

# Time Synch Protocol Security Intro and Requirements

IETF 91 - Honolulu  
saag, Thu 13 Nov, 1300 HST

Karen O'Donoghue

# Overview of “stuff”

- Two time related working groups in the IETF
  - ntp and tictoc
- RFC 7384
  - Security Requirements of Time Protocols in Packet Switched Networks
- Outside the IETF
  - IEEE 1588 Security Subcommittee

# Autokey History

- Autokey (RFC 5906)
  - Provides time server authentication
  - Published as an Informational RFC
  - Implemented but not widely deployed
  - Known issues and vulnerabilities
    - [https://zero-entropy.de/autokey\\_analysis.pdf](https://zero-entropy.de/autokey_analysis.pdf)

# So for today...

- NTS Discussion Goal:
  - Solicit help
    - Review and feedback for NTS solution
- Topics we can discuss separately
  - Additional requirements we should be addressing