CSCI 3330 Cybersecurity

Word of the day

ZEN vt. To figure out something by meditation or by a sudden flash of enlightenment. Originally applied to bugs, but occasionally applied to problems of life in general. “How'd you figure out the buffer allocation problem?” “Oh, I zenned it.” Contrast grok, which connotes a time-extended version of zenning a system. Compare hack mode. See also guru.

Cross-site request forgeries (CSRF)

- Same origin policy: scripts from one origin should not be able to read or manipulate content from another origin

Cross-site request forgeries (CSRF)

- Same origin policy: scripts from one origin should not be able to read or manipulate content from another origin
- But… you can still submit content

Demo

- https://jeffreyknockel.com/csrf.html
- https://tildesites.bowdoin.edu/~j.knockel/gradebook.php

Mitigations

- CSRF tokens
- Sec-Fetch-Site
  - cross-site
  - same-origin (same scheme, host, and port)
  - same-site (same pay-level domain)
  - none

SQL conditional statements

- CASE
  - WHEN … THEN …
  - WHEN … THEN …
  - …
  - ELSE … [optional]
- END

SQL subqueries

- SELECT * FROM table WHERE foo = (SELECT column FROM anotherTable WHERE bar = ?)

SQL introspection

- SELECT name FROM sqlite_schema WHERE type = "table";
- SELECT sql FROM sqlite_schema WHERE name = "nuclear_codes";
- https://brainhammer.com/sqlplayground/

Worms

Worms

- Virus: requires human interaction to spread
- Worm: self-replicating over a network
- Can grow exponentially!

Worms

- XSS meets the task
- Samy: MySpace worm that automatically added Samy as your friend

What is useful in Javascript?

- What is useful in Javascript for creating worms?

What is useful in Javascript?

- Read from the page (innerHTML, innerText, …)
- Create elements (innerHTML, createElement)
- Create changes

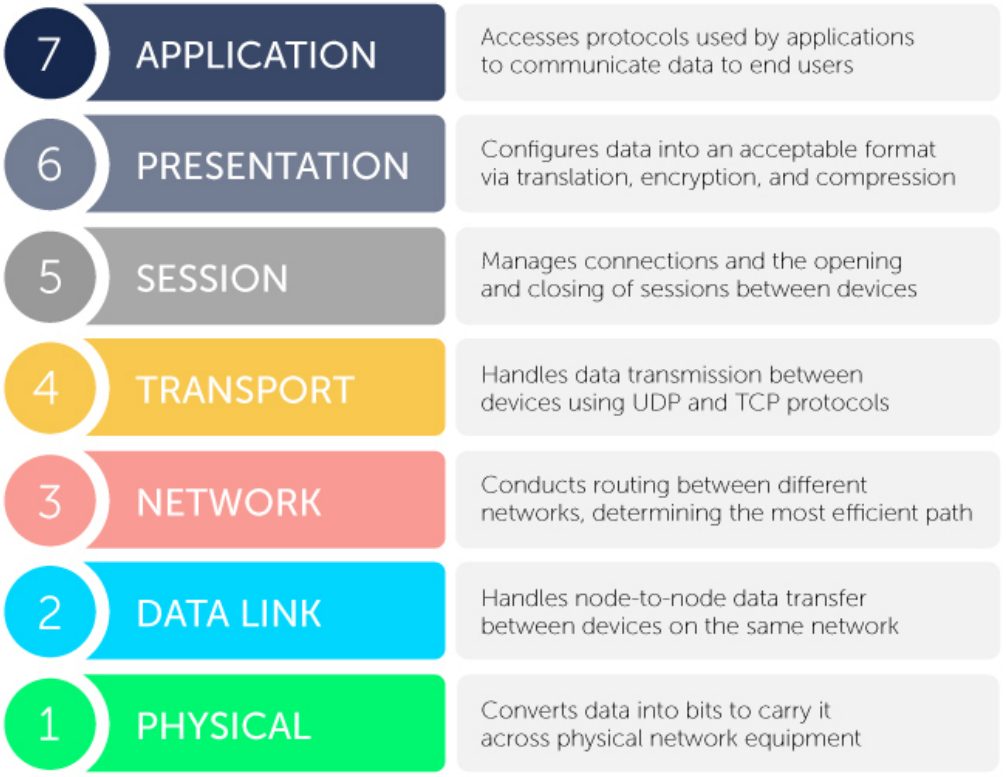
Worms

- Exponential spread… how do they know when to stop?
- ???
- ???
- ???

