Boeing Technology
Information Technology

Some Thoughts on the Future of Information Security

Stephen T. Whitlock
Chief Strategist
Information Security
The Boeing Company

My 1999 Ten Year Predictions

- **Governance**
  - **BS7799 or derivative used to evaluate an organization's security capability**
- **Infrastructure**
  - **Middleware, web, e-mail and applications use common authentication and authorization services based on PKIs.**
  - **Information protection tightly coupled to the information**
    - **Encryption, Signatures, Labels**
    - **Digital signatures enjoy full legal standing**
    - **Signed XML labels control document access**
  - **Authentication**
    - **Password usage declines; Certificates and biometrics become common**
  - **Authorization**
    - **Enterprise authorization services replace existing services**
    - **Authorization data contained in LDAP schemas, cached in attribute certificates, accessed by common authorization**
  - **Merger of security services with system management services**
- **Network**
  - **Traditional firewalls replaced**
    - **Replacement forced by end-to-end encryption, massive data volumes and protocol proxying**
    - **Virus checking, intrusion detection sensors, data content monitoring move to hosts**
    - **Network devices still perform some network filtering based on IP addresses**
  - **Intrusion detection widely deployed**
  - **Encryption common at multiple network layers**
    - **IPSec, TLS, Application, etc**
- **Encryption**
  - **PKIs use common, protocols and profiles**
  - **X.509 certificates and LDAP based directories dominant**
  - **Smart cards and similar devices allow certificate portability**
  - **Hardware encryption engines will first augment then be included in CPUs**
  - **The AES winner becomes the default secret key algorithm**
  - **RSA & DH key algorithms need increased key lengths**
  - **Migration to SHA-1 from MD hash algorithms**

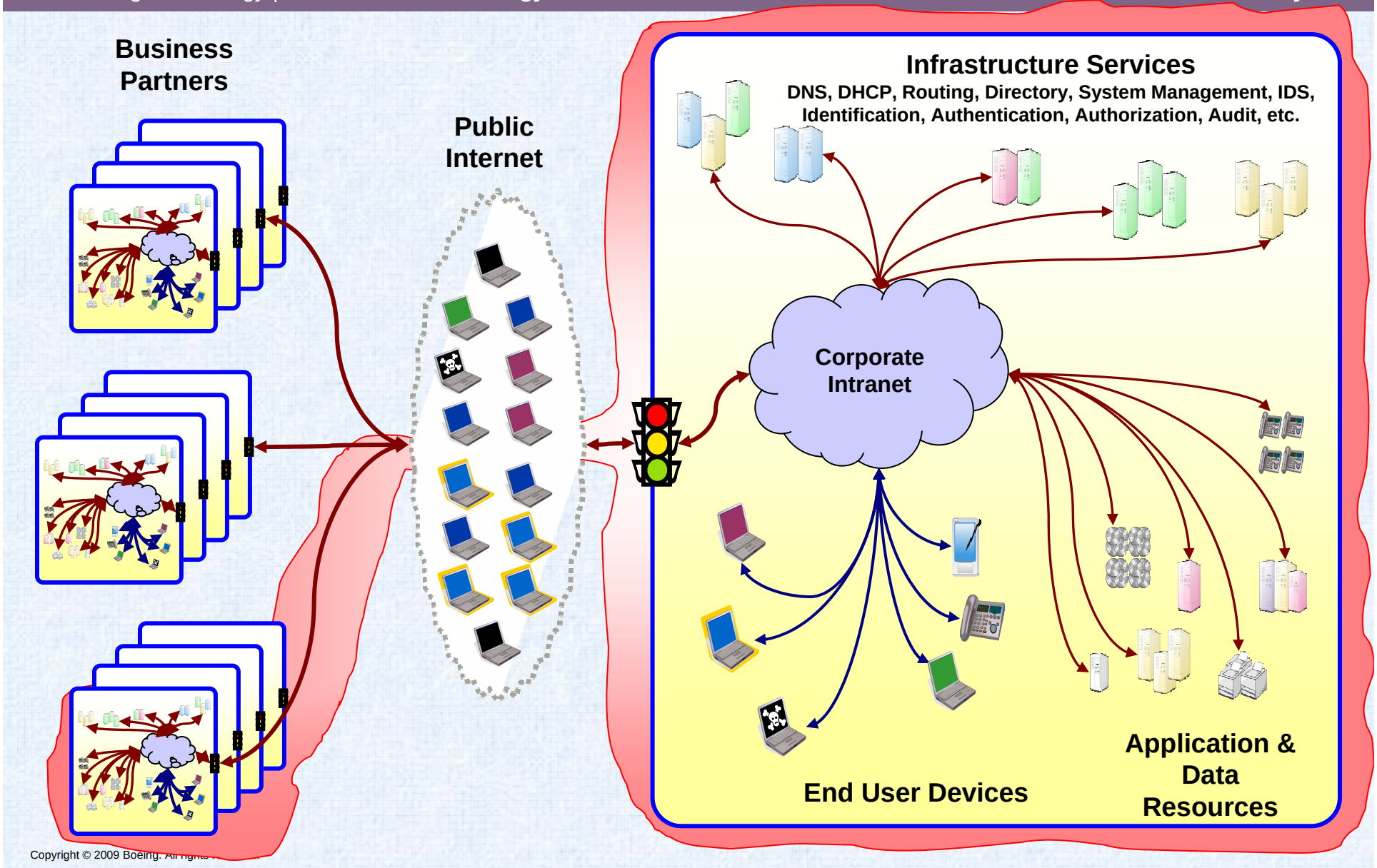
How did I do?

- **Governance**
  - **BS7799 or derivative used to evaluate an organization's security capability**
- **Infrastructure**
  - **Middleware, web, e-mail and applications use common authentication and authorization services based on PKIs.**
  - **Information protection tightly coupled to the information**
    - **Encryption, Signatures, Labels**
    - **Digital signatures enjoy full legal standing**
    - **Signed XML labels control document access**
  - **Authentication**
    - **Password usage declines; Certificates and biometrics become common**
  - **Authorization**
    - **Enterprise authorization services replace existing services**
    - **Authorization data contained in LDAP schemas, cached in attribute certificates, accessed by common authorization**
  - **Merger of security services with system management services**
- **Network**
  - **Traditional firewalls replaced**
    - **Replacement forced by end-to-end encryption, massive data volumes and protocol proxying**
    - **Virus checking, intrusion detection sensors, data content monitoring move to hosts**
    - **Network devices still perform some network filtering based on IP addresses**
  - **Intrusion detection widely deployed**
  - **Encryption common at multiple network layers**
    - **IPSec, TLS, Application, etc**
- **Encryption**
  - **PKIs use common, protocols and profiles**
  - **X.509 certificates and LDAP based directories dominant**
  - **Smart cards and similar devices allow certificate portability**
  - **Hardware encryption engines will first augment then be included in CPUs**
  - **The AES winner becomes the default secret key algorithm**
  - **RSA & DH key algorithms need increased key lengths**
  - **Migration to SHA-1 from MD hash algorithms**

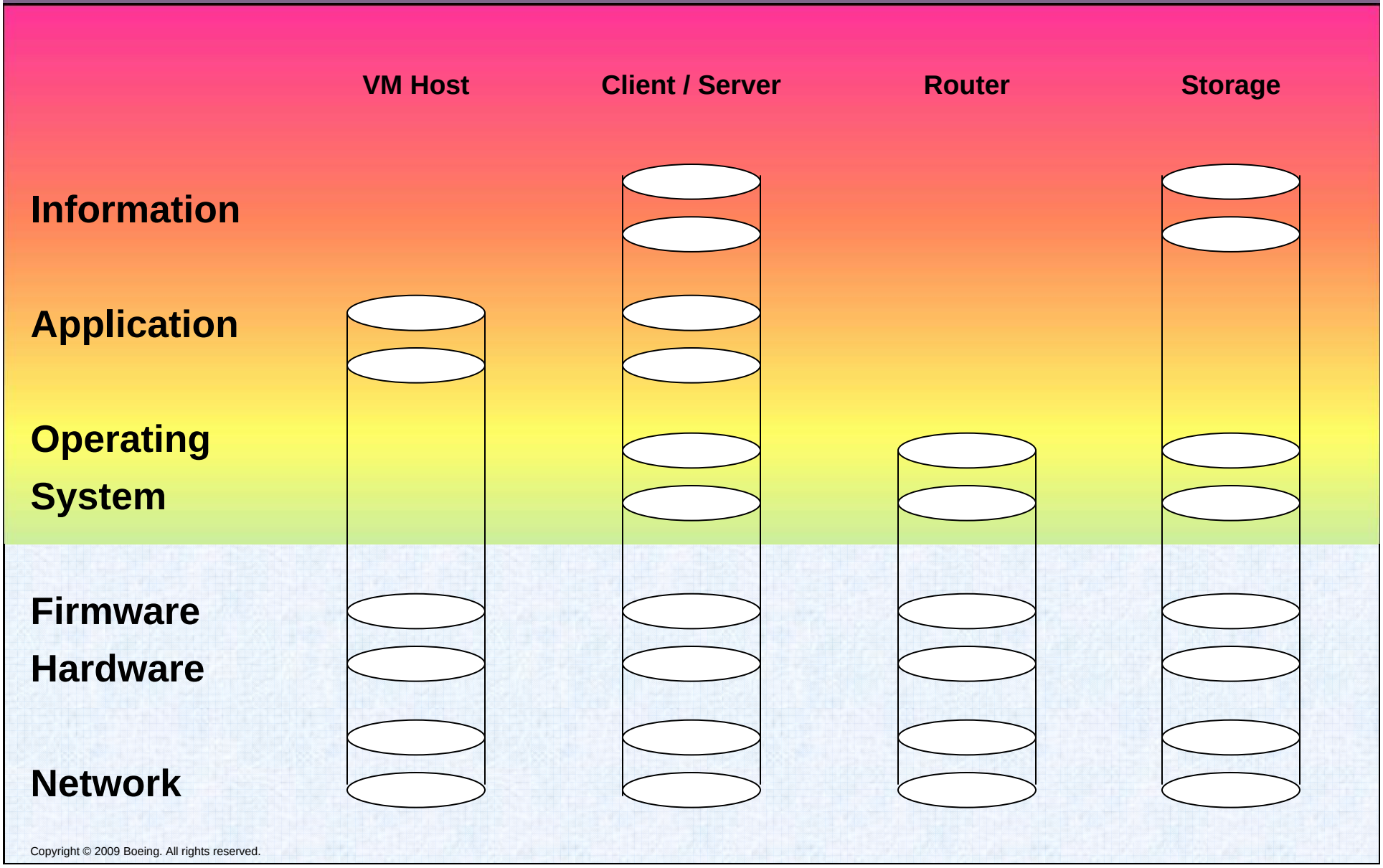
IT Security Challenges

- **Value – Corporate value has shifted from physical assets to information, making IT systems a target.**
- **Trust – The trend from monolithic corporations towards virtual enterprises creates an unstable workforce with shifting loyalties.**
- **Sentience – The emergence of intelligent devices challenges traditional notions of identity and authentication.**
- **Regulation – The proliferation of complex legal and regulatory requirements challenges enterprises that operate globally under different jurisdictions.**
- **Balance – The prevalence of dictatorial over negotiable security technologies presents a roadblock to enterprise collaboration.**
- **Division – Continued reliance on perimeter based security disrupts either the availability or consistency of information and application services.**
- **Usability – New generations of security technologies strain users with unnatural tasks and inconsistent interfaces.**

