DISA

Defense Information Systems Agency

Department of Defense

Security Automation

To 3rd Annual NIST Security Automation Conference and Workshop

Richard Hale
Chief Information Assurance Executive
Defense Information Systems Agency

September 19, 2006

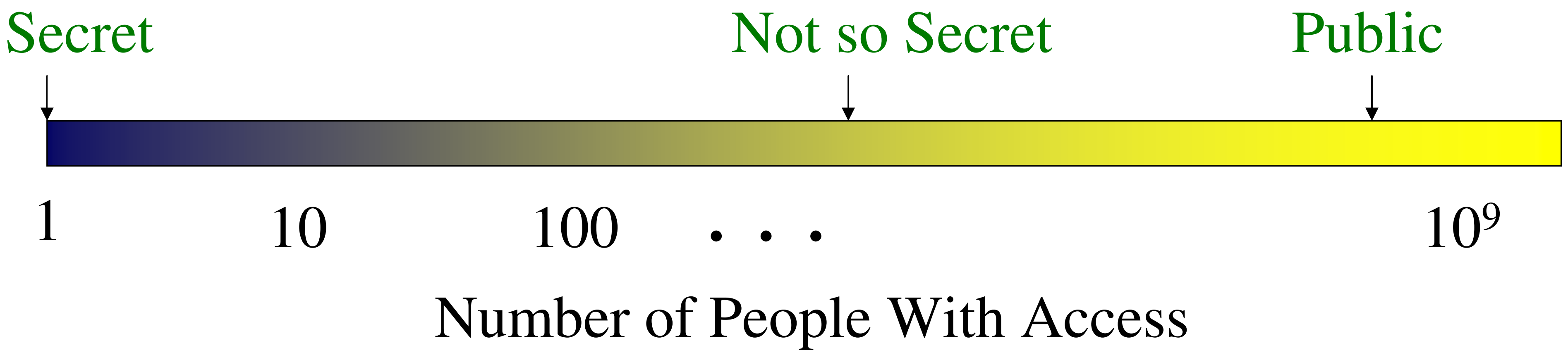
Goal 1. Assured DoD mission execution in the face of cyber attack

Or,

Goal 1. Dependability of the information and information infrastructure in the face of cyber attack

Goal 2. Ability to keep a secret while simultaneously sharing information broadly

More on Goal 2: *Sharing While Keeping a Secret*



These Are Complicated Problems

- Made more complicated by the fact that *everything is connected to everything else*…

- …by the fact that *DoD is a big place*, with much organizational and physical movement…

- …by the fact that organizations inside and outside DoD that have never worked together must do so, and do so well, often very quickly

- …and by the fact that *DoD has adversaries who employ large numbers of people who look for weaknesses* in us that may give them military advantage

The Old DoD Process for This

- The necessary dependability (in the face of cyber attack) defined by the mission or business process owner (still true)
- This owner also decided what measures were needed in order to provide that dependability
- (Mission owners generally had some guidance in the form of law, regulation, and or policy to help them determine the necessary dependability)

These Mission Owners Ostensibly Had Wide Latitude to Define How Dependability Needs Were Satisfied

- Keeping a secret was a bit different
  - There were community standards for defining the degree of confidentiality needed and for methods of achieving the right level.

- There were also rules on how to share while maintaining that confidentiality ("ask your boss if it's ok to share with someone, or "*need to know* ").

Today's DoD Infrastructure Must Properly Support Many, Many Missions

- The old notion that a "local" mission owner could completely manage "acceptable mission risk" for that person's systems seems quaint
  - Especially given that that many DoD (and other) missions could be affected by the "local" decision,
  - And that owner's mission might be affected by many other "local" decisions
  - But that owner is still responsible for mission success
- There is no easy answer to this.
- But,…

One Thing Is Clear

- Where it is possible to do so, community standards for certain things must be imposed in a manner analogous to building codes
  - if we are to have many missions/business processes co-exist on the single network.

