University of Pittsburgh

University of Pittsburgh
School of Computing and Information

Welcome to the

SAC-PA Workshop

The CI Cybersecurity Workshop for Education and Research

This workshop is part of the project supported by the National Science Foundation under Grant No. 1642117, entitled *CICI Regional: SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania.*

Supported by

University of Pittsburgh

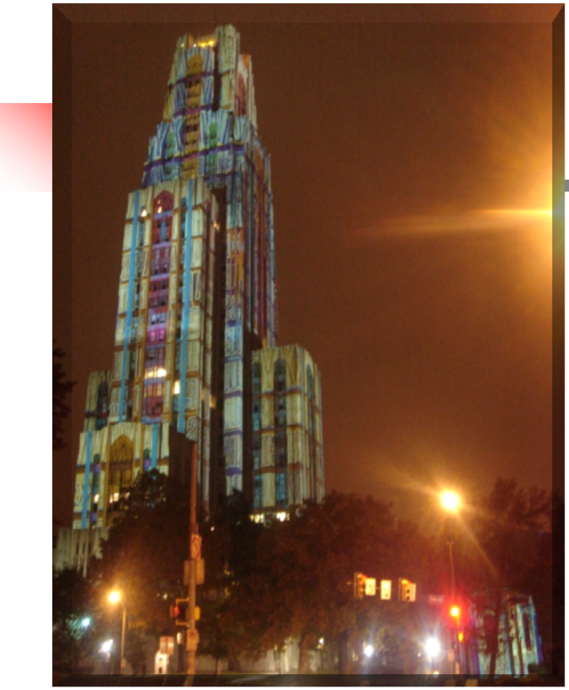
KINBER, A Commonwealth of Collaboration

Basic Info

- Breakfast, coffee breaks
- Meals
  - Lunch provided both days
    - Supported by University of Pittsburgh
      - Provost's Office, SCI
  - Dinner – on your own
- WiFi password:
- Need help?
  - Kelly Shaffer, Program Director at SCI
  - Runhua Xu, LERSAIS PhD student
  - Project team

NSF CICI Regional: SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania

Project overview



Funded by National Science Foundation

James Joshi (PI)

Professor, Director of LERSAIS

NSF CICI (Cybersecurity Innovation for Cyberinfrastructure)

- Objective:

  is to develop, deploy and integrate security solutions that benefit the scientific community by ensuring the integrity, resilience and reliability of the end-to-end scientific workflow

  - Collaboration, Shared cyberinfrastructure for Science
- Two areas (in 2016)
  - Resilient Security Architecture (for research cyberinfrastructure)
  - Regional Cybersecurity Collaboration
  - (Cybersecurity enhancement)
- Points of Contact:
  - Anita Nikolich, Program Director, CISE/ACI, telephone: (703) 292-4551, email: anikolic@nsf.gov
  - Kevin Thompson, Program Director, CISE/ACI, telephone: 703-292-4220, email:kthompso@nsf.gov

Motivation for SAC-PA project

- Data-driven scientific research & discovery
  - An unprecedented opportunity
- Cybersecurity is growing concern
  - Can be huge setback for scientific research/education if cyberinfrastructures are not protected
  - A significant national security issue
- Challenges:
  - Public-private cyberinfrastructure resources need to be interlinked/shared and protected
    - Need to help resource-constrained institutions
  - Cybersecurity needs and risks vary – requiring better ways to manage resources and institutional risk
  - Security best practices, better collaboration among stakeholders - sharing resources, expertise and information
- Regional collaboration and partnership among cyberinfrastructure providers and users critical !!
  - Such concerted collaborative effort is also very critical in addressing the National Cybercurity concerns

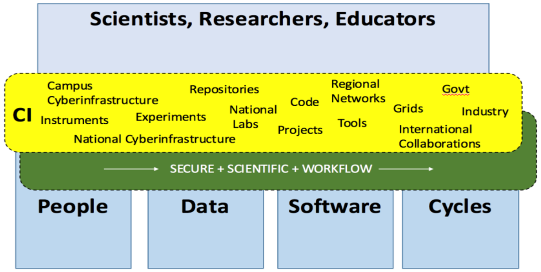

Scientists, Researchers, Educators
CI
Campus Cyberinfrastructure
Repositories
Regional Networks
Govt
Code
Grids
Industry
Instruments
Experiments
National Labs
Projects
Tools
International Collaborations
National Cyberinfrastructure
SECURE + SCIENTIFIC + WORKFLOW
People
Data
Software
Cycles

Figure 1. Cyberinfrastructure

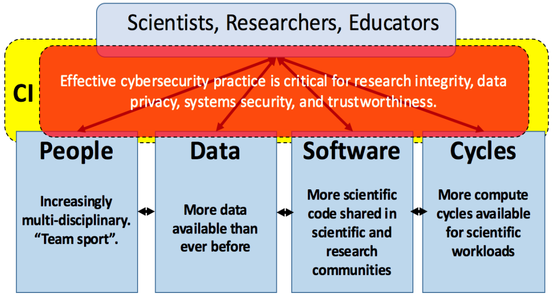

Scientists, Researchers, Educators
CI
Effective cybersecurity practice is critical for research integrity, data privacy, systems security, and trustworthiness.
People
Increasingly multi-disciplinary. "Team sport".
Data
More data available than ever before
Software
More scientific code shared in scientific and research communities
Cycles
More compute cycles available for scientific workloads

