CS558 Network Security

Lecture 1: Intro

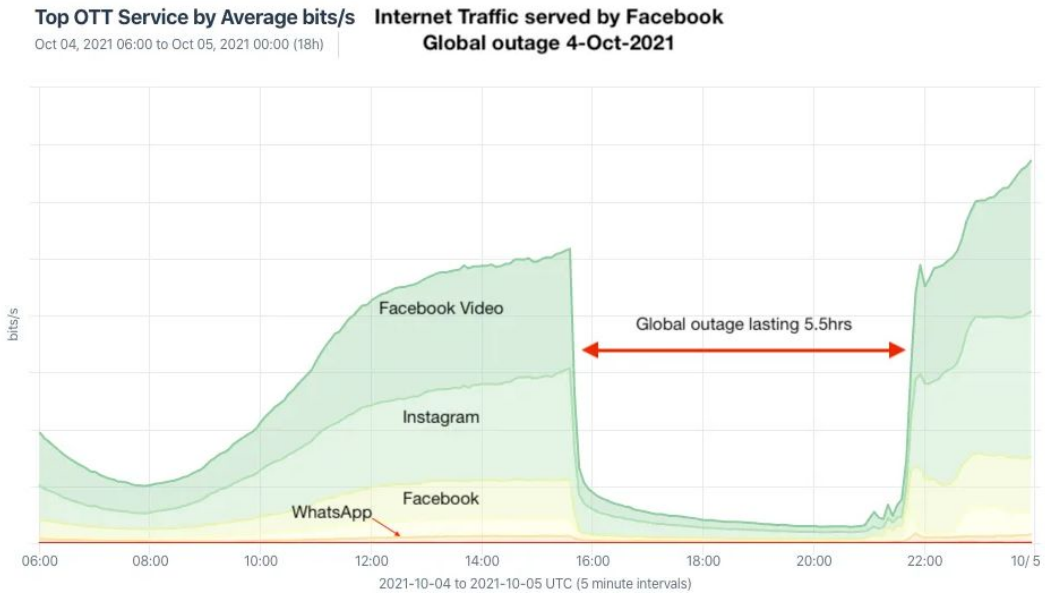
BOSTON UNIVERSITY

Course’s Major Technical Themes

Course's Major Technical Themes

Computer Networks

Computer Security



Let's Encrypt

BOSTON UNIVERSITY

Story 1: Corporate/National Defense

U.S. Army Cyber Command

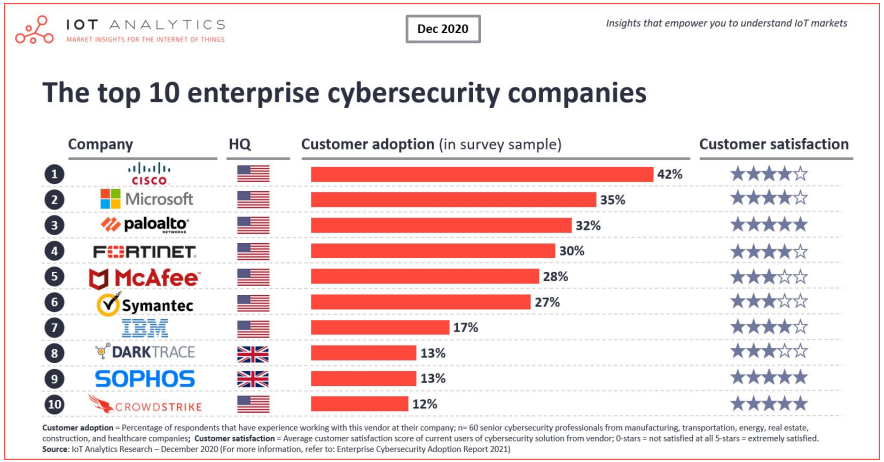
Fleet Cyber Command (10th Fleet)

Sixteenth Air Force (Air Forces Cyber)

