VPNs

CSH6 Chapter 32

"Virtual Private Networks & Secure Remote Access"

Justin Opatrny & Carl Ness

1

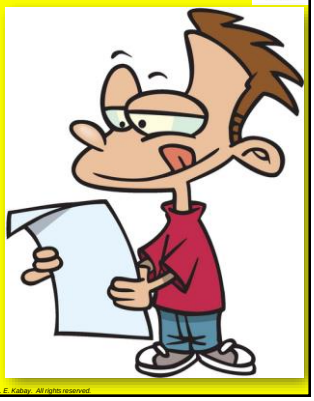
Topics

- Introduction
- Remote-Access VPNs
- Site-to-Site VPNs
- Extranets

OH NO!

49 SLIDES!!!

(MUST TALK LIKE SOMEONE ON LOTS OF COFFEE)



2

Introduction

- Borders Dissolving
- Secure Remote Access
- Virtual Private Networks
- VPN Technology Concepts

3

Borders Dissolving (1)

- Before Internet access, security → internal networks
- After ~1993, explosion in Internet connections
- Perimeter firewall reduced access by digital predators
- How to maintain network security for employees using mobile technology?
  - Laptop computers, cell phones
  - Home, traveling
- How to define extranets for business partners?

Borders Dissolving (2)

- Competitive advantage requires
  - Employee network & information access
  - From outside workplace
  - Coping with inclement weather, disruptions
  - Geographic dispersion of workforce
- B2B requirements growing
  - Vendors, suppliers, partners
  - Outsourcing
  - Support
- B2C demands
  - Growing expectations from consumers

Secure Remote Access

- Require extensive planning & review
  - Must not jeopardize safety of critical information & information systems
- Primary tools
  - Virtual Private Networks (VPNs)
    - ✓Secured connection
    - ✓Encrypted tunnel
  - Extranets
    - ✓Encrypted connection to Web application server outside internal NW
    - ✓Usually need connections from server to internal NW for data exchange

6

Virtual Private Networks

- Basic idea
  - Create stream of encrypted data through firewall
  - "Encrypted tunnel"
- Goals
  - Securely extend internal network
  - Protect data during transmission
  - Maintain security of system
- Two categories
  - Remote-Access VPNs
  - Site-to-Site VPNs

7

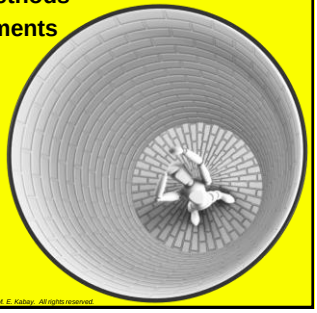
VPN Technology Concepts

- See other chapters in *CSH6* for background concepts, terminology, details & readings
  - Chapter 5: Data Communications & Information Security
  - Chapter 6: Network Topologies, Protocols & Design
  - Chapter 7: Encryption
  - Chapter 26: Gateway Security Devices
  - Chapter 37: PKI & Certificate Authorities

8

Remote-Access VPNs

- IPSec
- Transport-Layer Security
- User-Authentication Methods
- Infrastructure Requirements
- Network-Access Requirements



9

IPSec

- Basics
  - Suite of Internet Protocol (IP) layer protocols
  - Establish & protect VPN transmissions
  - Usually uses client-resident application
  - Create encrypted VPN tunnel into internal network
- Topics
  - Key Exchange & Management
  - Authentication Header vs Encapsulating Security Payload
  - Transport vs Tunnel Mode

IPSec: Key Exchange & Management

- Must establish and manage *Security Association* (SA) between client & server
- IPSec uses Internet Key Exchange (IKE)
  - Good reference: NIST *Guide to IPSEC VPNs* (SP 800-77)
- 2 phases in establishing SA
  - Phase 1 creates initial IKE SA
    - ✓Can use 2 modes:
      - Main mode
      - Aggressive mode
  - Phase 2 establishes IPSec SA

