Upcoming Meetings

- July 11
- August 15
- September 19
- October 17
- November 7 (Final Rate Setting)

- All meetings in 337A from 1:30-3:00pm
Agenda

- Two-factor authentication report and recommendation
- Original FY’12 initiatives approved by NPTF
- Revised FY’12 Identity Management goals
- Potential FY’13 security strategies and initiatives
Two-Factor Authentication Report (Criss)

- Background
- Application and technology selection
- Pilot details and results
- RSA SecurID
- PhoneFactor
- Costs
- Recommendation
Two Factor-Background

- Part of Strengthening PennKey program
- Addresses weakness of password-only authentication
- Pilot of two technologies during FY ‘11
Two Factor-Application and Technology Selection

- PennCommunity EntryView
- Token-based one-time password solution
  - RSA SecurID
- Two-channel phone based solution
  - PhoneFactor
Two Factor-Pilot Details and Results

- Two 90 day pilots
- More than 50 participants
- Gained experience with both technologies and received good feedback from pilot participants via end of pilot surveys
- Didn’t gain much experience with support
RSA SecurID Review

- Industry standard
- Supports more than web-based authentication
- Token distribution, support and identity proofing was challenging
- Public security compromises in recent months
- Not recommended
PhoneFactor Review

- Less well received by pilot users
- Less expensive, but still not cheap
- Requires more customization and development
- Relies on something many users have – a phone
- Some resistance from pilot users to using their personal cell phones for work purposes
- Concerns about the security of the service
- Problematic in cases where user may not be reliably reachable by phone
- Not recommended
## Costs – Does Not Include Support

<table>
<thead>
<tr>
<th>User Count</th>
<th>Service</th>
<th>Four Year TCO</th>
<th>Per Month / Per User Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Users</td>
<td>RSA SecurID</td>
<td>$121,776</td>
<td>$5.07</td>
</tr>
<tr>
<td></td>
<td>Phone Factor</td>
<td>$80,000</td>
<td>$3.33</td>
</tr>
<tr>
<td>1000 Users</td>
<td>RSA SecurID</td>
<td>$204,890</td>
<td>$4.27</td>
</tr>
<tr>
<td></td>
<td>Phone Factor</td>
<td>$130,000</td>
<td>$2.71</td>
</tr>
<tr>
<td>5000 Users</td>
<td>RSA SecurID</td>
<td>$749,050</td>
<td>$3.12</td>
</tr>
<tr>
<td></td>
<td>Phone Factor</td>
<td>$410,000</td>
<td>$1.71</td>
</tr>
</tbody>
</table>
Recommendation

- Neither service is a clear winner
- Technology and security concerns with both
- Lack of a specific application to protect nor expressed campus need
- Neither continuation of pilot nor production deployment recommended
- Revised FY ‘12 Two Factor goals suggested
Original FY’12 initiatives approved by NPTF (Mike)

- Two-Factor
  - Productionize central infrastructure and provide TSS support
  - $75,000

- Intrusion detection systems-local
  - Revise strategy document and do a pilot
  - $38,750
Revised FY’12 Identity Management Goals

- Two Factor Authentication
- Levels of Assurance
- Shibboleth
- InCommon
- Intrusion Detection Systems Border
Two Factor (Jim)

- Two new goals were developed with the intent of:
  - Keeping momentum going on Two Factor
  - Combining and retaining the beneficial aspects of both piloted solutions, while addressing their concerns
Two-Factor - Goal 1

- More work is necessary to identify what systems or applications will benefit most from Two Factor, to help focus thinking about how/where Two Factor should be applied
- Who are the ideal customers of this service?
- Outcome
  - Identify applications that could benefit from use of two-factor as component of LoA variable
Two-Factor – Goal 2

- Do more research on solutions that reconcile the pros and cons identified by the pilot with the intention of identifying a secure, workable and affordable solution

- Outcome
  - Evaluate and draft white paper on open-source, standards-based, one-time passcode generators for mobile platforms
Levels of Assurance (LoA)

- Authentication is how a user proves that they are who they say they are.
- LoA is a more granular look at authentication
  - How certain are we that the authenticated user is really who they say they are?
  - Did the user acquire authentication credentials initially in a secure way?
  - Do we have any reason to believe that the credential has since been compromised?
Levels of Assurance (LoA) Goals

- Develop framework for assigning LoA assertions to PennKey web authentications; identify how these assertions will be delivered to and used by internal web applications
- Draft policy to address how to properly assign, and use, LoA on PennKey protected web-applications
- Execute a pilot implementation of LoA on an application with highly sensitive data, such as MyPay (Stretch goal)
Shibboleth

- Shibboleth is an open source and standards-based web Single Sign On service which integrates with the PennKey WebLogin (CoSign) service.
- It supports:
  - Integration with 3rd party vendor applications
  - Authorization decisions using PennGroups
  - Federation with other institutions (InCommon)
Federation

