CSE 543 - Computer Security (Fall 2004)

Lecture 17 - Network Security

November 4, 2004

URL: http://www.cse.psu.edu/~cg543/

Coms. Security: the threats

- Adversary 1: some unauthorized

  entity attempting to gain access to host resource
- Adversary 2: an malicious intermediary passively listening on the network for sensitive data

Communications Security

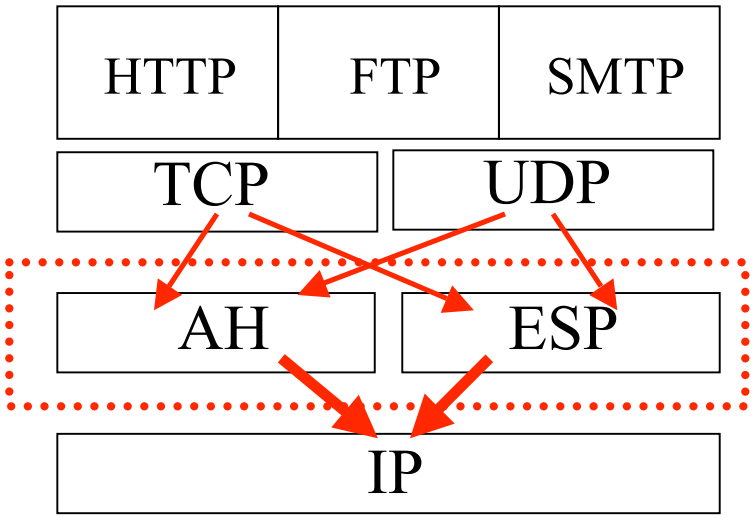
- A host wants to establish a secure channel to remote hosts over an untrusted network
  - Not Login – end-users may not even be aware that protections in place
  - Remote hosts may be internal or external
- The protection service must …
  - Authenticate the end-points (each other)
  - Negotiate what security is necessary (and how)
  - Establish a secure channel
  - Process the traffic between the end points

IPsec (not IPSec!)

- Host level protection service
  - IP-layer security (below TCP/UDP)
  - De-facto standard for host level security
  - Developed by the IETF (over many years)
  - Now available in most operating systems
    - E.g., Available in XP, OS X, Linux, BSD*, …
  - Implements a wide range of protocols and cryptographic algorithms
- Provides ….
  - Confidentiality, integrity, authenticity, replay protection, DOS protection

