Networking and Security Research Center Industry Day

Security Research Activities at Great Valley

Phil Laplante, CSDP, PE, PhD

Penn State Great Valley

Ongoing Projects at Great Valley

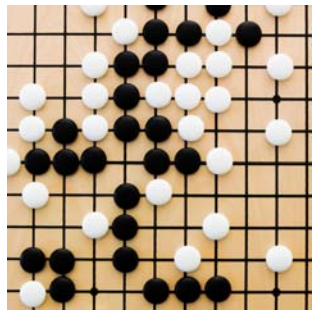
- Security Architecture
- Cybersecurity
  - Cyberpandemics
  - Digital forensics (pre-incident preparation)
- PE Software Licensure (for certified secure systems)

Architectural Patterns: Shortcomings

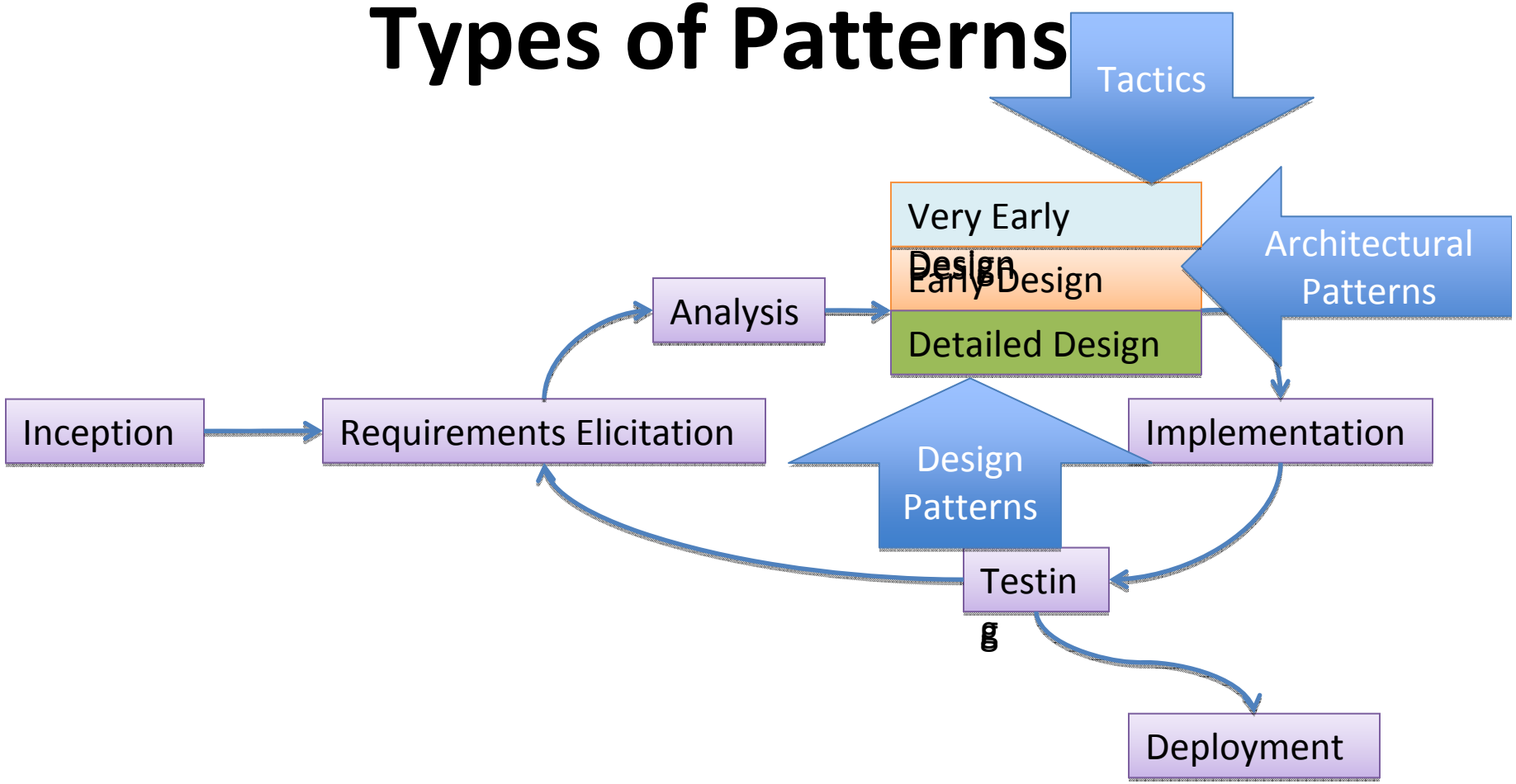
- Still too ***complex*** as a true ***starting*** point in design
- ***Multiple solutions*** per pattern
- Need for a ***more primitive*** and ***self-contained*** design concept
  - Something that maps directly to a ***particular concern*** such as security

