Security Research at WPI

Presented at

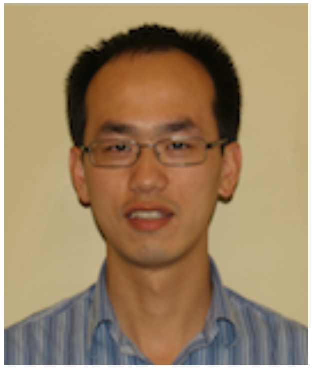
20 Years of Cryptography and Security at WPI

October 19, 2015

WPI Faculty in Security

Kathi Fisler (CS)

Thomas Eisenbarth (ECE)



Lifeng Lai (ECE)

Krishna (CS) Venkatasubramanian

Craig Shue (CS)

Berk Sunar (ECE)

Continued

Joshua Guttman
(CS)

Dan Dougherty
(CS)

Susan Landau
(CS)

Susan I. Mello-Stark
(CS)

William J. Martin
(Math)

Andrew Clark
(ECE)

Areas of Expertise

- Hardware security: Crypto accelerators, Side-channel attacks, Tamper-resilience, (Eisenbarth, Sunar)
- Privacy, cryptography policy: Cybersecurity policy, personal privacy (Landau)
- Access control: Access policies, formal verification (Dougherty, Guttman)
- Network security: Protecting enterprise servers, Geolocating targets, IP randomization (Shue)

Areas of Expertise (cont'd)

- Big Data Analysis: Anomaly/outlier detection, efficient information extraction (Lai, Paffenroth)
- CPS security: SmartGrid security, Security of medical devices, Wireless security (Venkatasubramian, Lai, Clark)
- Cloud security: Encrypted databases/file systems, leakage in VMs (Eisenbarth, Sunar, Shue)

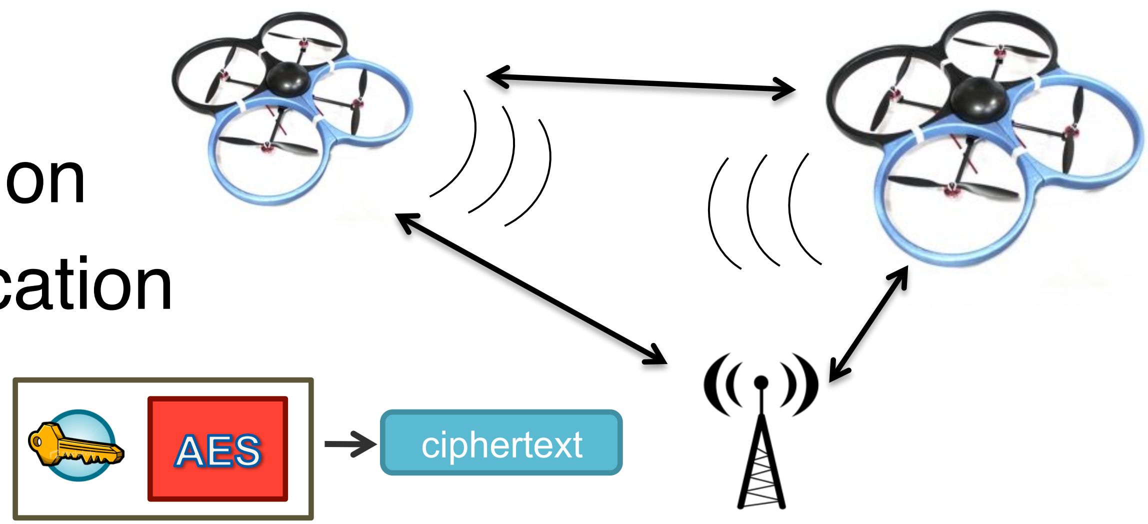
Research Interests- Thomas Eisenbarth

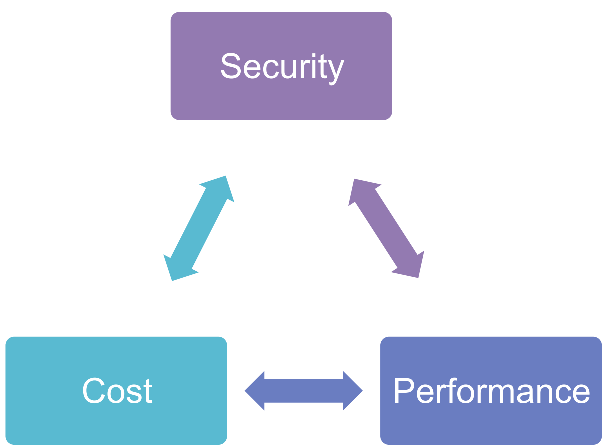
- Embedded systems security
- Side-channel analysis
- Attacks on implementation
- Embedded crypto implementation
- Cloud security

