NORTHROP GRUMMAN

Applying Protected Core Networking Concepts to Develop a Protected Trust Based Security Environment

Dennis McCallam
Principal Architect, Security
Northrop Grumman Corporation
October 2009

Agenda

- Current State of things
  - What about the threat
  - What are the problems we are trying to address
- A description of a Protected Core Network
  - As it relates to NATO coalitions
  - Why it is foundational to trust based security environments
- Features of a Protected Core Based Security Environment
  - Common services and a reference model
  - Deep dive on authentication

Protected Core Networking Improves Security

- **NATO’s next generation concept of coalition warfare**

- **A Protected Core is a transport network that:**
  - Offers transport service to users and primarily HIGH availability
  - Includes support for quality of service, priority handling, and security
  - Maintains service, even in situations with directed attacks
  - Set of Protected Core Segments working together (federated)

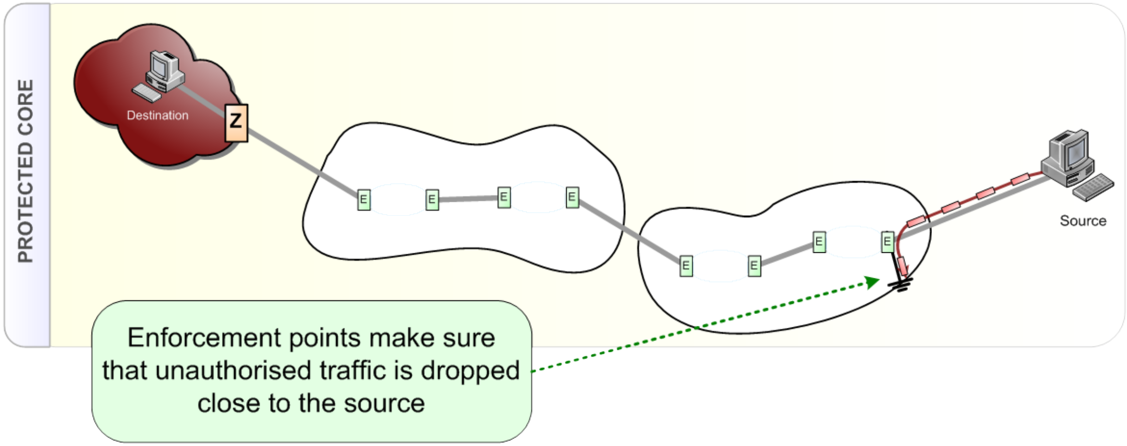
- Assumes security is handled by segment owners

- Its’ all about Availability, not Confidentiality and Integrity

Supports future military operations based on network enabled capabilities by providing the highest service availability.