Marine Corps Forces Cyberspace Command

Cyber National Mission Force

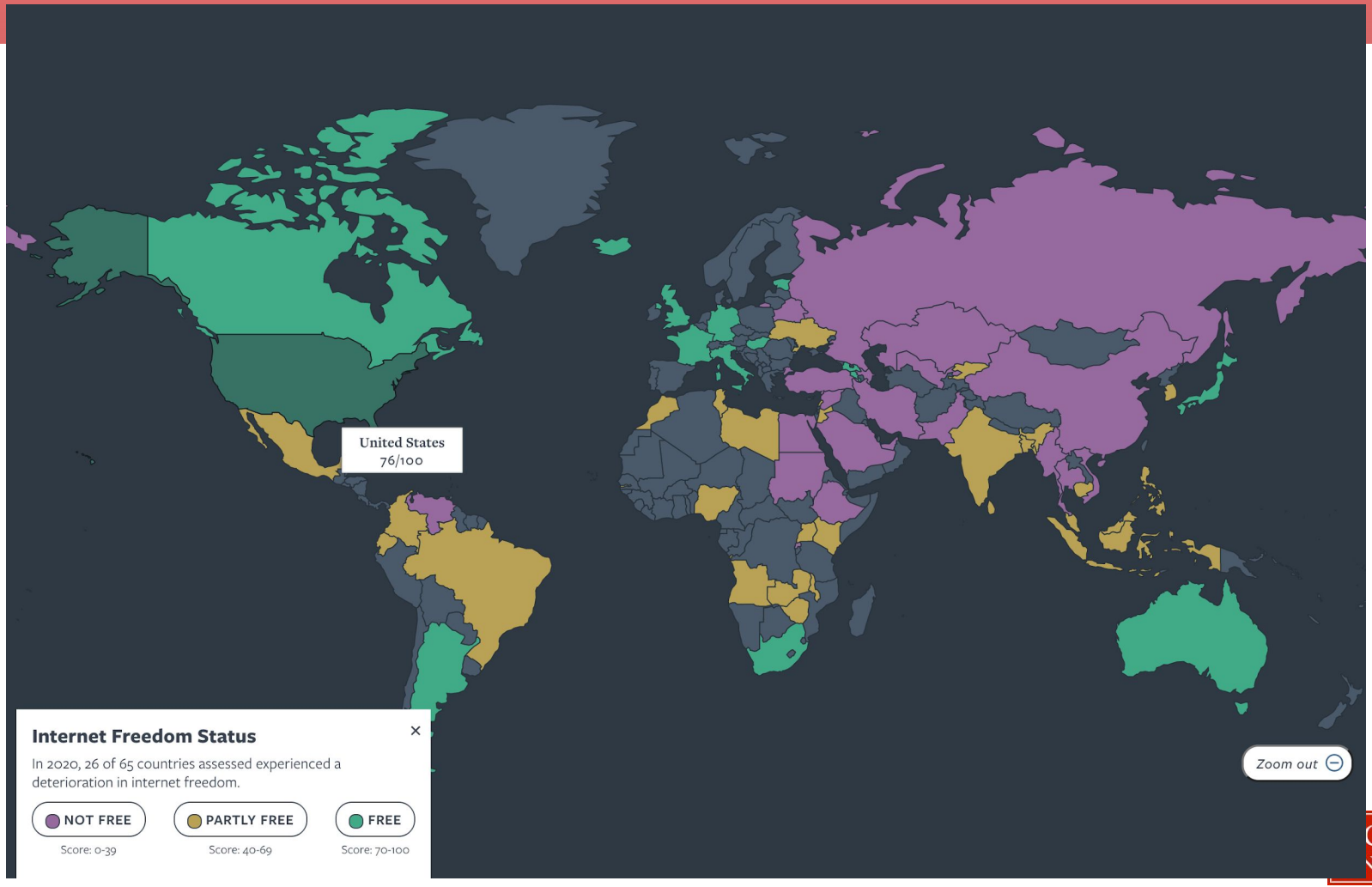
Joint Force Headquarters - DoD Information Network



BOSTON UNIVERSITY

Story 2: Civil Liberties and Surveillance

BOSTON UNIVERSITY


United States
76/100
Internet Freedom Status
In 2020, 26 of 65 countries assessed experienced a deterioration in internet freedom.
NOT FREE
Score: 0-39
PARTLY FREE
Score: 40-69
FREE
Score: 70-100
Zoom out

