



Boeing Technology  
Phantom Works

Phantom

# 21st Century Cyber Security Challenges

*A Perspective From Large-Scale Global Enterprise*

*M. Huang  
The Boeing Company*





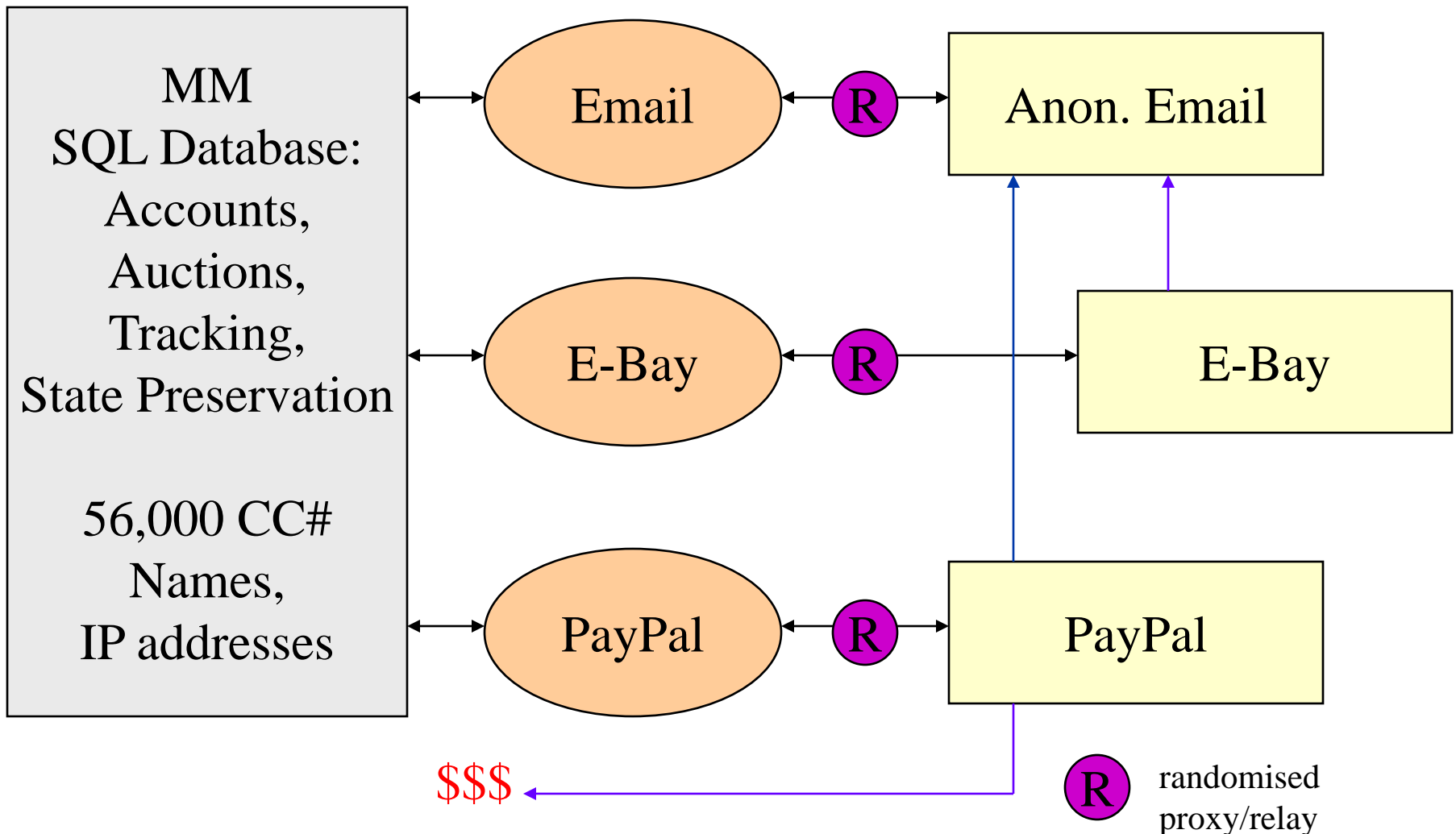








# Real-life Threats - Transaction Level Security



# The Challenges

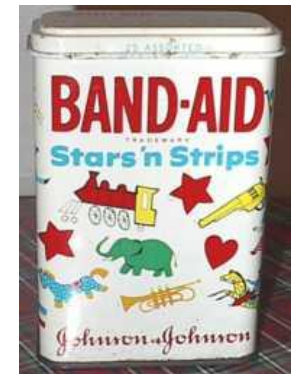
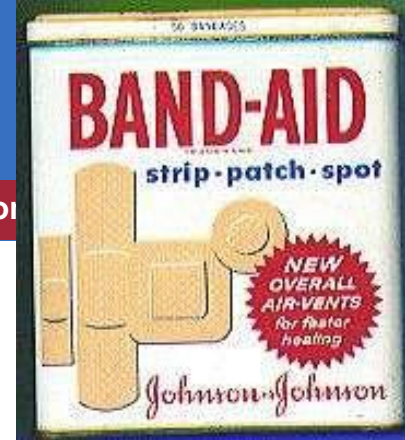
Boeing Technology | Phantom Works

E&IT | Mathematics and Computing Technology



# Today's Comprehensive Information Assurance Solutions

Boeing Technology | Phantom Works



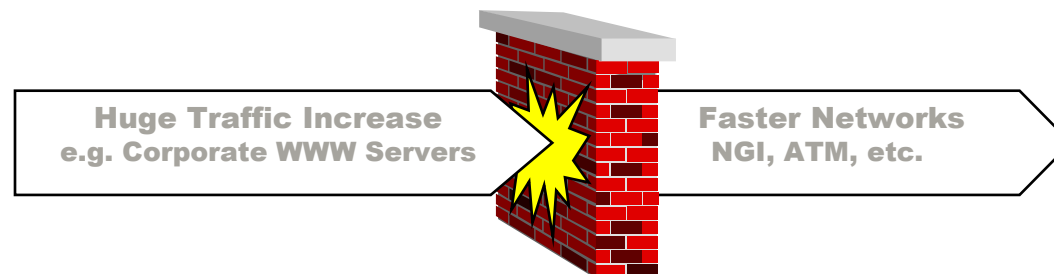
# The Old Paradigm: Castle, Moat and Draw Bridges

- Current network security models medieval castle construction
