Access Management: A Warm-Up

CAMP 2011

Rob Carter, Duke University

A Quick Overview - Four Questions, Three Answers

- ‘Ello, ‘ello. What’s all this, then?
- Why should I care?
- Why’s it have to be so hard?
- Anyway, whatcha gonna do about it?

What's all this then?

What's all this then?

(shameless plug)

- Internet2 Mace-Paccman effort
- Nearly four years discussing use cases, theory, strategies, vendors, solutions, best practices
- https://spaces.internet2.edu/display/macepaccman

What's all this then?

What's all this then?

- "problem" words
- paccman use case library
- access, privileges, system, information, department, group, automatic, business, role, central, hierarchy, delegate

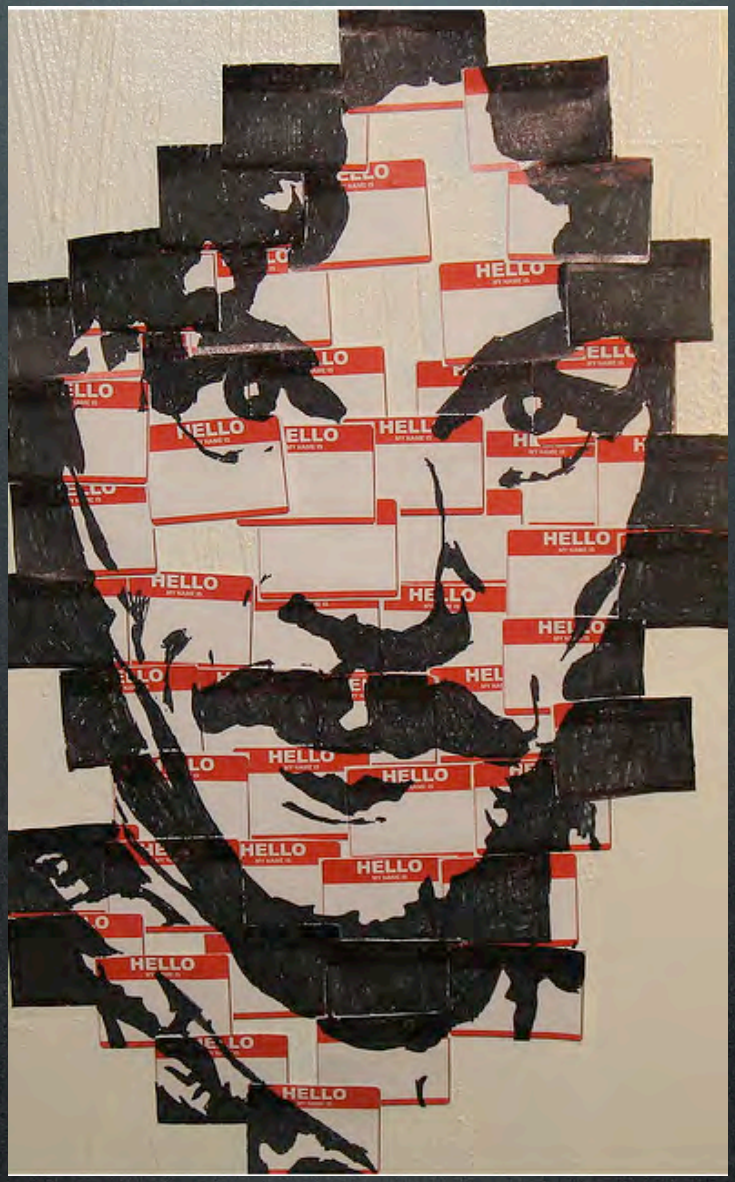
What's all this then?

- "Solution" words
- privilege, system, role, function, attribute, subject, access, group, rule, authorization
- Paccman glossary

What's all this then?

- Authentication
  - NIST: "Process of proving to a verifier that a claimant controls a token issued to a registered subscriber."
  - We: The process by which a system becomes assured of the identity of its user.

What's all this then?



What's all this then?

- Authorization
  - IT IS NOT AUTHENTICATION
  - IT IS STILL NOT AUTHENTICATION
  - Technically: The process of deciding if a subject should be allowed to act against a resource.
  - We: The process by which systems decide what an authenticated entity should be allowed to do

What's all this then?

AUTHORIZED PERSONNEL ONLY

Jack had always wondered what was beyond the forbidden door

Why should I care?

Why should I care?

