Security Metrics

Mark Torgerson
Sandia National Laboratories

2/5/2007

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

What is wanted in a Security Metric?

- Deterministic function of a system
  - M(A) tells you how secure the system A is
  - M(A)<M(B) means something

Function where you input a comm… n system

A number i… puted

That number tells y… ow how secure the system is

Industry can’t seem to define a metric with these properties

We will show that certain security metrics do not exist

Terms

- **Communication System:** A real collection of hardware, software, and human components brought together to facilitate communications of some kind
- **Adversary:** An entity that desires to gain some nefarious goal against the system
- **Security subsystem:** The system components used, either directly or indirectly, to prevent an adversary from achieving his goals
- **Weakness:** Something attribute of the system that an adversary may use to achieve his nefarious goals
- **Trust:** Confidence that one may have in their system in preventing an adversary from achieving his nefarious goals

Adversary

- Two adversarial attributes
  - **Knowledge**
    - Intellectual Resources
  - **Physical Resources**
    - Money
    - Computational power
    - Employees
    - Etc.

All adversaries discussed here have a physical resource bound B

All systems are insecure against a completely unbounded adversary

Weaknesses

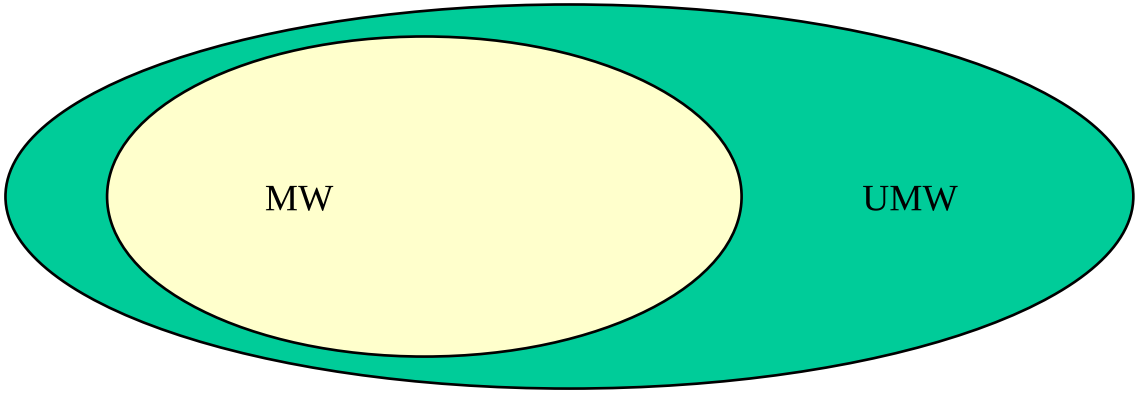
- **Rule of thumb**: No system is 100% secure

Weakness Axiom 1: Every real communication system has a non empty set of weaknesses

- **S** is the system
- **W** is the set of ALL system weaknesses
- **P** the protections placed on S

Weaknesses

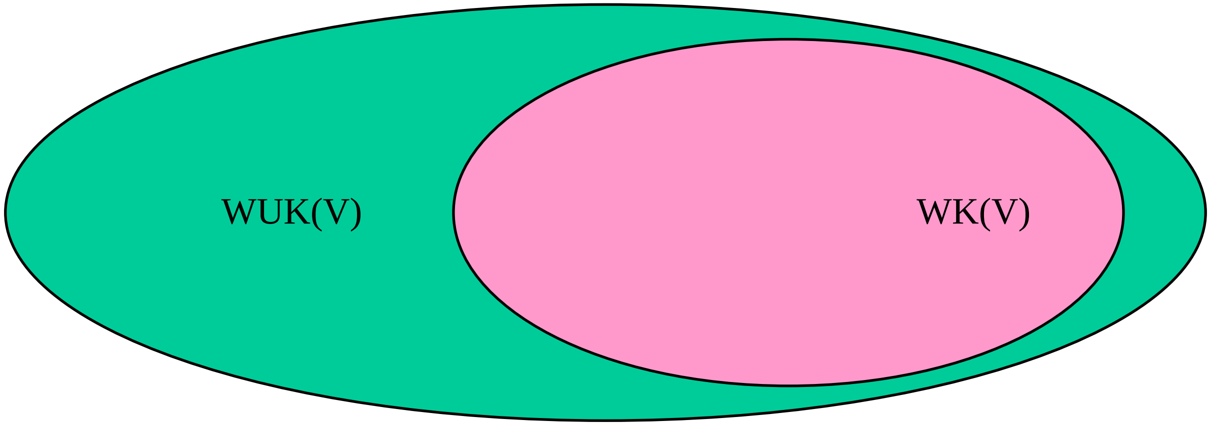
- MW(P) weaknesses mitigated by P
- UMW(P) weaknesses unmitigated by P



