JASONs Study
Cyber Security – Is Science Possible?

28 June 2010

Steven King, Ph.D.
Deputy Director for Cyber Security Technology
Office of the Director, Information Systems,
Office of the Director, Defense Research and Engineering

Outline

- Problem domain
- Questions for JASONs
- Cyber threat
- How can cyber security become scientific?
- Supporting fundamental questions
- Community development

Problem Domain

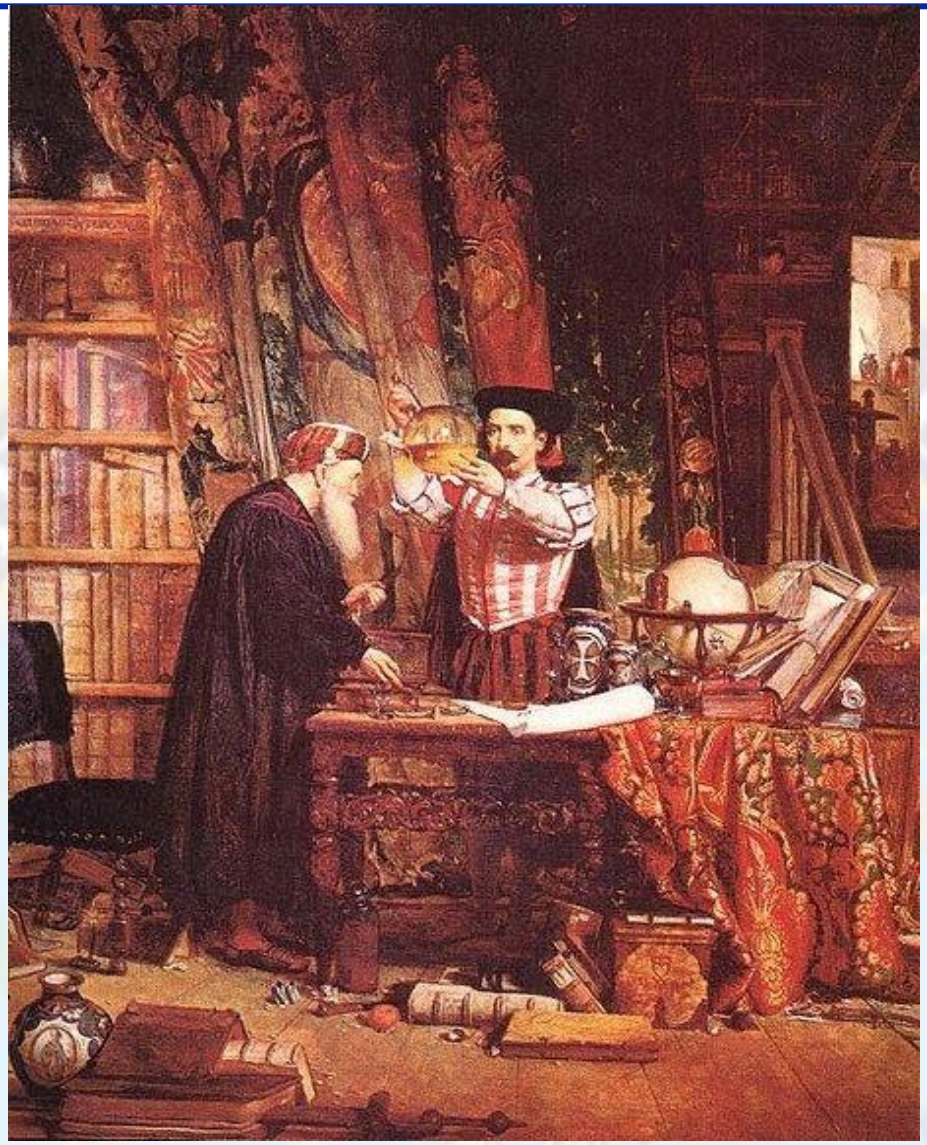
- ***Problem – How can cyber security become a more mathematical and scientific discipline?***
- We seek to secure a huge and extremely complex mesh of hardware, software, and people holding vital information about critical DoD assets
- Current state
  - Cyber threat is rapidly increasing, yet security is failing to comprehensively protect our systems
  - We do not have a sufficient scientific basis to make progress to fix the situation in a systematic and rigorous way
  - There is rigorous mathematics in selected areas
  - Measures and metrics are difficult to define and lack a solid foundation

- ***Impact of JASONs' analysis on DoD Science & Technology research agenda and ultimately on programs of record could be highly significant***

Questions for JASONs

- What areas of cyber security are amenable to a scientific approach?
- How can we structure a new initiative to give cyber security a more established scientific basis?
- What cyber research domains can be identified that will benefit from enhanced scientific methods?
  - What would a roadmap for research leading to science of cyber security contain?
  - What elements of scientific theory, experimentation, or practice should the cyber security research community adopt to make significant progress in the field?
  - What sorts of things are likely to be successful?
  - What other approaches should be considered?
- What measures and metrics can help us assess progress?
- How can the JASONs' recommendations be technically implemented?