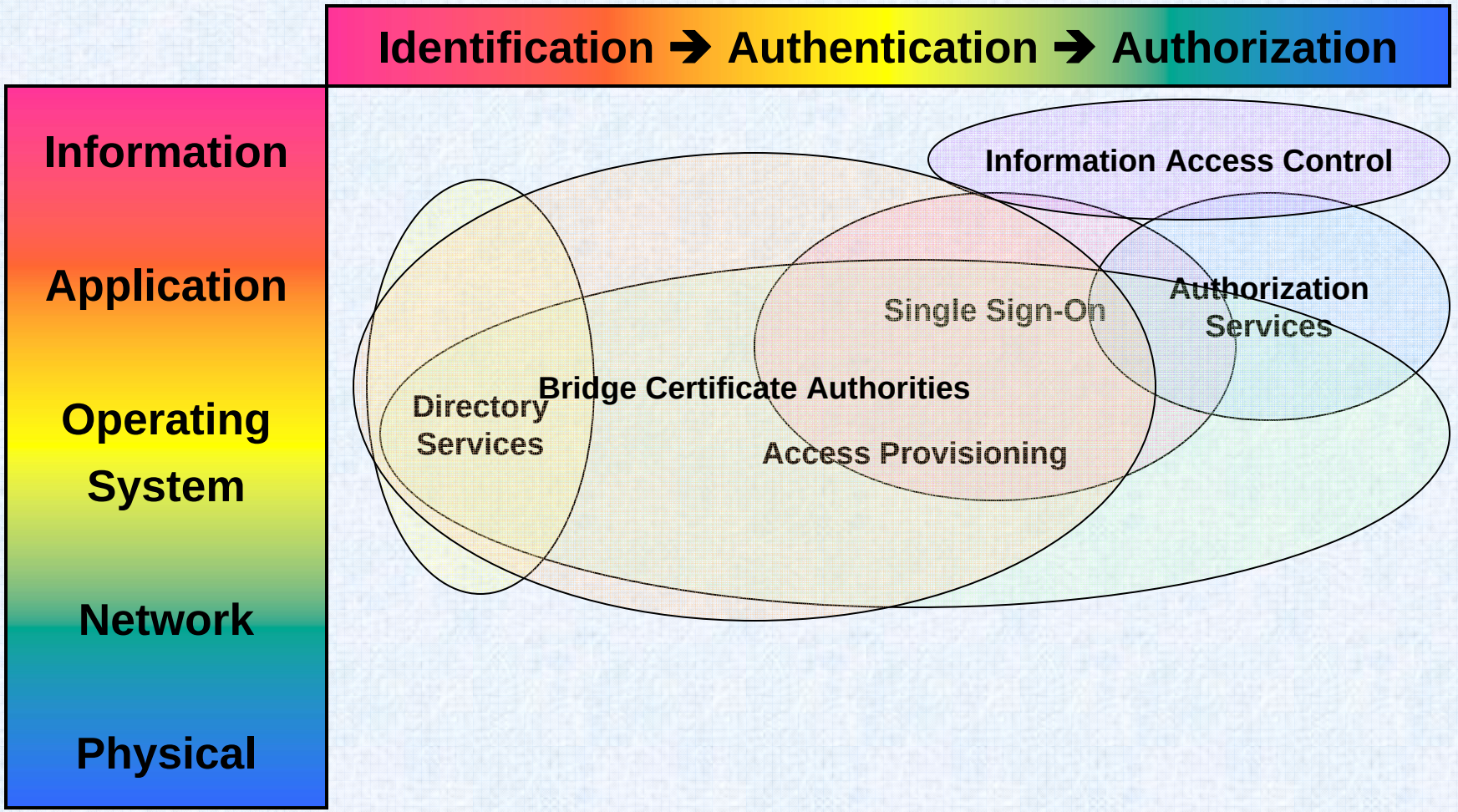
Typical IT Security Trust Boundary



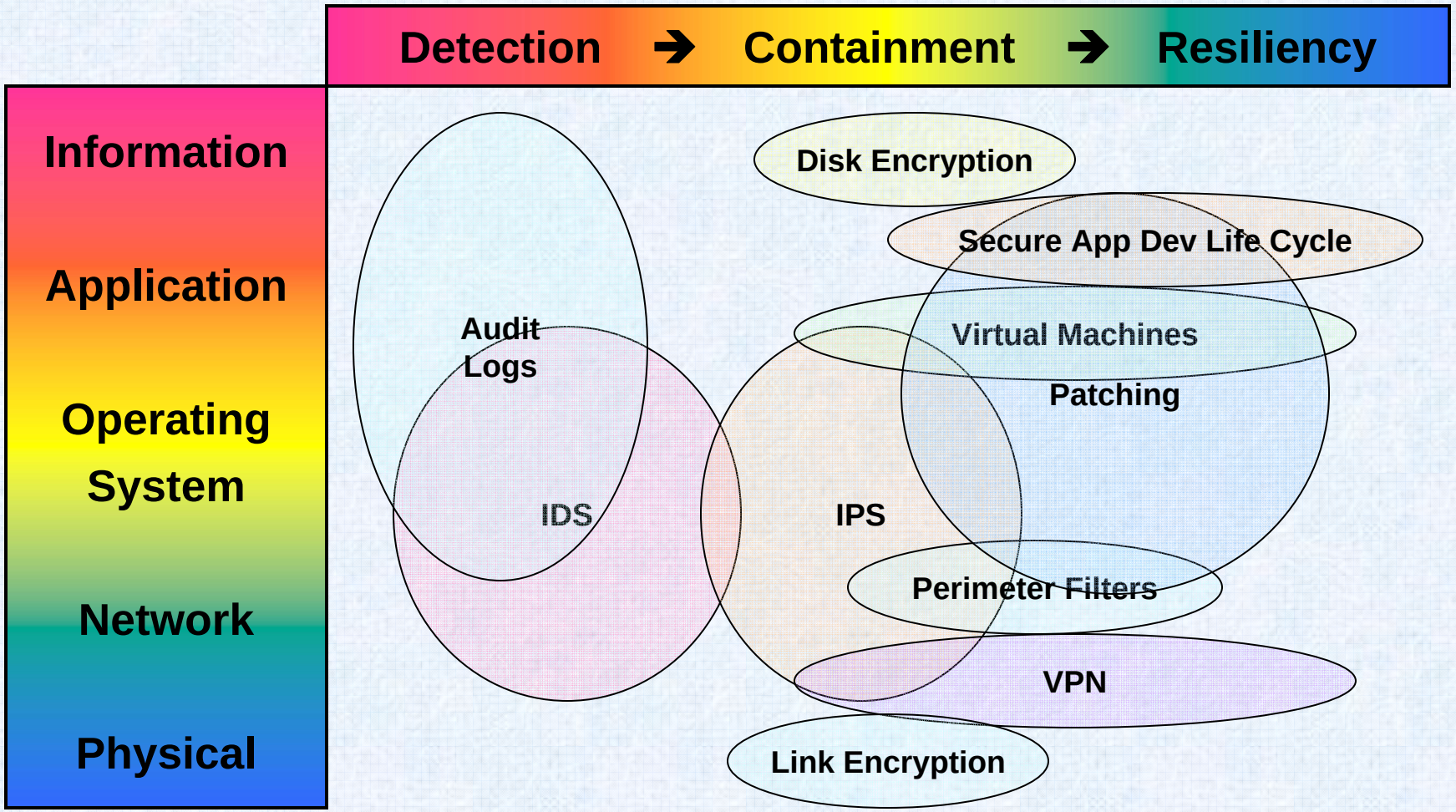
Trust Boundary Layer Examples



Collaboration Security Approach

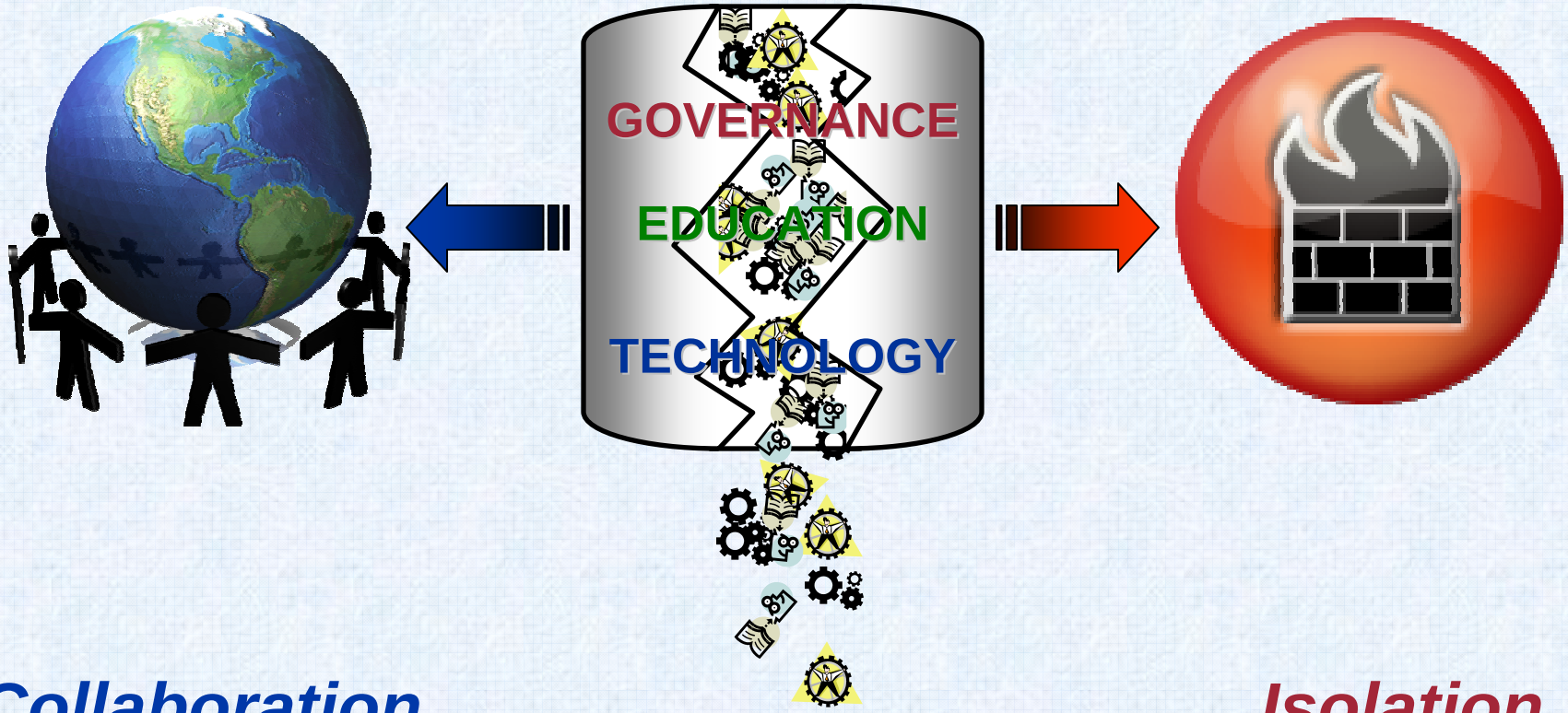


Isolation Security Approach



Security Tension – Conflicting Goals

Security Program



Collaboration ***Isolation***

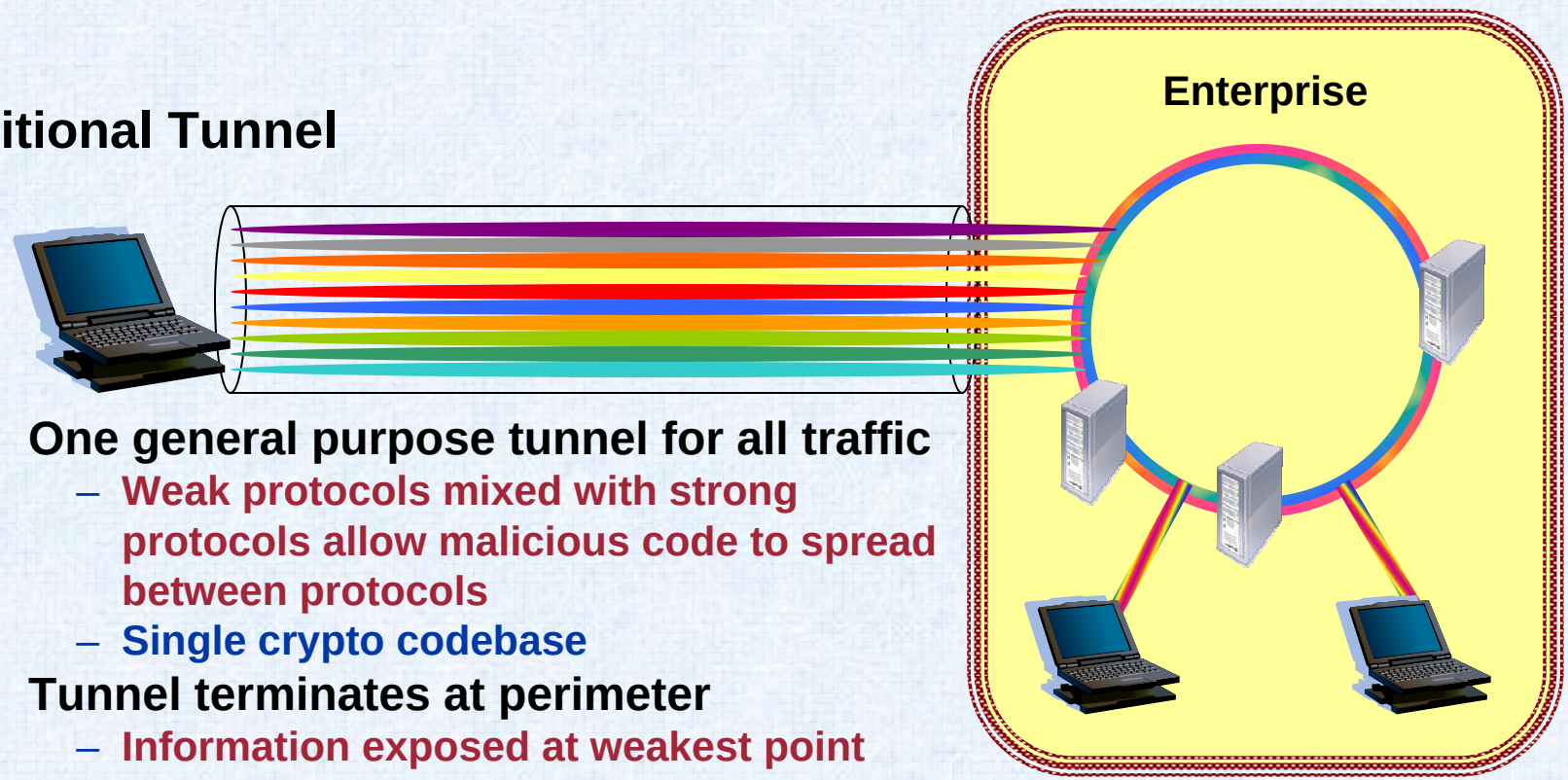
Are We Trying to Protect Too Much?

- **Communication Challenges**
  - **Network to network VPNs are too global**
  - **General purpose VPNs mix services and the related risk**
- **Environment Challenges**
  - **Information must be opened in a safe environment**
  - **Current Operating Systems and Applications are too large and too complex to secure**
