ΕΜΠΟΡΙΚΟ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

Η επιχείρηση μετά τα e

Ασφάλεια Δικτύων και Υποδομών

Παρουσίαση στα πλαίσια των κύκλων εκπαίδευσης του ΕΒΕΘ

Θεσσαλονίκη, Απρίλιος 2006

Σπύρογλου Οδυσσέας, M.Sc., Υπ. Δρ. ΑΠΘ
Μηχανικός – Αναλυτής Πληροφοριακών Συστημάτων

Agenda

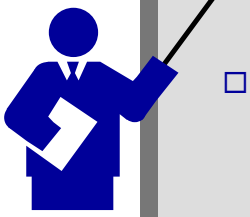
- Γιατί απειλείται η ασφάλεια;
- Πώς απειλείται;
- Συνιστώσες της ασφάλειας:
  - Ταυτότητα χρηστών (Identity)

    Χρήση κωδικών , τρόποι πιστοποίησης χρηστών, Kerberos, Digital Signatures

14/5/2006 **2**

Agenda – cont.

- Ακεραιότητα πόρων (Integrity)
  Firewalls, Proxy Servers, Κρυπτογράφηση Δεδομένων, IPSec
- Καταγραφή και παρακολούθηση (Active Audit)



14/5/2006 3

Όλα τα δίκτυα απαιτούν ασφάλεια

- Ανεξαρτήτως μεγέθους εταιρείας
- Internet σήμερα ότι η τηλεφώνια το 1940
- Ακόμα και sites μικρών εταιρείων «σπάνε»

14/5/2006 4

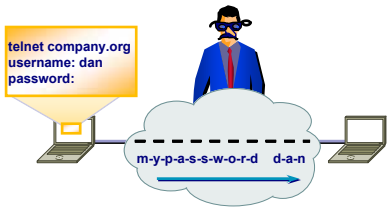
Γιατί ασφάλεια;

- 3 Κύριοι λόγοι
  - Έλλειψη πολιτικών ασφαλείας Access Control Lists
  - Κενά στην παραμετροποίηση συστημάτων
  - Ξεπερασμένη – Ελλιπής τεχνολογία

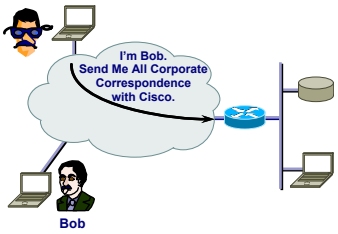
Και πολλοί που θέλουν να τα εκμεταλλευτούν

14/5/2006 5

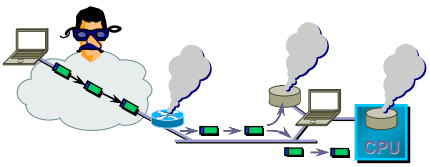
Απειλές



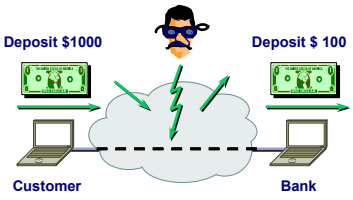
Loss of Privacy



Impersonation



Denial of Service



Loss of Integrity

14/5/2006 6

Στόχος: Εξισορρόπηση Αναγκών με κίνδυνους

Πρόσβαση		Ασφάλεια
Συνδεσιμότητα		Πιστοποίηση
Επιδόσεις		Authentication
Ευκολία		Άδεια
Διαχείριση		Authorization
Διαθεσιμότητα	Πολιτικές	Οικονομία
		Εξασφάλιση
		Assurance
		Εμπιστευτικότητα
		Confidentiality
		Ασφάλεια Δεδομένων
		Data Integrity

14/5/2006 7

Ασφάλεια Δικτύων : Αναλογία με φυσικό περιβάλλον

Πόρτες, κλειδαριές & φύλακες	→ Firewalls & access controls
Κλειδιά & Σήματα	→ Authentication
Παρακολούθηση κάμερες & σένσορες	→ Intrusion detection system

- **Συμπληρωματικοί μηχανισμοί**

14/5/2006 8

Στοιχεία της Ασφάλειας

- Ταυτότητα
  - Ακρίβεια στην ταυτοποίηση
  - Τι μπορούν να κάνουν οι χρήστες
- Αξιοπιστία
  - Εξασφάλιση λειτουργίας
  - Περιμετρική ασφάλεια
  - Ιδιωτικότητα
- Εσωτερικός έλεγχος
  - Εντοπισμός Ευπαθών σημείων
  - Εντοπισμός εισβολέων

