Phishing

What is Phishing?

- Spoofed emails, purportedly from a financial institution
- Ask you to login to "reset" or "revalidate" your account
- Often claim that your account has been suspended

A Phish


```
From: no-reply@flagstarbanking2.com
To: undisclosed-recipients:;
Subject: YOUR ACCOUNT HAS BEEN SUSPENDED !!!
Date: Fri, 29 Sep 2006 09:29:25 -0500

...

If you fail to provide information about your
account you'll discover that your account has been
automatically deleted from Flagstar Bank database.

Please click on the link below to start the update
process:

https://www.flagstar.com/Signon.cgi?update
Flagstar Bank
```

What's Wrong?

- The URL is a booby trap:

- When I clicked on it, I was actually redirected to a site in Colombia, via yet another indirection...
- The login page appears identical to the real one
- (One of the web sites I visited seemed to have several variant "bank" pages)

The Login Box

The URL Bar

They Want Data. . .

Please complete the fields below to recover account.

Required fields are in red.

First Name

Last Name

Card Number

Expiration Date 1 2006

Electronic Signature (ATM PIN)

Social Security Number (SSN)

Home Phone #

Email Address

Click here if you want to receive confirmation email.

Click here if you do not want to receive confirmation email.

Note: You will receive the confirmation email within 48 hours.

Continue

Some Mail Headers


```
Received: from plesk.salesforcefoundation.org
   ([198.87.81.9])
   by cs.columbia.edu (8.12.10/8.12.10)
   (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA
   bits=256 verify=NOT) for <smb@cs.columbia.edu>
Received: from adsl-68-20-44-198.dsl.chcgil.amerite
  (68.20.44.198) by 198.87.81.11
```

Where does `plesk.salesforcefoundation.org` come from? It is *asserted* by the far side. The `198.87.81.9` is derived from the IP header, and is hard to forge (but stay tuned for routing attacks, in a few weeks). A DNS lookup on `198.87.81.9` isn't very helpful; the mapping is controlled by the address owner, not the name owner.

Other Issues

- Why is the email from `flagstarbanking2.com`?
- The domain for the bank is `flagstar.com` — no "ing" and no "2".
- *That's legit!* — the real web site for their online service is `flagstarbanking2.com`
- We have trained users to accept weird, seemingly gratuitous differences; it can make life easier for the phisher

Tricks with URLs

- `http://cnn.com@some.other.site/foo`
  `cnn.com` is a userid
- `http://2151288839/foo`
  2151288839 is 128.58.16.7, `cluster.cs.columbia.edu`
- `http://rds.yahoo.com/_ylt=A0g...http%3a/`
  So the search engine knows what you clicked on

Defenses Against Phishing

Why Does Phishing Work?

- Lack of mutual authentication
- Reusable credentials
- Human factors

Mutual Authentication

- Users are typing passwords to the wrong site
- The browser never authenticates the site:
  - The phishing connection may not be SSL-protected at all
  - It may be the wrong site
  - It may be a deceptive site (`paypa1.com`)
  - It isn't the site the user *intended*

Examples of Server Authentication

- Certificate (but we've talked about the limitations of that approach)
- Personalization (user-supplied image, for example)
- Others?

DKIM — Domain-Key Identified Mail

- Another way to sign email
- Keys are stored in the DNS, rather than in certificates
- (How is the DNS protected? Must use DNSSEC — digitally-signed DNS records)
- Keys are domain-granularity, but can be delegated to individual users

Reusable Credentials

- The purpose of a phishing site is to collect passwords that can be used by the bad guys
- What if there were no passwords?

Non-Reusable Credentials

- Client-side certificates (more accurately, private keys)
- Challenge/response devices
- SecurID tokens and the like
- Many other forms

One-Time Credentials Won't Suffice

- What about man-in-the-middle attacks?
- Phishing site relays authentication from the client to the server; when you're logged in, it takes over
- These are already occurring in the wild

Human Factors

- How can a browser *reliably* tell the user they're at the wrong site?
- Most users don't even notice the pale yellow URL bar for SSL-protected connections
- Users are accustomed to frequent web site redesigns, including changes in authentication style
- We need to co-ordinate behavior of the user, the mailer, and the browser
- How does the user *know* that the link in the email is correct?

