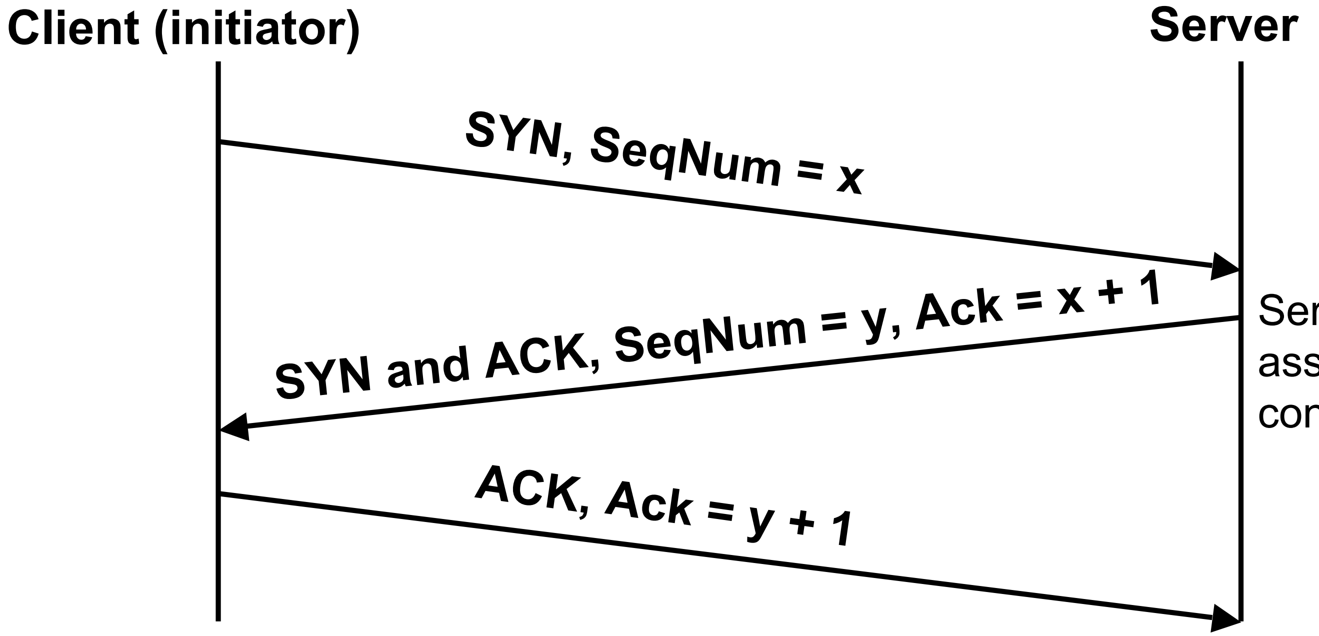
Transport-Level Denial-of-Service

- Recall TCP’s 3-way connection establishment handshake
  - Goal: agree on initial sequence numbers
  - Starting sequence numbers are ~~based on clock~~ random

to prevent attacker from guessing them to **establish** connections using spoofed source addresses



Client (initiator)