Embedded Security

Features:

- Entity authentication
- Secure communication
- IP Protection

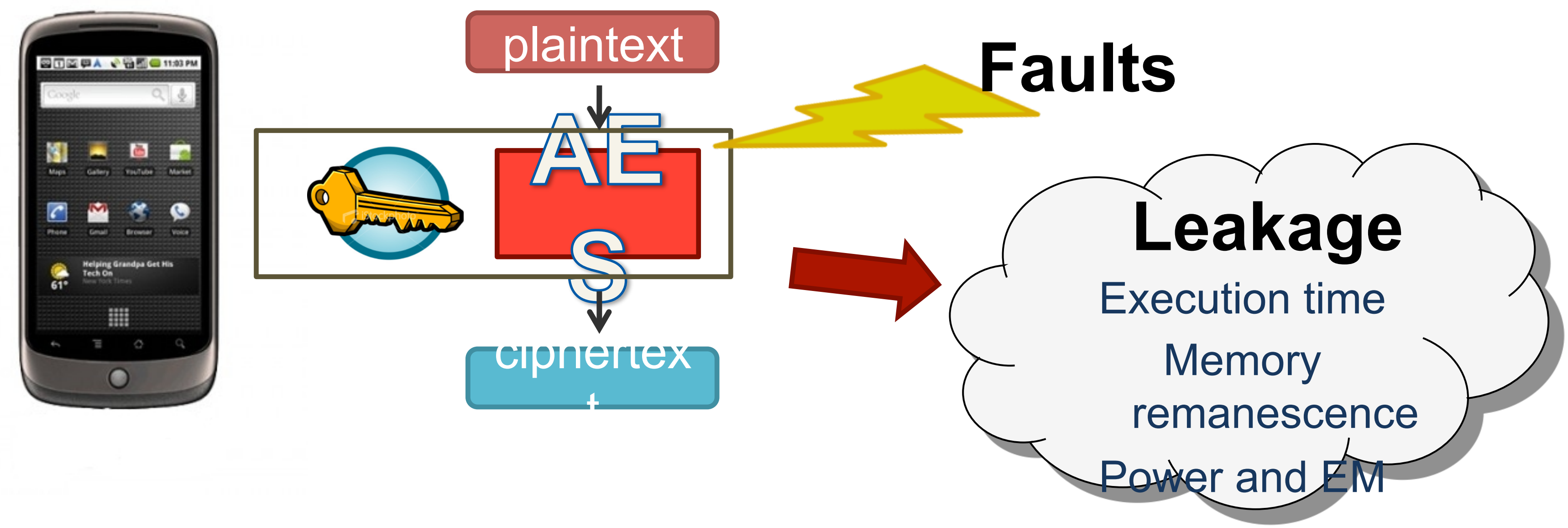




Challenges:

- Costly implementation
- Protocol weaknesses
- Physical attacks

Implementation Attacks



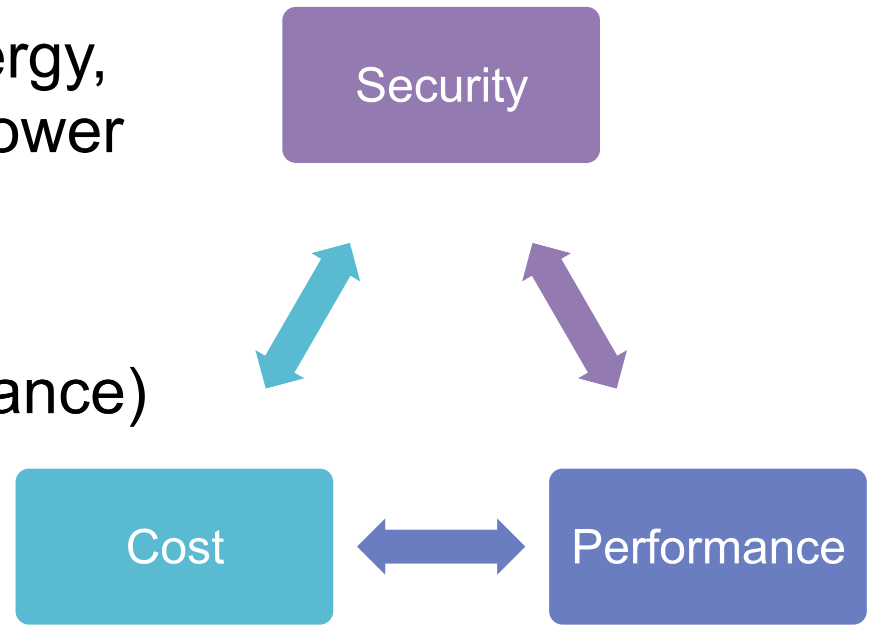
- Critical information leaked through side channels
- Adversary can extract critical secrets (keys etc.)
- Usually require physical access (proximity)