- **Information Challenges**
  - **Volume is increasing faster than manageability**
  - **Information protection tools either lack granularity, don't scale, or don't work between enterprises**

Reducing the Communication Attack Surface

Communication Attack Surface – Current State

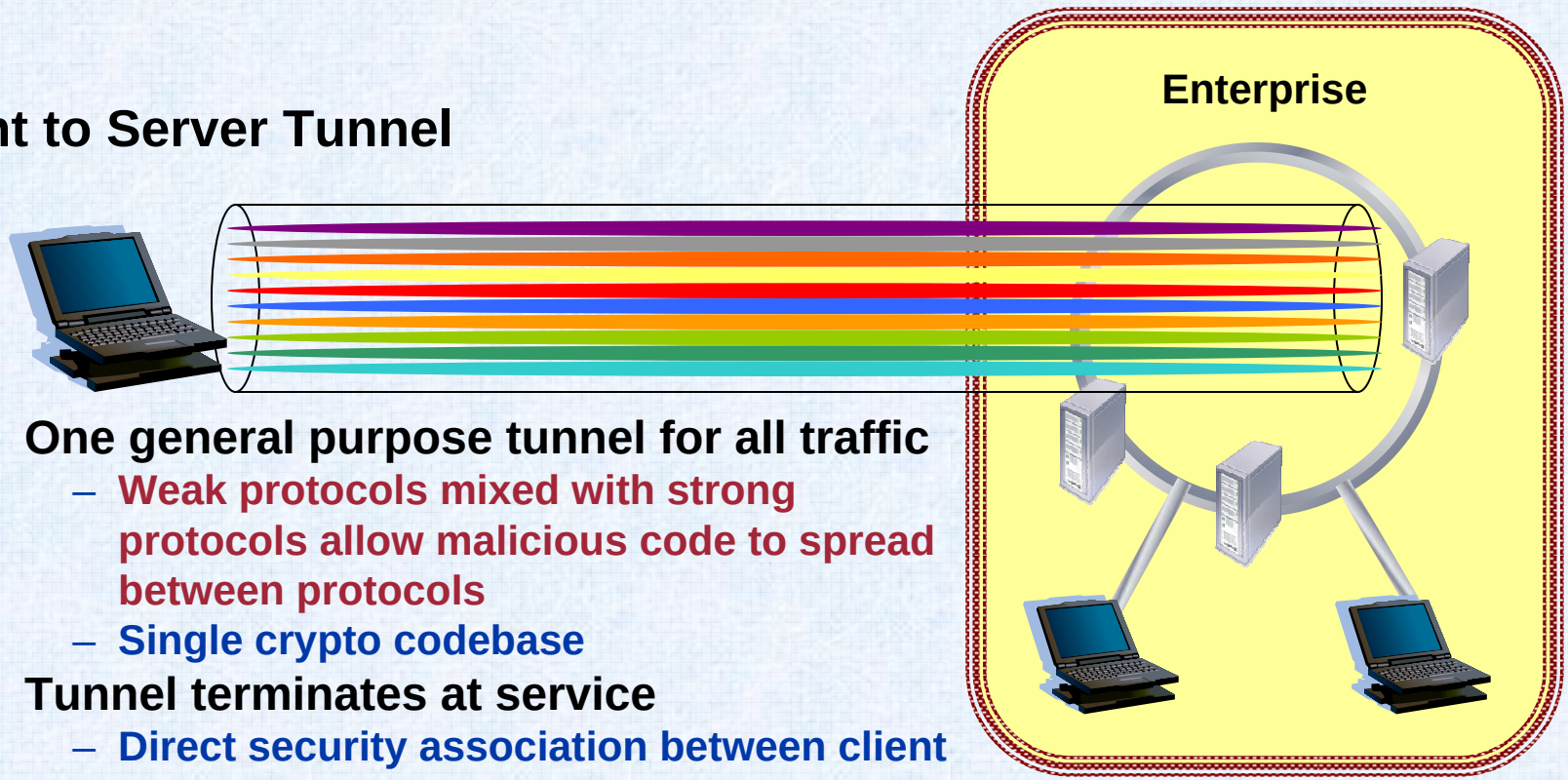
Traditional Tunnel



- One general purpose tunnel for all traffic
  - Weak protocols mixed with strong protocols allow malicious code to spread between protocols
  - Single crypto codebase
- Tunnel terminates at perimeter
  - Information exposed at weakest point
  - No security association between client and server
  - Traffic mixed on intranet allowing malware to spread
  - Easy to inspect traffic