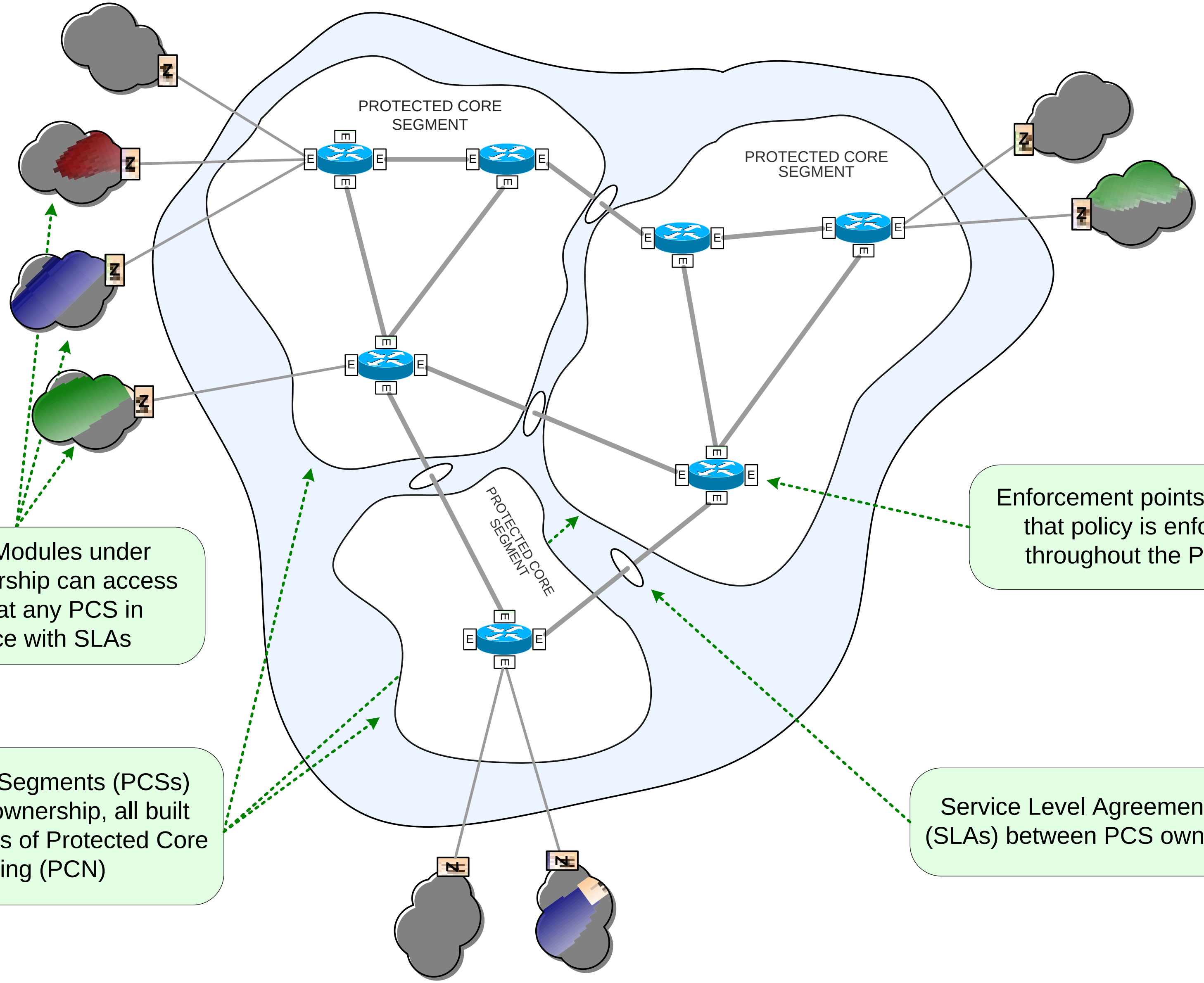
Definitions – How to construct a PCN

- The concept of Protected Core Networking:
  - Provide transport services in dynamic environments, focus on availability.
  - Utilizes multiple classes of network services for performance and security, and protection of all network components.
- A Protected Core Segment:
  - A network built on PCN working with other Protected Core Segments through Federation of Systems approach.
- A Protected Core:
  - Set of Protected Core Segments working together (federated) to achieve characteristics of Protected Core Networking.



Enforcement points make sure that unauthorised traffic is dropped close to the source

An Example PCore



Consumer Modules under different ownership can access the PCore at any PCS in accordance with SLAs

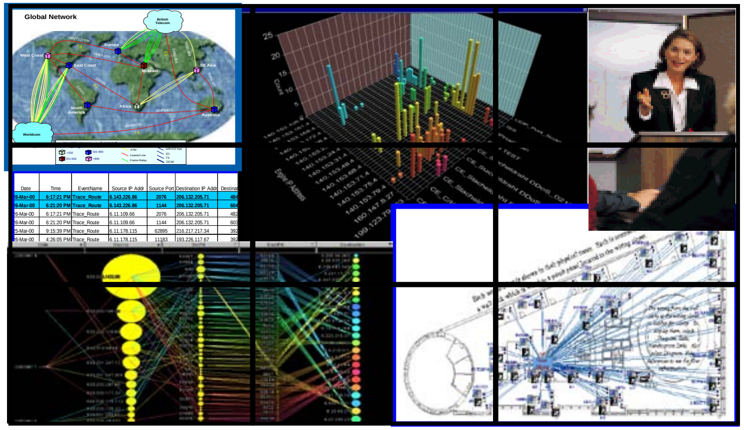
Protected Core Segments (PCSs) under different ownership, all built upon the principles of Protected Core Networking (PCN)

Enforcement points ensure that policy is enforced throughout the PCore

Service Level Agreements (SLAs) between PCS owners

Claims about applying PCN Concepts

- View this as an enterprise architecture framework
- Federated model widens attack surface
- Architecture built on trust, alleviates the need for some decisions……bake trust in
- Can develop autonomous yet integrated zones, a biological (even Borg) model
- “Value” of security is no longer linear
- Add Confidentiality and Integrity back in