More details on following slides

11

IKE Phase 1 Main Mode

- Most commonly used
- 3 *pairs* of packets
  - 1st pair negotiates 4-parameter protection suite
    - ✓Encryption algorithm (e.g., 3DES, AES)
    - ✓Integrity protection algorithm (e.g., HMAC-SHA-1)
    - ✓Authentication method (e.g., shared key, PKI certificate)
    - ✓Diffie-Hellman group* (category of keylength & type of encryption algorithm)
  - 2nd pair exchanges encryption keys using D-H
  - 3rd pair authentications each side of connection to other

*See SP800-77 pp 3-11 & 3-12

HMAC: hashed message authentication code

IKE Phase 1 Aggressive Mode

- 3 *packets* (not pairs of packets)
  - 1st & 2nd packets
    - ✓Negotiate all IKE SA parameters
    - ✓Perform key exchange
  - 2nd & 3rd packets
    - ✓Authenticate end-points to each other

13

IKE Phase 2

- *Quick mode* to establish IPSec SAs
- Each side maintains IPSec SA in SAD (Security Association Database)
- Initiating device creates & sends SA proposal to VPN server
- VPN server replies with SA selection & hash to authenticate connection
- Initiating device replies with hash generated from prompt received from server
- If server matches received hash with sent hash, server adds SA to SAD & connection proceeds

14

IPSec: AH vs ESP

- Authentication Header (AH)
  - Protects integrity of packet header & payload
  - Uses cryptographic hashing
- Encapsulating Security Payload (ESP)
  - More common implementation today
  - Encrypt entire packet
  - Create new IP header
  - Protects both integrity & confidentiality

15

IPSec: Transport vs Tunnel Mode

- Transport mode
  - Preserves original IP header
  - Provides confidentiality & integrity protection for payload
  - Incompatible with Network Address Translation (NAT)
    - ✓TCP integrity checks fail
    - ✓NAT alters IP address during transmission – therefore IPSec hash will be incorrect
- Tunnel mode
  - Protects both header and payload
  - Primary method today for host-to-gateway & gateway-to-gateway VPNs

16

Transport-Layer Security (TLS)

- TLS provides protection of client/server links
- Most common implementation: SSL (Secure Sockets Layer) → HTTPS
- Basics
  - 128-bit encryption
  - Widely available on browsers & servers
  - Client* provides SSL-related parameters for establishing HTTPS connection to server
  - Server responds with its SSL parameters + digital certificate
  - Client authenticates server

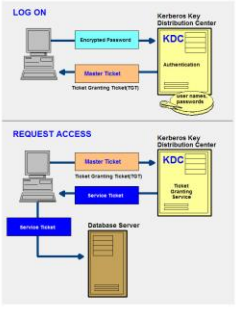
17

User-Authentication Methods

- Simplest method: user name & password
- Other methods
  - RADIUS: Remote Authentication Dial-In User Service
  - LDAP: Lightweight Directory Access Protocol
  - Kerberos: access control system
    - ✓Developed at MIT in 1980s
    - ✓Accepted by IETF in 2003
    - ✓See http://www.ietf.org/rfc/rfc1510.txt
    - ✓Diagram from CDE on next slide

18

Reprinted from Computer Desktop Encyclopedia
Copyright (c) 1981-2009 The Computer Language Company Inc.
Ver. 22.4, 4th Quarter 2009



It's About Tickets

After users are authenticated, they are granted a master ticket that is used to obtain service tickets. Service tickets act like session keys in other security systems.

Kerberos

- Login: user PW encrypted & sent to KDC
- KDC
  - Authenticates PW
  - Sends *master ticket* (a kind of session key) to user
- User sends master ticket to KDC when requesting service

Infrastructure Requirements

- VPN should be outside firewall
- Connection to internal networks protected by firewall
  - Restrict all external connections to internal network
  - Allow encrypted connections to VPN server to be relayed through firewall

Network-Access Requirements

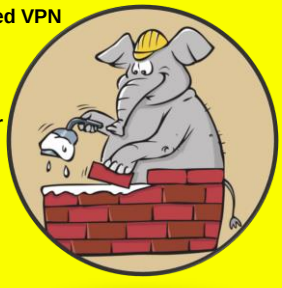
- IPSec
  - Can use *split tunneling* for better throughput
  - Enforce encryption on inbound traffic
  - Allow outbound traffic to Internet to be treated normally (not through encrypted tunnel)
  - But lose ability to inspect outbound traffic
- TLS/SSL
  - Dashboard allows administrator to control settings
  - Current implementations similar to IPSec flexibility

