Internet II

Priorities in Internet Communication

Slides with “*” are not testable material

Question: What do we care about in regards to secure communication over the internet?

Aspects of Internet Communication Security

- **Reliability**: Ensure that information arrives uncorrupted
- **Confidentiality**: Ensure only the intended reader can read the message
- **Integrity**: Ensure that the message delivered is not manipulated or changed
- **Authenticity**: Ensure that you are communicating with the desired party

Compromised Reliability?

DDoS (Compromised Reliability)

- Goal: Cut off communication between Alice and Bob
- Packet delays limit how much information can be transferred
- Too much communication leads to a Denial of Service
  - Think of a traffic jam!
- https://www.youtube.com/watch?v=OhA9PAfkJ10
- Attack Map: bit.ly/1b7EYDk
- Question: How can we protect against this?

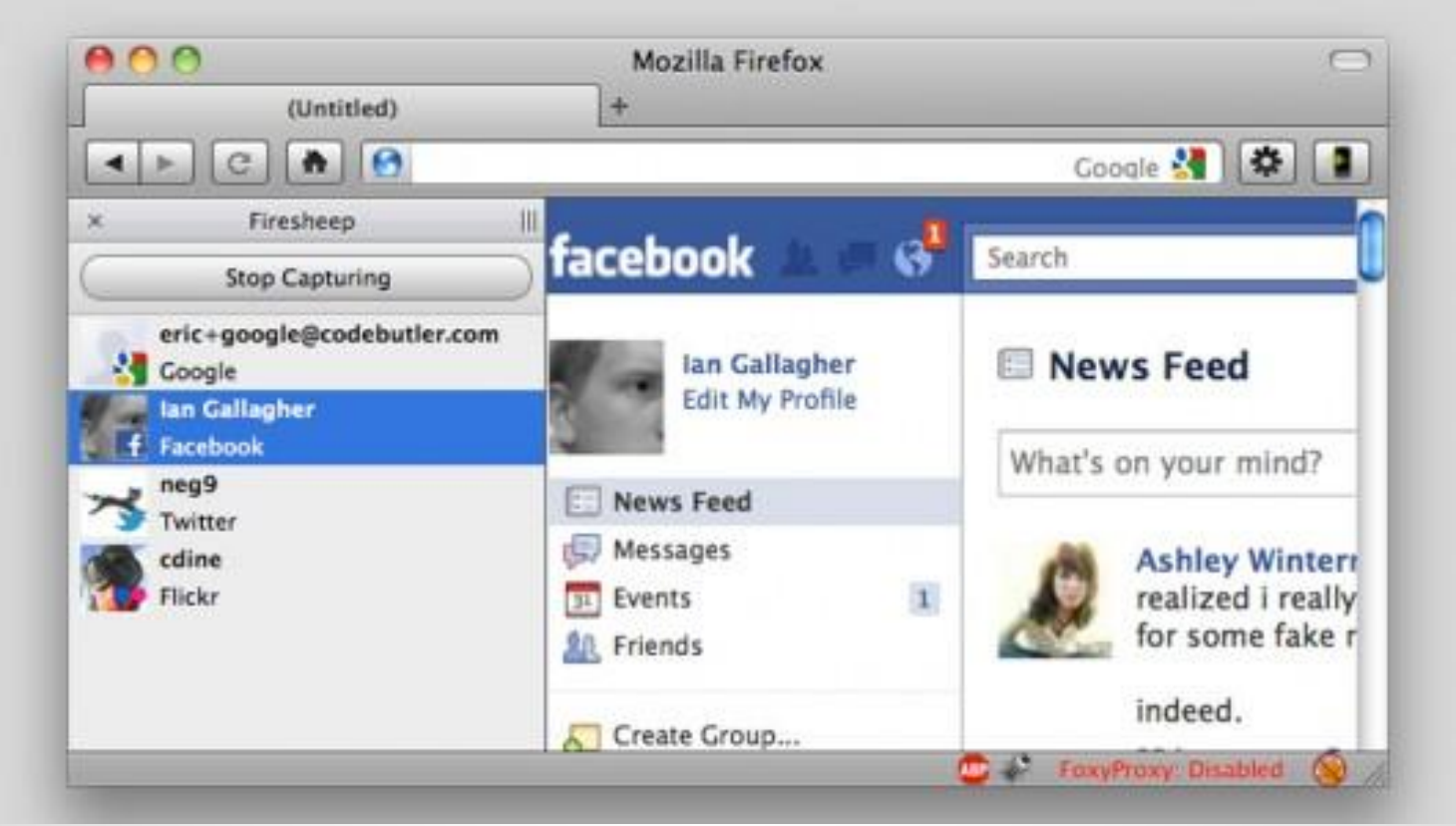
Use More Servers!*

- Use scalable server resources which allow you to use more servers only when you need them

Compromised Confidentiality?

Eavesdropping*

- Remember how many “hops” we saw in TraceRoute
- Each of these computer’s along the path sees this internet traffic
- http://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html



Firesheep allows a user to see all unprotected communication on a network. This included sending passwords and financial data!

Eavesdropping*

- Remember how many “hops” we saw in TraceRoute
- Each of these computer’s along the path sees this internet traffic
- http://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html
- **Question: How can we protect against this type of attack?**

Encryption

We can protect our information by encoding our traffic with a special key that only lets the owner of that key read the message.

Look for 

in the URL before entering passwords or any other information you want kept private.

Compromised Integrity?

Data Modification (Compromised Integrity)*

- Alice wants to make a deposit in Bob's Bank Account by sending the amount and Bob's bank account to the bank website
- Eve as usual has access to all communication between Alice and Bob
- Eve can intercept and change the account number from Bob's to her own!
- http://money.cnn.com/2013/10/28/technology/barack-obama-twitter-hack/
- Question: How can we protect against this?

Encryption!

- Again encryption can help by making it impossible for Eve to know what part of the message to modify

Compromised Authenticity?

Spoof!*

- As an attacker, we can alter communication to act as someone else
- http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
- How can we ever know that the person we are communicating with is really them?
- Question: How could you try to protect against an attack like this?

Key Signing Parties! (Extreme example) *

- Authenticity is a very difficult aspect to ensure and some go to great lengths to achieve it
- At key signing parties participants exchange encryption information in person.