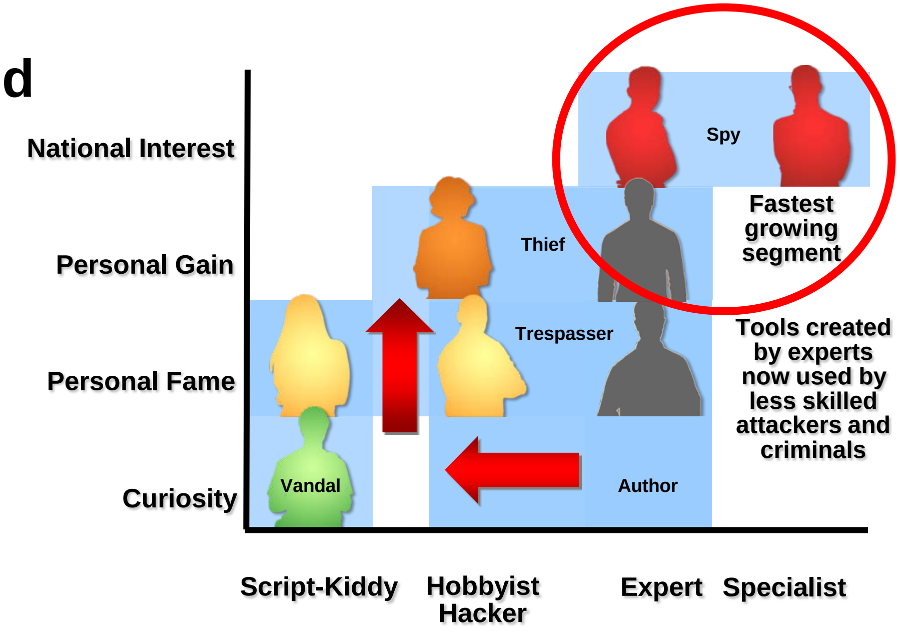


Date	Time	EventName	Source IP Addr	Source Port	Destination IP Addr	Destinat
26-Mar-00	6:17:21 PM	Trace_Route	6.143.226.86	2076	206.132.205.71	484
26-Mar-00	6:21:20 PM	Trace_Route	6.143.226.86	1144	206.132.205.71	604
26-Mar-00	6:17:21 PM	Trace_Route	6.11.109.66	2076	206.132.205.71	482
26-Mar-00	6:21:20 PM	Trace_Route	6.11.109.66	1144	206.132.205.71	603
25-Mar-00	9:15:39 PM	Trace_Route	6.11.178.115	62895	216.217.217.34	392
26-Mar-00	4:26:05 PM	Trace_Route	6.11.178.115	11183	193.226.117.67	392

Changing Threats To Data Security

The threat landscape has changed dramatically:

- They are persistent, sophisticated, and in some cases State sponsored
- Firewalls and intrusion detection devices can no longer keep the adversaries out of private networks
- They use common services that must be kept open on the firewalls in order for business to function
- They enlist the end user’s unwitting cooperation in order to insert themselves into the network