OPINION

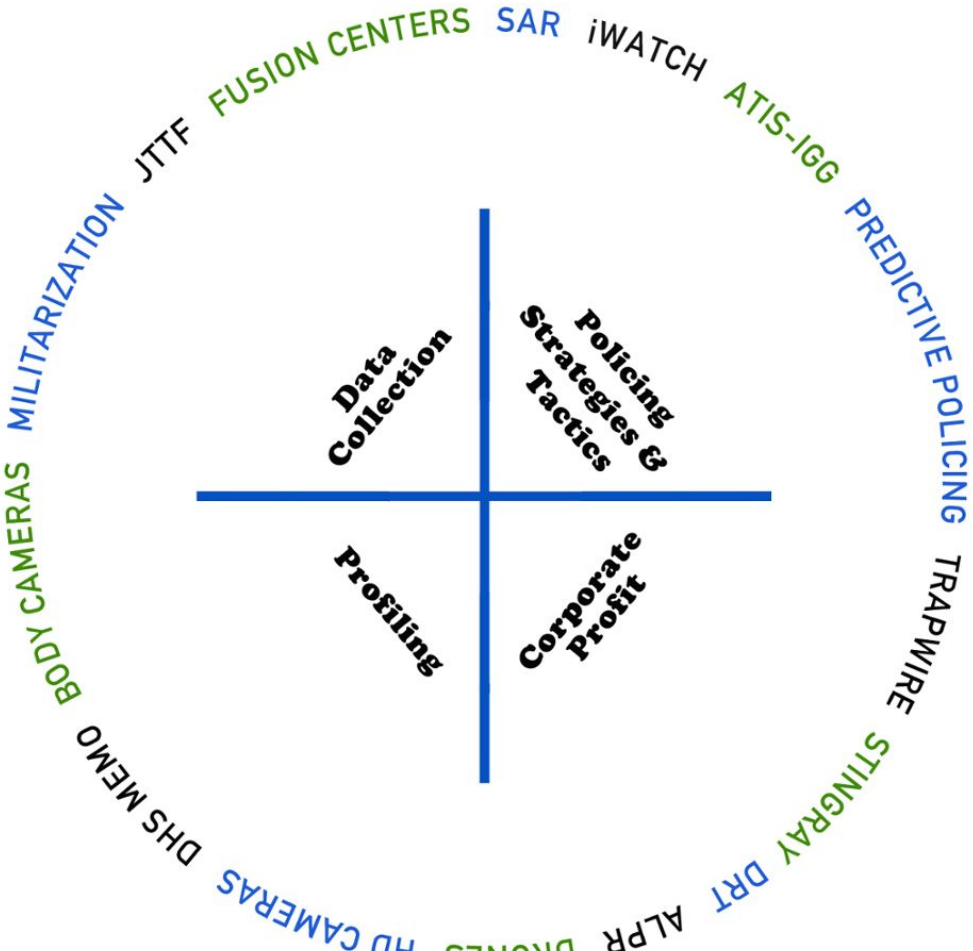
What It's Like to Live in a Surveillance State