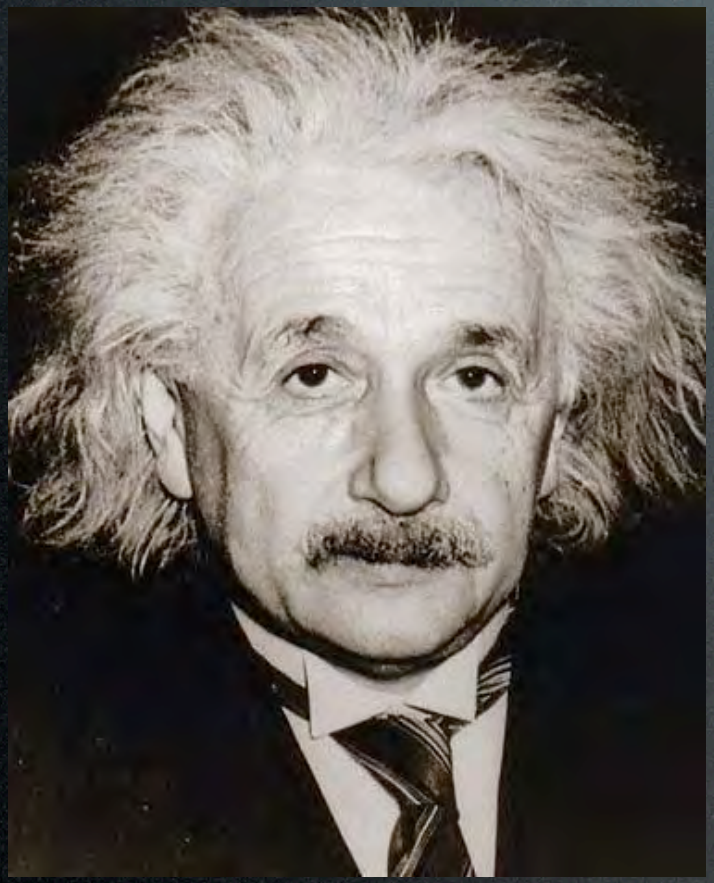
- Security and Privacy: Keeping out the rabble
- Resource Preservation and Cost Control
- Auditors, auditors, auditors
- HIPAA and FERPA and ID Theft, oh my!

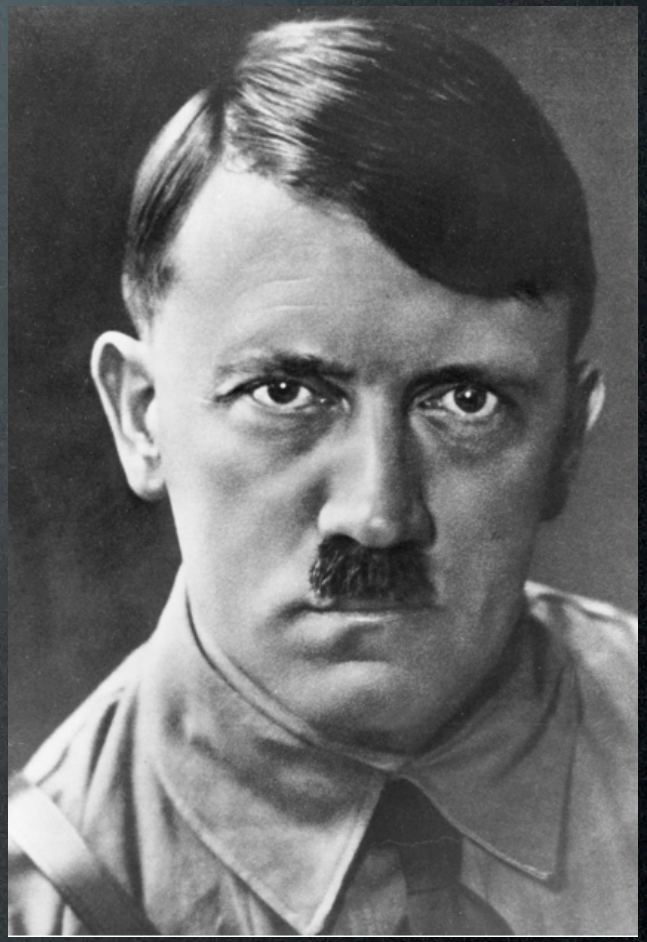
Why should I care?

- Why not equate authN = authZ?
- Some do, with adequate results...for a while...
- Sometimes, though, we may know someone **and** know better...

Why should I care?

- Consider tutoring candidates for your children:





Why should I care?

- Authorization is about limiting access, but also ensuring appropriate access
- Automation and “on time” access
- Done properly, “everything just works”
- Think of it as “rightsizing”.

Why's it have to be so hard?

- It's the nature of our institutions:
- Access Management problems tend to start out simple…
  - Students and faculty should have access to the SIS system…
- But they tend to complicate over time…

Why's it have to be so hard?

- Students and faculty should have access to the SIS system...
  - ...but faculty should only see their students...
    - ...unless the students have asserted FERPA...
      - ...and then, only during a given semester...
        - ...unless the dean approves an exception...
          - ...or the student requests a consult...

Why's it have to be so hard?

Why's it have to be so hard?

- Incremental improvement
- 80/20 rule
- Focus on laying foundations, winning hearts and minds first

Why's it have to be so hard?

Why's it have to be so hard?

- Expect push-back if authZ is a new practice in your organization
- Stress wins for users - automation, cost control
- Work up from real use cases
- Boil them **slowly**...

Anyway, whatcha gonna do about it?

- Focus for the afternoon -- what **can** we do about it?
- Before the break: Preparing for access management -- governance, policy, infrastructure (Keith Hazelton)

Anyway, whatcha gonna do about it?

- After break #1: Provisioning -- a first logical step toward privilege and access management. (maybe even **deprovisioning**?) (Jacob Farmer)
- After break #2: Deeper and more granular access management strategies -- groups and roles and privileges (oh my!) (Tom Barton)