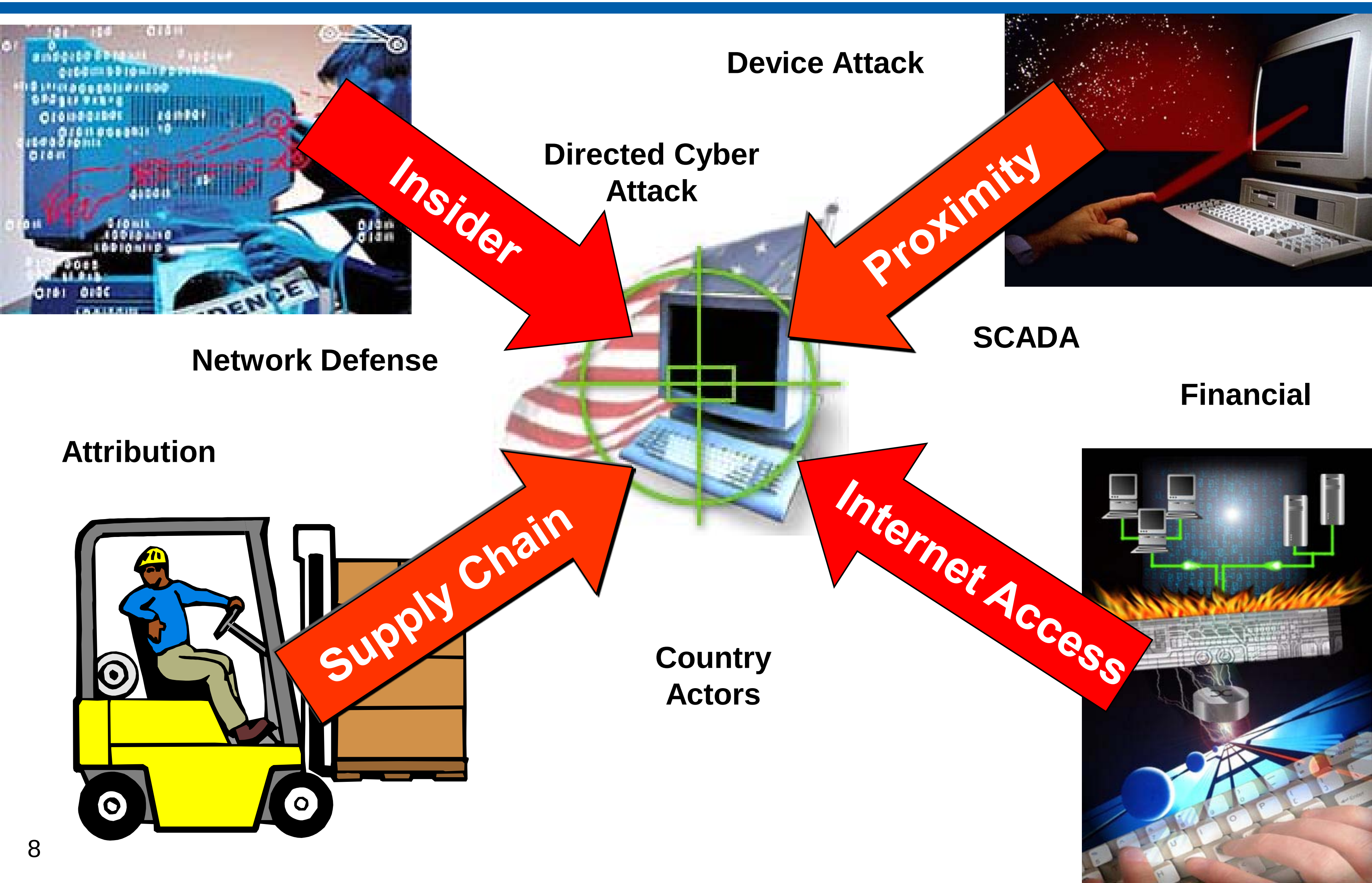


Fastest growing segment

Tools created by experts now used by less skilled attackers and criminals

Then	Now
Computer nerd	Determined, funded adversary
Thrill seeking	Profit or political gain
Illegal but benign	Criminal intent