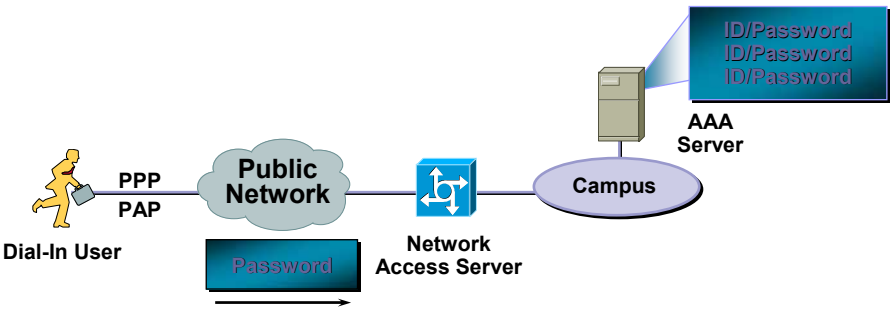
14/5/2006 9

Ταυτότητα

- Μοναδική ταυτοποίηση χρηστών και εφαρμογών
  - Username/password, PAP, CHAP, AAA server, one-time password, RADIUS, TACACS+, Kerberos, MS-login, digital certificates, directory services, Network Address Translation

14/5/2006 10

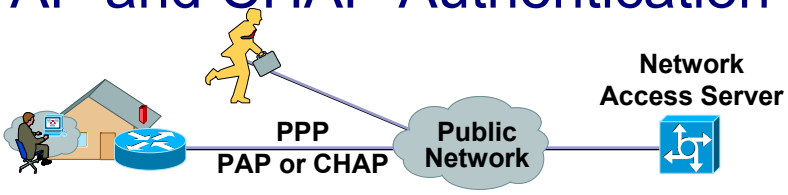
Username/Password



- User dials in with password to NAS network access server
- NAS sends ID/password to AAA server
- AAA server authenticates user ID/password and tells NAS to accept (or reject)
- NAS accepts (or rejects) call

14/5/2006 11

PAP and CHAP Authentication

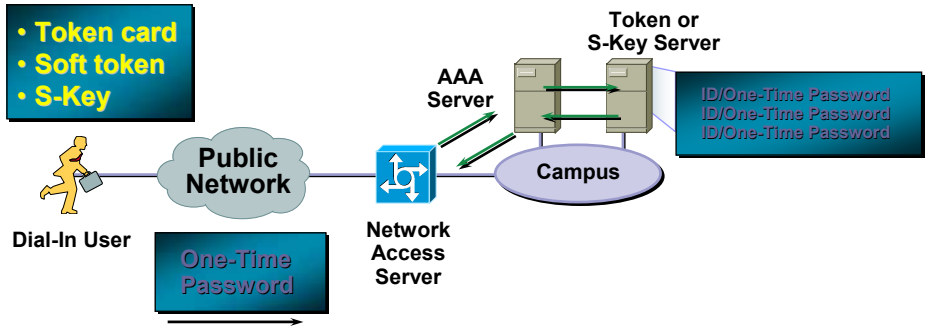


- Password Authentication Protocol (PAP)
  - Authenticates caller only
  - Passes password in clear text
- Challenge Handshake Authentication Protocol (CHAP)
  - Authenticates both sides
  - Password is encrypted

14/5/2006 12

One-Time Password

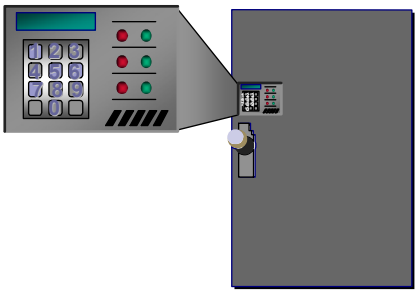
- Token card
- Soft token
- S-Key



- Additional level of security, guards against password guessing and cracking
  - Prevents spoofing, replay attacks
- Single-use password is generated by token card or in software
- Synchronized central server authenticates user
- S-key is a PC application that presents a dialog box to the user upon login into which the user must enter the correct combination of six key words.

14/5/2006 13

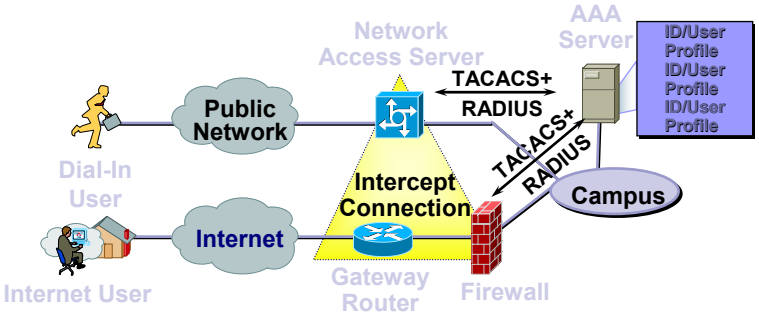
Authentication, Authorization, and Accounting (AAA)



- Tool for enforcing security policy
  - Authentication
    - Verifies identity— Who are you?
  - Authorization
    - Configures integrity— What are you permitted to do?
  - Accounting
    - Assists with audit— What did you do?

