org/rfc/rfc4306.txt