PENNSTATE

Identity and Access Management

Friends of Penn State (FPS)

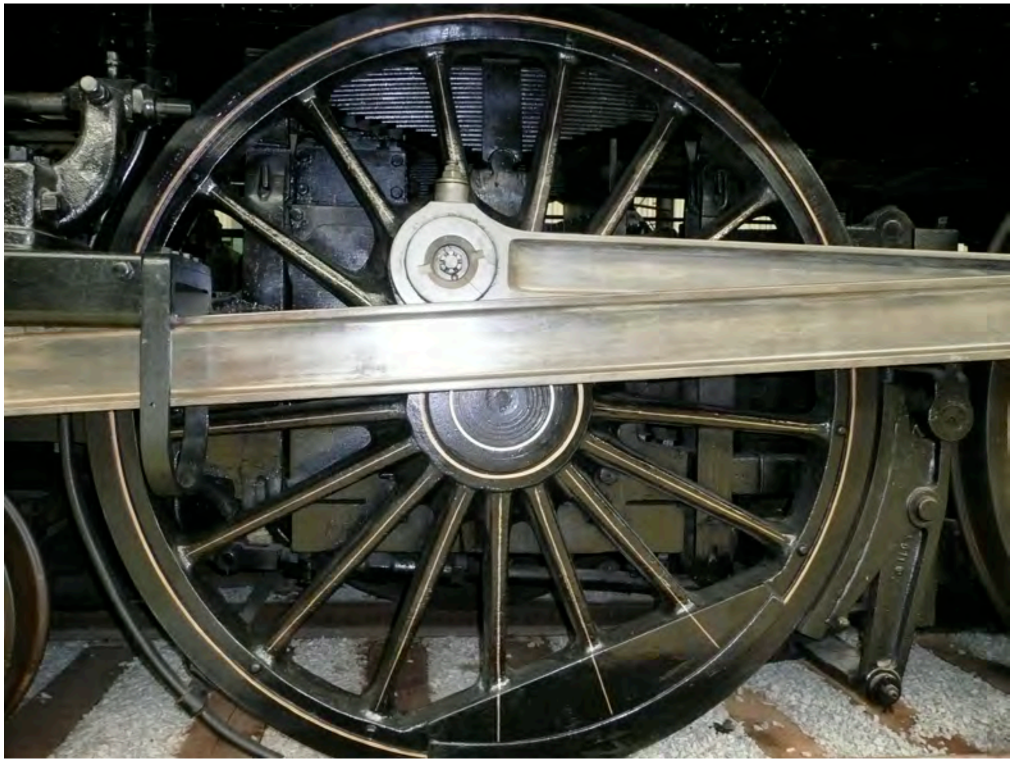
Jimmy Vuccolo, jvuccolo@psu.edu

Technical Manager

Identity and Access Management

Agenda

- FPS Overview
- Problems
- So What’s Next?

