What's Next in Multimedia?

(hopefully Security)

"Of What Use Is Wireless Multimedia Without Security?"

April 22, 2005

Bruce McNair

bmcnair@stevens.edu

201-216-5549

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"

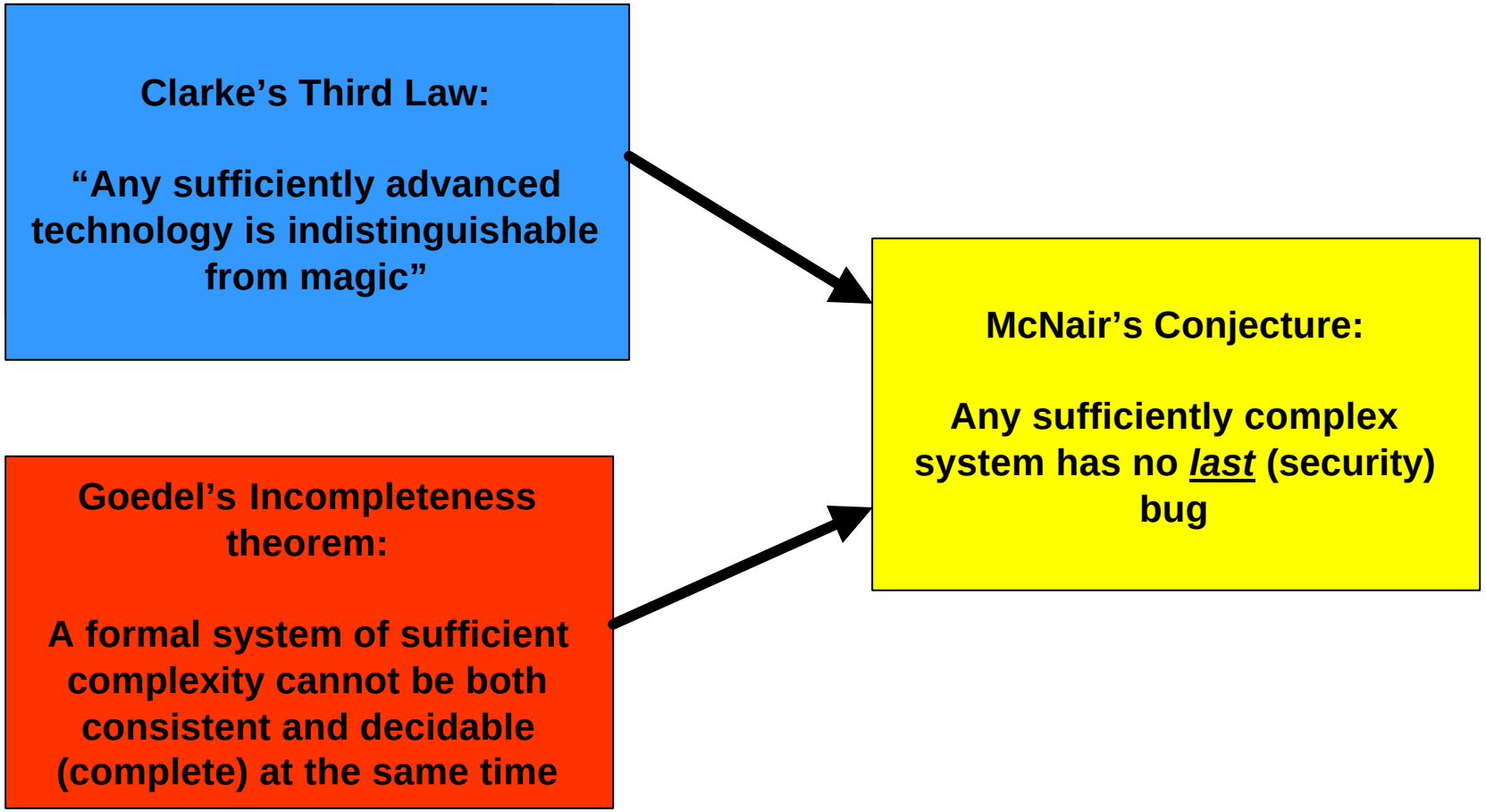
Goedel's Incompleteness theorem:

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

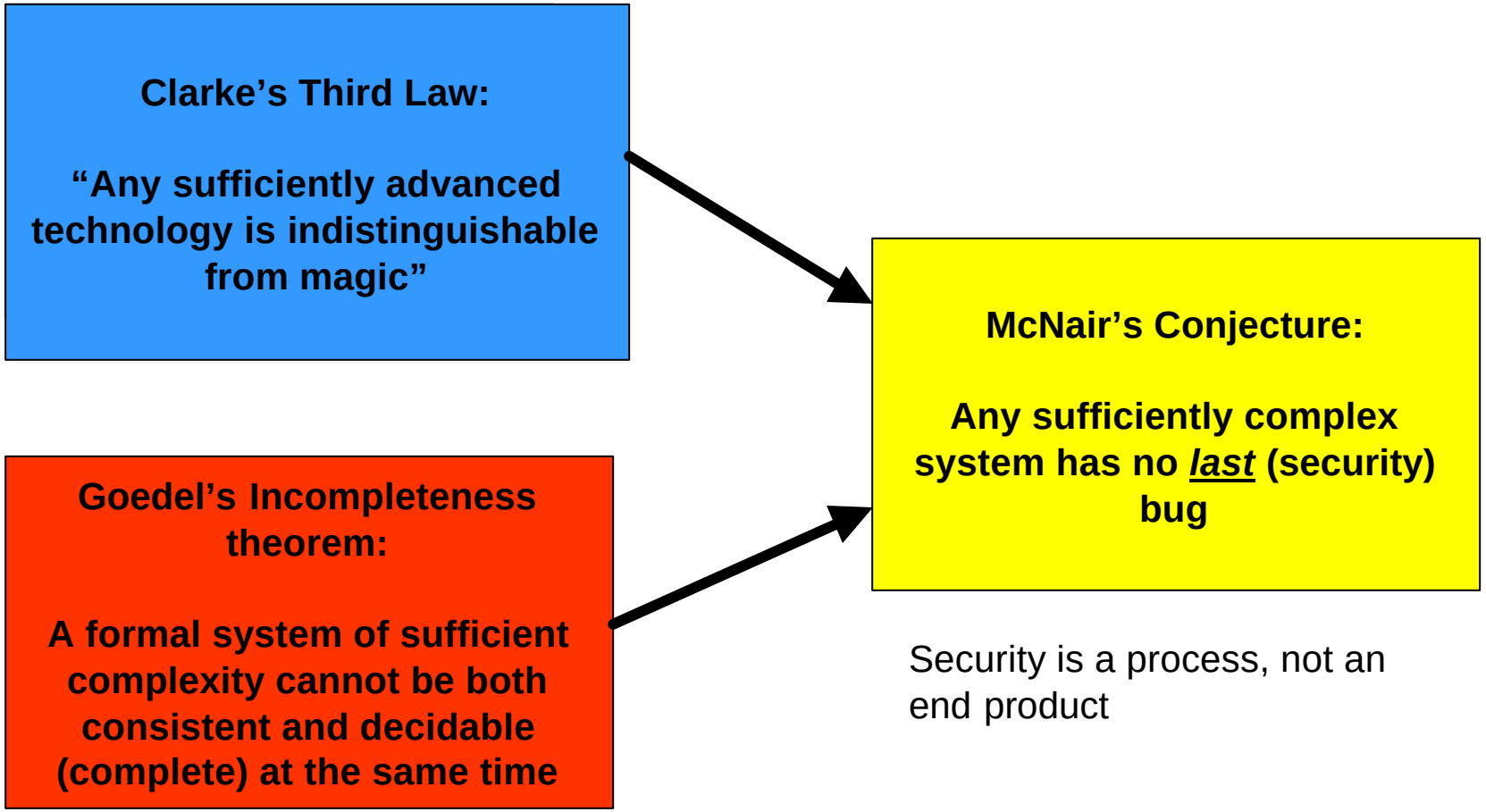
Developers cannot tolerate inconsistent formal specifications. System evaluators and customers take a dim view of incomplete specifications

Attackers love either

Consider:



Consider:



Security is a process, not an end product

How Does The Evolution of Technology Influence Security Needs?

