Wireless Security Panel

April 21, 2005

Bruce McNair

bmcnair@stevens.edu

Consider:

Clarke’s Third Law:

“Any sufficiently advanced technology is indistinguishable from magic”

Consider:

Clarke's Third Law:

"Any sufficiently advanced technology is indistinguishable from magic"

This is an understandable attitude for the average end user, but what if technologists start having such feelings?

Consider:

Clarke’s Third Law:

“Any sufficiently advanced technology is indistinguishable from magic”

Goedel’s Incompleteness theorem:

A formal system of sufficient complexity cannot be both consistent and decidable (complete) at the same time

Consider:

Clarke’s Third Law:

“Any sufficiently advanced technology is indistinguishable from magic”

Goedel’s Incompleteness theorem:

A formal system of sufficient complexity cannot be both consistent and decidable (complete) at the same time

Developers cannot tolerate inconsistent formal specifications. System evaluators and customers take a dim view of incomplete specifications

Consider:

Clarke’s Third Law:

“Any sufficiently advanced technology is indistinguishable from magic”

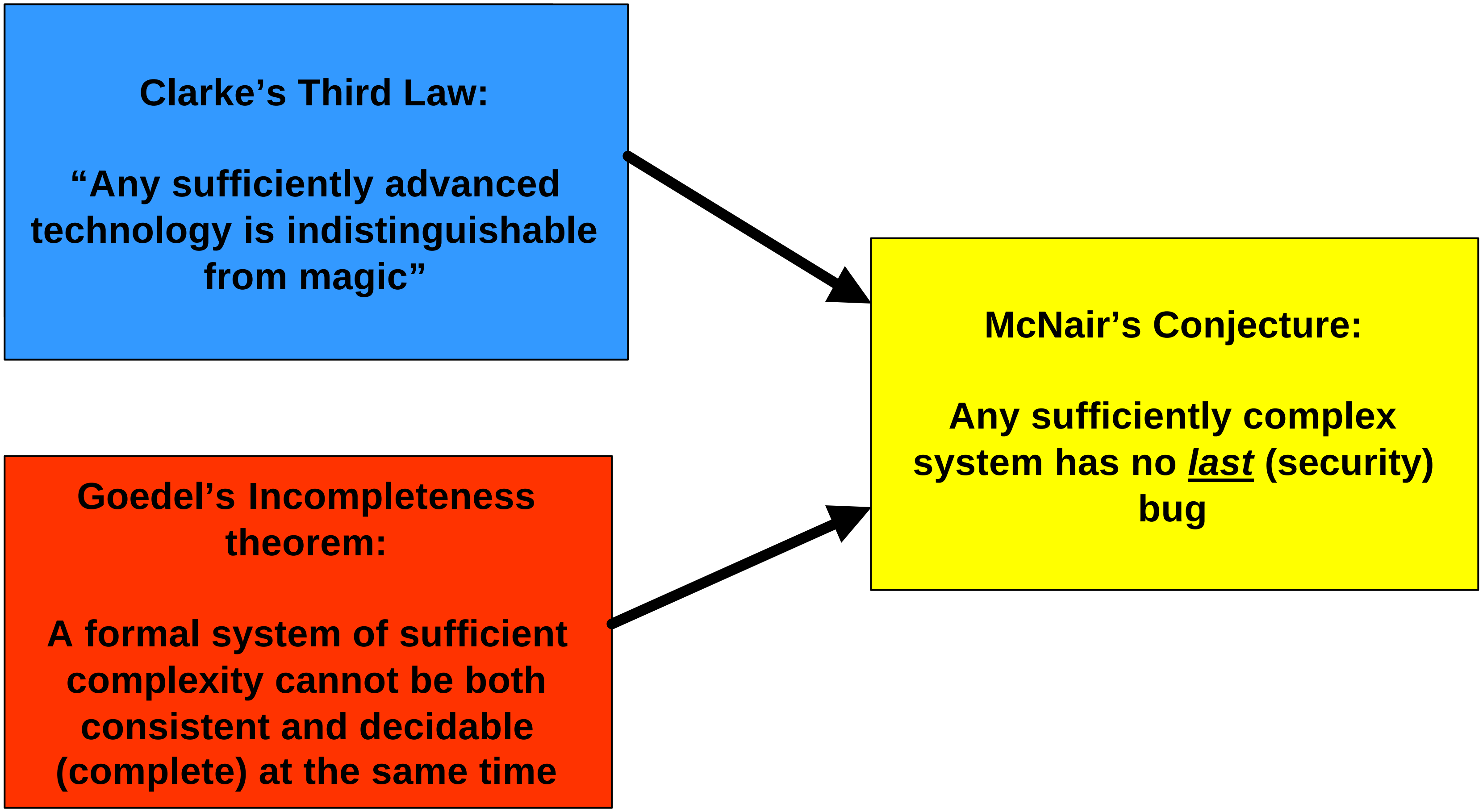
Goedel’s Incompleteness theorem:

A formal system of sufficient complexity cannot be both consistent and decidable (complete) at the same time

Developers cannot tolerate inconsistent formal specifications. System evaluators and customers take a dim view of incomplete specifications

Attackers love either

Consider:



Clarke’s Third Law:

“Any sufficiently advanced technology is indistinguishable from magic”

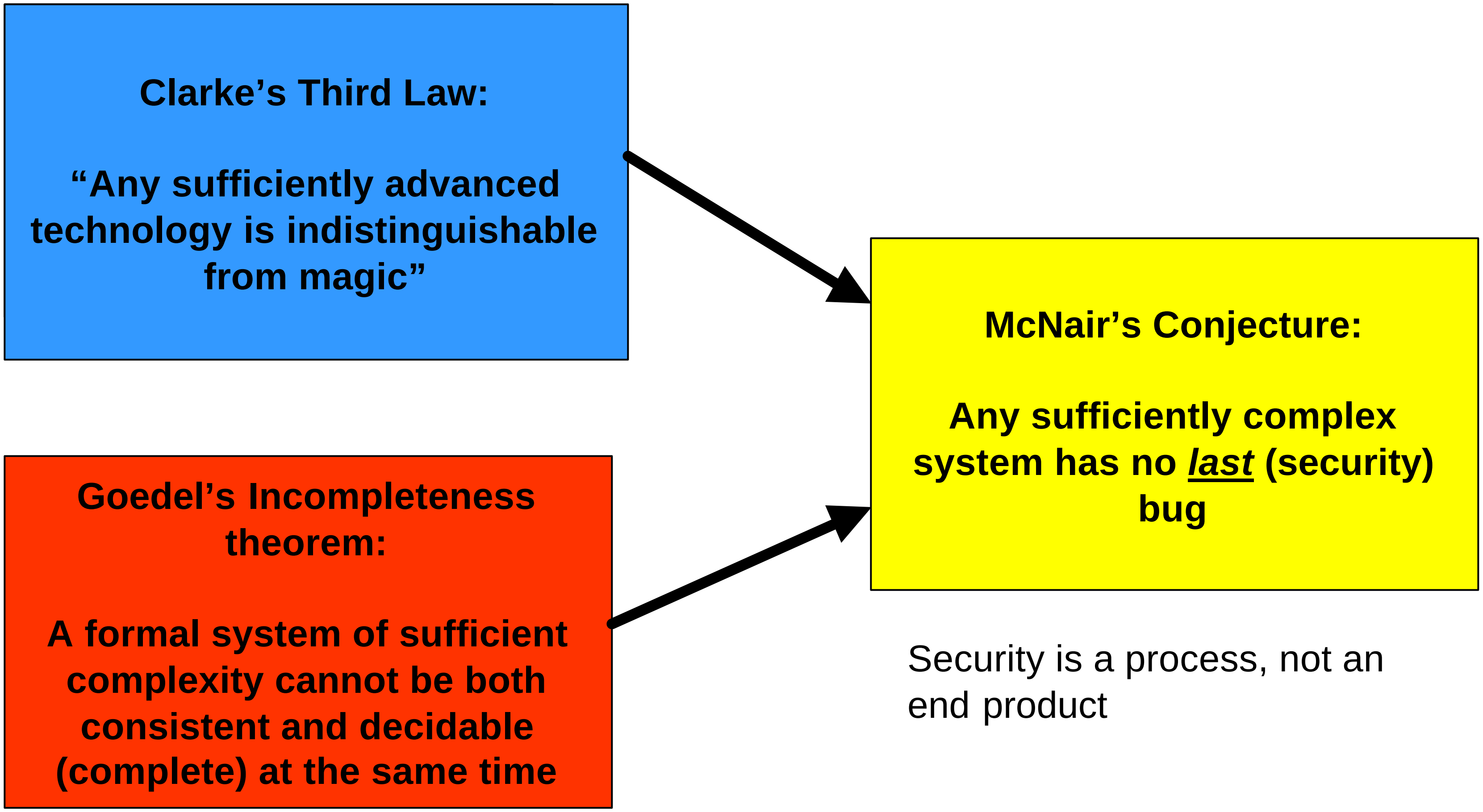
Goedel’s Incompleteness theorem:

A formal system of sufficient complexity cannot be both consistent and decidable (complete) at the same time

McNair’s Conjecture:

Any sufficiently complex system has no *last* (security) bug

Consider:



Clarke's Third Law:

"Any sufficiently advanced technology is indistinguishable from magic"

Goedel's Incompleteness theorem:

A formal system of sufficient complexity cannot be both consistent and decidable (complete) at the same time

McNair's Conjecture:

Any sufficiently complex system has no *last* (security) bug

Security is a process, not an end product

Quality Lessons

- Quality: “Meeting customer’s expectations”
- “Quality is Free” (title of Phil Crosby’s book)
- Quality is a process, not a product
- Continuous process improvement

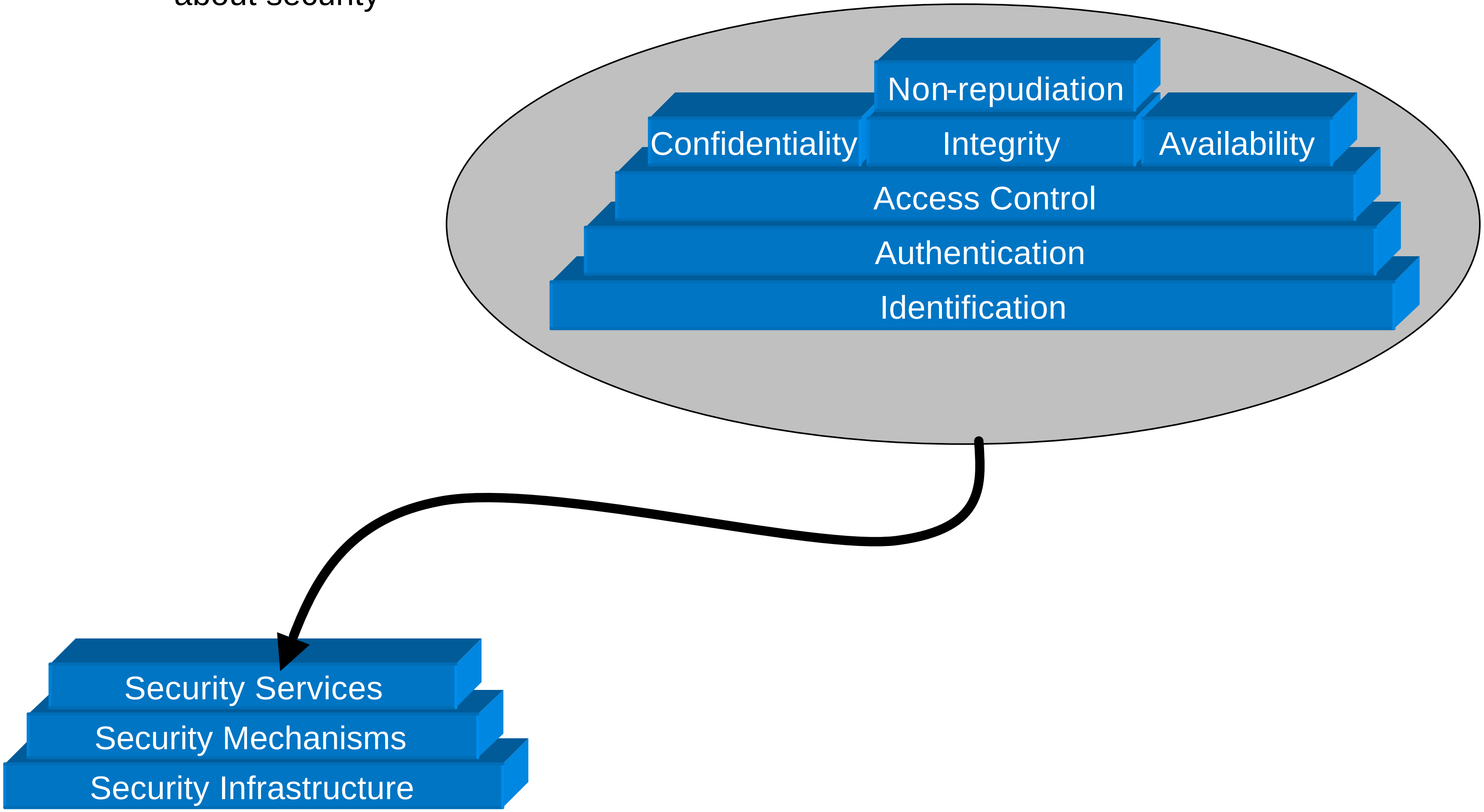
Applying Quality Lessons to Security

- Quality: “Meeting customer’s expectations”
- “Quality is Free” (title of Phil Crosby’s book)
- Quality is a process, not a product
- Continuous process improvement

- Security: “Meeting customer’s expectations, **in the presence of the actions of an adversary**”
- Security is Free
- Security is a process, not a product (see “Secrets and Lies” by Bruce Schneier)
- Security needs evolve as the threat environment evolves

But What is “Security?”

