Session 4

Ask An Old Guy

October 21, 2024

michael@barrow.me

What We'll Cover

---

1. Understanding IT Career Paths & Industry Evolution
2. Soft Skills, Communication, and Adapting to Change
3. Troubleshooting Strategies and Project Management
4. Cybersecurity
5. Computer Networking
6. Managing Technical Debt, Effective Escalation, and Scalability/Resilience
7. Vendor Selection, Ethics, Learning from Failure, and Open Source Participation

Cybersecurity

Goals for Today

- 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

Confidentiality: restrict access to appropriate people and programs

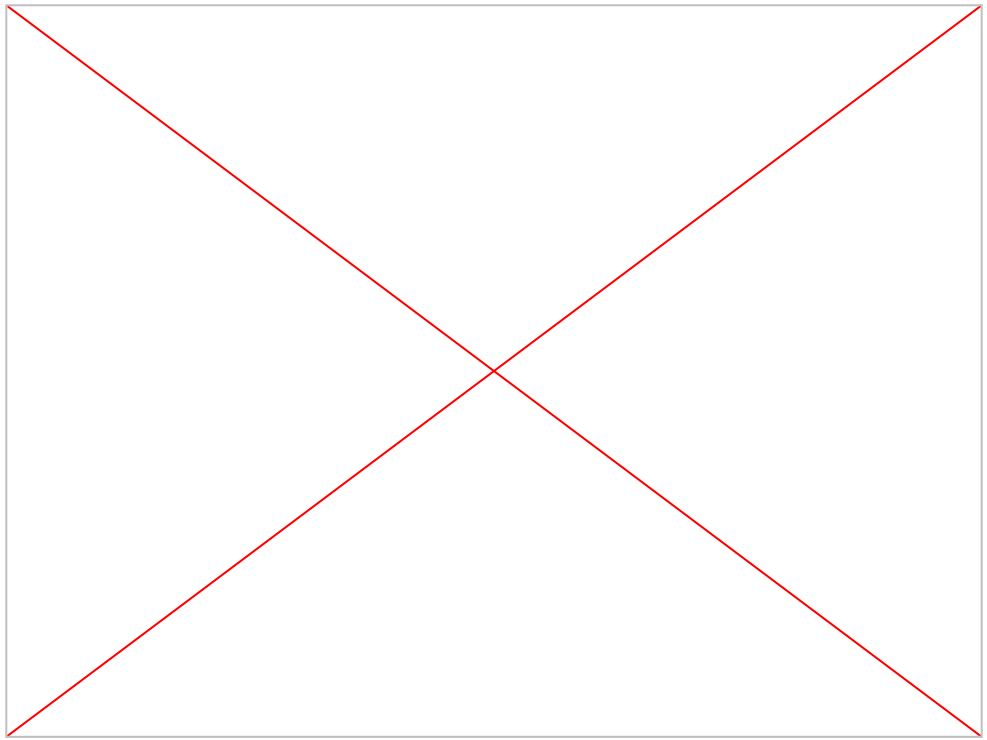
Integrity: keep programs and data as they should be, and keep track of what's happening

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

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

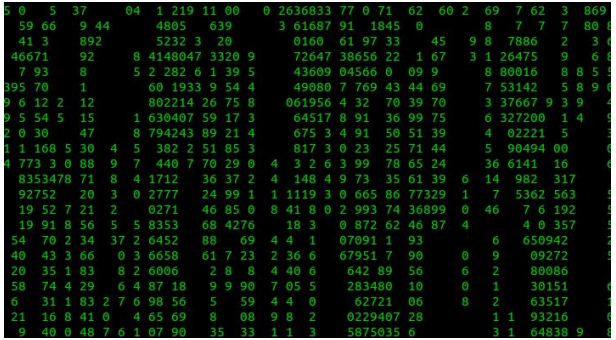
- "At rest" vs "in transit"
- Symmetric key encryption: single key for encryption & decryption
  - How do you share the secret key?
- Asymmetric or Public key encryption
  - Pair of keys (public & private) used: encrypt with one, but decrypt with the other
  - Applications: certificates, digital signatures

Integrity

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

WarGames (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 of alpha order

```
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 hashes are way better than MDH!