Embedded Crypto Implementations

Challenge: Constrains in Energy, Memory, and Computing Power

Tradeoffs:

- Public vs. secret key crypto (a factor of 1000 in performance)
- Lightweight crypto vs. standard ciphers



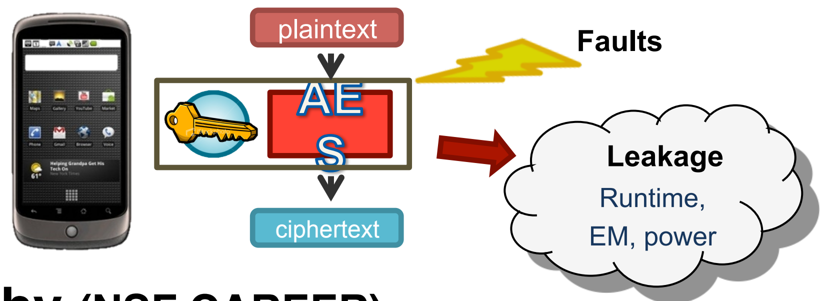
Current Research:

- Alternative crypto schemes → new services
- Countermeasures against implementation attacks and tampering
- Leakage resilient crypto cores

Current Research Projects

Interest: Applied Cryptography and Embedded System Security

- Building faster, smaller and cooler cryptosystems in HW + SW
- Breaking and protecting practical cryptosystems w/physical attacks



Project : Leakage Resilient Cryptography (NSF CAREER)

- Cryptographic primitives secure despite of side channel leakage
- Realistic assumptions & performance in software and hardware

Project : Statistics-based Framework for modeling SCA (NSF; w/NEU)

- Clean modeling of SCA and countermeasures→ predicting SCA

Project: Analyzing Information Leakage in the Cloud (NSF; w/ Sunar, WPI)

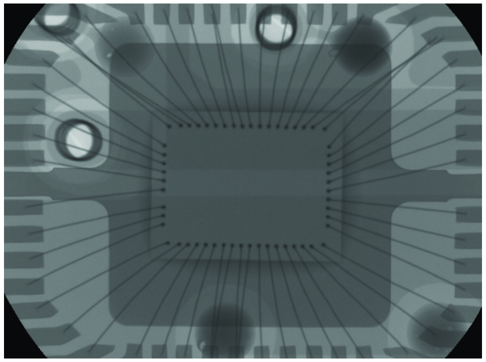
- Testbed for software side channel analysis in virtual machines/cloud

