Software Engineering Internship

Day #3

July 2024

Titanium Forest

Agenda

- Monday
  - Welcome & Orientation
  - Software Engineering & Version Control
  - Understanding APIs
  - Equity Evaluator project
- Tuesday
  - Javascript & React
  - ~~Directus CMS Intro~~
- Wednesday
  - Kanban
  - Cybersecurity Primer
  - Javascript & React Coding Time
- Thursday
  - SQL Databases
  - Directus CMS Intro

Kanban

What is Kanban?

Kanban is a visual workflow management method.

Originated in manufacturing, adapted for software development.

Focuses on continuous delivery without overburdening the team.

One of the Agile development methodologies.

Key Principles of Kanban

Visualize Work: Use a Kanban board to show tasks.

Limit Work in Progress (WIP): Prevents overload by limiting the number of tasks in progress.

Focus on Flow: Ensure smooth progress of tasks from start to finish.

Continuous Improvement: Regularly improve processes based on feedback.

The Kanban Board

Columns: Represent stages of work (e.g., To Do, In Progress, Done).

Cards: Represent individual tasks or work items.

WIP Limits: Set maximum number of tasks per column.

Example Kanban Board

Example of a Kanban Board

To Do: List of tasks to be started.

In Progress: Tasks currently being worked on.

Review: Tasks awaiting approval or testing.

Done: Completed tasks.

Benefits of Using Kanban

Flexibility: Adaptable to changes and new priorities.

Efficiency: Reduces waste and improves productivity.

Transparency: Everyone can see the work status.

Collaboration: Encourages teamwork and communication.

Introduction to Cybersecurity

Agenda

Define Cybersecurity and the CIA triad

Learn about tools & techniques used to secure environments

Understand the how’s, why’s, and what’s of cybercrime

Do some activities & exercises

Cybersecurity

The practice of ensuring the confidentiality, integrity, and availability of a computer system by managing and applying different tools, techniques, and procedures.

The CIA Triad

INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Confidentiality: restrict access to appropriate people and programs

Integrity: keep programs and data as they should be, and keep track of what's happening

Availability: ensure systems are accessible and working

Confidentiality

Restrict access to appropriate people and programs

Sneakers (1992)

Authentication vs Authorization

Authentication: Are you who you claim to be?

Authorization: Are you allowed to be here?

Confidentiality: Tools & Techniques

- Authentication: proving identity
  - Strong & unique passwords
  - Password managers
  - Multi-Factor Authentication (MFA)
  - Sharing is not caring
- Authorization: validating permission
  - Principle of least privilege
  - Role-based access control (RBAC)
- Encryption: Scrambling messages so they can't be read by others

