Hot Topics in Computer Security

Iliano Cervesato

http://www.qatar.cmu.edu/iliano

Outline

- Let's play a security game
- Cryptographic protocols
- Where did this guy say he's from?

Here is the game

- Threat
  - “Someone can break into my apartment and steal or destroy my stuff”
- Attacks and countermeasures
  - I have a basic protection, but worse things can happen, help me to find what and how to mitigate them

My apartment’s basic protection

Classic wooden door with a 3 points lock

On the balcony (2nd floor), PVC windows with a single point lock

But … what’s in my apartment?

What do we learn from the game

- You never prevent a threat
  - .... you lower the risk!
- Performing an attack has a cost
  - It's a balance between
    - the assets that you want to protect
    - the efforts an attacker will make
- Deploying a countermeasure has a cost
  - It's a balance between
    - the cost of recovering from the attack
    - the cost of a deploying a protection mechanism

But keep in mind ...

- Security should always serves the business and not constrains it, otherwise ...
  - nobody will invest in it
  - or will be disable to be more efficient
- What is your definition of the risk analysis for computer science?

Now you know ...

- Marketing guy: *"My software is totally secure!"*
  - You: *"Oh really? Against what?"*

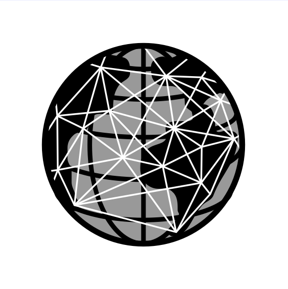
- Your boss: *"Design my information system and make it secure!"*
  - You: *"tell me what you want to protect and let's talk together about ...*
    - *potential threats*
    - *reasonable attacks to consider*
    - *and counter-measures to deploy to lower the risk"*

Do your own risk analysis

- How important is the data in your laptop?
  - What if someone accesses, copies, distributes modifies, deletes my data?
  - What if the system is down or not working well?
- But your information is larger than just your laptop, what about ...
  - the other machines you are using? Your phone and other digital devices?
  - your CMU account, your Gmail address, your MSN, your Facebook?

Computer Security

- Networked computer systems
  - Provide fast access to lots of information
    - Information society
  - Higher productivity
  - Much higher convenience
- Substantial opportunity for abuse