Worms

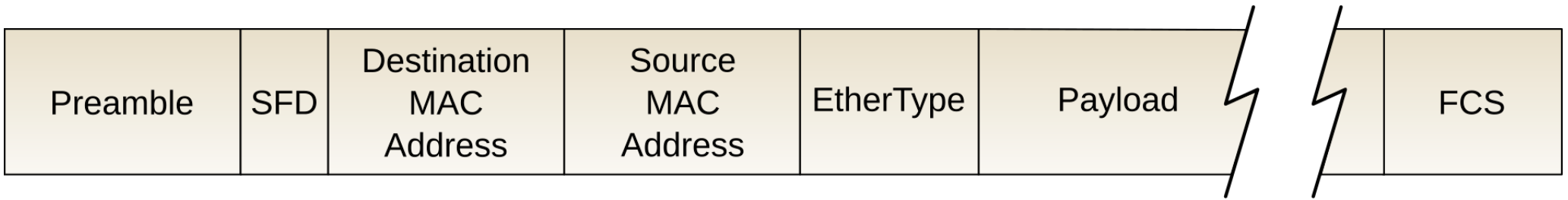
- Exponential spread… how do they know when to stop?
- Make change (e.g., MySpace profile)
- External coordination
- TTL (e.g., Stuxnet)

Network layers (OSI model)