IPsec Protocols and the stack

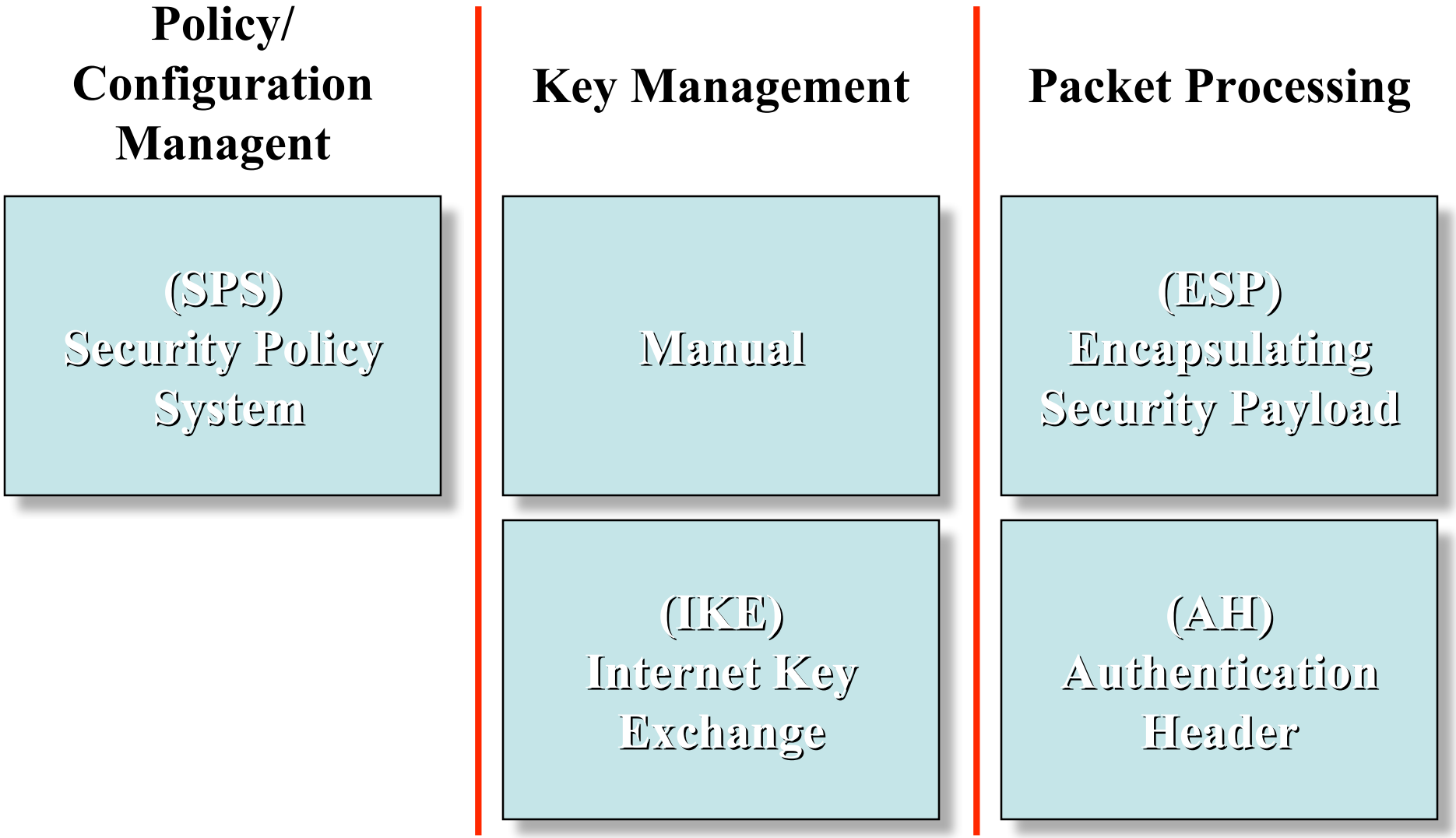
- IPsec puts the two main protocols in between IP and the other protocols
  - AH - authentication header
  - ESP - encapsulating security payload



- Tunnel vs. transport?

- Other function provided by external protocols and architectures
  - Key management/authentication
  - Policy

