Metadata

Theo Baschak

CryptoParty

Online HTML5 Slides

Presentation source/download available at
github.com/tbaschak/cryptoparty-metadata

Who I Am

- Primary Network Administrator of VOI Network Solutions – Winnipeg-based commercial Internet Service Provider and carrier.
- Involved with both Internet Exchanges in Winnipeg.
  - Elected member on the Board of Directors for MBIX.
  - Also involved with the creation and technical operations of WpgIX.
- Avid opensource software user/fanatic, and recently, contributor.

- “Due to recent revelations. . . ” / NSA / Global Surveillance / etc
- Will be talking tonight about:
  - Metadata
  - Your traffic, on the wire
  - Encrypting your data in transit

00 00 00 01

- Expectations of data privacy are no longer absolute
  - DO NOT TRUST PLAINTEXT, be wary of weak crypto
- Many previously “only theoretical” privileged access attacks now widespread
  - MITM attacks very real
  - And profitable too

00 00 00 10

- Metadata
  - More sources closer to users gives better information
  - Traditionally 5-tupple
    - ip_proto, src_ip, src_port, dst_ip, dst_port
    - along with timestamp
    - can be combined with DNS/Geo/BGP information
    - Provides information for troubleshooting and network planning
  - Detail Time Limited
  - Usage Graphs

00 00 00 11

- So What Can Your ISP See?
- Last CryptoParty Traffic - All SSL Ports, that was all
- Is this a concern?

00 00 01 00

- Routing Attacks
  - Accidental
  - On Purpose
- Implications of routing diversions
  - Plaintext can be considered compromised
- LinkedIn ‘Intro’ Email Proxying (2013-10-23 - 2014-03-07)

00 00 01 01

- Encryption
  - Always if you want your data to be private
  - When configuring SSL, check the ciphers, there are valid options which are silly

00 00 01 11

-

Questions / End

- Question & Answer period as time permits.

Questions / End

- Question & Answer period as time permits.
- Presentation source/download available at github.com/tbaschak/cryptoparty-metadata