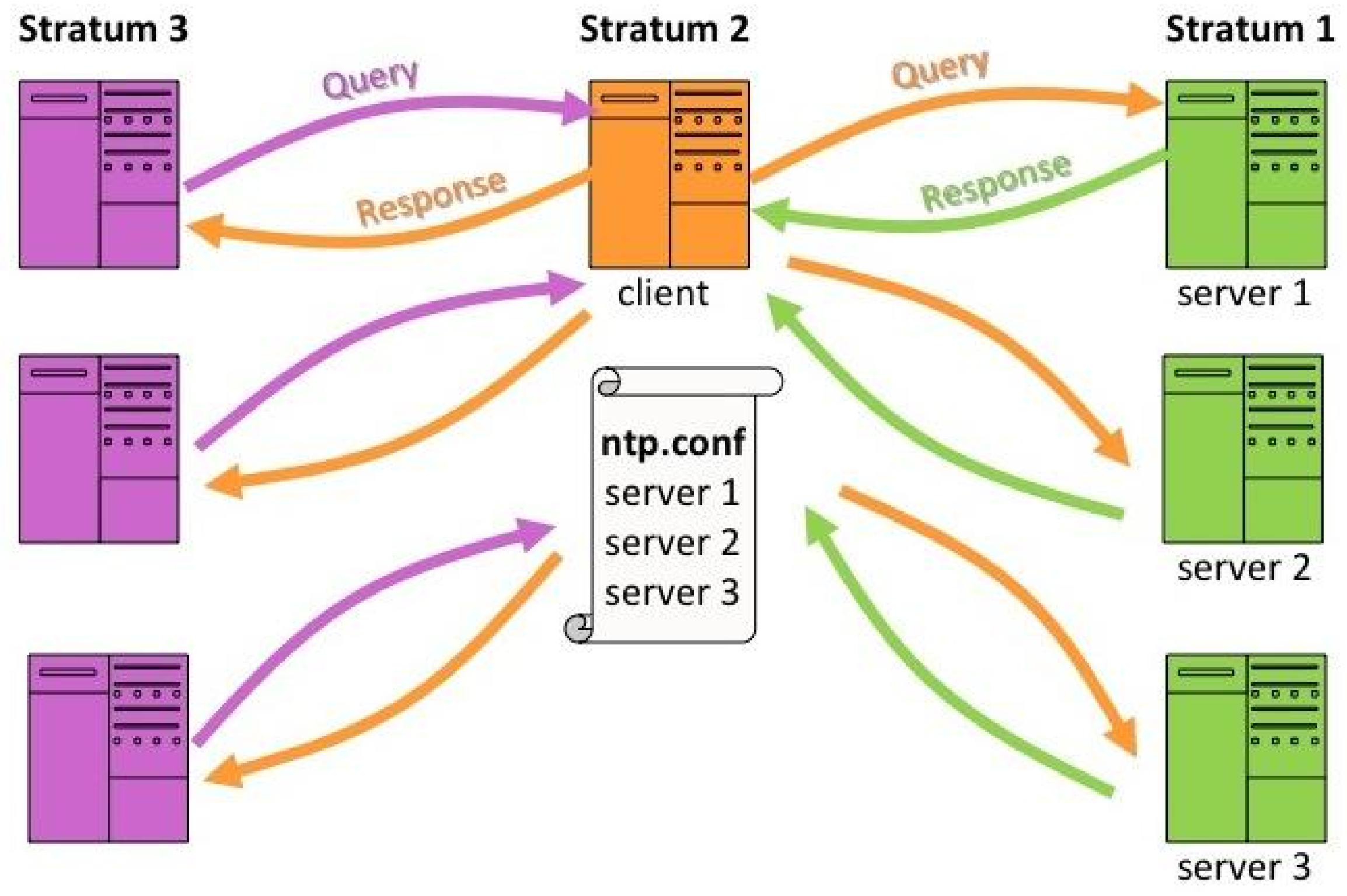
Universally Composable Network Time Protocol

Aanchal Malhotra, Oxana Poburinnaya, Ran Canetti, Kyle Hogan, Mayank Varia, Sharon Goldberg
(Boston University)

Network Time Protocol (NTP) gives time to computer systems on the Internet in a query-response fashion.



Why do we care about NTP security?