  - Hardened wall around the enterprise
  - A few strongly fortified access points
  - Little protection on the inside
- Castles began as simple walls with one gate
- Evolutionary design led to more complicated walls, complex gates and intricate defense mechanisms
- These evolutionary improvements were no match for revolutionary technologies like gunpowder



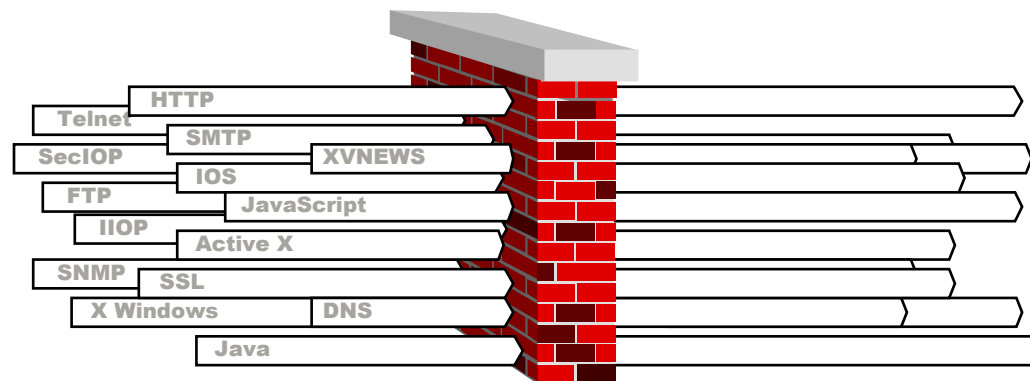
# Volume Challenge

- E-commerce, distributed collaboration, virtual enterprise, WWW, etc. generating large traffic volumes
- New network technologies - ATM, Internet-2, NTON, VOIP, video on demand
- CPU intensive tasks such as virus checking and intrusion detection sensors will not keep up