Final Thoughts on Phishing

- We have the basic technical mechanisms to authenticate email and web sites
- Human interaction with these mechanisms remains a very challenging problem
- Security is a *systems problem*

IPsec

What is IPsec?

- Network-layer security protocol for the Internet.
- Completely transparent to applications.
- Generally must modify protocol stack or kernel; out of reach of application writers or users.

History

SP3 Layer 3 security protocol for SDNS.

NLSP OSIfied version of SP3, with an incomprehensible spec.

swIPe UNIX implementation by Ioannidis and Blaze.

IPsec Many years of design in the IETF
Revised recently

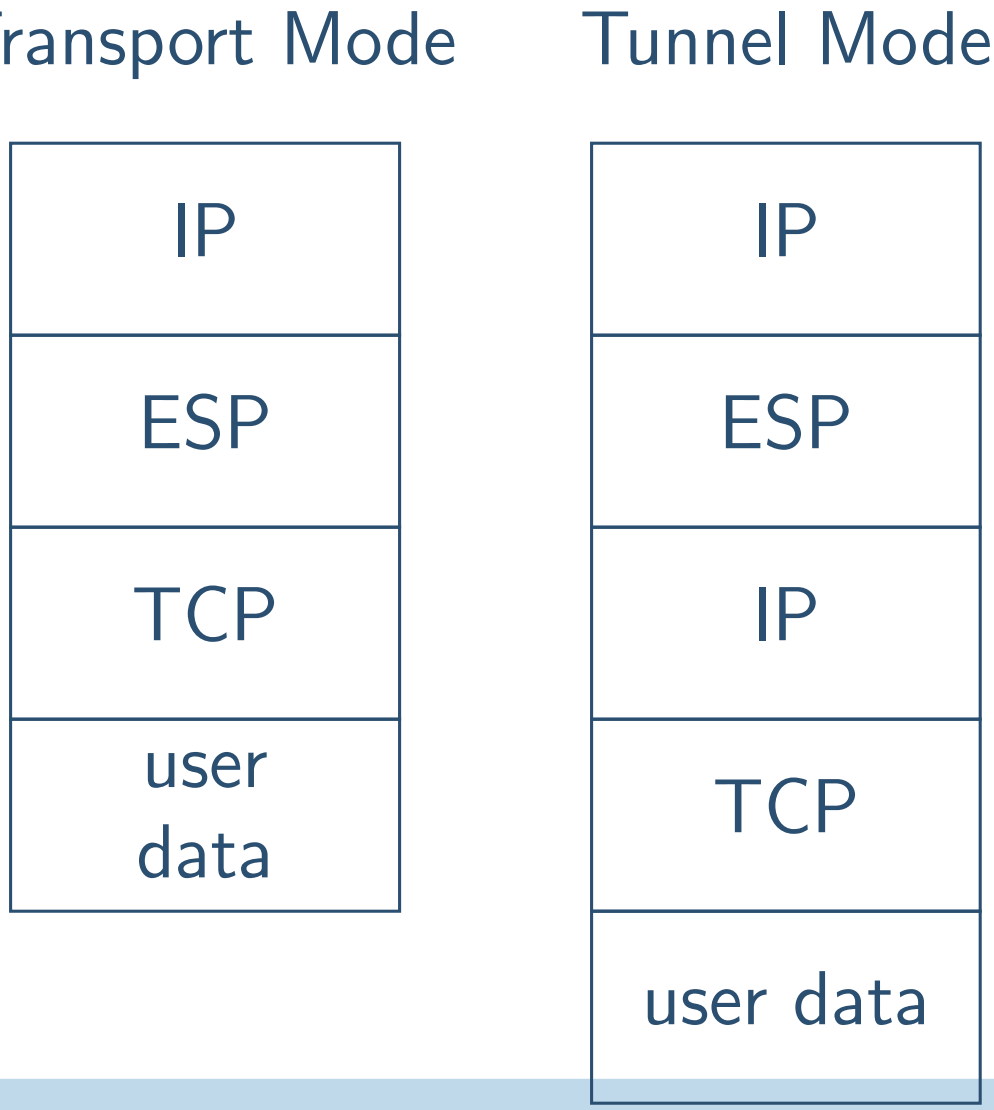
Why IPsec?

