Coffee Klatch Participants

- Mike Corn University of Illinois, Urbana-Champaign
- Jacob Farmer Indiana University
- Nate Klingenstein Internet2
- Doug Pearson REN-ISAC
- Joe St Sauver Internet2/University of Oregon
- Kris Steinhoff University of Michigan
- Matt Zekauskas Internet2
NETWORK ASPECTS

- General approach
- For Schools
- For connectors
- For potential service providers

- Matt Zekauskas,
  <matt@Internet2.edu>
Network general approach

- IP services are placed in the R&E routing table, tagged as Netplus services (see [http://noc.net.internet2.edu/i2network/maps-documentation/documentation/bgp-communities.html#Internet2 BGP Communities](http://noc.net.internet2.edu/i2network/maps-documentation/documentation/bgp-communities.html#Internet2 BGP Communities))
  - Provide value to all Internet2 members
- Some services require Layer 2 connections to extend the campus network into the cloud
- As new Netplus service providers come online, we look for direct Internet2 Network peerings
  - Ability to affect if utilization rises or performance issues arise
- Monitor usage
  - Work cooperatively if approach congestion
  - Work cooperatively if Netplus traffic affects other traffic
For schools

• Any services reachable by IP (most services) should “just be available” and work well given current R&E engineering.
• For services that act as extensions of the school’s network (HP/SHI Cloud services are the current example)
  – be prepared to extend a VLAN off campus to your connector
  – Address space used by the service is provided by the school
    ▪ Could be private or public
• Consider performance test points to verify performance off network (in general, and in support of these services).
For connectors

• IP-based services should require no extra work on your part. Monitor performance and utilization.
• Some services do require Layer-2 access. Be ready to extend a VLAN from the Internet2 Network backbone edge to campuses.
  – Need to be able to do this for Internet2 Advanced Layer 2 Services, support NSF GENI connections too
  – Could be done over a hybrid Internet2 port, multiple VLANs over a single connection to the Internet2 network.
  – Could be done using an Internet2 Advanced Layer 2 Services port
For providers

• Internet2 schools are used to clean high-performance connections
  – Including IPv6 addressability
  – “Jumbo” Ethernet frames – 9000 bytes http://noc.net.internet2.edu/i2network/maps-documentation/policy-statements.html#Jumbo Frames
  – Well-tuned connections http://fasterdata.es.net/fasterdata/host-tuning/
  – Performance closer to 1Gbps (and more!) than 1Mbps is the norm

• Performance test nodes are useful to understand performance issues http://psps.perfsonar.net/toolkit/

• Web-services-based service-specific statistics would be useful to the Internet2 Performance Portal

• Check out the Internet2 Network map for potential connection points; Internet2 Network Services will help engineer connections
For providers

- Maintain network headroom, troubleshoot and manage exemplary performance
- Coordinate service/outage notifications with Internet2
- Coordinate architecture changes that affect connectivity with Internet2
Internet2 Net+ Technical Architecture: An Introduction to Security Considerations

Internet2 Spring Member Meeting, Arlington VA
Combined Industry and Research Constituency Meeting
3:00-4:00 PM, April 23rd, 2012, Salon J

Joe St Sauver, Ph.D. (joe@uoregon.edu, joe@internet2.edu)
Internet2 Nationwide Security Programs Manager and
InCommon SSL/PKI Certificate Programs Manager

http://pages.uoregon.edu/joe/netplus-sec/  

JSS
Security and Cloud-Based Services

• Security (along with economics) may have a material impact on how and if cloud-based services get used.

• For cloud-based services to be embraced, they need to make financial sense, and they need to be adequately secure.

• We had an early “heads up” on this: when the Net+ cloud services were first announced during a previous member meeting plenary, and during the Q&A, Dave Farmer of Minnesota stood up and asked “What about security?”

• Security isn't the only thing that's important about cloud services, but it's certainly at least one important technical consideration
What Sort of "Cloud" Service Are We Talking About?