1. A structure is needed to talk about security



Non-repudiation

Confidentiality

Integrity

Availability

Access Control

Authentication

Identification

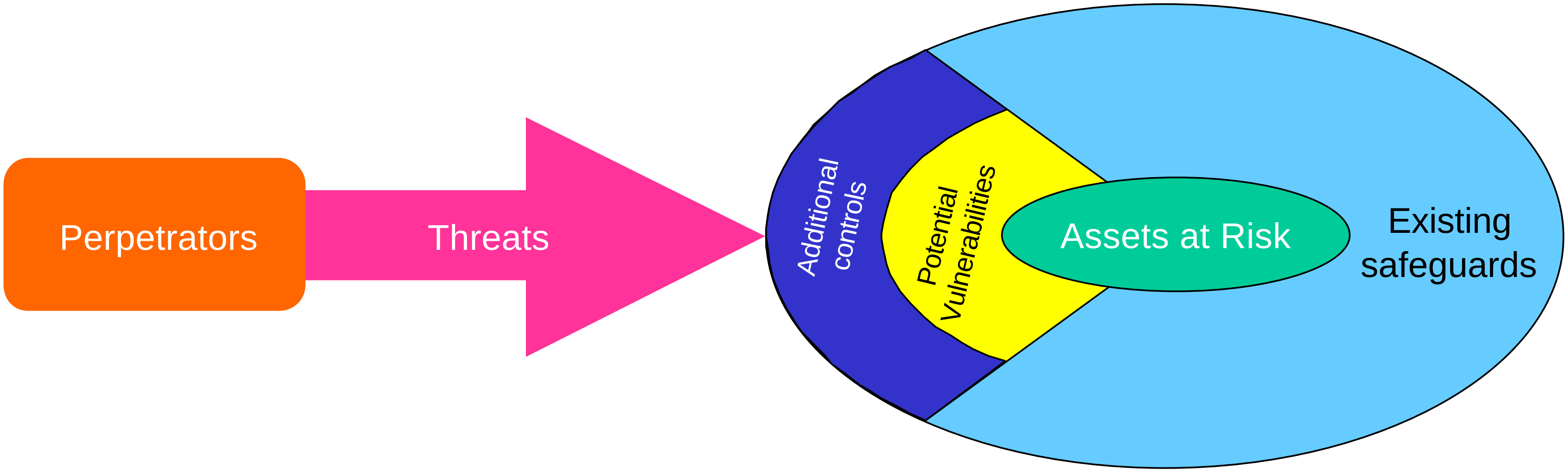
Security Services

Security Mechanisms

Security Infrastructure

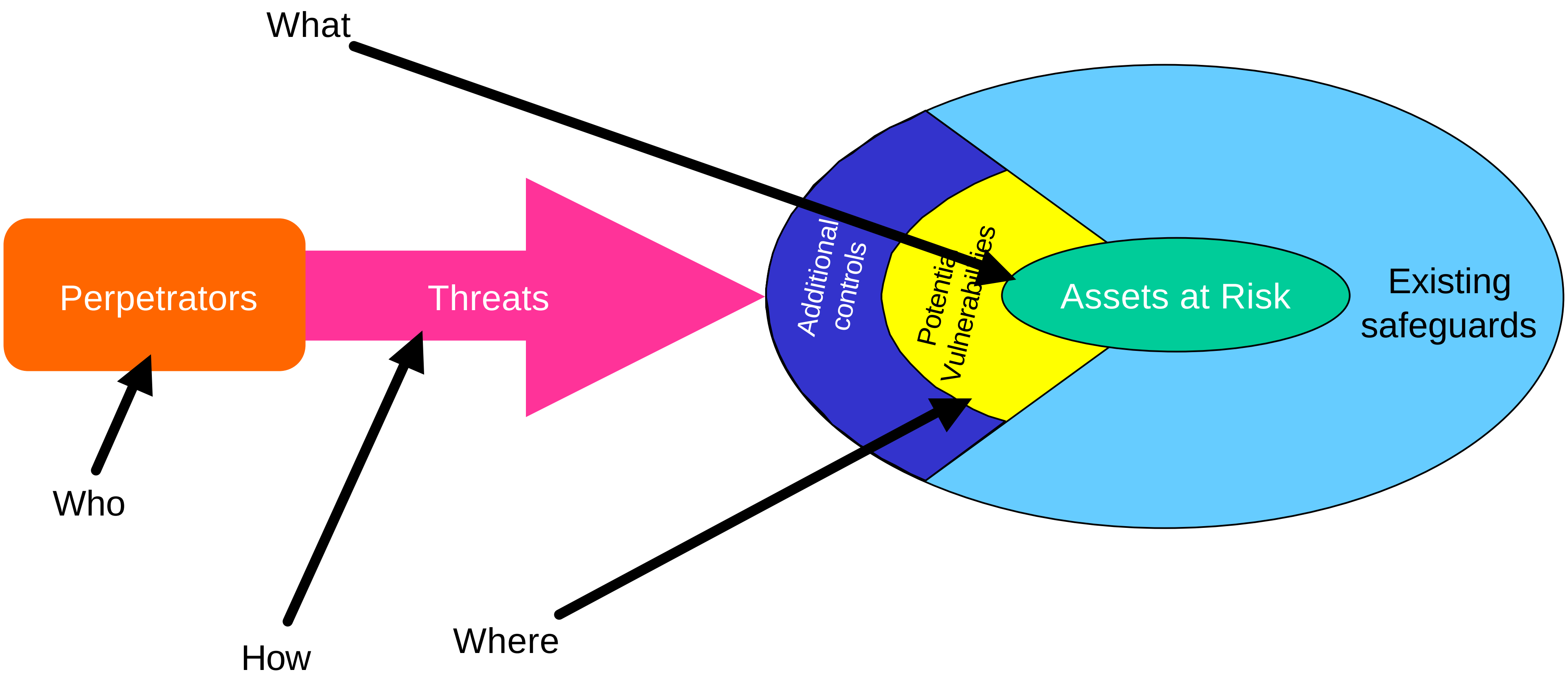
How To Evaluate Security Needs

2. An assessment process is needed



How To Evaluate Security Needs

2. An assessment process is needed



When?

Why?

How Not To Approach Security in Wireless Systems

~20th Century BC	Monoalphabetic cipher invented
~0th Century AD	Monoalphabetic cipher popular (Caesar cipher)
~15th Century	General attack on monoalphabetic cipher known
~16th Century	Polyalphabetic cipher invented
~17th Century	General attack on polyalphabetic cipher invented
~1917	Provably secure one-time pad invented
~1925	Polyalphabetic attack against incorrectly used “one-time” pad demonstrated
~1990	Wired Equivalent Privacy application of RC-4 stream cipher standardized in 802.11
~1995	17th Century attack against polyalphabetic ciphers renders WEP of questionable use

Lessons Learned

- Even not-so-advanced technologies can mystify technically savvy people when they don’t
  a) Consider the ramifications of their application
  b) Consider the skills and motivations of the attackers