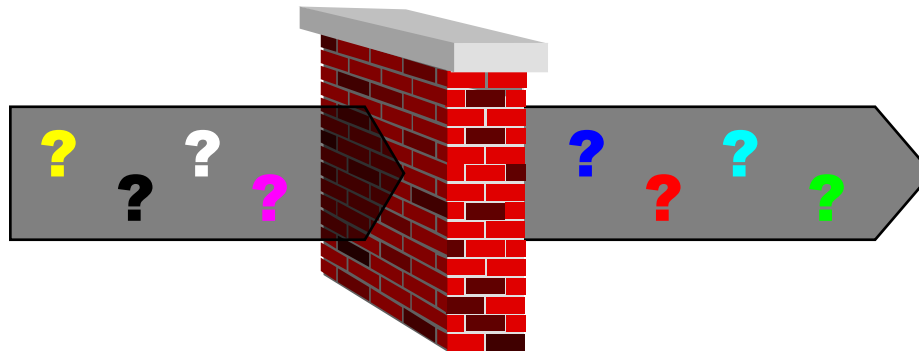
# Variety Challenge

- Increase in number and complexity of protocols
- Expanded practices of protocol wrapping
- Increase in services, some transparent



# Visibility Challenge

- Increased use of encryption
  - prevents data from being examined for viruses
  - prevents TCP port and protocol information from being used in system management, intrusion detection and other tools
- No real knowledge of packet contents

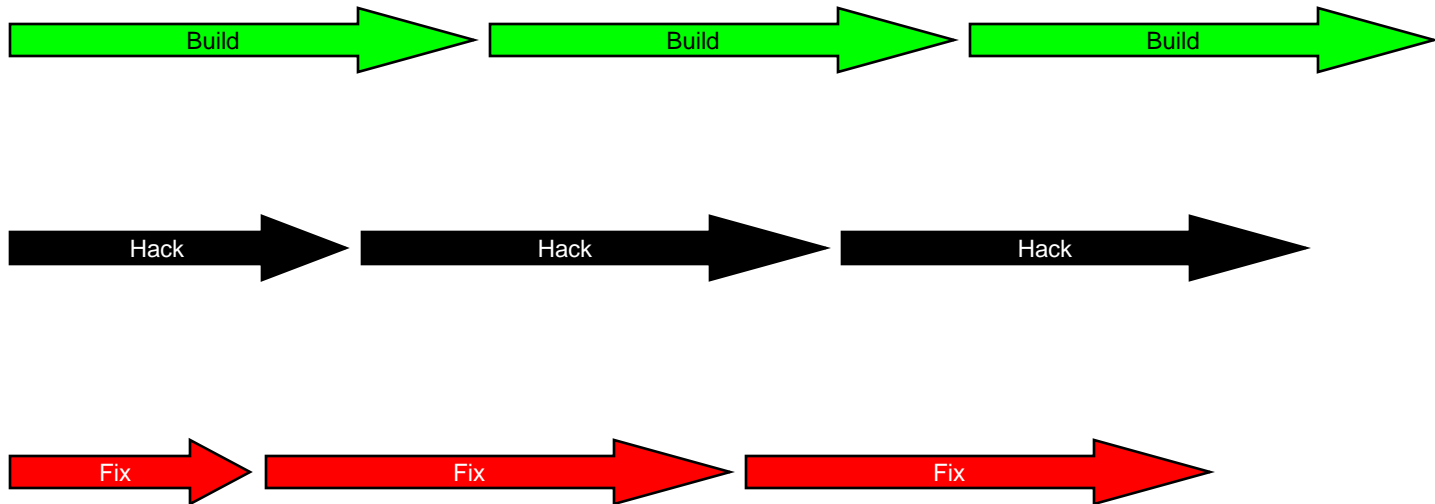


- Information security as final add-on
- Black boxes
- IA engineering processes?
- $\Sigma$  (parts) = total?