The major threat vectors



Insider

Proximity

Supply Chain

Internet Access

Device Attack

Directed Cyber Attack

Network Defense

SCADA

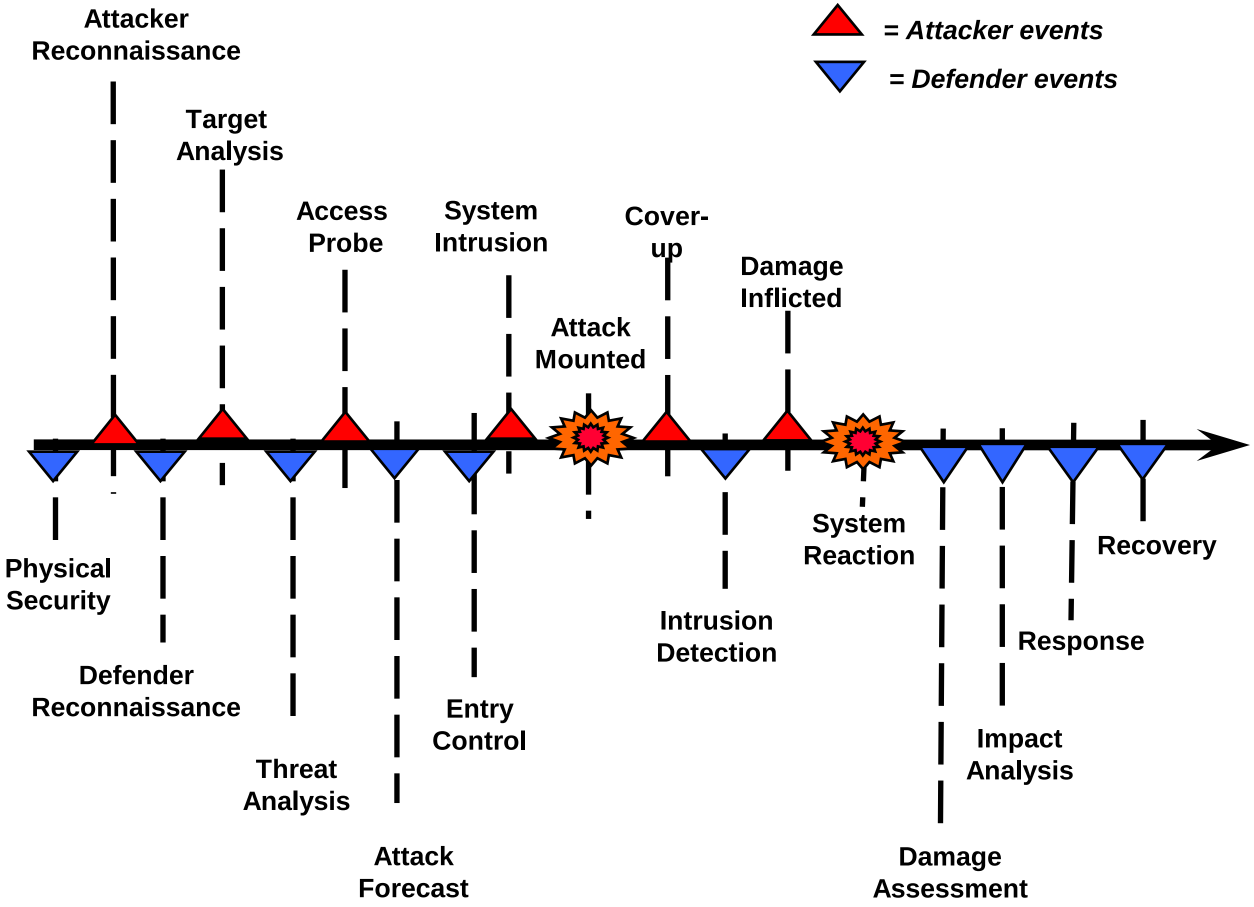
Financial

Attribution

Country Actors

Anatomy of an Incident

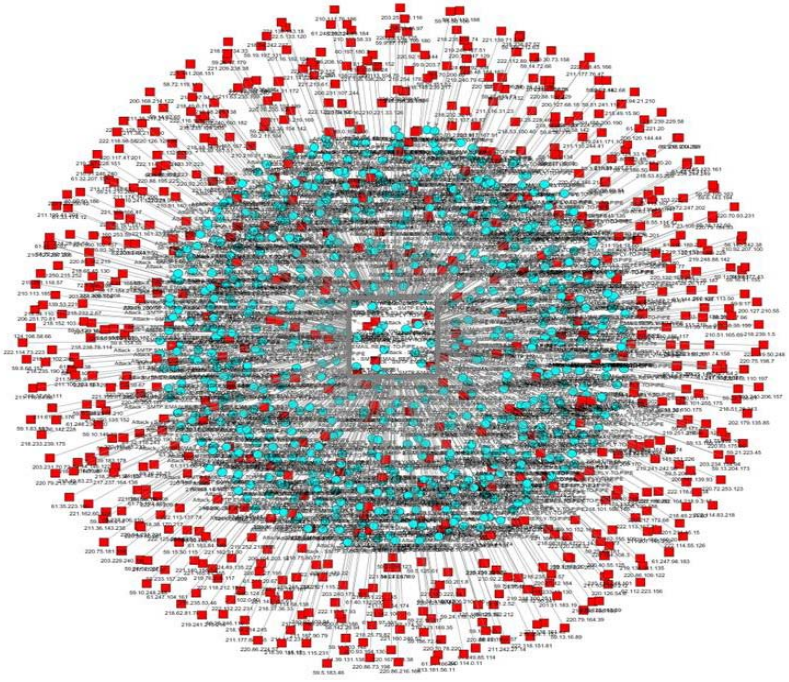
NORTHROP GRUMMAN



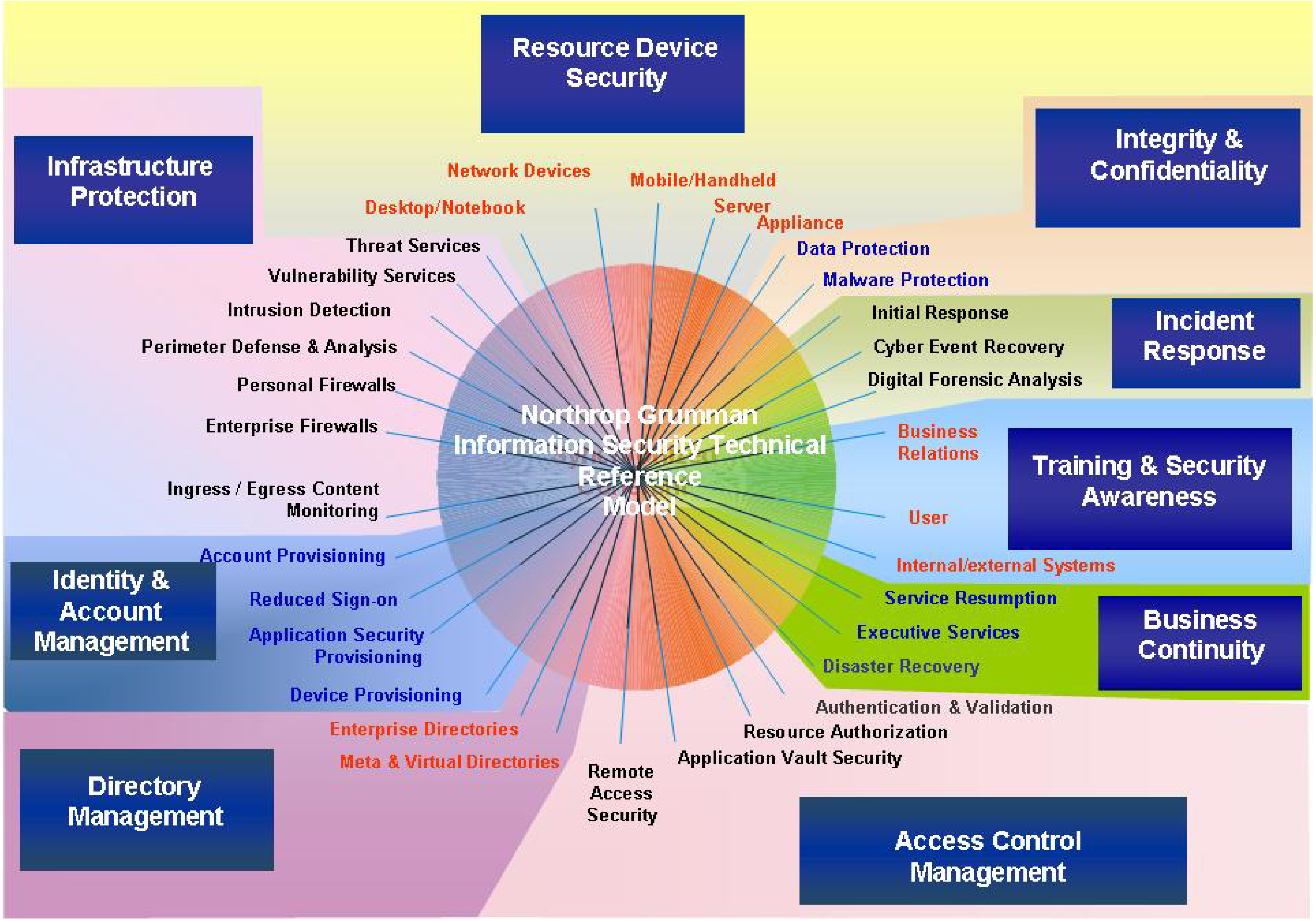
- Course look at the timeline of an attack showing more the reactionary state of defense
- How does this correlate to the Threat
- Issue becomes how to defend effectively at all points from a data view