By James A. Millward

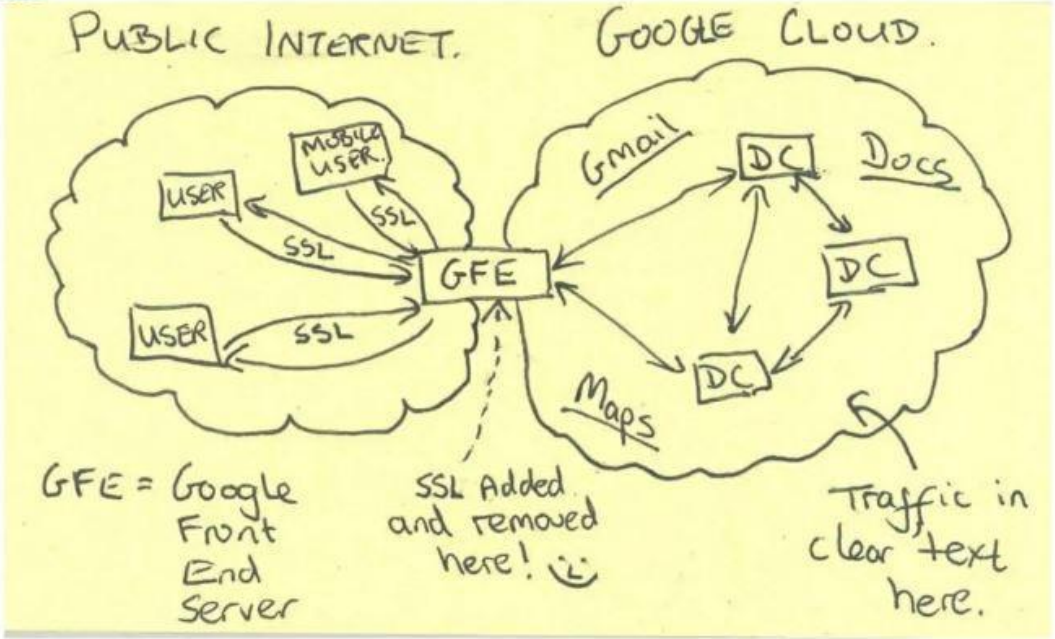
BOSTON UNIVERSITY


BLACK
LIVES
MATTER
DON'T SHOOT
CAN'T BREATH

BOSTON UNIVERSITY



Current Efforts - Google



Public Law 107–56
107th Congress

An Act

Oct. 26, 2001
[H.R. 3162]

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

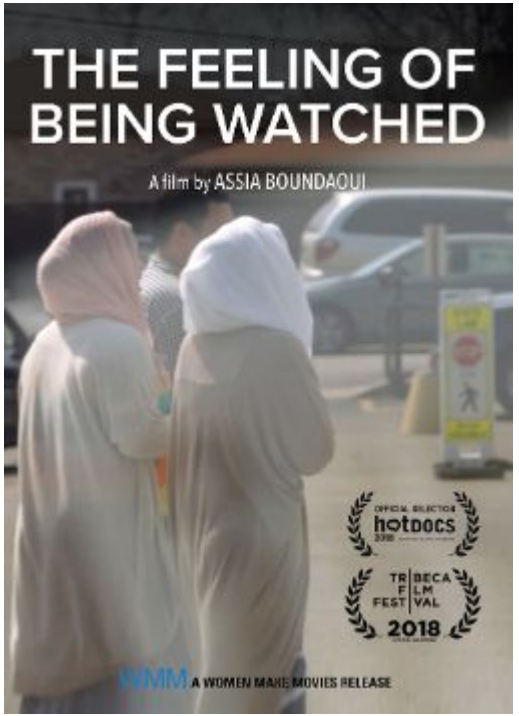
Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
18 USC 1 note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:



BOSTON UNIVERSITY

Oct. 26, 2001
[H.R. 3162]

Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
18 USC 1 note.