- We should often (but not always) think of these as defining a base-level of assurance, on which certain mission owners can build

A Few Essential Baseline Standards

- IA controls standardized across the federal government
- Ditto operating system, other device, and some application configuration standards
- Connection approval standards
- Lifecycle security processes that put the right incentives & risks on the right people
- Perimeter/sharing architectures and application structures
- Data standards for all of the above
  - Automation, measurement, reporting…

One Minute on Bad Guys

- Trying to get something done (stealing money, gaining advantage in warfighting, whatever)
- **No rules!**
- Some are well funded, patient and have access to the tradecraft of modern intelligence
  - Define the goal
  - Develop various plans to achieve the goal (no rules…)
  - Select a plan or plans that gives good balance of executability, risk, cost
  - Take however long it takes to develop & practice a sure means of executing the plan

What To Do Against Such a Patient Bad Guy

- Carefully designed layers
- All those baseline controls, standards, & compliance with them
- Aggressive monitoring for changes
- Aggressive detection, diagnosis, and reaction capability
- …
- And maybe churn as a strategy (to drive up uncertainty about the effectiveness of all that patient work)
  - Automation will likely be a key as we figure this one out

Readiness, or Are We Ready for the Bad Guy?

- The notion of being as ready as we can be for the range of missions we anticipate
  - DoD calls this *readiness*
- The notion of knowing where we may have mission risk so that we can consider it in plans
- So, *measure* things to
  - Drive compliance with readiness standards & drive up readiness
    - Instant-by-instant
    - In longer-term budget decisions
  - Understand where we are not as ready as we might be

So, A Fundamental DoD Problem

Configuring computers (including PDAs, *appliances*, etc.) securely, keeping them configured securely as things changes, and ensuring the right people know this is so (or not so)

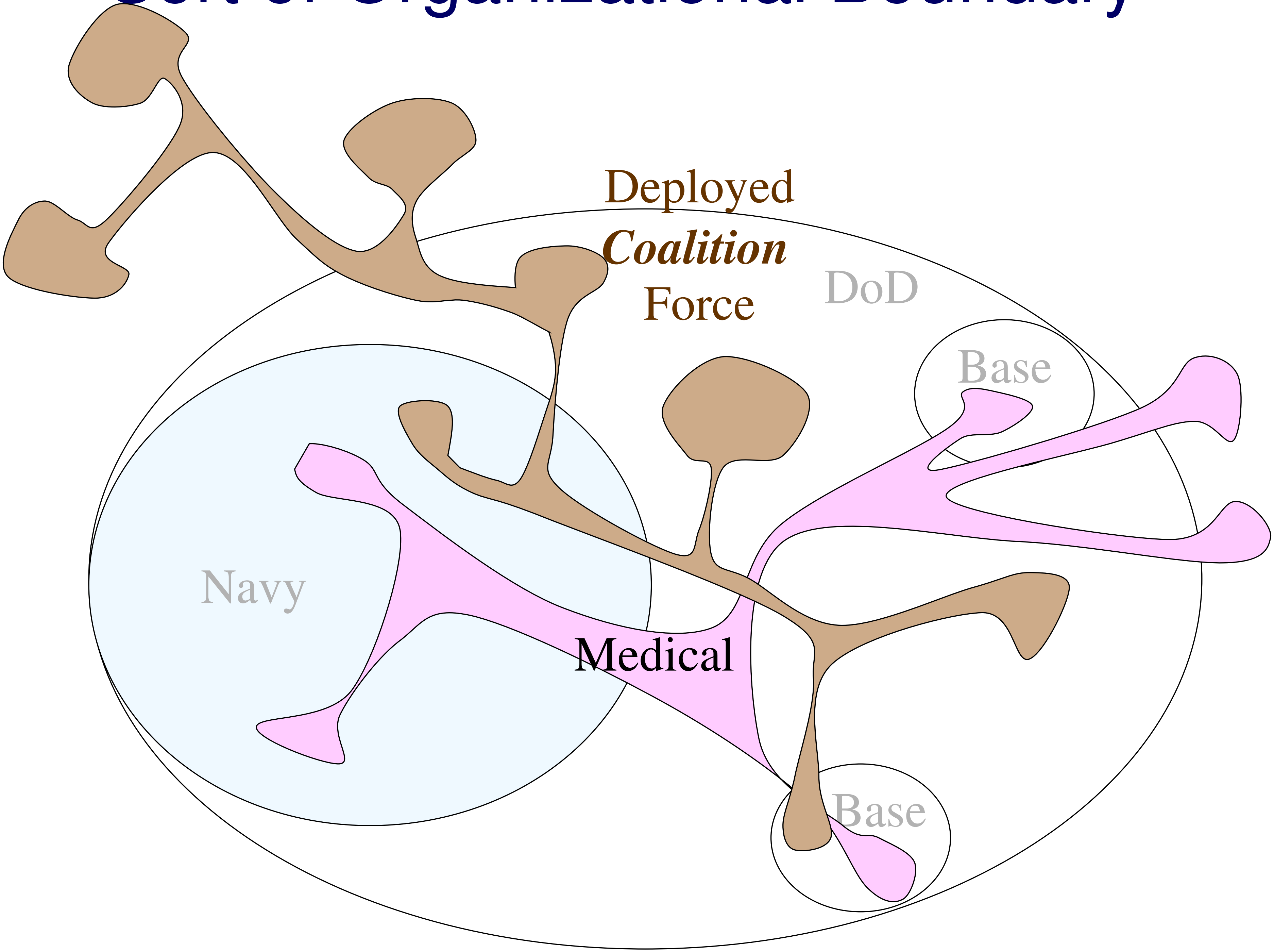
- **Always**
  - When we buy them, when we deploy them, when we change them
  - Even when we are mobile
  - Even when we are bringing organizations together in a task force, particularly DoD and non-DoD organizations

