Random Wanderings

Scott Bradner
ABCD
12/12/14

1

Agenda

Security Policy
IAM
Clouds
HUITAAG
Internet governance

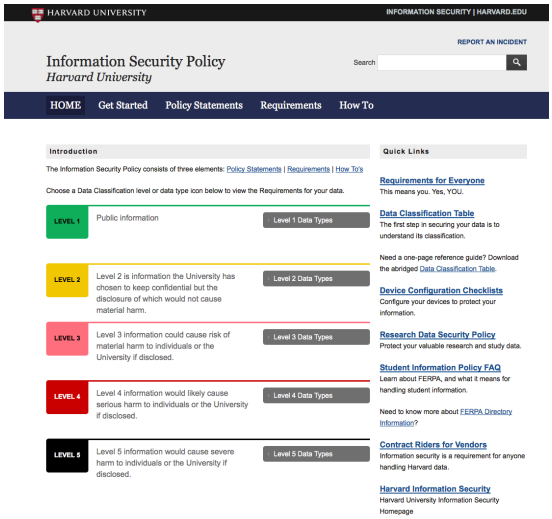
2

So Scott, what are you doing these days?

3

Harvard IT Security Policy

New Harvard IT Security Policy went live this week



4

New IT Security Policy

Developed by IT Security Workgroup

- Christian Hamer (CISO) (lead)
- Ben Gaucherin (deputy CIO)
- Ken Carson (Office of VP Provost for Research)
- Jim Schwartz (HBS)
- Peter Katz (OGC)
- Scott Bradner (Office of the CTO)
- Liz Eagan (HUIT IT Security)

Vetted by University IT Security Committee, CIOs, …

5

Concept

IT Security Policies (few will look at)

Moved away from general non-actionable dictates

- e.g., you must encrypt confidential info

Role & system based requirements

- e.g., user, system manager, user device, server
- Apply to all devices dealing with Harvard confidential info
  - Including personally owned devices

How-Tos

- Specific directions on how to meet requirements
  - e.g., how to configure smartphone to meet 'device must be secure' requirement

6

Identity and Access Management

7

InCommon Bronze

For the Harvard InCommon identity provider

8

InCommon Bronze

InCommon Bronze ≅ NIST Level 2

Harvard is the 4th (or 5th) to qualify

By itself, currently useless

- No current services requiring Bronze level certification
- Some may show up after a while

But an indicator of Harvard IAM's maturity

- i.e., Harvard's IAM systems & processes meet defined standards for security and controls

Almost ready for Silver

- Mostly missing documentation & an audit

9

IAM PR (from benefit highlights)

Benefits to end users

- Single, easy onboarding portal to claim accounts
- Self service portal for password changes etc.
- Folding in existing alumni, automatic adding of grads
- Access to common email & calendaring
- Multi factor authentication on the way
- Selected support for social media identities
- Enable access to external resources through InCommon

10

IAM PR, contd.

Benefits to people administrators

- Create and populate application access control groups
- Self service guest account management
- Central authorization service

Benefits for application owners

- Self service portal for application registration
- Support for non-Harvard applications
- Specific support for mobile applications
- Enable schools to get out of running their own IAM
- Support application and device authentication

11

Stepping on Clouds

12

Cloud Mandate

Move ¾ of existing HUIT applications "to the cloud"

- Plus all new applications

Why:

- Capitalizing on the benefits of the cloud (IaaS, or SaaS): elasticity, improved resiliency, pay for what you use, etc.
- Some cost savings - although not because it is necessarily much cheaper to operate in the cloud.
- Learning what is fast becoming a new way to do things - infrastructure as code vs. infrastructure as kittens, DevOps

13

Details

Scale: 587 total HUIT-run applications

Schedule: Move 440 applications within 3 years

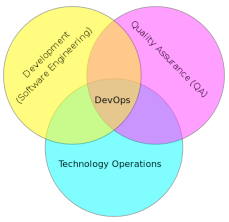
- One almost down, 439 to go

Generally vendor clouds

- Amazon AWS + others (e.g. VMWare compatible)