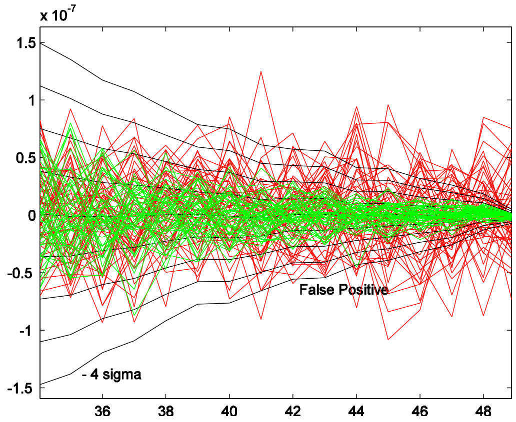
Research Interests – Berk Sunar

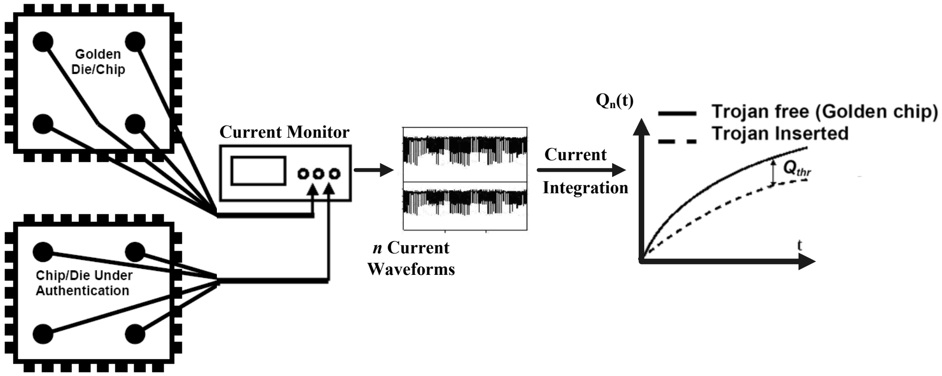
- Hardware Security
  - Cryptographic accelerators to eliminate performance bottlenecks
  - Low power, footprint, high speed
- Securing the IC Supply Chain
  - Physical unclonable functions (PUFs)
  - Tamper-resilience/identification
  - Trojan hardware and counterfeit detection

Counterfeit and Trojan Detection

- IC reverse engineering (2006)
  - E.g. ChipWorks delayering, X-ray/imaging
  - Expensive, does not scale
  - Useful for generating golden ICs
- IC Fingerprinting
  - Side-channel based (IBM/WPI 2007)
  - Transient analysis







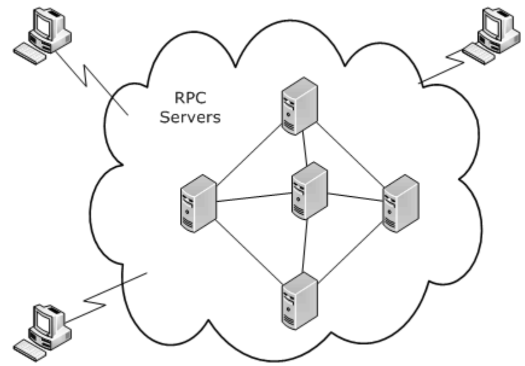
VERNAM Group
Security & Privacy @ WPI

Further Research Interests

- Secure computing and retrieval
  - Securing databases/files
  - Homomorphic encryption
  - Encrypted search
- Preventing info. leakage on the cloud
  - Cross VMM (Xen, VMware) Attacks
  - Popular crypto libraries:
    - OpenSSL, PGP/GPG, TLS, cryptlib, libgcrypt etc.
  - Stealing crypto keys from co-located guest OS's

Securing Distributed Applications

- More and more data is stored remotely on distributed systems & untrusted servers
  - E.g. Dropbox, PeopleSoft etc.
  - Web Mashups
- We don't even know where our data is stored or processed anymore



Sample Applications	Primary Need	Desired Operations
Medical Records, Financial Databases	Encrypted databases	SQL Ops: aggregation, averages, max, min
Media Servers	Encrypted cloud storages	Text search, replace
Access Protocols, DRM, eVoting	Blinded computations	Logic/arithmetic ops

"A distributed system is a system in which I can't get my work done because a computer has failed that I've never even heard of."
–Lamport

