MORE TLS
Threat Model

• Passive Attacks
• Active Attacks
A. Opportunistic Encryption
Fixing Passive Attacks is Easy.

1. Encrypt
2. Don’t authenticate the server
3. Don’t worry about downgrade attacks
4. Don’t tell anyone anything has changed
5. We’re done
Deploying Opportunistic Encryption

• Easy!
  • Can use anonymous cipher
  • Can just ignore the cert (e.g., self-signed)
Observation:

THIS MAKES SOME PEOPLE VERY UNCOMFORTABLE
1. Creating Confusion about Security
2. Discouraging “full fat” Encryption
3. Encouraging Active Attacks
4. TLS is to server authentication as peanut butter is to jelly.
Threat Model

- Passive Attacks
- Active Attacks?
B. Opportunistic Encryption with Server Authentication
Opp Encryption w/ Server Auth

- Protects against MITM
- EXCEPT for downgrade attack
- Might be mitigated with a pinning-like solution (?)
Observation:

THIS MAKES SOME PEOPLE VERY UNCOMFORTABLE
1. Barrier to Deployment
2. “Perfect” is the Enemy of the Good
3. Might as well do...
C. TLS Everywhere
Deploying TLS Everywhere

- Protocol-Specific; e.g., for HTTP, it would mean:
  - Only supporting HTTP/2.0 for HTTPS URIs
  - Combining with HSTS to mitigate downgrade attack
Observation:

THIS MAKES SOME PEOPLE VERY UNCOMFORTABLE
1. Cost / Overhead
2. Disempowers Intermediaries
3. Fragmentation
What We Should Focus On

1. Threat Model
2. Tradeoffs
3. Perceptions of Security