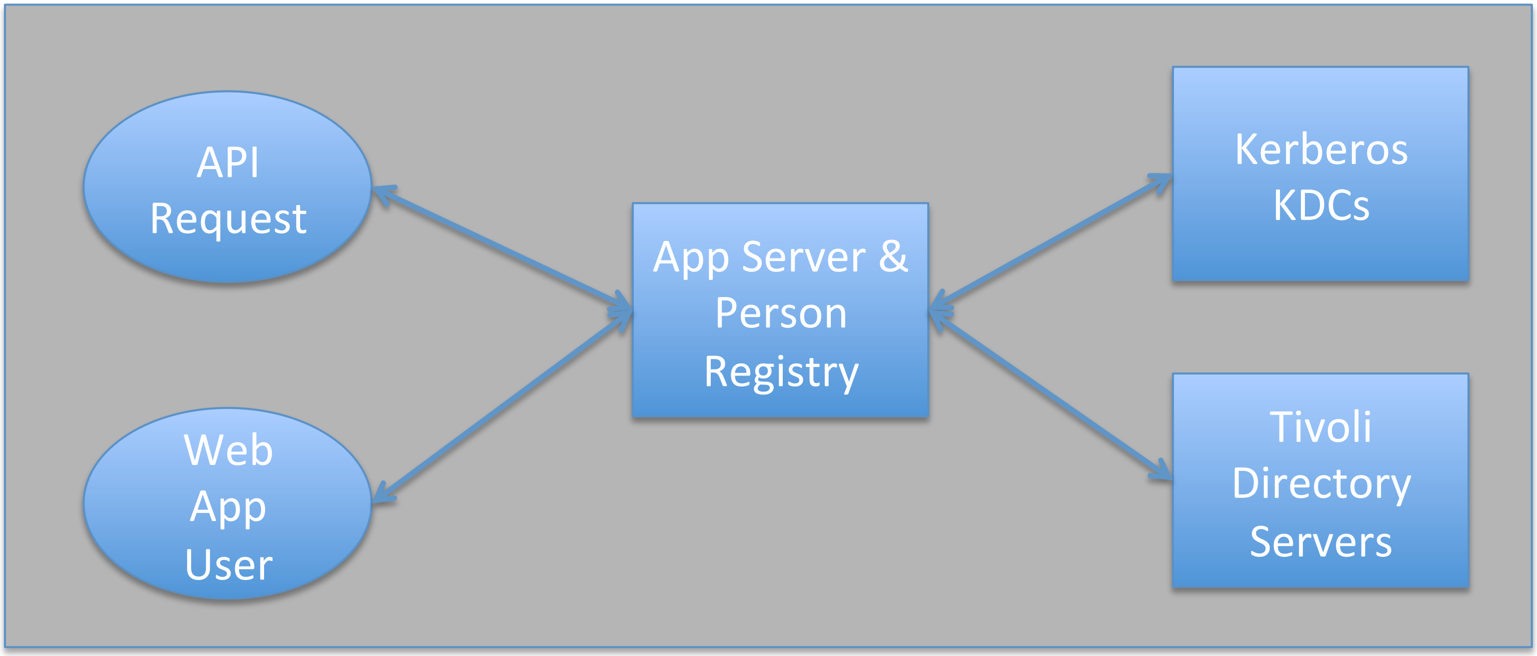


FPS OVERVIEW

What is FPS?

- An authentication system that allows users outside of Penn State to access **Web-based applications** inside of Penn State.
  - – Currently FPS has 1.6+ million identities.
  - – Features include:
    - Web-based account management system (https://fps.psu.edu/).
    - Developer APIs.

FPS Architecture



API Request

Web App User

App Server & Person Registry

Kerberos KDCs

Tivoli Directory Servers

FPS Components

- CGI Programs (https://fps.psu.edu/)
  - Create identity, change password, reset password, remove identity, update information and check identity
- HTTPS POST APIs (XML output)
  - Create identity, change password, reset password, authenticate identity, set data, get data, certify identity, un-certify identity, lock identity, unlock identity, remove identity, get all data, set all data, and remove role
- Help Desk Consultants Interface

Why did we do FPS?

- In 2004, stakeholders were moving more and more of their applications to the Web:
  - Undergraduate Admissions
  - Office of Human Resources
  - Penn State World Campus
  - And many more!
- We needed a solution to provide authentication for these applications.

How did we do FPS?

- Infrastructure at the time (IBM's DCE) used for Penn States' Access Account could not support the projected number of identities.
  - Because of that, we created a separate authentication realm, person registry and directory server.

FPS Benefits

- Mitigates risk in that FPS users cannot use wireless and computer labs.
- Provides an identity instantly as opposed to the standard University process which can take up to 1-3 days.

PENNSTATE
1855

Identity and Access Management

PROBLEMS

Data Collection

- When we started FPS, we standardized on the amount of data necessary to create an account.
- However without an established policy, stakeholders forced us to lift those requirements.
  - Today a person can obtain an FPS Account by specifying only their last name and a E-mail address.

Matching

- Each stakeholder area had their own requirements for matching users.
  - Undergraduate Admissions: first name, last name, gender, and date of birth.
  - Office of Human Resources: first name, last name, email address, postal code, daytime telephone and evening telephone number.
- We have a match appliance, but its useless because of inconsistent data collection.

Migration

- Migration is the moving between FPS and our Penn State Access Account and vice versa.
- From FPS to Access Accounts:
  - Only Undergraduate Admissions could identity which identities to migrate about 80% of the time.
- From Access Accounts to FPS:
  - Automatically migrated graduates to FPS.
  - About 10% per semester actually set up the FPS account.

Another Person Registry

- We already had a person registry for our Access Account holders, which we did not use for FPS, because of that we ran into the following problems:
  - Different/incompatible database technologies (FPS – DB2 and Access Accounts – Oracle).
  - A large number of stakeholders chose not to update their person data in FPS, so it became out of date and useless for matching.