Alchemy (Circa 700-1700)



Well-defined, testable goal (turn lead into gold)

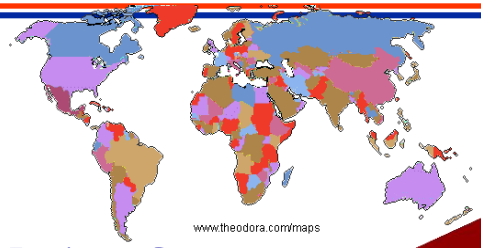
Established theory (four elements: earth, fire, water, air)

Methodical experiments and lab techniques (Jabir ibn Hayyan in 8th century)

Wrong and unsuccessful…but a precursor to modern chemistry

Sir Isaac Newton contributed to alchemy

Cyber Threat Spectrum



Nation States

Criminal Organizations

Trans-Nationals

Hackers

Sophistication of Adversary

Degree of Threat to US

Supply Chain

Insiders

LOW

MID

HIGH

Cyber Threat

- Threats
  - Capable nation-state and other well-funded entities with declared intent to attack US via cyberspace
  - Well-developed criminal element that is financially motivated to perpetrate attacks
- Ample evidence of increasing levels of technical sophistication
- Cyber adversaries have the ability to
  - Conduct reconnaissance to understand a defender's posture and resources
  - Exfiltrate valuable or sensitive information
  - Degrade legitimate use and manipulate information
  - Control a system for misuse, misdirection, or denial of use

How Can Cyber Security Become Scientific? (1)

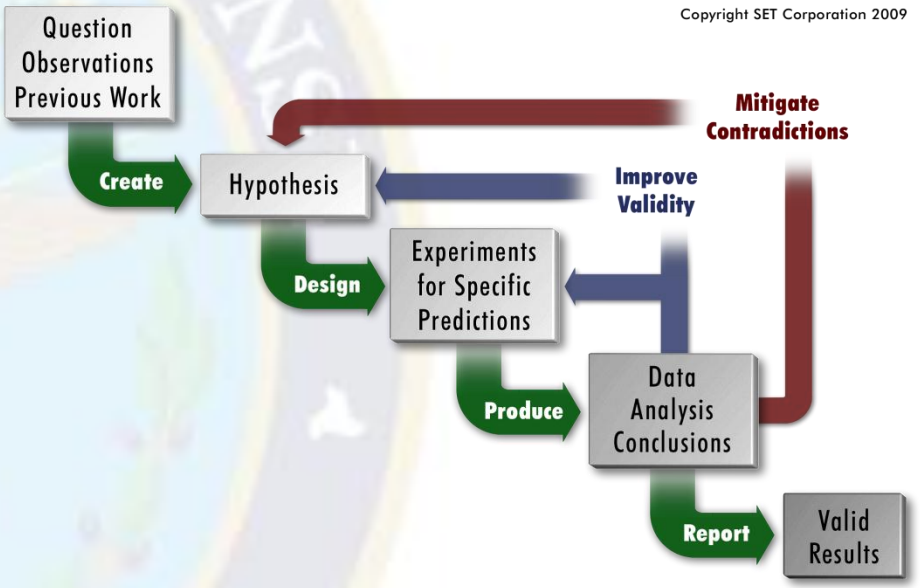
- Areas of mathematical rigor exist, including some important solutions
  - Cryptography and cryptographic mathematics based on number theory and algorithmic and computational complexity – very well developed
  - Syntax and semantics of computer/programming languages
    - Disciplined, restricted, safe, secure programming methods
  - Formal methods, correctness proofs, proof-carrying code, model checking, hardware verification
    - Based on first-order and higher-order logics and type theory
  - Security models, such as non-interference, non-deducibility, and others
  - Information theory
  - Information flow theories
  - Protocol analysis, including cryptographic protocol analysis
  - Mathematics and graph theory applied to networks

How Can Cyber Security Become Scientific? (2)

- Making these solutions effective or applicable in a wider domain really implies the need for radical changes in our computing and networking environment or in our fundamental thinking, e.g.,
  - New disciplined programming methods
  - New impositions of rigor on the developer and the user
  - New communications protocols with stronger security built in – a new Internet
  - New computational models – perhaps non-Von Neumann machines
- Many areas in our current thinking are very immature
  - Accounting for, or even modeling, the human element is very difficult
  - Adversary modeling needs to be greatly enhanced – there are several kinds of sophisticated adversaries with varying motives
  - Supply chain issues mean that we cannot simply trust the systems, devices, and products we acquire
  - Given the complexity of computing and networking there is much uncertainty concerning our systems – the complexity is in built

How Can Cyber Security Become Scientific? Experimentation (3)

- How do we structure the effort to do meaningful experiments?
  - Experimentation appears not work the same way in cyber security as in scientific disciplines – in cyber security demonstrations are more common
  - Need to collect and analyzed data in order to discover empirical phenomenologies
  - Repeatable cyber experiments may be possible in small, closed, and controlled conditions, but can they be scaled up to produce repeatable results on the entire Internet, or to the subset of the Internet that supports the DoD and the IC?
  - What techniques can we use to deal with systems that are so complex and large that models lack fidelity?
  - How do we deal with areas for which observations are sparse and incomplete