Introducing *Tactics*

- ***Finer grained*** concept than architectural patterns
  - Manifestation of the ***building blocks*** of an architectural pattern
  - Mapping between a ***single*** quality attribute and an aspect of an architectural pattern
  - Establishing the explicit ***traceability***



Types of Patterns

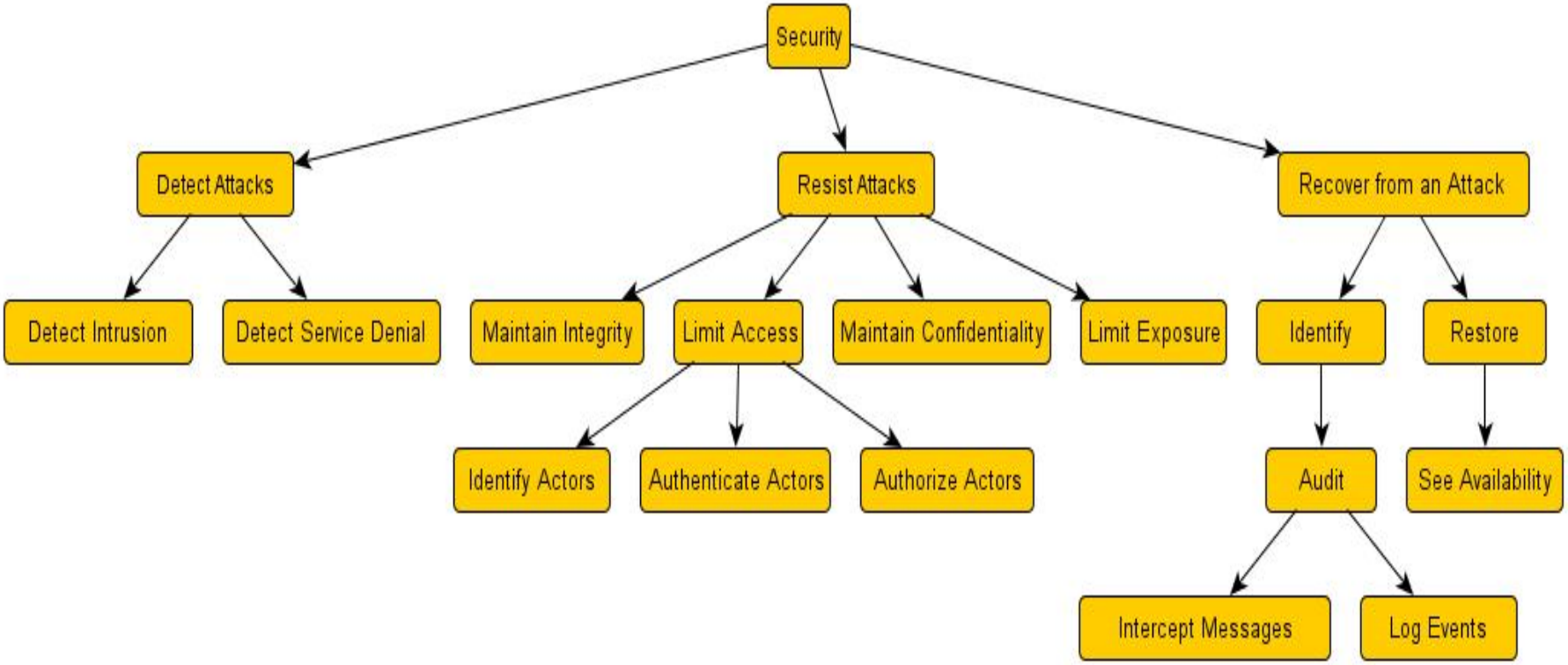


Software Development Life Cycle

Recent Results

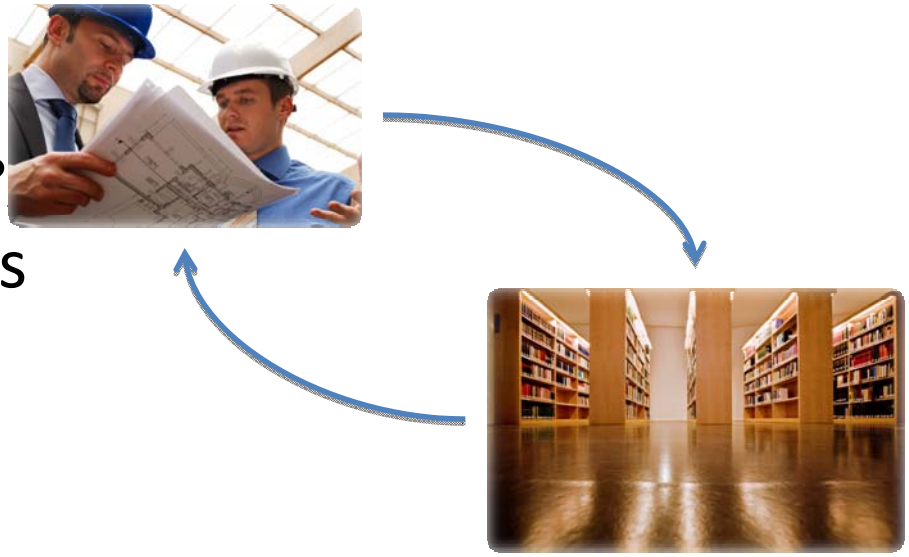
