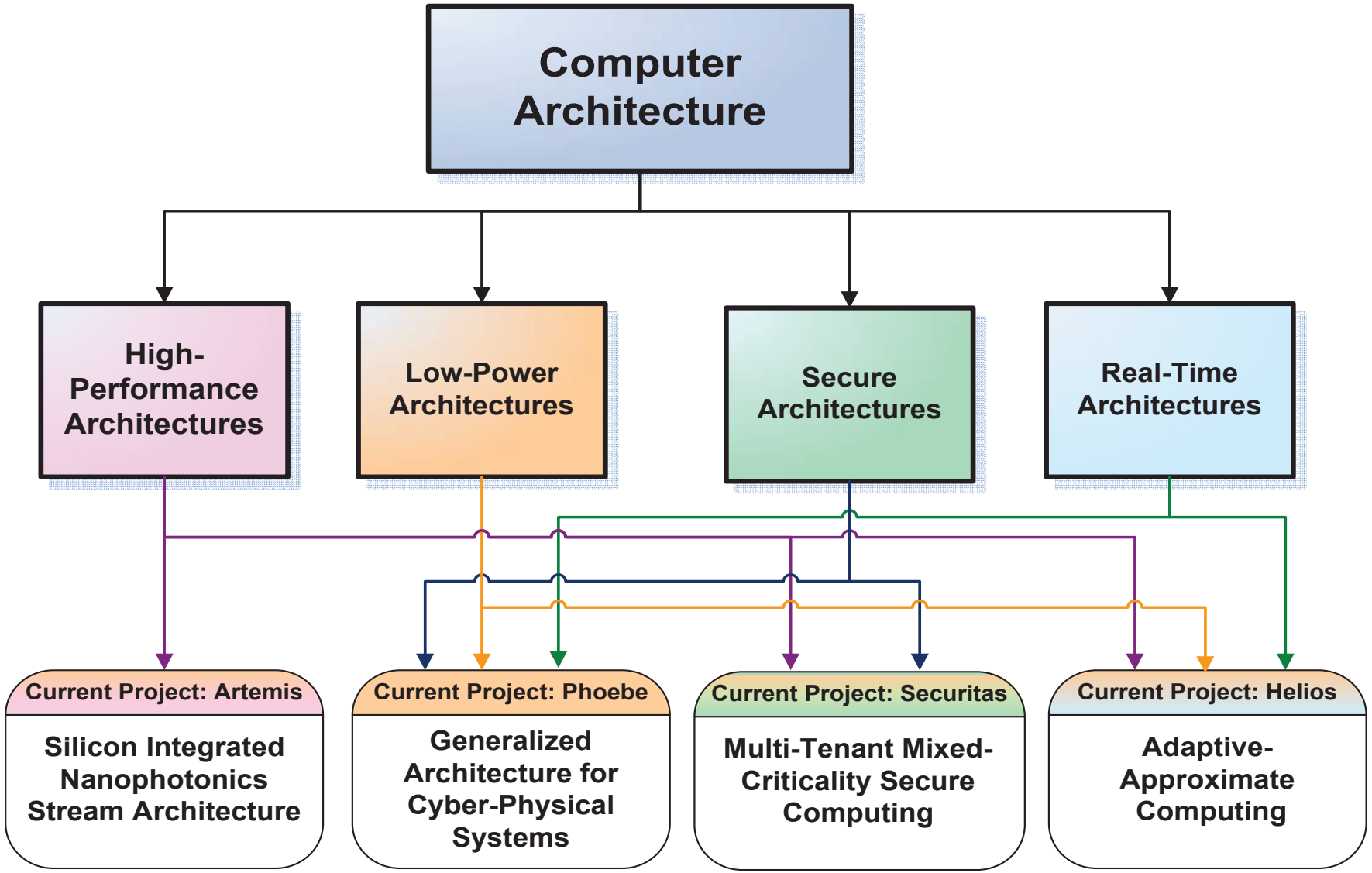
Introduction to Cybersecurity
A Software/Hardware Approach