Server

SYN, SeqNum = x

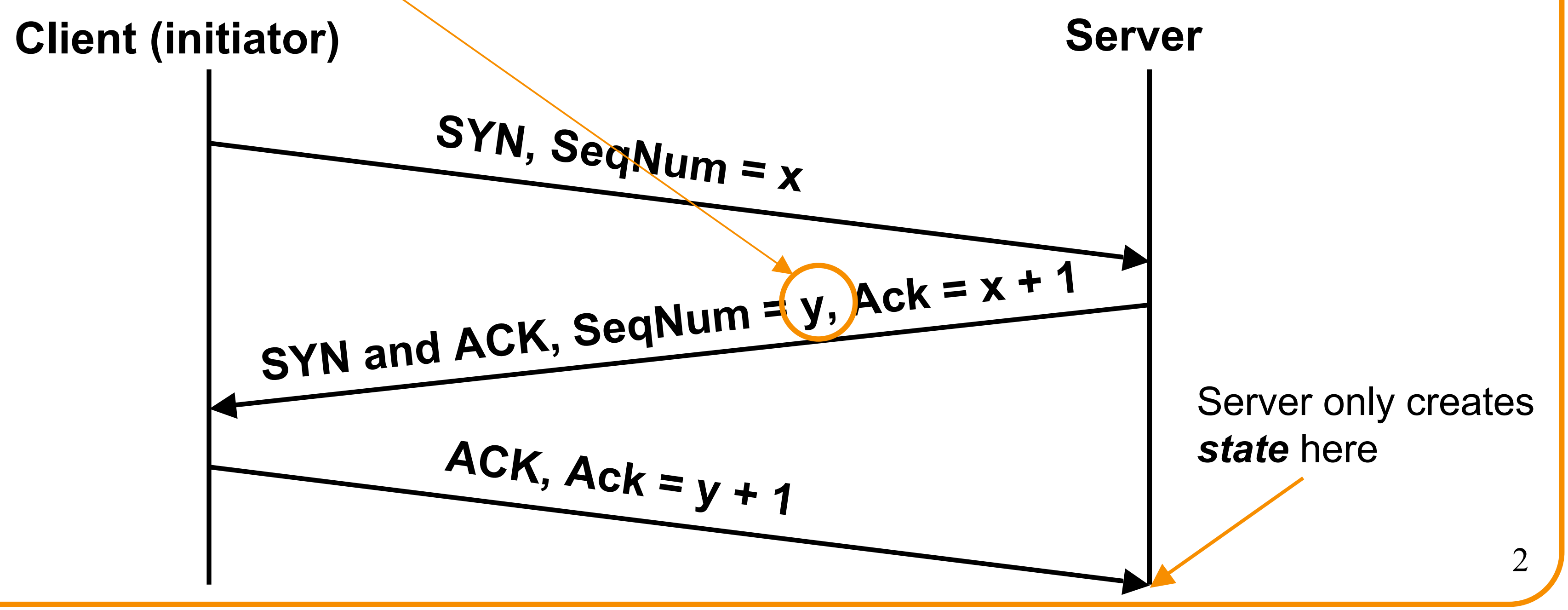
SYN and ACK, SeqNum = y, Ack = x + 1

ACK, Ack = y + 1

Server creates ***state*** associated with connection here

Flooding Defense: *SYN Cookies*

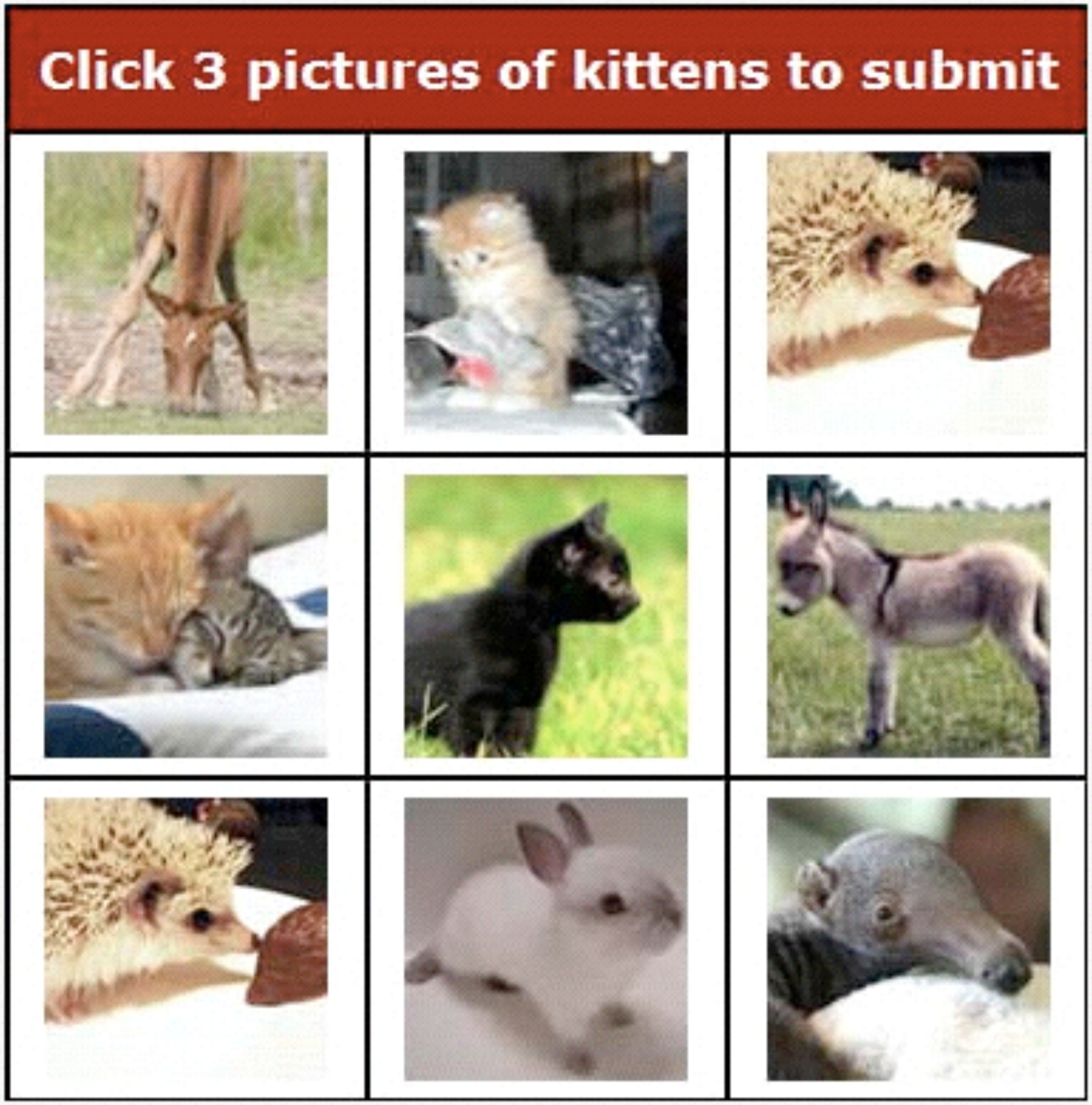
- Server: when SYN arrives, encode connection state entirely within SYN-ACK's sequence # y
  - y = SHA-1(client_addr, client_port, ISN x, *server_secret*)
- When ACK of SYN-ACK arrives, server only creates state ***if*** seq # y in it agrees with hash