Figure 2. Effective Cybersecurity Practice

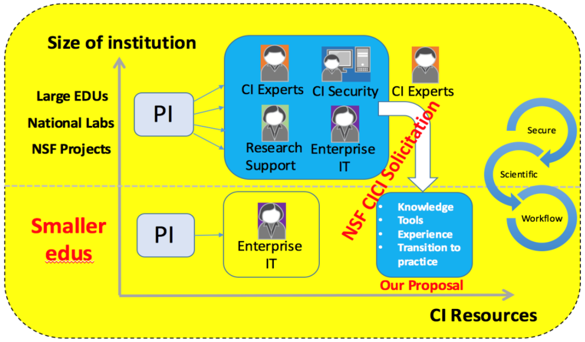


Figure 3. Project Landscape

SAC-PA Project Objectives

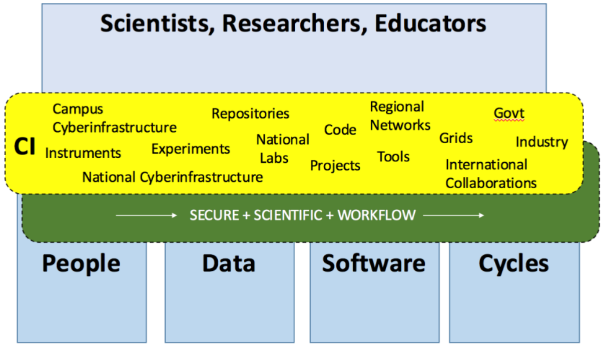
- Establish a regional collaboration and partnership framework, SAC-PA, within the state of Pennsylvania
  - Provide critical support to smaller academic institutions (schools and colleges, etc.), including resource constrained regional institutions that serve under-represented groups, females and high school teachers and students.
  - Enable concerted activities to promote the use of effective cybersecurity techniques and practice of security-assured cyberinfrastructure.

SAC-PA will provide a regional cybersecurity collaboration and partnership model that can be adopted by other regions, or be extended for national level collaborations.

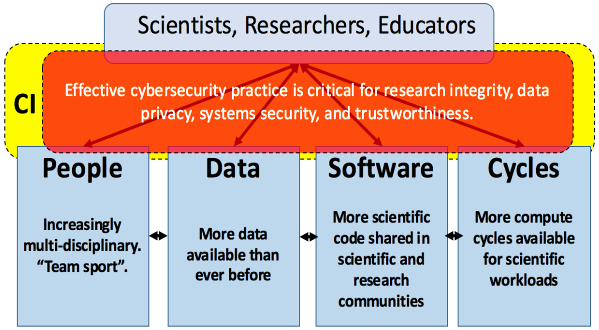
Key Tasks:

- Task 1: Develop and Deliver Regional Workshops for Cybersecurity
  - 3 workshops in Pittsburgh area
  - Emphasize smaller institutions, resource-constrained

  Goals:
    - **Understanding** of CI resources and Cybersecurity capabilities, & challenges
    - **Understand/Explore** existing/emerging cybersecurity challenges and solutions
    - **Develop** regional collaboration and partnership
      - Enable concerted cybersecurity activities
      - Promote effective techniques and practice



Scientists, Researchers, Educators
CI
Campus Cyberinfrastructure
Instruments
Repositories
Experiments
National Labs
Code
Projects
Regional Networks
Tools
Govt
Grids
Industry
International Collaborations
National Cyberinfrastructure
SECURE + SCIENTIFIC + WORKFLOW
People
Data
Software
Cycles



Scientists, Researchers, Educators
CI
Effective cybersecurity practice is critical for research integrity, data privacy, systems security, and trustworthiness.
People
Increasingly multi-disciplinary. "Team sport".
Data
More data available than ever before
Software
More scientific code shared in scientific and research communities
Cycles
More compute cycles available for scientific workloads

SAC-PA Workshops

SAC-PA 1 Workshop (June, 2017)
• Identify regional resources related to cyberinfrastructure & cybersecurity that relates to the scientific research community
• Presentations and discussion on cybersecurity challenges to the scientific research community
• Presentations, demos, and discussion on the state-of-the-art solutions, standards and best practices, and tools
• Security Education, Training and Awareness (SETA) + Transition to Practice
SAC-PA 2 Workshop (Nov/Dec, 2017)
• Cybersecurity Research to Practice
• Cybersecurity Tools and Techniques
• Security Standards, Best Practices and SETA
SAC-PA 3 Workshop (around May 2018)
• Delivery of training/tutorial modules developed
• Research, tools and techniques

Task 2: Training and Awareness Materials

- Task 2: Collaboratively Develop Training/Awareness Materials

  Develop and share cybersecurity training and awareness materials based on the needs and capabilities identified in the workshops

  - Cybersecurity/privacy tools;
  - Cybersecurity administration;
  - Cybersecurity standards (NIST, ISO, FISMA);
  - Cybersecurity risk management;
  - Cybersecurity regulations/compliances issues;
  - Cyberforensics;
  - Cyber-operational issues;
  - Cybersecurity incident handling, disaster management, and business continuity planning;
  - Host, Network and Cyberinfrastructure – prevention, detection and response; Threat Management, etc

Task 3: SAC-PA Collaboration/partnership

- Task 3: Establish Regional Partnership and a Shared Repository of Cybersecurity Resources/Capabilities.
  - Establish SAC-PA framework
  - Creation & sharing of innovative solutions, best practices & know-how, expertise and resources
    - ***Integrated and Shared Repository***
      - SETA materials
      - Practical Tools
      - Online resources (standards, guidelines, ..)
      - Expertise, Capabilities

Knowledge Sharing
Collaboration
Integrative, Concerted Efforts
Innovation & discovery
Standard/effective practices
…

Initial Partners for Collaboration

- Keystone Initiative for Network Based Education and Research (KINBER)
- University of Pittsburgh's CSSD's Information Security Team
- Open Science Grid
- Center of Trustworthy Scientific Computing (CTSC)
- Internet2
- Pittsburgh Supercomputing Center
- REN-ISAC
- National Cyber-Forensics & Training Alliance (NCFTA)
- Federal Bureau of Investigation (FBI, Pittsburgh)
- University of Pittsburgh Medical Center (UPMC) – IT Security
- SEI-CERT

Project Team

- James Joshi (PI), Professor, SCI, University of Pittsburgh
- Brian Stengel (Co-PI), University of Pittsburgh
- Balaji Palanisamy (Co-PI), Assistant Professor, SCI
- Michael B. Spring (Co-PI), Associate Professor, SCI
- Prashant Krishnamurthy (Co-PI), Professor, SCI
- David Tipper (Co-PI), Professor, SIS

