Finding Your Way In the Dark: Security From First Principles

Susan Sons

Senior Systems Analyst, IU CACR | Information Security Officer, OSG

https://cacr.iu.edu/principles

http://security.engineering/talks

Across Time

- The principles worked for Sun Tzu, for Augustus Caesar, for Cicero.
- They work as well with paper and ink records as with digital databases.
- They work on things I haven't thought of yet.
- Quit starting over every couple of years.

Across Roles

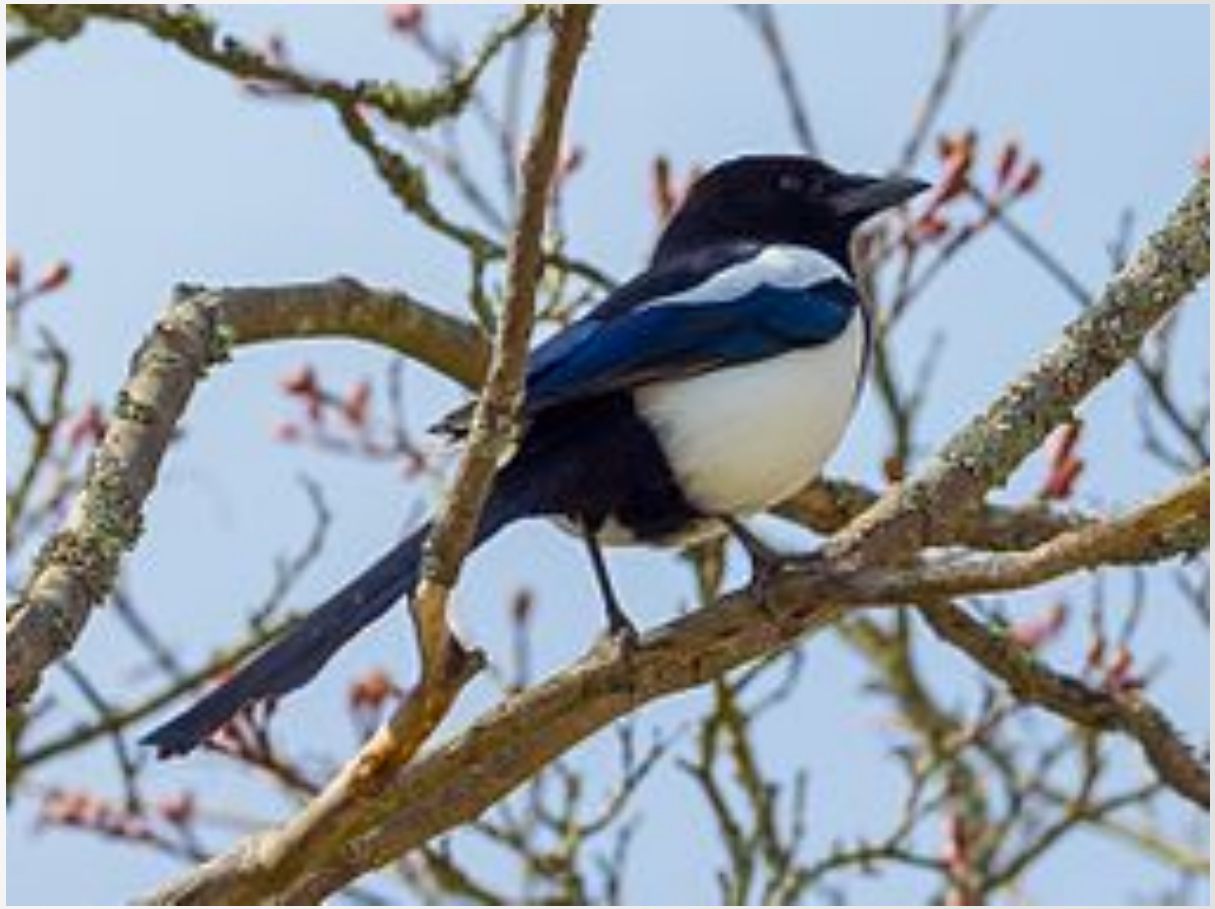
- What would happen if your programmers, systems administrators, policy-makers, managers, and information security experts *all spoke the same language?*
- It doesn't help security if management doesn't know enough to prioritize, or the systems and code owners don't know enough to implement.