- SSL doesn't protected against certain attacks
- Example: enemy sends forged packet with RST bit set; tears down connection
- Example: enemy sends bogus data for connection — SSL detects that, but can't recover, since TCP has accepted the data
- Also — SSL can't (easily) protect UDP

IPsec Structure

- Nested headers: IP, ESP, AH, maybe another IP, TCP or UDP, then data.
- Cryptographic protection can be host to host, host to firewall, or firewall to firewall.
- Option for user-granularity keying.
- Works with IPv4 and IPv6.

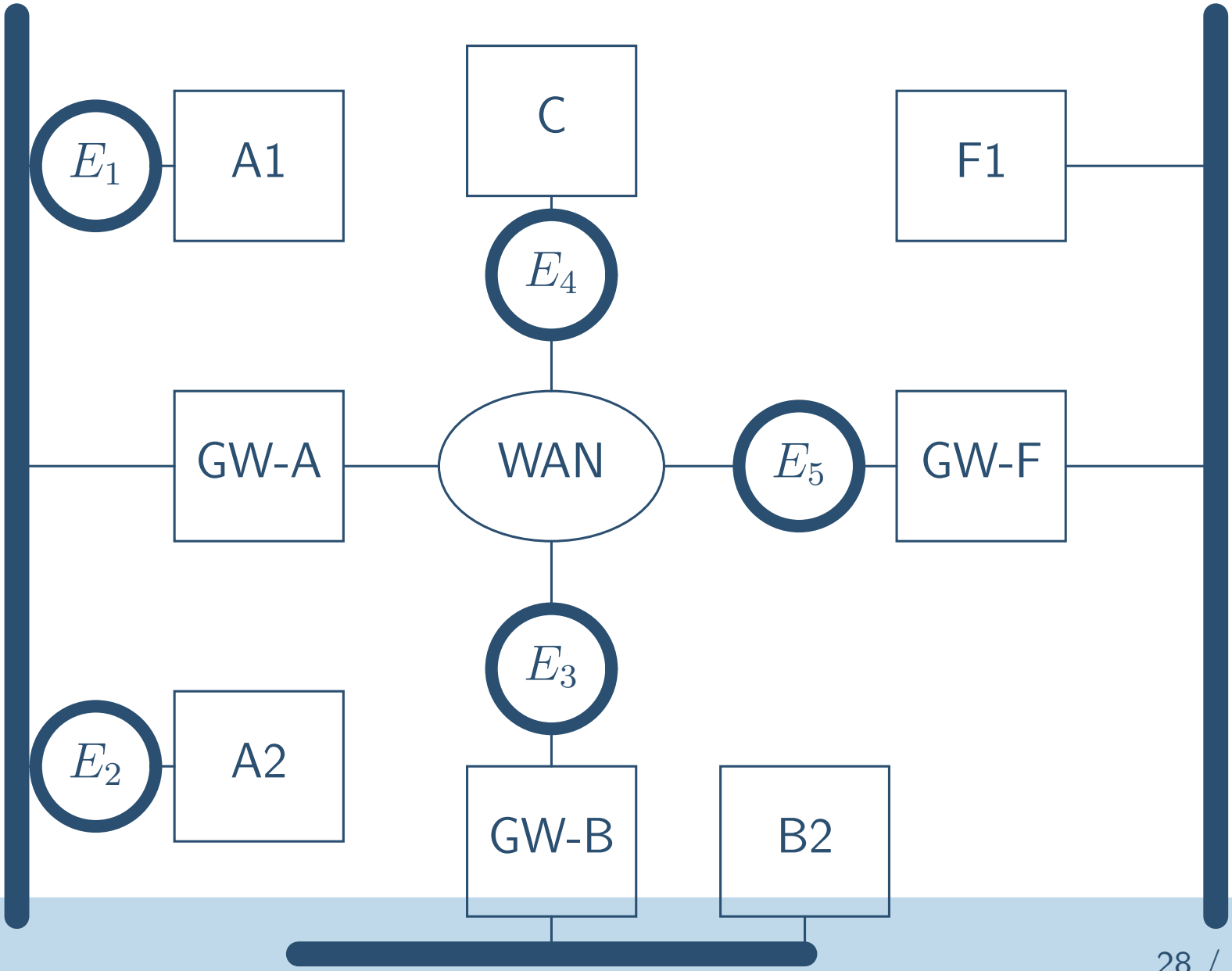
Some Packet Layouts



Tunnel and Transport Mode

- Transport mode protects end-to-end connections
- Tunnel mode — much more common — is used for VPNs and telecommuter-to-firewwall
- The inner IP header can have site-local addresses

Topologies



Paths

- A1 to F1:
  Encryptors E_1, E_5
- B2 to F1:
  Encryptors E_3, E_5
- A2 to C:
  Encryptors E_2, E_4

Uses for IPsec

- Virtual Private Networks.
- "Phone home" for laptops, telecommuters.
- General Internet security?