Challenges & Opportunities

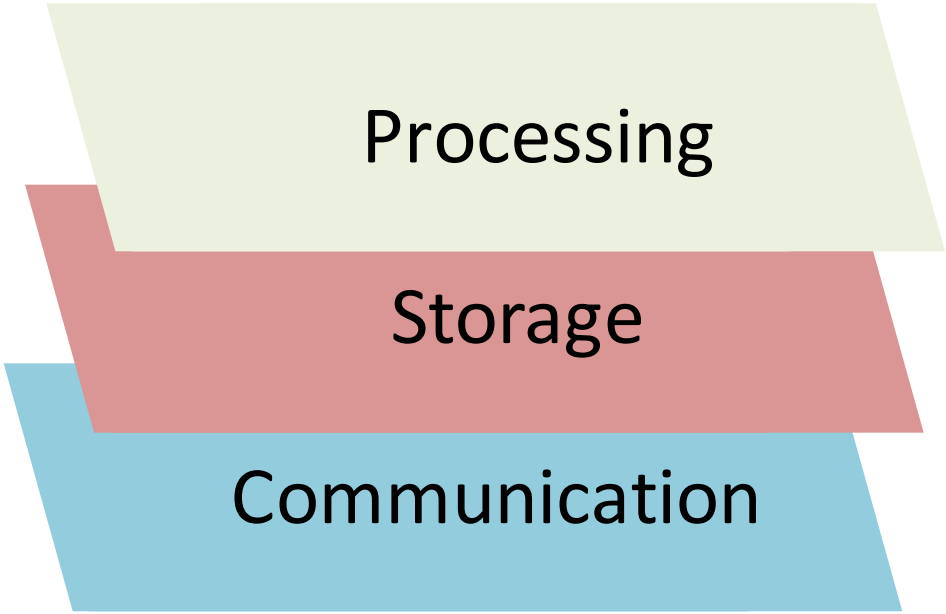
Prof. Michel A. Kinsy

BOSTON UNIVERSITY
Department of Electrical & Computer Engineering


Computer Architecture
High-Performance Architectures
Low-Power Architectures
Secure Architectures
Real-Time Architectures
Current Project: Artemis
Silicon Integrated Nanophotonics Stream Architecture
Current Project: Phoebe
Generalized Architecture for Cyber-Physical Systems
Current Project: Securitas
Multi-Tenant Mixed-Criticality Secure Computing
Current Project: Helios
Adaptive-Approximate Computing