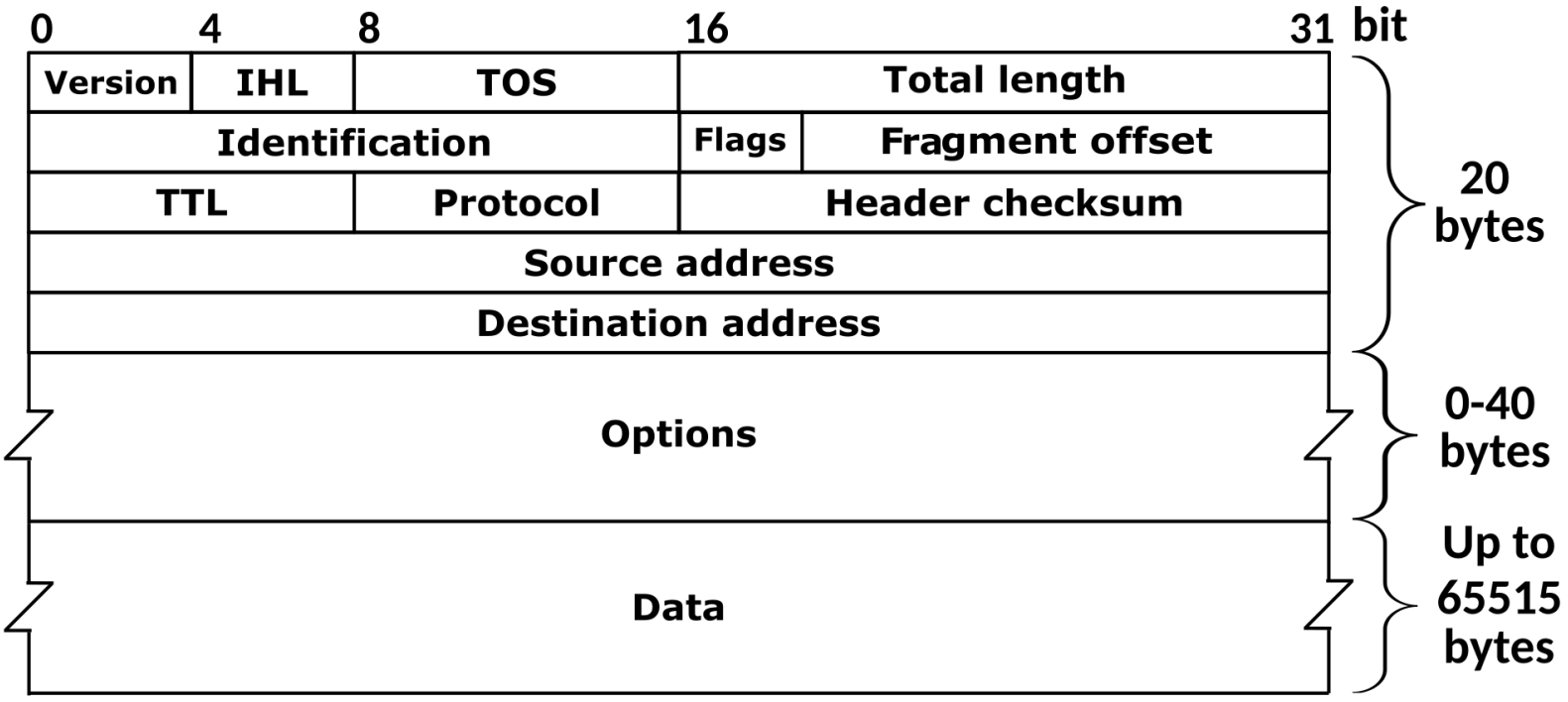


- Layer 8: user layer / political layer / etc.
- Often the most problematic layer…

Ethernet: Layer 2



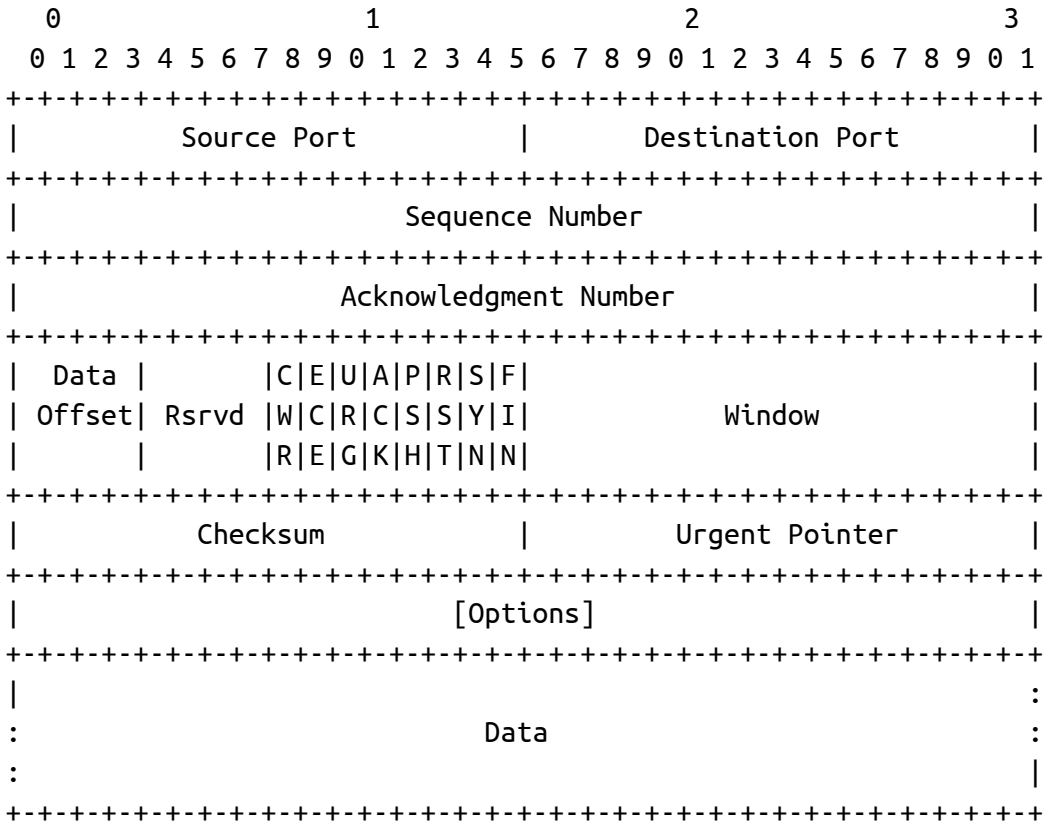
Internet protocol (IP): Layer 3



Notable fields

- Total length (max 65515)
- TTL (time to live)
- Identification / fragment offset
  - Fragments are keyed by (src addr, dst addr, protocol #, and IP id)

Transmission Control Protocol (TCP): Layer 4



Notable fields

- Sequence / acknowledgment #s
- Flags
  - SYN / ACK / FIN / RST
- Source/destination ports
  - Open ports / closed ports / filtered

Assignment 3

- Deadline: October 2, 2025, 10:00pm
- Unix permissions, SQL, and SQL injection vulnerabilities
  https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment3.pdf

Assignment 4

- Deadline: October 13, 2025, 10:00pm
- Advanced SQL information inference https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment4.pdf