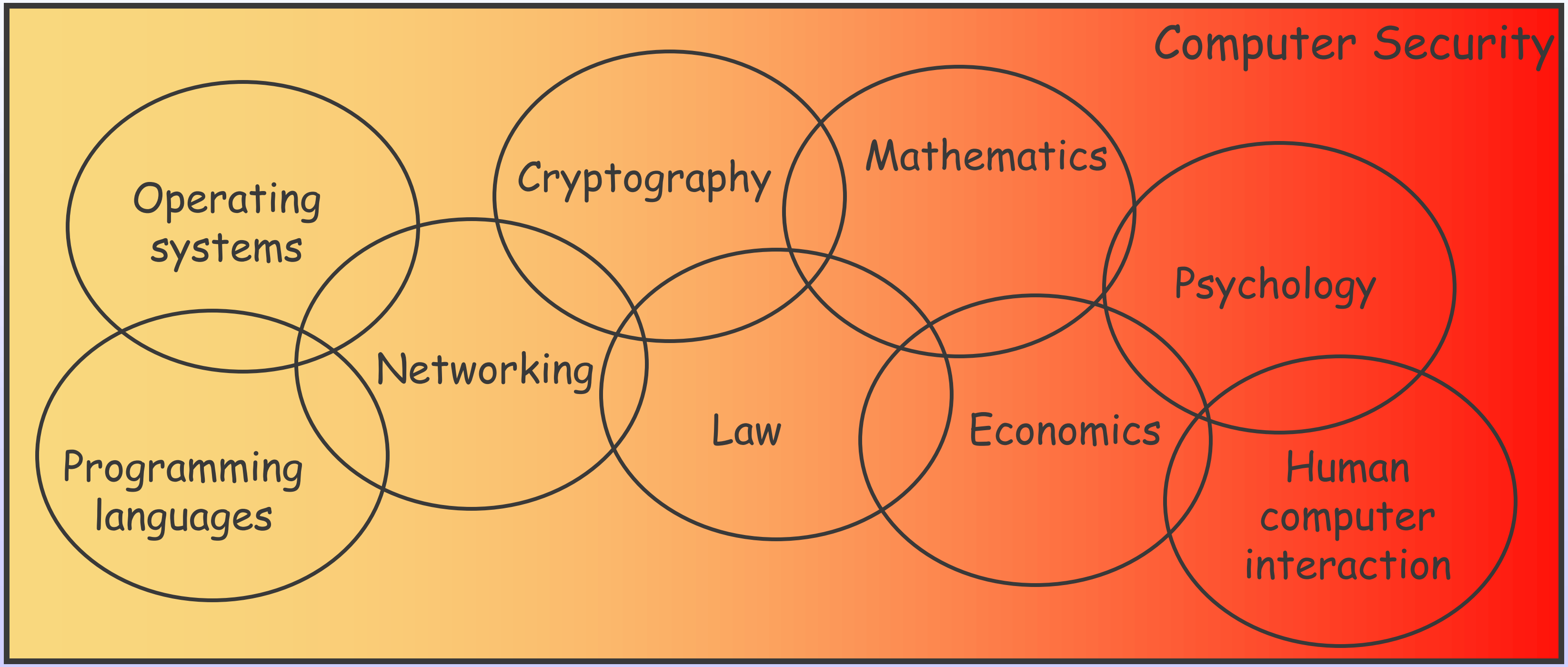


- Computer security
  - Mitigate risk
  - Prevent disruption, fraud, …

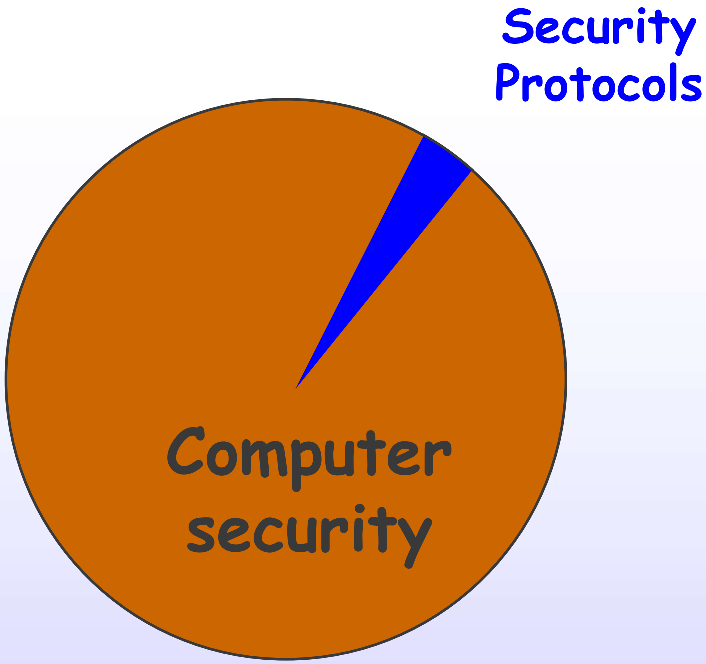
Is Cryptography the Solution?

Cryptography is not the same as security

- No crypto today
- 85% of all CERT advisories cannot be fixed by crypto
- 30-50% of recent security holes from buffer overflow



Computer Security is a Big Field!



- We are going to look at a tiny speck

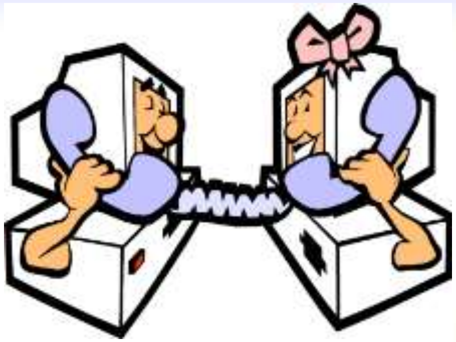
- Security Protocols

Protocols

Expected behaviors when engaging in communication

- When 2 people want to talk
  - Buying something
  - Driving conventions
  - Calling up your friend, …
- When interacting with an organization
  - Bureaucracy
  - Official visits by head of states, …
- …
- When computers want to talk

Computer Protocols



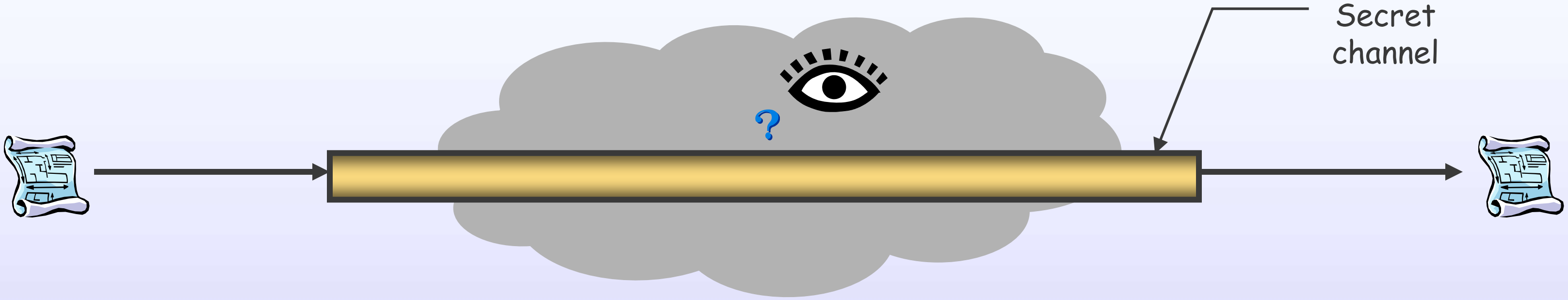
- What sets them apart?
  - No human involved!
    - Automated
    - Inflexible
    - No common-sense
- What protocols are there in a computer?
  - Hundreds!
  - Communication protocols
    - Email, http, Ethernet, …
  - Security protocols

Security Protocols

- Communication protocols ensure that communication actually happens
- Security protocols ensure that communication is not abused
  - Protect contents
  - Protect communicating parties
  - Protect intent of communication
  - Protect possibility of communication

Common Security Goals

- Confidentiality
  - Message cannot be observed in transit



  - Achieved using some form of encryption

Authentication

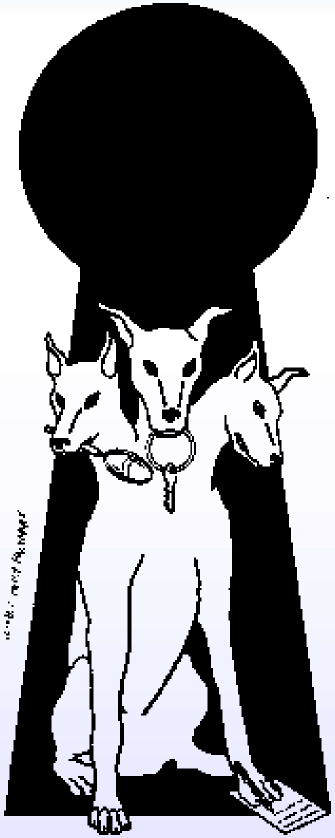
"On the Internet, nobody knows you're a dog."