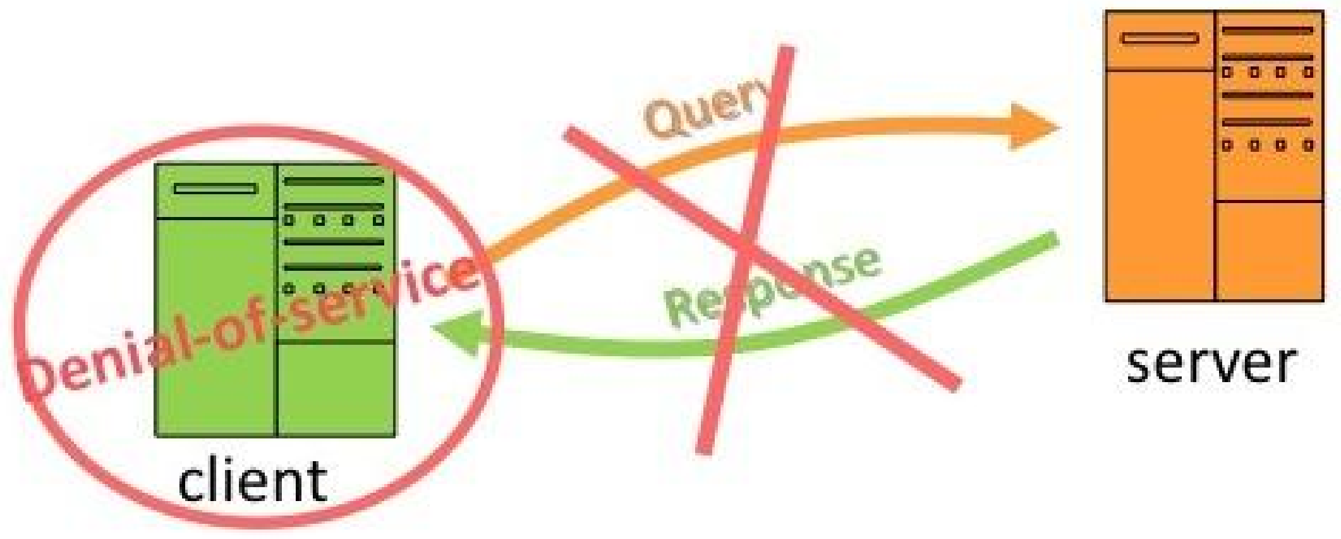
Most Internet protocols rely on PKI for security, which in turn relies on NTP security

If time goes bad, one can:

- Replay old (potentially compromised) certificates
- Expire valid certificates (potential DoS)
- Similar shenanigans for Certificate Revocation Lists

MACS Project Work on NTP security

- [1], [2] exploits protocol flaws for DoS attacks and IPv4 flaws for timeshifting attacks on NTP clients