Current Perimeter Centric Architecture

- Large flat network that is at best two-dimensional
- Protection mechanisms exist at the border where string authentication required
- Questionable configuration consistency - Data is scattered with multiple versions and copies
- International situation confusing due to information propagation and cross border data issues
- Protection uses risk as justification for investment



Security Architecture Components



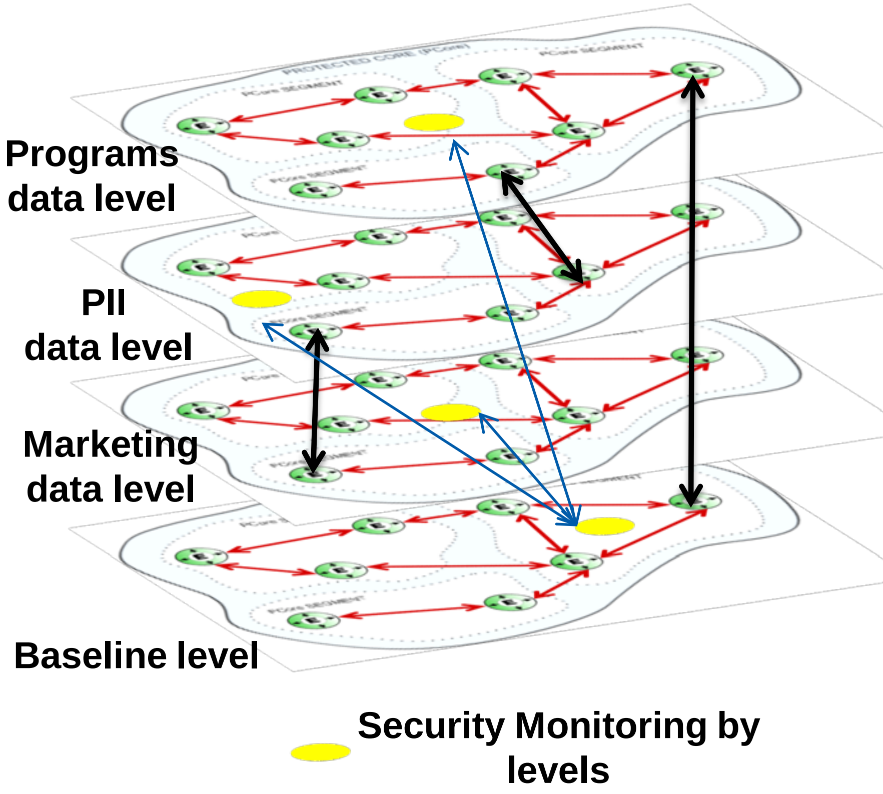
Technical reference model provides a "completeness" check