# The Pathetic Reality of Security

Boeing Technology | Phantom Works

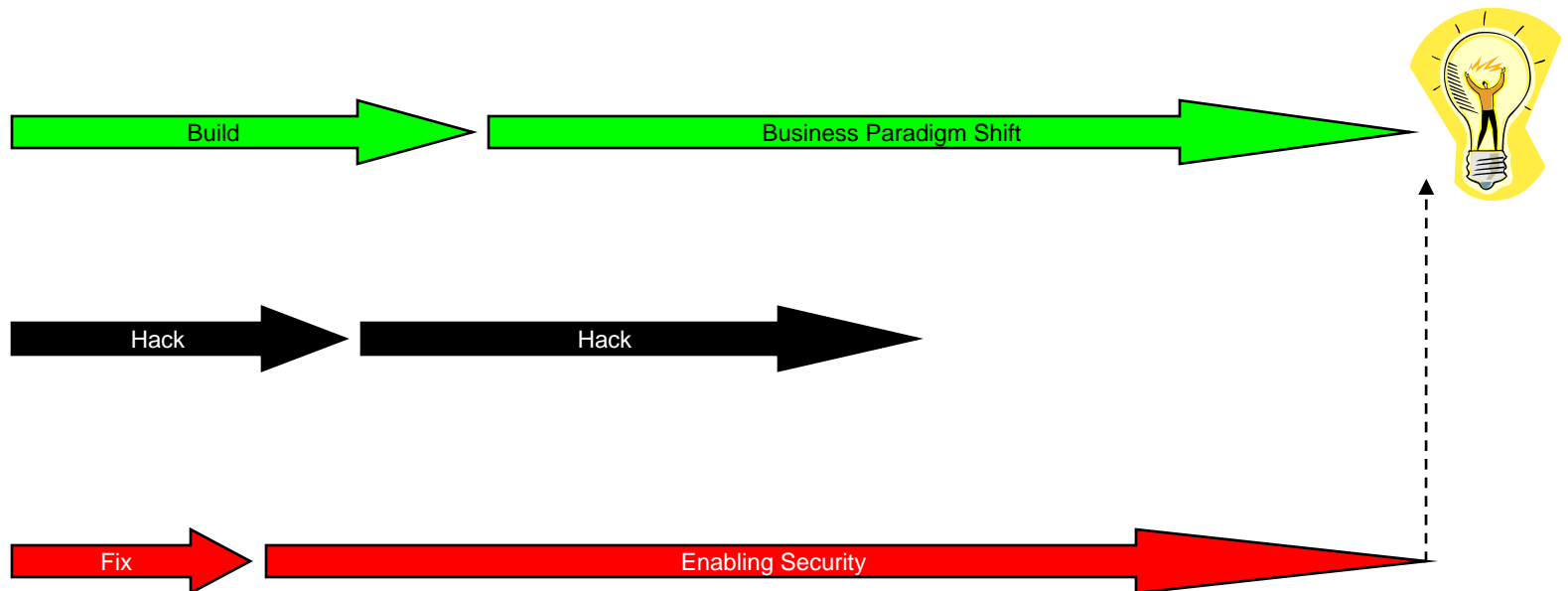
E&IT | Mathematics and Computing Technology