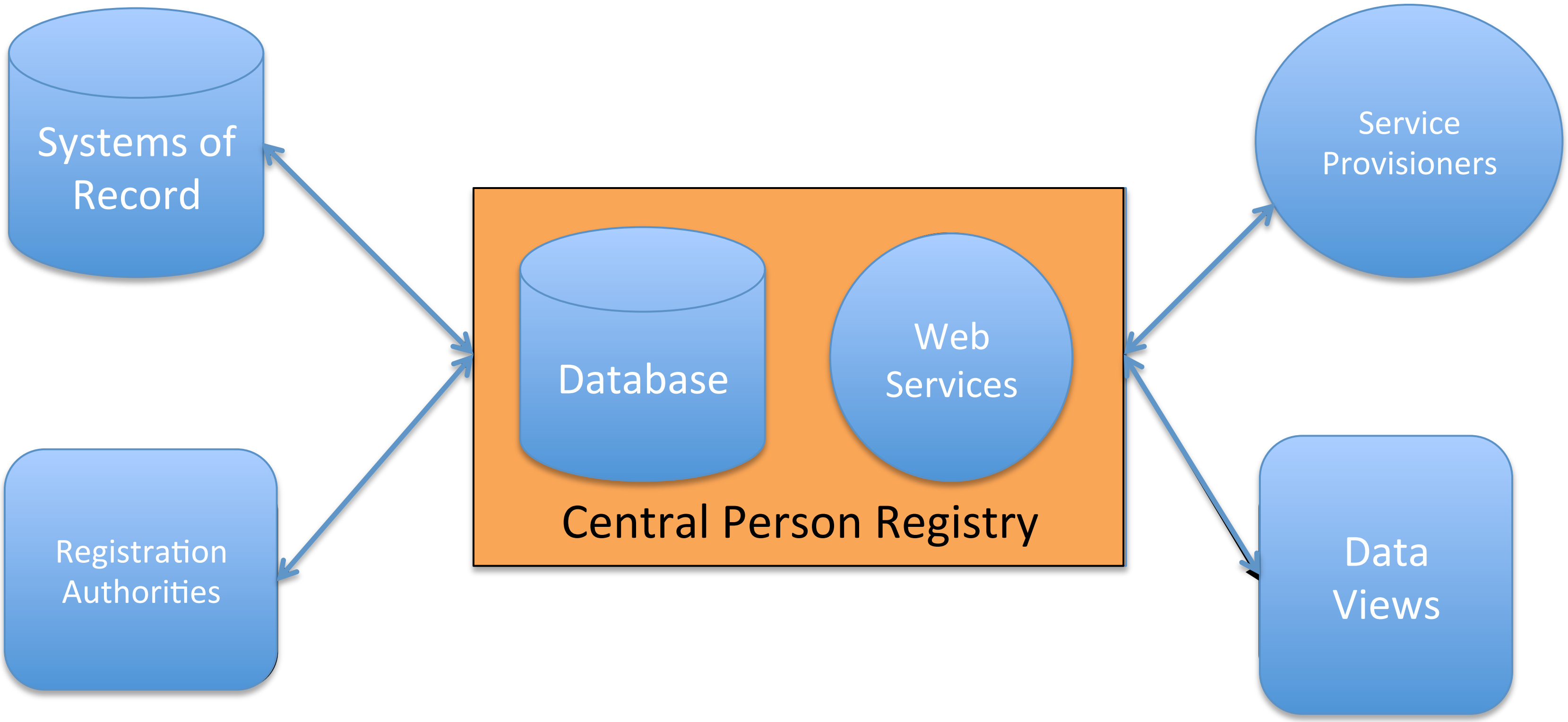
IAM to the rescue!

SO WHAT'S NEXT?

How are we fixing things?

- Penn State is currently developing a new **Central Person Registry** (CPR) that will consolidate identity information that is currently stored in separate non-integrated sources throughout the University.

CPR Architecture



PENNSTATE 1855 Identity and Access Management

HOW DOES THE NEW CPR ADDRESS FPS'S PROBLEMS?

Data Collection/Matching

- We are requiring a consistent minimum amount of data to be collected to identity a person in our registry (backed by policy).
- If the data requirements are not satisfied, the user can still exist in the registry, however they will not be used as part of our matching process.

Migration

- By extending the digital lifecycle of students and/or employees, we will no longer have a need for migration between realms.

Another Person Registry

- Yes, the CPR is another registry except it will be the only one.

WHAT ABOUT AUTHENTICATION?

Option #1

- Do another guest system, except this time:
  - Use the CPR for the registry (a single registry).
  - Use a common name space.
  - Develop a new Registration and Provisioning Process
  - Only migrate data to “prime” the CPR from FPS that we know is good, throw everything else away.

