1. How common is interception?
- Unencrypted communication is (still) very common (e.g., HTTP, email, FTP, telnet, etc.)
- Conventional wisdom tells us not to send sensitive information over unencrypted channels. It does not tell us the level of danger associated with sending unencrypted info
- Interception is easy -- but is it pervasive?

Goal: Find experimental evidence of interception
- How often is unencrypted communication intercepted (and acted upon)?
- Where does interception occur?
- What types of communication (SMTP, telnet, POP3, etc.) are most often intercepted?

2. Approach: Bait the eavesdropper
Bait communications between geographically and network-wise distinct endpoints.
- Mimic real communications (e.g., email) between fictitious entities
- Baits contain unique URLs pointing to webserver that logs all requests
- If adversary accesses the URL, it will be logged, indicating interception of bait email!
- For credentials, one-time unencrypted passwords are used for bait sessions

3. Example: Email bait
- Password reset emails with one time URL sent from bait website domains to bait client email addresses
  - Emails feature valid SPF, DKIM signatures
- Domain names related to tax, finance, file sharing etc. services to attract attention
- Domain Validated SSL certificates for bait domains
- Serves scheduled maintenance webpage when visited

4. Example: Telnet bait
- Better signal-to-noise ratio than email
- We instantiated telnet honeypots at different geographical locations
- We create telnet sessions from various geographical vantage points and ASes using VPN and Tor exits
- Clients connect to telnet servers using one time credentials
- Attempts (not by us) to reconnect using one-time credentials indicate eavesdropping

5. Status and Future Plans
5 telnet servers:
- 2 in US, 1 each in Russia, Brazil and Netherlands
- 10 clients connecting over 800 VPN endpoints plus permitting Tor exit nodes

Future plans:
- Expand the number of servers and clients
- Set up more bait services
- Examine one hop proxies providing TLS proxying