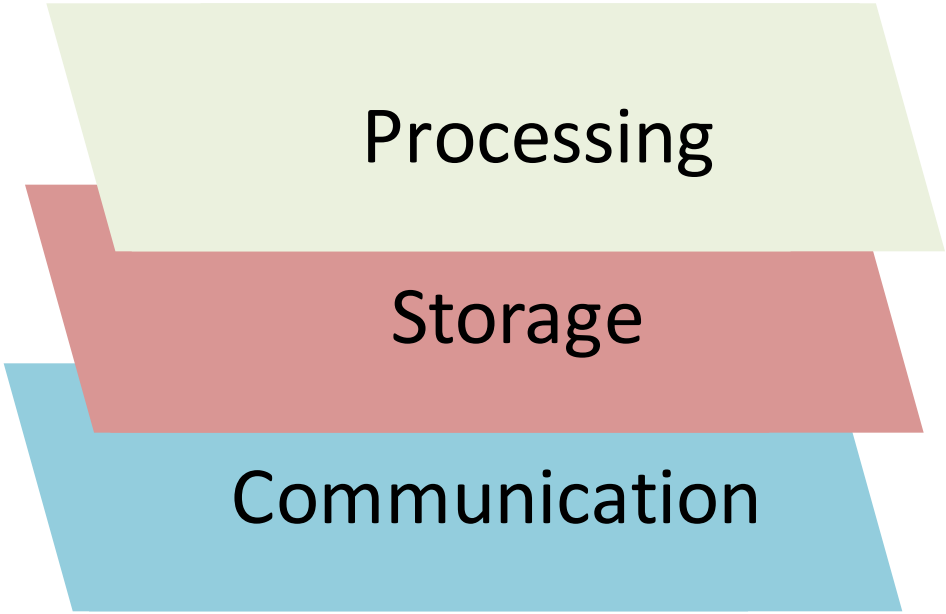
Computing Components

- Processing: Data creation/ manipulation/ transformation
  - Threads
  - Cores
  - Nodes
- Storage: Data at rest
  - Registers
  - Caches
  - Memories
  - Distributed storage
- Communication: Data in motion
  - On-chip
    - Buses
    - Network-on-Chips (NoCs)
  - Off-chip
    - Ethernet
    - High-bandwidth interconnect



Computing Components

- Processing: Data creation/ manipulation/ transformation
  - What we will cover in this course
    - Process Isolation
    - Core Isolation
    - Obfuscation
- Storage: Data at rest
  - What we will cover in this course
    - Access control
    - Integrity checking
    - Attack models
- Communication: Data in motion
  - What we will cover in this course
    - Data transition security through encryption and decryption
    - NoC based attacks



Large-Scale System Security Breaches

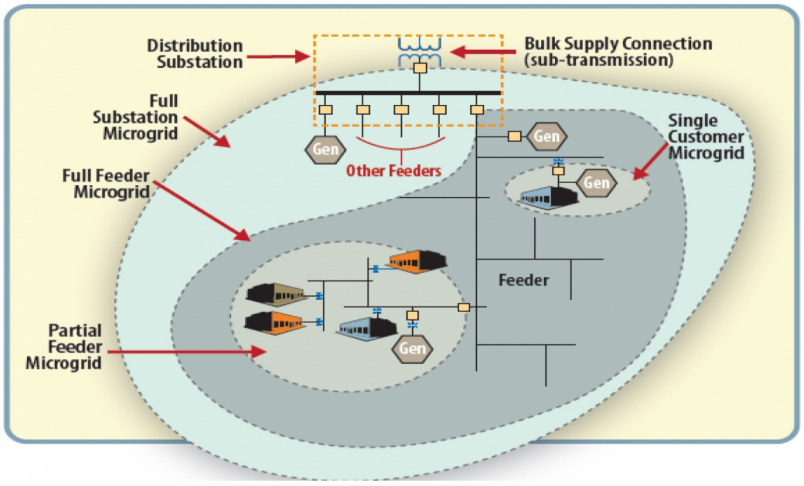
- The Emerging Mobile App "Wild West"
  - https://securityintelligence.com/how-to-protect-mobile-apps-essentials/
- Apple has now removed over 300 pieces of software from the App Store
  - http://www.wired.com/2015/09/apple-removes-300-infected-apps-app-store/
- Security researcher obtained physical access to the plane control system through the Seat Electronic Box
  - http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/
- Stuxnet computer worm is shown to work on Siemens SIMATIC WinCC SCADA system
  - http://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyberattack

Large-Scale System Security Breaches

- Home routers
  - Stealthy, destructive malware infects half a million routers https://www.wired.com/story/vpnfilter-router-malware-outbreak/
- Services sector: databases and data centers
  - Equifax breach of 145.5 million people's data
  - Yahoo hack that affected 3 billion accounts
  - Hospitals
    - https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
    - https://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it
- Fitness and wellness
  - Under Armour
    - https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/
- Internet of Things
  - World's largest DDoS attack launched from 152,000 hacked Smart Deviceshttps://thehackernews.com/2016/09/ddos-attack-iot.html
- 230 crypto keys are actively being used by more than 4 Million IoT devices
  - https://thehackernews.com/2015/11/iot-device-crypto-keys.html