- Ensure that we are talking with who we think
  - Much more subtle than secrecy
  - How to establish a secret channel in the first place
    - Negotiate parameters of channel
    - Ensure channel remains trusted
- Authentication protocols

Other Security Goals

- Non-Repudiation
  - Party cannot claim he didn't do it
  - For auditing, electronic contract signing, …
- Non-Malleability
  - Message cannot be changed en route
  - For electronic voting, …
- Anonymity
  - Hide who is communicating
- Availability
  - User can always get through
- …

Example: Kerberos

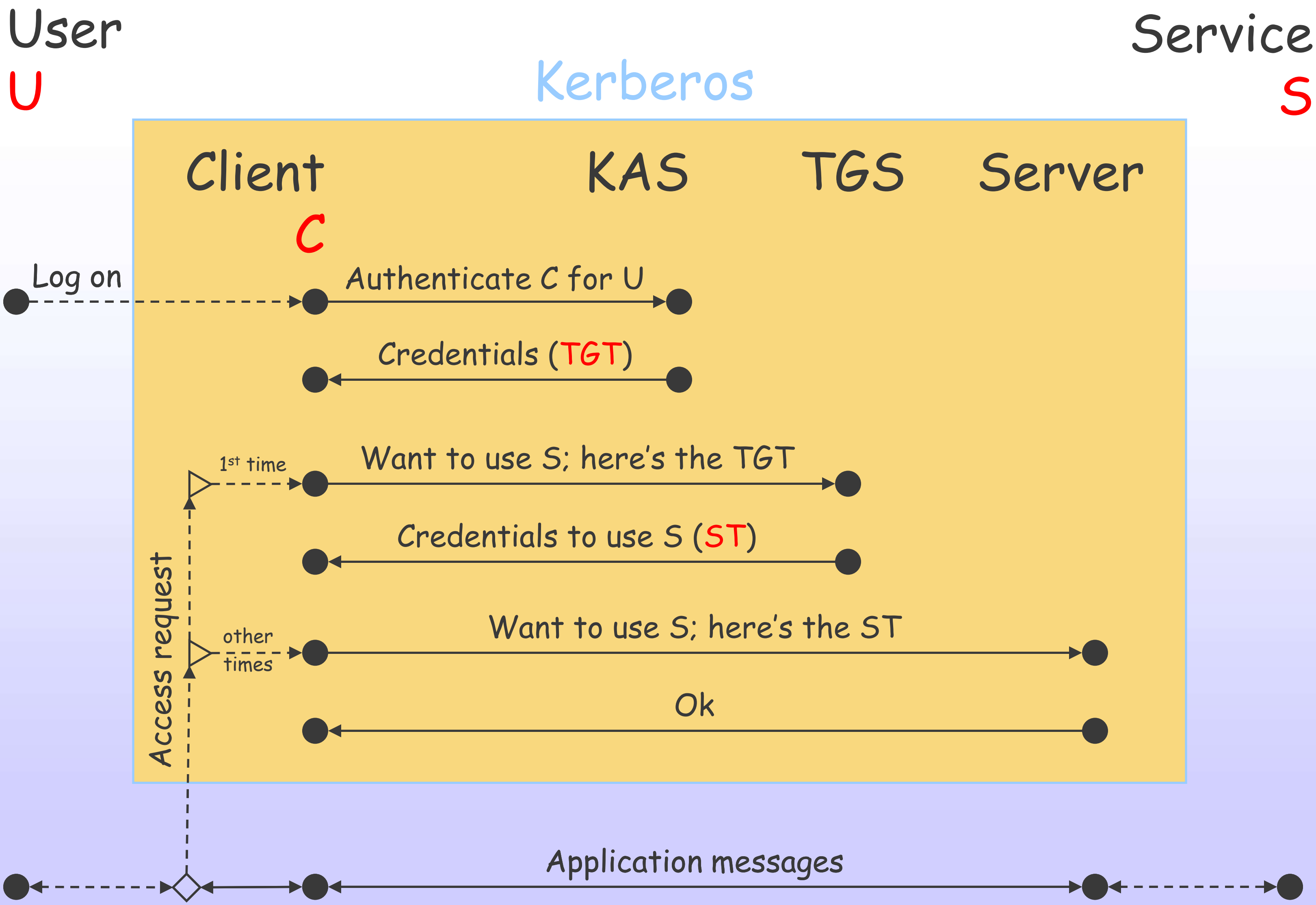


- Log in to your computer
- Access other computers without logging in again
  - Email, “i-drive”, printers, directory, …

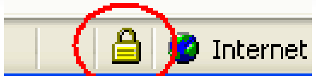
  … for 1 day

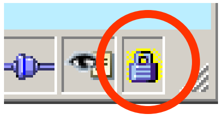
- Goals
  - Repeatedly authenticate a client to multiple servers
  - Transparent to user
- Ubiquitous

