The Bronzing of Harvard

Scott Bradner
March 4, 2015
Agenda

- The Existing Environment
- Why InCommon Bronze?
- Coverage Decisions
- The Certification Process
- Dealing with Certification Issues
- Lessons Learned
The Existing Environment: Harvard University

• Harvard has been around for a while (since 1636!)
  – 47 Nobel Prizes
  – 32 heads of state
  – 48 Pulitzer Prizes

• 11 principal academic units
  – Significant IT distribution among academic units

• Scale
  – 2,400 faculty and 10,400 academic appointments
  – officially 6,700 undergraduate and 14,500 graduate students
    • database has 24,011
  – 58,800 employees (including student employees)
  – 323,000 living alumni
The Existing Environment: Harvard ID Numbers

• Non-sequential 8-digit ID number (HUID) assigned to Harvard staff, faculty, students, and others
  – “Others” include contractors, library borrowers, spouses, tenants, overseers, employees of the Smithsonian Astrophysical Observatory and Harvard Management Company, sponsored accounts …

• “HUID for life”
  – Effort to ensure that any one person is assigned a maximum of one permanent HUID

• Not in Harvard’s FERPA directory list
  – Thus, must be kept confidential
The Existing Environment: Identity and Access Management

- Harvard started to develop a “single-sign-on” PIN System in late 1998
  - Based on then-existing ID card database … the only database that included all active persons assigned Harvard ID numbers
  - First augmented with telephone directory info
  - Later augmented with other info, such as roles
  - Evolved into Harvard’s current core person identity registry (IdDB)
- The system now supports more than 600 applications
  - This includes vendor applications through a proxy
The Existing Environment: Microsoft Active Directory

• Large University Active Directory

• Most active HUID holders are in University AD
  – Major use: Office 365 for staff

• Harvard’s new password management system will push the same passwords to both the PIN System and AD

• Thus, the status of AD needs to be taken into account when certifying for Bronze (or Silver)
The Existing Environment: IdDB

• IdDB gets regular feeds from many sources, including:
  – Human resources
  – Registrar systems (many)
  – Student Information System
  – Division of Continuing Education

• Now never forgets: 642,129 entries (as of 2/17/15)

• Fields include:
  – HUID number
  – Directory information
  – Role and status information
  – Miscellaneous information, including UUID and EPPN
    (learn more: http://iam.harvard.edu/resources/iam-database-information)
The Existing Environment: LDAP

• Harvard currently has two LDAP server sets, which are being combined:
  – HU-LDAP (directory information)
  – AuthLDAP (credentials)

• Many IdDB fields are exported into the LDAPs
The Existing Environment: Authentication via PIN System

• Applications redirect users to the PIN System for authentication
  – User prompted for credentials
    • HUID & password
  – Credentials checked against AuthLDAP
  – User redirected back to app with a signed token in the URL

• PIN System supports some “one-way federation”
  – Users can select other servers for credential checking, such as Active Directory or the Harvard Medical School authentication engine
The Existing Environment: Next-Generation Authentication System

• PIN System redone in 2013
  – From homebrew system to CAS-based solution (“PIN/CAS”)
  – Application interface and application configuration database maintained for compatibility

• PIN System will be rebranded in Summer 2015 as HarvardKey
  – Includes new login name based on email address
  – More robust self-service portal for users
  – Adding options for multifactor authentication
The Existing Environment: Harvard IdP

• Harvard’s Shibboleth IdP uses PIN/CAS for authentication
  – Gets attributes from LDAPs
  – *ScopedAffiliation* attribute calculated from role and status information

• Learn more: http://iam.harvard.edu/resources/incommon
Why InCommon Bronze?

• Theoretically useful by itself (in the future)

• An external set of technical and process standards also provides a good forcing function
  – “Certifying with InCommon verifies to the Harvard Community that University IAM efforts meet nationally recognized external standards”

• Reassures Harvard users that IAM is following good practices
  – Learn more: http://iam.harvard.edu/news/incommon-bronze
Coverage Decisions

• Basic decisions:
  – IdDB is for everyone, for all time
  – The Harvard IdP will only vouch to InCommon SPs for users we “know” and who are a current part of the Harvard Community
    • We do not vouch for others outside these criteria, even if they have valid Harvard credentials
  • Specifically, we decided to not attempt to validate everyone in IdDB for Bronze
Coverage Decisions: How Do We Know You?

- The Harvard IdP will vouch to InCommon SPs for the following categories:
  - Active paid employees
    - ID proofed by employment process
  - Active Harvard Community members who have picked up ID cards
    - Government-issued photo ID checked during card pick-up process
- This includes faculty, staff, on-campus students and others
  - Does not currently cover distance learners
- Will also add an additional in-person verification mechanism
  - Not currently considering remote proofing
The Certification Process

• Imported Assurance Profile 1.2 into a spreadsheet outlining requirements for both Bronze and Silver

• Went through line-by-line describing current status

• Identified the few gaps in Harvard’s systems:
  – Relevant to both Bronze and Silver:
    • Resistance to guessing authentication secret
    • SHA-1
  – Relevant to Silver only:
    • Securing authentication traffic
    • Stored authentication secrets
    • Strong protection of authentication secrets
Certification Issues: Resistance to Guessing

• The PIN/CAS system does not require people to change their passwords on a regular basis

• Harvard’s password complexity requirements have recently been strengthened

• When verifying to a Bronze SP, the Harvard IdP will only verify users who have changed their passwords since the new rules went into effect and within the last 5 years (within the last year for Silver SPs)
  – If time requirement not met, user receives an error of “your password must be changed”

• Thus, impact only on those who want to use Bronze or Silver SPs
Certification Issues: SHA-1

• Took time to coordinate certainty that all SPs using the Harvard IdP could support SHA-2

• Reconfiguration put into production Jan. 6, 2015
Certification Issues: Stored Authentication Secrets

• Issue for Silver certification

• Credentials stored using hash — no seed
  – Implemented whole-disk encryption for PIN/CAS
    • The next PIN/CAS update will use seeded hash
  – Will implement whole-disk encryption for AD
Certification Issues: Securing Authentication Traffic

• AD-specific issue for Silver certification

• Must configure AD to not use LM or NTMLv1
  – NTMLv2 may also be an issue

• Learn more: http://tinyurl.com/silver-ad-cookbook
Certification Issues: A Surprise

• U.S. Federal ICAM Privacy Assurance addendum was a surprise
  – Not in IAP — only in agreement

• Had to publish information on attribute release, etc.
  – See section 9 in http://iam.harvard.edu/resources/incommon-bronze

• Will likely support user managed attribute release control (e.g., PrivacyLens) at some point
Lessons Learned

- Bronze certification wasn’t difficult … once we made a few simplifying decisions:
  - Use role and status to decide whom we vouch for
  - Force password changes only on users of Bronze (or Silver) SPs
  - Use employment status and card pick-up status for ID proofing

- Harvard is ready for Silver certification, except for AD
  - And documenting (& paying) for an audit
Thank you!

Questions? Email scott_bradner@harvard.edu