Large-Scale System Security Breaches

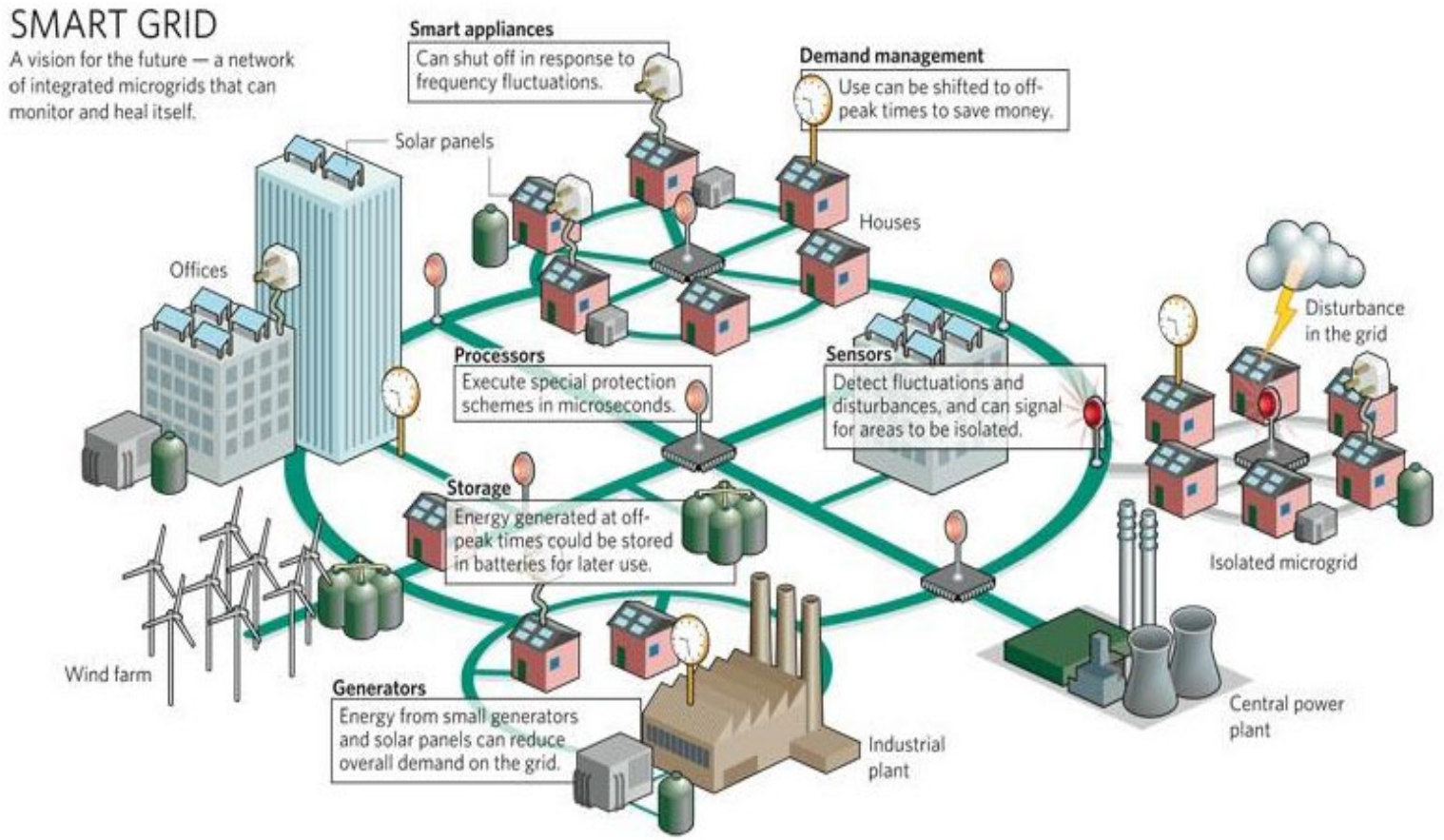
- Power grid systems: their control systems
- U.S. investigators find proof of cyberattack on Ukraine power grid
  - https://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/index.html



Source: U.S. Department of Energy

Example: Microgrids

An information-centric energy infrastructure: The Berkeley view



Source: http://www.energy-daily.com/images/smart-grid-electricity-schematic-bg.jpg.