Communication Attack Surface – Direct Connections

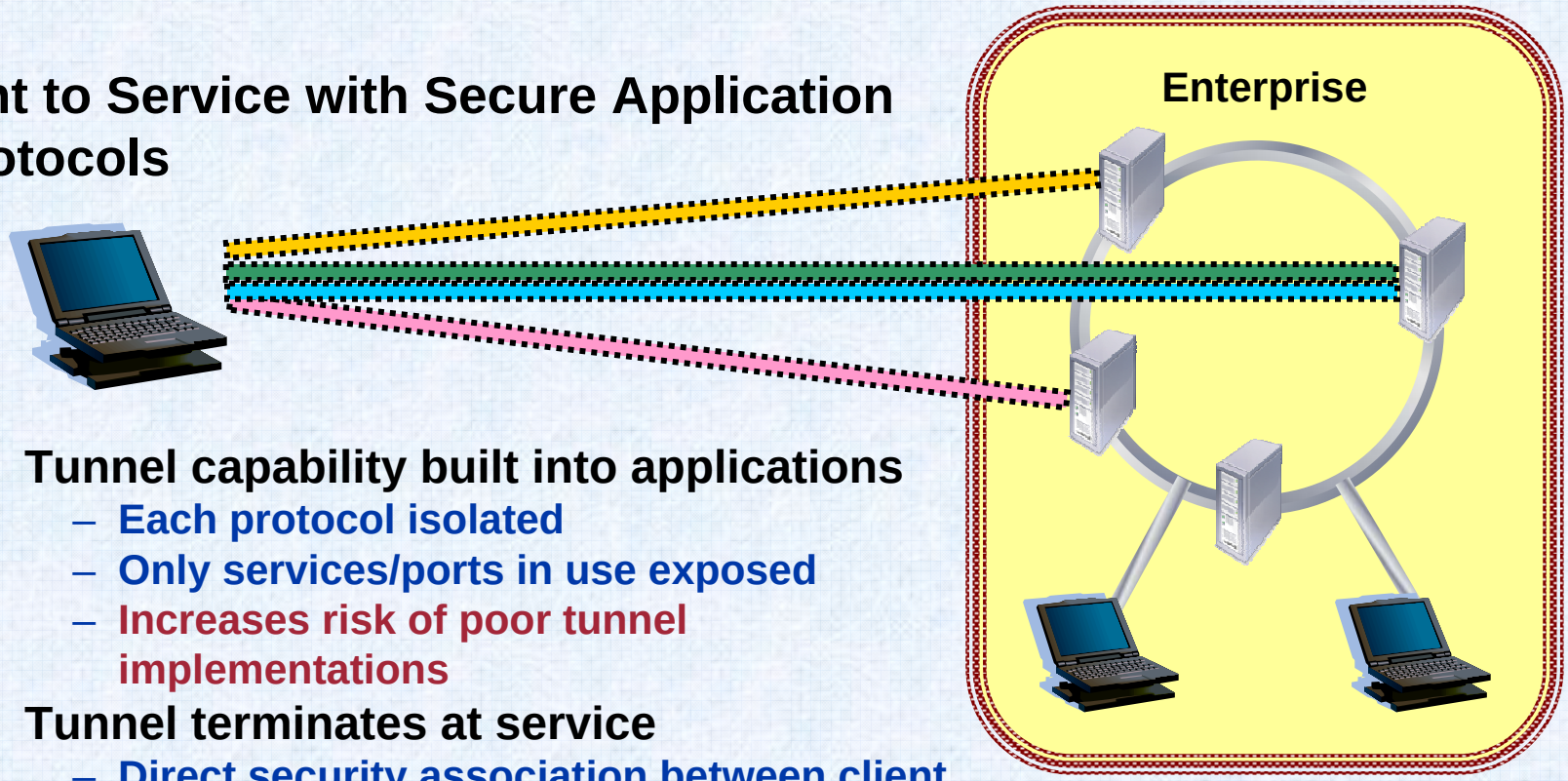
Client to Server Tunnel



- One general purpose tunnel for all traffic
  - Weak protocols mixed with strong protocols allow malicious code to spread between protocols
  - Single crypto codebase
- Tunnel terminates at service
  - Direct security association between client and server
  - Traffic not available to intranet
  - Perimeter not needed
  - Difficult to inspect traffic or block malware at perimeter

Communication Attack Surface – Secure Protocols

Client to Service with Secure Application Protocols



- **Tunnel capability built into applications**
  - **Each protocol isolated**
  - **Only services/ports in use exposed**
  - **Increases risk of poor tunnel implementations**
- **Tunnel terminates at service**
  - **Direct security association between client and server**
  - **Traffic not available to intranet**
  - **Perimeter not needed**
  - **Difficult to inspect traffic or block malware at perimeter**

Maturity

- **Reasonably Mature**
  - **Direct Connection examples**
    - **SSH**
    - **Windows 7 DirectAccess**
  - **Secure Protocol Examples**
    - **E-Mail - SMTP / TLS**
    - **Remote Access – RDP / TLS**
    - **EDI - AS2 (RFC 4130)**
- **More Information**
  - **http://www.opengroup.org/jericho/InhSecComs.pdf**
- **Estimated Timeframe: Now – 2 Years**

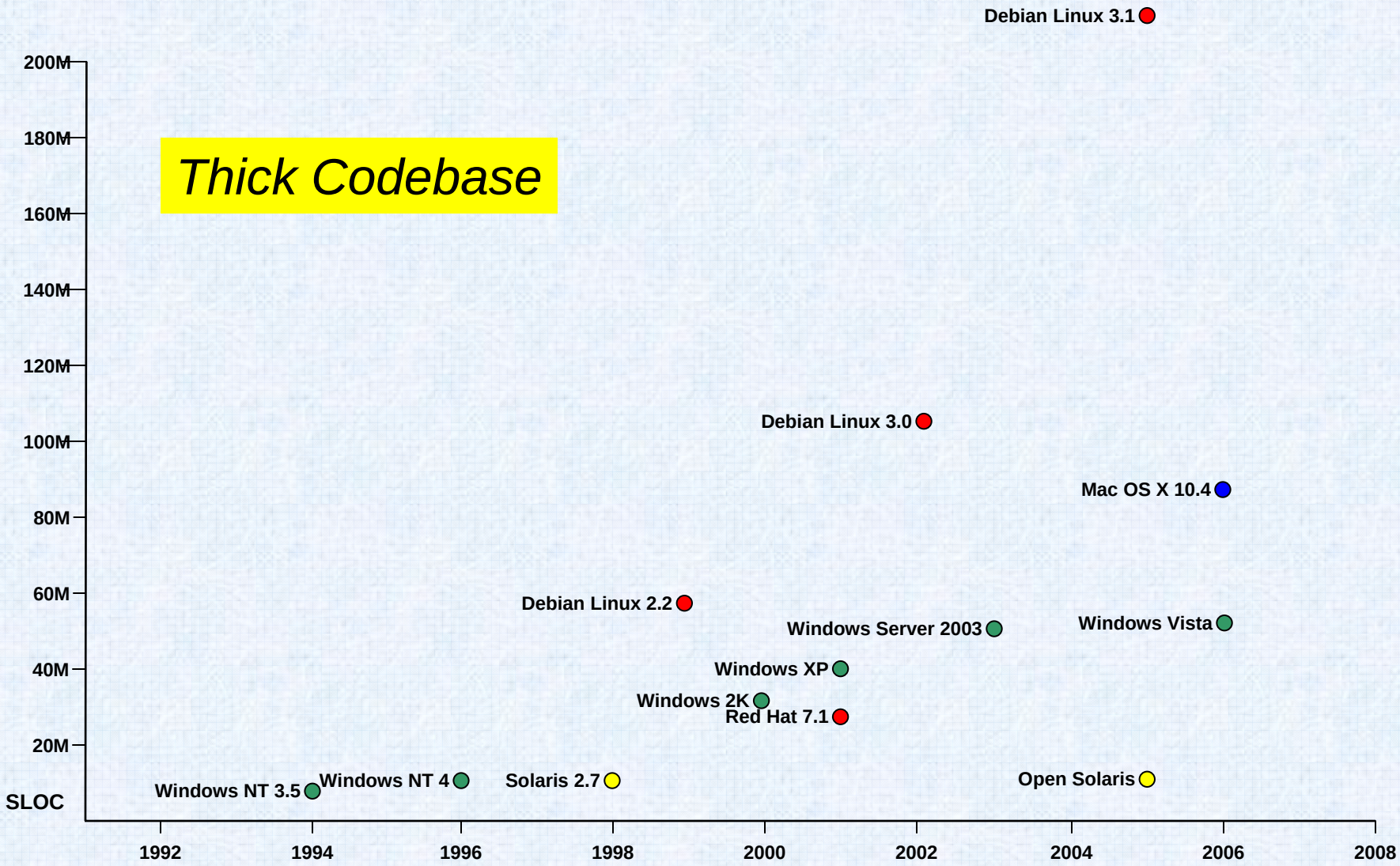
Reducing the Environment Complexity

Boeing Technology | **Information Technology** **Information Security**

Modern Operating Systems

Rich Functionality

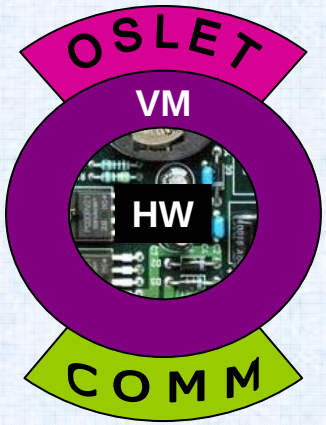
Source Lines of Code for Some OS (Wikipedia)