Project Page: http://www.sis.pitt.edu/lersais/research/sac-pa/
LERSAIS Page: http://www.sis.pitt.edu/lersais/

End of Day 1 … Discussion

- Comments/questions on presentations so far?
- Share info regarding your resources/capabilities/challenges
  - Educational and research facilities (Cybersecurity)
  - Cyberinfrastructures – availability/accessibility
- Share information about other CI and Cybersecurity resources/capabilities
- Other suggestions/ideas/thoughts?
- Interest for engagement/active participation

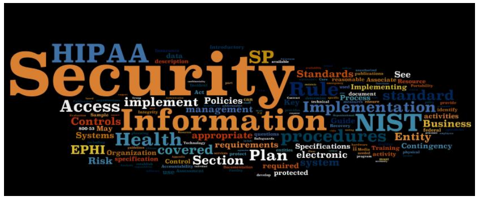
LERSAIS

- Laboratory of Education and Research on Security Assured Information Systems
  - Established in 2003
- NSA/DHS designated **CAE** since 2004
  - 5 CNSS IA certifications (one of about 15)
  - Re-designated in 2014 (till 2021)

    National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CAE IA/CD)
- NSA/DHS designated **CAE IA/CD-Research** (2008 -)
  - first group of 21 in US
  - Re-designated in 2014 - valid till 2021

IA Education programs & Outreach

- Security Assured Information Systems Track
  - MS/PhD in IST
  - MS/Phd in TEL&NET
  - Certificate of Advanced Studies
    - Post-BS and Post-MS (15 Credit)
    - CAS Online (started but currently paused !!)
  - BS IS focus on Cybersecurity
  - Ongoing development of Security Assured Health Informatics (NSF SAHI Project)
  - Integration with BigData/ IoT tracks/focus
  - DoD IASP and NSF CyberCorps SFS Programs

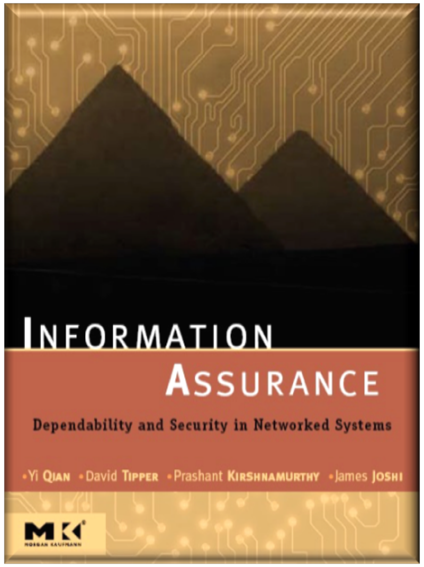


Other educational initiatives

- High School education – with FBI-Pittsburgh (Chris Geary) …. through Pitt's College in High School program
  - Three courses currently ; expected to include 10 schools in 2017 this year
- US Army War College Fellowship program at SIS
  - Beginning in academic year 2018 - 2019
- 5-year BS+MS Cybersecurity track
- Security Assured Health Informatics (SAHI)
  - Security tracks in Health Information Management (SHRS) & HealthIT Tracks in SAIS; Infrastructure for Research
- Certificate program for Management/C-level people
  - Exploratory – based on feedback from IAB

Key Research areas

- Security, Privacy and Trust Management Models
- Security in Wireless and Ad Hoc Networks
- Network Security and Survivability
  - DDoS, Network and Systems Survivability
- Security and Privacy in:
  - Cloud Computing, Social Networks, Big Data areas
  - Healthcare IT
  - Critical Infrastructures (SmartGrid, Nuclear Cybersecurity, etc.)
- Insider Threats in Critical Infrastructures, Cloud Environments, etc.
- Science of Security (Collaboration with SEI/CERT)
- Risk Management and Security Metrics
- etc.

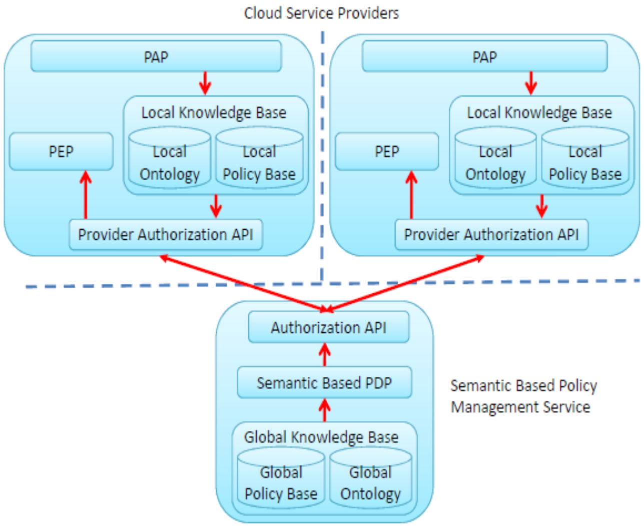

INFORMATION
ASSURANCE
Dependability and Security in Networked Systems
•Yi Qian •David Tipper •Prashant Kirshnamurthy •James Joshi
MK

Research Activities

- Advanced Access Control/ Trust Management Models/Approaches
  - Context based, Geo-social RBAC, Privacy/Trust aware RBAC
  - Secure Interoperation
    - RBAC, Trust based approaches
  - RBAC & Insider Threat Mitigation
  - Attribute based access (e.g., in Cloud)
- Insider Attack Mitigation
  - Cloud computing, Critical Infrastructure
  - Risk, Trust aware Access management
- Network Security
  - DDoS Attack, Some prior work in IPv6

Research Activities

- Security & Privacy in
  - Cloud computing & Social Network
    - Policy as a service; Access control in Cloud
    - **Privacy conscious execution in Cloud**
    - **Anonymization techniques**
    - **Privacy threat analysis (e.g., Identity Clone & Mutual Friend based attacks)**
    - Insider threats (NSA grant)
  - HealthCare IT
    - **Privacy aware Social Networks for Intimate Partner Violence**; Access control in Healthcare Systems
  - Location based services
    - Access/privacy control in LBSN
    - **Anonymization techniques**