So, SCAP is Fundamental to DoD

DISA is developing its SCAP transition plan so our content is SCAP compliant, and so we can use commercial tools to automate configuration, measurement, & reporting

More About How DoD Does Things

Everything DoD Does Crosses Some Sort of Organizational Boundary



How Do I Get *Speed* in Setting Up These (often) Ad Hoc Arrangements?

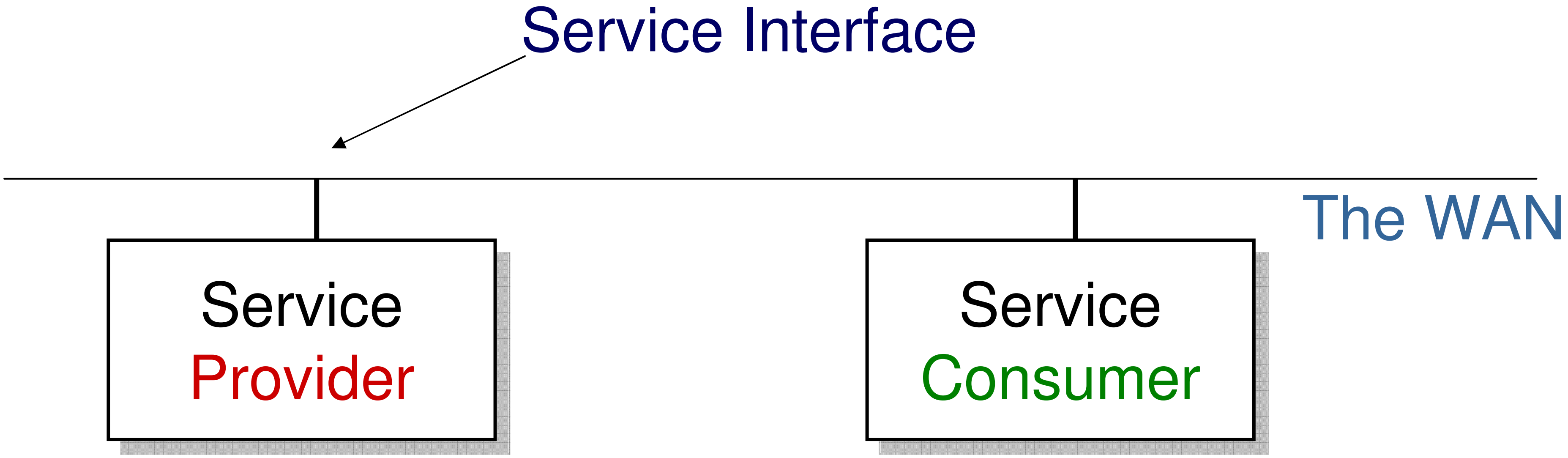
- I might be willing to share more, or collaborate more closely if I know my partner has the same baseline controls, and has implemented them properly (as I of course have…)
- Automated measurement and standardization of data standards for information about configuration might help
  - (if I can trust my partner's information)
- Integrity protection of results *at the tool that generates the results?*