Use Virtual Machines to Shrink Attack Surface

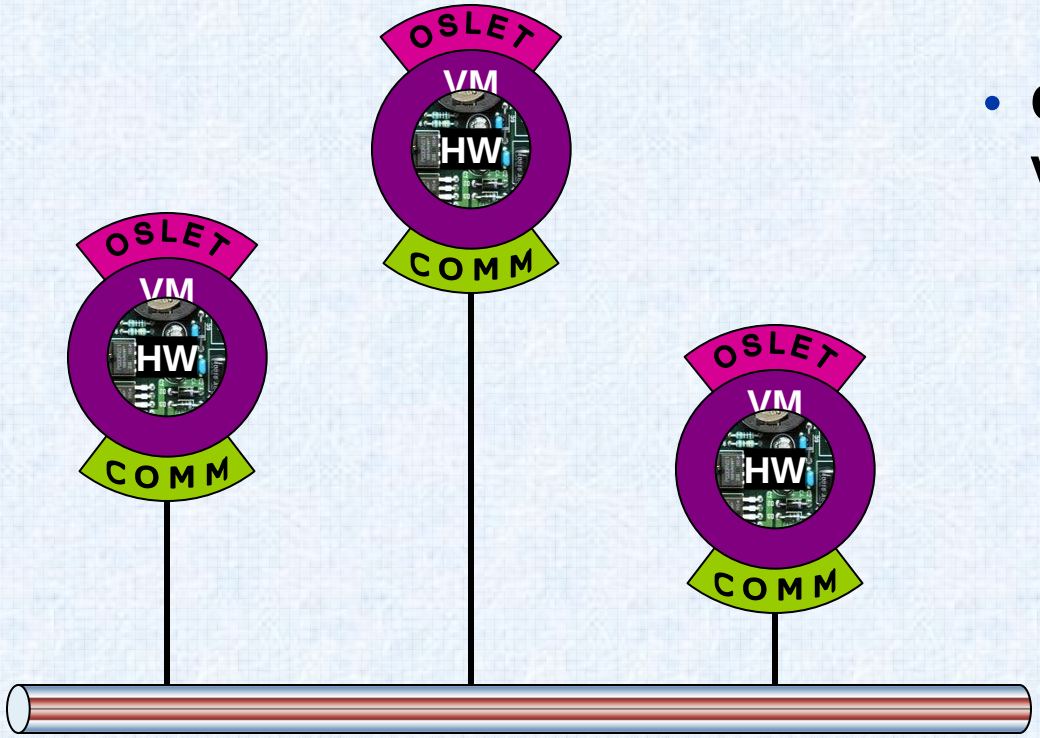
- **Codebase is measured in KBytes instead of MBytes**
  - **Size is within reach of correctness proof capability**
- **Separate VMs used for dedicated sub-OS functions**
- **Similar structure for complex applications**
- **Separate VMs for critical, normal, and high risk functions and applications**

Structure



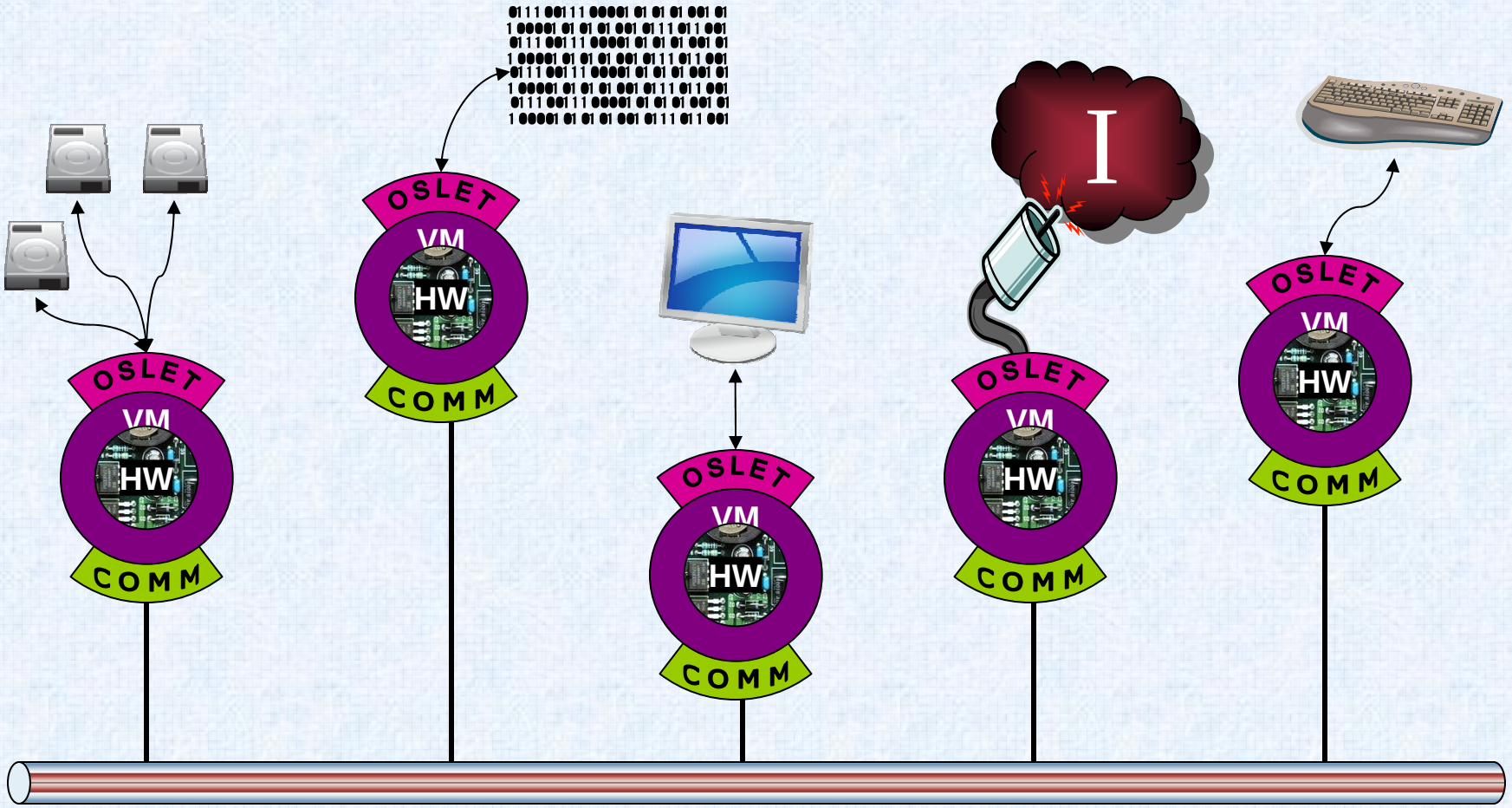
- **VM running on hardware**
- **OSlet - Application or driver specific piece of OS code to connect VM to application or hardware**
  - **Unique OSlets for different tasks or services**
  - **Pre-Built OSlets created, certified and distributed as images**
- **Secure communication service running on VM**
  - **Filter services**
  - **VPN services**

OSlet Communication & Validation

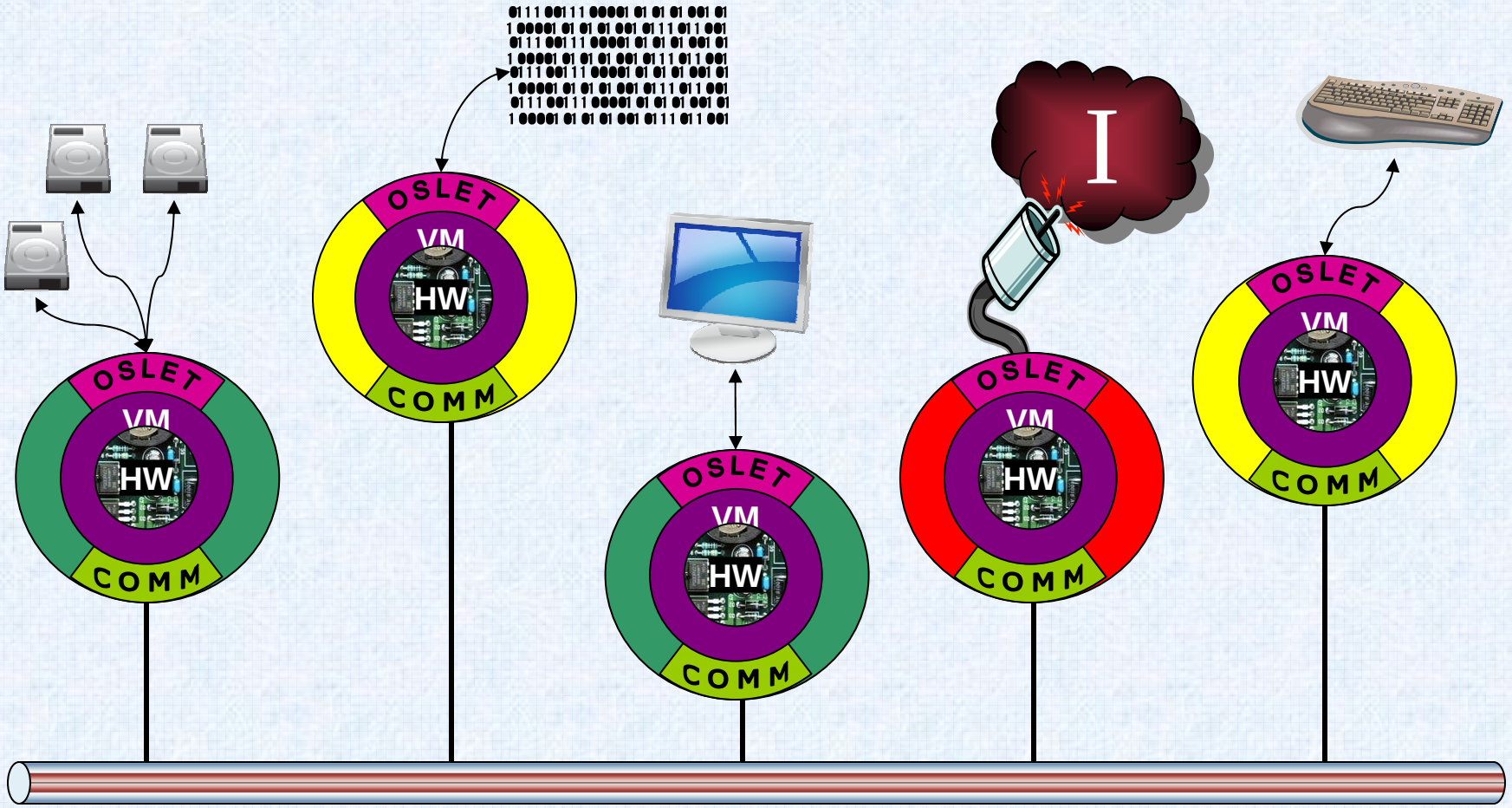


- **Communication security**
  - **Confidentiality**
  - **Authentication**
  - **Security Association**
- **OSlet correct state validation**
  - **Security association between OSlets**
  - **Verified Software State**
  - **Security Operating Level**
  - **Environmental Risk**
  - **Candidate Protocols**
    - **IETF NEA**
    - **TCG IF-MAP**