This can’t be a cloud discussion unless we have at least one slide trying to figure out what the heck is “in scope,” right? 🙄

- Cloud-based end-user applications (e.g., Box.net): yes
- Cloud-based infrastructure (e.g., HP/SHI): yes
- Future Net+ cloud-based services: yes

- NOT necessarily outsourced email (probably the single most popular “cloud service”)
- NOR Amazon Web Services (different model)
- NOR bring your own device/mobile applications, even if they’re cloud based (again, different risks)

JSS
Speaking of Risks, What Is The Cloud Risk Model?

- When we talk about a service being secure, we're really talking about managing risk.
- What are the main risks we worry about when it comes to the cloud?

1) *Data breaches* (e.g., classic PII spill of protected information)
2) *Incident non-detection*, e.g., you're Own3d but don't know it
3) *Non-availability of a critical service* (e.g., network's down, service can't find the customer's data, service is discontinued, etc.). If we're talking some best effort recreational service, that's one thing, but non-availability of a cloud-based ERP service would be something else…
4) *Compliance failures* (death by auditors/attorneys when regulatory mandates aren't met)
5) *Embarrassment*... :-(

- At least two or three of those five *aren't* a matter of what might be considered traditional *technical* system and network security.
How Do We Know That We're Appropriately “Managing” Risk (Assuming We Are)

• **Professional Expertise** (I'm not detecting us getting hit, and I'm not hearing reports that we've been hit, and I've managed all the security risks I've been able to, and I'm working a 20 hour day so...)

• **Historical Reputation**: we haven't been hacked previously, so we must be okay (but prior performance doesn't guarantee future returns)

• **Expenditures**: we're spending everything we've been able to get for securing things (but what if you’ve got a CISO who's bad at making the case for adequate resources?)

• **Audit**: the auditor doesn't return any findings (but what if we've got a crumby auditor who's asleep at the switch?)

• **Common Sense Test**: if something bad happens, will what we're currently doing pass the public "sniff test"? That is, are we doing what a reasonable person would normally do?

• **Insurance**: if we screw up, we don't have to pay...
The Cloud’s Different…

• The customer can't directly assess the security of the facilities, or the hardware-level OS install, or the configuration of the routers and firewalls and intrusion detection systems; I need to trust the expertise of the cloud provider's team, instead (even if I've never met them, and never will meet them).

• Many cloud providers may be new, and thus may not have had much time to build a reputation for being secure (or having security issues)

• Security capex/opex is fixed and bundled in as part of the service; my choice is effectively "do it" or "don't do it" (or nag/pick at the provider in an effort to potentially get them to make changes for everyone). Should there be an "extra secure" option available for some incremental price?

• I probably won’t get to see the cloud provider's audit reports (although they might share selected bits and pieces with me)

• We don't yet know how the public will view a choice to use the cloud for some services... Brilliant? Idiotic? Both at the same time?

• Can I insure IT services done in the cloud? Who's willing to write that insurance policy currently?
Security From the Point of View Of The Cloud Services Provider

- It's a big pain to answer many of the same security questions for each and every potential new customer.
- Higher ed is probably a bigger pain than many (we do odd things in odd ways -- who else cares about stuff like IPv6 and DNSSEC, eh?)
- Need to answer security questions carefully -- if you answer in error, you may be caught out by the customer (oops!), or, if someone gets hacked because you answered incorrectly, you may even have liability.
- Some questions you may not WANT to answer; security through obscurity isn't, but at the same time you don't want to give potential attackers a big leg up when it comes to successfully attacking you – getting the balance right is hard.
- But unresolved security concerns may stall/halt adoption of a cloud based solution, so you can't just ignore security issues.
- Security measures increase costs; increased costs decreases the attractiveness of the cloud based service as an economic issue.
- Security also has the potential to reduce usability; the harder it is to use, the lower the likelihood that the service will be used.
- No matter what you do, someone's not going to be happy (too “security happy”/too hard to use/too expensive; doesn't take security seriously enough/too easily hacked/not secure enough for our applications…}
What Can Higher Education Do?

