The Science of Security
Questions and Promising Approaches For a Science of Security

18 November 2008

Gamay Room

1

Charge Topics

- **What are the most important ideas from other fields that we should try to integrate into cyber security?**
- **What steps are needed to establish more useful security metrics?**
- **Formal methods – reducing complexity**
- **How do we establish fundamental principles of security? Do we have those principles?**
- **How do we get to the right level of abstraction?**
- **Can we constrain the space to then reason about security**
- **How do we build better adversary models?**

2

What are the most important ideas from other fields that we should try to integrate into cyber security?

- **Need to consider formal methods from other disciplines – max-SAT model checking**
  - Neighborhoods
  - Digital discrete transitions
- **Is the inability to**
  - Boundary of digital vs continuous modeling
- **Integer programming to linear programming reasoning**
- **Cryptography – zero-knowledge proofs, notions of basic principles and definitions, "weave crypto into the fabric of your systems", identity based encryption**
- **Bio – robustness/ fragility, self-adaptive systems, diversity and survivability, avoid the superficial analogies, diseases and microbial ecosystems**

3

What steps are needed to establish more useful security metrics?

- **Limited metrics to evaluate the science of security**
- **Why is this hard**
  - A metric provides an abstraction to reduce something and has less content. This requires assumptions.
  - Any assumption embedded in a metric can be a vulnerability
  - Can security be priced
-

4

Formal methods – reducing complexity
Can we constrain the design reason about security

- **Revisit layered architecture**
- **Near decomposability – develop components independently**
- **Network problem – can we generate desirable global properties from local elements**
- **Solving problems using different scales of locality**
  - Congestion control
- **Abstraction oriented programming languages and run-time monitoring**
  - Human understanding
  - What is the value

5

How do we establish fundamental principles of security? Do we have those principles?

6

How do we build better adversary models?

- **Know your adversary; goals, motivations**
- **Abstraction to need to know less about the adversary; delete a conjunction**
- **Abstract the modeling of the attack**
- **Understand: resources, interface, access,**
- **Reason about adversaries**
  - Idealize things that are "real adversaries"
  - Are their natural adversaries to the security structures (reasoning for science)
  - Understand and align the motivation of neutrals to beneficial behavior
  - Shared risk

7

Questions

What are the questions that need to be asked to advance cyber security science?

What are the priority research areas?

What theory is needed?

What experimentation is needed?
- Good experiment intervention to deliberately introduce an observation of an effect
- How do we make security experimentation good?

Since progress in science is often driven by new technology are there advances in technology needed to improve the tools for security science?

Can security be viewed as a feedback problem?

Consider the following:
- Absolute security vs. risk management
- Prevention vs. accountability
- Perfection vs. diversity
- Enforcement vs. relocation of trust

8

Assumptions and observations

9

Questions

10

Promising Approaches

- **Development of hyper-properties for security**
  - Hyper-safety
  - Hyper-liveness
- **Development of distributed control/security models**
- **Control Theory - Layered Architecture for Security**
  - Constrain the problem to de-constrain the solutions
  - Robust / fragility
  - Extend theories to networks
- **Develop Canonical Attacker Models**

11

Promising Meta–approaches Making a Science

- **Testbeds**
  - Canonical datasets
- **Standards for publication**

12