- Developed a methodology for mining tactics from architectures.
- Built a new security tactics hierarchy
  - Revised version of 2003 hierarchy by Bass, Clements and Kazman

Security Tactics Hierarchy



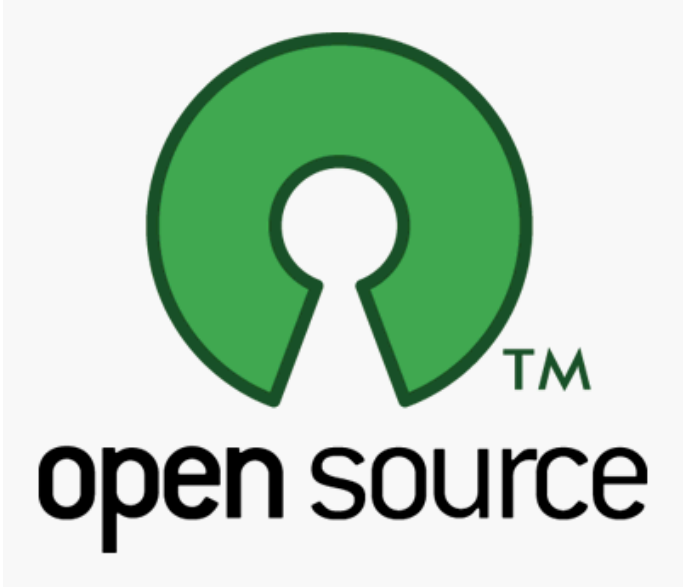
Ultimate Goal of our Research

- ***Build*** a ***repository*** of other tactics (e.g. reliability, safety) whose effectiveness is ***verifiable*** to help software architects develop their own ***customized*** structural design that is both secure and problem-specific.