Unscrambling Encryption

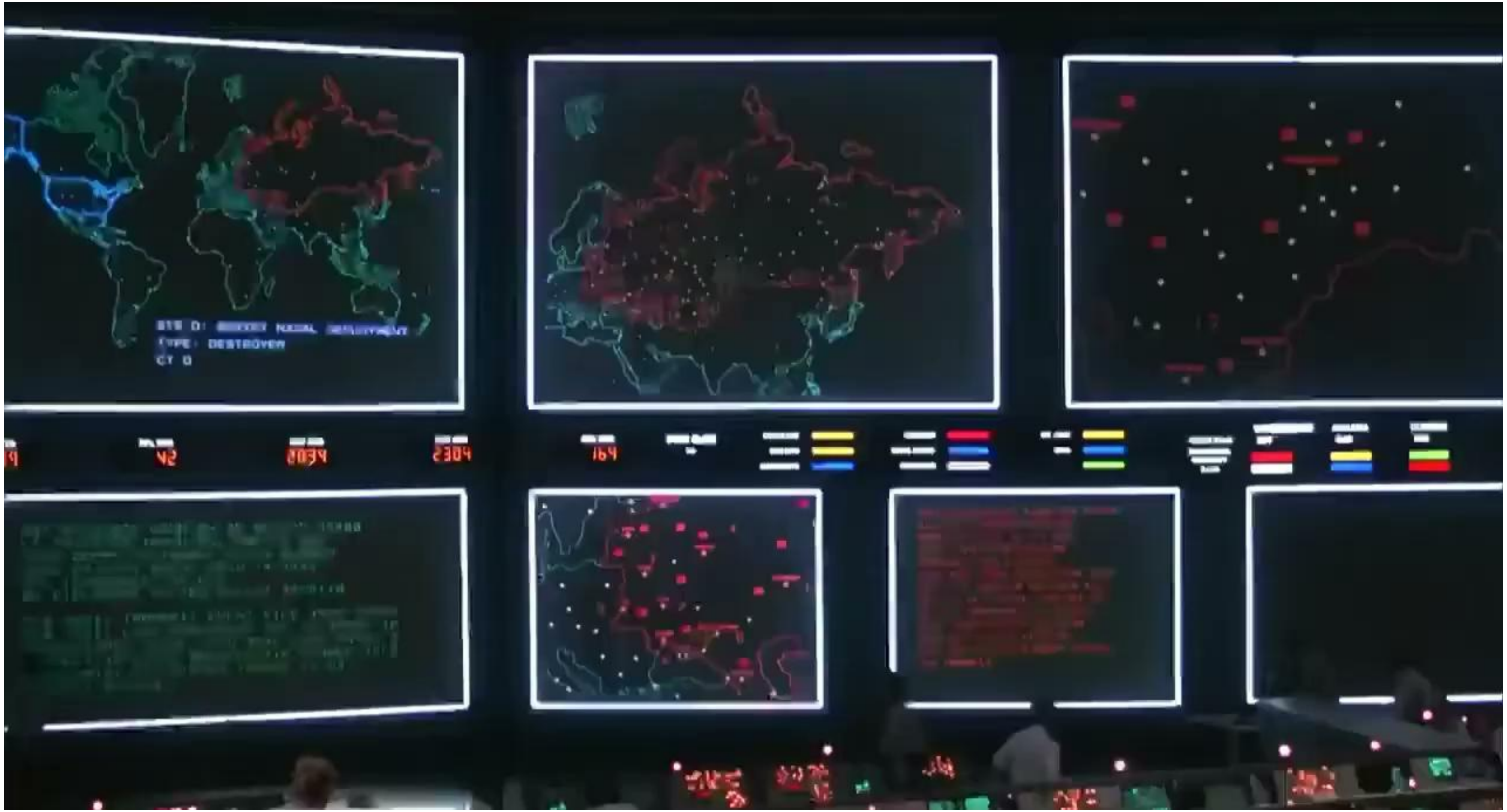
- Encryption: plaintext + key → ciphertext; decryption: ciphertext + key → plaintext
- Changing the key results in different ciphertext

```
"Hello, world" + "this is 1 key" = U2FsdGVkX18+VPzjAO1aD+S48GSz5Yxxxarv60y7ynI=
"Hello, world" + "a key this is" = U2FsdGVkX19SM+nJQJzlKeimL2WTOTdjJeOUOi4Ulkw=
```

- "At rest" vs "in transit"
- Symmetric key encryption: single key for encryption & decryption
  - How do you share the secret key?
- Asymmetric or Public key encryption
  - Pair of keys (public & private) used: encrypt with one, but decrypt with the other
  - Applications: certificates, digital signatures

Integrity

Keep programs and data as they should be, and keep track of what's happening



War Games (1983)