# Enabling Security

Boeing Technology | Phantom Works

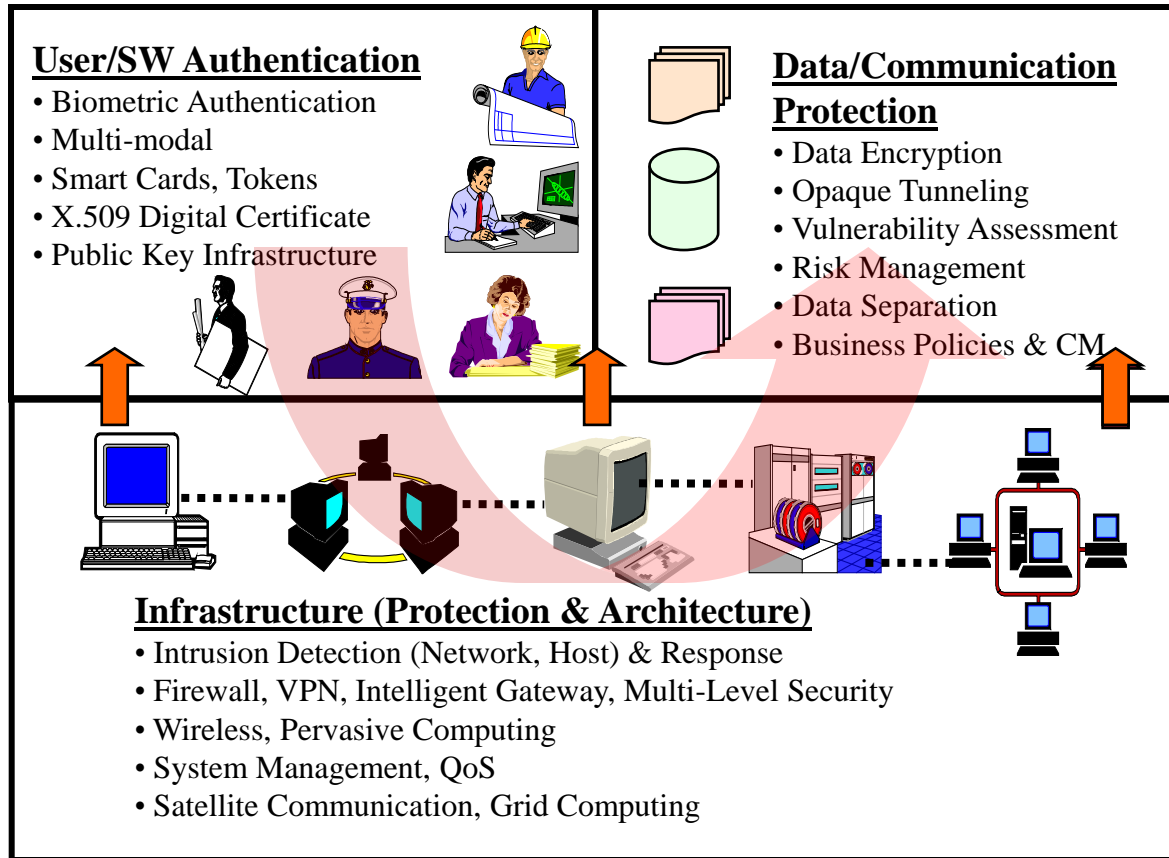
E&IT | Mathematics and Computing Technology



# The Inevitable/Driver (s) and the Collision (s)

- **Enabling technology factors. E.g.:**
  - Pervasiveness
  - Bandwidth
  - Mobility/wireless
  - Storage
  - Integration
- **Collisions of the inevitable (s), social factors & new paradigms**
  - Computation
  - Value proposition
  - Business processes
  - Society & human life
- **Security Challenges!**

# New Challenges Example



# Authorization Policies (Axioms)

- Mechanical engineers who are citizens have access to privileged engineering information
- Interns have no access to any information
- Supervisors have access to secret information
- Any one with access to secret information has access to both privileged and confidential information
- Technicians have access to privileged information only if they have clearance
- **CEO cannot be auditor**

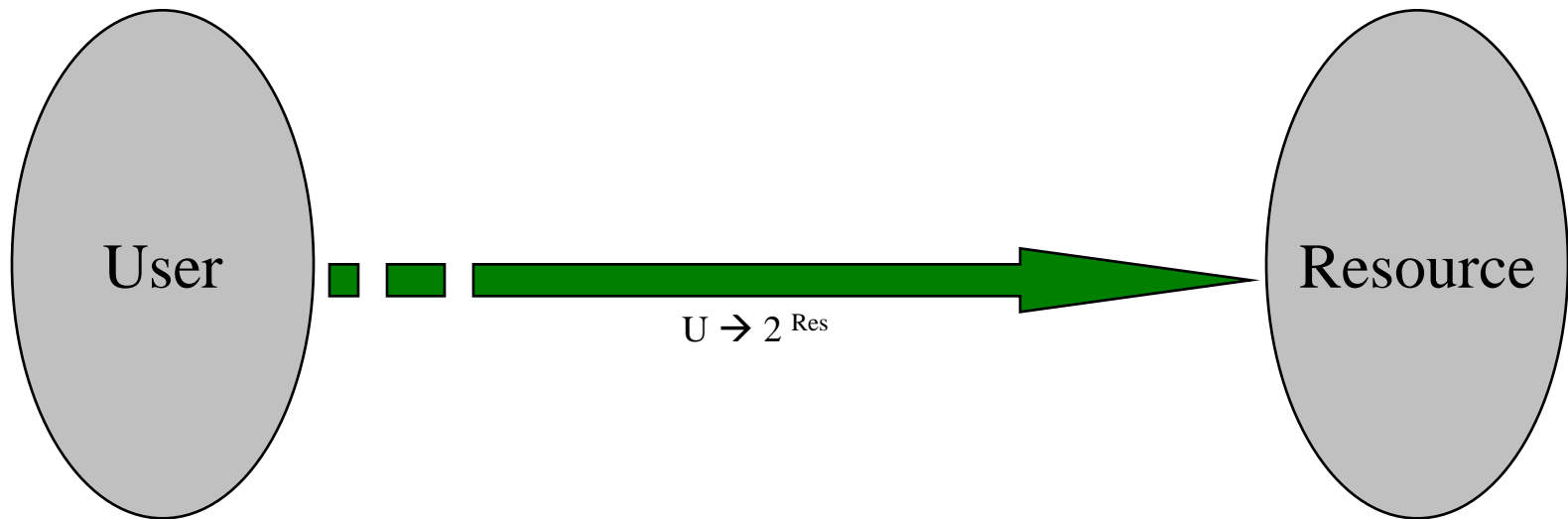
# Authorization Formal Policy & Complexity