Site-to-Site VPNs

- VPNs mostly used for client remote access
- But also used for secure internal communications
  - Can create equivalent of secure WAN (Wide Area Network)
  - Reduce complexity of physically-wired WAN
- Topics in next slides relating to Trusted VPNs
  - MPLS
  - Site-to-Site VPNs
  - Information Assurance Considerations

MPLS: Multiprotocol Layer Switching (1)

- Not traditional encrypted VPN
- Similar service
- Complex issues in deployment
- Service providers differ in offerings
- Topics on next slides:
  - Purpose
  - Requirements



23

MPLS (2): Purpose

- Typical WAN topologies = star, ring or mesh (or combinations)
- MPLS creates
  - Meshed
  - Routed
  - Virtual network at
  - Service provider level
- MPLS free to route packets from 1 WAN endpoint to another in virtual network
- Eliminates hub as single point of failure
- Can provide multiple QoS (quality of service) levels
  - Prioritize traffic
  - Allow specific protocols more bandwidth at times

Site-to-Site (S2S) VPNs

- Purpose
  - Extend WAN concepts to areas where traditional direct connections (T1, frame relay…) are too expensive
  - Leased lines be too slow
- Alternative WAN
  - Use / share Internet connection
  - Higher bandwidth, lower cost
- Backup
  - Redundancy at relatively low cost
- Requirements
  - Internet, VPN end-points (routers)
  - Possibly VPN-enabled gateway security device (firewall)

25

IA Considerations

- Remote-access VPN Considerations
- Fidelity of Mobile Device
- VPN Client Management
- Protection of VPN Device
- Cryptographic Options
- Traffic Inspection
- Processing Power
- Interception
- Site-to-Site VPN Considerations
- Implications of Elusive VPNs
- Impact of IPv6

26

IA Considerations

- Remote-access VPN Considerations
  - By nature of VPN, assuming hostile environment for data transmission
- Fidelity of Mobile Device
  - Essential to protect laptops, phones…
  - Firewall, antivirus, patches, encryption
  - Status may change during connection
  - Network Access Control (NAC)
    - ✓Interrogate connecting device at login
    - ✓Verify security status
    - ✓Complex management issue

27

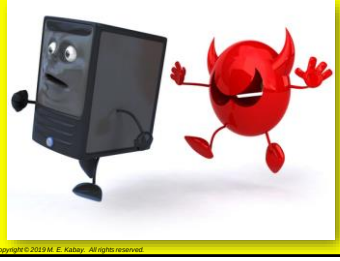
VPN Client Management

- IPSec requires client-side app or embedded OS
- Need to maintain up-to-date configuration
- Avoid user involvement
  - Push updates rather than pulling
- TLS/SSL VPN less complex to administer
  - Automatic downloads of small Java applets or ActiveX controls
  - Code can remain resident – avoid delay at re-initiation of sessions

28

Protection of VPN Device

- Configure firewall to stop access to all unused ports
- Remove unacceptable cryptographic modes
- Limit access to network management protocols such as ICMP & SNMP using ACLs
- Don't allow insecure protocols such as FTP or HTTP for administration
- Use strong I&A (e.g., token-based, two-factor)



29

Cryptographic Options

- Selection of cryptographic protocol
  - During IKE negotiation
- Cipher suite determines what is available
  - Remove unacceptably weak protocols from cipher suite
  - Prevents incompatible clients from connecting

30

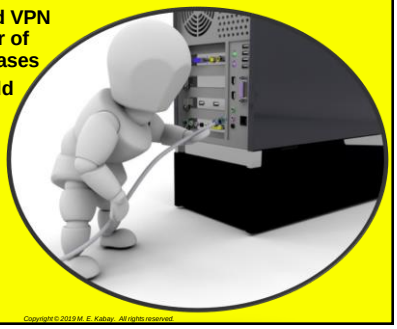
Traffic Inspection

- Encrypted traffic on VPN interferes with content inspection
- Limit inspection to post-decryption packets inside network after VPN device processes data stream
- Some VPN systems do provide administrative dynamic decryption of packets for content inspection

