The Threat of Pervasive Surveillance

- Eavesdropping every packet on every wire
  - Unencrypted? → Payload analysis
  - Encrypted? → Metadata analysis
  - Fingerprinting and association
- Compromise of intermediate systems
- Compromise of cryptographic protocols
- Compromise of endpoints
- Compromise beyond the endpoints

Evaluating protocol resistance: scope

- Eavesdropping every packet on every wire
  - Unencrypted? → Payload analysis
  - Encrypted? → Metadata analysis
  - Fingerprinting and association
- Compromise of intermediate systems
- ~~Compromise of cryptographic protocols~~
- ~~Compromise of endpoints~~
- ~~Compromise beyond the endpoints~~

Evaluating protocol resistance: scope

- ~~Compromise of cryptographic protocols~~
  - Best evaluated separately
- ~~Compromise of endpoints~~
  - Outside the scope of protocol design
- ~~Compromise beyond the endpoints~~
  - Very much outside the scope of protocol design