CS144
An Introduction to Computer Networks

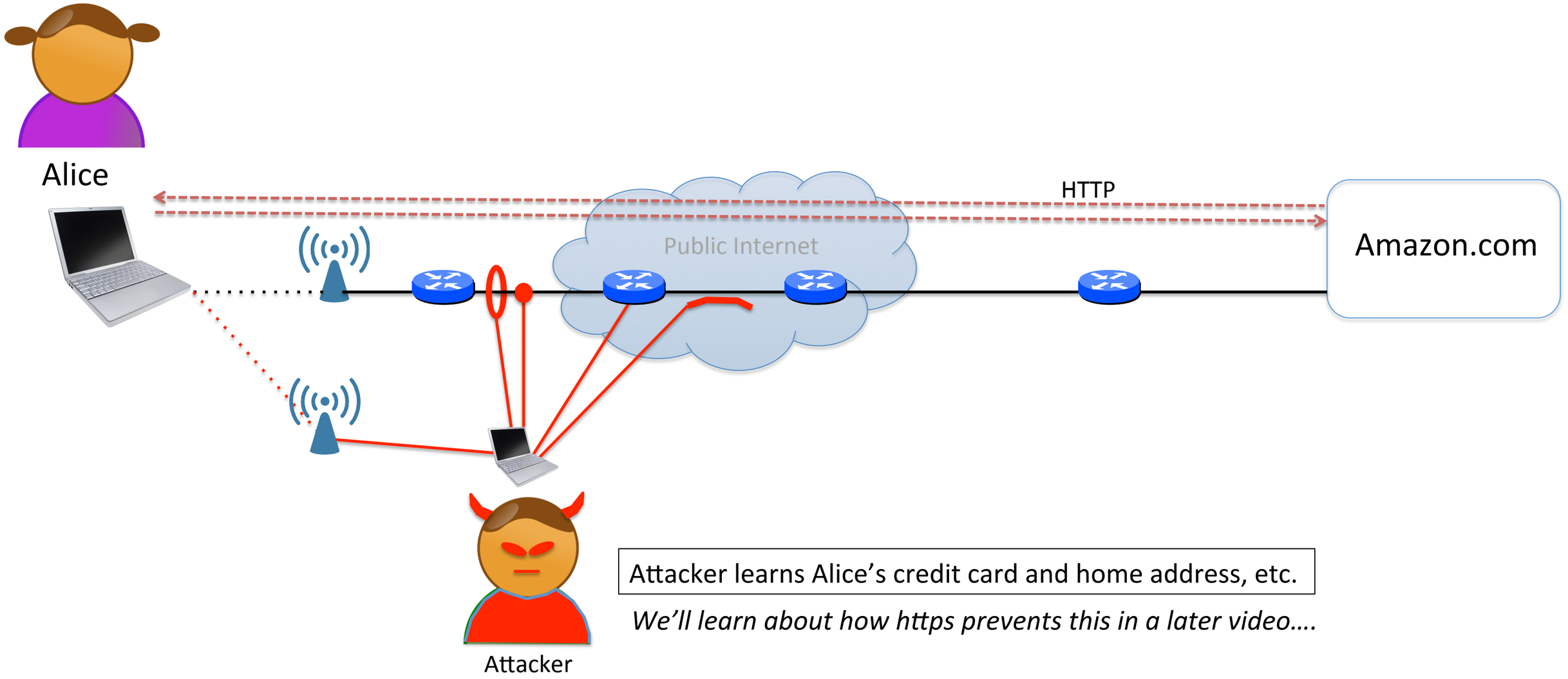
Network Security

Nick McKeown
Professor of Electrical Engineering
and Computer Science, Stanford University

How can communication be compromised?

1. **Eavesdrop** – Passively "sniff" and record network data (or metadata). For example:
   - Passively tap an electrical or optical cable.
   - Listen to WiFi (as we did in class, using Wireshark).
   - Compromise a router to duplicate and forward data.
2. **Modify, delete, insert** – Actively tamper with our data by:
   - Changing contents of packets.
   - Redirect packets to another server.
   - Take over control of an end-host.
3. **Prevent communication** – Usually called "denial of service".