- $(\forall x) (\forall \tau) (M(x) \wedge C(x) \wedge \Pi(\tau) \Rightarrow A(x, \tau))$
- $(\forall x) (\forall \tau) (I(x) \wedge (\Pi(\tau) \vee \Gamma(\tau) \vee \Sigma(\tau)) \Rightarrow \neg A(x, \tau))$
- $(\forall x) (\forall \tau) (S(x) \wedge \Sigma(\tau) \Rightarrow A(x, \tau))$
- $(\forall x) (\forall \tau) (\forall z) (\Sigma(\tau) \wedge A(x, \tau) \Rightarrow (\Pi(z) \vee \Gamma(z)) \Rightarrow A(x, z))$
- $(\forall x) (\forall \tau) (T(x) \wedge \Pi(\tau) \wedge A(x, \tau) \Rightarrow CI(x))$
- $(\forall x) (C(x)) \Rightarrow \neg A(x)$
- $(\forall x) (A(x)) \Rightarrow \neg C(x)$

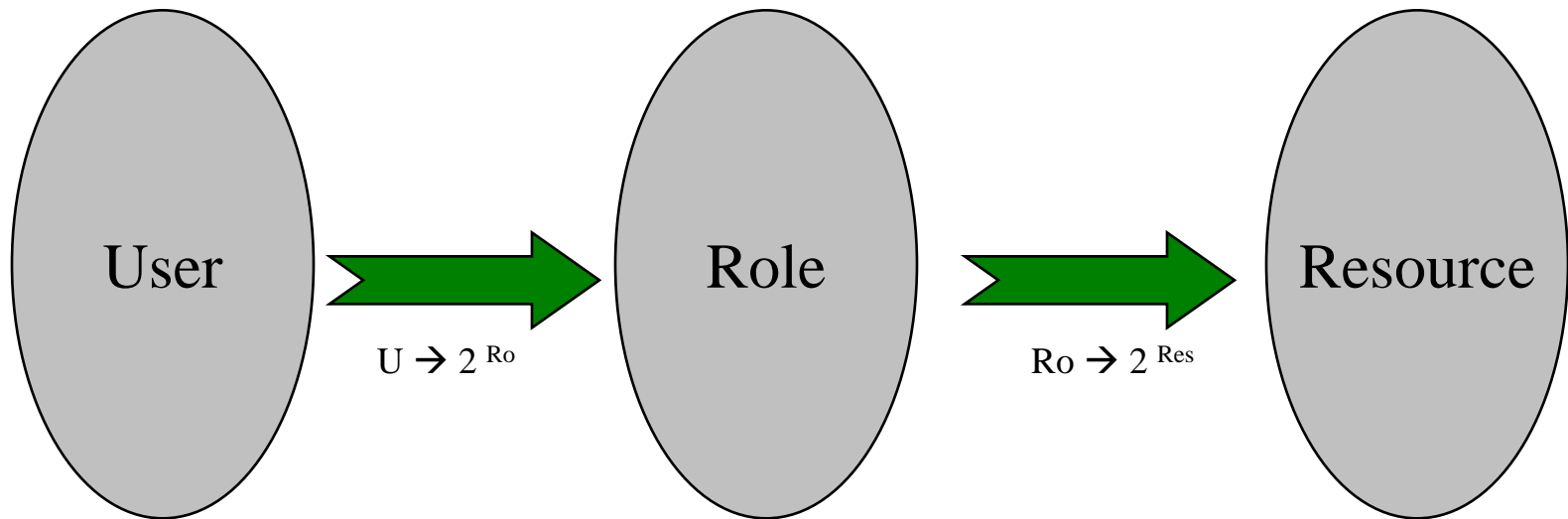
# The Complexity of Authorization

Boeing Technology | Phantom Works

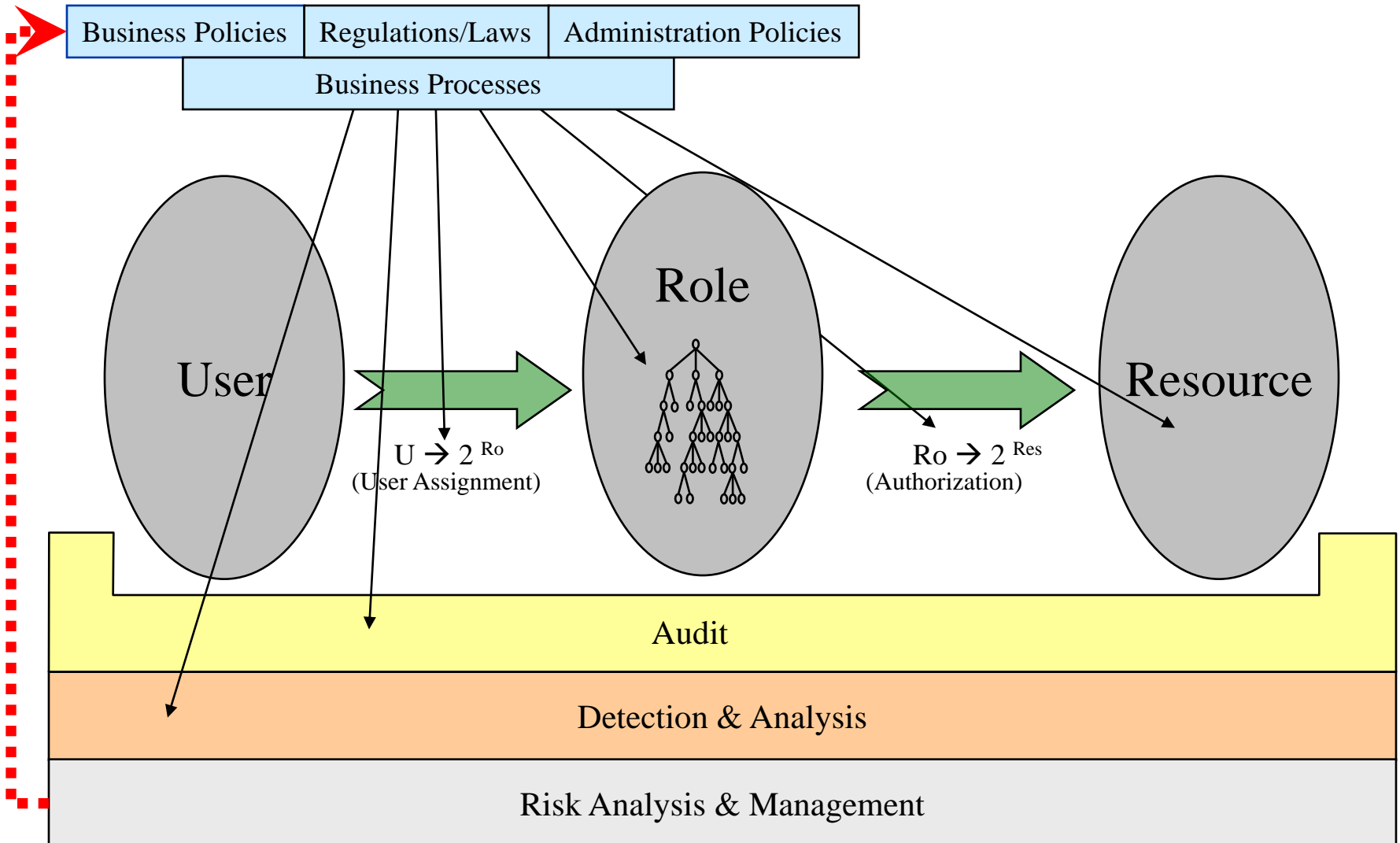
E&IT | Mathematics and Computing Technology



