CSU Subnet Managers
September 19, 2018

It’s Still Hot!
Agenda

- ACNS Projects – Dave Hoffman
- Middleware – Randy Miotke
- Licensing – Diane Noren
- Security – Zach Campain
- Network / Telecom – Greg Redder
MDM

Reschedule Mobile Device Management discussion.

• Time conflict
• Will find a time in the next couple of weeks to get interested parties together.
ACNS Project Updates

Dave Hoffman

Cray Computer

• Old OS and cannot be updated which is a security threat. We will put the access to the Cray from off campus behind Duo beginning 1/1

• Our maintenance agreement on the Cray ends Sept 30 and will not be renewed. We will keep the Cray running as long as we can but encourage people to move their research computing needs to Summit in Boulder.

• Ofc 365
  – All new students get Ofc 365 account as default email.
ACNS Project Updates

• DUO Update
  – Discussing whether to put in front of RamWeb, email, eID

• Voicemail
  – Unified messaging, may need to switch before December.

• Unizin book order tool
  – Bookstore plans to implement, likely for spring 2019.
CSU Identity Stack

• eID
  – Identity management solution
  – Client self-service and administrative account management
  – Scheduled maintenance processes
  – Ad hoc provisioning processes
• Shibboleth Identity Provider (TIER)
• Grouper (TIER)
• COmanage – collaborative orgs and external ID registry (TIER)
• On-campus and cloud-based Service Providers
• Active Directory
• OpenLDAP eduPerson directory and grouper support
• CSU SAML federation for campus-only Service Providers
Entity Registry

- COmanage
  - Centralized person registry
  - Provides unique CSU identifier
  - Account linking
    - Identity solution for collaborative organizations (COs)
    - Target use is external population
Social Authentication

• Cirrus Identity
  – Social to SAML Gateway
    • Social discovery service (iframe & embedded)
    • Handles OAuth, OpenID to social identity services
    • Returns SAML assertions back to SP
  – Proxy
    • Allows using the same developer account across SPs
    • Provides a consistent identifier from social IdPs
Grouper

• SOR and delegated groups management
  – Courses and enrollments
  – Student, staff, faculty, associate departments
  – External population – alumni, donors, community patrons

• Management of access policies and service eligibility
  – Delegated and role-based
Shibboleth IdP

• New LDAP directories with extended schemas
• In the SAML assertion to SPs
  – Grouper memberships eduPersonEntitlement
• Native Duo integration
RabbitMQ – Messaging

• Ensure all requests are processed
• Allows web applications to continue without waiting for a response from API
External Identities Architecture and Flow

1. Discovery and return of authenticated identifier
   - Devices:
     - Donor Connect Website
     - Registrar Website determines identity
     - Cloud Services (AWS) Social SAML Gateway Social Proxy

2. Query External ID

3. If no external ID, prove who you are
   - Devices:
     - Message Listener Application (5 Sec Cron)

4. Add Identity Message

5. Check Queue

6. Create Identity
   - Devices:
     - COmanage (Identity Management)

7. Set initial group membership
   - Devices:
     - Directory Services (LDAP)

8. Use data
   - Devices:
     - Banner
     - HR
     - eID

   - Groups:
     - Grouper (Group Management)
Demo
TIER Identity Stack

• **Trust & Identity in Education & Research (TIER)**

• Packaged suite of components
  – Shibboleth Identity Provider
  – Grouper
  – COmanage
  – midPoint
  – Set of APIs to provide consistency and flexibility
  – Regular integration and release schedule
TIER

Identity Sources
- Campus Systems
- Person Registration & Update Service
- Unique Identifier Creation
- Master Person Store
- Demographic Data
- Affiliation Data
- Contact Data
- Account Information

Entity Registry

The TIER Architecture
- Person Match / Deduplication
- Relying Party Data
  Aka "Metadata"
- Attribute Resolver

Identity Consumers
- Cloud Providers
- Research Partners
- Campus Applications
- Enterprise Directories
- Operating Systems

Integration Services
- APIs, Application Messaging, Workflow / Orchestration

Groups Service
- Automatically Maintained Groups
- Manually Maintained Groups

Provisioning Service
- Group-based Provisioning
- Request-based Provisioning
- Resource Catalog
- Approval Workflow
- Provisioning Connectors
Reference groups represent the current state of membership for all subjects as known to the enterprise. They are used to configure access, governance, policy, audit, compliance, and reference groups as well as audit and compliance.
Current Identity Projects

- Docker - containerize IAM stack
  - Grouper
  - RabbitMQ
  - Shibboleth IdP
- midpoint
  - Entity registry
  - Very flexible provisioning engine based on roles and access policies
- TIER person data matching
- CSU Federation
- External Identities Invitation Service
  - FAMweb and RamRecords
CSU Federation Updates

• New VM for metadata aggregate in-progress
  – Updated OS and back-end applications
• New federation signing certificate to be deployed this fall
  – SPs will need to download and test the new certificate
• Test metadata aggregate coming soon
Questions?

