EECS 388 Discussion

Review HW3 / Intro to HW4

Homework 3 Part 1

Central Sign-on Facility

a. **Security Advantage**
   The central site can focus on improving security. The user only has to memorize one really strong password.

b. **Security Disadvantage**
   All eggs in one basket? If it is compromised all the sites are compromised.

Homework 3 Part 1

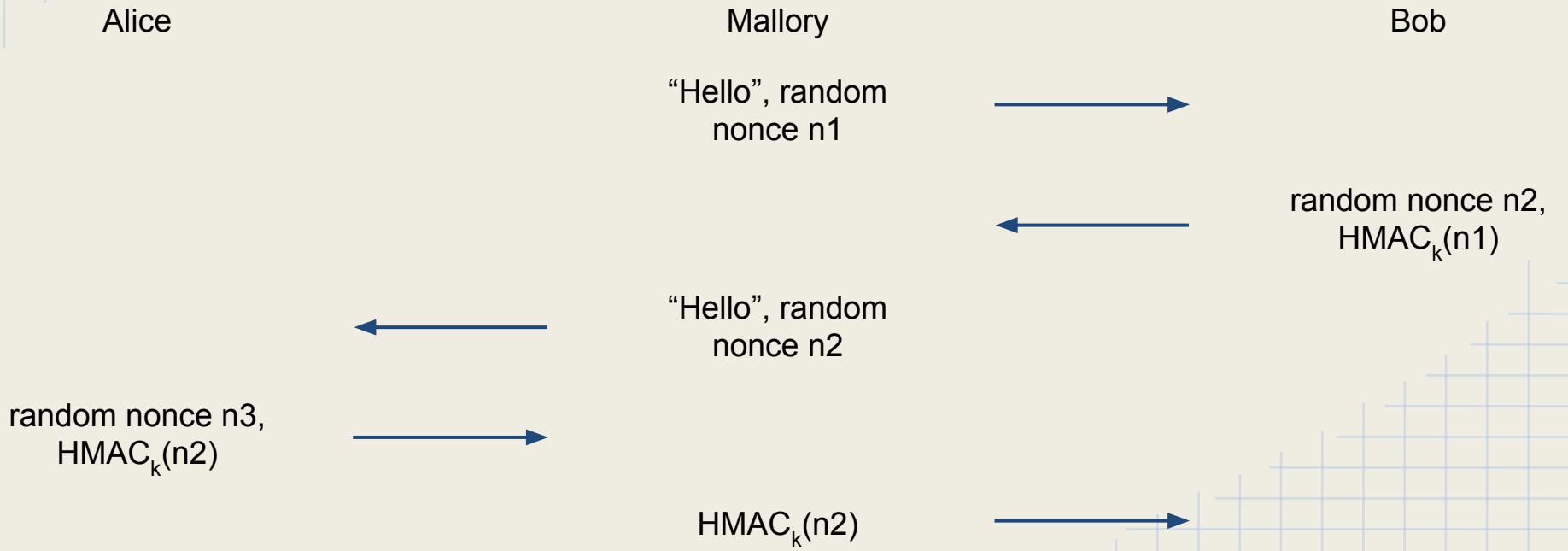
Central Sign-on Facility

c. **Impersonate the user in other websites**
   Site A can take the signature and use it for another site.

d. **Simple fix?**
   Sign(user || site identity)