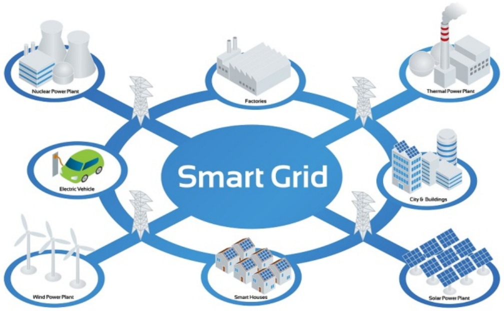


Other Ongoing Research Activities

- Cybersecurity in Critical Infrastructures
  - Secure SmartGrid
    - Key management issues
    - Insider threats
    - Microgrid security

    (David Tipper, with Center of Energy)
  - Nuclear Cybersecurity
    - Insider threats (NSA grant)

      (also with Adam Lee, James Joshi, Daniel Cole)
- Critical Infrastructure Resilience
  - Where to locate microgrids, availability improvement, etc.



Thanks a lot!

Welcome again ！

Active Funded IA Projects

- NSA CyberSecurity Research Grant: Towards Insider Threat Assessment and Mitigation ($264,553)
  - James Joshi (**PI**), Prashant Krishnamurthy, David Tipper

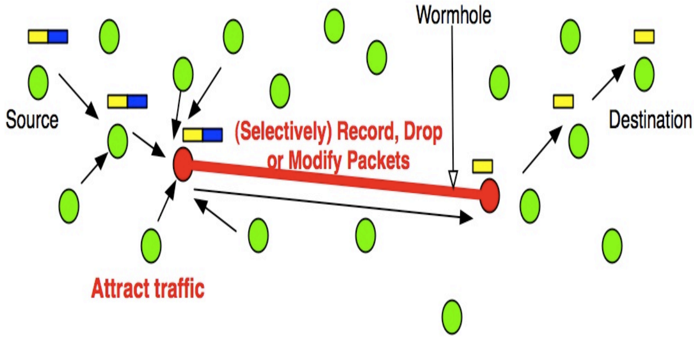
- SAC-PA – Towards *Security Assured Cyberinfrastructures* in Pennsylvania ($499,951)
  - James Joshi (**PI**), Balaji Palanisamy, Brian Stengel, Michael Spring, Prashant Krishnamurthy, David Tipper

- A Curriculum for Security Assured Health Informatics ($897,055)
  - James Joshi (PI), SIS & HIM colleagues (Bambang, Leming)

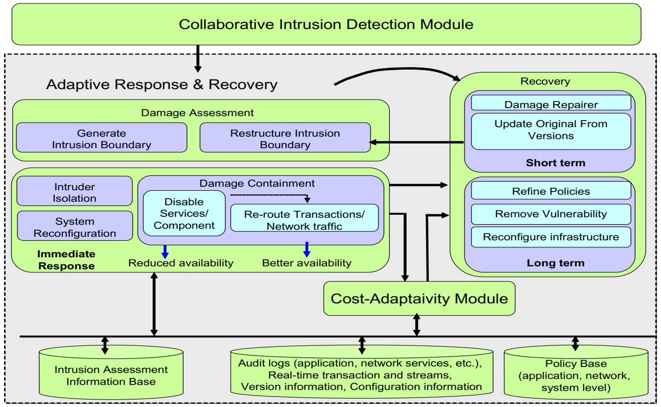
- NSF CyberCorp SFS Second Round is ending (James Joshi (PI))
- Science of Security (collaboration: Pitt + SEI-CERT)
  - Mike Spring, Eric Hatleback, Jonathan Spring (SEI), James Joshi

Other Sample Funded IA Projects

- ARSENAL: A cross layer Architecture for Secure resilieNt TacticAL mobile ad hoc networks: ARO- MURI UC-schools (Davis, Riverside, Santa Barbara, Irvine), Penn State, BYU, Utah)
  - David Tipper, Prashant Krishnamurthy



- Dynamic Data Driven Defense Mechanisms for Cybersecurity, NSF CSR-SGER Grant
  - David Tipper (PI; Taeib Znati), James Joshi, Prashant Krishmnamurthy

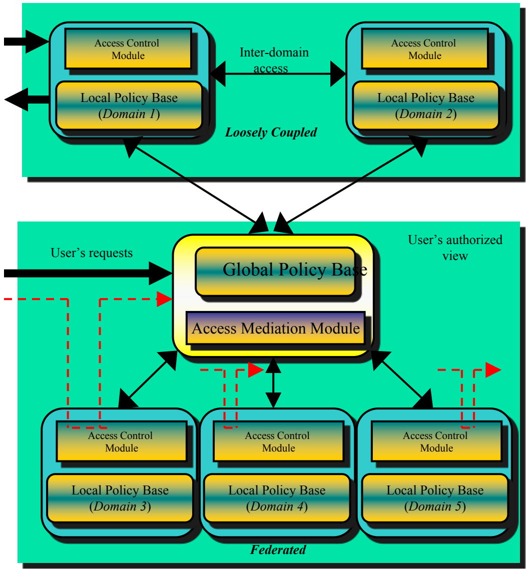

Collaborative Intrusion Detection Module
Adaptive Response & Recovery
Damage Assessment
Generate Intrusion Boundary
Restructure Intrusion Boundary
Intruder Isolation
System Reconfiguration
Damage Containment
Disable Services/ Component
Re-route Transactions/ Network traffic
Immediate Response
Reduced availability
Better availability
Recovery
Damage Repairer
Update Original From Versions
Short term
Refine Policies
Remove Vulnerability
Reconfigure infrastructure
Long term
Cost-Adaptaivity Module
Intrusion Assessment Information Base
Audit logs (application, network services, etc.), Real-time transaction and streams, Version information, Configuration information
Policy Base (application, network, system level)