Outbound Packet Processing

- Compare packet — src and dst addr, src and dst port numbers — against *Security Policy Database* (SPD)
- If packet should be protected, consult *Security Association Database* (SADB) to find SA
- Add appropriate IPsec header

Inbound Packet Processing

- If IPsec-protected, look up SA, authenticate, and decrypt
- Compare packet — src and dst addr, src and dst port numbers, as before — against SPD to see if it *should* have been protected, and by which SA
- If the protection characteristics match, accept the packet
- If they do not match, discard it

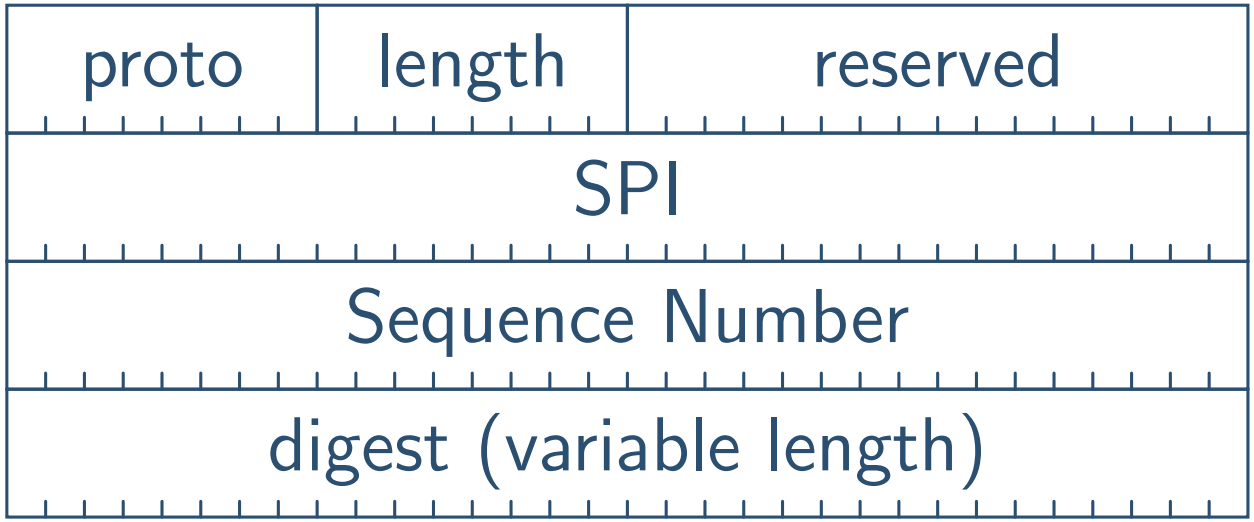
Typical Rule Characteristics

- IP address range or subnet: protect everything going to 128.59.0.0/16
- Port number list or range: 25,110,143
- Protect all addresses and/or all port numbers: full protection

Authentication Header (AH)

- Based on keyed cryptographic hash function.
- Covers payload and portion of preceeding IP header.
- Not that useful today, compared to ESP with null authentication

