Three question regarding IPsec

Sjouke Mauw

ECSS group
Eindhoven University of Technology
The Netherlands

http://www.win.tue.nl/~ecss/

TU/e

IPsec

IPsec = security enhancement to IP.

Questions:

Q1: Should IP contain security provisions?

IPsec

IPsec = security enhancement to IP.

Questions:

Q1: Should IP contain security provisions?

Q2: Is IPsec a good security enhancement to IP?

IPsec

IPsec = security enhancement to IP.

Questions:

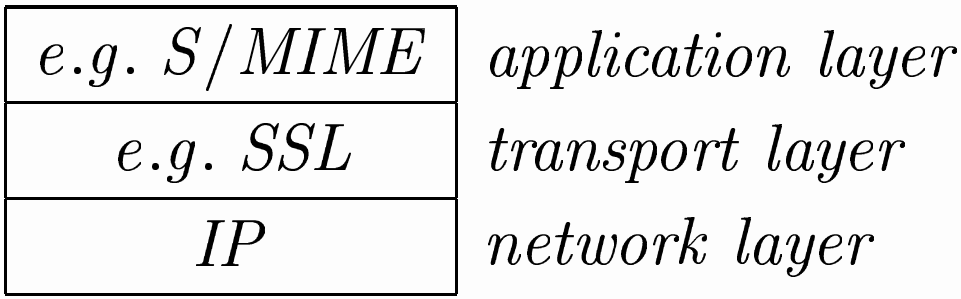
Q1: Should IP contain security provisions?

Q2: Is IPsec a good security enhancement to IP?

Q3: Can (and should) we formally verify IPsec?

Q1: Should IP contain security provisions?

IP is fundamental for all internet communications.



Where to put security provisions?

Low level	*high level*
general	*specific*
simple	*feature rich*
hidden to user/application	*application (and user) aware*

Where to put security provisions?

Low level	*high level*
general	*specific*
simple	*feature rich*
hidden to user/application	*application (and user) aware*

General opinion: security at every level.

A1: Yes, IP should consider security.

Q2: Is IPsec a good security enhancement to IP?

Seems to work, but

- IKE contains vulnerabilities.
- Many insecure implementations.

Quoting Bruce Schneier

"*IPsec was a great disappointment to us. Given the quality of the people that worked on it and the time that was spent on it, we expected a much better result.* "

Quoting Bruce Schneier

"*IPsec was a great disappointment to us. Given the quality of the people that worked on it and the time that was spent on it, we expected a much better result.* "

"*The development of IPsec seems to have been burdened by the committee process that it was forced to use, and it shows in the results. Our main criticism of IPsec is its complexity. IPsec contains too many options and too much flexibility; there are often several ways of doing the same or similar things.* "

Quoting Bruce Schneier

"*IPsec was a great disappointment to us. Given the quality of the people that worked on it and the time that was spent on it, we expected a much better result.* "

"*The development of IPsec seems to have been burdened by the committee process that it was forced to use, and it shows in the results. Our main criticism of IPsec is its complexity. IPsec contains too many options and too much flexibility; there are often several ways of doing the same or similar things.* "

A2: IPsec is not as good as required.

Q3: Can (and should) we formally verify IPsec?

- Formal methods are essential for security protocols.
- Application of formal methods in this domain matures.
- Research question: compositionality of security properties.

Q3: Can (and should) we formally verify IPsec?

- Formal methods are essential for security protocols.
- Application of formal methods in this domain matures.
- Research question: compositionality of security properties.

A3: Yes, we can and will have to apply formal methods to IPsec

Q3: Can (and should) we formally verify IPsec?

- Formal methods are essential for security protocols.
- Application of formal methods in this domain matures.
- Research question: compositionality of security properties.

A3: Yes, we can and will have to apply formal methods to IPsec , but. . .

- Why construct such an important protocol without providing formal proofs of correctness?
- Apply formal methods already in design phase; do not leave it as an exercise for the scientific community.