14/5/2006 14

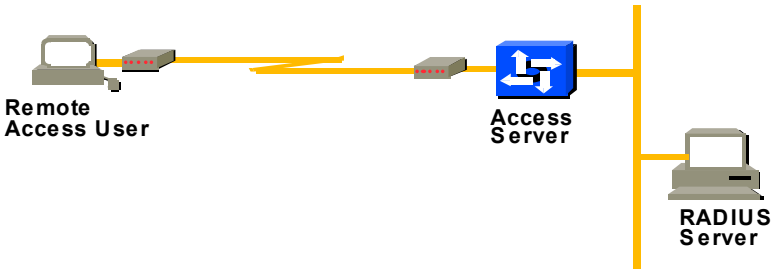
AAA Services



- Centralized security database
- High availability
- Same policy across many access points
- Per-user access control
- Single network login
- Support for: TACACS+, RADIUS (IETF), Kerberos, one-time password

14/5/2006 15

RADIUS

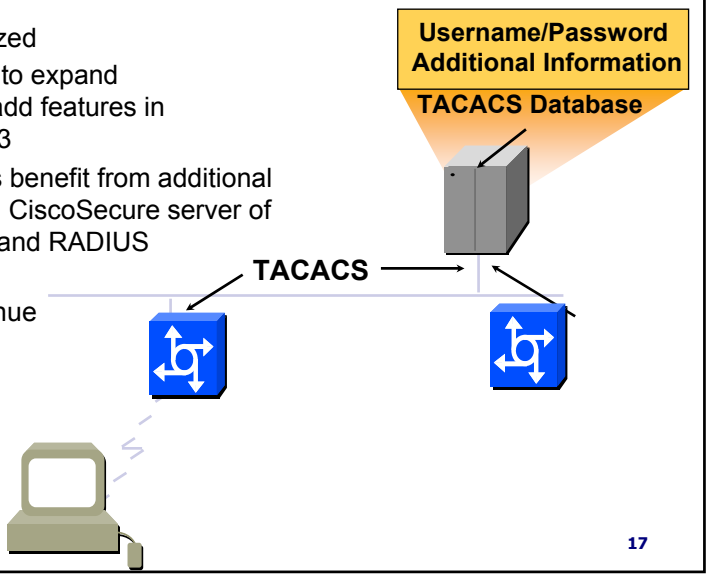


- **RADIUS is an industry standard—RFC 2138, RFC 2139**
- **Cisco has full IETF RFC implementation**
- **Cisco has implemented many nonstandard vendor proprietary attributes**
- **Cisco hardware will work well with non-Cisco RADIUS AAA servers**
- **Cisco is committed to providing the best RADIUS solution**

14/5/2006 16

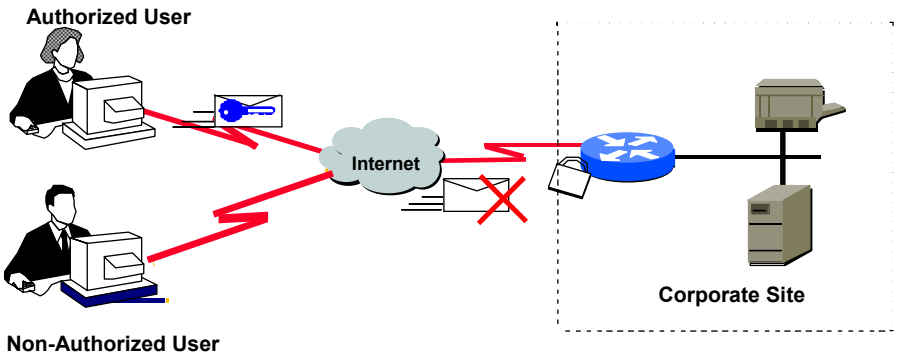
TACACS+ Authentication

- Local or centralized
- Cisco continues to expand TACACS+ and add features in Cisco IOS™ 11.3
- Cisco customers benefit from additional functionality with CiscoSecure server of both TACACS+ and RADIUS
- Cisco enterprise customers continue to ask for TACACS+ features



14/5/2006 17

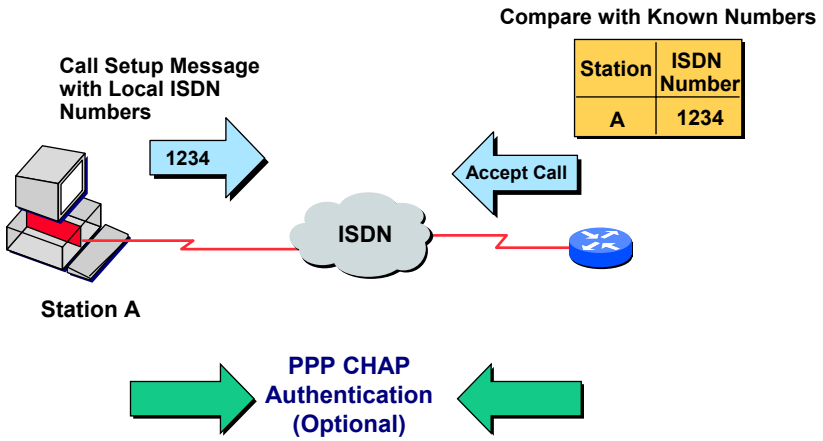
Lock-and-Key Security



- Dynamically assigns access control lists on a per-user basis
- Allows a remote host to access a local host via the Internet
- Allows local hosts to access a host on a remote network

