




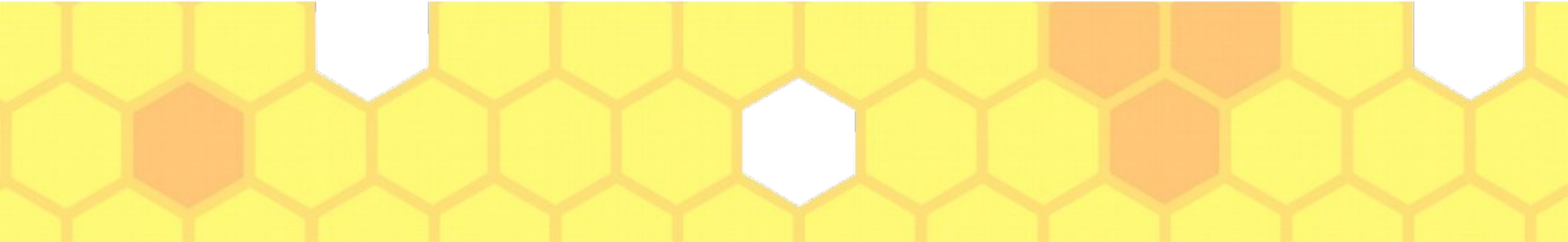
CSE 468 Fall 2023

jedimaestro@asu.edu





Why are you paying the extra money and investment of time to get a B.S. from ASU instead of just staying home and reading Wikipedia? Or watching free lectures from MIT professor?



My thoughts...

- Prof. Gary Gear (ERAU): A bachelor's degree is a “license to learn”
- ASU is a research university
 - Surprising amount of experience in the room
- We're here *together* in the classroom for a reason



Outline

- A little about me and the course
- Syllabus
- Rainbows



“For the mind does not require filling like a bottle, but rather, like wood, it only requires kindling to create in it an impulse to think independently and an ardent desire for the truth.”