- Reminder – Banner maintenance on Sunday
- eID will be unavailable
Licensing – Diane Noren

Adobe:

- **Creative Cloud**
  - Renews Sept. 30
  - $262.50 per Named User
  - $183.75 per Device - must have computer name
  - Device licenses are for computer labs
    - Must be installed by IT staff
    - Must notify RAMtech if computer name changes
    - Renewal emails in process.

- **Acrobat Pro**
  - FTE based
  - Renews February
Licensing

• **Adobe E-sign**
  – Renewed
  – $1.55 per completed document
  – Invoice emails will be sent in October.

• **Microsoft**
  – EES was renewed July 1.
  – I have not started billing yet.
  – Invoice emails will be sent in October.
RAMtech

• **Endnote**
  – Renewal notices sent
  – Version 9.0

• **Chem-Bio-Office**
  – Renewal notices sent
  – Chem-Draw 17.1

• **Mathematica**
  – Renews Nov.30,2018

• **Maple**
  – Renewal notices Sent
• **SPSS-Amos**
  – January 1 renewal

• **Zoom**
  – Consolidating licensing under one CSU agreement
  – Cost will be less than current pricing
  – Still finalizing
  – Contact [Diane.Noren@colostate.edu](mailto:Diane.Noren@colostate.edu) before renewing your single zoom licenses online
RAMtech

- Apple
  - Back to School promotion for personal use ends Sept. 25, 2018
  - Mac OS 12.0 coming

Questions?
Cybersecurity Update

Steve Lovaas, Zach Campain, ACNS
Security Topics

1. Increased risks, elevating security

2. Critical changes coming by Halloween

3. Elevating cybersecurity on campus

4. Acceptable/minimum OS and browsers

5. Security of the Web, evolving
Increased risks, elevating security

The past year has seen notable compromises around the nation, including substantial loss of credentials and personal information. Some of the most notable include:

• Colorado Department of Transportation
• Home routers/Russian spyware
• HP printer/fax as a proof of concept – fax machines are now weaponized
• CSU credential compromise led to financial loss (this semester)
Increased risks, elevating security

CSU needs to shore up and improve its defenses, as it’s not so much a matter of IF as of WHEN we will be the target of a major attack.

The following slides list several areas in which we will implement new technologies and procedures, as well as tightening up existing controls. Please be on the lookout for more information!
Critical changes coming by Halloween

• TLS 1.2 only for O365 login
  – Microsoft announced this change to us
  – Client needs to be NEWER than Android 4.3, IE 10, Mac OS X 10.8, Firefox 26
  – We don’t see many instances ON campus, but affects off campus too

• Mac OS X 10.11 (El Capitan) will be end of life
  – Coincides with the release of OS X 10.14
  – No more patches or security fixes, so no longer allowed on campus or Pulse
Elevating cybersecurity on campus

- Acting to shore up some issues, better enforce existing policies
- Next phase of multifactor authentication with Duo
- Investigating more advanced cloud security/anti-phishing tools
- Hiring another FTE
- Hiring student interns
Minimum OS versions – supported and getting security updates

- Windows 10 (versions 1803, 1709, 1703 -- version 1607 is EOL April 2019)
- Windows 8.1 (not Win 8)
- Windows 7 SP1 (EOL January 2020)
- Mac OS X (10.14, 10.13, 10.12)
  - 10.11 will be EOL as soon as 10.14 is released, 9/24/2018
- Linux (each distro’s latest supported kernel and current patches)
- Chrome OS (latest OS update)
  - 10991.0 latest as of 8/7/2018 (full OS updates released every 6 weeks)
  - Enable auto-updates
Minimum browser versions

- IE 11 (not 10)
- Edge (version is tied to Windows)
- Firefox v62 or later
  - V61 and older are no longer supported
  - V60.2.9 Extended Support Release (9/5/2018) is still supported
- Chrome v69
  - V68 recently superseded (9/2018)
  - V67 and older “discontinued” by Google
Security of the Web, evolving

• Prepare for HTTPS everywhere (in calendar 2019)
  – Get rid of HTTP links on your pages (use HTTPS instead)
  – HTML security response headers
    (concept/recommendations on ACNS security page)
• Prepare your servers for TLS 1.2 only
  – 1.0 and 1.1 are considered Deprecated (Internet-Draft doc filed 6/18/18)
• TLS 1.0 and 1.1 are deprecated and considered a configuration error.
• We’ll have interns doing more testing and notification
Security of the Web, evolving

• ACNS doing scans, with some external tools
  – BitSight – commercial platform, great breadth
  – U of Texas “dorkbot” – in-depth web application scan (XSS, SQLi, etc.)
  – Both useful services – please whitelist rather than blocking if you see in your logs

• Test your own site regularly
  – Set the scan to NOT be posted publicly
  – Qualys SSL Scan (ssl Labs.com) – Get an A/A+ to be open to the internet
  – Mozilla Observatory (observatory.mozilla.org)
    • Grade heavily influenced by security headers
    • Please consult ACNS security page for recommendations first
"Between a rack and a hard place."