Example OSlet Services

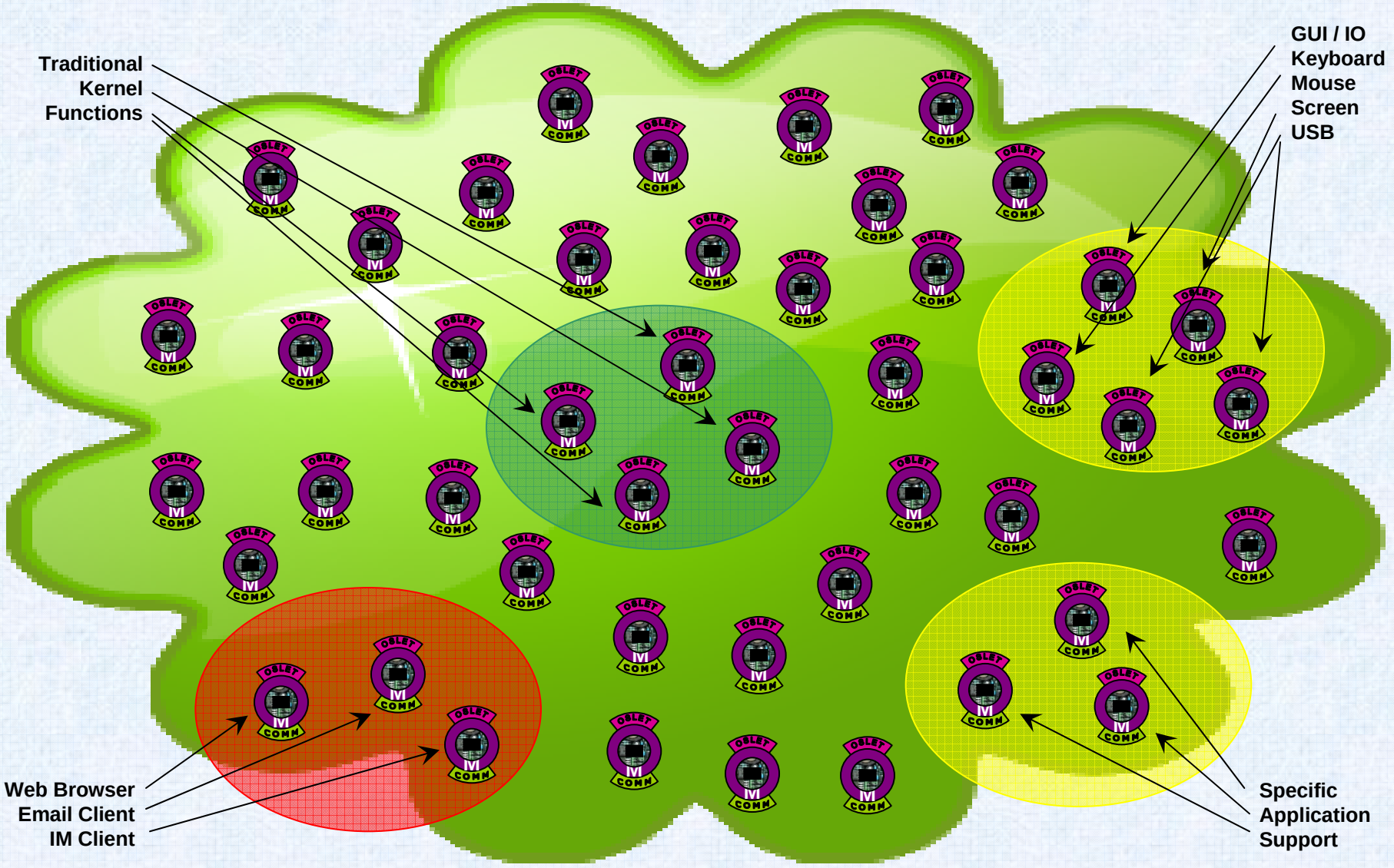


Different OSlet Trust Levels

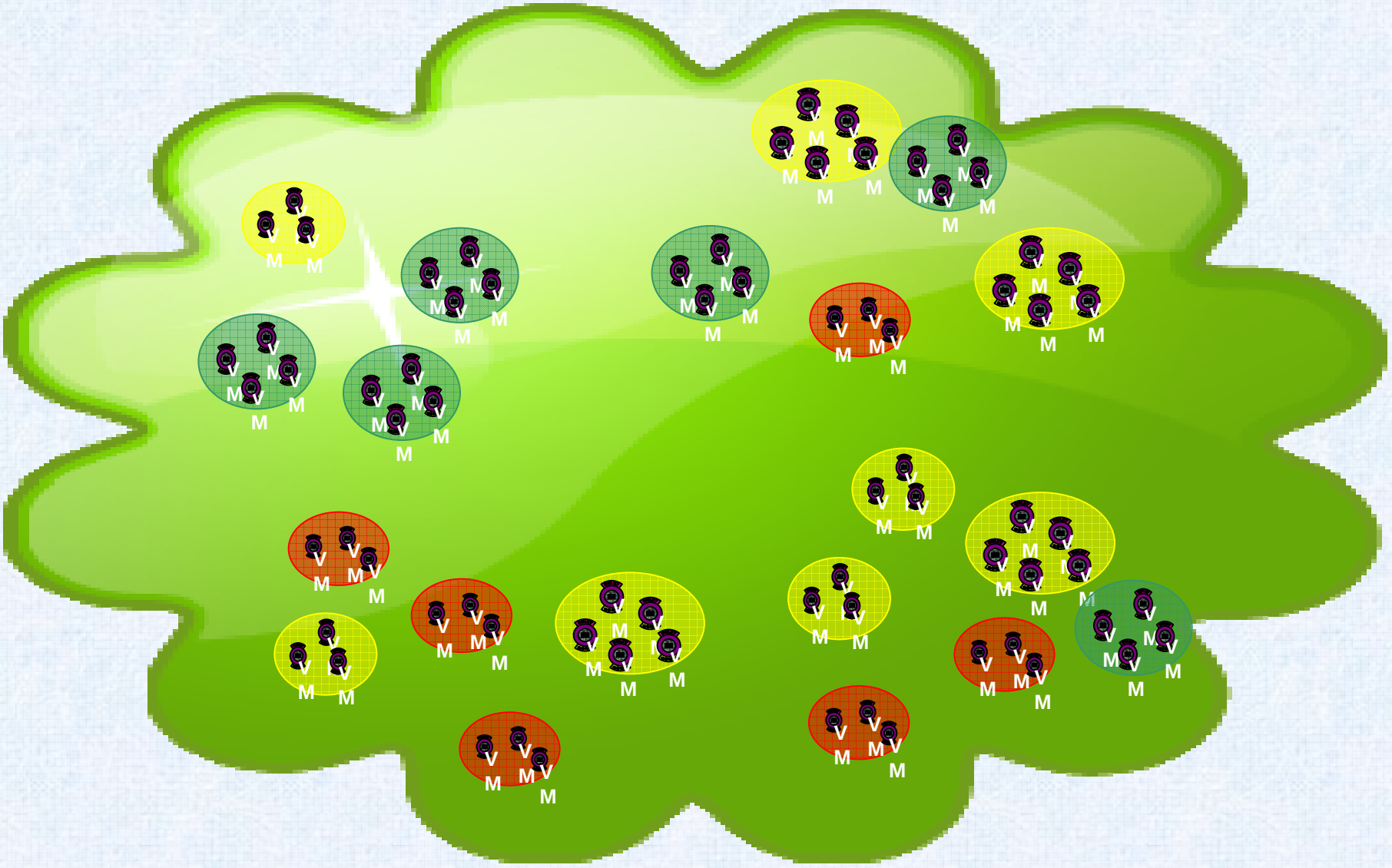


Many OSlets Support Necessary OS Functionality

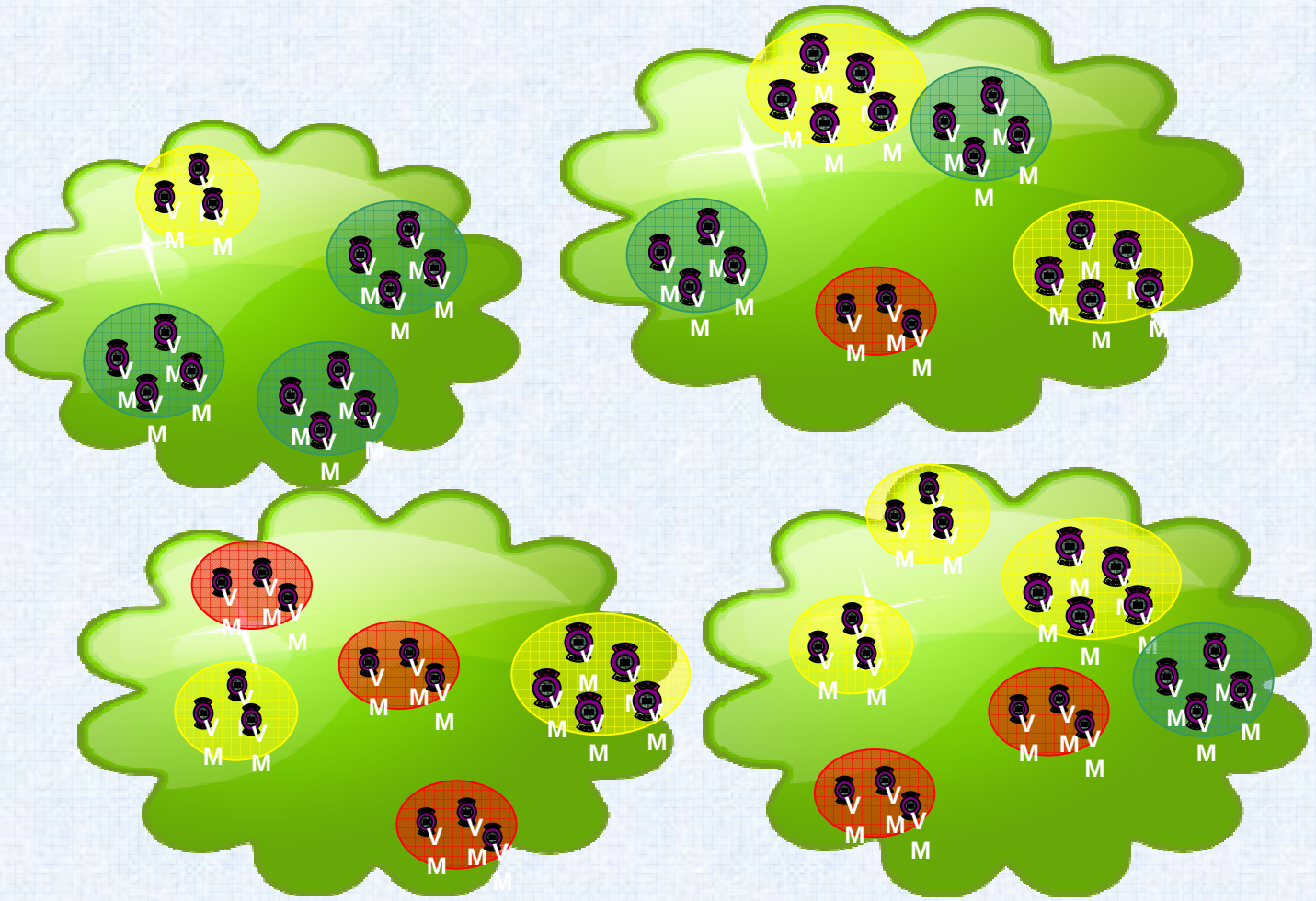
Granular OSlet Clusters Provide Specific Functions