Future Work

- Use open source projects as a ***proving ground*** for scientifically verifying the effectiveness of a tactic.



Ongoing Research

Evidence-Based SE through Open Source

- The methodology
  - ***Identify***
    - Multiple open source projects
    - Defect and tactic pairs
      - For example, privilege escalation and separation
  - ***Compare***
    - The number of defects
      - before and after the tactic within the same open source project by tracking the history of the defects
      - With or without the tactic among multiple open source project
  - ***Analysis***
    - If the number of relevant defects
      - Goes down
      - Is smaller
    - The tactic is effective

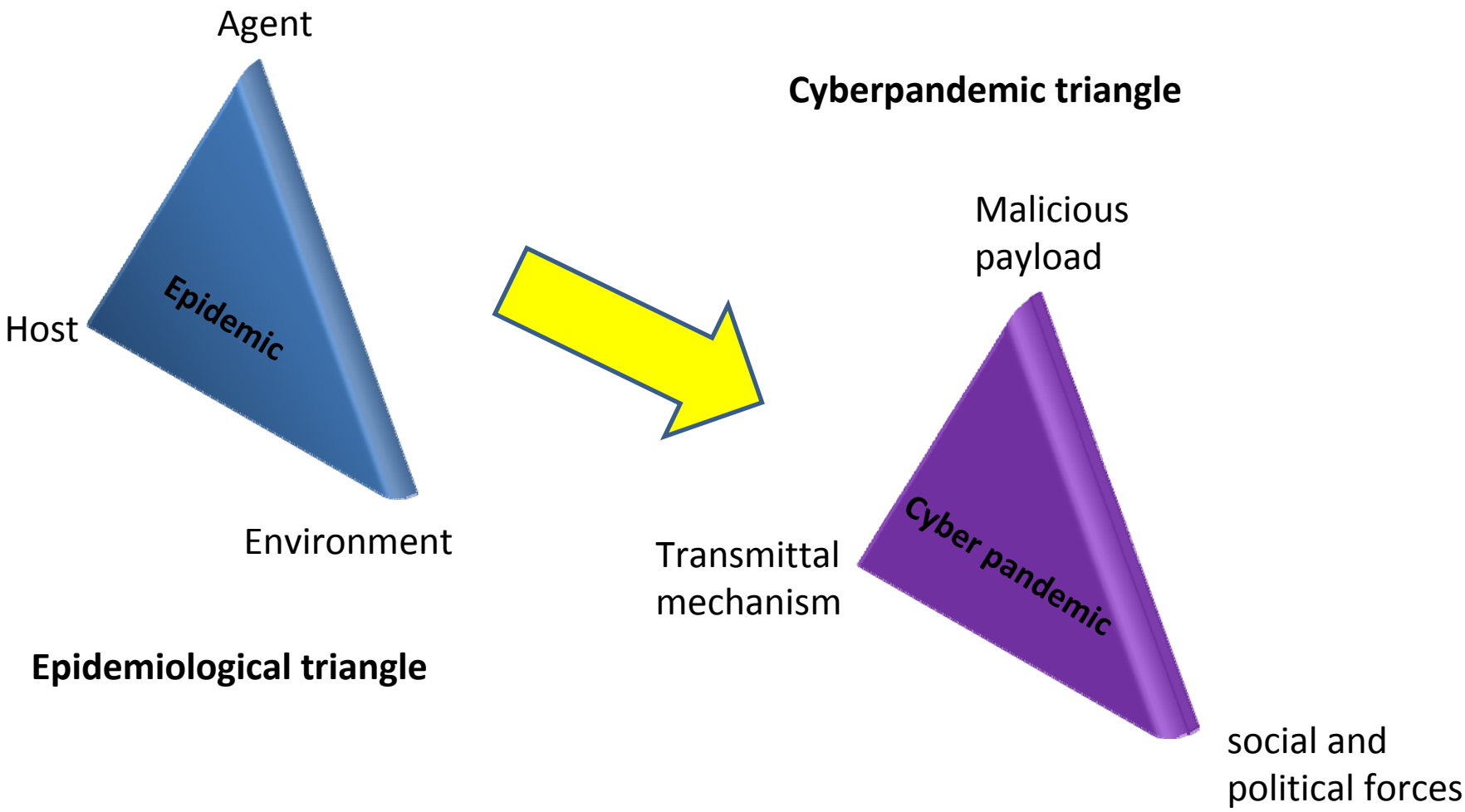
Foster a Community Process

- Build a tactics repository through a natural community process based on consensus
- Problems
  - Time
  - Verification

Partnership Opportunities