AH Layout



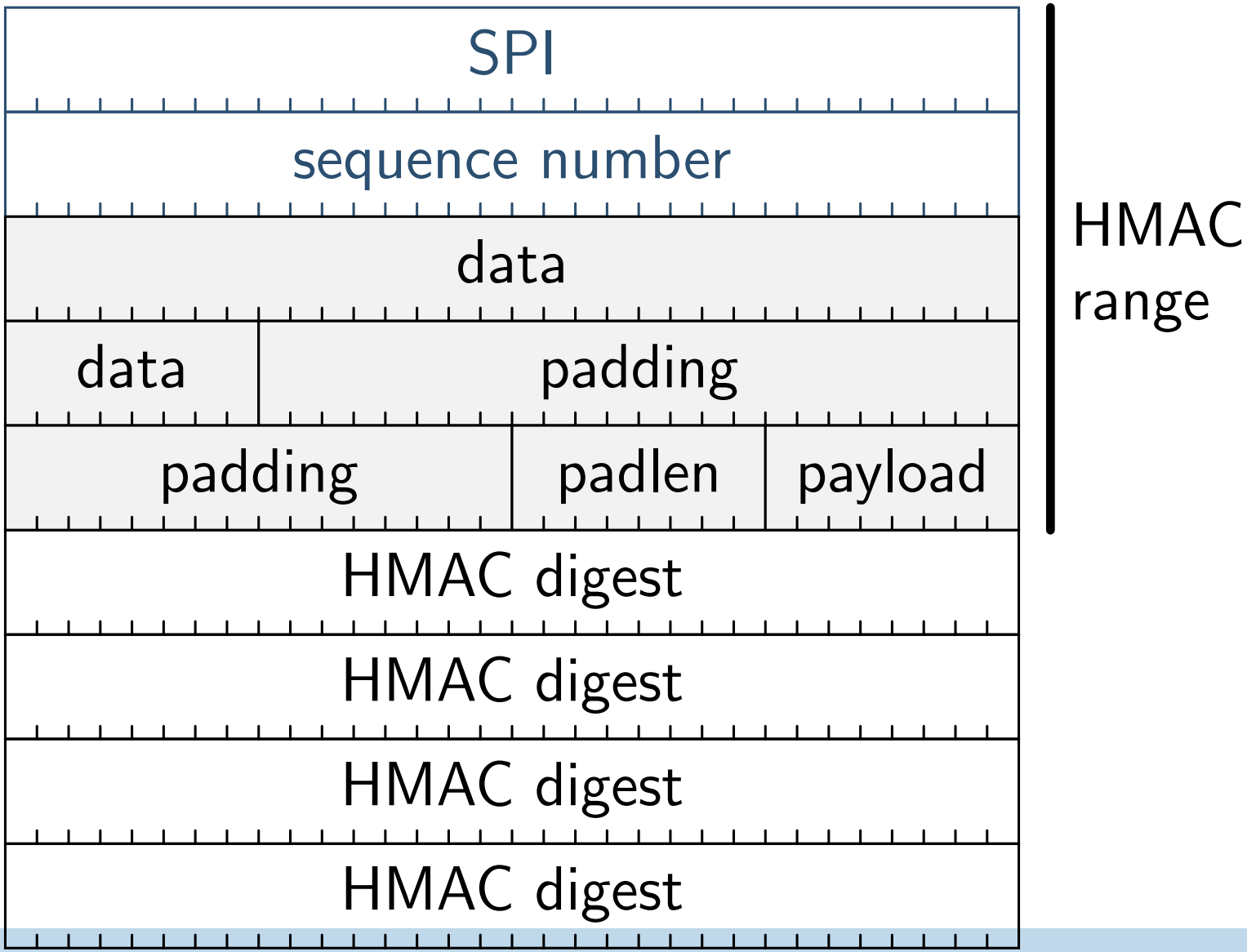
What is an SPI?

- SPI — Security Parameter Index
- Identifies *Security Association*
- Each SA has its own keys, algorithms, policy rules
- On packet receipt, look up SA from ⟨SPI, dstaddr⟩ pair

Encapsulating Security Payload (ESP)

- Carries encrypted packet.
- An SPI is used, as with AH.
- Preferred use of ESP is for AES in CBC mode with HMAC-SHA1

ESP Layout



Using ESP

- Can be used with null authentication or null encryption
- With null encryption, provides authentication only
- Easier to implement than AH

IPsec and Firewalls

- Encryption is not authentication or authorization
- Access controls may need to be applied to encrypted traffic, depending on the source.
- The source IP address is only authenticated if it is somehow bound to the certificate.
- Encrypted traffic can use a different firewall; however, co-ordination of policies may be needed.

IPsec and the DNS

- IPsec often relies on the DNS.
  - Users specify hostnames.
  - IPsec operates at the IP layer, where IP addresses are used.
  - An attacker could try to subvert the mapping.
- DNSSEC may not meet some organizational security standards.
- DNSSEC — which isn't deployed yet, either — uses its own certificates, not X.509.

CS@CU

Implementation Issues

- How do applications request cryptographic protection? How do they verify its existence?
- How do adminstrators mandate cryptography between host or network pairs?
- We need to resolve authorization issues.