-Plutarch

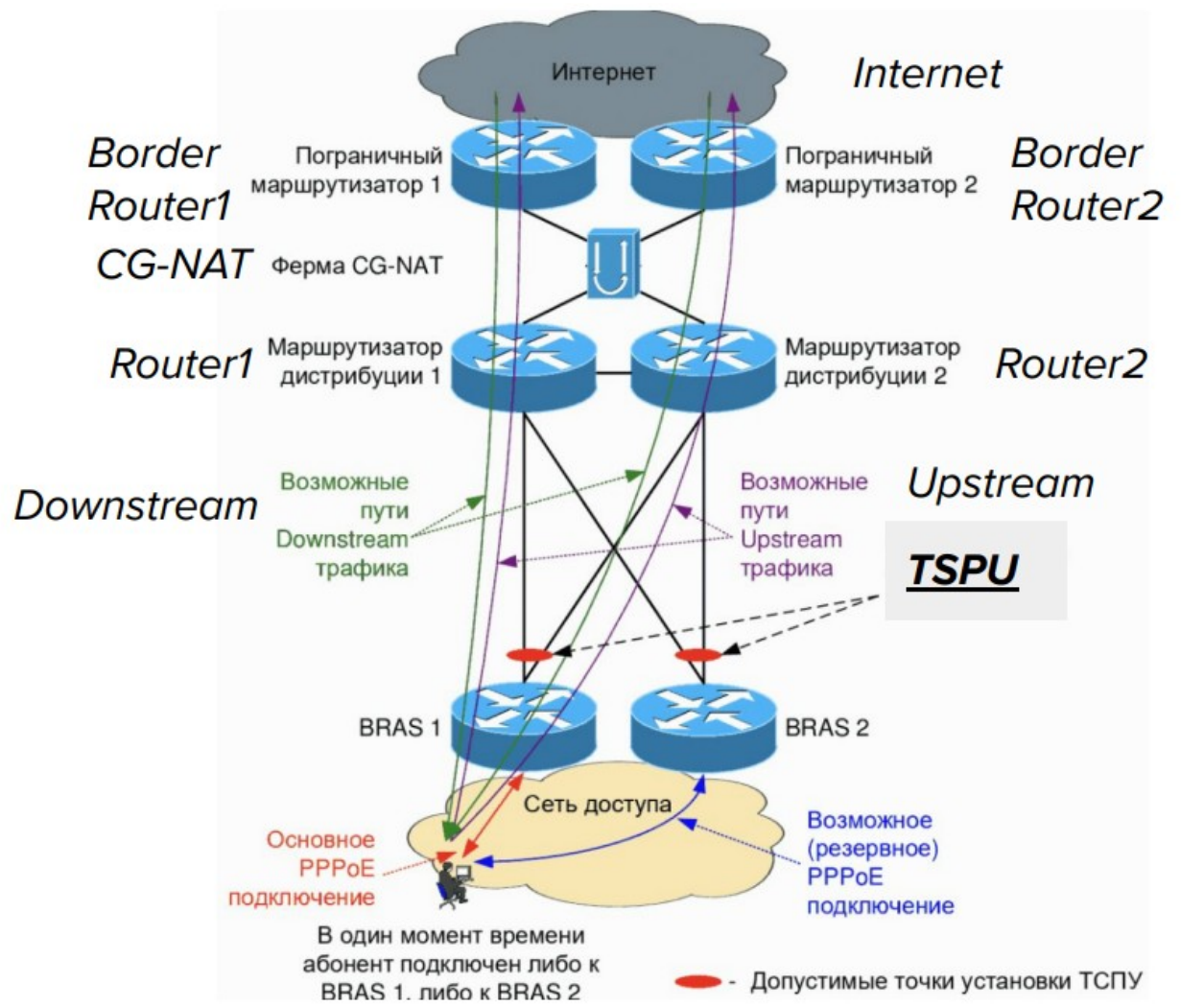


A little about me...

- Associate Professor in SCAI, joint appointment in Biodesign Center for Biocomputing, Security, and Society
- Started at ASU in 2020, was at the Univ. of New Mexico for 13 years before that
- Research is about Internet freedom



Measuring censorship



VPN security (and privacy and availability)



Algorithm 1 Opcode Fingerprinting Logic

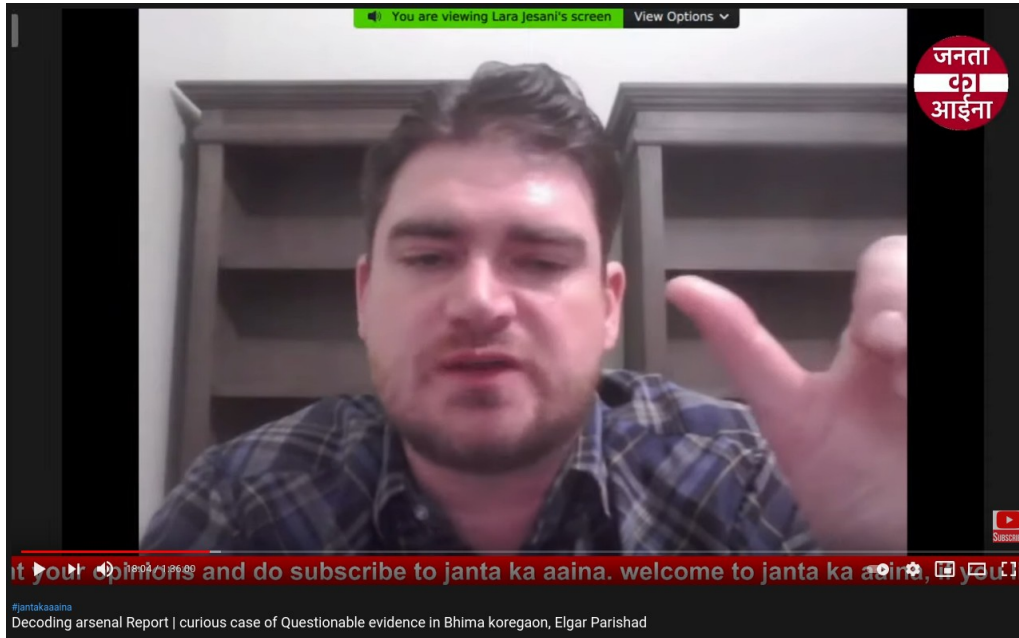
Require: $N \geq 0$
 $OCSet \leftarrow \{\}, CR \leftarrow Opcode[0], SR \leftarrow Opcode[1]$
 $i \leftarrow 2$
while $i \neq N$ & $i < |Opcode|$ **do**
 if $Opcode[i] \in CR, SR$ & $|OCSet| \geq 4$ **then**
 Return False
 end if
 $OCSet += Opcode[i]$
 $i \leftarrow i + 1$
end while
Return $i == N$ & $4 \leq |OCSet| \leq 10$
#At least 4 different Opcodes needed to complete handshake. In total 10 Opcodes defined by the protocol.

```
+int buffer_reverse (struct buffer *buf) {  
+ int len = BLEN(buf);  
+ if ( len > 2 ) {  
+   int i;  
+   uint8_t *b_start = BPTR (buf) + 1;  
+   uint8_t *b_end   = BPTR (buf) + (len - 1);  
+   .....  
+ }
```