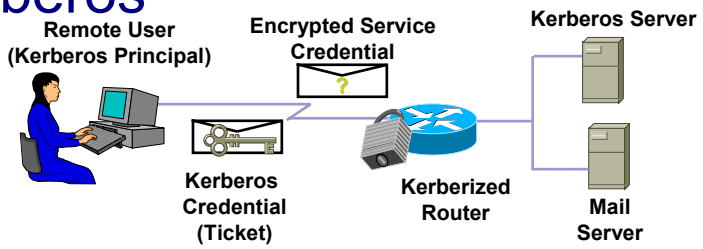
14/5/2006 18

Calling Line Identification



14/5/2006 19

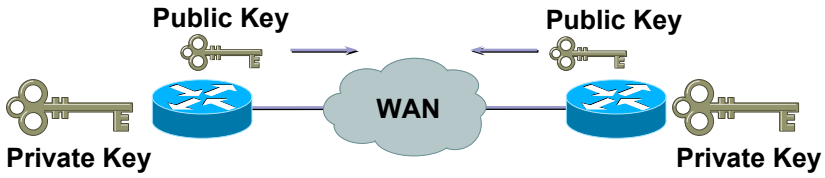
User Authentication with Kerberos



- Authenticates users and the network services they use
- Uses “tickets” or “credentials” issued by a trusted Kerberos server
  - Limited life span; can be used in place of standard “user/password” mechanism

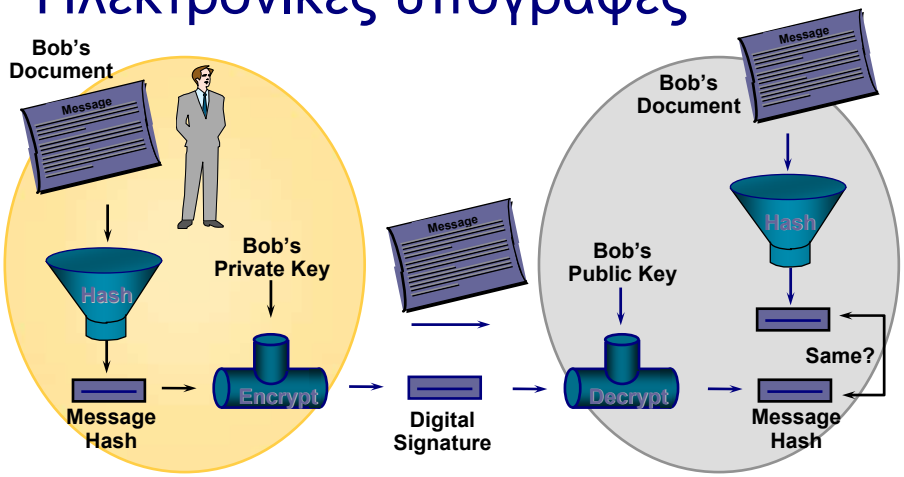
14/5/2006 20

Δημόσια Κλειδιά



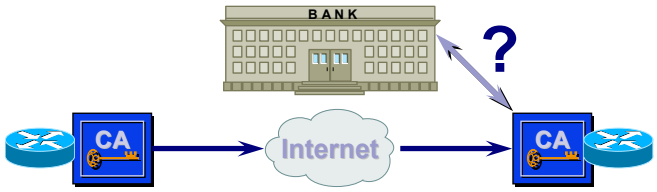
- By exchanging public keys, two devices can determine a new unique key (the secret key) known only to them

Ηλεκτρονικές υπογραφές



- If verification is successful, document has not been altered

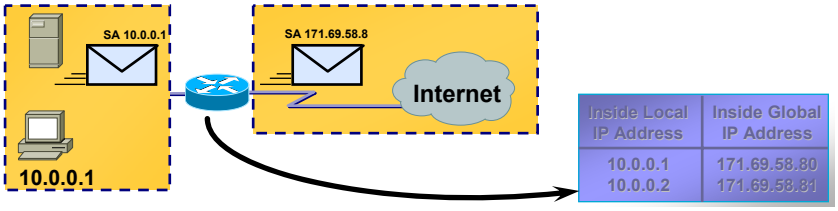
Πιστοποιητικά



- **Certificate Authority (CA) verifies identity**
- **CA signs digital certificate containing device's public key**
- **Certificate equivalent to an ID card**
- **Partners include Verisign, Entrust, Netscape, and Baltimore Technologies**