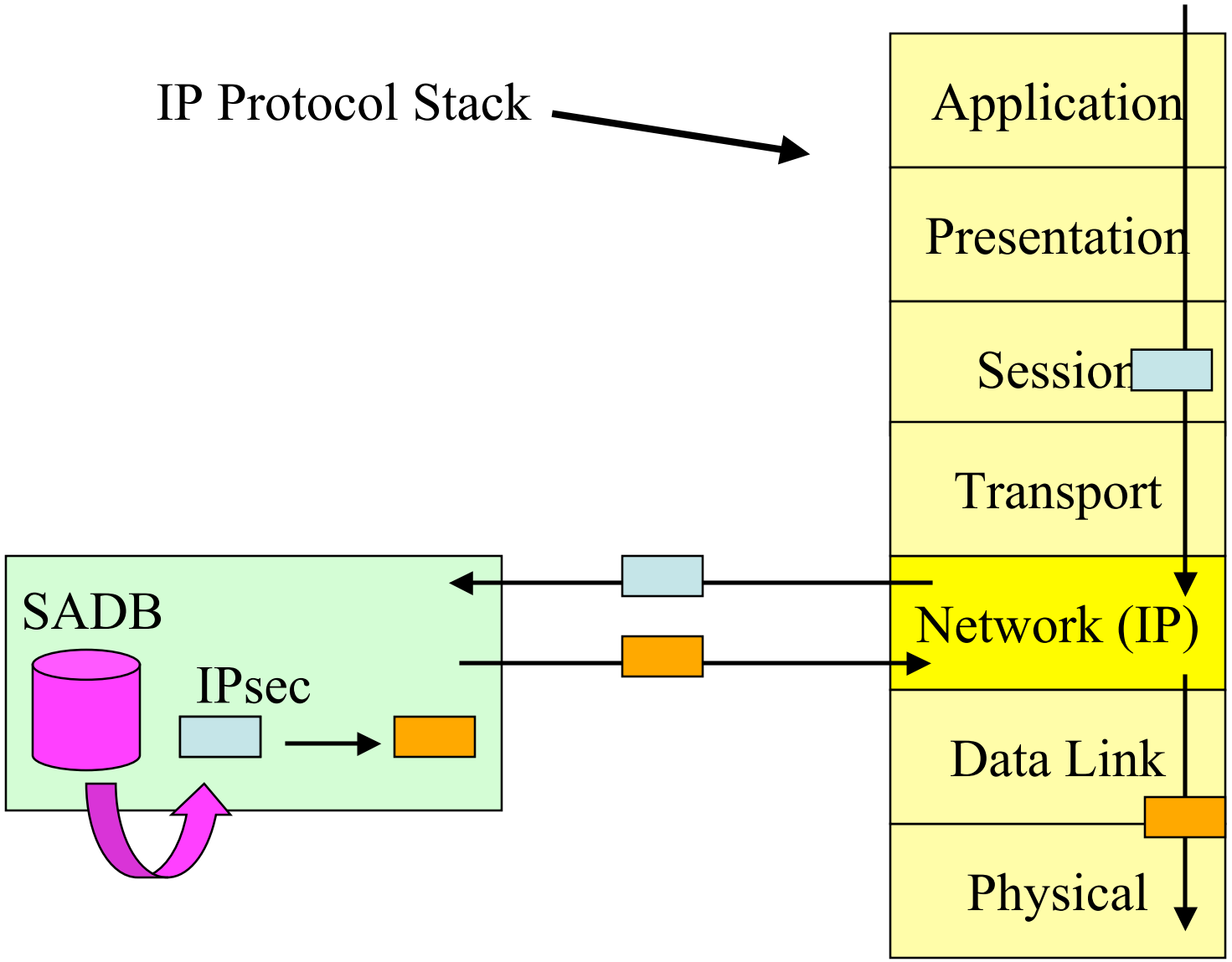
IPsec Protocol Suite



Internet Key Exchange (IKE)

- Built on of ISAKMP framework
- Two phase protocol used to establish parameters and keys for session
  - Phase 1: negotiate parameters, authenticate peers, establish secure channel
  - Phase 2: Establish a security association (SA)
- The details are unimaginably complex
- The SA defines algorithms, keys, and policy used to secure the session

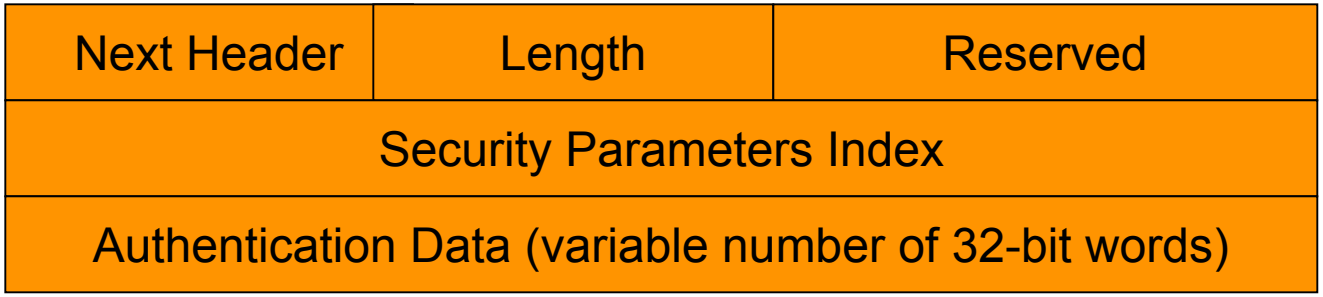
IPsec: Packet Handling (Bump …)



