CSU Subnet Managers
March 21, 2018

Happy Equinox!
Hug the Druid of your choice.
Agenda

- IS – Josh Clark
- ACNS Projects – Dave Hoffman
- Middleware – Randy Miotke
- Licensing – Diane Noren
- Security – Steve Lovaas
- Network / Telecom – Greg Redder
IS Update

Josh Clark

• Banner
• KFS
• HR
Middleware

Randy Miotke

Classroom Support Services Video Library

• Local instance of Kaltura (local)
• Moving to a new version in late March or early April
Shibboleth Identity Provider

- New LDAP Servers – target first week of April
- eduPersonEntitlement attribute will contain Grouper group memberships
External Identities

• Advancement in final testing - live shortly

• Authenticate with federated SAML IdP or social provider (Google, etc.)

• Person verification
  – Former students/applicants - Registrar
  – Donors – Advancement

• COmanage
  – Entity (person) registry for external
  – Provides local unique identifier
  – Link multiple external accounts to one registry record
  – Invitation service
Grouper Maintenance

- Wednesday 8:00 pm to 9:00 pm
- Modifying structure of production to follow Trust and Identity in Education and Research (TIER) deployment guidelines for Grouper
- About TIER
- No expected interruption in service
Licensing – Diane Noren

• Microsoft EES- Enrollment for Education Solutions
  – CSUs current subscription based model- Office 365
  – Working on completing billing for current year (July 1, 2017 to June 30, 2018)
  – Please send account # to Diane.Noren@colostate.edu
    If you have not already done so
Microsoft Licensing Presentation

Date: March 29
Location: Morgan Library
Room: Event Hall
Time: 10:00 am to Noon

Microsoft presenters: Kris Swanson & Chris Galli
EES updates and changes

Email questions to Diane.Noren@colostate.edu by March 23 at 5:00 pm.
Adobe

• Acrobat Pro
  – Renewed March 1, 2018
  – Have to license all FTEs per year
  – Current per FTE price $10.49
  – Will use same FTEs as Microsoft
  – Working on billing

  – Individual License will be $39.99 per year

  – Individual license directly from Adobe
    • $14.99 per month or $179.88 per year
SAS

- SAS renews July 1
  - Have fewer individuals using SAS
  - Still have 100 licenses left from this year
  - If 100 fewer license estimated cost for renewal will be $156.99 per year for next year
  - Need confirmation of # of SAS licenses for renewal
  - Send counts to Diane.Noren@colostate.edu
  - Single License Directly from SAS $6000.00
Apple Presentation

Date: April 18, 2018

Location: Morgan Library

Room: Event Hall

Time: Morning- final start time being finalized

Will send out final details once confirmed

Presenters: Aaron Grider – CSU account rep
Mark Coppin – Apple Accessibility
Project Updates

• **Duo Two-Factor Authentication**
  – Open Enrollment has begun
  – Update on Pulse Secure using secure.colostate.edu/2fa
  – Go Live on track for April 25

• **Research Data Storage**

• **Office 365 for Students**
  – Will be live Aug 1 for all student enrollments

• **Retire the SL-100**

• **CSU LENS** – Learning ENvironment Survey
  – Mid-Semester Pilot
  – Live for Fall 2018

• **Bridge** – Professional Development LMS
  – TOD and TTC live for summer 2018
Security Update

- Out of date
- Ransomware – review of CODOt attack
Out of Date

• Multiple sources of data
  – Duo
    • Can’t block with Duo under our basic “Duo MFA” license
    • Security checkup available in Duo app
  – BitSight
    • Sees devices open through the firewall, but also traffic headed outbound
  – Pulse
    • Blocking XP, Android 4.4.2, Mac OS X 10.9 and 10.10
    • Haven’t yet enabled this for Duo connections, to smooth roll-out process
Out of Date: from Duo

Operating Systems
Devices with Out-of-Date

- Total devices
- Devices with out-of-date Operating Systems

278 of 694 Devices have out-of-date Operating Systems
Set policy to block vulnerable devices

Try Duo Access

No new releases on this day.