Figure 4: XOR-Patch that leaves first byte un-reversed



Surveillance and targeted attacks



Let C be the RSA encryption of 128-bit AES key k with RSA public key (n, e) . Thus, we have

$$C \equiv k^e \pmod{n}$$

Now let C_b be the RSA encryption of the AES key

$$k_b = 2^b k$$

i.e., k bitshifted to the left by b bits. Thus, we have

$$C_b \equiv k_b^e \pmod{n}$$

We can compute C_b from only C and the public key, as

$$\begin{aligned} C_b &\equiv C(2^{be} \pmod{n}) \pmod{n} \\ &\equiv (k^e \pmod{n})(2^{be} \pmod{n}) \pmod{n} \\ &\equiv k^e 2^{be} \pmod{n} \\ &\equiv (2^b k)^e \pmod{n} \\ &\equiv k_b^e \pmod{n} \end{aligned}$$



Interested to know more?

<https://jedcrandall.github.io>
(and/or come to office hours)



Syllabus

- Link from the previous slide, or Google my name
- Slides will also be on the course website, everything else will be in Canvas
 - No Piazza or anything else like that



Three Parts of CSE 468

- Part 1: Internet and Crypto
 - Introducing this today
- Part 2: Network Intrusion Detection Systems (NIDS)
 - Deep Packet Inspection (DPI) and ways to evade it
- Part 3: Malware and Side Channels
 - Attacks on the DNS system, *etc.*



Part 1: Internet and Crypto

- What are the fundamentals of how the Internet is built that determine how we do confidentiality, integrity, and availability?
 - Or, what do rainbows have to do with network security?