- Shane Vigil, Housing & Dining Services
NOC/Telecom

Greg Redder, ACNS

1. Upgrades
   • Fiber & Copper
   • Wireless
   • Construction

2. Policies/procedures
NR Addition

- Moved fiber and switching infrastructure to new MDF.
- 3 new IDFs
- 4 switches supporting 372 ports
- 39 Access Points
TMI

- 1 MDF, 6 IDF: 8 switches & 1,300 ports
- 56 wireless access points
- New fiber link along MAX corridor to tie South Campus to Main Campus!
More construction...

Next up:
- Richardson Design
- Animal Sciences Addition
- A/Z Addition

Bid stage:
- Sheppardson addition/remodel
Building MDF/IDF upgrades completed since last meeting

Computer Science – partnership between central funding and CS (mostly CS!)

Facilities North MDF
MDF upgrades for this calendar year

Strategy: *Focus on buildings with the most general assignment (GA) classroom seats or buildings with 1G links that are 70% utilized.*

- 14 MDF upgrades installing redundant management module
- Moby: upgrade to dual 10G links + redundant management module
Routing changes

- Using West Campus and South Campus core routers to route (instead of just switch) networks
- Reduces load on campus core routers
WiFi upgrades

• A few 802.11n APs left, but mostly converted campus to 802.11ac!

• Added redundancy for wireless infrastructure between two main campus data centers

• WiFi traffic now behind data center firewalls – partly funded by students to help address detection and mitigation of security issues
WiFi upgrades

• NAT pools greatly increased to aid in logging of problems

• Reworking of some IP space to help devices stay connected when moving between buildings.
Wave 2 WiFi upgrades

- Microbiology
- Tiley House (1405 S. College)
- BSB
- Wagar
- LSC
- Education

- TiLT -remodel project
- NR (original section upgraded, new addition installed)
- Engineering
- Admin -Central funding
- Shepardson
- Gifford
Wave 1 WiFi upgrades

- RIC/BRB/Discovery (IDRC)
- MERC
- Painter
- Hartshorn
- Facilities South
- Powerhouse Energy Institute
- Washington School
- Aggie Labs
- Centennial
Survey says...

Q4 Overall, how satisfied are you with WiFi on campus?

Answered: 209  Skipped: 0

- Very satisfied
- Satisfied
- Neither satisfied nor dissatisfied
- Dissatisfied
- Very dissatisfied

Percentage distribution:
- Very satisfied
- Satisfied
- Neither satisfied nor dissatisfied
- Dissatisfied
- Very dissatisfied
Policies and Procedures

- Challenges/Solutions
- Documentation
- Helpdesk
- Physical Security
Challenges

• No central model for supporting non-MDF network equipment.

• Support of systems ACNS/Telecom didn't configure and aren't involved in the regular maintenance of.
Solutions

Support of a standard, scalable, supportable configuration:

– *Switches in locked communication rooms configured by, managed and supported by central networking services.*

• Work on a model to support switches in communication rooms centrally.

• Continue to help fix problems outside of the standard configurations

• Continue to offer to help transition non-standard configurations to standardized configurations.
Helpdesk

- Border firewall requests to be made by Primary/Secondary network managers

- Victims of our own success – need to forward incomplete requests from end users to College/Dept IT staff
Documentation

• Pending revision of Network Operations Policy

• Quarterly revisions of ACNS/Telecom Design Standards

• Audit of communication rooms and associated access paperwork
Documentation

New documents for:

• Requesting communication room access
• Requests to install non-central equipment in communication rooms

New processes in ACNS/Telecom being developed:

• Processing of requests
• Storing of signed documents
• Auditing of access to and equipment in communication rooms
First line of support: You!

Per Network Operations Policy (existing and draft versions):

Network Managers are "first line of support" required to have ability to look at network equipment in communication rooms in their areas of responsibility.
Keys

Per June 1 ACNS/Telecom Design Standards:
Newly designed communication rooms required to have card access.

Four physical keys will exist:
1. Head of ACNS/Telecom Field Operations (Jon Friedrich)
2. Head of NOC/Telecom (Greg Redder)
3. CSUPD
4. Access Services (guys who make the key!)

Rationale: Expansion of life-safety, mission critical equipment in communication rooms.
Keys

ACNS/Telecom will work on retrofitting existing communication rooms in the coming 30 years!
"MDF" & "IDF"

MDF = "entrance facility"
IDF = "equipment room"
"netcom"

- NOC + Telecom = NetCom
Thank you
Next Subnet Managers Meeting

Wednesday, November 28, 2018
10 – 11:30 am
LSC 304 – 306

Apple will do a presentation at the end of the business portion of the meeting.