Other Sample Funded IA Projects

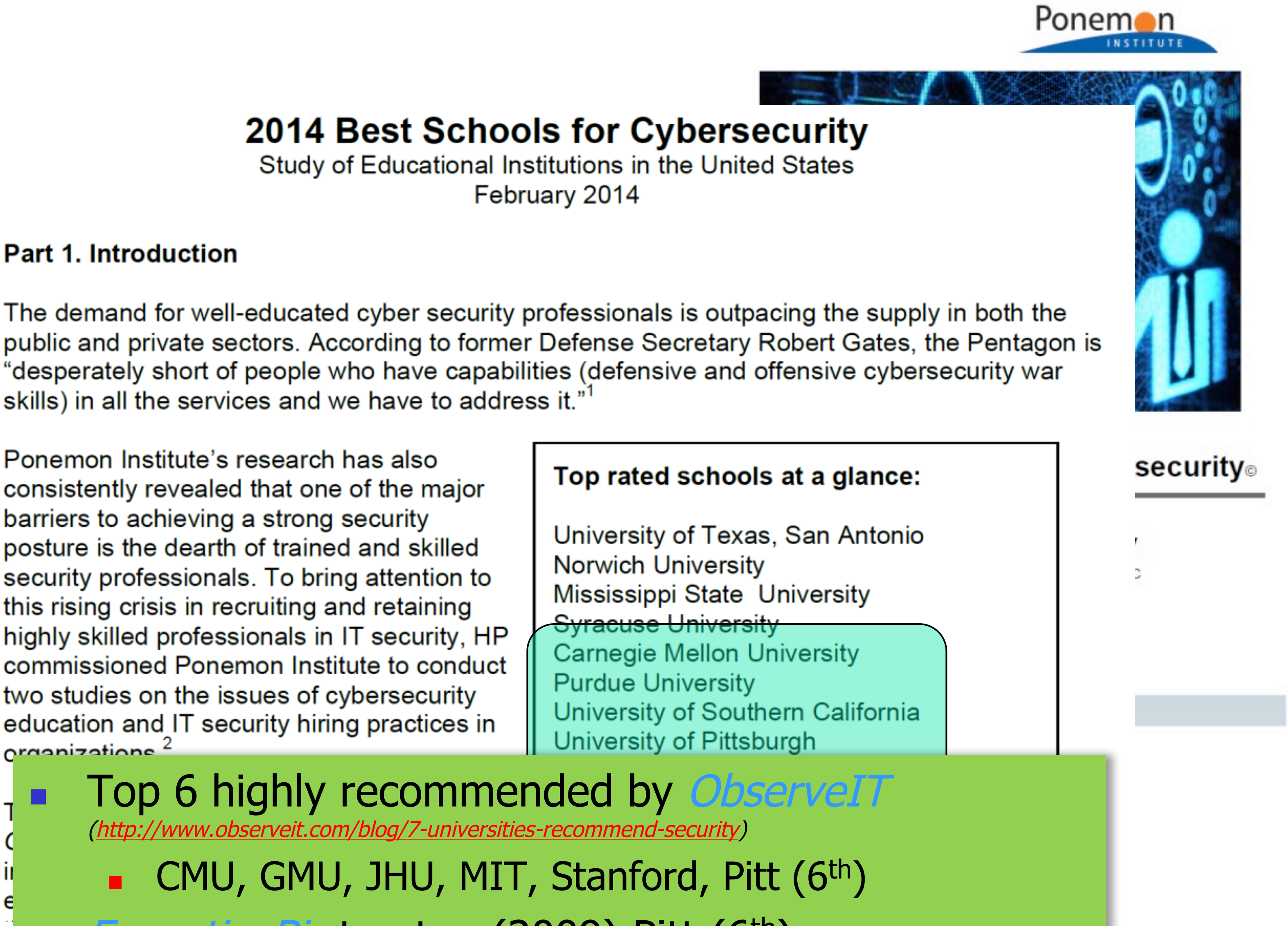
- MiMANSaS: Metrics, Models and Analysis of Network Security and Survivability, NSF CT-ER Grant (Collaboration with 2 other institutions)
  - David Tipper (TEL) with Duke and University of Missouri – Kansas City
- Coping with Jamming Attacks in Wireless Ad Hoc and Mesh Networks
  - Prashant Krishnamurthy (with UC Irvine)
- E-SPAWN: Efficient Security and Privacy Solutions for Applications in Wireless Sensor Networks (Partial support from Norwegian Research Council)
  - Vladimir Zadorozhny and Prashant Krishnamurthy

Other Sample Funded IA Projects

- Ditributed Collaborative Traffic Monitoring for DDoS Mitigation (Cisco Research Grant)
  - James Joshi
- NSF CAREER: A Trust-based Access Control Management Framework for Secure Information Sharing and Multimedia Workflows in Heterogeneous Environments (NSF-IIS)
  - James Joshi



- Security in Agent Based Pervasive Environment
  - James Joshi;
  - Funded by/Collaboration with Ajou University, S. Kore



Ponemon INSTITUTE

2014 Best Schools for Cybersecurity

Study of Educational Institutions in the United States
February 2014

Part 1. Introduction

The demand for well-educated cyber security professionals is outpacing the supply in both the public and private sectors. According to former Defense Secretary Robert Gates, the Pentagon is "desperately short of people who have capabilities (defensive and offensive cybersecurity war skills) in all the services and we have to address it."[1]

Ponemon Institute's research has also consistently revealed that one of the major barriers to achieving a strong security posture is the dearth of trained and skilled security professionals. To bring attention to this rising crisis in recruiting and retaining highly skilled professionals in IT security, HP commissioned Ponemon Institute to conduct two studies on the issues of cybersecurity education and IT security hiring practices in organizations.[2]

Top rated schools at a glance:

University of Texas, San Antonio
Norwich University
Mississippi State University
Syracuse University
Carnegie Mellon University
Purdue University
University of Southern California
University of Pittsburgh