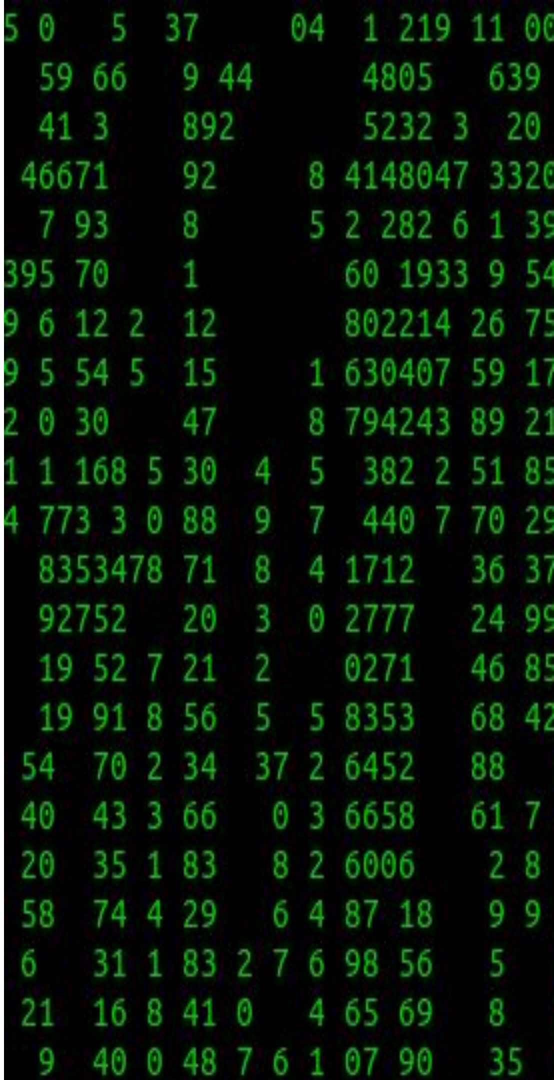
Integrity: Tools & Techniques

Change control processes & procedures

Logging and auditing

Anti-virus & anti-malware software

Hashing algorithms: generate a "fingerprint" of data, files, or programs



Dude, what the hash?!

- Generates a "fingerprint" that represents the input data
- You don't want collisions in cars...or hashing algorithms!
- Michael's Dumb Hash (MDH) - sum up the order of the letters in the alphabet

MDH

```
CAT ON HAT = 3 + 1 + 20 + 15 + 14 + 8 + 1 + 20 = 82
HELLO = 8 + 5 + 12 + 12 + 15 = 52
HAT ON CAT = 8 + 1 + 20 + 15 + 14 + 3 + 1 + 20 = 82
```

Real

```
sha1(CAT ON HAT) : 013279442a97e8b3ff301b9888c04610926de4a3
sha1(HAT ON CAT) : 0ae3d3bcd0f83683d520130b558d177d030e71fc
sha256(CAT ON HAT): f70dcf829b87c12c3da8e1bb0ad4a4581380f70219c4a0c70c2110673ced17b8
sha256(HAT ON CAT): dab9174f6f75f42b9da826affd807a40d44337085434444f3eaf002087b020980
```

Is hashing a form of encryption?

Hashing != Encryption!!!

If you have a hash, there is no way to turn it back into the input data!

(At least not without brute force)

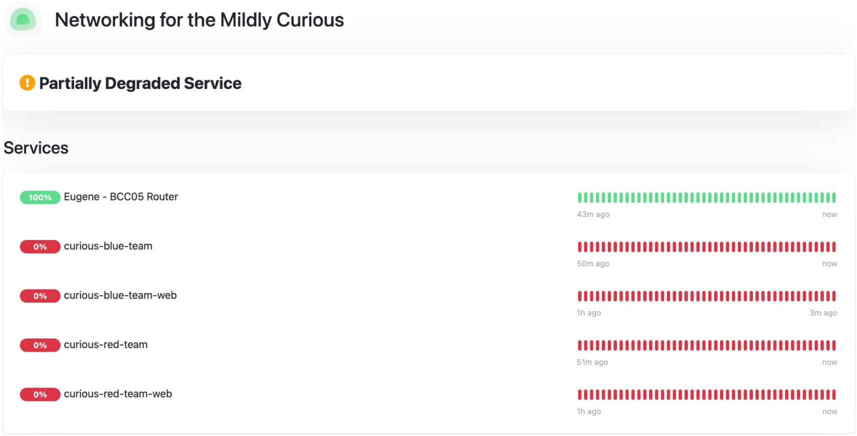
Availability

Ensure systems are accessible and working

The Matrix Reloaded (2003)

Availability: Tools & Techniques

- Monitoring
- High availability (HA)
- Backups
- Disaster recovery (DR)
- Testing
  - DR tests
  - Table top exercises



