Last time...

- “Content distribution networks are beneficial for both content providers and clients in terms of performance and reliability.”
  - Overcome first-mile and peering point bottlenecks
  - Tricky problems: cache coherency, redirection

Questions from last time...

- Doesn’t this defeat the purpose of DNS caching?
  - Yes – we have to use short timeouts.
- What about dynamic content?
  - Yup, CDNs don’t help here.
- How do CDNs load balance a flash crowd to a single URL?
  - Cache Array Routing Protocol (p. 702-3)
- Who decides who participates in an overlay network?
  - The administrator, or the overlay nodes themselves

Last few weeks...

- Growth & evolution: How do we cope as networks grow and evolve over time?
- Interdomain routing: hierarchy and policy
- Addressing: structural hierarchy
- DNS: hierarchy and caching
- CDNs: caching, network and data locality
- Overlays: deploying new behaviors in a subset of the Internet
This week…

• Cooperation and competition: How do we manage differing interests?

• Topics:
  – Fairness of resource allocation
  – Transit and peering
  – Incentives for providing services:
    Multicast, QoS, CDNs…
  – Network security

Network Security

• What do you think network security is about?
What do we mean by “security”?

• Networks are fundamentally shared
  – Many parties handle your messages!

• Privacy: Messages can’t be
• Integrity: Messages can’t be
• Authenticity: Messages can’t be

• These are in addition to…
  – Protecting networked systems from compromise
  – Ensuring services are available to legitimate users

Approaches at 10,000 feet

• Physical security
• Security through obscurity
• Throw math at the problem

Why is security difficult?

• It’s a negative goal.

• Assumptions may turn out to be invalid.

• It depends on the behavior of people.

Basic Encryption for Privacy

• Cryptographer chooses functions E(), D() and keys $K^E$, $K^D$
• Cryptanalyst “attacks” the system by trying to figure out the keys
  – What does the attacker know?
Secret Key Encryption (DES, IDEA)

- a.k.a. “shared key” or “symmetric key”
- Single key is shared between parties
  - Used for both encryption and decryption
  - Often chosen randomly, but must be communicated

Plaintext → Encrypt with secret key → Ciphertext
Ciphertext → Decrypt with secret key → Plaintext

DES: Block encryption

Each Round:
- Initial permutation
- 56-bit key
- Final permutation

DES uses a 64 bit key (56 + 8)
Message encrypted in 64 bit blocks
16 rounds to encrypt each block

DES: Cipher block chaining

- Chain together blocks in longer messages by XORing ciphertext with plaintext

Public Key Functions (RSA)

- Public and private key are mathematically related
  - Public key is published
  - Private is a secret
Public Key Encryption (2)

- Start with large prime numbers $p$ and $q$
- Choose encryption key $e$ so that $e$ and $(p-1)(q-1)$ are relatively prime
- Set decryption key $d = e^{-1} \mod ((p-1)(q-1))$

- Public key: $<e, n>$
  - Encrypt with $c = me \mod n$
- Private key: $<d, n>$
  - Decrypt with $m = c^d \mod n$

Authentication Protocols

- Three-way handshake for mutual authentication

```
Client    Server
ClientId, E(x, CHK)  
E(y + 1, CHK)  
E(SK, SHK)  
E(x + 1, SHK), E(y, SHK)
```

Authenticity and Integrity

- Sometimes we want to know a message is authentic, but don’t care if it’s private.
- With public key encryption (RSA) for privacy…
  - Anyone with my public key can send me a confidential message
  - So I can’t be sure who sent the message!

RSA Digital Signature

- Only one person can send this message…
- …But anyone who knows the public key can check the authenticity.
A Faster “RSA Signature”

- Encryption can be very slow, e.g., RSA is ~1Kbps
- Let’s just encrypt just the message checksum instead!
  - Faster to compute a checksum and encrypt it than to encrypt entire message
- Problem: Easy to alter data without altering checksum

Message Digests (MD5, SHA)

- Cryptographic checksum or hash
  - Typically small compared to message (MD5 128 bits)
  - “One-way”: infeasible to find two messages with same digest

Cryptography in Protocols

- These techniques can be applied at different levels:
  - IP packets (IPSEC)
  - Web transfers or other transports (SSL/TLS, Secure HTTP)
  - Email (PGP)
- More on this next time…

Key Concepts

- Security properties: privacy, integrity, and authenticity
- Cryptographic mechanisms are used to support these properties
  - Secret key encryption
  - Public key encryption
  - Message digests