Another Thing About DoD:
The DoD Data Strategy

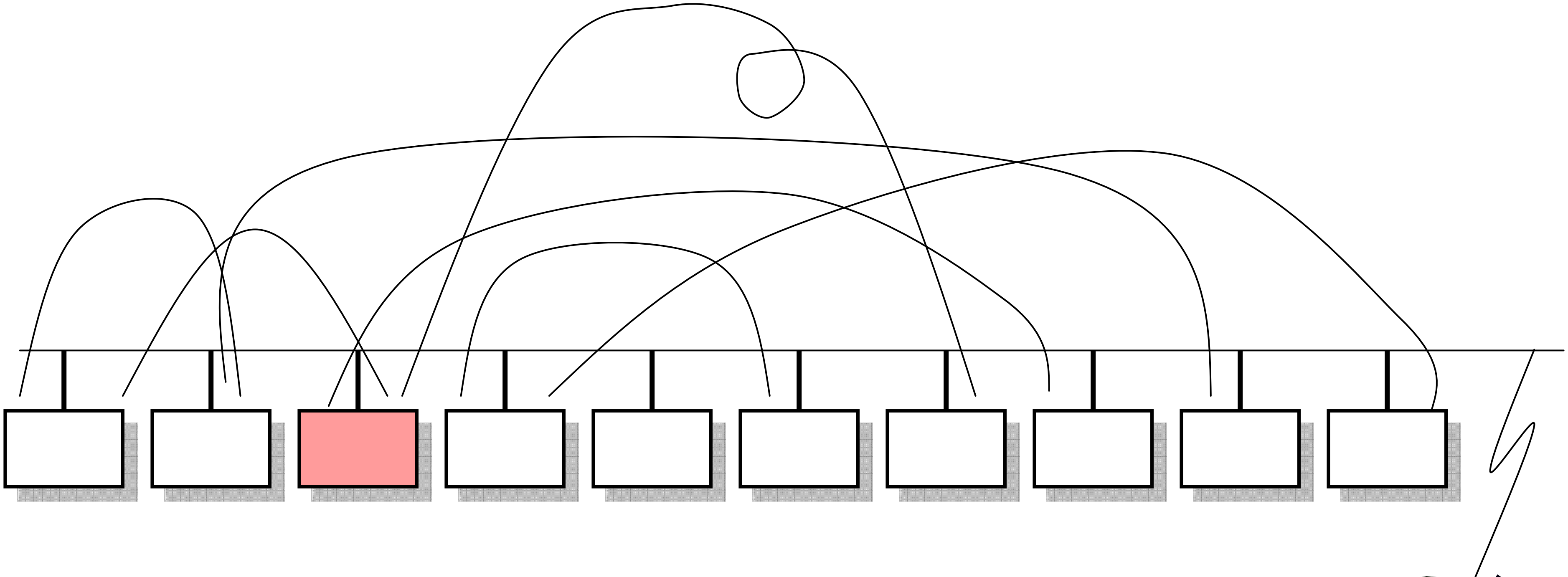
The Strategy: ***Make your data available in a form others can use***

- Publish your data so others can consume it
- Advertise the availability of the data so others can find it
- Publish some things about it so others can understand it
- Where you can, use community standards for definition of information

