Philosophical Questions
(Usually Not Worth Discussing*)

Is there science in computer system security?

Yes, but of course there should be more.

Realistic Goal?
Can we be a real science like physics or chemistry?

Unlikely – humans will always be a factor in security.

How far can we get without modeling humans?

How far can we get with simple models of human capabilities and behavior?

Some Questions a Science of Security Should Be Able to Answer

Resilience: Given a system $P$ and an attack class $A$, is there a way to:

Prove that $P$ is not vulnerable to any attack in $A$?

Construct a system $P'$ that behaves similarly to $P$ except is not vulnerable to any attack in $A$?

Establishing Improvement

How can we determine if a system $Q$ is “more secure” than system $P$?
Meaning of “Science”

**Systematization of Knowledge**
Ad hoc point solutions vs. general understanding
Repeating failures of the past with each new platform, type of vulnerability

**Scientific Method**
Process of hypothesis testing and experiments
Building abstractions and models, theorems

**Universal Laws**
Widely applicable
Make strong, quantitative predictions

---

**Meaning of “Science”**

**Systematization of Knowledge**
Ad hoc point solutions vs. general understanding
Repeating failures of the past with each new platform, type of vulnerability

**Scientific Method**
Process of hypothesis testing and experiments
Building abstractions and models, theorems

**Universal Laws**
Widely applicable
Make strong, quantitative predictions

---

**Metrics**

“When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts advanced to the stage of science.” Lord Kelvin
Large increases in cost with questionable increases in performance can be tolerated only in race horses and [computer security].

Lord Kelvin

Metrics: Promising Approaches?

Comparative metrics
- Attack Surface [Howard; Manadhata & Wing, TSE May 2011]

Experimental metrics
- more systematic “red team” approaches

Economic metrics
- Active research community; WEIS

Epidemiological metrics
- model spread over network, but need assumptions

Entropy/Computational complexity metrics
- Define attacker search space; automated diversity

Meaning of “Science”

Systematization of Knowledge
- Ad hoc point solutions vs. general understanding
- Repeating failures of the past with each new platform, type of vulnerability

Scientific Method
- Process of hypothesis testing and experiments
- Building abstractions and models, theorems

Universal Laws
- Widely applicable
- Make strong, quantitative predictions

Formal Methods and Security

Lots of progress in reasoning about correctness

Systems fail when attackers find ways to violate assumptions used in proof

- Need formal methods that make assumptions explicit in a useful way
- Combining formal methods with enforcement mechanisms that enforce assumption

Formal Methods vs. Complexity

Pessimist’s View

Formal Techniques Capability vs. Complexity

Optimist’s View

Deployed Systems vs. Complexity

Loosely Due to Fred Chang

## Formal Methods Approaches

**Refinement:** Can we develop refinement approaches (design → ... → implementation) that *preserve security properties* the way they are used to preserve correctness properties now?

**Program analysis:** What security properties can be established by dynamic and static analysis? How can computability limits be overcome using hybrid analysis, system architectures, or restricted programming languages?

## Summary

### Systematization of Knowledge

- Valuable and achievable: need the right incentives for community

### Scientific Method

- Progress in useful models; big challenges in constructing security experiments

### Universal Laws

- Uncertainty if such laws exist; long way to go for meaningful quantification.

---

“In science there is only physics; all the rest is stamp collecting.” — Lord Kelvin

David Evans  
http://www.cs.virginia.edu/evans