Server only creates ***state*** here

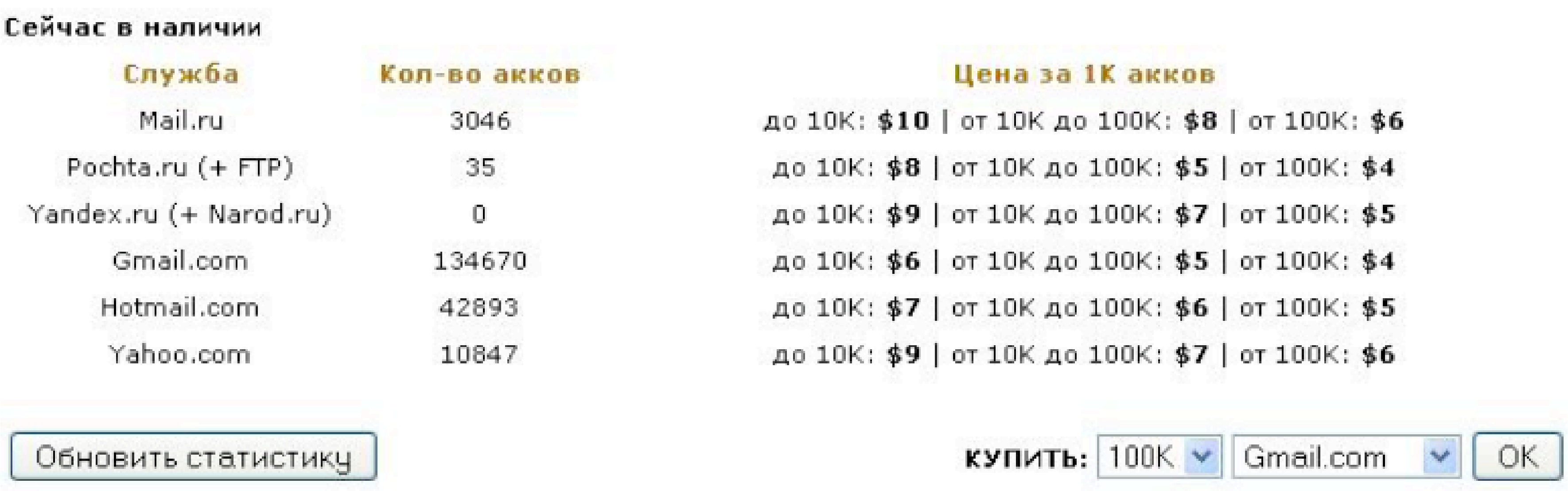
SYN Cookies: Discussion

- Illustrates general strategy: rather than *holding* state, *encode* it so that it is returned when needed
- For SYN cookies, attacker must complete 3-way handshake in order to burden the server
  - Can't use spoofed source addresses
- Note #1: strategy requires that you have enough bits to encode all the state
  - This is just barely the case for SYN cookies
    - 24 bit hash + 5-bit timestamp + 3 bits to remember MSS
    - Can't remember any TCP options …
- Note #2: if it's expensive to generate *or check* the cookie, then it's not a win



Click 3 pictures of kittens to submit

The KittenAuth system. Source: ThePCSpy.com.



Сейчас в наличии

Служба	Кол-во акков	Цена за 1К акков
Mail.ru	3046	до 10K: **$10** | от 10K до 100K: **$8** | от 100K: **$6**
Pochta.ru (+ FTP)	35	до 10K: **$8** | от 10K до 100K: **$5** | от 100K: **$4**
Yandex.ru (+ Narod.ru)	0	до 10K: **$9** | от 10K до 100K: **$7** | от 100K: **$5**
Gmail.com	134670	до 10K: **$6** | от 10K до 100K: **$5** | от 100K: **$4**
Hotmail.com	42893	до 10K: **$7** | от 10K до 100K: **$6** | от 100K: **$5**
Yahoo.com	10847	до 10K: **$9** | от 10K до 100K: **$7** | от 100K: **$6**

купить: 100K Gmail.com