We Believe the Service Oriented Architecture (or SOA) Is Important to Achieving This

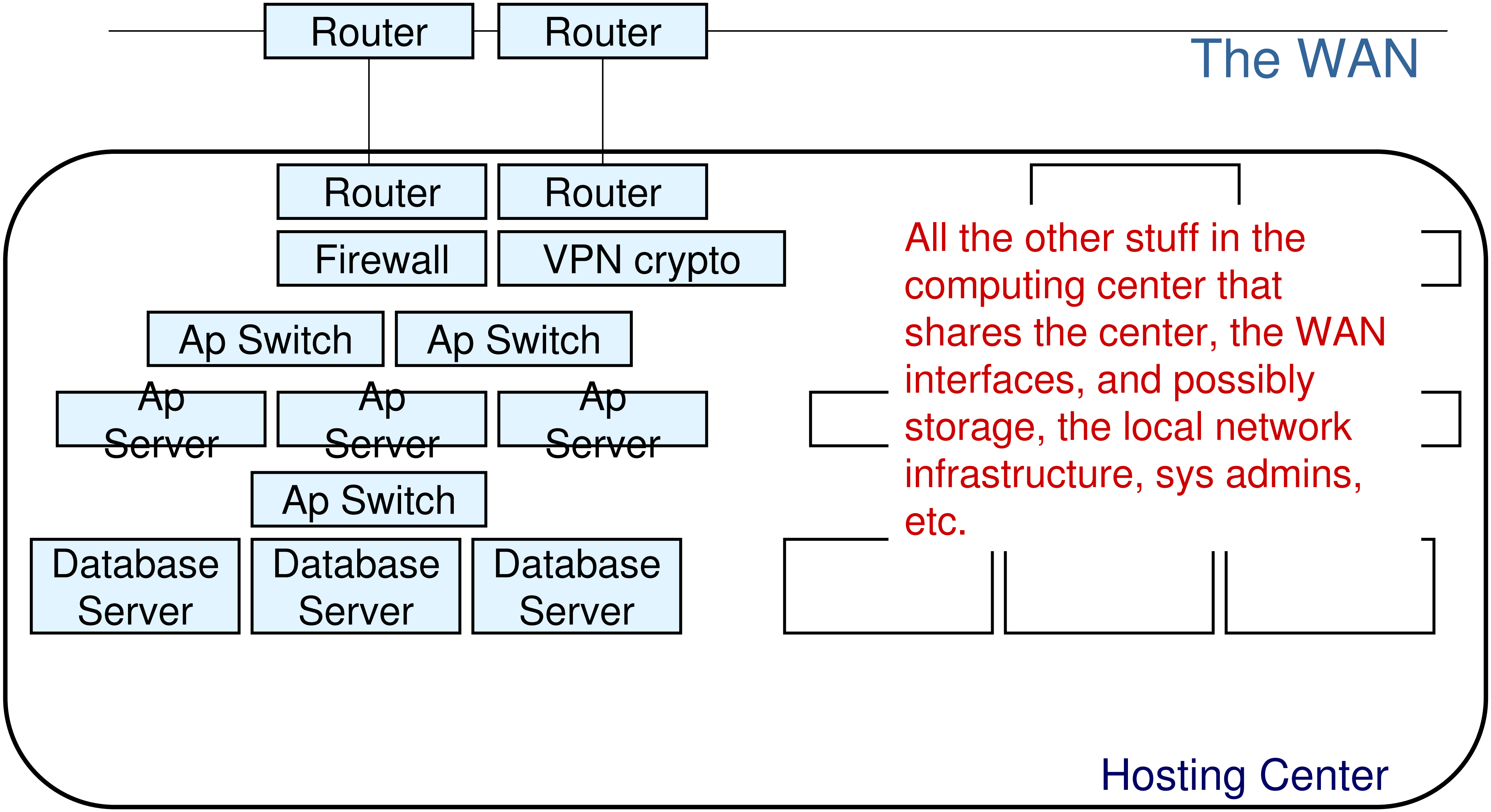


Composition of Services to Build a Capability



Our service is a participant in a composed application serving a soldier in the field

The Service May Be Very Complicated Inside



All the other stuff in the computing center that shares the center, the WAN interfaces, and possibly storage, the local network infrastructure, sys admins, etc.

