Selected Topics in Cybersecurity

Eugene H. Spafford
Purdue University CERIAS

First of all…

- These are not new concerns
  - – Some of us have been trying to warn people for decades
  - – There is a body of established principles, largely ignored
  - – Small population of practitioners
- We know how to fix many of the problems without new research
  - – E.g., use a language with bounds checking
  - – E.g., reduce size and functionality
  - – Companies/government/users don’t want the
    - delay
    - cost

Second of all…

More spending on faster patches for unsafe, poor quality systems will not result in a safer infrastructure.

Intrusion detection, firewalls, anti-virus technology, wrappers, scanners, etc. are all add-ons to protect fundamentally unsound systems. (Which then need forensic technologies!)

Do you agree?

"…From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a firm requirement for security. ***As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, <u>proper security will not be a reality</u>***."

Do you agree?

“…From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a firm requirement for security. ***As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, <u>proper security will not be a reality</u>***.”

<u>Preliminary Notes on the Design of Secure Military Computer Systems</u>, Roger Schell, USAF, 1/1/73

Third point…

Cyberterrorism by Al Q'aeda terrorists is not the only threat. It may not be the biggest threat.

Consider:

- Domestic terrorists (religious, racist, fascist)
- Opportunistic crime
- Organized crime (narcocriminals, Mafia, Russian mob, Triads, etc.)
- Political espionage and sabotage
- Anarchists and vandals

How did we get here?

- Attitude of “make it work” rather than “make it trustworthy.”
- Attitude of “first to market wins”
- Relative immunity from liability
- Consumer demand for novelty
- Concern with ease of use over appropriateness of use
- Difficulty of development/customization

…note that this is how we teach!

Security & Privacy?

- Confidentiality
- Integrity
- Availability
- Auditability
- Control
- Accuracy

- "The right to be let alone"
- Control over what information about you is revealed, and to whom

Critical Concepts

Security is an unattainable absolute.

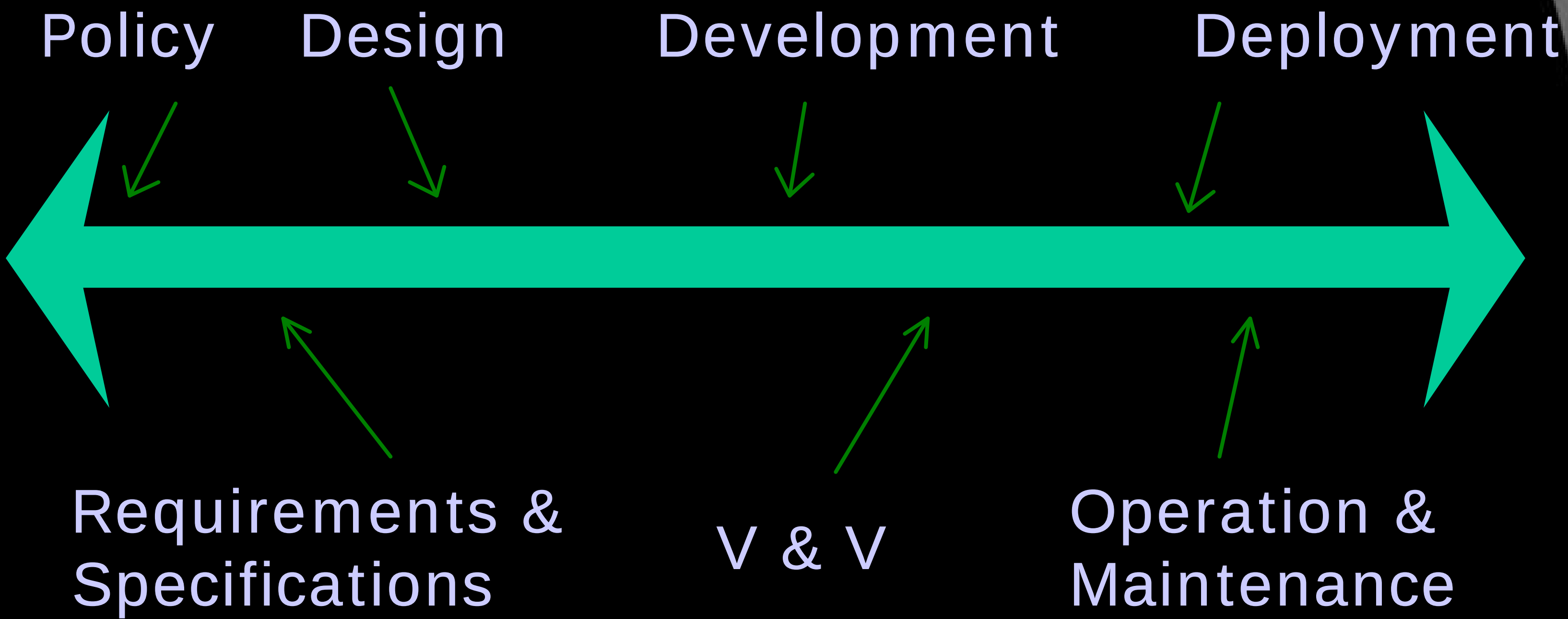
We should be seeking high levels of trust, based on sound methods of assurance.

