TDC 375 – Network Protocols
TDC 563 – P&T for Data Networks

X.509 Certificate Insight & Probing
Lightning Talk
Goals

• Obtaining X.509 certificates in use in the wild
• Store results in an easily maintained database
• Utilize database for various “insight” scenarios
Scanning strategy

• You could use something like nmap/zmap
• custom code and solutions
  • two-stage SYN scan with follow up app check
  • passive certificate extraction
• How do you probe the entire Internet?
• Do you white list prefixes?
• Responding to and limiting complaints
X.509 certificate properties

- Time stamps
  - Discovery time, valid/expiry times
  - Address, port
  - Certificate in PEM format
  - Serial, version, hash signature
  - Issuer detail
  - User detail (subject, organization, email etc)
Insight ideas

- Subject and Alt host names
- Email addresses
- Expiry times
- Algorithms used
- Duplicate certificates
- Patterns of certificates used by common software