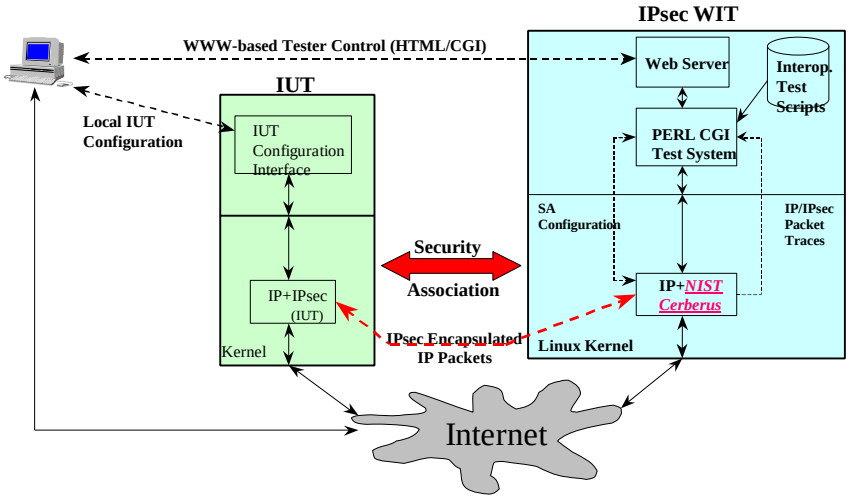
Internet Security Protocols



Goal

To expedite the research, development, standardization and commercialization of next generation Internet security and IPv6 technology. To deliver rapid prototypes and testing technology that makes a demonstrable impact in the IPsec research and development community.

Technical Objectives

- Expedite the development and improve quality of IETF IPsec standards
- Develop leading edge prototypes of emerging IETF IPsec specifications.
- Design and develop automated testing technology that will expedite the commercial availability of IPsec products.
- Research protocols and techniques for security policy management and advanced testing and verification techniques.

Expected Impact

- Deliver testing technology that makes a demonstrable impact on the Internet security research and development community.

Potential Customers and Collaborators

Customers

- IETF IPsec working groups
- Our test tools and prototypes are being used by 100s of organizations in the Internet research and development community.
- ANX security working group.

Collaborators

- NSA
- INRIA, Korea Telecom
- Cisco, Bay Networks, IBM T.J. Watson, BBN Technologies, NSA, Sable Systems

Recent Products

- *Cerberus/PlutoPlus* - reference prototype of IETF IPsec and IKE protocols (FY98)
- *IPsec-WIT* - on line, WWW based interoperability test system for IPsec / IKE. (FY98)

Planned Accomplishments (FY99-00)

- Expand test systems to address PKIX certificate protocols (FY99)
- Analyze the applicability of IPsec to IPv6 (FY99)
- Prototype and analyze security policy management protocols (FY00)
- Develop formal modeling techniques to assess the security properties and generate test suites for IPsec / IKE / PKIX (FY00)
- Analyze the scalability of IPsec / IKE / PKIX in large scale VPN environments (FY00)