How Kerberos works



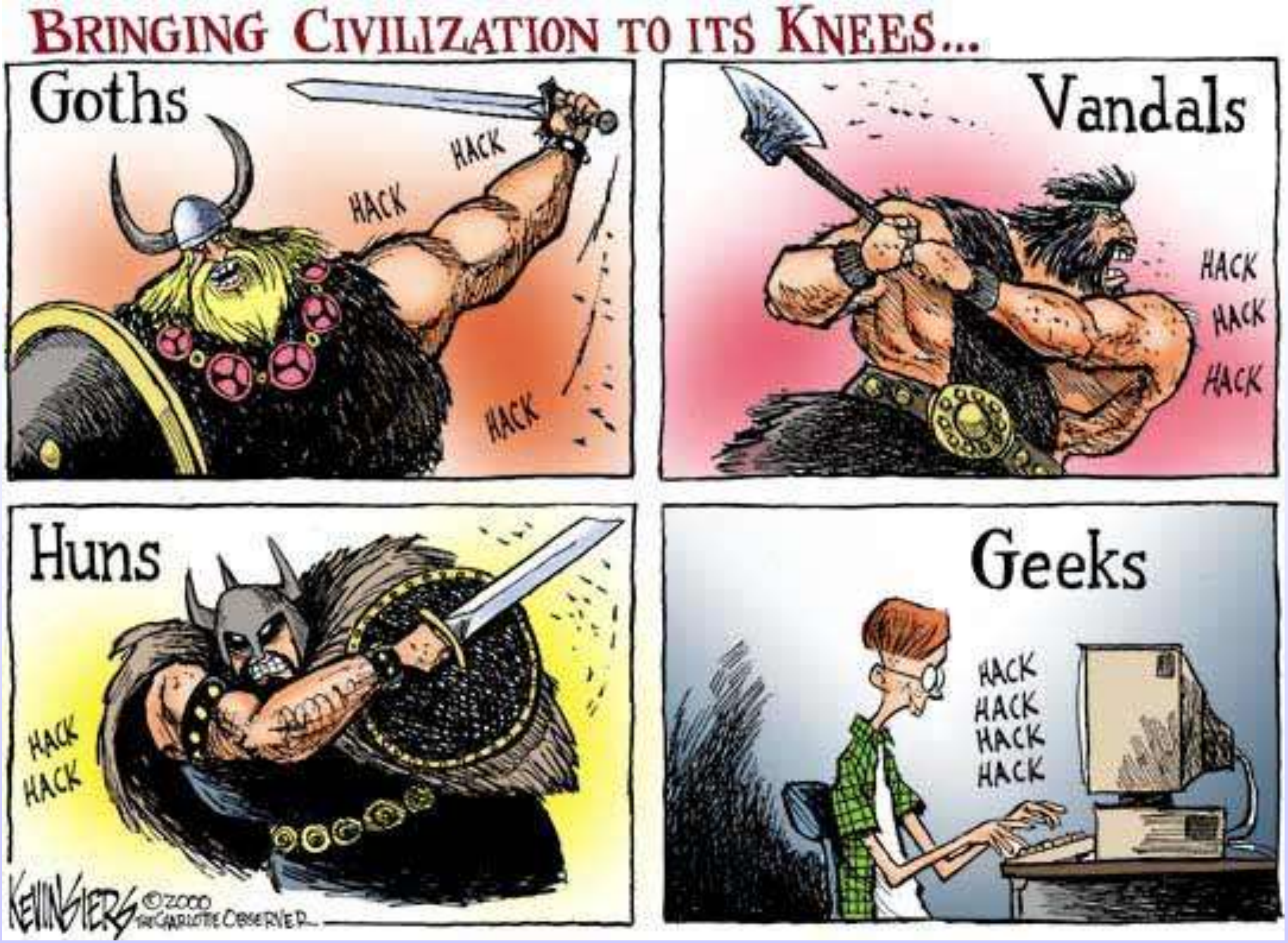
Other Popular Protocols





- SSL / TLS protocol
  - Authenticates client to server
  - Encrypts communication
  - ➢ HTTPS (secures web page)
  - ➢ Secure email download (POP3S, IMAPS)
- SSH protocol
  - ➢ PuTTY (Log to remote computer, copy files, …)
- PGP
  - Send encrypted/authenticated email
  - ➢ Enigmail

What is there to care about?


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

The Problem

- Security protocols are extremely hard to get right
  - Minuscule programs
  - Extremely complex interactions
    - Bugs can take years to discover

  - Generally it's not the crypto
  - It's the piping

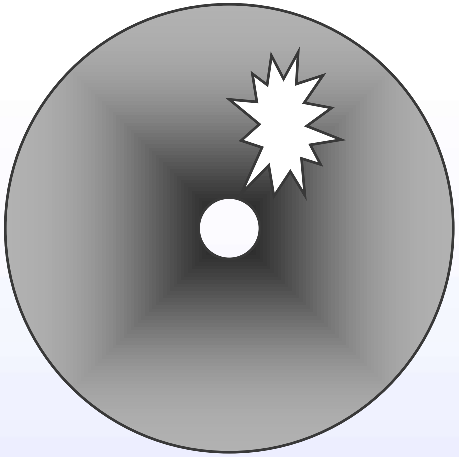
Correctness vs. Security

- Correctness: satisfy specifications
  - For reasonable inputs, get reasonable output
- Security: resist attacks
  - For unreasonable inputs, output not completely disastrous

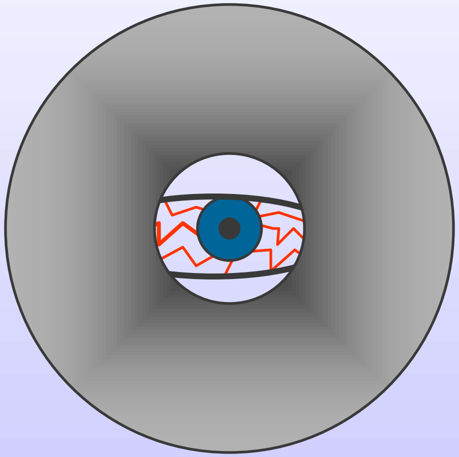
Difference:

- Random events vs. active attacker

Attacks

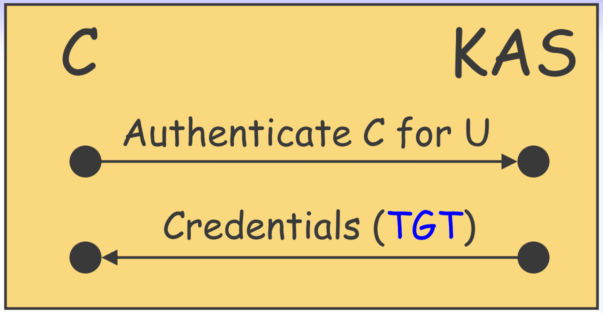


- Attacker can break secrecy of the channel



- Attacker can break authentication
  - Got the piping wrong

Example: Kerberos

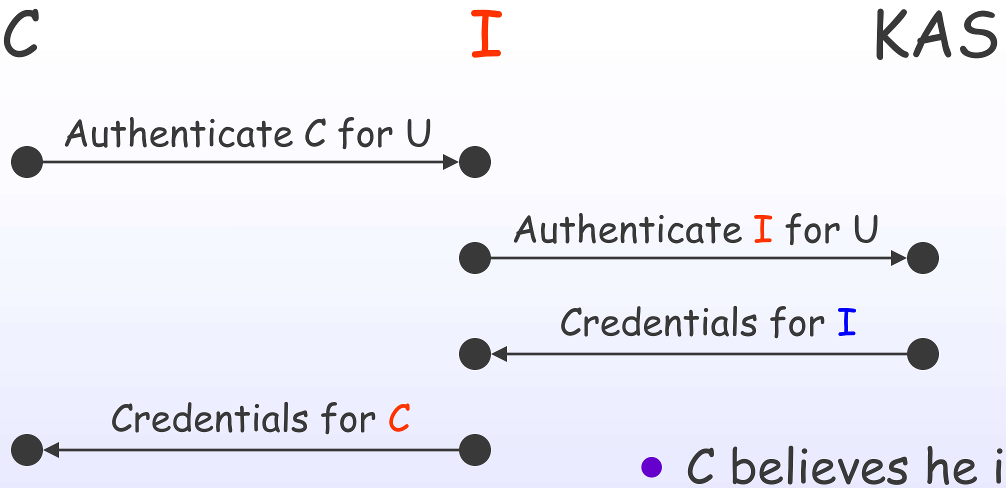


C

KAS

Authenticate C for U

Credentials (TGT)



C

I

KAS

Authenticate C for U

Authenticate I for U

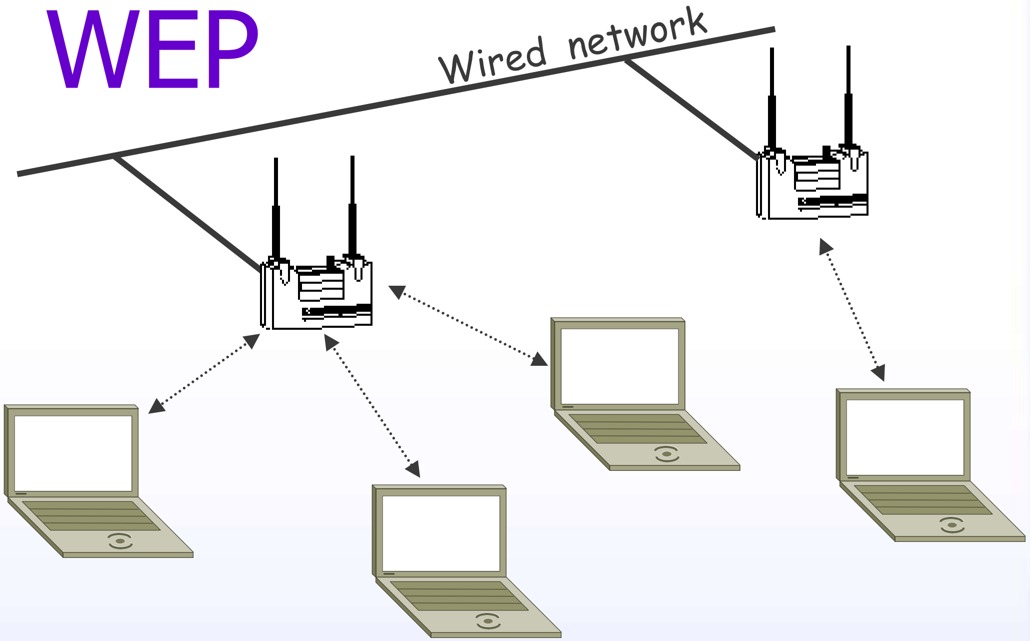
Credentials for I

Credentials for C

- C believes he is talking to KAS
- KAS believes he is talking to I
- I knows the key that C obtained from KAS

- Discovered 10 years after exchange was designed
- Immediately fixed in all implementations

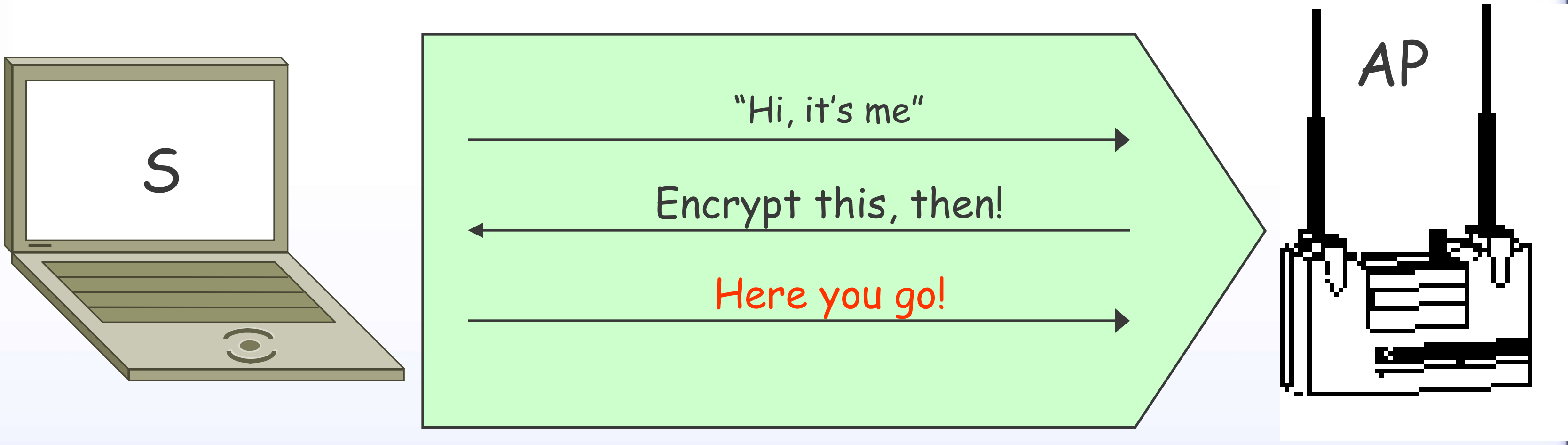
Another one: WEP



- Standard wireless network
  - Principally a communication mechanism
  - Has built-in security protocol: WEP
    - Confidentiality (prevent eavesdropping)
    - Access control (prevent unauthorized access)
    - Integrity (prevent tampering with messages)

Fails at all 3!