- MW and UMW
  - Are functions of P
  - Partition W
  - System constants
  - Independent of who is viewing the system

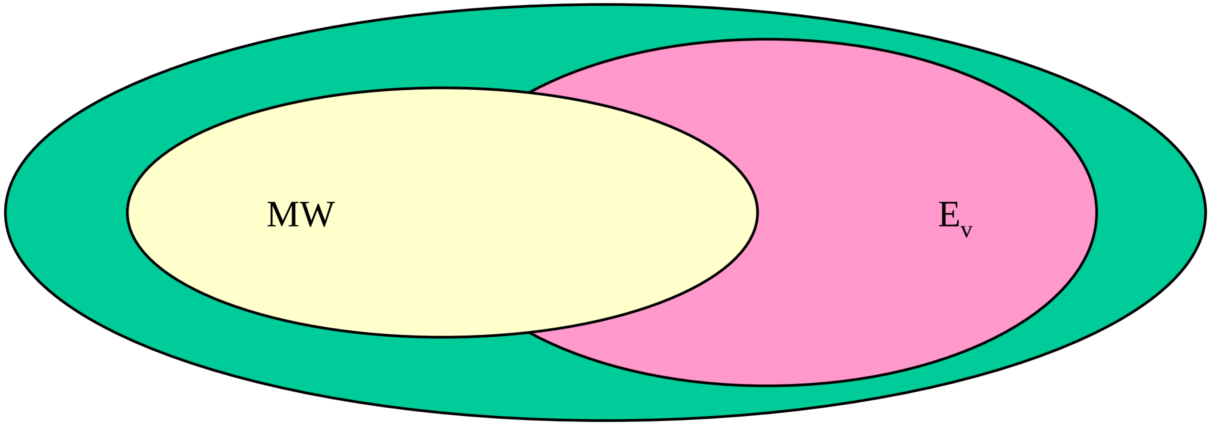
Known Weaknesses

- V is a viewer of the system
- WK(V) is the set of weaknesses known to V
- WUK(V) is the set of weaknesses unknown to V



Exploitable Weaknesses

- The weaknesses exploitable by V
  - $E(P,V)=UMW(P) \cap WK(V)$ → E_v



Definition of Security….

If V is an adversary and E_V is empty, then S is secure against V

More Axioms

Weakness Axiom 2: For viewer, V, of the system we have that WK(V) is a strict subset of W

Weakness Axiom 3: The system owner cannot know WK(V) for all adversarial viewers of the system

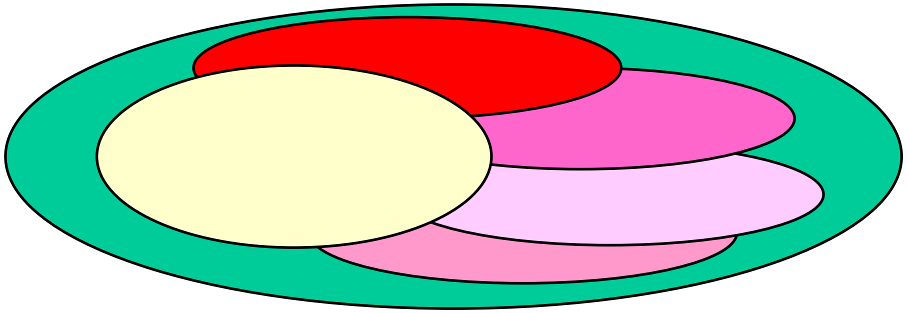
Security Metrics

- Real valued function of the communication system
  - Owner computable
  - Non trivial
  - Meaningful

Metric Axiom 1: Sets comprised of unknown weaknesses are not measurable

Weakness Based Metrics

- **Theorem 1:** There are no security metrics that include WUK(V) in a non-trivial way
- $E = \cup_V E_v$ E embodies all weaknesses that the system owner should be concerned about



- **Theorem 2:** E is not measurable and thus no non-trivial security metric exists using that quantity

The main point of the story

- Weakness-based metrics are the metrics of choice
  – Weaknesses or lack thereof embody the security of the system
  – One cannot know all of the unmitigated weaknesses
  – No nontrivial security metric of unknown weaknesses exists

No metric exists that can tell you how secure your system is in an absolute sense

The main point of the story Does Not Say…

- The main point does not say that you cannot secure your system
  - One may create a system so that E is empty and is thus secure against all real adversaries
  - You will just never know when you have done that

- The main point does not say that all security metrics are trivial
  - Some value can be had from measuring known aspects of the system

Further Research

- What aspects of the system can we use to estimate the security of the system?
- What constitutes a good estimate of the system security?
- What methodologies and processes give reasonable estimates on security?

Maybe we should use the term “security estimators”

Rather than “security metrics”

QUESTIONS?