1800s	Telegraph	Is the telegraph operator a busy-body who will share the contents of my telegram?
1890s	All calls placed by operators	Can the operator redirect customers to my competitor?
1930s – 1950s	Telephone party lines	Can the neighbors hear our conversation?
1960s – 1970s	Long distance calling	Can "phone phreaks" steal free calls
1980s	Cellular phone calling Credit card calling	Can criminals steal calling card numbers, clone cell phones to get free, untraceable calls?
1990s	Wireless LANs	How long does it take to break a WEP key?
Early 21st Century	Identity theft, consumer fraud, etc.	Will someone capture my ID credentials, payment tokens, ???
The Future	???	Things are not likely to get easier…

Who Is Motivated to Address Security?

Who Is Motivated to Address Security?

Financial Institutions?	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?
Trade Associations?	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?
Trade Associations?	Who makes up trade associations?

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?
Trade Associations?	Who makes up trade associations?
Universities?	

Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The “Government?”	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?
Trade Associations?	Who makes up trade associations?
Universities?	Is it a sustainable funding area?

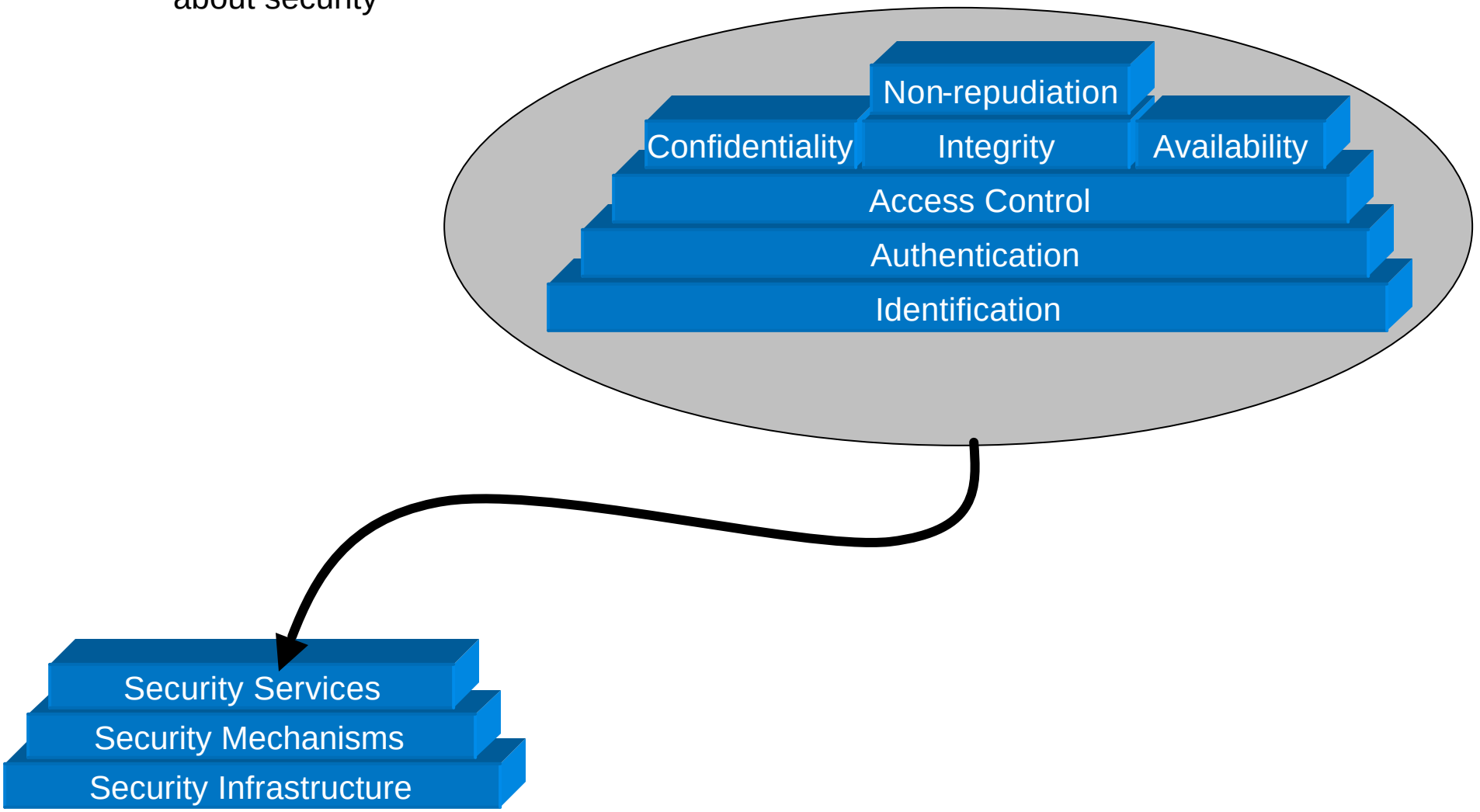
Who Is Motivated to Address Security?