OSlet Based OS Physically Contained



OSlet Based OS Distributed Over Internet



Maturity

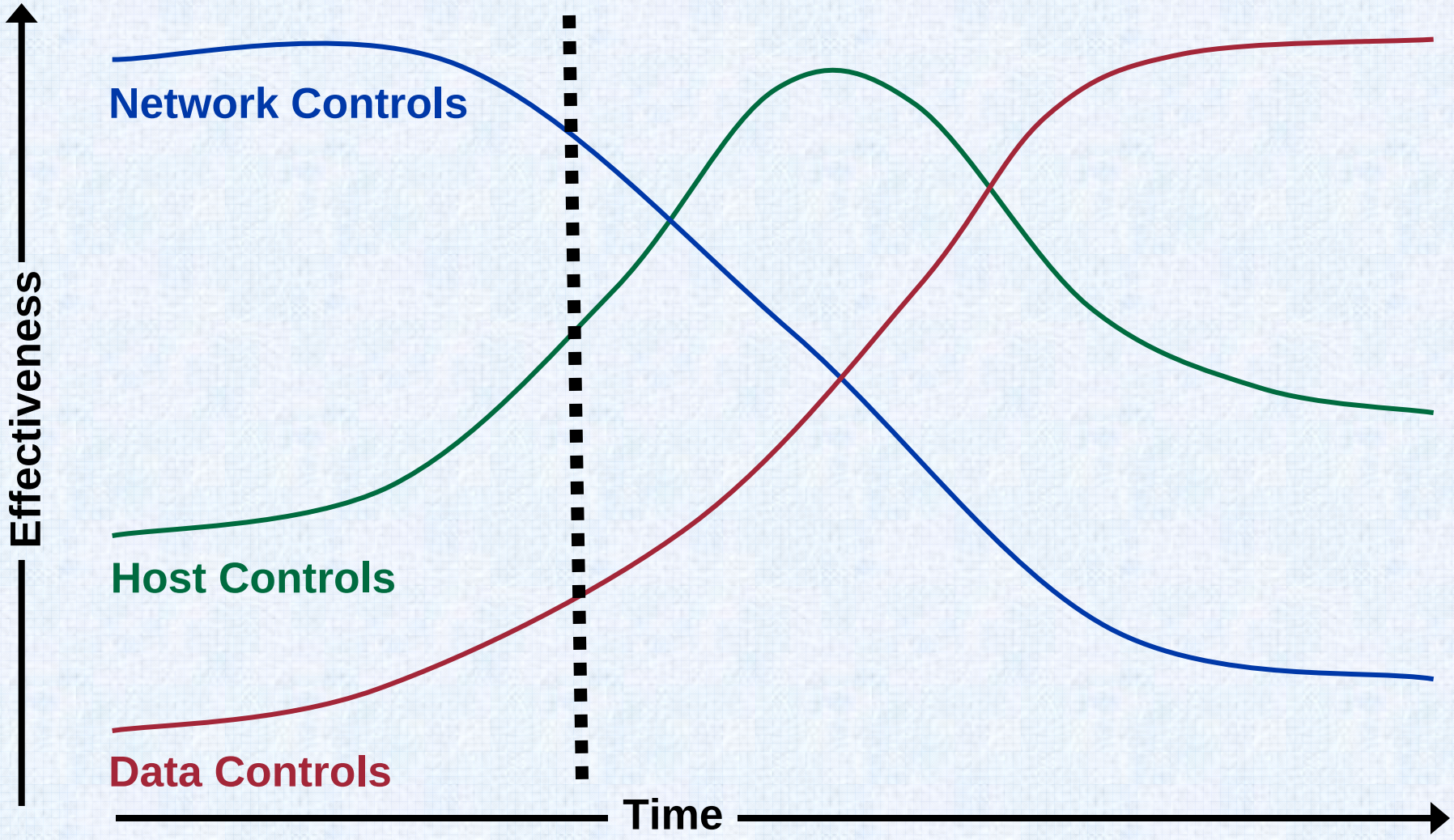
- **Reasonably mature**
  - **Virtual machine technology**
  - **Code analysis tools**
  - **Secure tunnel technology**
  - **Filter / firewall technology**
- **Less mature**
  - **Security association protocols (IF-MAP, NEA)**
  - **Distributed OS functionality**
  - **Distributed application functionality**
- **Even less mature**
  - **How distributed can you make a functioning OS or application?**
  - **What can be evolved from distributed kernels, pre-boot environments and similar technology?**
- **Estimated Timeframe: 2-5 Years**

Virtual Machine RFI

- 1.0 Background
  - In August 2007, the US Deputy Secretary of Defense directed the Assistant Secretary of Defense for Networks and Information Integration to develop and implement a comprehensive approach for safeguarding unclassified information.
  - To facilitate this effort, the Defense Industrial Base Cyber Security / Information Assurance Task Force was established to develop the processes and capabilities needed.
  - A technology and architecture team was chartered to investigate innovative, future-looking approaches to today's problems.
- 1.1 Intent of the RFI
  - It is the intent of the ASD office to use this market research to explore the feasibility and maturity of virtualization-based security solutions and identify organizations which have plans to or experience in providing them.
  - Specifically, the DIB Task Force is interested in exploring the availability of virtualization-based commercial solutions for the following problems in network security:
- https://www.fbo.gov/spg/ODA/WHS/REF/HQ003409TSB0710_01/listing.html

Information Protection Challenges

An Information Centric Future of Access Controls

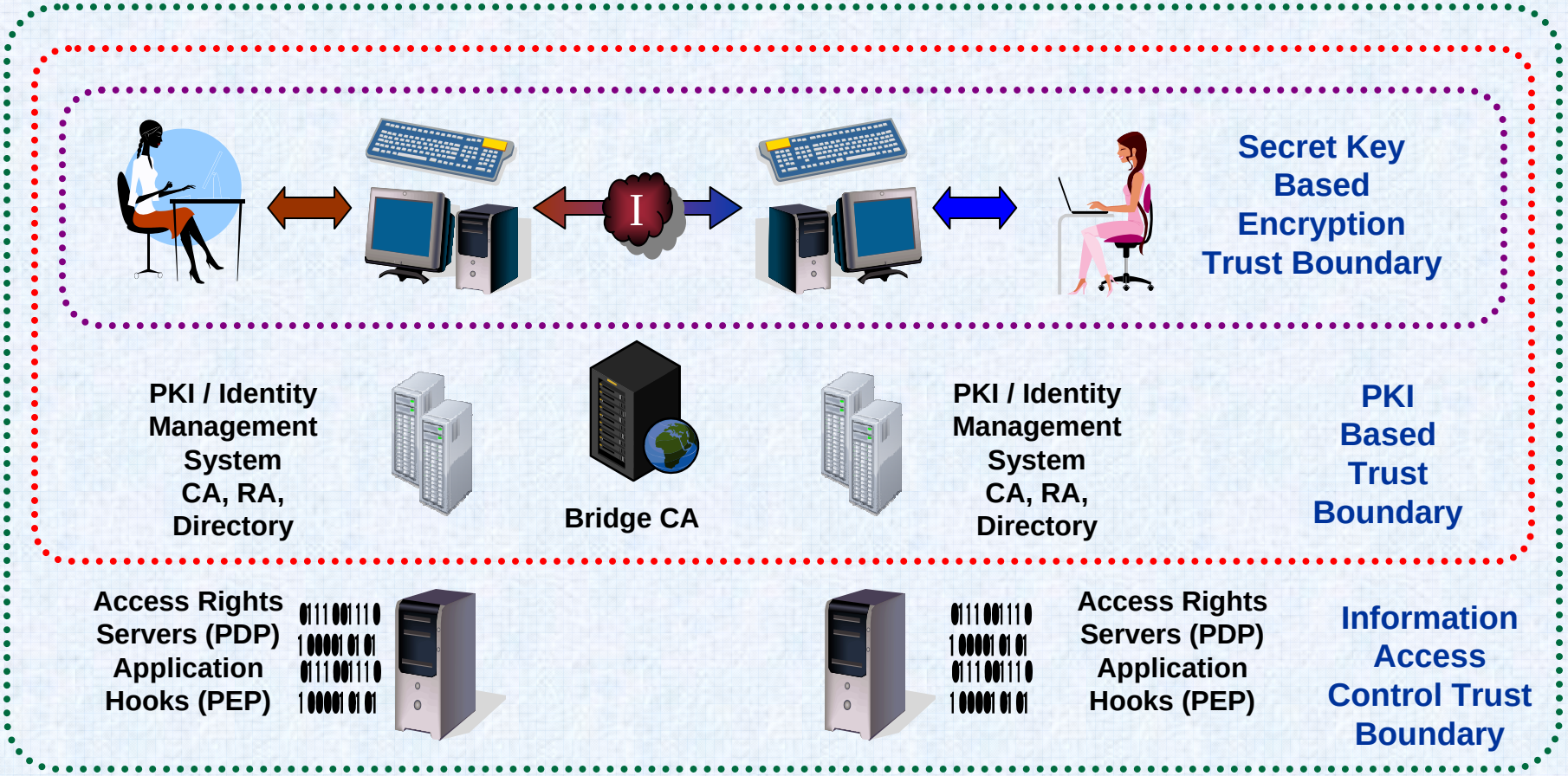


See: Dan Hitchcock, Evolution of Information Security Technologies, 2005 at http://movetheworld.wordpress.com