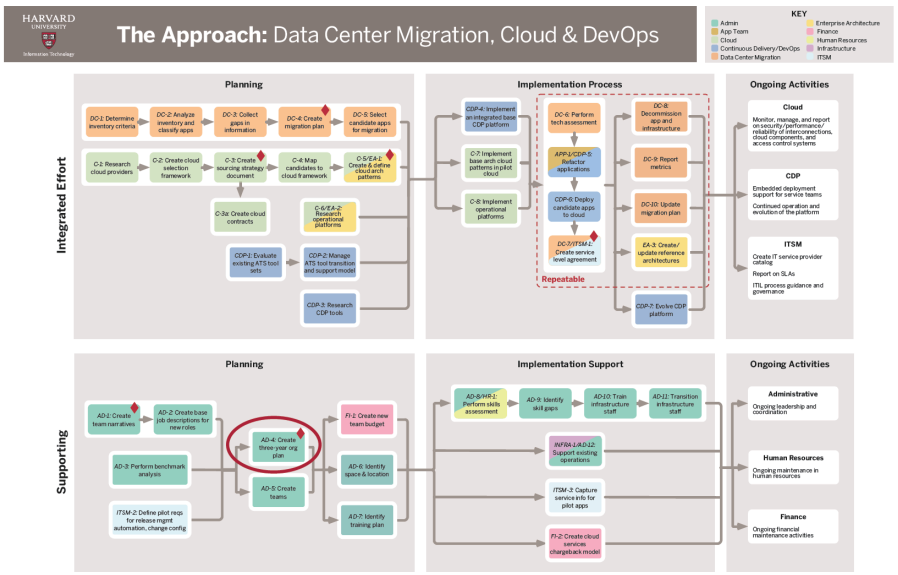
Will work on automating deployment process

Using "DevOps" philosophy



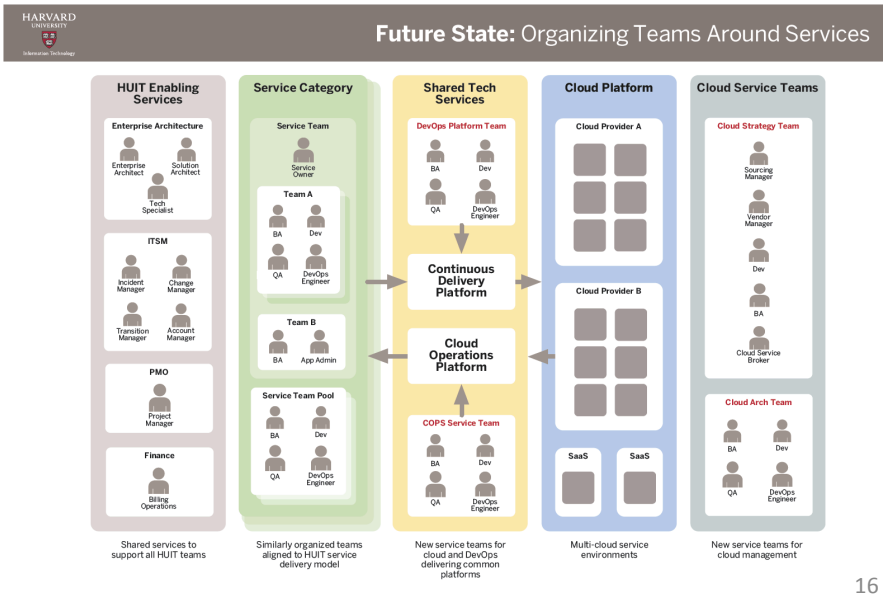
14

Approach



15

Future State: Organization



16

HUITAAG

HUIT Architectural Advisory Group

17

HUITAAG

Group formed to run the "technical decision process that will guide the current and future technical evolutions and re-designs within HUIT"

Permanent Members

- Jim Waldo (CTO & Chair)
- Ben Gaucherin (Deputy CIO)
- Jason Snyder (Managing Director of Arch. & Eng.)
- Christian Hamer (CISO)
- Jefferson Burson (Director of Networking)

Others join in discussion based on topic

18

HUITAAG, contd.

"As HUIT moves to adopt and adapt to new technology trends, decisions will need to be made to insure that there is a rational, common design to the technology. The design of the network, the form of the infrastructure, and the way in which software is built, bought, or modified will need to be coordinated in such a way that evolution of one component does not cause problems or limit the functionality of another. Just as important, decisions that are made in one part of the organization need to be known by other parts of the organization, both to guide the thinking in those other parts and to insure that some level of common use is maintained."

19

HUITAAG, contd.

Wiki: https://wiki.harvard.edu/confluence/display/HUITArch/HUIT+Architectural+Advisory+Group

Includes the decision backlog and per-decision sets of pages

First topic: VPC architectural considerations for use of Amazon AWS

20

Internet Governance: A perpetual "threat"