Financial Institutions?	To protect their assets To meet insurers needs
The "Government?"	To address National Security, Homeland Security needs
Communications carriers	To protect their revenue stream To comply with regulations
Equipment vendors?	If it helps to get an edge over the competition
Standards bodies?	Who makes up standards bodies? What is their level of experience in the subject area?
Trade Associations?	Who makes up trade associations?
Universities?	Is it a sustainable funding area?

Who addresses end user needs for privacy, guaranteed access to their information, protection against outside attack, etc.?

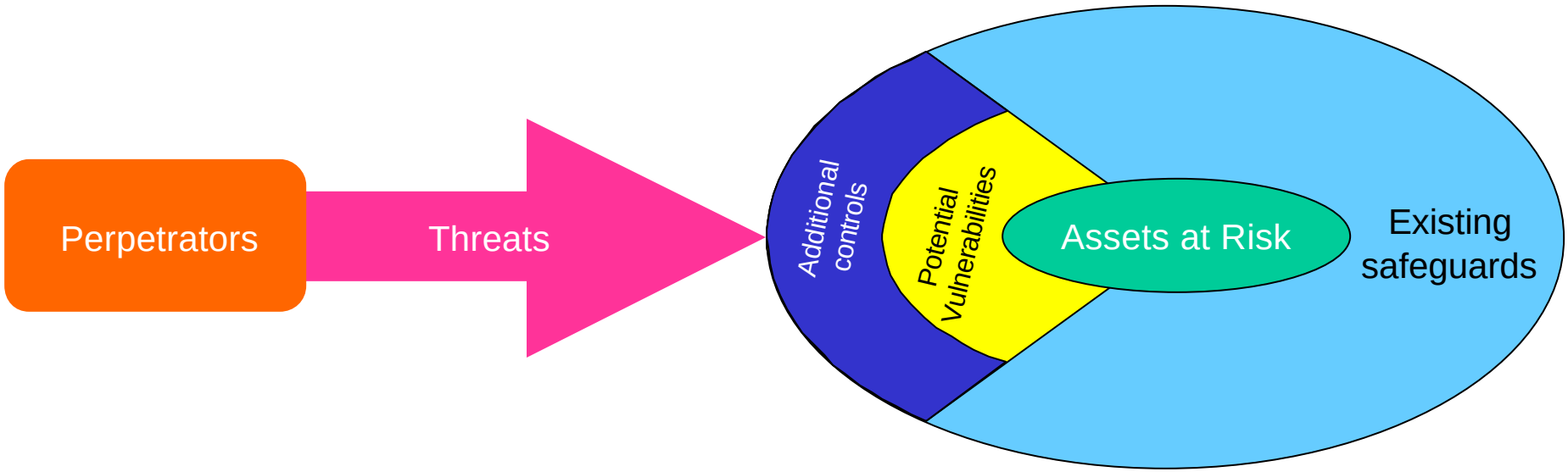
But What is “Security?”