WEP Authentication



S

“Hi, it’s me”

Encrypt this, then!

Here you go!

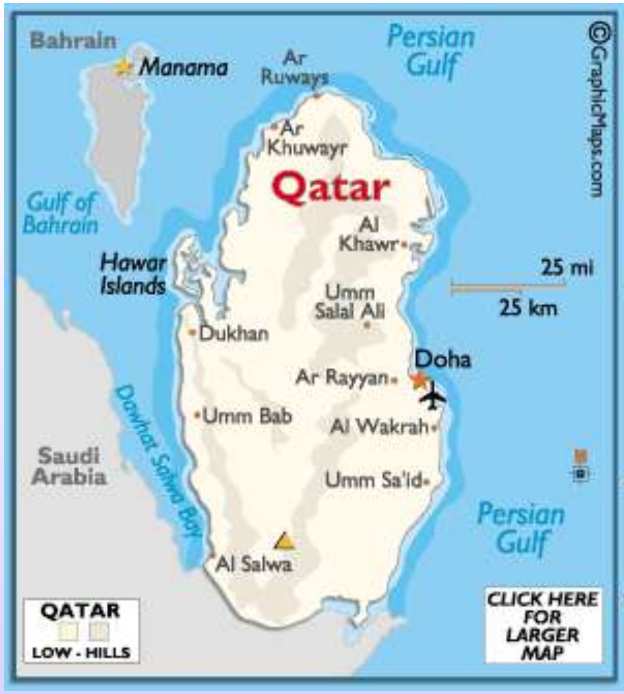
AP

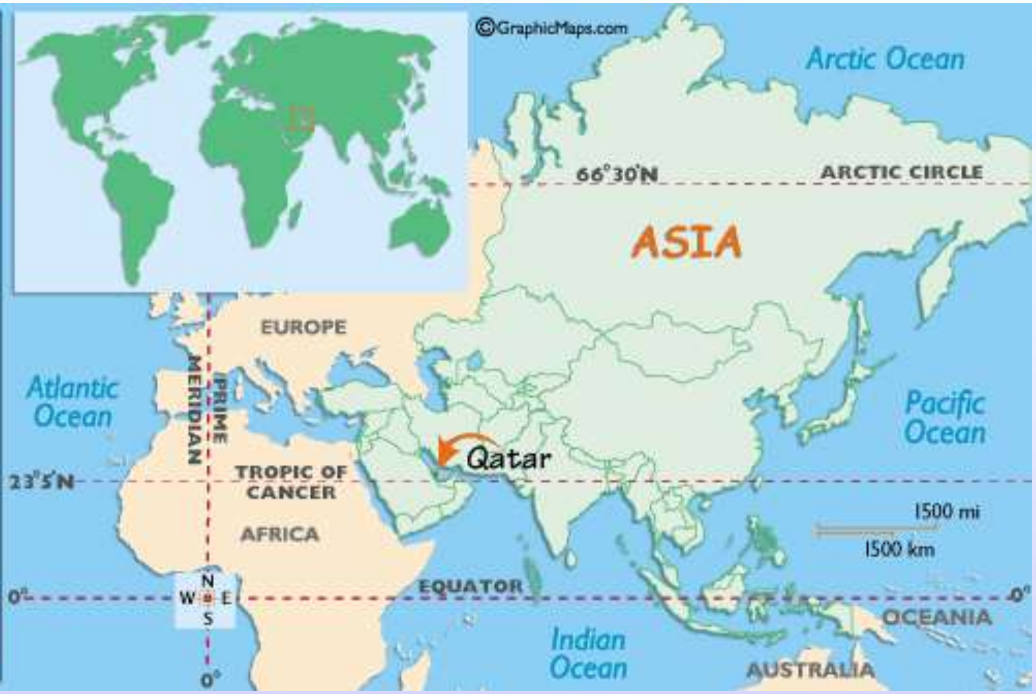
- Should you stop using WiFi? NO!!!
  - Fine <u>communication</u> suite
  - Use standard protocols on top of it
  - (now replacements to WEP are available)