14/5/2006 **23**

Network Address Translation



- Provides dynamic or static translation of private addresses to registered IP addresses
- Eliminates readdressing overhead—Large admin. cost benefit
- Conserves addresses—Hosts can share a single registered IP address for all external communications via port-level multiplexing
- Permits use of a single IP address range in multiple intranets
- Hides internal addresses
- Augmented by EasyIP DHCP host function

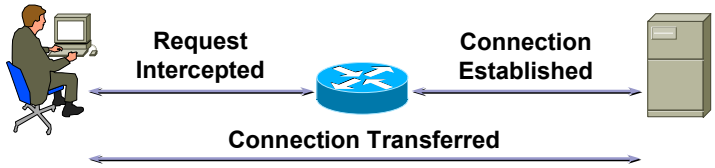
14/5/2006 **24**

Integrity—Network Availability

- Ensure the network infrastructure remains available
  - TCP Intercept, route authentication

14/5/2006 25

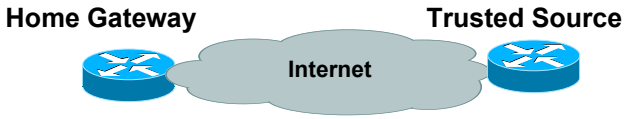
TCP Intercept



- Protects networks against denial of service attacks
- TCP SYN flooding can overwhelm server and cause it to deny service, exhaust memory, or waste processor cycles
- TCP Intercept protects network by intercepting TCP connection requests and replying on behalf of the destination
- Can be configured to passively monitor TCP connection requests and respond if connection fails to be established in a configurable interval

14/5/2006 26

Route Authentication



- Enables routers to identify one another and verify each other's legitimacy before accepting route updates
- Ensures that routers receive legitimate update information from a "trusted" source

14/5/2006 27

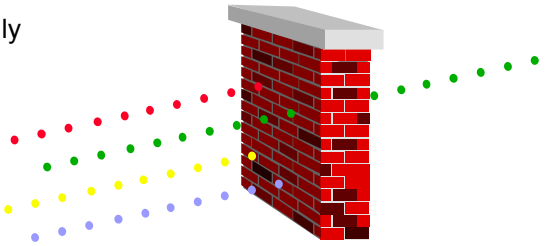
Integrity—Perimeter Security

- Control access to critical network applications, data, and services
  - Access control lists, firewall technologies, content filtering, CBAC, authentication

14/5/2006 28

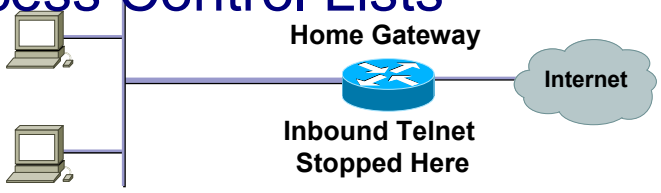
Access Lists

- Standard
  - Filter source address only
  - Permit/deny entire protocol suite
- Extended
  - Filter source, destination addresses
  - Inbound or outbound
  - Port number
  - Permit/deny specific protocols
  - Reflexive
  - Time-based



14/5/2006 29

Policy Enforcement Using Access Control Lists



- Ability to stop or reroute traffic based on packet characteristics
- Access control on incoming or outgoing interfaces
- Works together with NetFlow to provide high-speed enforcement on network access points
- Violation logging provides useful information to network managers

14/5/2006 30

Importance of Firewalls

- Permit secure access to resources
- Protect networks from:
  - Unauthorized intrusion from both external and internal sources
  - Denial of service (DOS) attacks

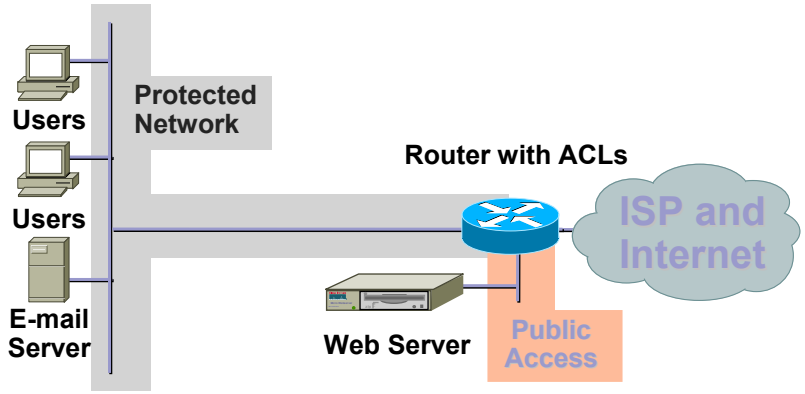
14/5/2006 31

What Is a Firewall?