# Complexity Decomposition – Entitlements & Roles



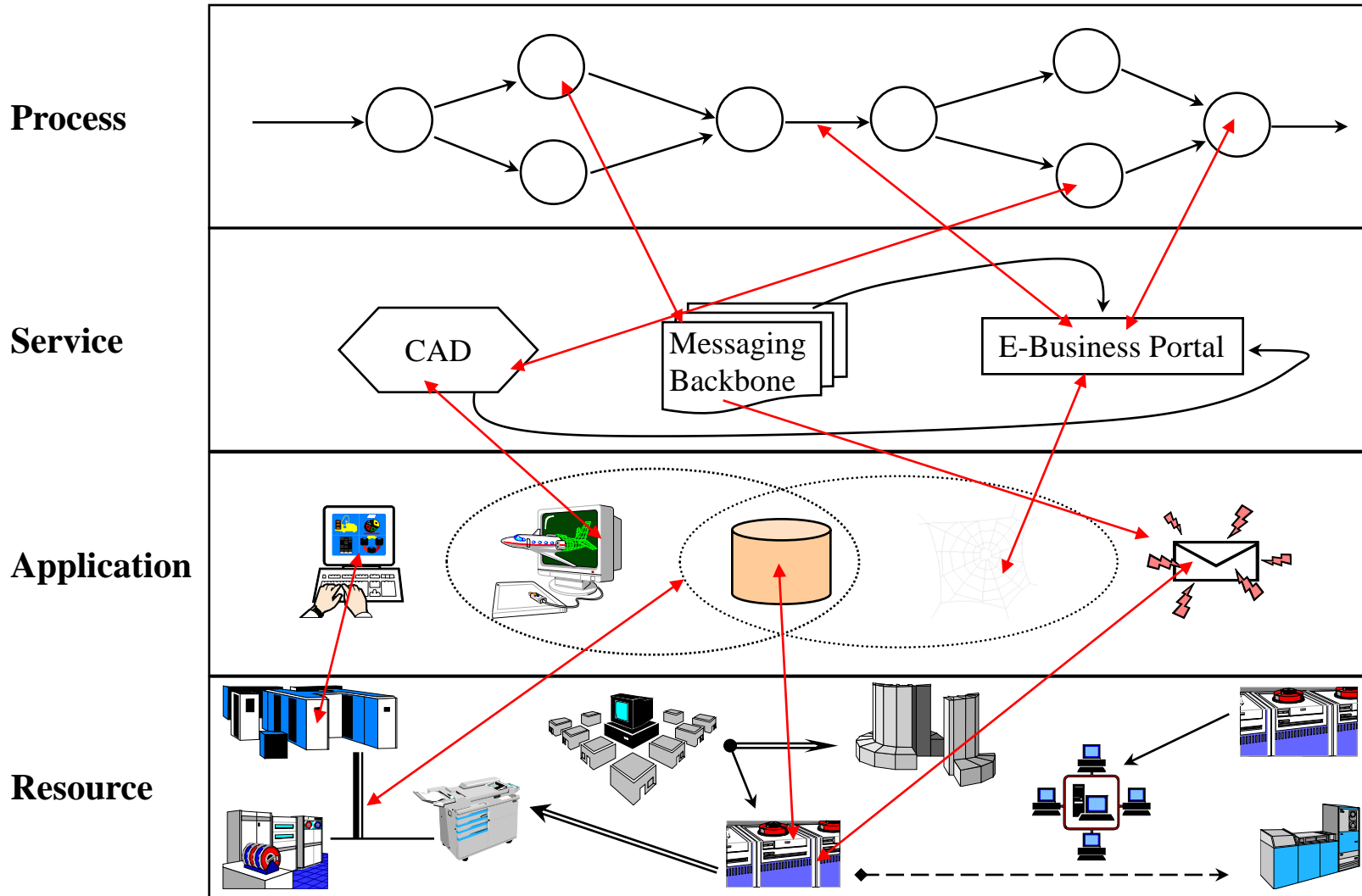
# Closed-Loop Security & OSI Layers



# Security in Context, or Not?

Boeing Technology | Phantom Works

E&IT | Mathematics and Computing Technology



**BOEING**

**END**