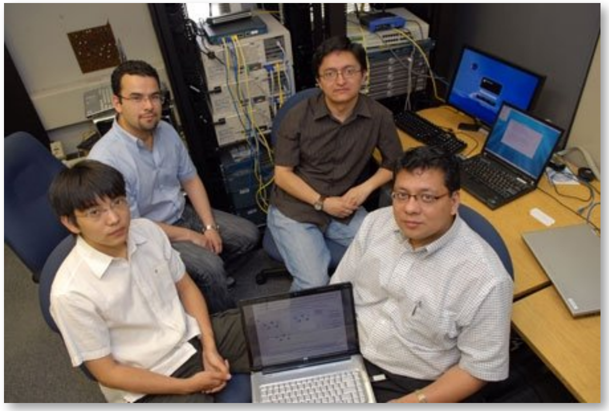
security©

- Top 6 highly recommended by *ObserveIT* (http://www.observeit.com/blog/7-universities-recommend-security)
  - CMU, GMU, JHU, MIT, Stanford, Pitt (6th)
- *ExecutiveBiz* top ten (2009) Pitt (6th)
  - http://blog.executivebiz.com/2009/09/top-10-universities-preparing-future-cyber-security-professionals/

Key LERSAIS Affiliated People

Affiliated faculty

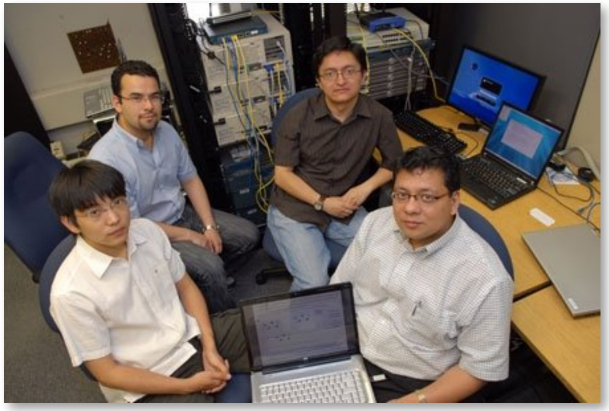
- James Joshi (Director), Michael Spring, Balaji Palanisamy, David Tipper, Prashant Krishnamurthy, Eric Hatleback, Vladimir Zadorozhny, (IST)
- David Thaw (Law),
- Adam Lee (CS), Taieb Znati (CS), Daniel Mosse
- Bambang Parmanto, Leming Zhou (HIM)



LERSAIS Homepage:
http://www.sis.pitt.edu/lersais/

LERSAIS

- SIS faculty affiliated with LERSAIS not here:
  - Balaji Palanisamy (Co-director),
  - David Tipper,
  - Prashant Krishnamurthy,
  - Michael Spring,
  - Eric Hatleback



LERSAIS Homepage:
http://www.sis.pitt.edu/lersais/

Proposal Cybersecurity Center at Pitt

- Working on proposal for creating of an ambitious Cyber Security Research Center (CyRes)
  - Since about last two years; currently paused !!
  - Key focus
    - Holistic, collaborative, multi-disciplinary research
    - Creating critical mass of researchers to address basic and applied research

Sample IA projects related to SIS faculty

	Project title	PI(s)	Source	Amount
1	Towards Insider Threat Assessment and Mitigation	Joshi et al	NSA CAE	$264,553
2	CICI: Regional: SAC-PA: Towards Security Assured Cyberinfrastructure in Pennsylvania	Joshi et al.	NSF CICI	$499,951
3	A Curriculum for Security Assured Health Informatics	Joshi et al.	NSF-DGE	$897,055
4	DiCoTraM: Towards a Distributed Collaborative Traffic Monitoring System	Joshi	CISCO	$54,034
5	ARSENAL: A cross layer Architecture for Secure resilient tactical mobile ad hoc networks,	Tipper, Krishnamurthy	ARO-MURI	$715,000
6	Collaborative Research: NeTS: WN: Coping with Jamming Attacks in Ad hoc / Mesh Networks	Krishnamurthy	NSF-NetS	$149,998
7	CT-ER: Collaborative Research: MiMANSaS: Metrics, Models and Analysis of Network Security and Survivability	Tipper	NSF-CT-ER	$23,397
8	CSR: SGER: Dynamic Data Driven Defense Mechanisms for Cybersecurity	Tipper, Joshi, Krishnamurthy	NSF-CCF	$104,537
9	A Trust-based Access Control Management Framework for Secure Information Sharing and Multimedia Workflows in Heterogeneous Environments	Joshi	NSF-CAREER	$ 416,419
10	CISCO CIAG Equipment Grant for Laboratory	Joshi, et.al.	CISCO-CIAG	$130,000
11	Survivable and Secure Wireless Information Architecture	Krishnamurthy, Tipper	NIST	$432,076
12	Design and Restoration Techniques for Fault Tolerant Wireless Access Networks	Tipper	NSF-ANIR	$300,000
13	Security Architecture for Wireless Residential Networks	Krishnamurthy	Univ Pitt	$13,230
14	Self-Configuring Multi-Networks for Information Systems Survivability	Tipper	DARPA	$1,251,241
15	Network Design and Traffic Recovery Procedures for Survivable Wide Area Networks	Tipper	NSF-CCR	$274,097
16	Role Assured Publicly Accessible Information (RAPAI)	Spring	Pitt/NSA	$25,000
17	A Security Assured Survivable Information System (SASIS)	Joshi	Univ Pitt	$16,000
18	TeleContinuity, Disaster-Proof Telecommunications, Advanced Technology Award	Thompson	NIST	$145,971

THANKS!