How Do I Decide Whether to Consume A Service From Someone?

Probably via a combination of things

1. The assertions of quality, reliability, functionality, security, etc. made by *the service provider*
   - *Backed up by measurements and data made by the service provider*
2. Audits of these assertions made by a third party
   - When audited, did the service meet (my community's) baseline controls & configuration standards
   - Does it still meet them RIGHT NOW?
   - If it doesn't, what's my risk to the vulnerabilities of the service? (a role for CVSS scores and a CVSS calculus?)

How Do I Decide? (part 2)

- I’ll also need to be able to consume these assertions & audits in a automated way (back to measurement and reporting standards)

- Especially since I need to understand the answer to the bigger question, namely…

…What Are the Security Properties of the Composition?

- How does all of this information roll-up to define readiness, compliance, & risk to my overall warfighting process?

- Automated measurement, and perhaps some method of totting-up vulnerabilities gives me a start at answering this

- *We're almost full circle to the mission owner*; it may be possible, with sufficiently rich and reliable information about the properties of all these services, to make meaningful choices about appropriate risk for a particular mission

Of Course There Are More Hard Problems With This

1. With whom am I willing to share information about my vulnerabilities?
    - …with whom *should* I share?

Hard Problems (2)

2. As a service consumer or mission owner, how much information about a service do I really need?
   - Vulnerability data without architecture data hard to interpret
   - Unless it’s essential, I don’t want to know the details of the innards of someone’s service
   - But, I do want to know how much to trust information I get from a service, and
   - I do want to know whether I can trust the service to properly protect information I give it

One More Topic…

…*Security*

Remember the Orange Book? (This is Really Ancient History)

(I personally have never seen an Orange Book, but some of the NIST and NSA people here are that old)

The Orange Book Specified Two Types of Things

1. Features

2. <u>Assurance</u>
(that those features work right)

Assurance? *What's That?*

- ***Trustworthiness*** of some property
  - (Is this property *worthy* of my trust? Is it good enough for my purpose?)

- ***Goes in and out of vogue***, except with bad guys

DoD (and all of us) Need Automation of Configuration, and of Measurement of Configuration

- But *bad guys often love centralization* (it can give them a high payoff if they can exploit the centralized function)

We must all avoid engineering-in weaknesses in our *centralization* of configuration or measurement functions

Back To Assurance

- **So, all those configuration automation & configuration measurement products *and processes* I'd like to see deployed in DoD must strongly resist attack**
  - By apparently trustworthy insiders
  - By attackers outside the system management center
  - By attackers modifying the descriptions or measurements between the description writer and the organizations consuming the description
  - Ditto between the central management console and the computer being configured or measured
  - Etc., etc., etc.