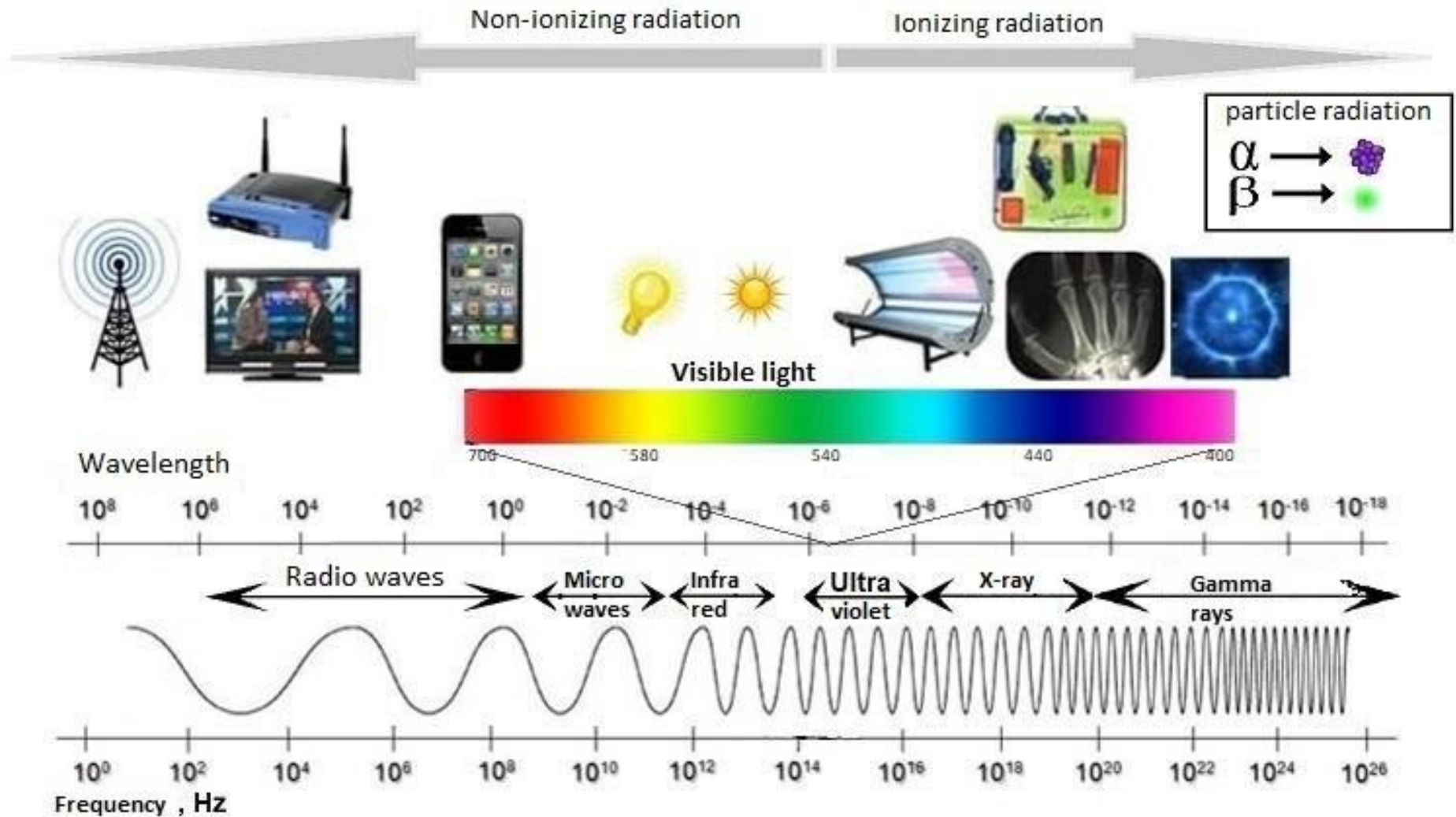


Warmth

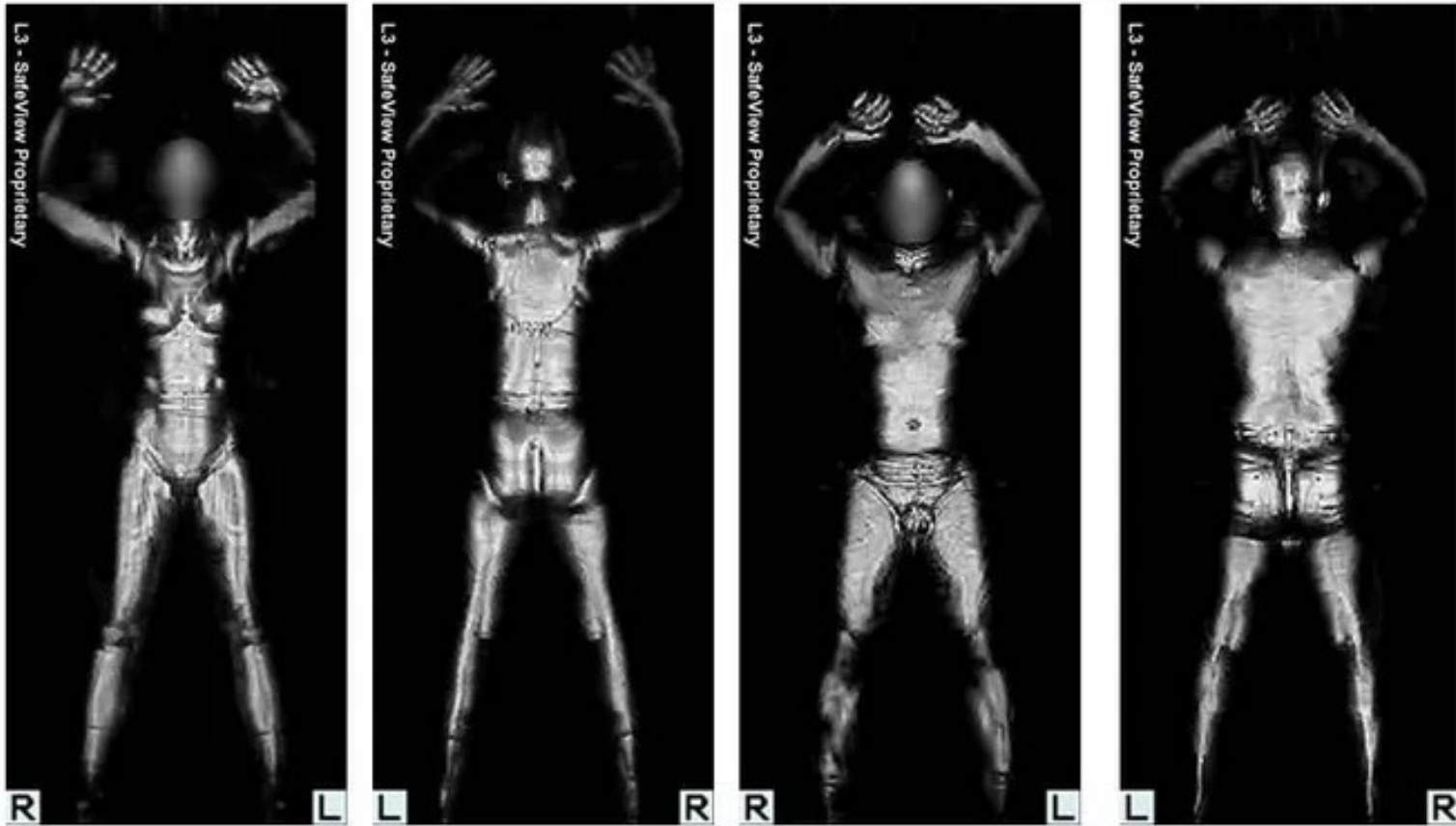
Sunburns



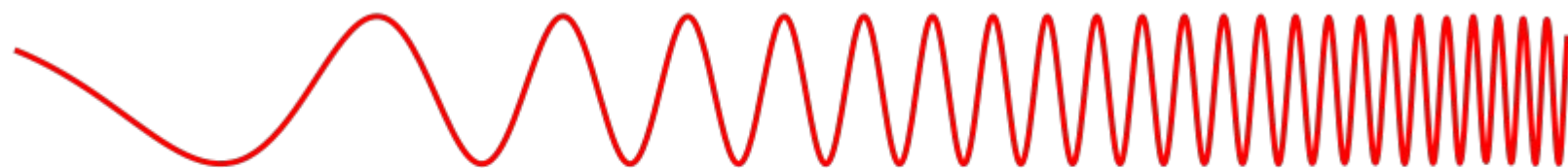
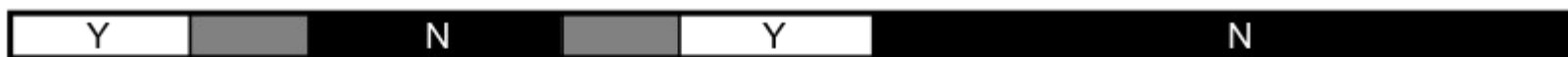
The electromagnetic spectrum



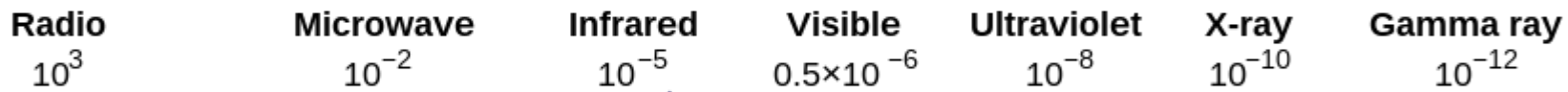
<https://www.uib.no/en/hms-portalen/75292/electromagnetic-spectrum>