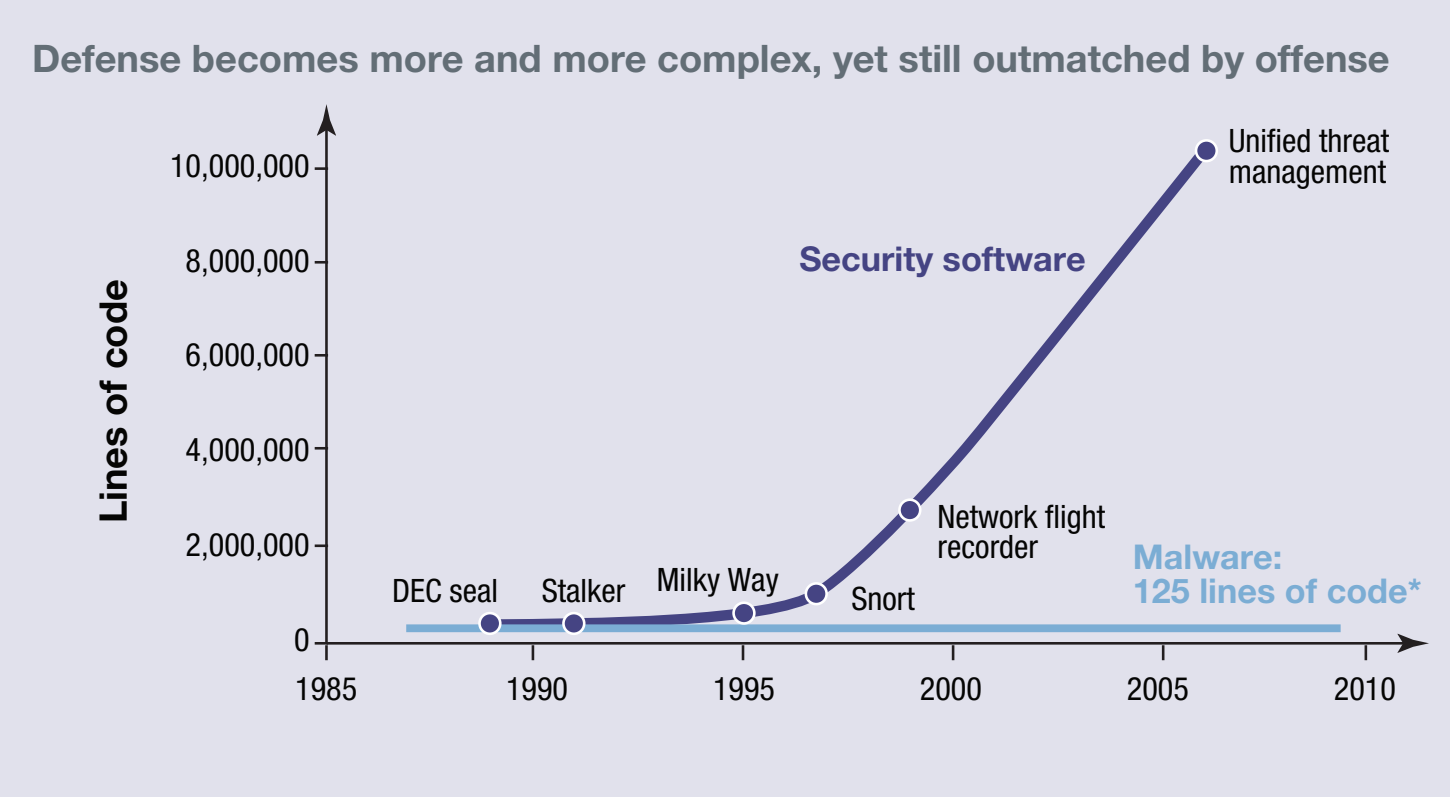
Example: Cybersecurity of Microgrids

- Computation requirements
  - The control systems deal with continuous, computational intensive dynamics, discrete events, and generic commands
    - Low and high-performance processing units required
  - The correctness, stability, and efficiency in controlling these system are closely related to the data propagation delay in the control (low-latency, and hard real-time)
    - Fast and predictable execution units are imperative
- Security requirements

Example: Cybersecurity of Microgrids

- Computation requirements
- Security requirements
  - Local control algorithms change over time, due to changes in the physical plant functions or capacity