31

Processing Power

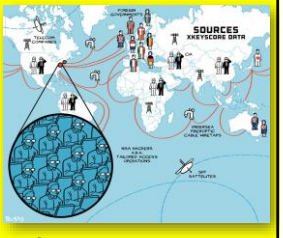
- VPN can easily become a bottleneck
- Monitor processing power required to maintain bandwidth
- Increase dedicated VPN devices as number of connections increases
- Can sometimes add hardware encryption accelerators



32

Interception (1)

- Possible to capture packets
  - Datagram Protocol spreads packets over multiple routes
  - Thus end-point interception only practical approach
  - Massively parallel computational power can crack encryption



- Person-in-the-middle (PITM) attack
  - While VPN session being established
  - Address Resolution Protocol (ARP) poisoning to redirect traffic to attacker's system

33

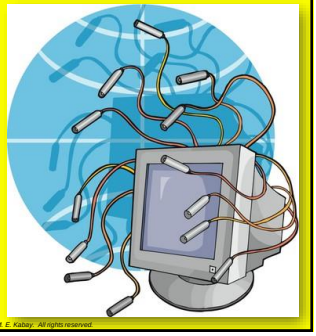
Interception (2)

- IPsec MITM vector: preshared key
  - Group name & password
  - Authenticate IPsec connection
  - *Fiked* emulates VPN termination & collects user credentials
  - Can defend using client or computer certificate for IPsec authentication
- SSLStrip (2009)
  - ARP-poisoning to intercept client request for TLS/SSL
  - Establishes valid TLS/SSL session with server
  - Creates HTTP session with user but puts fake lock icon into browser window
  - Can reduce risk by forcing use of direct TLS/SSL connections, not redirection from HTTP to HTTPS

34

Site-to-Site VPN Connections

- Infrastructure Design
- Cost
- Availability



35

Site-to-Site VPNs: Infrastructure Design

- Multiprotocol Layer Switching (MPLS) changes WAN administration
  - Can provide any-to-any connectivity
  - More difficult to troubleshoot than hub/spoke topology
- Increased number of security devices
- Maintain Border Gateway Protocol (BGP) routing security
  - Both sides must authenticate before being added to routing table
- VPN naturally puts Internet in contact with internal networks
  - Implement gateway security devices (GSD)

Site-to-Site VPNs: Cost

- New / converted circuits
- QoS (quality of service) monitoring
- Support for MPLS and routing
- Time for redesigning network routing infrastructure
- Site-to-site (S2S) VPNs require high processing power
  - May need code upgrades ($$)
- Higher administrative costs for managing increased number of devices

37

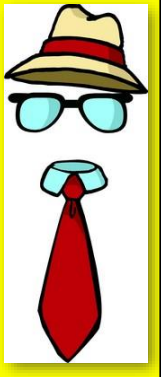
Site-to-Site VPNs: Availability

- VPNs quickly become necessity
- Mobile workforce may be severely impaired if VPNs go down
- Can load-balance across redundant systems
- Ideally, connections in process will not be dropped
- Must have redundant (independent) infrastructure elements
  - Internet links
  - Power
  - Other network components

38

Implications of Elusive VPNs

- More VPNs in use than administrators may be aware of
  - GotoMyPc
  - Malicious VPNs such as botnet control channels
  - Laplink™ software could allow unauthorized access to work PC
- Bypass normal administrative controls
- Peer-to-peer (P2P) networks use VPN-like features
- Skype can encrypt voice calls and file transfers
- Must plan for these in defining policies



39

Impact of IPv6

- We are running out of IPv4 address space (or have already)
- Yet migration to IPv6 still not evident in real world
- Verify that VPN infrastructure is IPv6 compliant
- Expect to have to translate IPv6 into IPv4 for foreseeable future
- IPv6 does provide support for IPSec automatically

Extranets

- Information Assurance Goals
- Extranet Concepts
- Types of Extranet Access
- Information Assurance Considerations

41

Extranets: Information Assurance Goals

- Protecting shared information assets
  - Increased security issues with external accessors
  - Competitive advantage, regulatory requirements
- Preventing information exposure
  - Principle of least privilege
  - Identity management
  - Access management
- Minimizing ancillary risks
  - Restrict outsiders' access to non-essential services