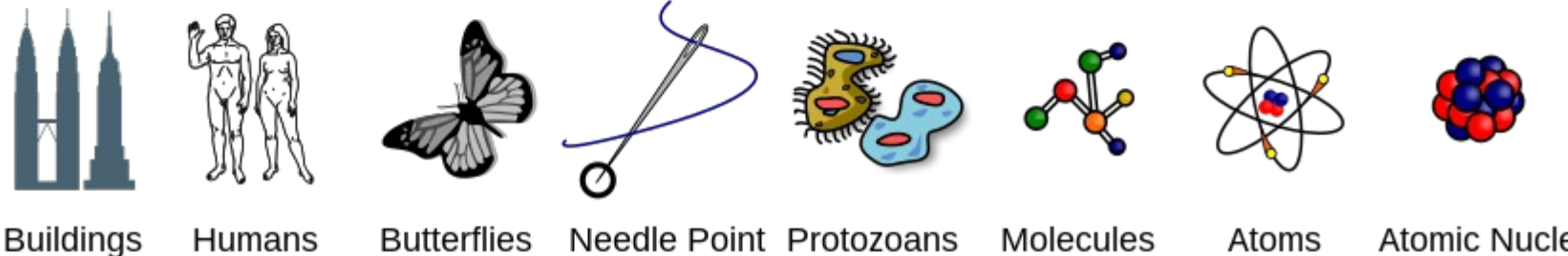
Penetrates Earth's Atmosphere?



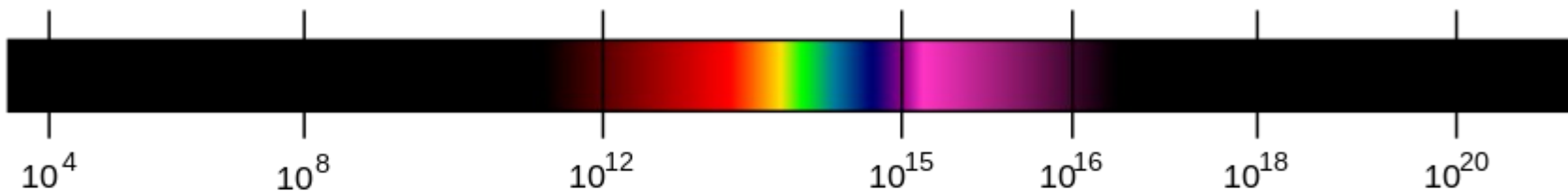
Radiation Type
Wavelength (m)



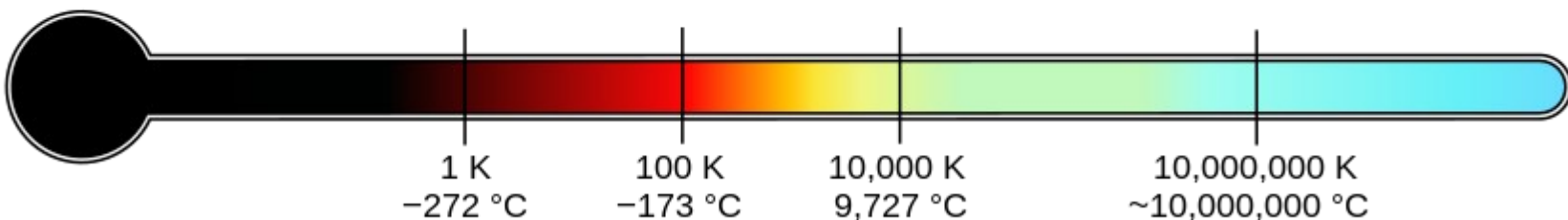
Approximate Scale of Wavelength



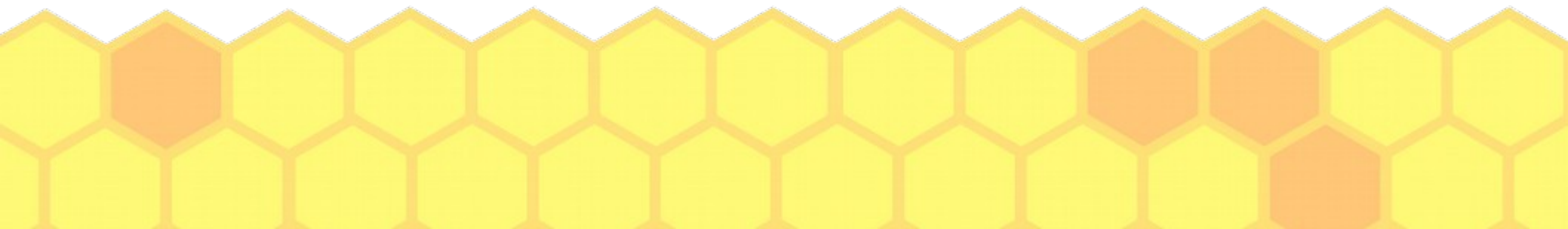
Frequency (Hz)