Security Architecture Description

- Everything being under the same roof gives latitude and allows for some “security truths” to be assumed
- Backup and contingency concepts have to be fully developed.
- Concept of hierarchical/federated security
  - Linkages between segments can be “understood” as part of the architecture components
  - Follow the precepts of minimal essential information: only the data that is absolutely required
  - Communications are encrypted and well defined
- Layered security reporting/auditing
  - Can establish a multi-tier approach to reducing data load, pre-process at edge points, aggregate at Core level
- Mini-management functions (Core and segment level)
- Credentialing
  - Well defined approach to vetting individuals and network components
  - Have functions for add/delete/modify for all actors
  - Credentials never passed in the clear, always encrypted
  - Federate the identity management and use certificates

Notional Architecture by Function

- Un-flatten the network
  - Opportunity with IPv6
  - Focuses security monitoring
  - Example here is via data
- Access
  - Tightly controlled
  - Can set in the paths
  - "Have to be in the right lobby to get the right door"
- Security Monitoring and Control
  - Local, allowing for disconnect if necessary
  - Reduction of information can begin at lower levels
  - Better ability to aggregate and react in real-time



Programs data level

PII data level

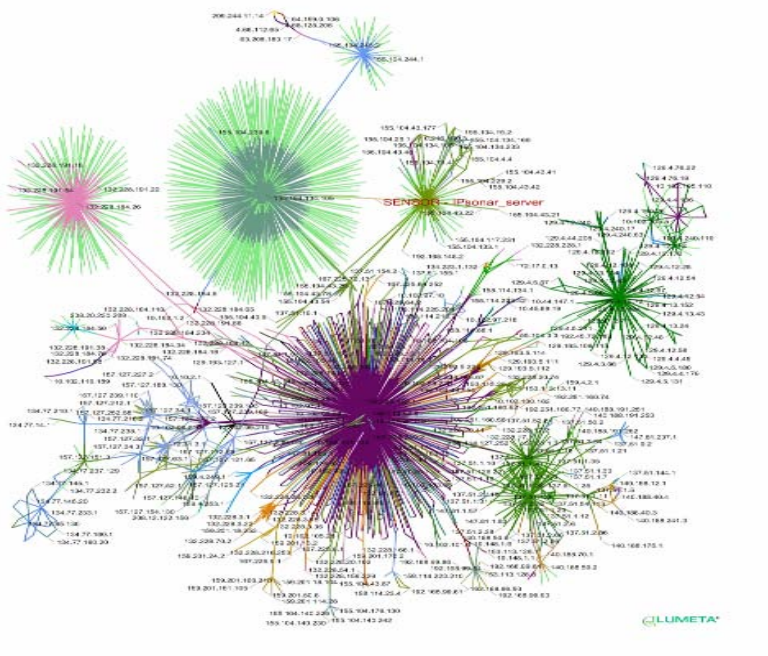
Marketing data level

Baseline level

● Security Monitoring by levels

Tracking information... the value of labeling

- Information tags/labels contain both attributes and policies
  - Data is labeled and tagged, therefore tracking throughout the system is straightforward
  - Cross border handling correlations can be easily done
- Indicates storage areas and network travel paths
- Identification analyzes duplication, confirming users roles and information use patterns
- Visually depicts the enterprise network and data types
- Can correlate who is using what, where it is being used, and how it is used.



Color coded view of the network and the information within

Variety in Authentication

Token	13th Century	Today
Name	William	Wmcleve2
Location	William of York	111.17.20.2
Hard (Provisioned) Possession	Medallion, sword, crest	Provisioned laptop, key fob, BlackBerry
Soft Possession	Password	Password
Appearance	Hair/eye/height	Facial scan
Knowledge	Secret	Secret
Biometric	Scar	Retina, fingerprint
Certification (3rd party verification)	Letter from king, with seal	Medium assurance soft PKI certificate