IPsec AH Packet Format

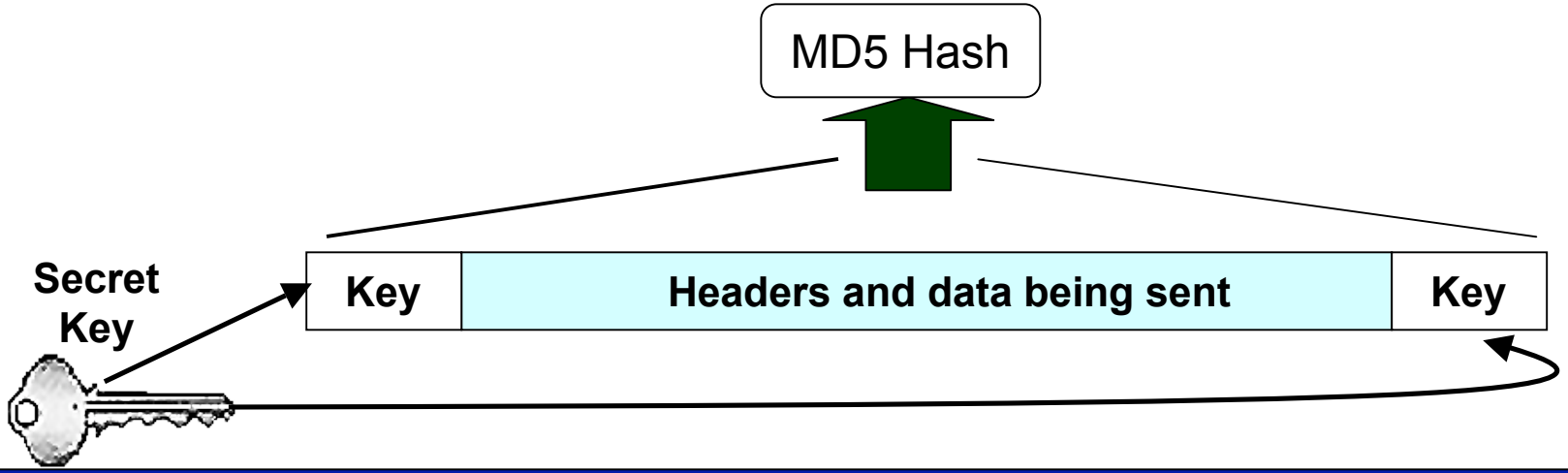
IPv4 AH Packet Format

AH Header Format



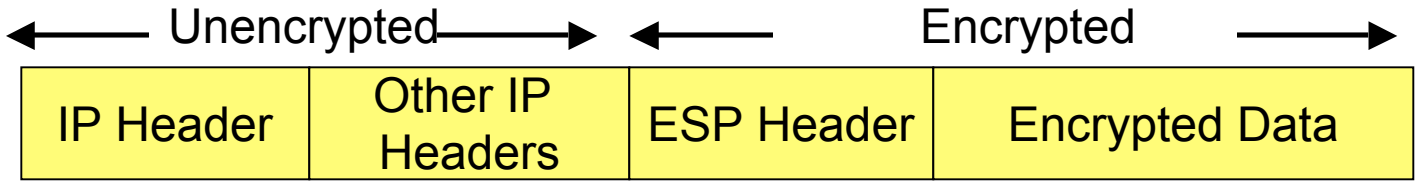
IPsec Authentication

- SPI: (spy) identifies the security association for this packet
  - Type of crypto checksum, how large it is, and how it is computed
  - Really the policy for the packet
- Authentication data
  - Hash of packet contents include IP header as as specified by SPI
  - Treat transient fields (TTL, header checksum) as zero
- Keyed MD5 Hash is default



