

T-110.5190 Seminar on Internetworking: Spring 2006: Mobile Communities

Janne Lindqvist

TKK/TML

Topics

- Authentication in wireless networks
- Internet Protocol Security Architecture

Authentication in wireless networks

- <http://prisms.cs.umass.edu/mcorner/papers.html>
Transient Authentication, Mark Corner's
- SOLA: A One-bit Identity Authentication Protocol for Access Control in IEEE 802.11
- What are these transient or lightweight schemes? What are their applicability?
- We have WPA and WPA2 and 802.11-something for authentication, too. So why do we need new ones?

Suitability?

- Familiarity with security principles such as authentication protocols.
- Wireless network knowledge is probably not required, but can be helpful.

Internet Protocol Security Architecture

- IPsec just got changed: a number of new RFCs that updates the architecture, ESP, AH, and IKEv2 have been published.
- What actually changed and what's the relevance of the changes?
- How about operating system and software support?
- Mobility.

References

- <http://www.rfc-editor.org/cgi-bin/rfcsearch.pl> type IPsec.
- RFC 4301-4306.

Suitability?

- Familiarity with the “old” IPsec is useful.
- The new IPsec most likely does not have any helpful second source references available.