Out-of-Date Devices by Operating System:
- Android - 148
- iOS - 57
- Mac OS X - 10
- Windows - 63
Out of Date: from Duo

Browsers
Devices with Out-of-Date

- Total devices
- Devices with out-of-date Browsers

126 of 694 Devices have out-of-date Browsers
Encourage your users to update

Try Duo Access

No new releases on this day.

Out-of-Date Devices by Browser:
- Chrome - 109
- Edge - 3
- Firefox - 14
- Internet Explorer - 0
- Safari - 0
Out of Date: from Duo

Plugins
Devices with Out-of-Date

- Total devices
- Devices with out-of-date Plugins

54 of 694 Devices have out-of-date Plugins
Identify risky devices

Try Duo Access

No new releases on this day.

Out-of-Date Devices by Plugin:
Flash - 54
Java - 1
Out of Date: Duo Mobile Security Checkup
Out of Date (Desktop): from BitSight

- **Grade Comparison**
  - in the **bottom 20%** of all companies

- **Grade Distribution**
  - 13,066 estimated users

- **Software Currency by Number of Users**
  - Over the last 60 days
  - Operating Systems:
    - Unknown: 1.5%
    - Unsupported: 13.2%
    - Supported: 90.1%
  - Browsers:
    - Unknown: 0.6%
    - Unsupported: 86.2%
    - Supported: 86.2%

- 1311 bad
- 804 bad
Out of Date (Mobile): from BitSight

Mobile Software

Grade Comparison

in the bottom 20% of all companies

Grade Distribution: 5,116 estimated users

Software Currency by Number of Users

Over the last 60 days

818

386
Out of Date: What to Do?

• IT Security Policy
  – Only operating systems and applications that provide high levels of security shall be used, and security updates (patches) shall be applied in a timely manner.

• How does YOUR unit manage OS versions and patches?
  – Are we doing a good enough job?
  – How might we do better?
Ransomware: CDoT

• Overview:
  – 1\textsuperscript{st} attack Feb 21, SamSam malware evaded McAfee
  – Spread throughout desktops, encrypting files, demanding Bitcoin
  – CDoT did not pay, shut down 2000+ desktops, reverted to manual processes
  – Employees used personal devices for email, Google for shared docs
  – Public servers on a separate network, not affected
  – Dozens of employees, FBI, and National Guard working on recovery
  – 2\textsuperscript{nd} attack March 1, SamSam had morphed and re-infected
Ransomware: CDoT

• Analysis
  – Still no root cause identified, but SamSam can propagate through phishing or infected web servers
  – SamSam has been in the wild since 2015, $300k in bitcoin so far
  – This was a zero-day variant that CDoT’s anti-malware did not catch
  – Choice to shut down, clean, and use manual processing
  – Extremely inconvenient, embarrassing, and expensive, and it’s not done yet!
Ransomware: CDoT

• Duo has launched, VPN only for now
• How are you updating OS and assuring patches?
• Ransomware – Are you ready?

• Questions?
  – Steven.Lovaas@ColoState.edu
Security Update: Take-Aways

What would you do?

– Don't ever pay
– Keep endpoints and servers patched and up to date
– Rely on preparation.
  • Backups! (not just Windows roll-back feature)
  • Remember that ransomware can encrypt automatically mapped network shares
  • Keep critical services away from user networks
  • Plan for how to do without your desktop/laptop and everything on it
NOC (Network Operations Center)
Greg Redder

- Data Network
- Telecom/NOC Projects (Construction)
- Wireless
- Voice
Data Network
(peak devices per month)
Data Network

MDF upgrades since last meeting:
- Clark C (new switch, had dual 10G)
- RBL (new switch, had dual 10G)
- LSC (new self-funded switch, had dual 10G)
- BSB (new switch, had dual 10G)
- Yates (new switch + dual 10G)
- Environ. Health (new switch)
- A/Z (new switch + dual 10G)
- SBB (new switch, had dual 10G)
- Centennial Hall (new switch)
- MRB (new switch + dual 10G)
Data Network

Border upgrades

• New routers over Thanksgiving & Winter Breaks
• Bigger, better, faster. 100G capable!
Data Network