    - Programmable architectures are required
  - The system wide control is a network of independent or loosely coupled local controls
    - Robust network security is needed
      - Firewalls, intrusion detection, deep packet sniffing, logging, unauthorized access monitoring, etc.

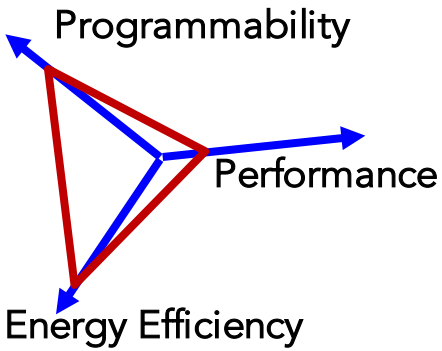
Why Hardware Level Security?



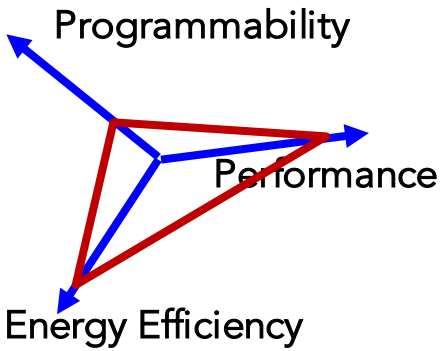
Source: Defense Advanced Research Projects Agency (DARPA) Brief to Defense Science Board (DSB) Task Force (May 2011). Data through 2010.

Architecture Design Challenge

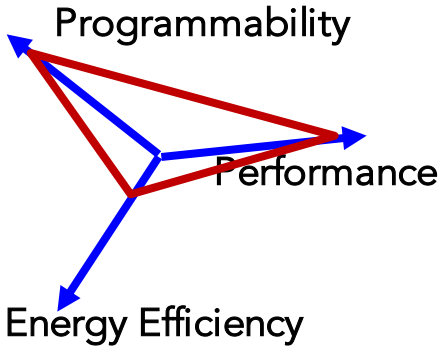
- Relatively easy to get two of three, harder to get all three!



