Agentúra Ministerstva školstva, vedy, výskumu a športu SR pre štrukturálne fondy EÚ

Operačný program VZDELÁVANIE

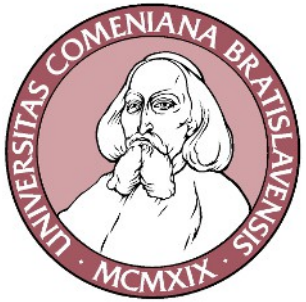
Európska únia
Európsky sociálny fond

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

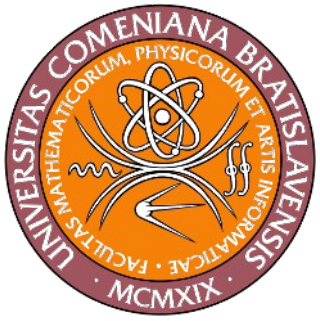
Príprava štúdia matematiky a informatiky na FMFI UK v anglickom jazyku

ITMS: 26140230008

dopytovo – orientovaný projekt



Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je spolufinancovaný zo zdrojov EÚ



Security of IT infrastructure

Virtual Private Networks (VPN)

RNDr. Jaroslav Janáček, PhD.

Motivation

- physical private networks
  - means of physical security can be used to protect transmitted data against external attackers
  - can be easily used only for small range networks in protected environment
  - difficult for long range networks
    - e.g. interconnection of remote branches
  - inflexible
    - needs physical secure communication lines

Motivation

- Is not it sufficient to deal with security on higher network layers (transport, application)?
  - it is not always possible – it requires cooperation with the applications
  - it is often good security practise to have multiple protection layers
    - software contains bugs that can be often exploited
    - the probability of simultaneous occurrence of two phenomena is often much lower that the probabilities of occurrence of the individual phenomena

The Role of VPN

- creation of secure communication channel
  - protection of confidentiality and integrity of the transmitted data and authentication of the endpoints
- on network or link layer
- transparent for higher layers
  - without the need of cooperation with the applications

Implementation of VPN

- cryptographic means
  - encryption
  - HMAC
  - authentication
  - key management
    - PKI
    - static pre-shared secret

VPN Scenarios

- secure interconnection of several private physical networks across a public network
  - e.g. interconnection of several physically dislocated branches
- secure connection of a remote computer across a public network to a protected network
  - e.g. connection of a home computer, or of a notebook in some remote location to a protected network (e.g. to the office)

Negative Aspects of VPN

- VPN creates a “hole” to the protected network
  - the remote computer connected via a VPN is usually treated in the same way as a computer connected directly to the protected network,
  - but it also has (or can have) other connections to the outside world that are not under control of the protected network's administrator.
- Usage of VPN has to be controlled using means of organizational security.

Specific solutions

- IPsec
  - optional part of IPv6 and IPv4
  - protocols AH, ESP, ISAKMP/IKE, IKEv2
  - different implementations on many platforms
    - not always fully compatible
- OpenVPN
  - open-source product
  - key management based on SSL/TLS
  - Linux, Windows, Mac OS X, Solaris, ...BSD, ...

IPsec

- cryptographic protection of confidentiality and/or integrity and authentication of endpoints on the network layer
- operations are driven by a policy (SPD = Security Policy Database)
  - accept the packet without modification
  - drop the packet
  - apply an IPsec transformation to the packet

Security Policy Database (SPD)

- the record for the packet being processed is looked up in SPD according to
  - the source and destination IP address
  - the transport layer protocol and port numbers
- the record specifies the transformation
  - IPsec mode
  - IPsec protocol
  - tunnel endpoint IP addresses (in tunnel mode)

Security Association (SA)

- SA describes security parameters of a unidirectional communication channel providing specific security services to protect the transmitted data
  - SPI (Security Parameters Index)
    - identifies SA at the recipient
  - mode
  - protocol
  - cryptographic algorithms
  - cryptographic keys

Transport vs. tunnel mode

- transport mode
  - IPsec header (AH, ESP) is inserted between the IP header and the transport layer header
  - provides for security between the endpoint computers
- tunnel mode
  - the original IP packet is wrapped into a new packet
  - new IP header and IPsec header are added
  - the new IP packet can have different source and destination addresses – the endpoints of the tunnel
  - typically used for VPN between networks

AH Protocol (51)

- integrity protection
  - of fixed fields of the IP header preceding the AH header
  - of transport layer (and higher) data
    - of the entire original IP packet in the tunnel mode
- protection against replay-attack
  - 32 (or 64) bit sequence number
- AH fields
  - next header, payload length, SPI, seq #, ICV

ESP Protocol (50)

- protection of confidentiality and/or integrity
  - of transport layer (and higher) data
    - of the entire original IP packet in the tunnel mode
- protection against replay-attack
- ESP fields
  - SPI, seq #
  - data, padding, padding length, next header
  - ICV

AH vs. ESP

- both can provide integrity protection
  - AH covers fixed fields of the IP header
  - ESP does not cover the IP header
- interaction with NAT
  - AH cannot be used if there is a NAT in the network path
  - ESP can be **partially** used
    - it may be difficult to distinguish individual ESP flows
    - solution – encapsulation to UDP datagrams

SA and key management

- manually
- ISAKMP/IKE
  - ISAKMP – SA management protocol and a framework for key management
  - IKE – key management protocol
  - 2 phases
    - 1st phase – establishment of ISAKMP SA – bidirectional secure communication channel
    - 2nd phase – creation of pairs of SA for AH/ESP
  - authentication using PKI or a pre-shared secret

SA and key management

- IKEv2
  - an attempt to improve ISAKMP/IKE
  - functionally similar (2 phases as well)
  - incompatible
  - authentication
    - PKI
    - pre-shared secret
    - EAP

IPsec support

- ISAKMP/IKE
  - Windows 2000/XP/Vista
  - Windows Server 2008/2008
  - Linux, OpenBSD, ...
- IKEv2
  - Windows 7
  - Windows Server 2008 R2
  - Linux, OpenBSD, ...

OpenVPN

- protection of confidentiality and integrity and authentication of endpoints
- protection against replay-attack
- UDP or TCP
  - no problems with passing through NAT (in TCP mode it even supports passing through CONNECT capable web proxy)
- IP or L2 (link layer) tunnel
  - tun/tap network interface

OpenVPN – key management

- static (pre-shared) keys
- SSL/TLS
  - server authentication
    - using PKI
  - client authentication
    - using PKI
    - name + password

IPsec vs. OpenVPN

- IPsec
  - transport mode
  - was mandatory in IPv6 (later proposed to become optional)
  - supported by many OS
- OpenVPN
  - simpler key management protocols
  - no problems with passing through NAT and firewalls
  - tunnel presented as a virtual network interface
  - common implementation – 100% compatibility across platforms
  - also supports L2 tunnels