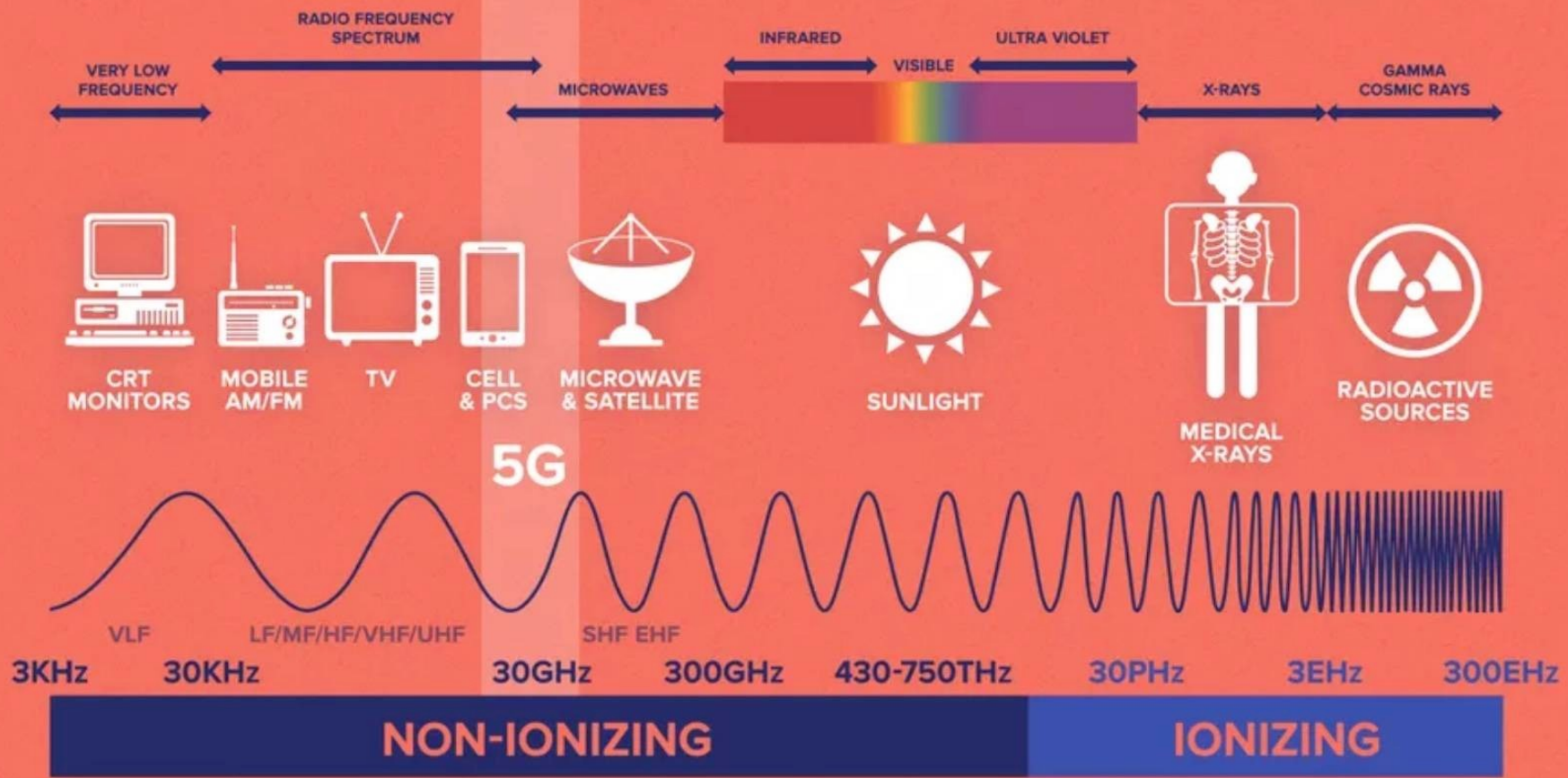
Temperature of objects at which this radiation is the most intense wavelength emitted



https://commons.wikimedia.org/wiki/File:EM_Spectrum_Properties_edit.svg



THE ELECTROMAGNETIC SPECTRUM



<https://www.islandssounder.com/news/part-i-the-hype-about-5g/>

Doctors at the X-Ray be like: "This is completely safe, don't worry"