A Carnegie Mellon Campus in Qatar …

جامعة كارنيجي ميلون في قطر
Carnegie Mellon Qatar

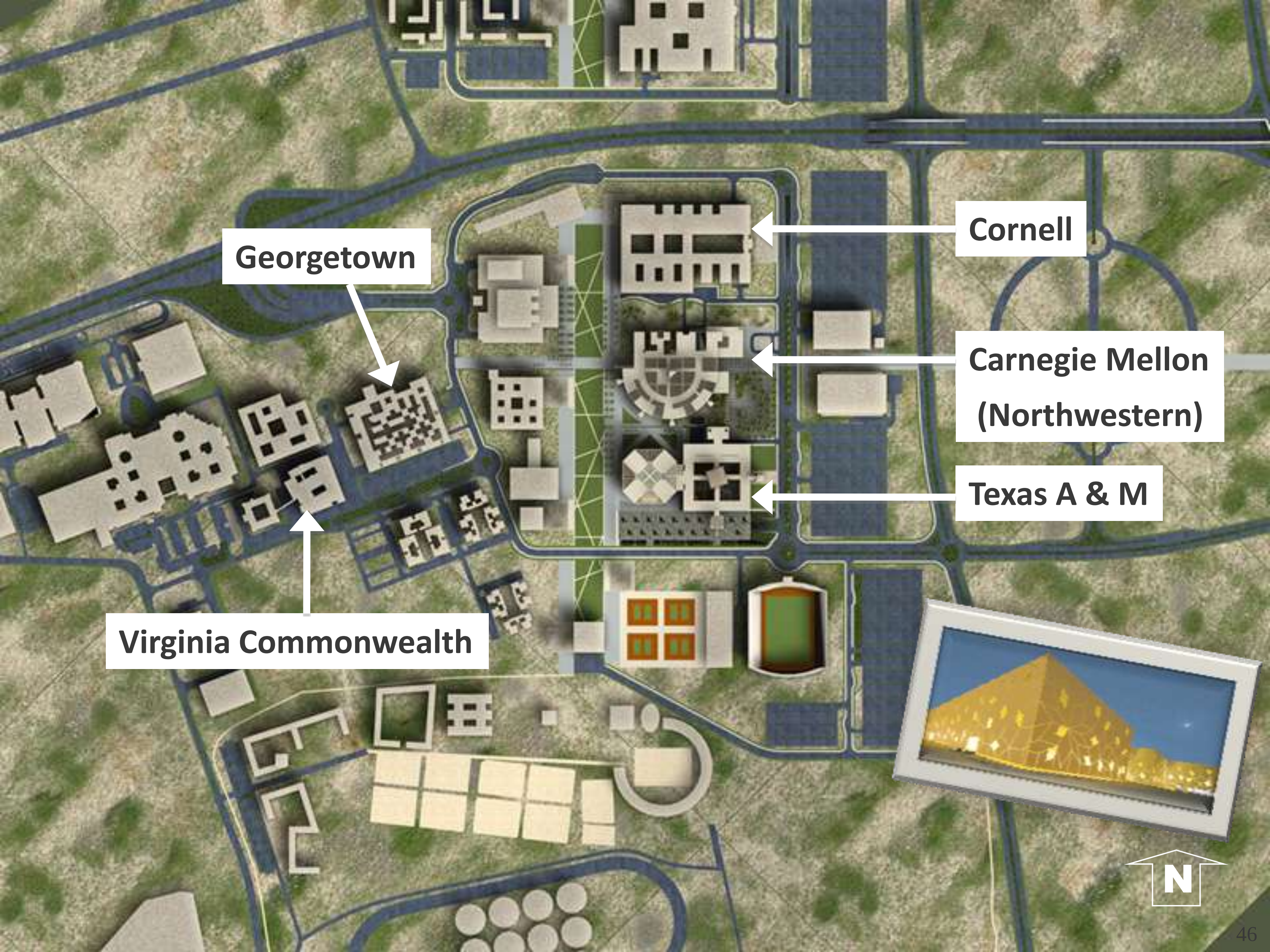
Where Is Qatar anyway?





What is CMU doing there?

- Launched in 2004
- 3 undergraduate programs
  - CS, BA, IS
- 3 classes of graduates
- ~275 students enrolled this fall


Georgetown
Cornell
Carnegie Mellon
(Northwestern)
Texas A & M
Virginia Commonwealth
N

One University, Two Campuses

Pgh and Doha campuses share

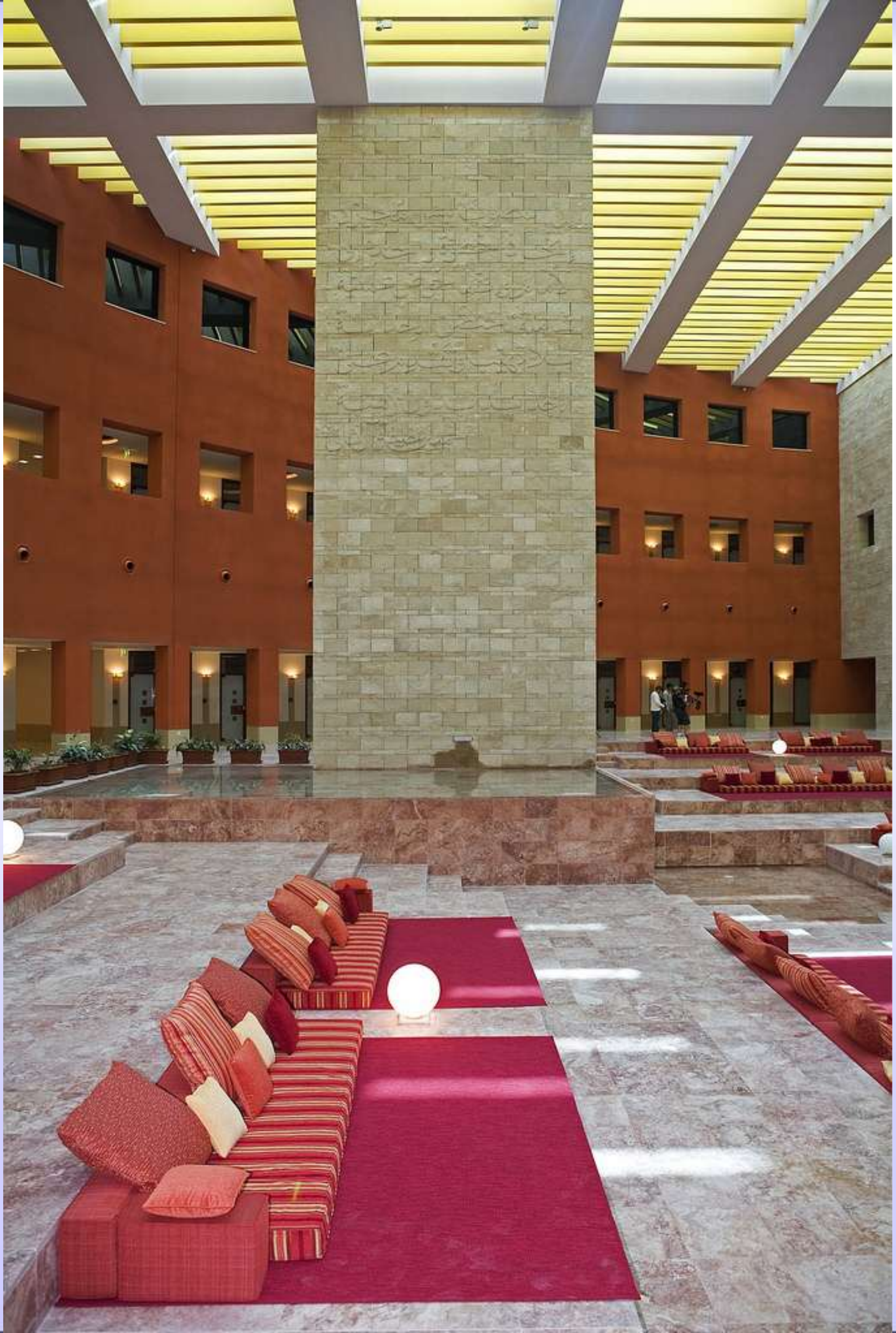
- same admission process
- same curricular requirements
- same faculty standards
- same tuition
- same degree