Upgrades Pending

Border: Adding 20G to/from FRGP
- 60G (30G on each "side")
- 10G "ResearchLAN"
- TOTAL = 70G

Edge:
- "hand me down" switches from MDF upgrades going into some IDFIs prioritized by buildings with the most General Assignment seats.
- Looking into way to fund IDF infrastructure
Communication rooms:

No garbage
No ladders
No trash
No foolin'

(There's a charge to pay hourly staff to "clean" up MDFs/IDFs, including cabling, not meeting standards. Please let us know if you are having areas where this is an issue and we'll work with you on changing the locks.)
Telecom/NOC Projects

WCNR Addition
- Cable pulls started
- 4 communication rooms
- 360+ edge ports
- 40 access points

TMI
- 7 communication rooms
- 1300+ data ports
- 62 access points

Next up:
- A/Z addition
- Richardson Design Center
- Animal Science addition
Wireless
(Peak devices per month)
Traffic to WiFi exceeds 3Gbits/sec now!
Wireless

Issues:

– Alexa, Apple HomePod, Google Home, oh my!
– Most can only connect on open network (csu-guest)
– IOT items in general probably don't have encrypted traffic
Wireless

Upgrades since last meeting (802.11ac wave2):

- A/Z
- Rockwell
- Rockwell West
- Morgan

Upgrading to wave 1

- Equine Center (completed)
- ERC (in progress)
Wireless

Miscellaneous

– All wireless goes through data center firewall for NAT to the Internet – allows for better threat detection and mitigation.

– Reminders:
  • eduroam: Use csu-eid or eduroam. Don't configure both.
  • csu-guest: Don't set up csu-guest.

– Survey – stay tuned

– Turn off wireless service on printers and don't move your phone!
Voice

Concurrent calls stats

Number of concurrent calls

<table>
<thead>
<tr>
<th>Day</th>
<th>Calls Avg Peak</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-02-26</td>
<td>101</td>
</tr>
<tr>
<td>2018-02-27</td>
<td>91</td>
</tr>
<tr>
<td>2018-02-28</td>
<td>98</td>
</tr>
<tr>
<td>2018-03-01</td>
<td>96</td>
</tr>
<tr>
<td>2018-03-02</td>
<td>91</td>
</tr>
<tr>
<td>2018-03-03</td>
<td>125</td>
</tr>
<tr>
<td>2018-03-04</td>
<td>135</td>
</tr>
<tr>
<td>2018-03-05</td>
<td>138</td>
</tr>
<tr>
<td>2018-03-06</td>
<td>129</td>
</tr>
<tr>
<td>2018-03-07</td>
<td>120</td>
</tr>
<tr>
<td>2018-03-08</td>
<td>109</td>
</tr>
<tr>
<td>2018-03-09</td>
<td>124</td>
</tr>
<tr>
<td>2018-03-10</td>
<td>96</td>
</tr>
<tr>
<td>2018-03-11</td>
<td>6</td>
</tr>
<tr>
<td>2018-03-12</td>
<td>4</td>
</tr>
<tr>
<td>2018-03-13</td>
<td>6</td>
</tr>
<tr>
<td>2018-03-14</td>
<td>5</td>
</tr>
<tr>
<td>2018-03-15</td>
<td>87</td>
</tr>
<tr>
<td>2018-03-16</td>
<td>125</td>
</tr>
<tr>
<td>2018-03-17</td>
<td>6</td>
</tr>
<tr>
<td>2018-03-18</td>
<td>5</td>
</tr>
</tbody>
</table>
Voice

Current issues:
- Caller IDs
- Silent Voicemail
- Presence
- Small number of calls not completing
Voice

PoE

• Continuing move across campus to turn this off except where needed.
• Other PoE devices?
• Conference room phones
Voice

Data activation

• How best to get vlan information when IT Manager doesn't make the request?

FAX Server

• Trying to gauge need/interest in a dedicated FAX server
NOC
&
Telecommunications

thank you!
Next Subnet Managers Meeting

Wednesday, May 16, 2018

10 – 11:30 am

LSC 376 - 378