Option #2

- Convince stakeholders to embrace social media and/or other identities (OpenID).
  - CPR will store which identity the user is using.
  - This solution is a tough sell.

Option #3

- Use a combination of Option's 1 and 2 for the short-term and once a comprehensive Access Management solution is in place, provision Access Accounts for everyone.
  - Currently at Penn State AuthN == AuthZ, in the future that will change with things like IAP, affiliations and so on.

In Summary

- FPS solved a need for a guest system and helped to mitigate risk.
- With FPS comes a number of problems, like matching and data collection.
- The new Central Person Registry will solve all of FPS's problems and loads more!

Contact and Community Information

- E-Mail: iam@psu.edu
- Web Site: https://iam.psu.edu/
- Follow “PennStateIAM” on:
  - Delicious
  - Twitter
  - YouTube
  - Facebook

When the Guests Take Over the House

InCommon CAMP June 2011

Columbus, Ohio

RL "Bob" Morgan

University of Washington

Co-Chair, InCommon TAC

Topics

- Guest systems at UW
- Social<->SAML
- Why systems must grow
- NSTIC / Identity ecosystem
- Registries
- It's all about attributes

Guest-NetID Systems at UW

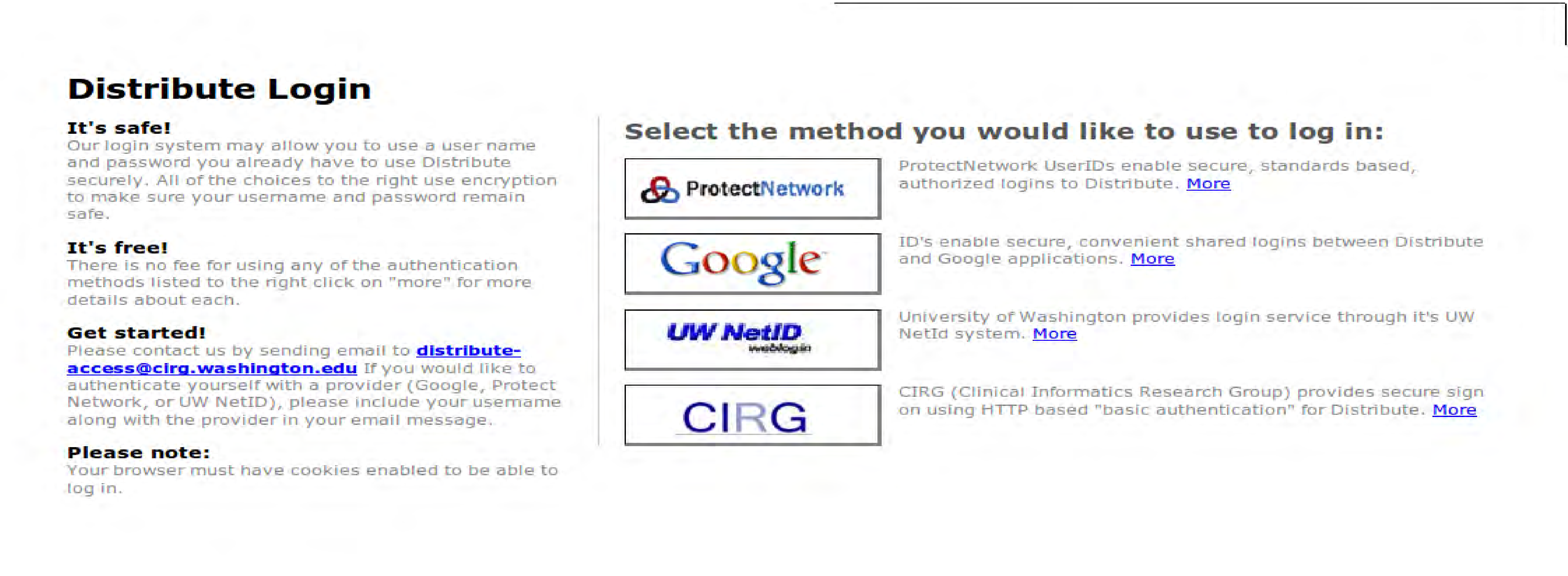
- "temp netid"
  - explicitly for "temporary" access, so non-personal, no linked services; mostly for UW-wireless-to-Internet access
- new "manual" sponsored UW NetID processes
  - "Bronze" process == "deferred" identity proofing
  - "Silver" process == equivalent-to-hiring ID proofing, but can be done by any staff member ...
  - new Person Registry Web Service for reduced-latency programmatic person-entry creation

Some UW Use Cases

- UW Educational Outreach Testing Service
  - 40K users/year for statewide online testing
  - use social IDs? SP site would have had to integrate, so a social-SAML gateway might have helped
  - but UW has interest in getting these people UW NetIDs ...
- School of Social Work new online mentoring service
  - starting with 5K email addresses, want to create accounts; how to do "verified email address" ?
  - does UW NetID guest process help? not really ...