- All traffic from inside to outside and vice versa must pass through the firewall
- Only authorized traffic, as defined by the local security policy, is allowed in or out
- The firewall itself is immune to penetration

14/5/2006 32

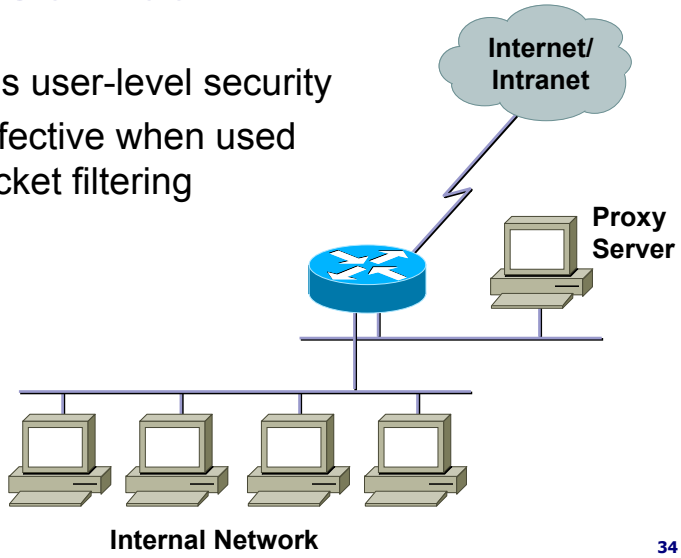
Packet-Filtering Routers



14/5/2006 33

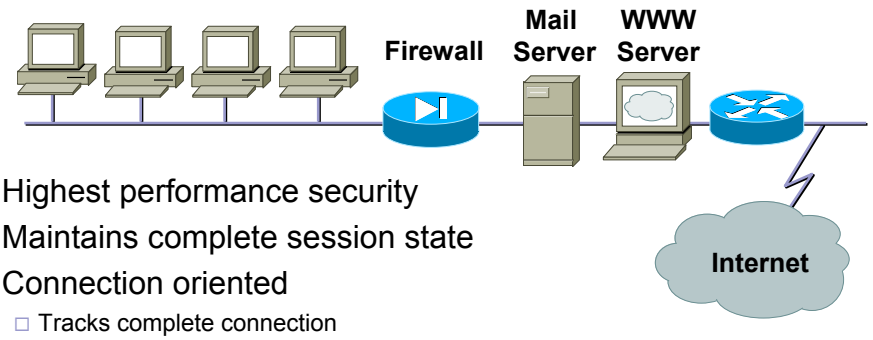
Proxy Service

- Provides user-level security
- Most effective when used with packet filtering



14/5/2006 34

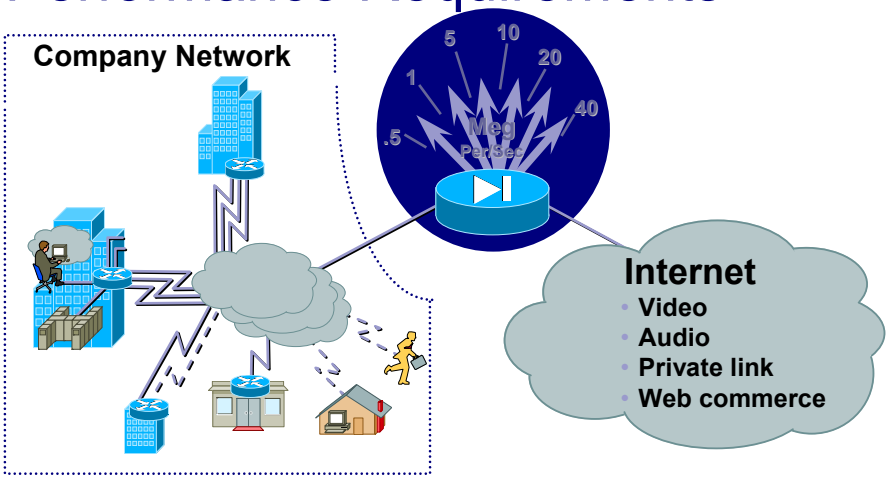
Stateful Sessions



- Highest performance security
- Maintains complete session state
- Connection oriented
  - Tracks complete connection
  - Establishment and termination
- Strong audit capability
- Easy to add new applications

14/5/2006 35

Performance Requirements



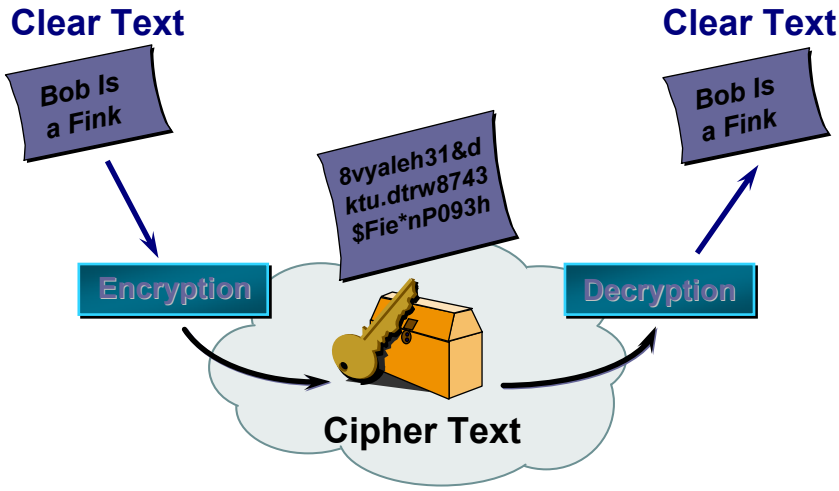
14/5/2006 36

Integrity—Privacy

- Provide authenticated private communication on demand
  - VPNs, IPSec, IKE, encryption, DES, 3DES, digital certificates, CET, CEP