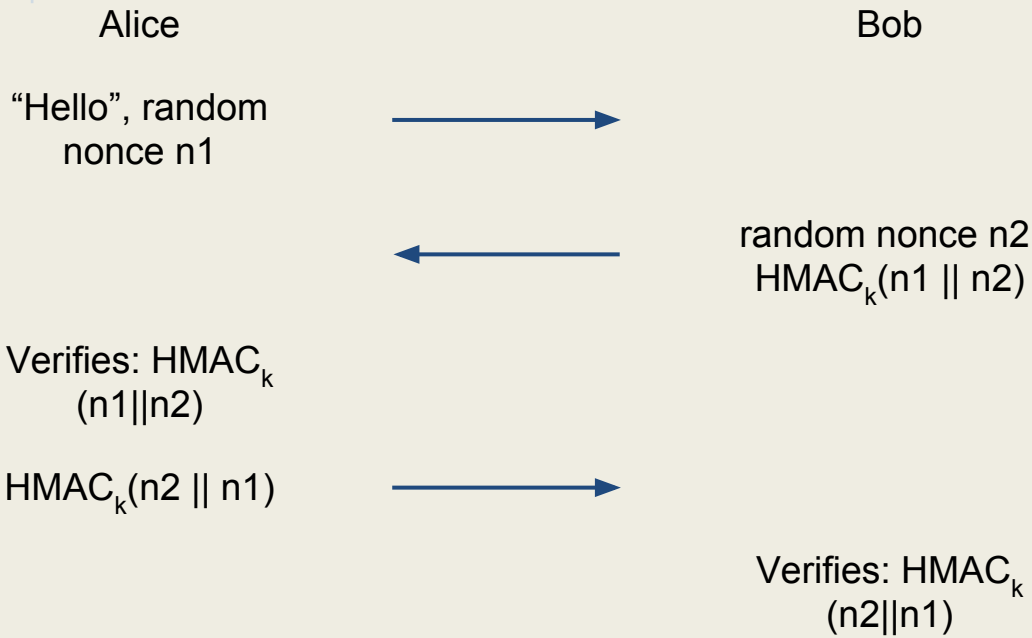
Homework 3 Part 1

Shared key for authentication



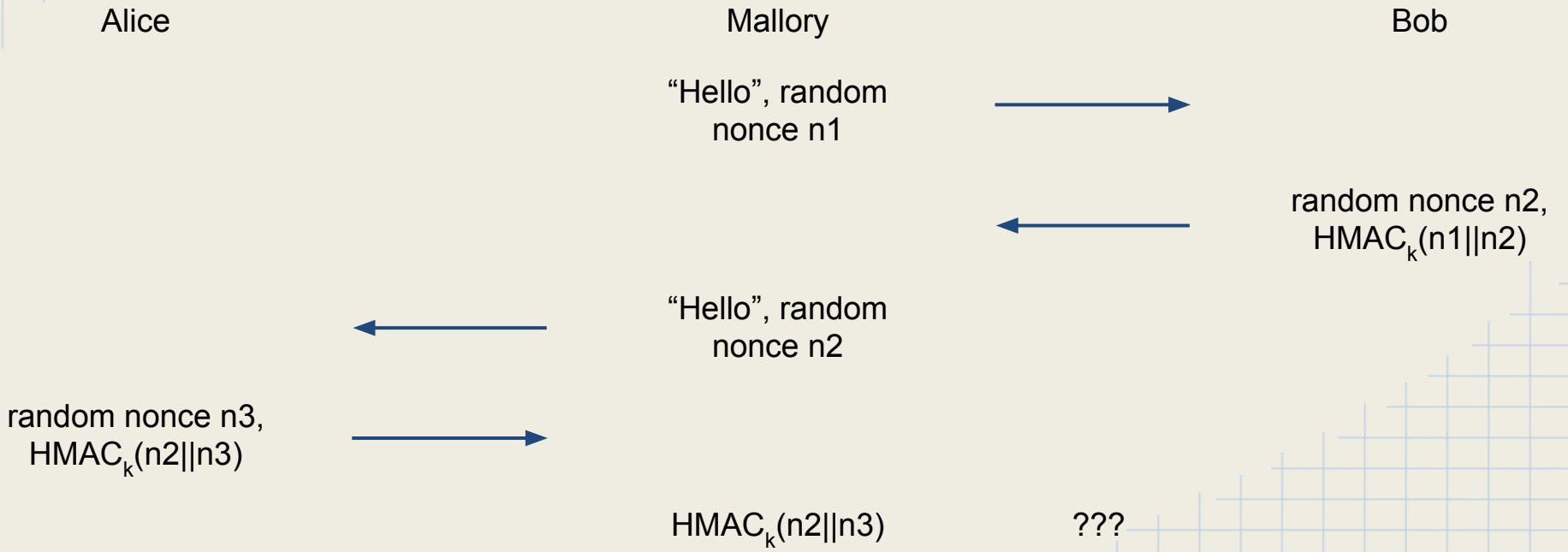
Homework 3 Part 1

BETTER Shared key for authentication



Homework 3 Part 2

Shared key for authentication



Homework 3 Part 2

Password Cracking

a. n = (26 + 26 + 10)8 = 218, 340, 105, 584, 896 possible passwords
   t = n/2(4million)s

b. **Botnet size?**
   7581 node botnet to crack one hash per hour on average

c. **Bytes?**
   n entries 8-bytes + 32-bytes = 7.76 PB

Homework 3 Part 2

Password Cracking

d. **Rainbow table size?**
Each chain has start and end (16 bytes) 16(N/k) bytes.

e. **k = 5000**
651 GB

f. **Time?**
30,325 hrs

Homework 3 Part 2

Password Cracking

g. **Compare?**
   Time vs space?

h. **More secure?**
   We would need to brute force the server secret too

i. **Even more secure?**
   Per user-salt…other ideas?

j. **Bitcoin mining...**
   ~10mins… Moore's law

Homework 4 Intro

Denial of Service (DoS) Attack

- **Strategy:** send an overwhelming number of requests to a server
- **Goal:** the targeted machine or network resources are unavailable for others

Homework 4 Intro

Distributed DoS (DDoS)

- Launch DoS attack using multiple machines or botnet, a collection of internet connected programs that await orders
- As of 2014, the frequency of recognized DDoS attacks had reached an average rate of 28 per hour.

Homework 4 Intro

(1) Think like a defender

- What are the techniques to prevent DoS?
- How effective are they?

(2) Learn about attacker tools and some history

- What's LOIC and how does it work?
- Who would use DoS attacks and why?