TITLE II—ENHANCED SURVEILLANCE PROCEDURES

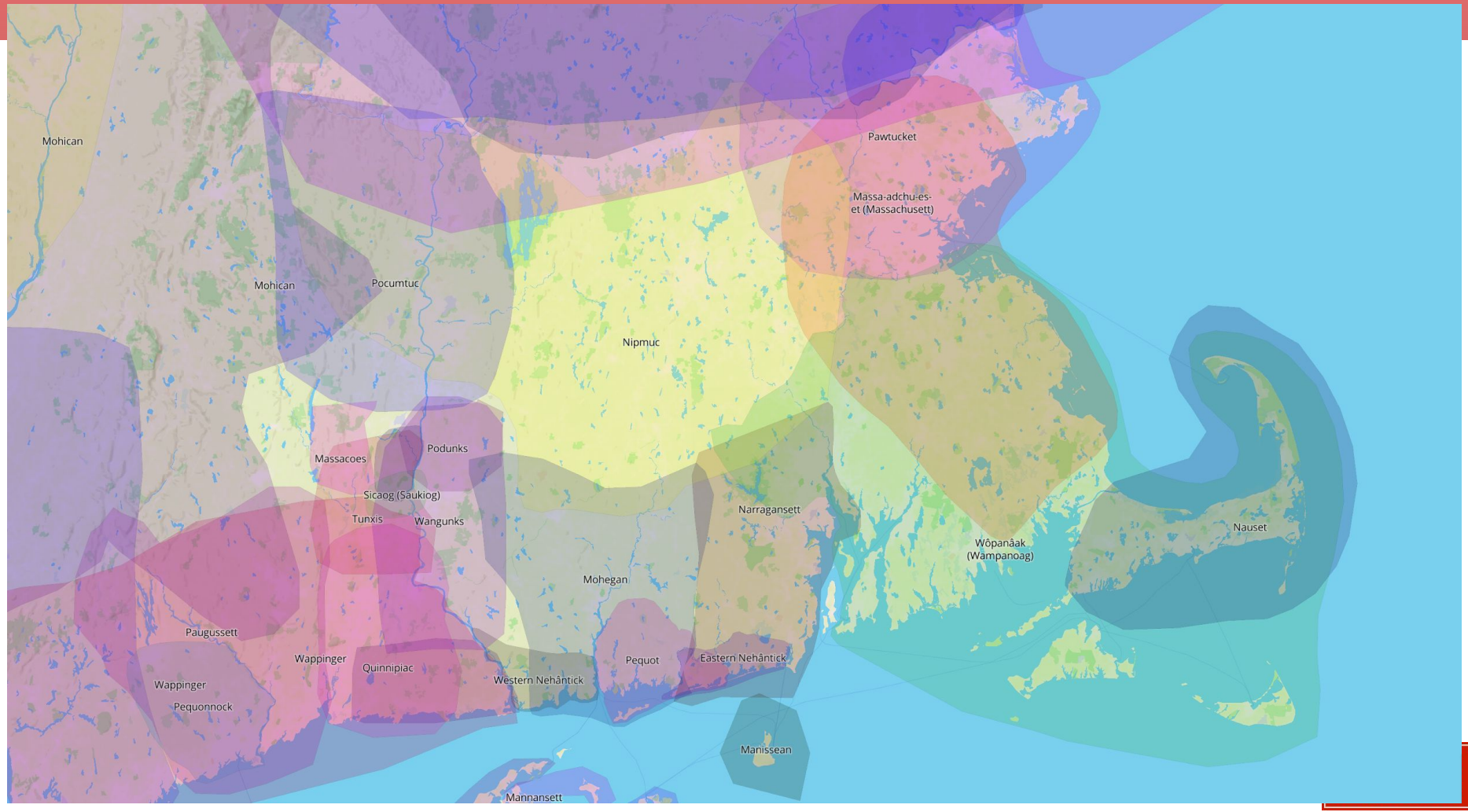
BOSTON UNIVERSITY

https://www.zinnedproject.org/

BOSTON UNIVERSITY

“Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool, and it confers on the field an intrinsically moral dimension.”

-- Phil Rogaway, “The Moral Character of Cryptographic Work,” 2015


Mohican
Pawtucket
Massa-adchu-es-et (Massachusett)
Mohican
Pocumtuc
Nipmuc
Podunks
Massacoes
Sicaog (Saukiog)
Tunxis
Wangunks
Narragansett
Nauset
Wôpanâak (Wâmpanoag)
Mohegan
Paugussett
Wappinger
Quinnipiac
Pequot
Eastern Nehântick
Western Nehântick
Wappinger
Pequonnock
Manissean
Mannansett

Course Learning Goals

- Know and understand the fundamental tools that secure the modern internet
- Educated guess as to **WHY** components of secure protocol are there
- Develop/deepen adversarial thinking
- Strengthening independent learning skills

Course Outline

Part 1: When Networking Protocols Go Wrong

(Or, “Wait… what if someone doesn’t play nice?!?”)

- ARP, DNS, BGP, TLS.