```
sha1(CAT ON HAT)  : 013279442a97e8b3ff301b9888c04610926de4a3
sha1(HAT ON CAT)  : 0ae3d3bcd0f83683d520130b558d177d030e71fc
sha256(CAT ON HAT): f70dcf829b87c12c3da8e1bb0ad4a4581380f70219c4a0c70c2110673ced17b8
sha256(HAT ON CAT): dab9174f6f75f42b9da826affd807a40d4433708543444f3eaf002087b020980
```

So, hashing is a form of encryption, right?

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

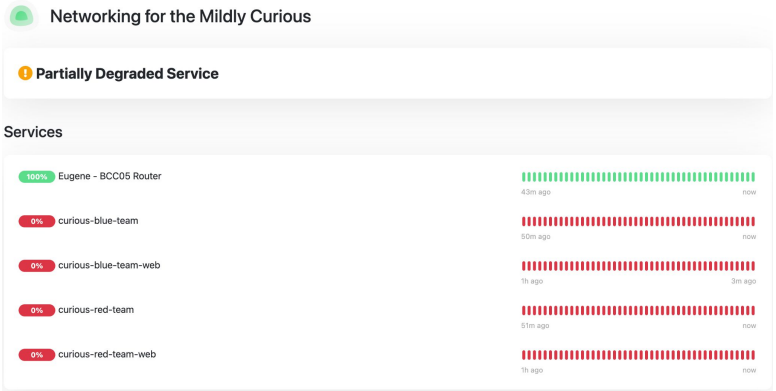
Availability

Ensure systems are accessible and working

The Matrix Reloaded (2003)

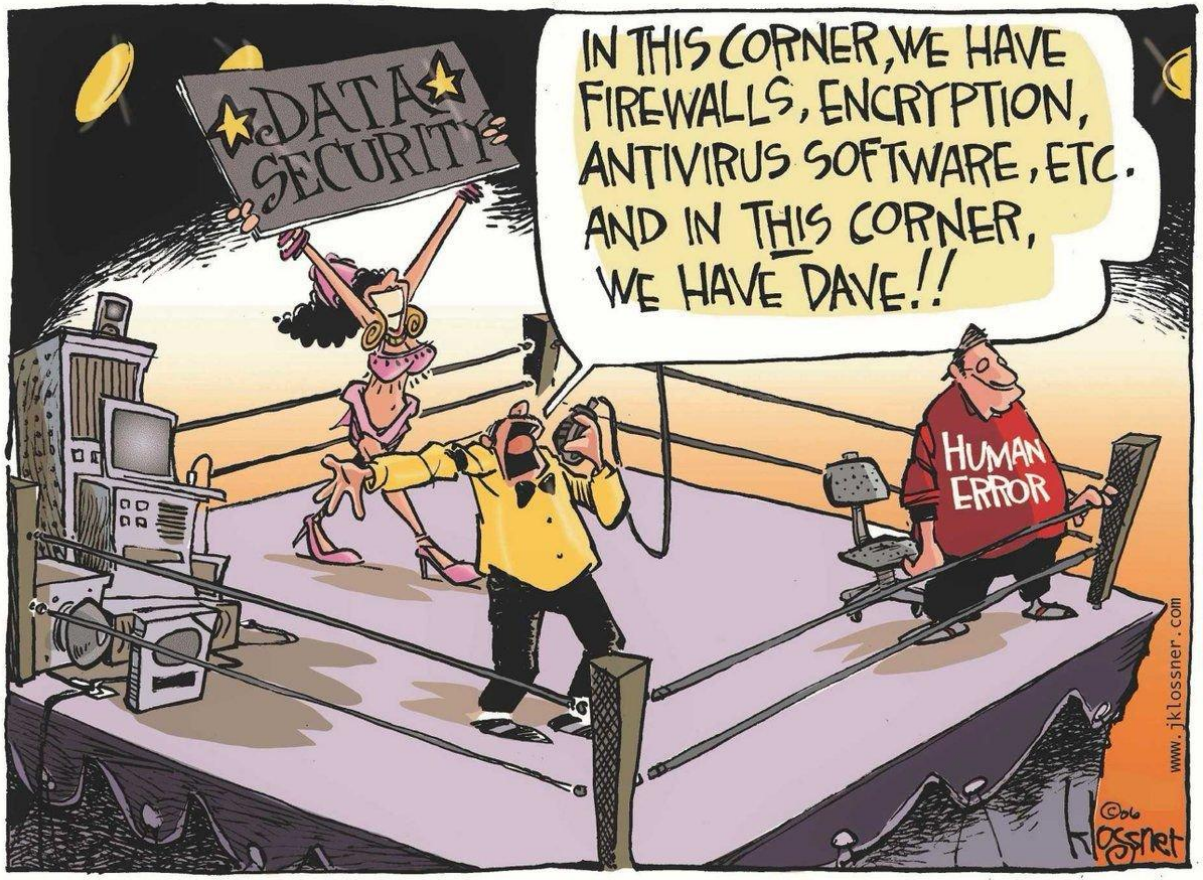
Availability: Tools & Techniques

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



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
JKLossner

Dave

Cybercrime

Why do people do it?

- Money
- Power
- Money & 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

Let’s Play!

Ask an old guy!