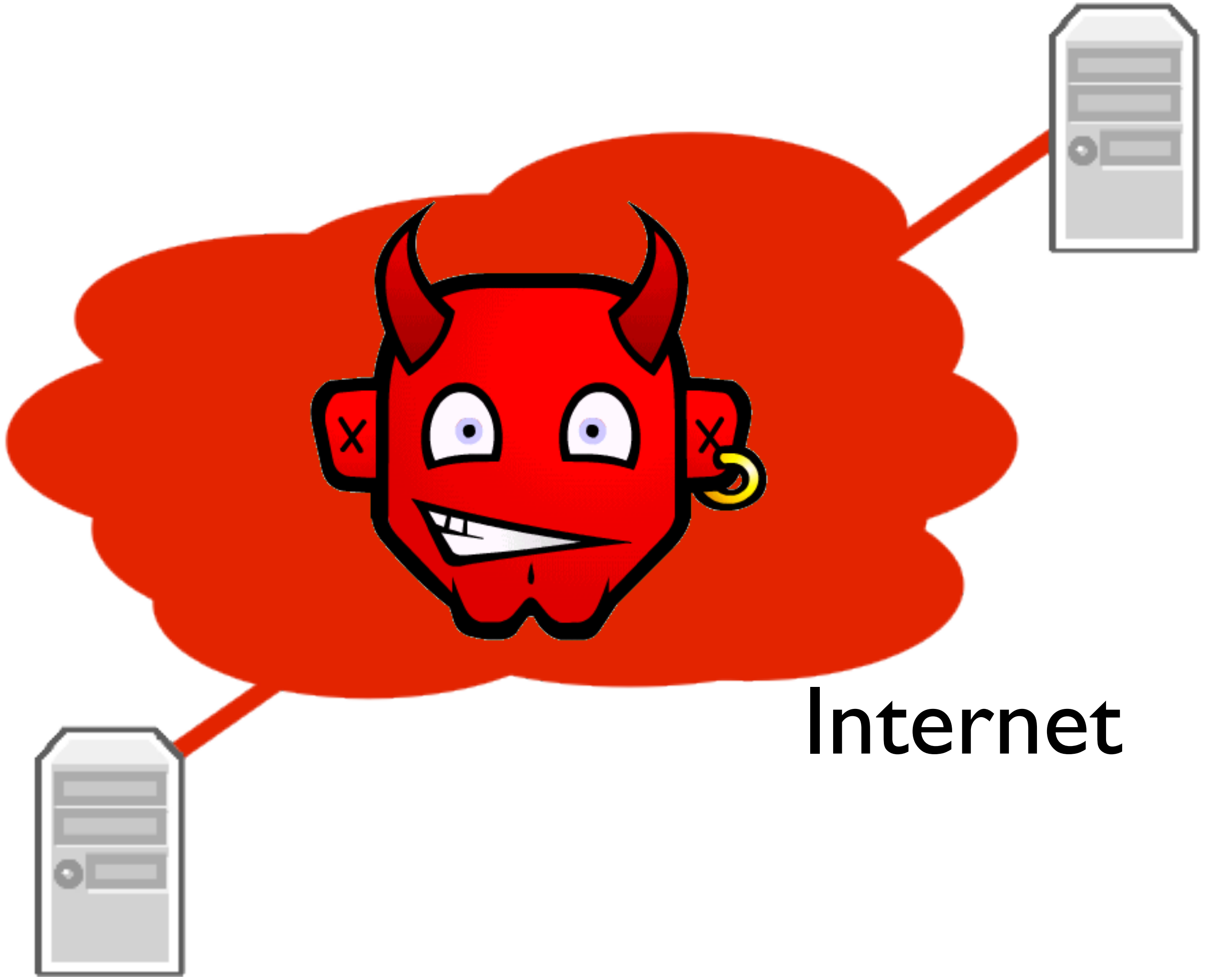
CS144
An Introduction to Computer Networks

Unit 8: Security

The Problem



http://commons.wikimedia.org/wiki/File:Devil_cartoon_charactor.gif

What you learned: Attacks

Eavesdropping, tampering, suppression

Spoofing, man-in-the-middle

Redirection/hijacking at layers 2, 3, and 4

Denial of service

What you learned: Principles

Confidentiality

Integrity

Authenticity

What you learned: Tools

Block ciphers (EBC mode, CBC mode)

Cryptographic hashes: *collision resistance*

Message authentication codes

Public key encryption/decryption

Signatures and certificates

Most Important Lesson

It’s easy to make a mistake.

Use existing, open source implementations.

Be careful and follow best practices.