A federation is a collection of organizations that have agreed to interoperate using a common set of rules

- Purpose is to provide a framework for the safe sharing of online resources

- External users access Penn resources using their home organization credentials

- Penn users access resources at other institutions and government agencies (like NIH) using their PennKey
InCommon

- InCommon is an example of a federation, it serves the Higher Ed and research communities
- InCommon identity assurance program
  - Criteria campus identity management systems must meet to satisfy requirements of higher risk applications
  - Two identity assurance profiles
    - Bronze
    - Silver
Shibboleth & InCommon Goals

- Continue to provide guidance, support for Penn customers who wish to use federated authentication with Shibboleth and InCommon
  - Documentation
  - Facilitate access to consulting services
- Conduct gap analysis to identify changes/enhancements needed in the IdM environment to meet federation Bronze & Silver level requirements as they exist at InCommon (whether draft or final) as of November 2011
Perimeter Intrusion Detection System (IDS) (Josh)

- Prior NPTF proposal emphasized local vs. border IDS solutions
- NPTF approved $38,750 to:
  - Study the options, write a report recommending solution
  - Implement limited pilot of chosen solution
- Revised goals propose evaluation of an enterprise-wide vendor solution for border IDS
Border/Perimeter IDS

- “Border”, in this case, defined as looking at attack traffic entering/exiting the university network
- Essential for assessing risk, identifying threats and compromises across the University
- Research is needed to determine best solutions, network architecture, staffing, and costs. Need to do the research now to have a deployable approach in FY’13.
- What are our peers doing?
## Peer Benchmarking

<table>
<thead>
<tr>
<th>Organization</th>
<th>Using an IDS?</th>
<th>If yes, what product and how is it deployed? (at the edge, at the core, selectively on specific subnets or networks, etc)</th>
<th>Are you using any other network based security tools that you feel like mentioning (filtering, firewall, IPS, etc.)?</th>
</tr>
</thead>
</table>
| Columbia     | Y              | "PaIRS" - written by Columbia and looks at the borders and core | Port anostic bandwidth limits  
GULP  
Blocking netbios, 1443, 1444  
Firewalls in use - details not known |
| Dartmouth    | Y              | Tipping Point & Stealth Watch | Evaluating Palo Alto |
| Yale         | Y              | Snort (perimeter), Stealth Watch throughout the network | * Router filters (Light) on Yale's Internet routers,  
* internal (data center, departmental) network firewalls,  
* WebSense web proxy server for "secure" managed workstations.  
* blocking cisco + netbios ports |
| Brown        | Y              | "Targeted": Snort currently in front of critical assets and subnets; expanding its use. | Recently redesigned network using VRF, and built several security zones.  
Investigating Palo Alto.  
Have firewalls - details not known |
| Princeton    | Y              | McAfee Intrushield (IPS) | Router ACLs at the perimeter. Juniper Netscreen firewalls at the core.  
RSA enVision for log collection and analysis. |
| Duke         | Y              | Snort at the perimeter and in-between VRF's | Tippingpoint (which is sitting in "front" of Snort). Tried using Tippingpoint IPS as an IDS, "and quickly discovered that would not work." |
| Harvard      | Y              | No details provided | No details provided |
| MIT          | Y              | No details provided | Evaluating firewall |
| Cornell      | Y              | No details provided | No details provided |
| Penn         | N              | N/A | Arbor used for analyzing campus flow data. Juniper firewalls individually deployed and managed at the local (building and subnet) level, not at core. |
IDS – New Goals

- Recommend a Border IDS solution and develop the associated project plan
  - Representatives from ISC N&T and Information Security evaluate possible border/core IDS vendor solutions and associated network enhancements or modifications
  - Recommend specific border/core product in written report that includes plan for implementation (including funding requirements).
The cost to do the 5 initiatives discussed is equal to or higher than the $113,500 approved for FY’12.

We seek your consensus to move forward in this direction instead.

FY’12 revised goals:
- Two Factor Authentication
- Levels of Assurance
- Shibboleth
- InCommon
- Intrusion Detection Systems Border
Potential FY’13 Security Strategies and Initiatives (Josh)

- IDS Border pilots or full implementation
- Central Information and Event logging
  - This is another area of information security where we lag behind our peers and that will ultimately prevent us from moving forward with automated solutions to help assess and mitigate risk (e.g., SIEM)
- PennKey password entropy improvements (e.g., minimum password length, etc.)
- ISC Information Security and N&T will continue to baseline with our peers (not only Ivy+, but also through EDUCAUSE)
Potential FY’13 Security Strategies and Initiatives

- What else are you interested in?
Future Meetings (Mike)

- Other than IdM and security, what other topics do you want to hear about?