IPsec and IKEv2 for the Contiki OS

Secure communication and the Internet of Things

Vilhelm Jutvik
Uppsala University

March 25, 2014

The case for IoT

The IoT will bring cheap and flexible communication to our everyday things

Problem statement

As the IoT will control and monitor sensors as well as machines in our surroundings, security is a natural concern. There is no consensus of how to deal with this issue.

Research question

IPsec and IKEv2 is one method of securing the Internet.

Question: Can IPsec and IKEv2 be implemented within the current hardware boundaries while still being interoperable with other Internet hosts?

Research question

IPsec and IKEv2 is one method of securing the Internet.
Question: Can IPsec and IKEv2 be implemented within the current hardware boundaries while still being interoperable with other Internet hosts?

Contiki

Contiki is an operating system designed for computers with severely constrained resources.

IPsec and IKEv2

Security in the IP (network) layer instead of in the application (like that of TLS).

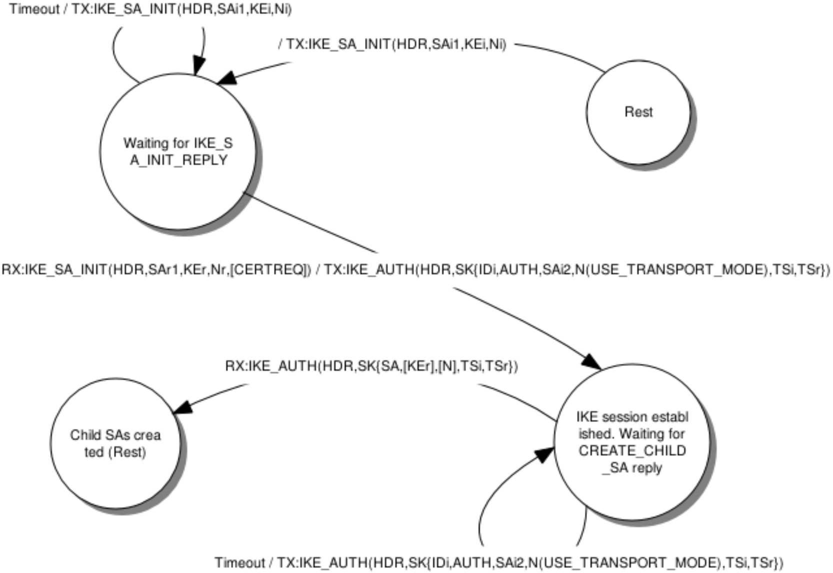
Implementation

Using the method of experimental computer science, I implemented IPsec and IKEv2 on Contiki and evaluated it.

Implementation: IPsec

IPsec was implemented as a part of Contiki's μIP stack.

Implementation: IKEv2



Timeout / TX:IKE_SA_INIT(HDR,SAi1,KEi,Ni)

/ TX:IKE_SA_INIT(HDR,SAi1,KEi,Ni)

Rest

Waiting for IKE_S A_INIT_REPLY

RX:IKE_SA_INIT(HDR,SAr1,KEr,Nr,[CERTREQ]) / TX:IKE_AUTH(HDR,SK{IDi,AUTH,SAi2,N(USE_TRANSPORT_MODE),TSi,TSr})

RX:IKE_AUTH(HDR,SK{SA,[KEr],[N],TSi,TSr})

Child SAs crea ted (Rest)

IKE session establ ished. Waiting for CREATE_CHILD _SA reply

Timeout / TX:IKE_AUTH(HDR,SK{IDi,AUTH,SAi2,N(USE_TRANSPORT_MODE),TSi,TSr})

Supporting libraries

Porting TinyECC to Contiki: ContikiECC

Evaluation

ROM, RAM, heap and stack consumption was measured.

Conclusion

IPsec and IKEv2 can be used in Contiki on current hardware, but future platforms will make it practical.