IPsec ESP Packet Format

IPv4 ESP Packet Format



ESP Header Format

Security Association Identifier
Opaque Transform Data, variable length

DES + MD5 ESP Format

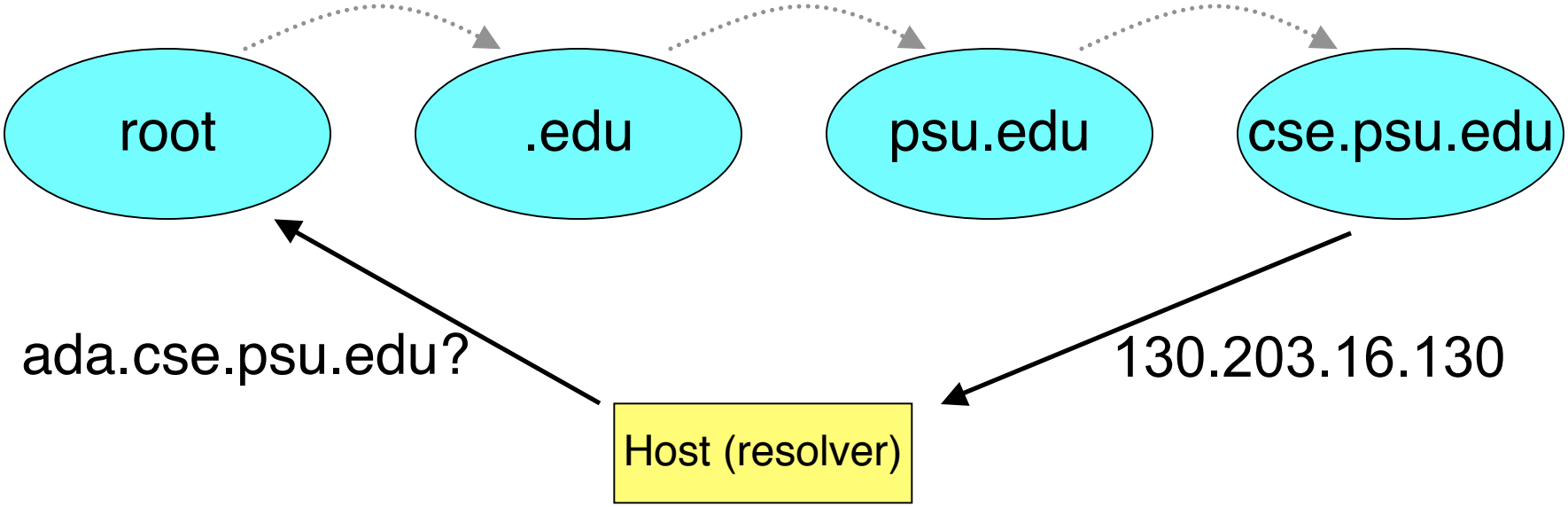
Security Parameters Index (SPI)
Initialization Vector (optional)
Replay Prevention Field (incrementing count)
Payload Data (with padding)
Authentication checksum

Practical Issues and Limitations

- IPsec implementations
  - Often not compatible (ungh.)
  - Large footprint
    - resource poor devices are in trouble
    - New standards to simplify (e.g, JFK)
  - Slow to adopt new technologies
- Issues
  - IPsec tries to be “everything for everybody at all times”
    - Massive, complicated, and unwieldy
  - Policy infrastructure has not emerged
  - Large-scale management tools are limited (e.g., CISCO)
  - Often not used securely (common pre-shared keys)