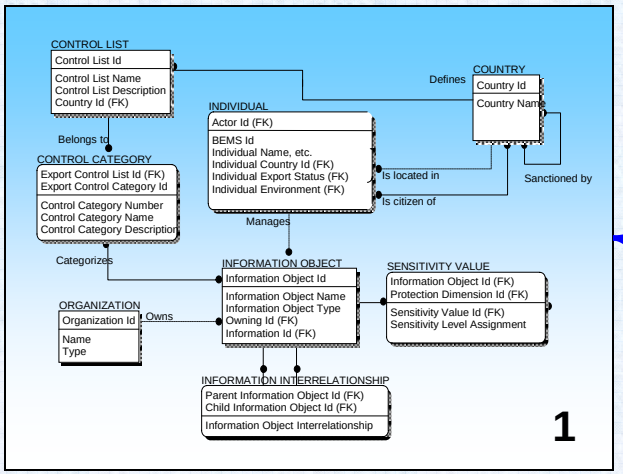
Gaps with Today's Approach

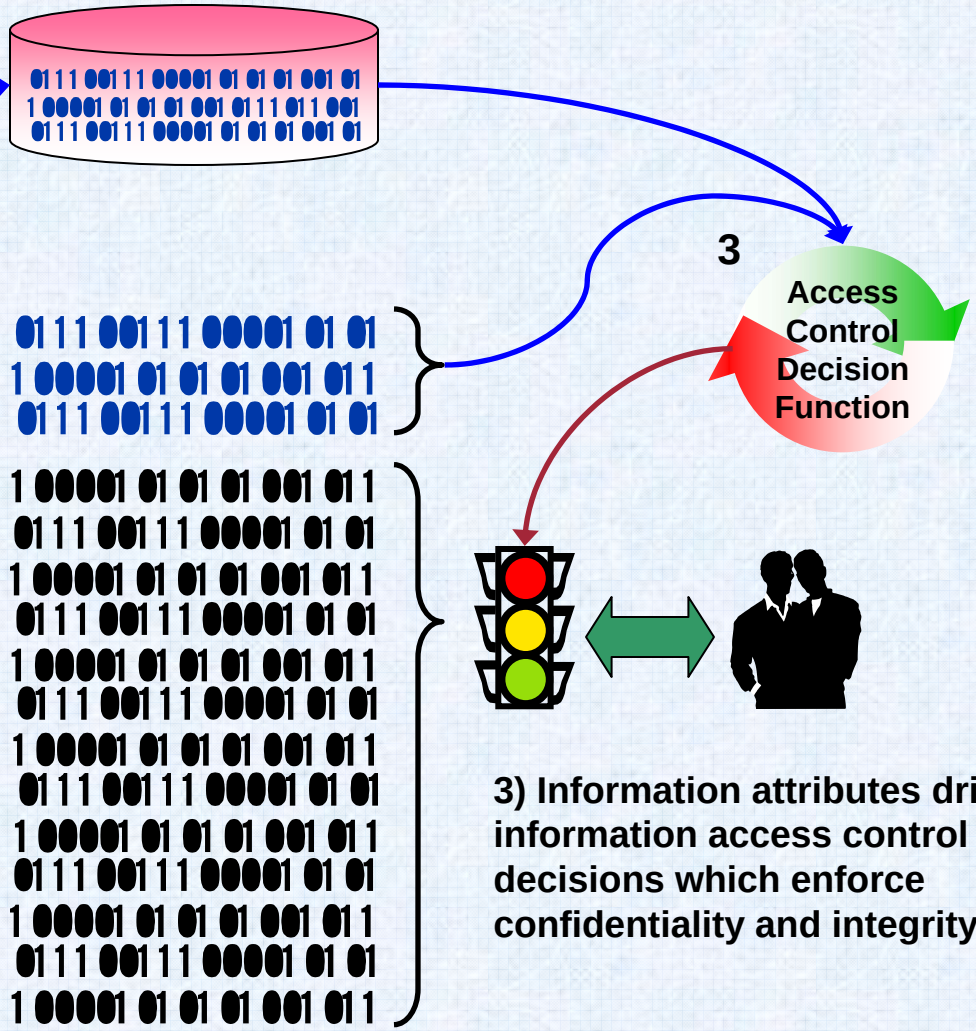
- **Protection is too far removed from information**
  - **Protection changes as information moves between environments**
  - **Outer layer breaches expose information**
  - **Most vulnerable at points of change**
- **Protection is too global**
  - **As protection moves farther away from information it tends to encompass more information, making breaches more significant**
- **Protection is asymmetric**
  - **Malware and intrusions growing faster than preventive technology**
- **Attack surface is too large**

Attack Surface / Trust Boundary Is Too Large



Information Security Architecture





1) An Information security governance model defines information attributes, relevant principals and their attributes, and relationships to the information being protected

2) Standardized information attributes are extracted from the model and populated by directly appending to or linking to the information

3) Information attributes drive information access control decisions which enforce confidentiality and integrity

Information Protection Tools Today

- **Secret Key Encryption**
  - **Confidentiality**
  - **Small attack surface (algorithm + key – and local app/OS)**
  - **Unscalable key management**
  - **Protection not granular enough – no control after decryption**
- **PKI Based Services**
  - **Signature**
    - **Protects integrity**
    - **Origin attestation**
  - **Encryption**
    - **Confidentiality (and usually signature)**
    - **Not granular enough…**
  - **Identity management issues replace key management issues**
  - **Attack surface now includes**
    - **PK & Hash algorithm**
    - **Certificate management infrastructure**
    - **Identity management infrastructure**
- **Rights Management Technology**
  - **Encryption + destination and operation control**
  - **Not interoperable**
  - **Often confused with copy protection**
  - **Attack surface includes all of the above plus rights management service infrastructure**

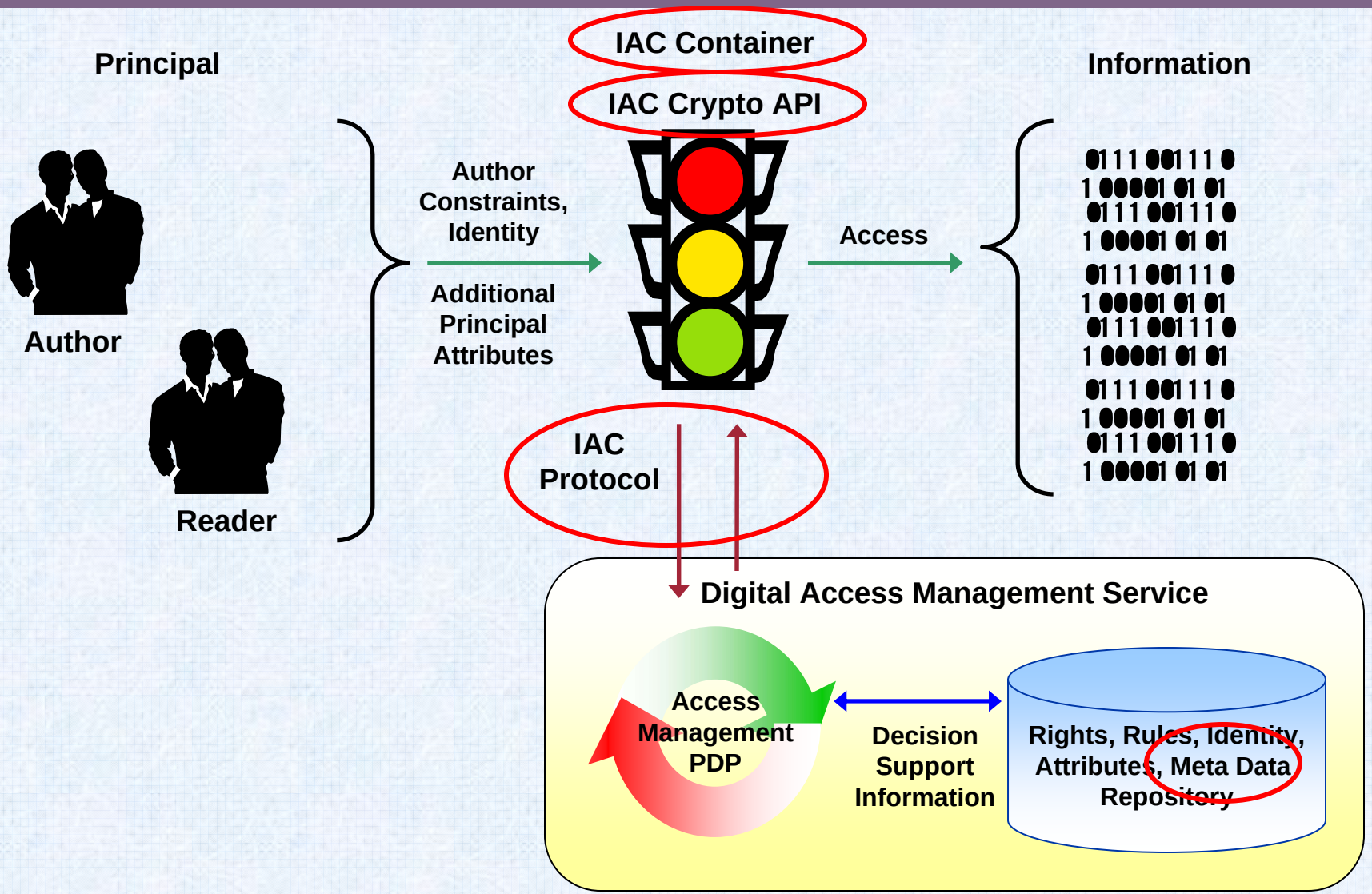
Necessary Information Access Control Capability

- **An open, standard container for encapsulating protected information**
- **An open programming interface that can be used to apply and query the associated rights**
- **An open, secure protocol for communicating between consumers of IAC protected data and the server or enterprise that controls the data's IAC attributes**

- **An accepted meta data standard for the access control information required to process the document**

- **Limit the attack surface,**
  - **Start the IAC trust chain with a protected private key**
  - **Leverage TPM technology**

Information Access Control (IAC) Standardization



Maturity

- **Reasonably mature**
  - **Supported, stable products from multiple vendors**
- **Less mature**
  - **No product interoperability**
  - **Large attack surface**
- **Estimated Timeframe: 2-3 Years**

Summary

- **We can't protect everything**
- **We can do some things better**

- **Limit communication exposure by restricting tunnel access to what's necessary**
- **Use VMs to divide and conquer complex operating systems and application security**
- **Standardize information access protection to aid secure collaboration**

- **Guidance from**
  - **Good security practices (simplicity, least privilege, etc)**
  - **Jericho Forum Commandments – design principles**

Relation to Jericho Forum Commandments

- **Communication Challenges**
  - JFC#1 The scope and level of protection should be specific & appropriate to the asset at risk
  - JFC#4 Devices and applications must communicate using open, secure protocols
- **Environment Challenges**
  - JFC#5 All devices must be capable of maintaining their security policy on an untrusted network
  - JFC#7 Mutual trust assurance levels must be determinable
- **Information Challenges**
  - JFC#8 Authentication, authorization and accountability must interoperate outside of your area of control
  - JFC#9 Access to data should be controlled by security attributes of the data itself
  - JFC#11 By default, data must be appropriately secured when stored, in transit and in use
- http://www.opengroup.org/jericho/commandments_v1.2.pdf

Answers?