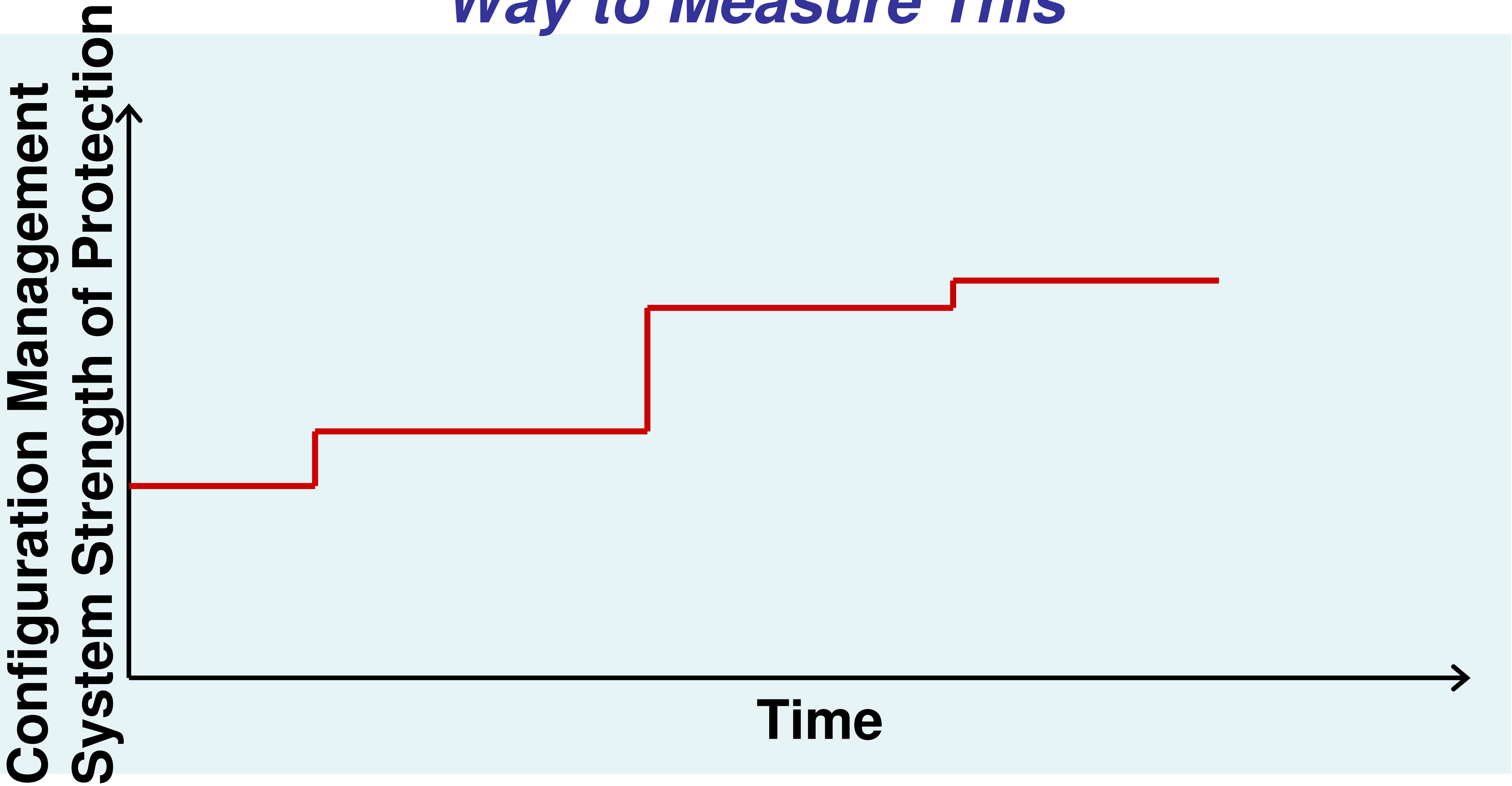
Assurance Needed in Many Places

- The description “supply chain” must provide a strong pedigree & provide integrity protection for configuration descriptions, measurement descriptions
- Strong, often two-way, authentication is needed in many interactions
  - For instance, between a central console and a computer being measured
- Integrity protection everywhere is essential
- The key management that may underlie these mechanisms and assurance must be strong
- …

But We Can Over Do Assurance Too Early, and Drive Non-Deployment of Essential Things

Yellow Book Lesson: Better Was the Enemy of Good Enough

Need Some Notion Of Steadily Increasing Assurance (of the security of the central managers, of the security of the description generation and distribution process, etc.) and a *Way to Measure This*



My Conclusions

- SCAP is *essential* to DoD
  - For security, mobility, speed, ability to work with ad hoc partners, etc.
- DoD must begin requiring SCAP compliance in various configuration and IA tools, date is TBD
- There is good potential for more standards and automation
- Security in the SCAP ecosystem and SCAP tools is fundamental if we’re to realize the promise of SCAP

www.disa.mil

iase.disa.mil

DEFENSE INFORMATION SYSTEMS AGENCY