DNS - The domain name system

- DNS maps between IP address (12.1.1.3) and domain and host names (ada.cse.psu.edu)
  - How it works: the “root” servers redirect you to the top level domains (TLD) DNS servers, which redirect you to the appropriate sub-domain, and recursively ….
  - Note: there are 13 “root” servers that contain the TLDs for .org, .edu, and country specific registries (.fr, .ch)

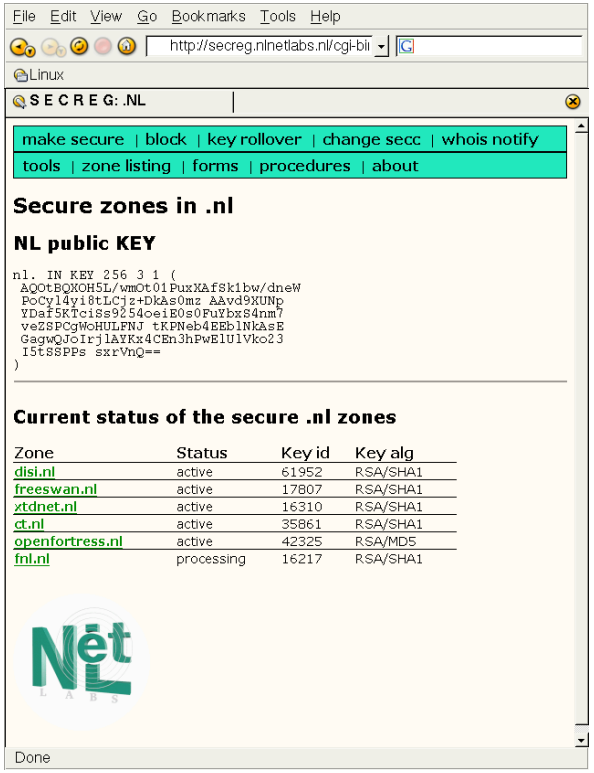


DNS Vulnerabilities

- Nothing is authenticated, so really the game is over
  - You can not really trust what you hear …
  - But, many applications are doing just that.
  - Spoofing of DNS is really dangerous
- Moreover, DNS is a catalog of resources
  - Zone-transfers allow bulk acquisition of DNS data
  - … and hence provide a map for attacking the network
- Lots of opportunity to abuse the system
  - Relies heavily on caching for efficiency -- cache pollution
  - Once something is wrong, it can remain that way in caches for a long time (e.g., it takes a long time flush)
  - Data may be corrupted before it gets to authoritative server

DNS-sec

- A standard-based (IETF) solution to security in DNS
  - Prevents data spoofing and corruption
  - Public key based solution to verifying DNS data
  - Authenticates
    - Communication between servers
    - DNS data
    - Public keys (a bootstrap for PKI?)