Assurance is an on-going process, not a set of add-on features.

Understanding Assurance

- Assurance requires
  - Limiting what happens
  - Limiting who can make it happen
  - Limiting how it happens
  - Limiting who can change the system
  - Providing recovery mechanisms
- Users don’t tolerate limits well
- But users don’t understand risks

Where to Assure



Policy

Design

Development

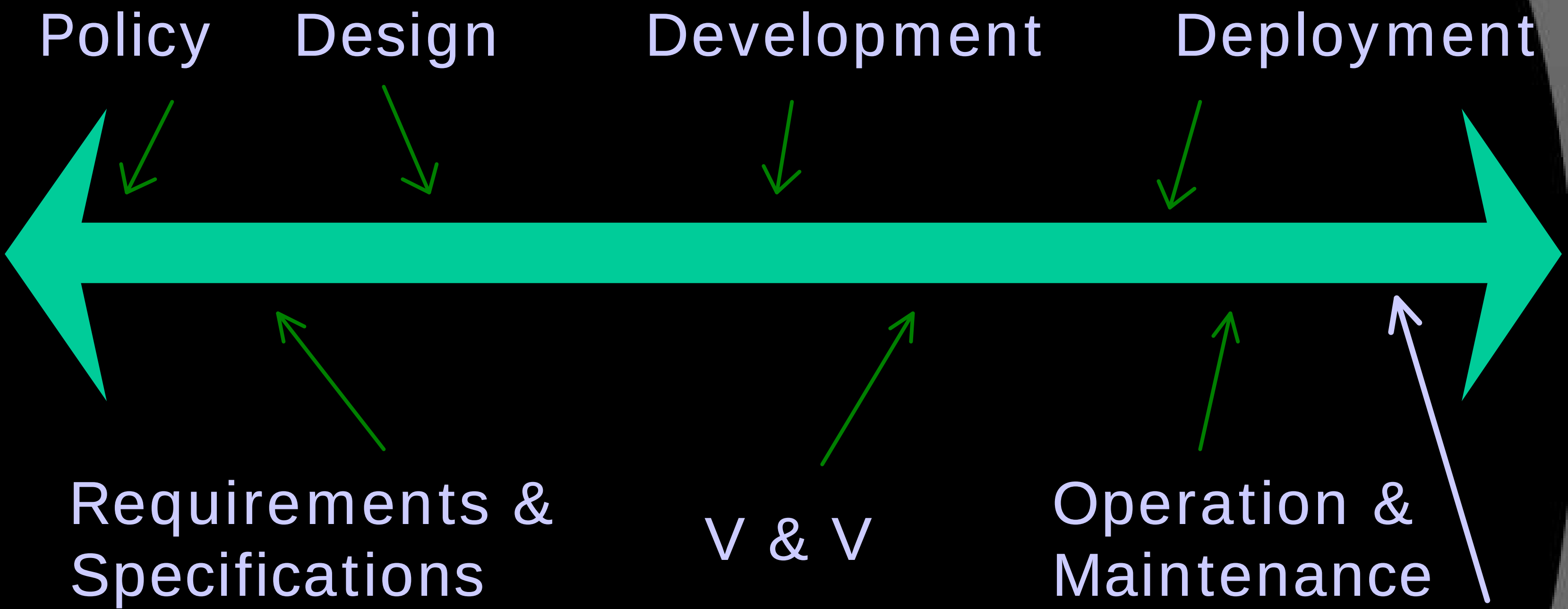
Deployment

Requirements & Specifications

V & V

Operation & Maintenance

Where to Assure



Current business practice

What are some research areas?

1. SCADA & resource control
2. Convergence of telecom and other services
3. Wireless
4. Authentication & access control
5. Software engineering tools & techniques
6. Graceful degradation
7. Forensics
8. Wide-scale analysis and fusion
9. Modeling and emergent effects
10. Economics and metrics