Authentication – Single factors

NORTHROP GRUMMAN

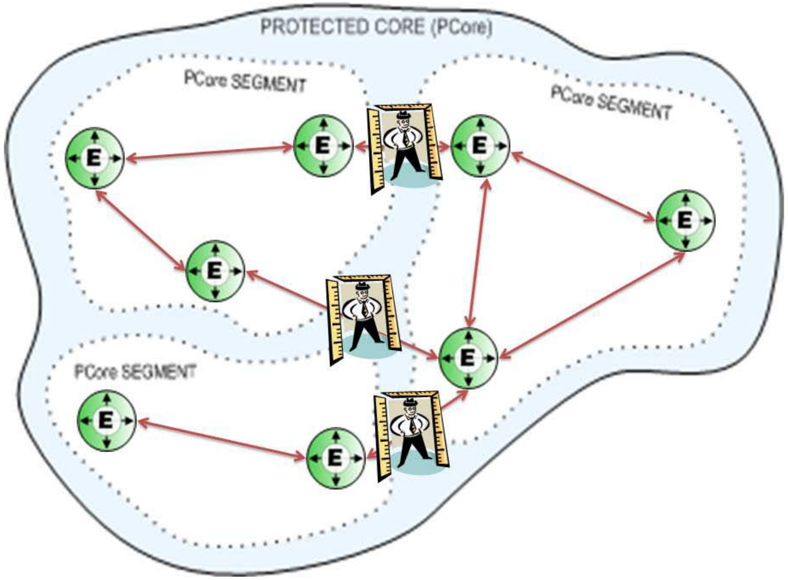
Method/Artifact	Assurance
Self-registered User ID/Shared Password/User Id	Little or no trust
Biometric: no control on biometric initialization.	Little or no trust
IP Address	Little or no trust
Private Password associated with User ID	Low Trust
Biometric: Trusted initialization local verification	Low Trust
Site Key	Low Trust
Biometric: Trusted initialization + central verification	Medium Trust
Trusted Medium assurance SW/ x.509 certificate	Medium Trust
One-time Password, Soft token	Medium Trust
RSA Hard token/PIN	Strong Trust
Medium Assurance HW/x.509	Strong Trust

Aggregation Results – Strength and Resilience

Aggregated Authentication Artifacts (examples)	
Active Directory Id and Password (AD/PW)	🟢
Site key + AD/PW	🟦
Enterprise medium assurance certificate + AD/PW	🟦
(RSA) One Time Password + AD/PW	◆
Medium assurance certificate + pin +AD/PW	◆
Trusted medium assurance certificate + verified biometric + AD/PW	◆ ◆
Properly provisioned laptop + fingerprint + physical access	◆ ◆

Implementing authentication in a PC environment

- Different segments can use different approaches
  - Have to know which credential is valid and from where in the architecture can it be invoked
  - Wide latitude of which piece of information ties to which credential
- Looking for 2 things:
  - Authentication Consistency – All facets of the data seem to match (Joe is on vacation, not in the plant, not on the interior network, on the portal)
  - Authentication Inconsistency – Something is out of line (Joe is on vacation, not in the plant, on the interior network, not on the portal)



"We must look for consistency. Where there is want of it we must suspect deception."

http://www.sherylfranklin.com/sh-gillette.html

Provisioning: an Authentication Artifact

- Requires a vetted and certified trusted provisioning process
  - User is vetted
  - Provided with laptop serial #aa-tt, that is fingerprint enabled
  - Certified/trusted examiner loads laptop TPM with user's fingerprint and locks it in
  - User plugs into internal corporate network, swipes finger, is authentication……no need for user id/password

- Why does this work?
  - User was properly vetted by organization
  - Laptop was specifically assigned to user
  - Laptop only accessible by user and selected admins
  - Fingerprint properly loaded and vetted serves as combination user id/password but is stronger
    - Laptop is something you have and was specifically assigned to you (so it is something you have and to some degree something you know and are)
    - Fingerprint is something you are

CAI Enhancements

- Can fully federate identities, ensuring current status are maintained
- Authentication approaches allow greater flexibility from the usual User ID/Password/Token/Card
- With federating the security monitoring functions, can be less reactive
- IPv6 offers greater control potentials

Summary

- Increased the bad guy expose time, have forced a lot of running the hallways to find the right door
- Attack sensed in one area allows for blocking that subnet stemming the infection
- Attacks learned in one segment are lessons to all segments
- Attack surface is not smooth, no guarantee for the attacker that entry in one area ensures freedom to other areas
- Adding/subtracting segments based on enterprise functionality
- Can monitor internal use/mis-use much better.

Assessment of the Challenges

• This is large undertaking but manageable (leverage IPv6)	◐	●	◐
• Requires re-thinking about architectures	●	●	●
• Technologies will enforce change	◐	◐	●
• Will result in new policies, directives, and SOP	●	●	
• Data identification and labeling becoming SOP	2 ●	◐	◐
• Investment has positive Enterprise impacts	◐	●	●

Legend ● **People** ● **Process** ● **Technology**

NORTHROP GRUMMAN