Also doctors at the X-Ray:



Microwaves

- EHF (Sir Jagadish Chandra Bose – Bengali scientist)
30 to 300GHz
 - Point-to-point, satellite, IEEE 802.11ay (20 Gbps), security screening at the airport, 5G
- SHF – 3 to 30 GHz
 - Point-to-point, radar, satellite phones, microwave ovens, 5G
- UHF – 300 MHz to 3 GHz
 - TV, cell phones, satellites, GPS, WiFi, Bluetooth, walkie talkies, garage door openers, industrial controllers





Radio waves

- VHF – 30MHz to 300MHz
 - Line of sight, but refracted up to 100 miles or so
 - FM radio, TV, amateur radio
- HF – 3MHz to 30MHz
 - Reflected off the ionosphere
 - Military, amateur radio, maritime, CB radio
- MF – 300KHz to 3 MHz
 - AM radio, maritime



As you go lower than 300 KHz...

- Weather, beacons, time, radio in other parts of the world, RFID, submarine communications



I'm not an expert in psychology or marketing, but I think it's safe to assume...

- Humans don't like to be fried alive
- Humans don't like their devices to have wires



In general, for practical CSE 468 purposes...

- Higher frequencies carry more information
 - We'll touch on information theory later in the semester
- Infrared and visible light cannot pass through objects (like walls)
 - Microwaves and radio waves can, basically
- Everything at a higher frequency than visible light is bad for us



Because of these reasons...

- The backbone of the Internet and servers are wired
 - Specifically, fiber optics (180 THz to 330 THz)
 - Need blessings from governments to bury the wires
 - Confidentiality: Light is **easy** to copy
 - Integrity: Light is **hard** to change in transit
 - Availability: Censorship, throttling, and shutdowns



Because of these reasons...

- The other (not servers) edges of the network (*i.e.*, people and their devices) are increasingly wireless
 - Need blessing from governments to use broadcast frequencies
 - Easy to find a high-powered transmission (see *Pump up the Volume*)
 - Attackers can receive and transmit at any frequency
 - Governments (*e.g.*, local law enforcement), stalkers, cartels, human traffickers, financially motivated attackers, nosy neighbors, *etc.*
 - Eavesdropping (C), spoofing (I), jamming (A)



We need cryptography

- Make your messages sent and received over the Internet unreadable to eavesdroppers (**confidentiality**)
 - Hide metadata about who you're talking to and what you're doing to evade censorship (**availability**)
- Make sure your messages sent and received over the Internet are not modified (**integrity**)



Crypto is more than “CIA”

- Non-repudiability
- Perfect forward secrecy
- Backward secrecy (*a.k.a.* future secrecy)
- Deniable encryption
- ...



Alternatives to crypto



- Code division multiple access (CDMA)
 - Invented (in the U.S., at least) by Hedy Lamarr (basically)
- Information theory, randomized algorithms, *etc.*
 - Currently not practical in terms of solving all our problems
- Line-of-sight, directional antennae
 - Not entirely practical for security reasons, but increasingly common for other reasons
 - Line of sight attacker (*e.g.*, drone or in the Internet backbone)



CSE 468 Computer Network Security

Practical network security exposure and hands-on experience about basic security concepts, case studies and useful tools.



This semester

- Studying PCAPs to understand...
 - **Why** things (e.g., header fields and payloads) are encrypted/obfuscated the way they are
 - **Why** everything is about to change
 - **Why** deep packet inspection (DPI) is not straightforward
- Because we care about fundamentals, *i.e.*, the “**why**” part, we won’t be able to avoid...
 - Computational complexity, abstract algebra, quantum physics, relativity, classical physics