42

Extranet Concepts

- Service NW vs DMZ
  - Don't count on DMZ (weak security) for extranet services
  - Define specific firewall architecture with particular settings for extranet servers
- N-Tier Architecture
  - Distribute functions across multiple servers
  - E.g., separate front-end user-server from back-end database server
- SSL Encryption
  - Enforce HTTPS Secure Sockets Layer traffic
  - Verify that padlock icon is implemented correctly

Types of Extranet Access

Norwich University extranets
* owa for e-mail
* my.norwich.edu
* BannerWeb

- Vendor/Partner Information Sharing
  - ERP (enterprise resource planning)
  - SCM (supply chain management)
- E-Commerce
  - EDI (electronic data interchange)
  - CRM (customer relationship management)
  - B2B (business to business)
  - B2C (business to client)
- Employee Self-Service
  - E-mail
  - Benefits systems
  - Access to intranet systems

44

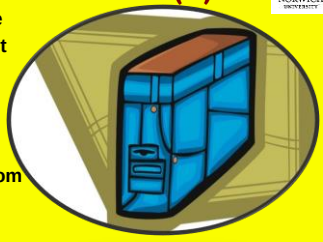
Extranets: Information Assurance Considerations (1)

- Technical Security
  - Cannot secure using only a single point
  - Need security at multiple layers
- Traffic Inspection
  - Difficult between nodes
  - May have to inspect traffic on extranet server before encryption
    - ✓Increases processing load on server CPU
  - Or may terminate SSL upstream and send cleartext data to extranet server
    - ✓Relieves extranet server of need for decryption / encryption processing

45

Extranet IA Considerations (2)

- Internal Network Exposure
  - Compromise of extranet server must not allow breach of inside resources
    - ✓Ensure appropriate firewalls to shield internal networks from extranet
- Server
  - Harden servers by removing vulnerable unused services
    - ✓Configure for minimum functionality required
  - Close attention to patches
  - Intrusion prevention/detection devices
  - Virtualization has additional complexities



46

Extranet IA Considerations (3)

- Application
  - Many systems susceptible to common attacks
    - ✓Buffer overflows
    - ✓SQL injection
    - ✓Cross-site scripting (XSS)
  - Developers must keep security in mind throughout process
    - ✓Use best practices
    - ✓Stay current on threat landscape

BO: failure to prevent data outside bounds of a buffer from being accepted in input and then used.

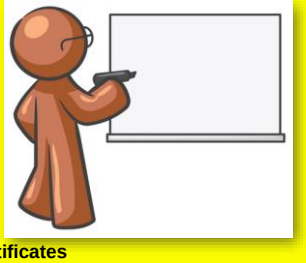
SQLI: DB query sw doesn't test query statement for correctness.

XSS: Browser executes hostile script; e.g., hiding code in bogus URL for non-existent page.

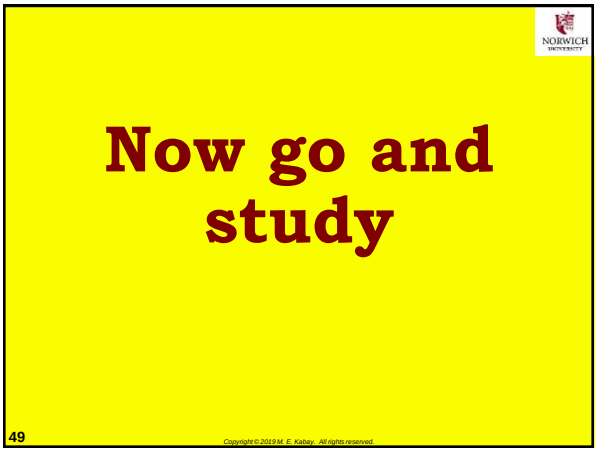
47

Extranet IA Considerations (4)

- Policies
  - Provide written policies about requirements for access & use
  - Establish expectations
  - Useful for legal proceedings
- Access & Identity Management
  - I&A support access controls
  - But passwords a poor authentication method
  - Better: issuing digital certificates
- Availability: critical issue – plan for it!
- Impact of IPv6: infrastructure support issues



48


NORWICH
UNIVERSITY
Now go and study
49
Copyright © 2019 M. E. Kabay. All rights reserved.