14/5/2006 37

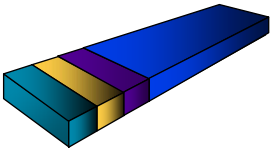
Encryption and Decryption



14/5/2006 38

What Is IPSec?

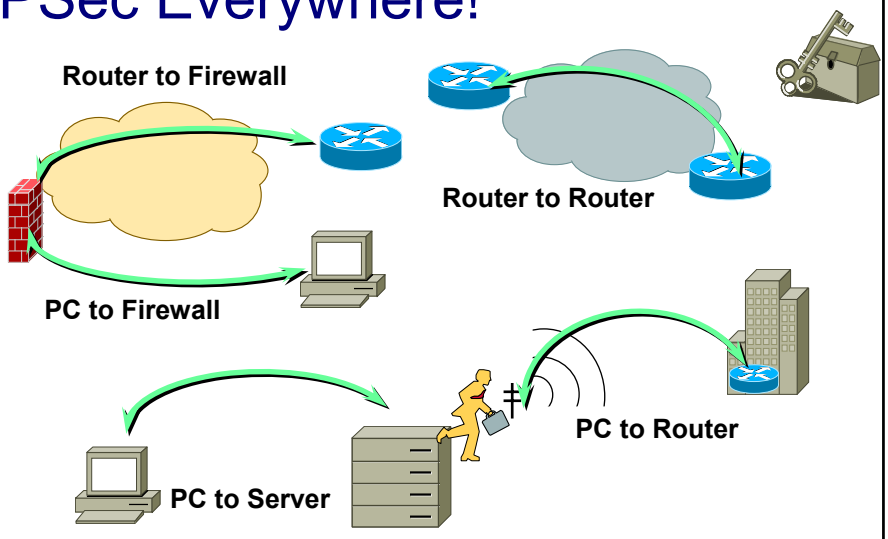
- Network-layer encryption and authentication
  - Open standards for ensuring secure private communications over any IP network, including the Internet
  - Provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy
  - Data protected with network encryption, digital certification, and device authentication



- Implemented transparently in network infrastructure
- Includes routers, firewalls, PCs, and servers
- Scales from small to very large networks

14/5/2006 39

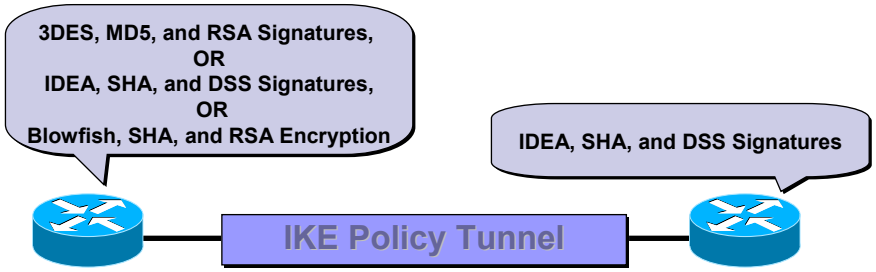
IPSec Everywhere!



14/5/2006 40

IKE—Internet Key Exchange

- Automatically negotiates policy to protect communication
- Authenticated Diffie-Hellman key exchange
- Negotiates (possibly multiple) security associations for IPSec

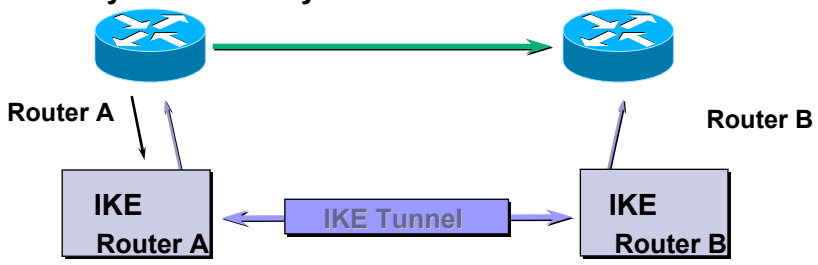


14/5/2006 41

How IPSec Uses IKE

1. Outbound packet from Alice to Bob—No IPSec security association yet

4. Packet is sent from Alice to Bob protected by IPSec SA



2. Router A's IKE begins negotiation with router B's IKE

3. Negotiation complete; router A and router B now have complete IPSec SAs in place

14/5/2006 42

Encryption—DES and 3DES

- Widely adopted standard
- Encrypts plain text, which becomes cyphertext
- DES performs 16 rounds
- Triple DES (3DES)
  - The 56-bit DES algorithm runs three times
  - 112-bit triple DES includes two keys
  - 168-bit triple DES includes three keys
- Accomplished on a VPN client, server, router, or firewall