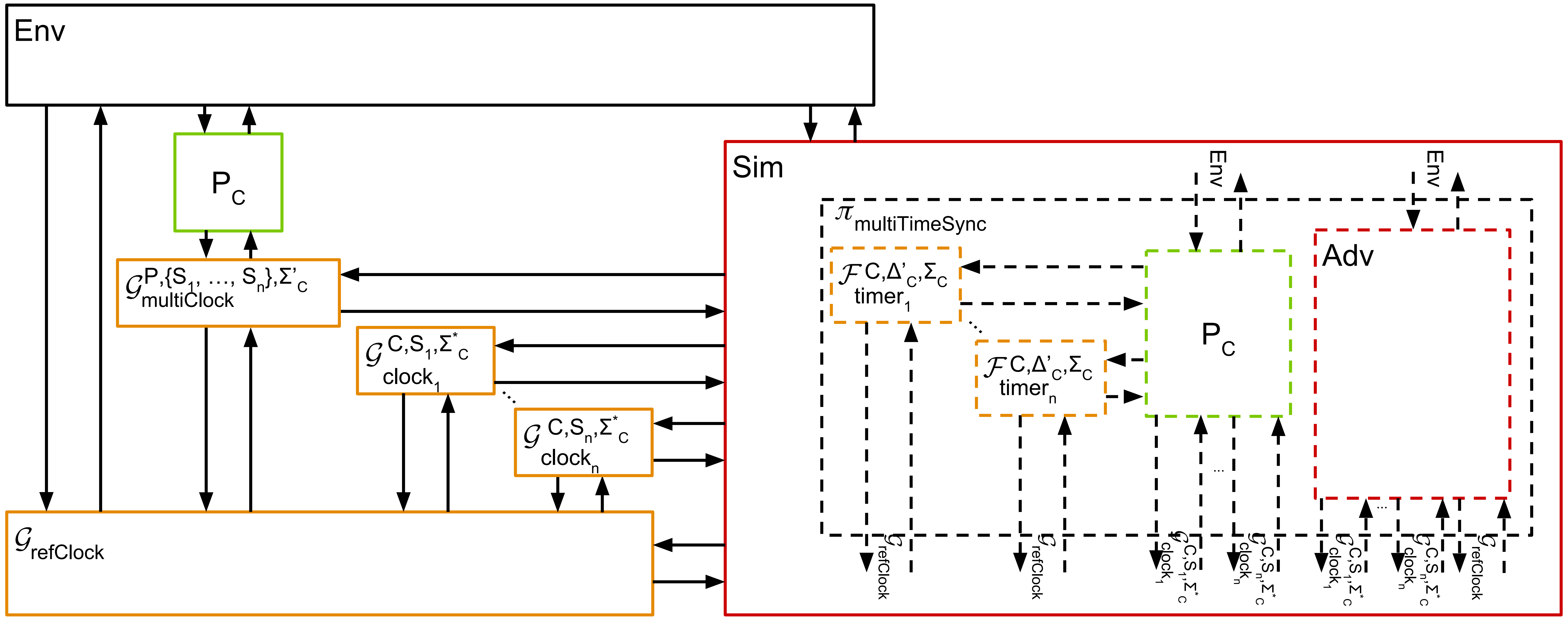
- Following work points out flaws in current protocol, proposes a new unauthenticated NTP protocol & proves its security

Our Proposed Security Model

- shows NTP security when composed with other protocols
- previous security analysis only guarantees NTP security as stand-alone protocol

Universal Composability

- provides protocol security under concurrent composition with itself or other protocols
- useful for NTP as synchronous time is important for many other protocols


Env
P_C
$\mathcal{G}^{P,\{S_1,\ldots,S_n\},\Sigma'_C}_{multiClock}$
$\mathcal{G}^{C,S_1,\Sigma^*_C}_{clock_1}$
$\mathcal{G}^{C,S_n,\Sigma^*_C}_{clock_n}$
$\mathcal{G}_{refClock}$
Sim
Env
Env
$\pi_{multiTimeSync}$
$\mathcal{F}^{C,\Delta'_C,\Sigma_C}_{timer_1}$
$\mathcal{F}^{C,\Delta'_C,\Sigma_C}_{timer_n}$
P_C
Adv
...
...
$\mathcal{G}_{refClock}$
$\mathcal{G}_{refClock}$
$\mathcal{G}^{C,S_1,\Sigma^*_C}_{clock_1}$
$\mathcal{G}^{C,S_n,\Sigma^*_C}_{clock_n}$
$\mathcal{G}^{C,S_1,\Sigma^*_C}_{clock_1}$
$\mathcal{G}^{C,S_n,\Sigma^*_C}_{clock_n}$
$\mathcal{G}_{refClock}$

Ideal Functionality $G_{MultiClock}$

- models NTP behaviour in order to provide necessary security guarantees
  - bounds the shift and drift in a party's clock from participating in the protocol
- any real world implementation of NTP that realizes this functionality provides the same guarantees.

Impact of Our Work

- **Certificate Revocation**
  - expired certificates should be kept on revocation list for at least as long as the offset that could be introduced in client's time
  - prevents a client with slow clock from being unable to tell that it had been revoked
- **New NTP Protocol**
  - unauthenticated - secure against off path attackers
  - authenticated - secure against on path attackers

References:

1. A. Malhotra, I. E. Cohen, E. Brakke, and S. Goldberg. Attacking the Network Time Protocol. In *Network and Distributed System Security Symposium* (NDSS), Feb. 2016.
2. A. Malhotra, and S. Goldberg. Attacking NTP's Authenticated Broadcast Mode. *SIGCOMM Computer Communication Review*, April 2016.