Death By Checklists

Where does information security come from?

Just Seven Principles

Don't be this guy.



The Information Security Practice Principles (ISPP)

- **Comprehensivity**: *Am I covering all of my bases?*
- **Opportunity**: *Am I taking advantage of my environment?*
- **Rigor**: *What is correct behavior, and how am I ensuring it?*
- **Minimization**: *Can this be a smaller target?*
- **Compartmentation**: *Is this made of distinct part with limited interactions?*
- **Fault Tolerance**: *What happens if this fails?*
- **Proportionality**: *Is this worth it?*

You've probably seen some of these before:

- **Comprehensivity**: *End-to-end encryption, Inventory, Reconnaisance*
- **Opportunity**: *Information Sharing, Common Tools, Pentesting*
- **Rigor**: *Governance, Monitoring, Auditing, Follow-Through*
- **Minimization**: *Attack Surface, Compactness, Data Minimization*
- **Compartmentation**: *Least Privilege, Forward Secrecy, Airgap, Clean APIs*
- **Fault Tolerance**: *Resilience, Revocability, Defense in Depth*
- **Proportionality**: *Usability, Risk Acceptance, Fighting to the Goal*

The Principles In Practice

Comprehensivity

Opportunity

Rigor

Minimization

Compartmentation

Fault Tolerance

Proportionality

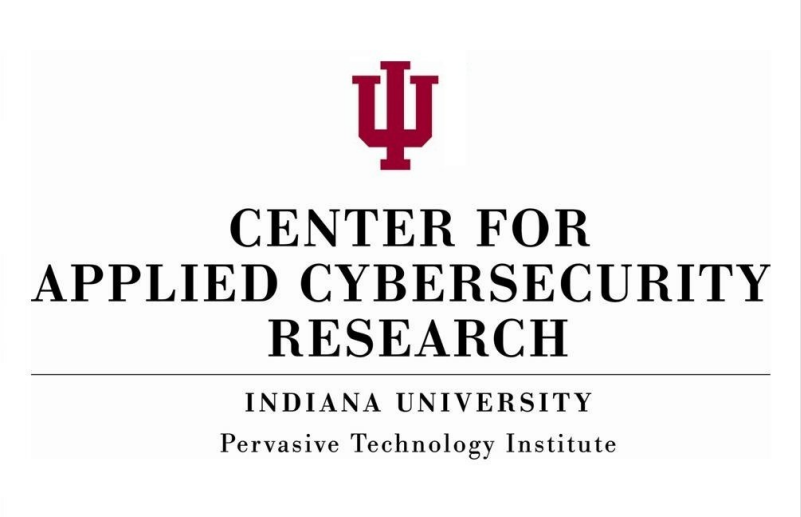
The Information Security Practice Principles (ISPP)

- **Comprehensivity**: *Am I covering all of my bases?*
- **Opportunity**: *Am I taking advantage of my environment?*
- **Rigor**: *What is correct behavior, and how am I ensuring it?*
- **Minimization**: *Can this be a smaller target?*
- **Compartmentation**: *Is this made of distinct part with limited interactions?*
- **Fault Tolerance**: *What happens if this fails?*
- **Proportionality**: *Is this worth it?*

Q & A

Don't stop now!

- Go to https://cacr.iu.edu/principles to find the printable refcard and the academic whitepaper.
- Find slides and info about this talk at http://security.engineering/talks
- Watch the O'Reilly Security mailing list for the upcoming practical whitepaper.
- Reach me at sesons@iu.edu



Using and Sharing This Work:

Slides and talk notes will be available by the end of the day tomorrow at:

http://security.engineering/talks