- Software architecture analysis and diagnosis
- Tactics repository construction and maintenance
- Security architecture collaboration

Cyberpandemics

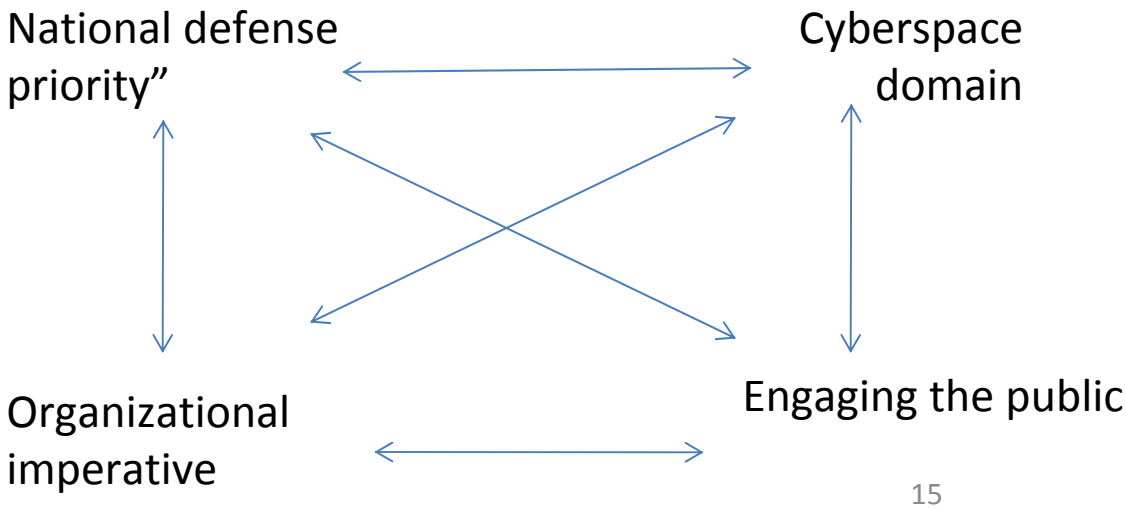


Conditions for a Cyber pandemic

- Complexity
  - people packed too tightly in cyberspace
  - complex social interactions (difficult to track)
- Multiple simultaneous attacks
  - multiple, orthogonal vector mechanisms
  - one or more non-cyber components
  - analogy is attack to immune system and nervous system
- Symptoms emerge long after infection has occurred
  - makes widespread dispersal likely, difficult to prevent,
- *Infected elements in the cyber-attack may be coordinated to work in concert* (e.g. Botnet worm).

Four Forces*

- Four forces related to managing cyber security:
- A starting point for nexialism



*William W. Agresti, "The Four Forces Shaping Cybersecurity," *Computer*, pp. 101-104, February, 2010.

