SEMtech!

Student Engagement & Mentoring in Technology

Activity 1: "Who Gets In?" – The AAA+N Simulation Game

Objective: Walk through and *experience* each step of the AAA+N model using a live-action simulation.

How it works:

1. Create a "secured resource" zone (classroom corner, digital system mockup).
2. Assign roles:
    - **User** (trying to gain access)
    - **System Guard** (performs Identification + Authentication)
    - **Access Manager** (handles Authorization)
    - **Logger** (Accounting)
    - **Auditor** (Nonrepudiation review)

Steps:

- The User states their identity (Identification).
- Provides ID or password (Authentication).
- The Access Manager checks permissions (Authorization).
- The Logger writes down the attempt (Accounting).
- The Auditor verifies logs match the claimed actions (Nonrepudiation).

Debrief Discussion:

- What happens if a step is skipped?
- What could go wrong without accounting or nonrepudiation?

STEM Linkage: Builds system design and access policy fluency—foundational for cybersecurity roles, digital auditing, and compliance analysis.

Activity 2: "Access Control Puzzle" – AAA+N Card Challenge

Objective: Reinforce distinctions between Authentication, Authorization, Accounting, and Nonrepudiation using real-life tech examples.

How it works:

- Provide each group with a deck of **scenario cards** (examples below).
- Students must match each card with the correct AAA+N concept.

Example Scenarios:

- "Entering a password on a login screen" → Authentication
- "A system determines your access to shared folders" → Authorization
- "Logs show you downloaded 12 files from a secure drive" → Accounting
- "Digital signatures confirm you approved a contract" → Nonrepudiation

Twist: Add **"Red Herring" cards** to provoke deeper discussion (e.g., "Typing your name in a form" – is that really authentication?).

STEM Linkage: Sharpens analytical thinking and encourages precision in evaluating digital interactions—essential for system architects and security analysts.

Activity 3: "Incident Response: Who Did It?" – A Forensic Investigation Lab

Objective: Apply Accounting and Nonrepudiation by solving a breach through access log analysis.

Scenario:
"A secure financial report was accessed without authorization at 2:13 PM. You must determine **who accessed it**, whether they were **authenticated and authorized**, and whether they can **deny involvement**."

How it works:

- Provide a mock access log:
  - Username, login time, IP address, actions taken
- Include:
  - A digital signature trace or system event
  - A list of authorized users

Students work in teams to:

- Identify the user responsible
- Determine if proper authentication & authorization occurred
- Examine log integrity (Accounting)
- Decide if sufficient evidence supports Nonrepudiation

SEMtech!
Student Engagement & Mentoring in Technology

Debrief Questions:

- How did you use each element of AAA+N?
- Could the user claim they didn't access the file? Why or why not?

STEM Linkage: Builds investigation and compliance skills—core to digital forensics, SOC roles, and secure system design.

Final Bonus: AAA+N Summary Poster Creation

Wrap the unit by having students design a **visual one-pager** or infographic summarizing:

- What each concept means
- A real-world example
- Why it matters for data integrity and security

They can post it in the classroom or add it to a cybersecurity portfolio.