1. A structure is needed to talk about security



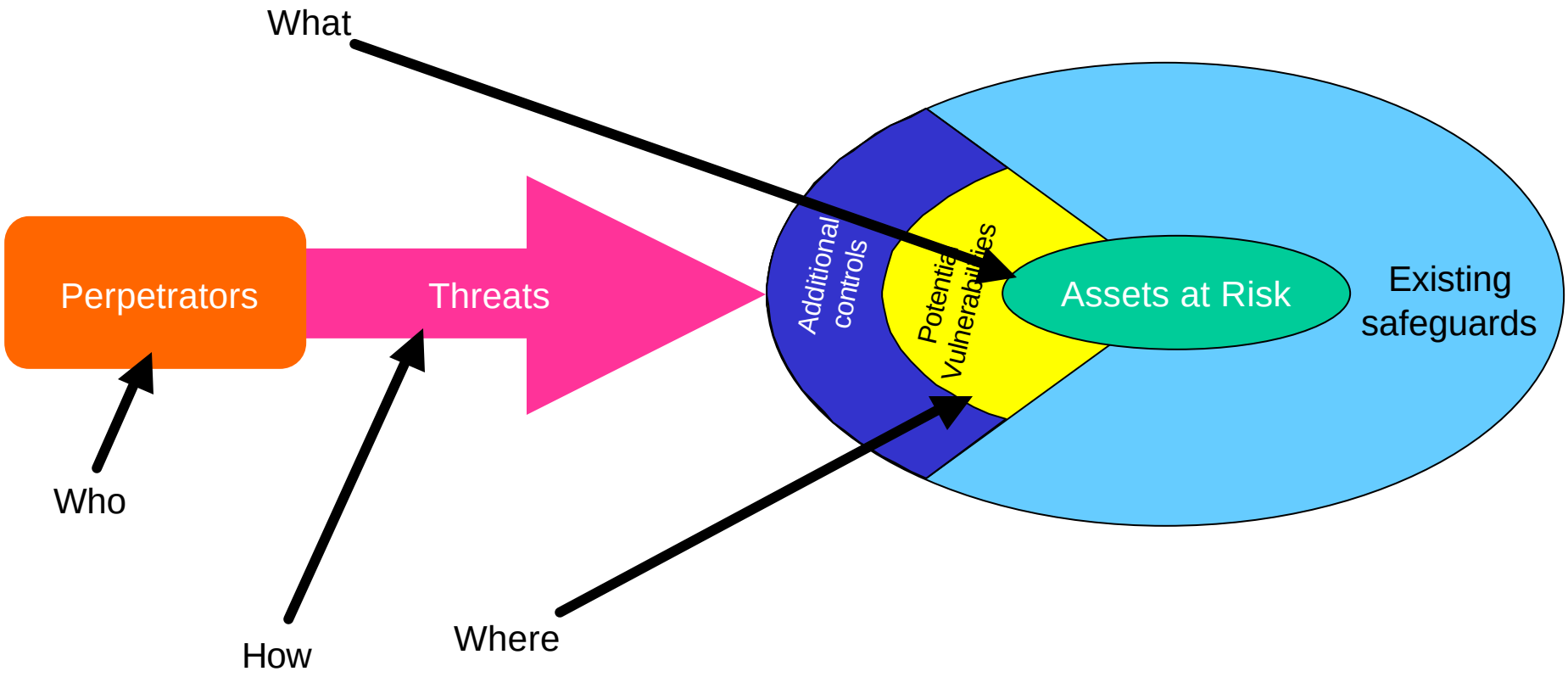
How To Evaluate Security Needs

2. An assessment process is needed



How To Evaluate Security Needs

2. An assessment process is needed



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

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
  c) Learn from others' past misteaks (sic)