Challenges of Cyber Security Education at the Graduate Level

Ravi Sandhu
Executive Director and Endowed Professor
Nov. 9, 2012

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Cyber technologies and systems have evolved

Cyber security goals have evolved
- Computer security
- Information security = Computer security + Communications security
- Information assurance
- Mission assurance

Cyber security research and practice are loosing ground
Graduate Cyber Security Education

Tech-Light  Tech-Medium  Tech-Heavy

World-Leading Research with Real-World Impact!
Cyber Security as a Discipline

Computer Science and Engineering

Cyber Security
Cyber Security as a Discipline

Computer Science and Engineering

Cyber Security
Fundamental Challenge I

- Too much material to teach
- Growing faster than teachers can keep up
  - Computer science theory
  - Computer system principles and practice
  - Cyber security theory
  - Cyber security system principles and practice
  - Statistics, sociology, organizational theory, economics, psychology, game theory ….
  - Laws, regulations, compliance ….
  - Privacy ….
  - History, successes and failures
  - …..

The packaging challenge
Immature field

What is fundamental to cyber security?

Where are the boundaries of a cyber system?

What are the goals of cyber security?

The discipline challenge
Enable system designers and operators to say:

This system is secure
Enable system designers and operators to say:

This system is secure

There is an infinite supply of attacks

Not attainable
Enable system designers and operators to say:

This system is secure enough

Many successful examples
The ATM (Automatic Teller Machine) system is

- secure enough
- global in scope

Not attainable via current cyber security science, engineering, doctrine

- not studied as a success story

Similar paradoxes apply to

- on-line banking
- e-commerce payments
Enable system designers and operators to say:

This system is secure enough

In an innovative ecosystem the innovation drive will ensure that the bar for enough will be fairly low.
Cyber Security is all about tradeoffs

- Let’s build it
- Cash out the benefits
- Next generation can secure it

- Let’s not build it
- Let’s bake in super-security to make it unusable/unaffordable
- Let’s sell unproven solutions

There is a middle ground
We don’t know how to predictably find it
Develop a scientific discipline
- to predictably find the sweet spots for different application and mission contexts
- to predictably find, incentivize and deploy microsec that leads to desirable macrosec outcomes
- that can be meaningfully taught in Universities at all levels: BS, MS, PhD

Prognosis
- we shall succeed (we have no choice)
- but we need to change to succeed
ICS Projects

- Secure information sharing
- Social network security
- Secure data provenance
- Attribute based access control
- Botnet and malware analysis
- Smart grid security
- Hardware security
- Future internet