CMU Computer Science in Qatar

- 12 faculty, 6 postdocs
- 90+ students
  - 25+ courses
- 3 labs
  - Lots or research opportunities
- Lots of activities
  - 50+ invited speakers
  - Dozens of clubs

negie-Mellon University
PENNSYLVANIA 1900

… and the Professors?



Interesting Visitors

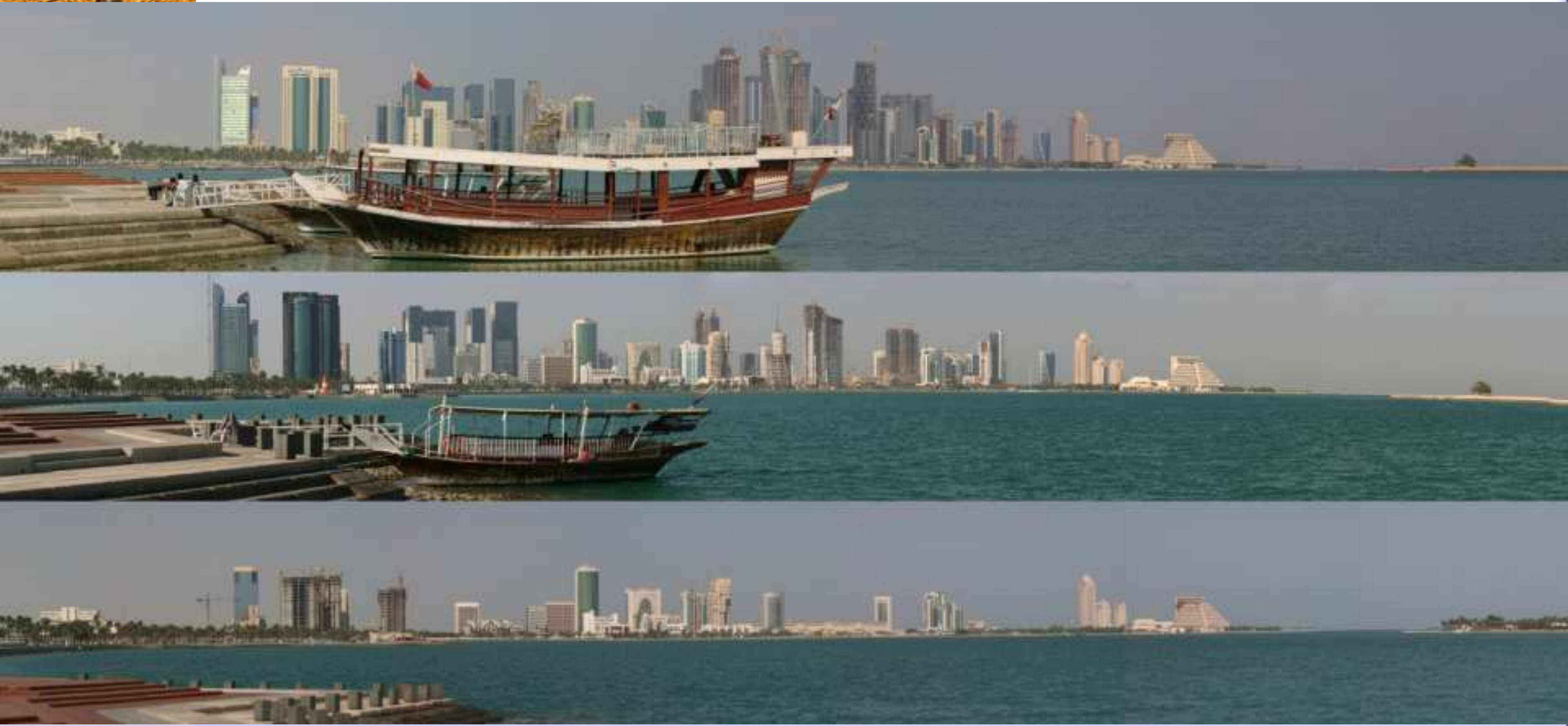
What is it like to live in Qatar?

Hot Dusty Beige

What is it like to live in Qatar?

Pleasant

What is it like to live in Qatar?



Booming

What is it like to live in Qatar?

Fun

What is it like to live in Qatar?

Interesting

What is it like to live in Qatar?

Surprisingly similar to the US …

… in some ways

What is it Like to Live in Qatar?

Strikingly different in other ways

Further Information

- Visit the CMU-Q website:
  - www.qatar.cmu.edu
- Check us out on Flickr
  - www.flickr.com/photos/carnegiemellonqatar/
- Follow us on Facebook
  - www.facebook.com/CarnegieMellonQ

Thank you!