- Higher ed is good at executing the “huddle together for safety” herd response -- those who like that strategy may want to wait until a bunch of colleagues have already begun using the cloud so they can enjoy safety in numbers (but that's not what Internet2's about)

- Start with comparatively low risk applications (e.g., academic applications rather than administrative applications, although beware academics with “hidden PII” in research datasets). Unfortunately, academic applications may be a low priority/have limited funding, and cloud computing, as an outsourced service, needs funding; academic applications can also quickly pose scaling challenges (lots of students and lots of poorly funded researchers looking for cheap options)

- Seek numerous third party certifications and attestations, so that if something goofy does happen, the finger pointing game will allow you to say, “Hey, but they passed all the certifications and audits that they should have passed...”

- Encourage the provider to become completely transparent with nothing to hide -- provide completely detailed security information about all aspects of the service, much as "open source software" totally exposes every detail of the software to public scrutiny.
What Would Internet2 Security Like To See From Cloud Service Partners?

1) Providers should complete the Cloud Security Alliance GRC Stack (https://cloudsecurityalliance.org/research/grc-stack/), and make the completed documents freely available for community review. By doing so:
   - The completed assessment eliminates the answer-the-same-set-of-questions-from-scratch time-after-time-for-each-new-customer hassles
   - The GRC Stack’s structured and systematic coverage ensures all major issues get considered and addressed
   - It's an industry best practice

2) Encourage providers to follow the model of Amazon Web Services, and have a non-passworded web site that publicly provides transparent information about security, compliance and privacy related issues (http://aws.amazon.com/security/ )
SAML Enabling Net+ Services
Security and Net+ Services

• Some of the specifics that we've encouraged the vendors to provide, conduct, or have:
  – clear communications and documentation concerning security that serves the needs of various parties, e.g. including enterprise IT applications, information security office, enterprise leadership, and service owners
  – clear description of security controls, being careful to scope to the domain(s) that they apply (for example, when saying that the cloud is protected by IDS, does that apply just to the control/management plane, or to the service plane as well?)
  – robust technical public-facing web-based documentation concerning the security controls
  – a good full-fledged security FAQ and white paper
Security and Net+ Services

- (more specifics)
  - certifications and accreditation, e.g. CSA Cloud Security Alliance, SAS 70, SSAE 16/SOC reports, ISAE 3402, FISMA, PCI DSS, ISO 27001, FIPS 140-2, HIPAA
  - periodic audits to ensure compliance, performed by external organizations, for certifications and accreditation like PCI DSS, SOX and HIPAA
  - periodic penetration tests performed by external organizations to audit various infrastructure and software security controls
  - some type of SDL on any custom software written and maintained by the provider
  - communication concerning security incidents
  - description of encryption (if applicable), key controls, etc.
  - staff vetting procedures
Security and Net+ Services

• (more specifics)
  – a description of components of service that are outsourced
  – a description of components of service that are outside the US
  – two-factor authentication for administration and operations
  – a description of physical security
  – policy and practice for disk disposal
  – a description of the disaster plan
  – a description of how security affects performance and end-to-end Internet (e.g. by firewalls, etc.)
  – a description of how the provider responds to law enforcement or other legal compulsions to disclose data
  – some form sort of ongoing channel of communication for security matters, possibly conducted through REN-ISAC
Internet2 is not ‘certifying’ the security of the service
  – Need to ensure enough information is provided for schools to make their own risk-based decision

Should be approached as w/any outsourced service

Special attention to integrations
  – OneCloud
  – openBox apps

Brings MDM to the forefront (and our lack of being prepared for it)

Data Classification – force the business to decide what’s appropriate
Review and understand the contract
Perform risk analysis (see Berkeley model)
Develop use cases and review with security office
Meet with data stewards
  – Review use cases
  – Review service security
  – Make determination on acceptable data for use with service
Think through “incident response”
  – Account compromise, lost mobile device ….