Networking for the Mildly Curious

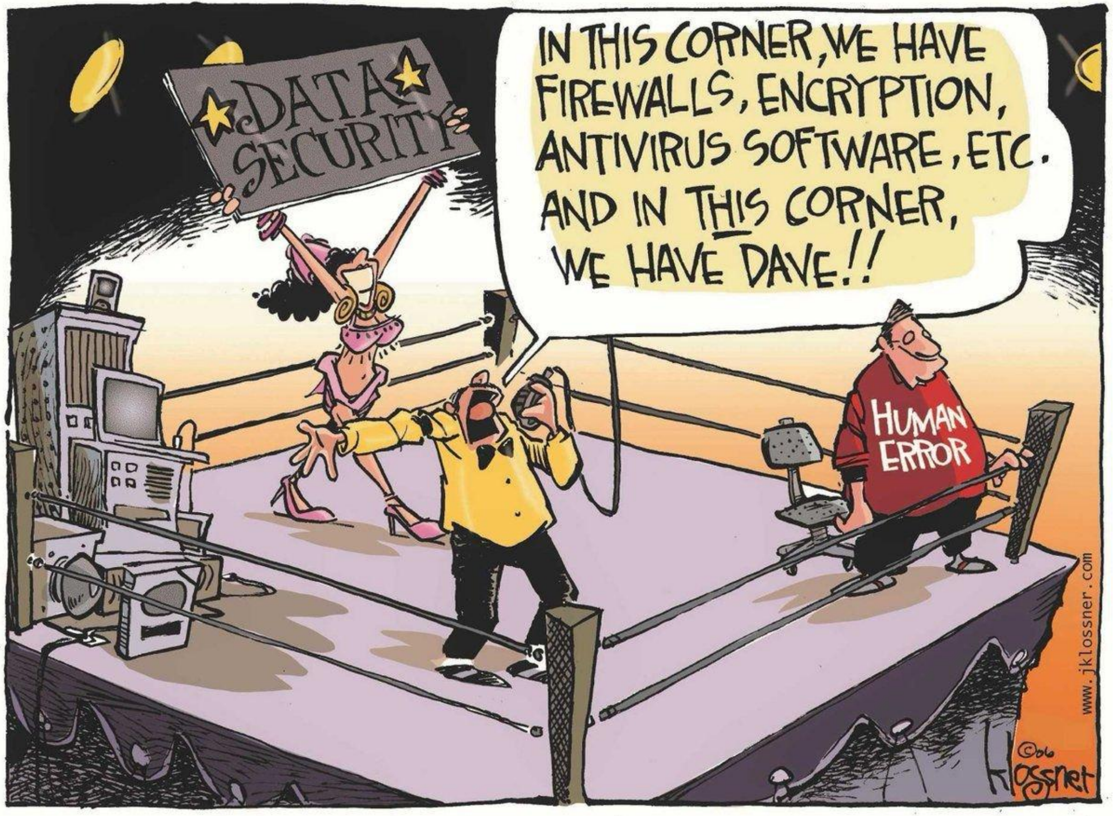
Partially Degraded Service

Services

100%	Eugene - BCC05 Router	43m ago	now
0%	curious-blue-team	50m ago	now
0%	curious-blue-team-web	1h ago	3m ago
0%	curious-red-team	51m ago	now
0%	curious-red-team-web	1h ago	now

General Tools & Techniques

- Firewalls
- Policies & regulations
- 3rd party reviewers: auditors, penetration testing (pentests)
- Secure development lifecycle & "shifting left"


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Dave

Cybercrime

Hackers (1995)

Why do people do it?

- Money
- Power
- Money and Power

Common Cybercrimes

- Malware: ransomware, adware, spyware, trojans, keyloggers, botnets
- Phishing: spear/whale phishing, SMiShing, social engineering
- Identity attacks: brute-force, credential stuffing, man-in-the-middle (MiTM), SIM cloning
- Injection attacks: SQL injection, cross-site scripting,"0 day"
- Advanced persistent threats (APT), supply chain attack
- Denial of Service (DoS), distributed Denial of Service (DDoS)
- Insider threats

Simple Cybersecurity Toys

https://cybernerds.infrastructuresquad.com/