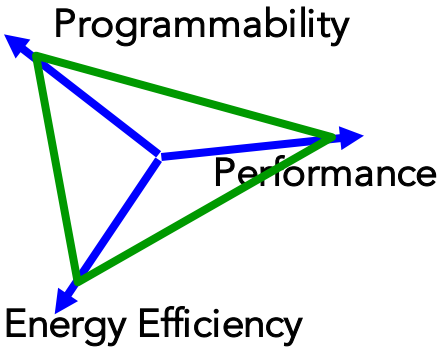
Uniprocessor



ASIC

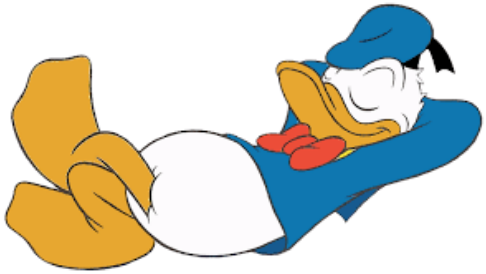


Superscalar



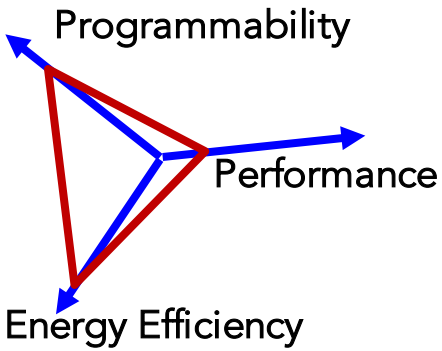
The general design objectives of the community have been:

- If only I could get all three!
- Image the future of computing!

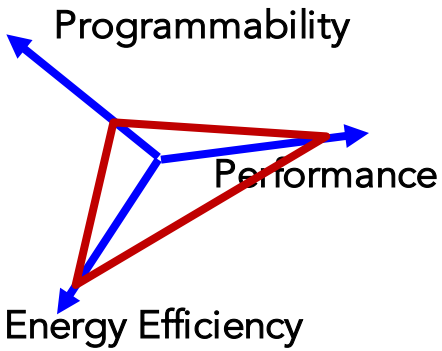


Architecture Design Challenge

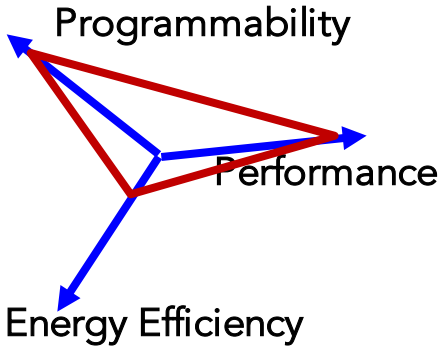
- Relatively easy to get two of three, harder to get all three!



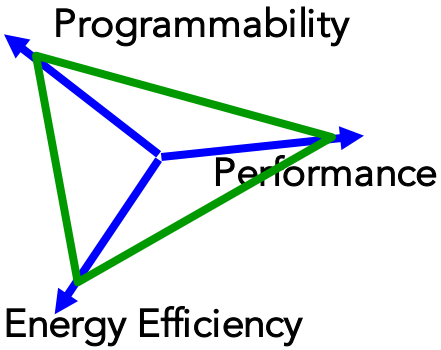
Uniprocessor



ASIC

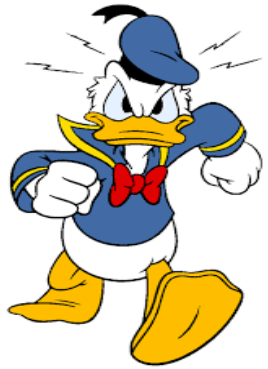


Superscalar



What about security?

- What about privacy-preserving computing?
- What about the integrity of the execution?
- On-chip data confidentiality?
  - Albert! You really know how to kill a party!!!



Computer Architecture Security

- The mainstream wake-up call
- Meltdown and Spectre
  - Meltdown security vulnerability allows a local, unprivileged, userspace process to read data from any memory location mapped to the process, including kernel memory
    - The key reason why this vulnerability is so terrifying
  - Spectre security vulnerability allows a local, unprivileged, userspace process to read data from memory locations assigned to other processes

In Class Activity

- Concept of Information Obfuscation
  - Problem statement
    - It has recently been shown that a robbers (aided perhaps by accomplices at the electricity company) can use victims' household electricity usage profile to determine if the victims are on vacation of not.
    - One such profile may look like this:

    - Our objective is to propose efficient solution for obfuscating the power usage profile.

Next Class

- Introduction to C/C++ and Computer Organization