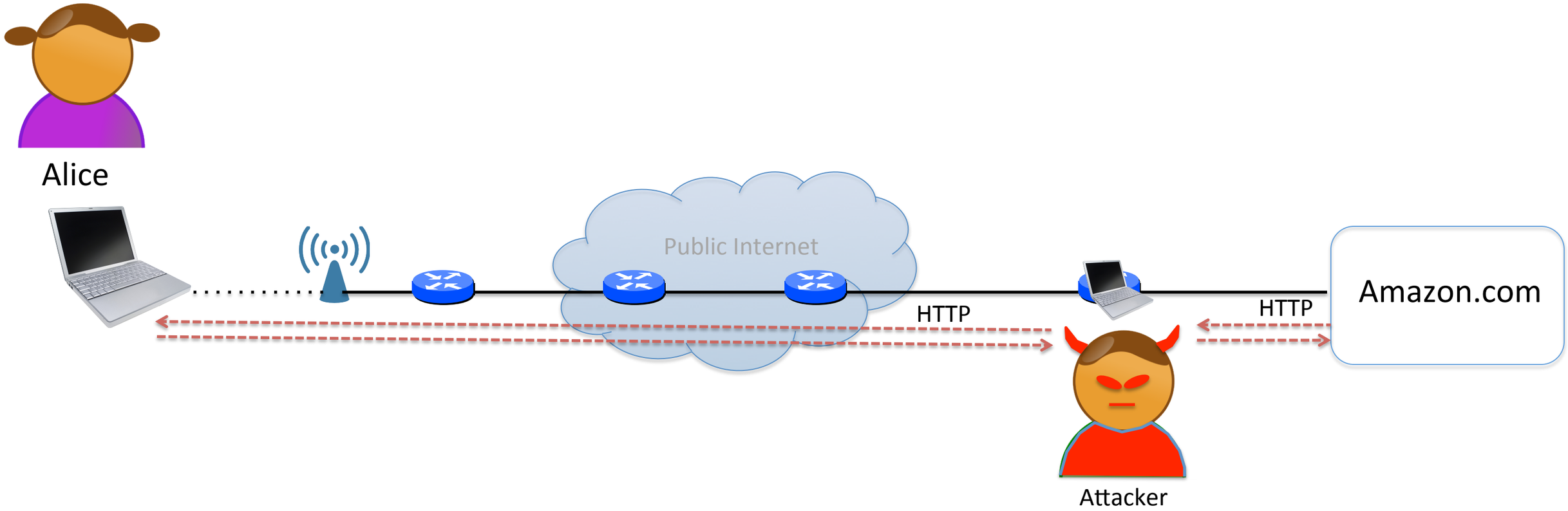
An example: Eavesdropping



Attacker learns Alice's credit card and home address, etc.

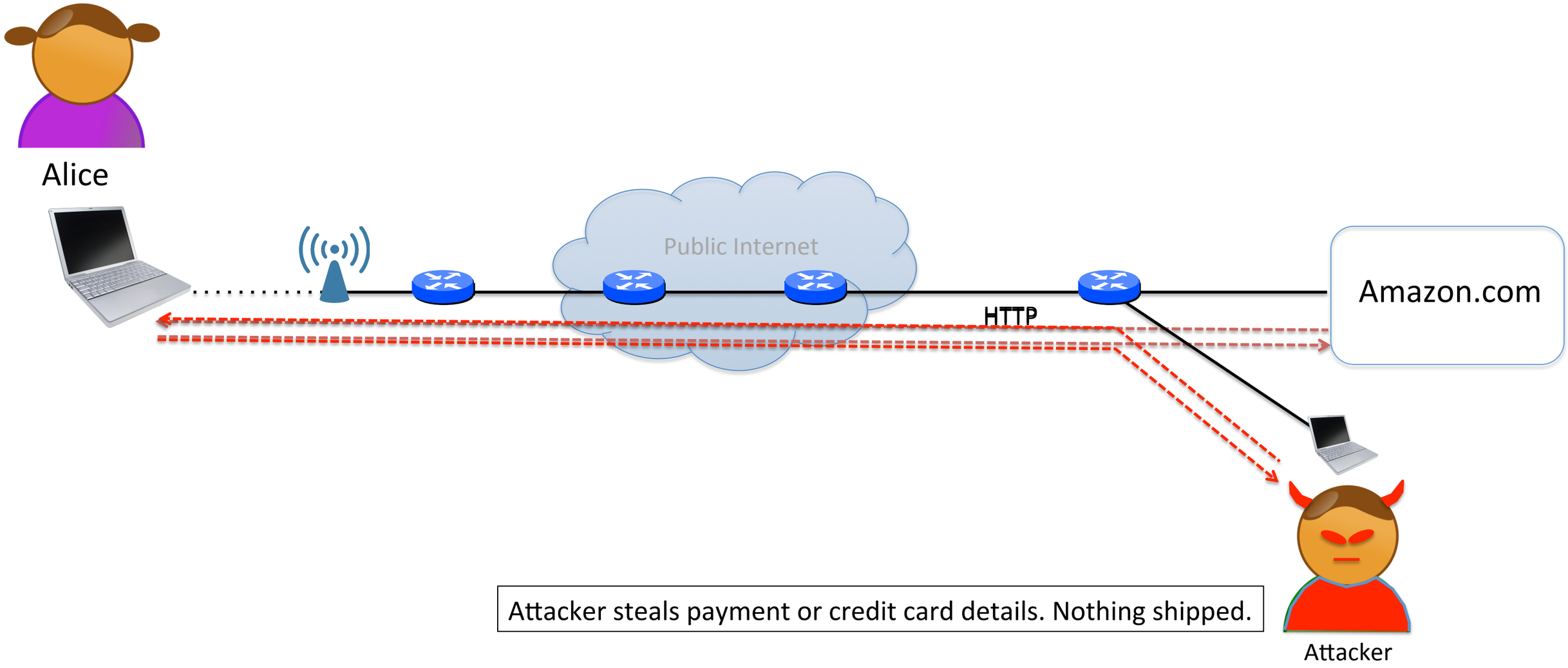
We'll learn about how https prevents this in a later video….

An example: Man-in-the-middle



Attacker changes shipping address, or prevents communication.

An example: Routing redirection



What we want

1. **Secrecy/confidentiality:** No one can listen-in to our communication. We will study encryption.
2. **Integrity** – Our messages are not altered in transit. We will study message authentication codes (MACs).
3. **Authentication –** Confirm the identity of the other party. We will study digital signatures and certificates.
4. **Uninterrupted communication** – We don't want someone to prevent us from communicating.

Types of attack

In the next few videos we will study different types of attack

1. Eavesdropping.
2. Redirecting Ethernet, IP and DNS traffic.
3. Hijacking a running TCP connection.
4. Denial of service.

<The End>