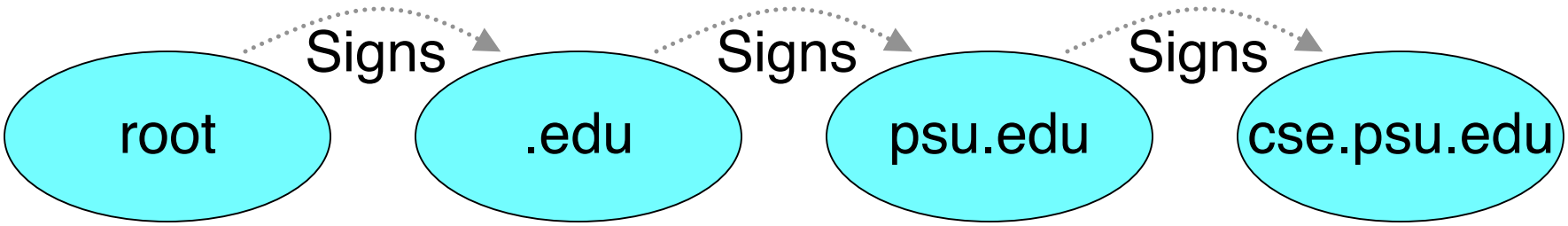
DNSsec Mechanisms

- TSIG : transaction signatures protect DNS operations
  - Zone loads, some server to server requests (master -> slave), etc.
  - Time-stamped signed responses for dynamic requests
  - A misnomer -- it currently uses shared secrets for TSIG (HMAC) or do real signatures using public key cryptography
- SIG0: a public key equivalent of TSIG
  - Works similarly, but with public keys
  - Not as popular as TSIG, being evaluated

- Note: these mechanisms assume clock sync. (NTP)

DNSsec Mechanisms

- Securing the DNS records
  - Each domain signs their “zone” with a private key
  - Public keys published via DNS
  - An indirectly signed by parent zones
  - Ideally, you only need to sign root, and follow keys down the hierarchy

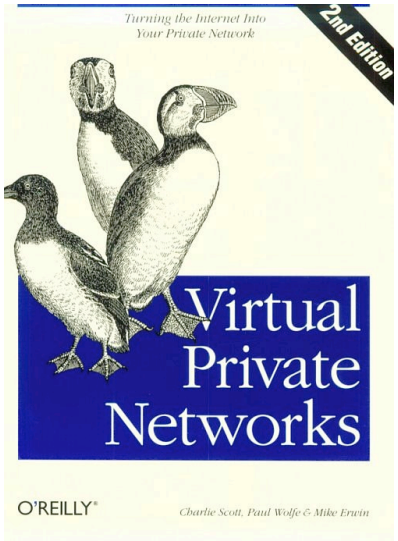


DNSsec challenges

- Incremental deployability
  - Everyone has DNS, can't assume a flag day
- Resource imbalances
  - Some devices can't afford real authentication
- Cultural
  - Most people don't have any strong reason to have secure DNS ($$$ not justified in most environments)
  - Lots of transitive trust assumptions (you have no idea how the middlemen do business)

- Take away: DNSsec will be deployed, but it is unclear whether it will be used appropriately/widely

Practical Issues and Limitations



- VPNs
  - Great for extending network
  - Most are built on IPsec
  - VLANs provide physical separation
- Issues
  - VPNs extend you network to many endpoints
    - Little control over hosts outside your perimeter
  - Key Management often poorly managed
    - E.g., company "X" single key problem
    - Leads to complex host ejection (stolen laptop)

Address Resolution Protocol (ARP)

- Protocol used to map IP address onto the physical layer addresses (MAC)
  1) ARP request: who has x.x.x.x?
  2) ARP response: me!
- Policy: last one in wins
- Used to forward packets on the appropriate interfaces by network devices (e.g., bridges)

- Q: Why would you want to spoof an IP address?