14/5/2006 43

Breaking DES Keys

- Exhaustive search is the only way to break DES keys (so far)
- Would take hundreds of years on fastest general purpose computers (56-bit DES)
  - Specialized computer would cost $1,000,000 but could crack keys in 35 minutes (Source: M.J. Wiener)
- Internet enables multiple computers to work simultaneously
- Electronic Frontier Foundation and distributed.net cracked a 56-bit DES challenge in 22 hours and 15 minutes

Consensus of the cryptographic community is that 56-bit DES, if not currently insecure, will soon be insecure

14/5/2006 44

Why Active Audit?

- The hacker might be an employee or "trusted" partner
  - Up to 80% of security breaches come from the inside (Source: FBI)
- Your defense might be ineffective
  - One out of every three intrusions occur where a firewall is in place (Source: Computer Security Institute)
- Your employees might make mistakes
  - Misconfigured firewalls, servers, etc.
- Your network will grow and change
  - Each change introduces new security risks

Firewalls, authorization, and encryption do not provide VISIBILITY into these problems

14/5/2006 45

Why Active Audit?

- Network security requires a layered defense
  - Point security PLUS active systems to measure vulnerabilities and monitor for misuse
  - Network perimeter and the intranet
- Security is an ongoing, operational process
  - Must be constantly measured, monitored, and improved

14/5/2006 46

Active Audit—Network Vulnerability Assessment

- Assess and report on the security status of network components
  - Scanning (active, passive), vulnerability database

14/5/2006 47

Active Audit—Intrusion Detection System

- Identify and react to known or suspected network intrusion or anomalies
  - Passive promiscuous monitoring
  - Database of threats or suspect behavior
  - Communication infrastructure or access control changes

14/5/2006 48

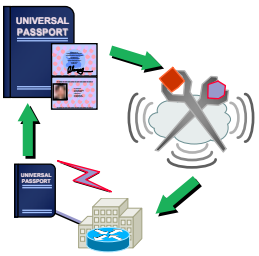
IDS Attack Detection

	"Atomic" Single Packet	"Composite" Multiple Packets
Context: (Header)	Ping of Death Land Attack	Port Sweep SYN Attack TCP Hijacking
Content: (Data)	MS IE Attack DNS Attacks	Telnet Attacks Character Mode Attacks

14/5/2006 49

Active Audit

- Actively audit and verify policy
- Detect intrusion and anomalies
- Report



14/5/2006 50

Περίληψη

- Κρίσιμη απαίτηση για όλα τα δίκτυα
- Απαιτεί κοινή, ευρέως εφαρμογή
- Απαιτεί πολύ-επίπεδη υλοποίηση

14/5/2006 51

Πολιτική Χρηστών

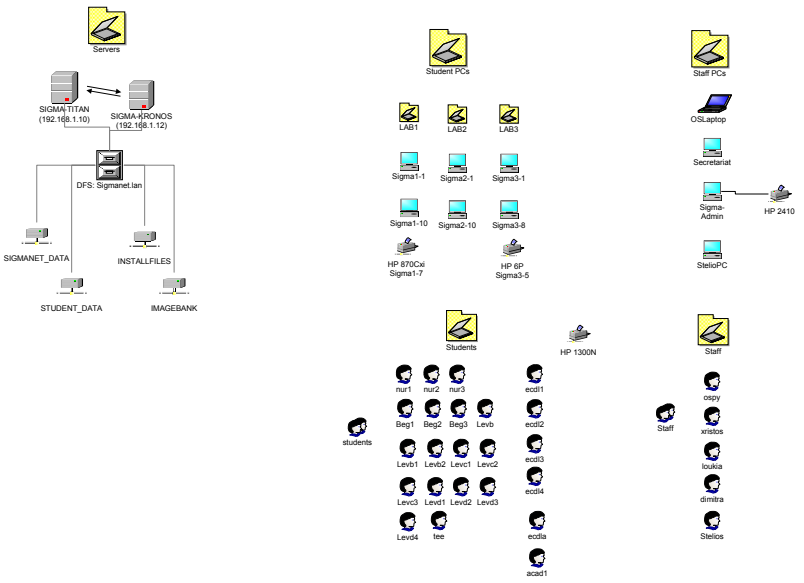
- Ποιοι είναι;
- Που έχουν πρόσβαση;
- Σε τι επίπεδο;
- Τι απαιτήσεις έχουν;

14/5/2006 52

Λύσεις Λογισμικού

- Firewall
- Antivirus
- Antispyware
- Filtering
- Cryptography

14/5/2006 53



14/5/2006 54