Lessons Learned from History

- **Prevention activities**
  - surveillance
  - education
  - research
- **Preparedness activities**
  - plans for a cyber pandemic (e.g. recovery, relocation of critical assets..)
- **Response activities**
  - controlling the pandemic
  - minimizing damage and economic disruption
  - documenting the current response activities and outcomes

Partnership Opportunities

- Evaluate your cyberpandemic exposure
- Education is the best preventative
- Develop prevention and monitoring plans
- Develop contingency and recovery plans

PE Licensure Project

- Only Texas licenses software engineers who work on systems that affect the "health, safety and welfare of the public"
- Nine more states will soon *re*quire licensure: AL, DE, FL, MI, MO, NM, NY, NC, VA
- Work underway to develop software PE licensure exam
- Will include significant number of questions in "Safety, Security and Privacy"

PE Licensure Project

- Partners
  - NCEES
  - NSPE
  - IEEE – USA
  - IEEE Computer Society
  - Texas Board of Professional Engineers
  - Prometric
- First exam will be administered in 2013.

Partnership Opportunities

- Nominate licensed PEs with software engineering experience to participate in the project.
- Determine you licensure "exposure".
  - Does your product need to be signed by PE?
  - Do you need licensed PEs?
  - What about offshore providers?
  - What about externally furnished components?

Researchers

- Dr. Phil Laplante, Professor of Software Engineering
  - Areas: security architectures, cyber security, licensure
  - Other collaborators: NIST, NPS, UNO, SEI/Hawaii, Dr. Jungwoo Ryoo, CISSP, PSU Altoona
- Dr. Colin Neill, Associate Professor of Software Engineering
  - Areas: security architectures, software metrics
- Dr. Raghu Sangwan, Associate Professor of Software Engineering
  - Areas: security architectures, global software engineering, software metrics
- Dr. Joanna DeFranco, Senior Lecturer
  - Areas: digital forensics, global software engineering

Questions

Contact: Phillip A. Laplante, CSDP, PE, PhD
Professor of Software Engineering
Penn State
plaplante@psu.edu

Further Reading

Publications

- Keith W. Miller, Jeffrey Voas and Phil Laplante, “In Trust We Trust,” *Computer*, October 2010, pp. 91-93.
- Ryoo, J., R. Kazman, and P. Laplante, "Utilizing the Specifications of Security Tactics as the Baseline for Creating Traceability Metrics", in *Proc. of The 11th International Workshop on Information Security Applications (WISA 2010), Jeju Island, Korea, August 2010, pp. 65-66.*
- Sangwan, R. “Design and Analysis of Architectures for Security” in the SERC Systems Security Workshop, March 31 – April 1, 2010, Washington, D.C., USA.
- Jungwoo Ryoo, Phil Laplante, and Rick Kazman, “A Methodology for Mining Security Tactics from Security Patterns,” 43rd *Hawaii Conference on Systems Sciences*, January 5-8, Koloa, Kuaui, HI, 2010.
- Jungwoo Ryoo, Phillip Laplante, and Rick Kazman. Open source-based strategies for security tactics retrieval. In Proceedings of the 10th Korean Computer Scientists and Engineers Association (KOCSEA) in America Technical Symposium, Las Vegas, NV, December 2009.

Publications

- Jungwoo Ryoo, Phil Laplante and Rick Kazman, In Search of Architectural Patterns for Software Security, *Computer*, 42 (6): 98-100, June 2009.
- Phil Laplante, Bret Michael, and Jeffrey Voas, "Cyberpandemics: History, Inevitability, Response," *Security & Privacy*, vol. 7, no.1, January/February 2009, pp. 63-67.
- Sangwan, R. and Neill, C., "Characterizing Essential and Incidental Complexity in Software Architectures," in *Proceedings of the 8th Working IEEE/IFIP Conference on Software Architecture*, August 14 – 17, 2009, Cambridge, UK.
- Neill, C., Sangwan, R. and Paulish, D., "An Architecture-Centric Approach to Systems Design," in *Proceedings of the 19th Annual INCOSE Symposium*, July 20 – 23, 2009, Singapore.