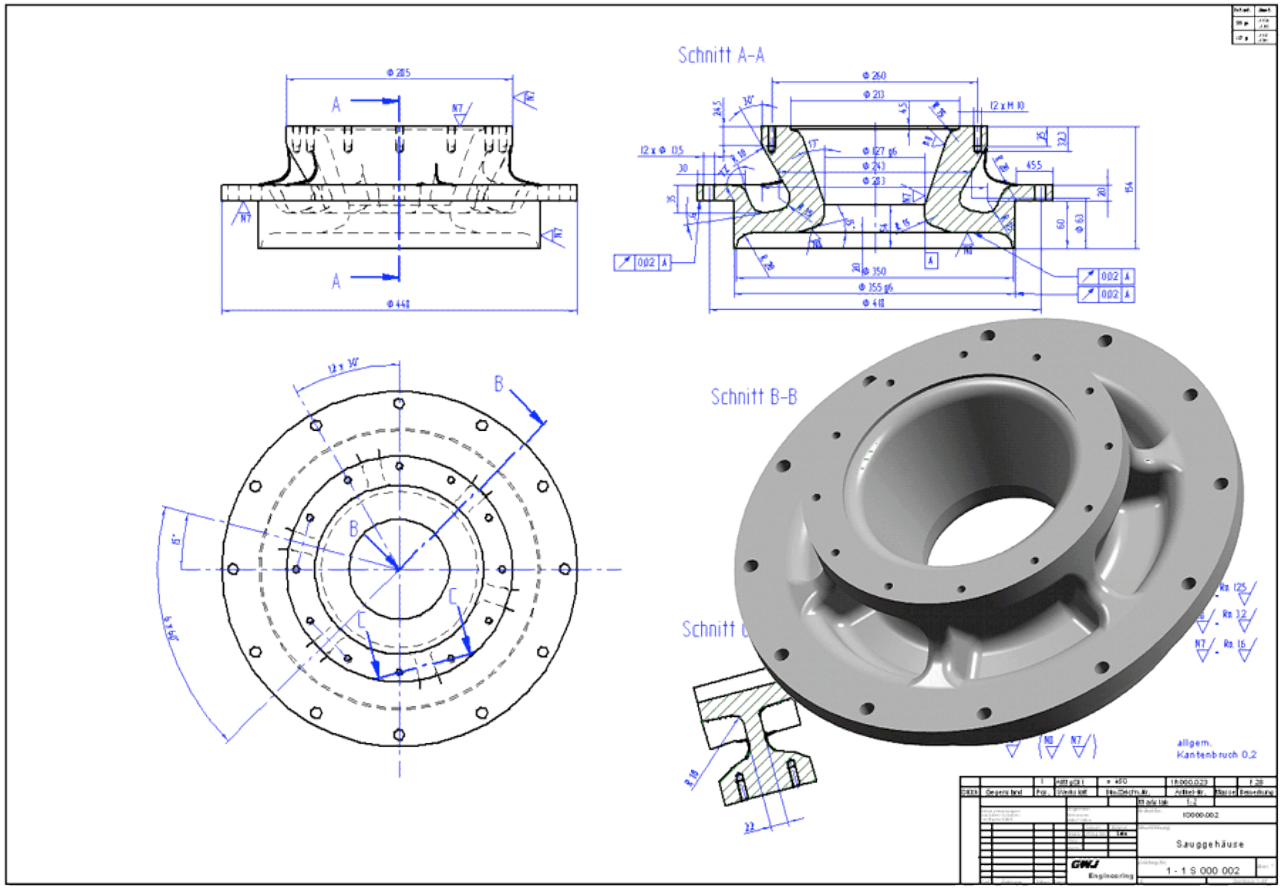
ARP poisoning

- Attack: replace good entries with your own
- Leads to
  - Session hijacking
  - Man-in-the-middle attacks
  - Denial of service, etc.

- Lots of other ways to abuse ARP.
- Nobody has really come up with a good solution
  - Except smart bridges, routers that keep track of MACs
- However, some not worried
  - If adversary is in your perimeter, you are in big trouble
  - You should never should validate the source of each pack independently (e.g., via IPsec)

ARP Security Solutions

- Not many … but people are trying



- Homework: How would you fix it?

Homework (due 11/16)

- Solve the ARP security problem.
  - Issues: what are the security problems in ARP (you probably need to look up related works)
  - Constraints: what are the constraints of the problem
  - Solutions: what does the design space look like, which solutions appear to be best and why

- Note: pretend you are writing to the security expert in a company. You need to convince him (Prof. McDaniel) that the problem is worth solving, that you understand the constraints, and that your solution will work.
- You are REQUIRED to work alone
- 2 Pages of Latex formatted (Word will receive 0%)
- You have all degrees of freedom, you choose best solution