21

some of the players

22

not players

Don't blame the weatherman for the weather

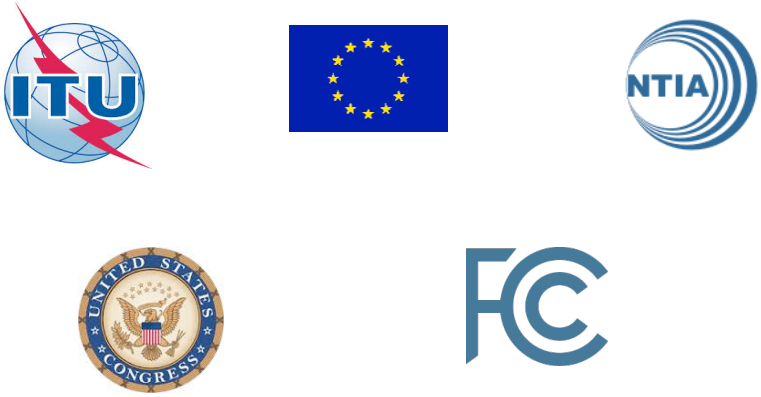
23

governance issues

regulations, settlements, technology standards, peering, security, emergency use, espionage / monitoring, national boundaries, attribution, societal disruption, business disruption, trademark, copyright, operation of critical infrastructure, censorship, spam, have/have not balance, domain names, resource assignment policies, government roles, network neutrality, exchange point management, market dynamics, subsidies, competition, cybercrime, cyberwar, patents, identification, attribution, …

24

Playing Fields



25

example: protocol standards

TCP/IP developed in U.S. in early 1970s
ISO started to develop network standard in 1977
OSI was offered TCP/IP as base, they declined
ARPANET adopted TCP/IP in 1983
OSI published protocol specifications in 1984
- mandated by many governments (including U.S.)
- but not a success in market (too complex, etc.)

U.S. relaxed requirement in 1994
ITU started to develop new net standard in 2004
- still under development – little deployment

last month India proposed reengineering protocols
- and the Internet archecture

26

An aside, open standards

everyone can participate

v

if you might be impacted, you are “in the room”

government role in traditional SDOs ensures representation of all parties

tends to reduce number of disruptive standards

27

Four contests

ITU

network neutrality

IANA function

NETmundial Initiative

28

ITU

29

ITU

The International Telecommunications Union

- U.N. treaty organization
- the traditional home of telecommunications standards

originally formed in mid 1800s

standards voted on by "member states"

imposed by regulation in some countries

few ITU standards are relevant to the Internet

- not because they have not tried
- H.323 (voice over IP), Next Generation Network (NGN)

30

ITU governance

- every now & then – meet to review treaties
  - World Conference on International Telecommunications (WCIT) – 2012, previous in 1988
- every 4 years
  - World Telecommunication Standardization Assembly (WTSA) – 2012
    - Set ITU-T structure and plan for next 4 years
  - Plenipotentiary Conference (PP) – nov 2014
    - set ITU plan for next 4 years
- contribution driven
  - thus not always controlled

31

ITU & Internet

- the ITU has long recognized that the Internet was intruding on their traditional territory
- e.g., shortly before PP-98 (1998)
  - IETF was approached about submitting IETF standards to ITU-T for review
- every PP since have included proposals to take over some or all of the Internet standards or assignment functions
  - to date, all blocked, mostly by U.S. coordinated efforts
  - but some ITU-T contributions request this anyway

32

Why Care?

ITU acts like a vote of the member states empowers it

- even over non government entities such as the IETF, RIRs & ICANN
- ambiguous legal picture in many countries

revision of Internet settlement regulations could have significant impact on Internet business model

putting Internet standards under government control could change nature of the standards

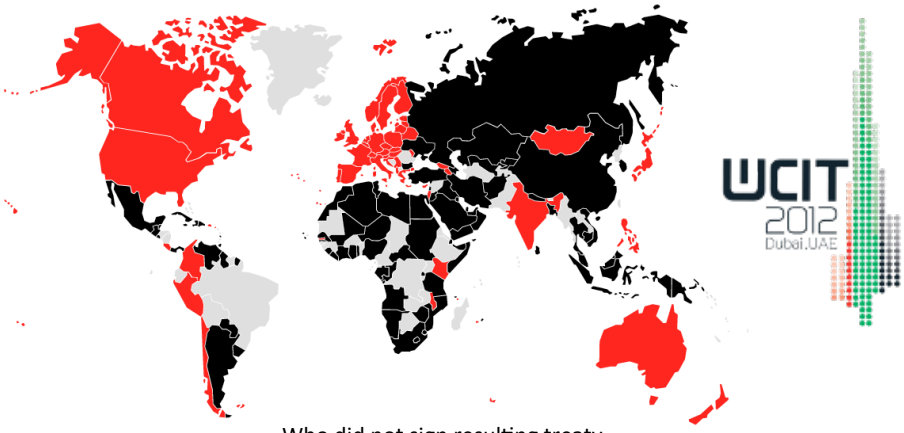
- protect incumbents, require backdoors, etc.