Information Security specialization

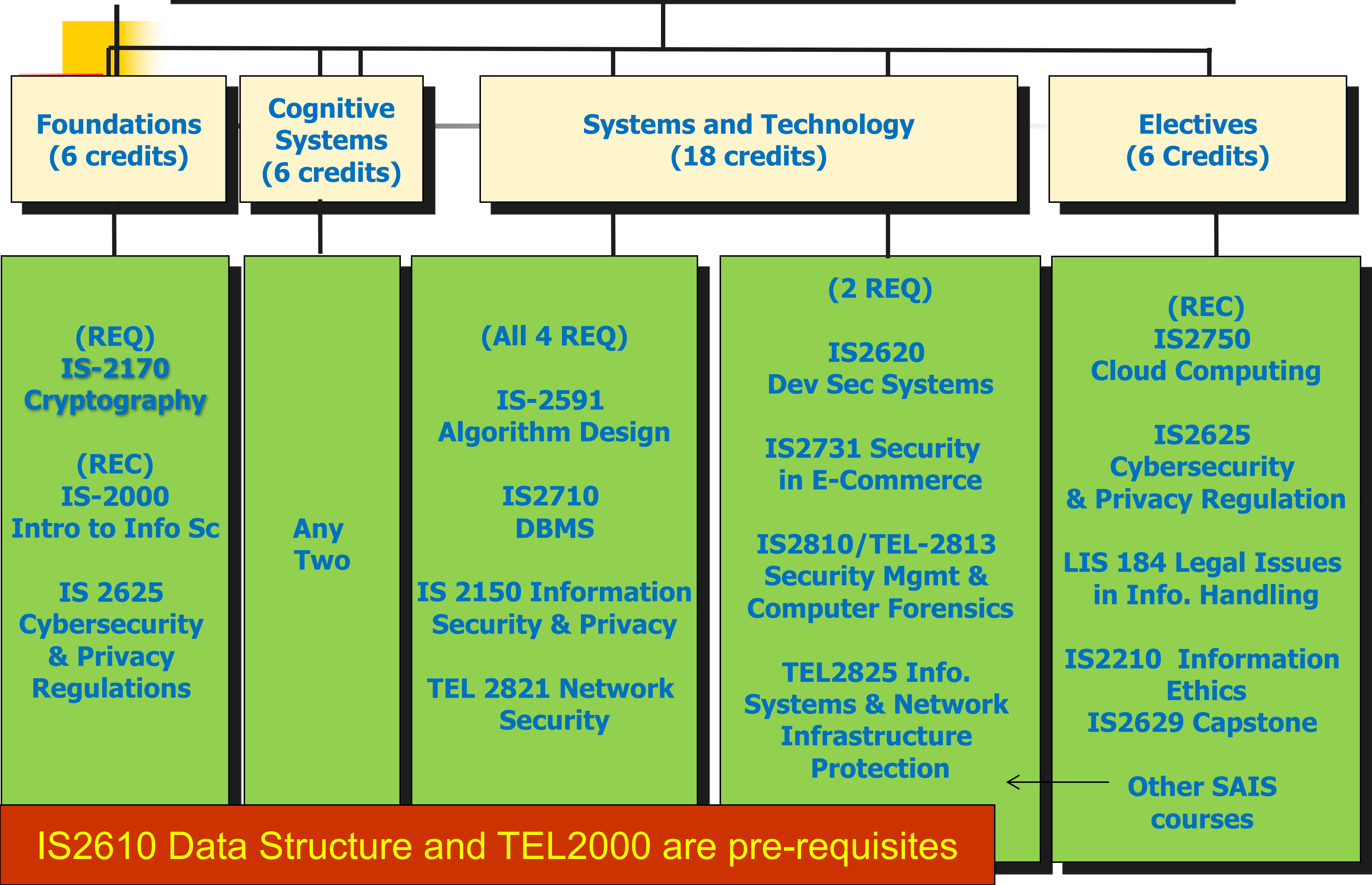
MS - Information Sciences
MS - Telecommunications and Networking
Certificate of Advanced Studies
(CNSS Certifications)

CORE Courses

1. Introduction to Security & Privacy
2. Cryptography
3. Network Security

1. Developing Secure Systems
2. Security Management & Computer Forensics
3. Security in E-commerce
4. Information System and Network Infrastructure Protection
5. Capstone course
6. Cybersecurity & Privacy Regulation
7. CyberCrime
8. Information Ethics
9. Legal Issues in Information Handling (LIS)
10. Science of Cybersecurity (Special topics)

MSIS
Security Assured Information Systems Track



Foundations (6 credits)

(REQ)
IS-2170
Cryptography

(REC)
IS-2000
Intro to Info Sc

IS 2625
Cybersecurity
& Privacy
Regulations

Cognitive Systems (6 credits)

Any
Two

Systems and Technology (18 credits)

(All 4 REQ)

IS-2591
Algorithm Design

IS2710
DBMS

IS 2150 Information
Security & Privacy

TEL 2821 Network
Security

(2 REQ)

IS2620
Dev Sec Systems

IS2731 Security
in E-Commerce

IS2810/TEL-2813
Security Mgmt &
Computer Forensics

TEL2825 Info.
Systems & Network
Infrastructure
Protection

Electives (6 Credits)