More UW use cases

- Clinical Informatics
  - building prototype systems for clinical outreach
  - UW participants, also local accounts, also those wanting to use social accounts, so built multi-login, with account linking



Distribute Login

It's safe!
Our login system may allow you to use a user name and password you already have to use Distribute securely. All of the choices to the right use encryption to make sure your username and password remain safe.

It's free!
There is no fee for using any of the authentication methods listed to the right click on "more" for more details about each.

Get started!
Please contact us by sending email to **distribute-access@cirg.washington.edu** If you would like to authenticate yourself with a provider (Google, Protect Network, or UW NetID), please include your username along with the provider in your email message.

Please note:
Your browser must have cookies enabled to be able to log in.

Select the method you would like to use to log in:

ProtectNetwork UserIDs enable secure, standards based, authorized logins to Distribute. More

ID's enable secure, convenient shared logins between Distribute and Google applications. More

University of Washington provides login service through it's UW NetId system. More

CIRG (Clinical Informatics Research Group) provides secure sign on using HTTP based "basic authentication" for Distribute. More

InCommon "SocialID" collaboration

- many sites working on social-id integration for campus SPs
- taking a close look at gateway solutions
  - OpenID or multi-protocol? how many providers?
  - how is identity info mapped to SAML attributes?
  - transparency of gateway
- should InCommon offer a gateway as a service?
  - or are gateways less problematic when run at more local scale?
  - some successful businesses in this area (Janrain, Gigya)

Facebook: an eco-tale

- value begins in a community, by definition exclusive
- a successful community grows: not every person of interest goes to Harvard ...
- exclusivity is recreated in the larger system via other means
- every successful system aspires to global scale
  - i.e., no built-in barriers to who can be assimilated, er, who can participate
- so too with the systems we build to support our institutions
- but global domination tends not to last forever ...

NSTIC

- National Strategy for Trusted Identities in Cyberspace
  - Obama administration initiative to promote "identity ecosystem"
  - http://www.nist.gov/nstic/, run by NIST / Dept of Commerce
  - gov encouragement of private-sector work
  - "Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation." (also: passwords are bad)
  - many stakeholders: social providers, HE, financial, retail, law enforcement ... almost everyone
  - sound familiar? InCommon/HE has been template for this vision

Social Provider Evolution

- not just throwaway email addresses any more
  - stable, long-term, reality-linked personal/social identity is the core of their business model (i.e., selling that identity info)
- having your account hacked is a bad user experience
  - biggest problem is username/password reuse across sites
  - Playstation (etc) breakin ripples across industry, creates great understanding of password risks, promotes interest in federation
- making huge investments in login system protection
  - global monitoring, pattern matching, "login resistance"
  - meets assurance goals even without strong passwords?

Social Identity Provider Next Steps

- linking with mobile telephony providers
  - every mobile phone is potential strong authentication device, linked to real-world identity via credit cards
  - reduce/eliminate passwords via OAuth, OpenID Connect
  - create cross-industry business model
- recognition?
  - face recognition, behavior patterns, ...
- building value for relying parties
  - in support of that (inter)national strategy ...
  - and how does the privacy part work?

Role of HE Identity?

- if "social" identity really becomes better ...
  - then it won't just be for guest users, it will be for (potentially) any user
- if authentication isn't our core value ...
  - then it's about attributes, relationships: student, faculty, staff, researcher, resource entitlements, group memberships, course roles, etc: stuff we're doing anyway
  - NSTIC envisions role of attribute providers distinct from authentication providers;
HE can lead the way again ...

Future of "Guest" Systems

- We're all guests
  - some just stay longer than others ...
- Identity linkage/agility is key
  - federation will be "in the platform" of systems we deploy, whether on-premise or in the cloud
  - campus netid systems won't go away, but person registries must support verified linkage with other identities
  - role for multi-institution person registry services? privacy?
- User experience is key
  - invitation-based workflow, profile access