33

WCIT 2012

promise: consensus, no voting

actual: vote to expand ITU role in Internet



Who did not sign resulting treaty

34

PP 2014

- many submissions
- non-representative: from India
  - redo addressing & naming to be country based
  - take over Internet address & name policy development
  - redo architecture to ensure internal traffic stays in-country
  - record all Internet transactions
  - develop new "secure, robust and tamper-proof protocols"
- in the end, no substantive directions
  - after a lot of work, U.S. less listened to

35

network neutrality

36

network neutrality

a neutral network is in the spirit of the original Internet end-to-end architecture

- carriers just transport packets without regard to who sent them, who is to receive them, or what is in them

enables "permissionless innovation"

but the concept is foreign to traditional carriers

growing issue in U.S.

- less of an issue elsewhere

37

information services

Telecommunications Act of 1996 created a class of "information services"

- not subject to FCC regulation

FCC said that Internet service providers were offering information services

- direct connect ISPs were generally small and not part of telephone or cable providers at the time
- today, almost all residential Internet service is from a telephone or cable provider

ISPs generally respect the e2e principle

38

e2e abuse

some ISPs have abused e2e

- blocked VoIP (Madson River), degraded Bit Torrent (Comcast) and Netflix (Cogent)
  - and they all said they were not doing anything

so, call for FCC to regulate to stop such abuse

FCC has tried multiple times, always overturned in court

- with good cause

in the middle of another try

- FCC initial proposal got over 4 M, mostly negative, comments

39

White House input

Obama asked FCC to regulate ISPs as "Title II" common carriers

but Title II comes with lots of baggage

- used to regulate telephone carriers
- FCC can set prices, define services & operations, etc.

many activists want Title II but want the FCC to "forebear" from most regulations other than those that block unequal treatment of packets

- risks: courts could require some additional regulations, future FCC could be more supportive of regulation

general agreement: full Title II would hurt Net

40

other inputs

carriers say they will sue to block any regulations
- except for Comcast, which agreed to some to buy NBC

carriers threaten to stop investing in infrastructure

National Security Telecommunications Advisory Committee (NSTAC) called for prioritization of emergency and national security traffic
- lots of technical reasons this is a bad idea

Some content owners want free transport of their content (e.g. Netflix)

others want to regulate ISP peering

41

going dark

The FBI says they want regulations to require back doors in all Internet applications
- e.g., to counter Apple's iOS and iMessage locks
  - now using All Writs Act (1798) to force compliance

so they can wiretap or get at contents
- never mind that they can not show any example where this would have made a difference
- "a child will die"

note: the real bad guys already have their own tools and are incented to hide

42

IANA function

IANA function

3 core Internet coordination functions are performed by the Internet Corporation for Assigned Names and Numbers (ICANN) under contract from the U.S. National Telecommunications and Information Administration (NTIA) – part of the DoC

- record protocol values
- allocate IP address blocks to regional registries
- maintain root zone file for the domain name system

U.S. "control" long resented by many outside the U.S.

IANA transition

Last spring, NTIA said they might surrender control if specific conditions were met

- Multistakeholder model, maintain stability of DNS, meet needs of IANA customers & maintain open Internet

NTIA/IANA Stewardship Transition Coordination Group formed

- which will review proposals
- many proposals expected

45

IANA transition, contd.

NTIA has not committed to transition, will evaluate proposals

some in Congress do not want to "give away the Internet"

- particularly to be controlled by governments hostile to freedom

46

NETmundial Initiative

47

meanwhile

ICANN CEO, Fadi Chehadé, initiated, with the Brazilian President, a NETmundial meeting in Brazil last spring

- "Global Multistakeholder Meeting on the Future of Internet Governance"
- claims to not be an ICANN effort

anger after Snowden revelations part of cause

850 attendees, little solid result

NETmundial

48

NETmundial Initiative

Fadi Chehadé, with the World Economic Forun, have created the NETmundial Initiative

not related to NETmundial meeting

49

not to mention

World Summit on the Information Society (WSIS)

Internet Governance Forum (IGF)

China's World Internet Conference last month

Internet Society

the copyright industry

stop the Internet, we want to get off

the EU parliament

vote to break up Google

the NSA

destroyed U.S. moral authority in debate

50

or

the message of the Arab Spring

U.S. DoJ subpoenaing offshore data

calls for data sovereignty

Law enforcement want ICANN's help in making Internet sites disappear (e.g., illegal drug sites)

51

idealists

Some idealists say the Internet does not need governance

But some of them admit that regulations may still be useful:

"any company that handles Internet datagrams may not read or modify the content, nor infer intent or meaning for the purpose of deciding what datagrams to deliver or to not deliver"

David Reed

52

review

2014 ends with no significant changes in the Internet governance picture – 2015 looks interesting

but we keep getting close to the cliff of government control of the Internet

- at least a dozen times in the last dozen years

will the cliff is always be there?

- likely

the Internet is too important to leave to the people who know how it actually works

53

54