Retroactively estimating system clock skew from stored web browser cookies
1. Why?
2. Mechanism for deriving skew from cookies
3. Data & data processing
4. Demonstration of algorithm
Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.

John claims that he did no such thing and that some other person working the next shift must have been responsible.
Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed. John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32. An investigation of security camera footage shows John leaving the store premises at 10:30.
Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed.

John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32.

An investigation of security camera footage shows John leaving the store premises at 10:30.

...?
Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed. John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped **10:32**. An investigation of security camera footage shows John leaving the store premises at **10:30**.

→ *What was the skew of the PC’s clock with respect to the clock of the security camera?*
Time. It matters.

John is a suspect in a fraud case – supposedly, he has tampered with the electronic cash register (PC software) in the grocery shop where he is employed. John claims that he did no such thing and that some other person working the next shift must have been responsible.

A forensic investigation shows that the fraudulent records were timestamped 10:32. An investigation of security camera footage shows John leaving the store premises at 10:30.

→ What was the skew of the PC’s clock with respect to the clock of the security camera? Or: what were their respective skews with respect to some universal clock?
Skewed up clocks

Fig. 17 – A clock with periodic jumps (sampled hourly).

Fig. 19 – Two different hosts “sharing” an IP address?
Server time ends up on your machine

Clocks in sync

CLIENT
local clock = \textcolor{red}{13:00}

store cookie
creation time \textcolor{red}{13:00}
expiry time \textcolor{red}{14:00}\textcolor{red}{-01:00}
(difference $\Delta_C$ \textcolor{red}{01:00})

GET

SERVER
local clock = \textcolor{red}{13:00}

\textit{calculate cookie expiry}
local time 13:00
+ constant $\Delta_S$ 01:00+
\textcolor{red}{14:00}

Set-Cookie: name = value; expires = \textcolor{red}{14:00}
Server time ends up on your machine

**Client-side skew**

CLIENT (+00:10 skew)
local clock = 13:10

store cookie
creation time 13:10
expiry time 14:00-
(difference \( \Delta_c \) 00:50)

GET

SERVER
local clock = 13:00

calculate cookie expiry

local time 13:00
+ constant \( \Delta_s \) 01:00+
14:00

Set-Cookie: name = value; expires = 14:00

\( \Delta_s - \Delta_c = 00:10 \)
Acquiring server deltas

HTTP/1.0 200 OK
Server: nginx/1.2.0
Date: Fri, 21 Sep 2012 05:51:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie:
anonymid=h7cvgx1h6is4h3;
domain=.renren.com;
path=/;
expires=Wed,20-Sep-2017 05:51:57 GMT
Acquiring server deltas

HTTP/1.0 200 OK
Server: nginx/1.2.0
Date: Fri, 21 Sep 2012 05:51:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie:
anonymid=h7cvgx1h6is4h3;
domain=.renren.com;
path=/;
expires=Wed,20-Sep-2017 05:51:57 GMT

→ Shodan Research HTTP Header Survey
Acquiring server deltas

Histogram of expiry times (sanitized)

Count

Diff. between response 'Date' & cookie 'expires' log(seconds)

- 1 second
- 1 minute
- 1 hour
- 1 day
- 1 week
- 1 month
- 2 years

1 year
Demo time