(REC)
IS2750
Cloud Computing

IS2625
Cybersecurity
& Privacy Regulation

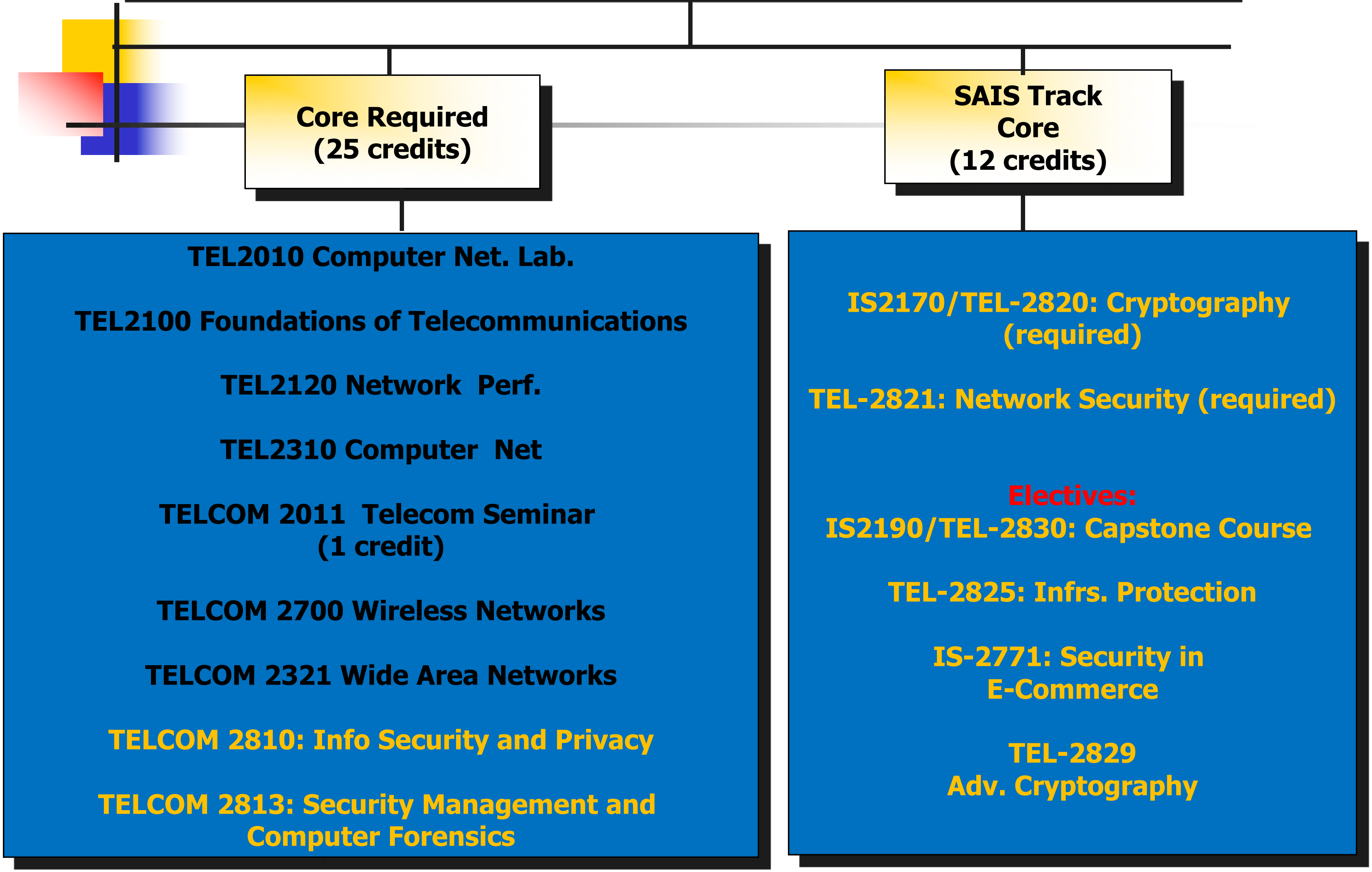
LIS 184 Legal Issues
in Info. Handling

IS2210 Information
Ethics
IS2629 Capstone

Other SAIS
courses

IS2610 Data Structure and TEL2000 are pre-requisites

MST
Security Assured Information Systems Track



Core Required
(25 credits)

TEL2010 Computer Net. Lab.

TEL2100 Foundations of Telecommunications

TEL2120 Network Perf.

TEL2310 Computer Net

TELCOM 2011 Telecom Seminar
(1 credit)

TELCOM 2700 Wireless Networks

TELCOM 2321 Wide Area Networks

TELCOM 2810: Info Security and Privacy

TELCOM 2813: Security Management and Computer Forensics

SAIS Track
Core
(12 credits)

IS2170/TEL-2820: Cryptography (required)

TEL-2821: Network Security (required)

Electives:

IS2190/TEL-2830: Capstone Course

TEL-2825: Infrs. Protection

IS-2771: Security in E-Commerce

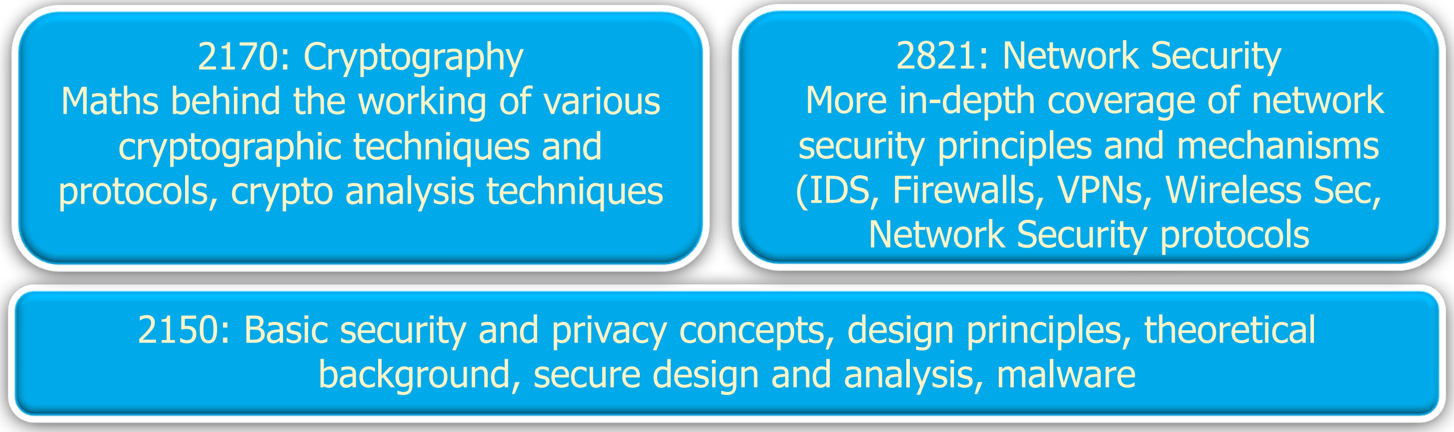
TEL-2829
Adv. Cryptography

SAIS CAS

- Core Courses

INFSCI 2150	Information Security and Privacy
INFSCI 2170	Cryptography
TELCOM 2821	Network Security

- Covers:
  - Online versions - the same as the physical class versions



2170: Cryptography
Maths behind the working of various cryptographic techniques and protocols, crypto analysis techniques

2821: Network Security
More in-depth coverage of network security principles and mechanisms (IDS, Firewalls, VPNs, Wireless Sec, Network Security protocols

2150: Basic security and privacy concepts, design principles, theoretical background, secure design and analysis, malware