How Can Cyber Security Become Scientific? (4)

- Science or scientific method deals with
  - Systematizing and/or generalizing theories and bodies of knowledge
  - Applying the scientific method of forming hypotheses, performing experiments, collecting and analyzing data, and validating results
  - Discovering empirical phenomenologies through induction
  - Developing general or universal principles and theories
  - Capturing objective results from the healthy competitive tension between experimenters and theorists
- However, in cyber security we do not have this situation, because
  - We cannot fully isolate the salient variables
  - We do not have a good agreed upon notion of what security is

Human Elements (1)

- Nature exists – but humans use strategies, can cheat, can be surprising, can be unpredictable
  - Adversaries actively and creatively seek to violate models and assumptions
- Security is intimately connected with human capabilities and behavior
  - Defenders
    - Will they interpret events correctly?
    - Will they access and share the right information to enable defense?
    - Given situational awareness, will they take optimal defensive actions
    - Are they susceptible to deception, or can they be bought?
  - Adversaries and attackers – why we need a good adversary model
    - What are their motivations? What are their goals? How well resourced are they? What is their situational awareness? How stealthy are they?
    - Do they deceive and mislead to manipulate reactions? Do they collude?

Human Elements (2)

- Adversaries may turn the formal models and scientific theories against the defenders
  - Detailed specifications or formal models may help the attacker get round the security defenses – a specification may be a blueprint for what to avoid
  - Security models work against attackers who follow a security model, but attackers do not have to follow the model
  - We have many instances of attackers going under the radar – using low-level protocols, applying protocols in perverse ways, or using covert channels

Supply Chain

- Supply chain for ubiquitous technologies that underlie DoD and other critical systems is globalized, uncontrolled, and often opaque
  - Leaps in system functional capabilities have been made by harnessing advances of commercial industry
  - Development and production of key components no longer in US
- Need ways to guard against
  - Gray market and counterfeit components with unknown functional and performance characteristics
  - Insertion of illicit capabilities, such as embedded malware and “extra” network functionality

What Can We Take from Other Sciences?

- How can cyber security be improved or made scientific by drawing from other sciences and applying their principles and methods, or by making analogies with other sciences and applying analogical principles and methods?
  - Are there any “natural laws” in cyberspace that can form the basis of scientific inquiry in the field of cyber security?
  - Are there specific mathematical abstractions or theoretical constructs that should be considered in building a science of security?
  - Are there philosophical/methodological foundations of science that the cyber security research community should adopt?
- What are the impediments to advancing a scientific basis for cyber security?

What Sciences Can We Leverage?

- Which traditional scientific domains and methods can contribute to a science of cyber security, either directly, by reapplication, or by analogy?
  - For example, complexity theory, theory of dynamical systems, network and graph theory, logic and formal methods, game theory, information theory, discrete mathematics, economics, social sciences
- What bodies of knowledge can we leverage to develop the science?
  - How can we learn from other disciplines such as image reconstruction, tomography, genetics, immunology, epidemiology?
- What kinds of properties should we look for?
  - What is a general notion of security for secure systems?
  - How do we define or specify the universe of security properties?

What is Measurable in Cyber Security?

- How can we improve our ability to quantify and measure cyber security?
  - Can measurement theory or practice be expanded to improve our ability to quantify cyber security?
  - How can we establish metrics that can be used to measure with repeatable results the cyber security status of a system, of a network, of a mission?
- Comparative metrics may be more useful/feasible than absolute metrics
  - How can we quantify the security of two systems A and B in a way that establishes which is more secure for a given context?
  - How can we quantify the security of a system A and a system *f*(A) (where *f* is some function that transforms an input program or system definition)?

Countering the Cyber Threat: Can a Science of Cyber Security Help?

- Having a Science of Cyber Security, if such can be developed, will not solve the whole cyber problem
- We will still need security engineering, practical solutions, and lots of human awareness of the problem
- Subduing the cyber threat will require a full panoply of responses
- The expectation is that a scientific approach will bring order, rigor, and a reduction of some of the systemic problems we are now encountering

Backup

Uncertainty

- Our complex, interdependent, and dynamic systems never have a known or well-defined baseline
  - Dependencies extend far beyond organizational and physical boundaries
  - New system pieces appear before current inventories can be completely integrated
- Systems and components routinely suffer compromises
  - Some undetected
  - Some are known but difficult to eradicate
- We need better models for analyzing how to achieve desired functions in systems with damaged and degraded or partial capabilities
  - Models of security tend to be binary – secure or unsecure – and localized within organizational boundaries or abstraction layers
  - We need ways to reason about uncertainty and results within tolerances

Community Development and Education

- What steps are recommended to develop and nurture scientific inquiry into forming a science of cyber security field?
- What is needed to establish the cyber security science community?
- How can educate a class of scientifically-based defenders of cyber space?