Part 2: Privacy on the web

- Censorship Resistance (Tor, Accessing Tor)
- A little bit of secure messaging

Course Logistics

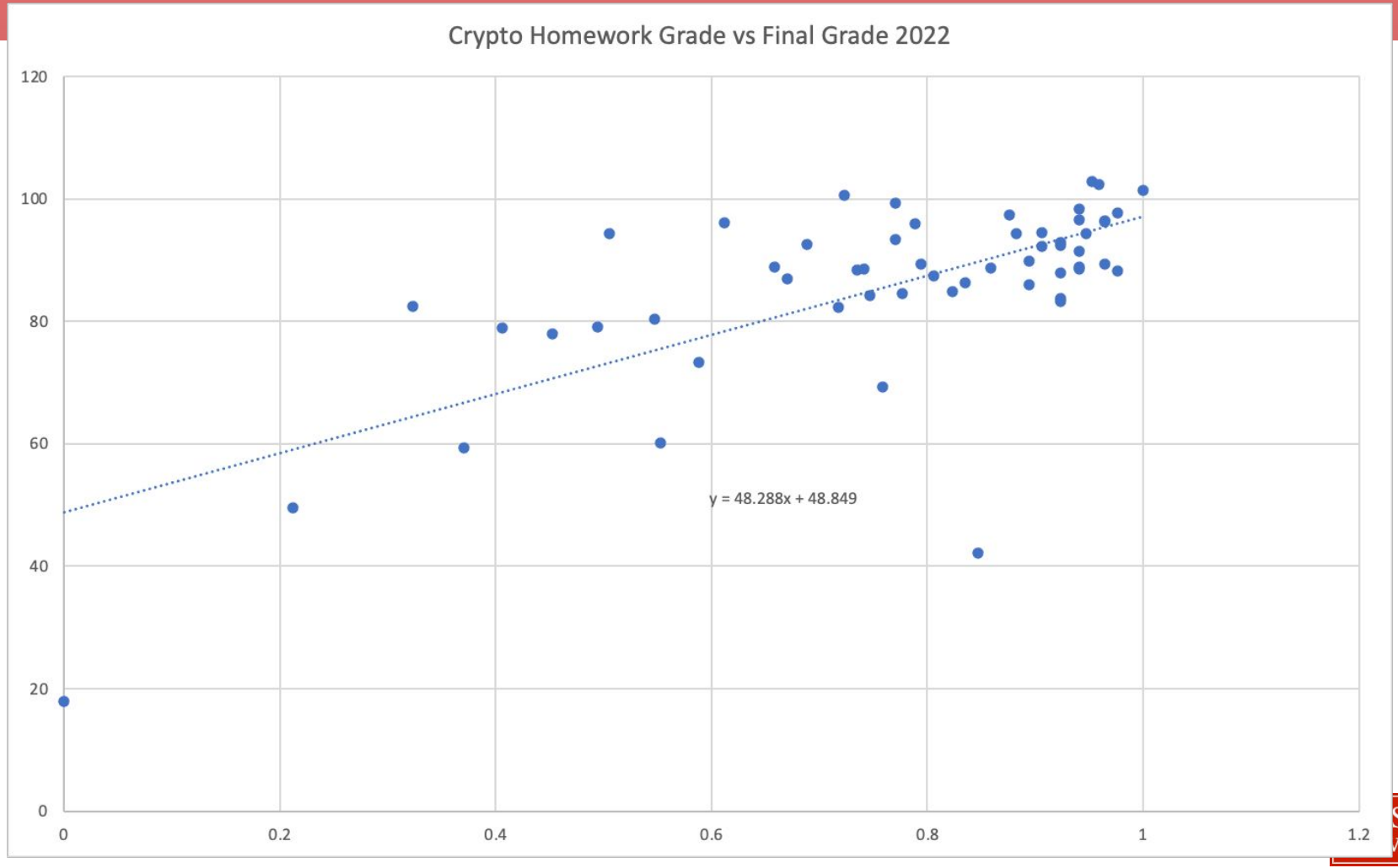
- Piazza and Gradescope (https://www.gradescope.com/courses/489834 Code: K3XEWR)

- Assignments (Mostly monday nights @9pm)
  - 3 Written Homeworks (30%)
  - 2 Programming Assignments (32%)
  - Cumulative Final Exam (25%)
  - Weekly Reading Assignments (15%)
    - Summary ~150 words
    - 1 thing you found interesting
    - 1 thing you found confusing
    - 1 thing you googled to learn more about
  - Weekly Question (3%) (Friday@9pm)
- Labs/Review Sections

What will be helpful to know?

- Crypto Basics
  - Symmetric Key Encryption
  - Public Key Encryption
  - Message Authentication Codes
  - Digital Signatures
  - Cryptographic Hash Functions
  - Pseudorandom Functions (will come up later and are less important)
- Crypto Homework

- Good High-level Understanding of Networking
- Python


Crypto Homework Grade vs Final Grade 2022
120
100
80
60
40
20
0
0
0.2
0.4
0.6
0.8
1
1.2
y = 48.288x + 48.849

Things to know about me

- Applied Cryptography is my home
- Slides will make way more sense in context
- Can’t spell to save my life
- Offline Friday night - Saturday night
- Office Hours

BOSTON UNIVERSITY