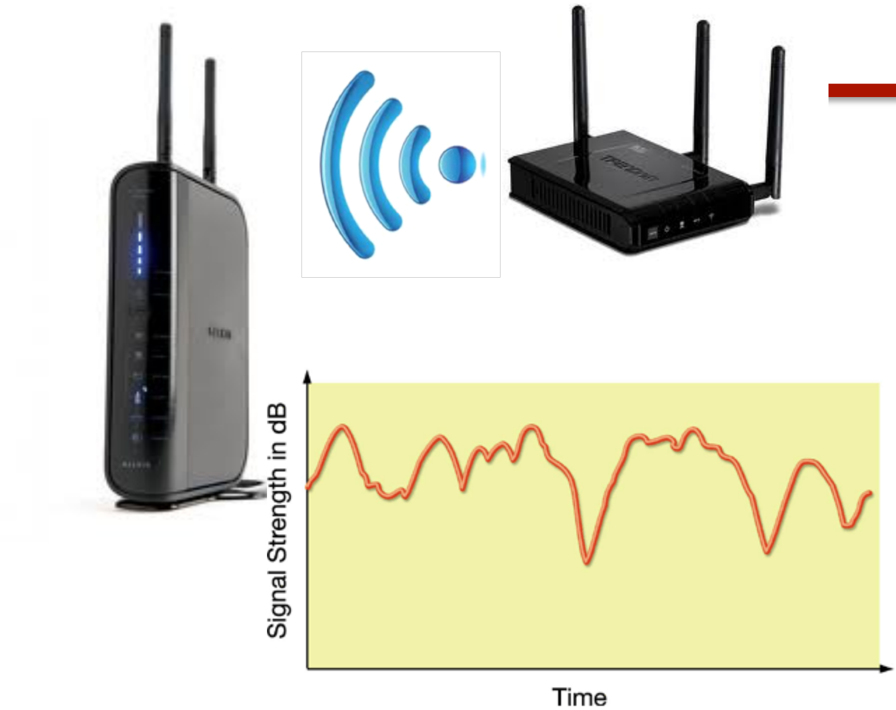
A Powerful Tool: Homomorphic Encryption

- Homomorphic Encryption
  - Allows computations on *encrypted data*
- Bottleneck: Efficiency
  - More efficient HE algorithms
  - Use hardware GPUs, FPGA/ASIC
  - Bring new algorithms under HE
    - Multimedimedia (Voice/audio) processing
    - Networking tasks (e.g. packet filtering, spam detection)
    - Financial transactions (blinded optimization/negotiation)

Research Interests:
Lifeng Lai's

- Secure wireless communications
- High dimensional signal processing and
- Inference with applications in security and other areas

Lifeng Lai's main research thrusts



Secure wireless communications

High dimensional signal processing and inference with applications in security and other areas

Research Sponsor

NSF

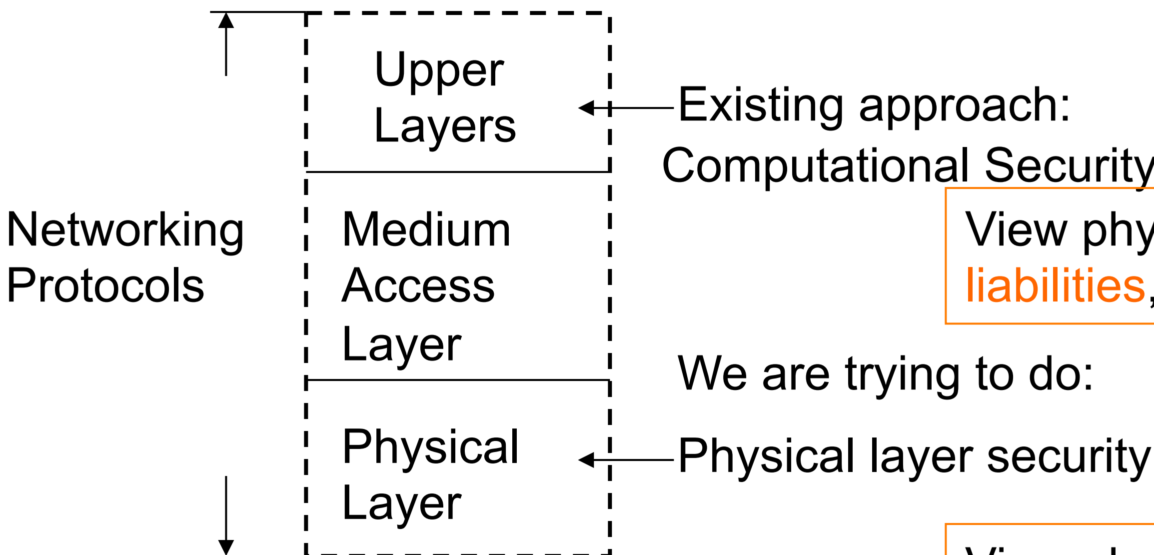
Qatar National Research Fund
Member of Qatar Foundation

Defense Threat Reduction Agency
United States of America

Air Force Research Laboratory

Secure Wireless Communications

How to secure sensitive information transmitted over wireless networks?



View physical layer phenomena as liabilities, and tries to overcome them

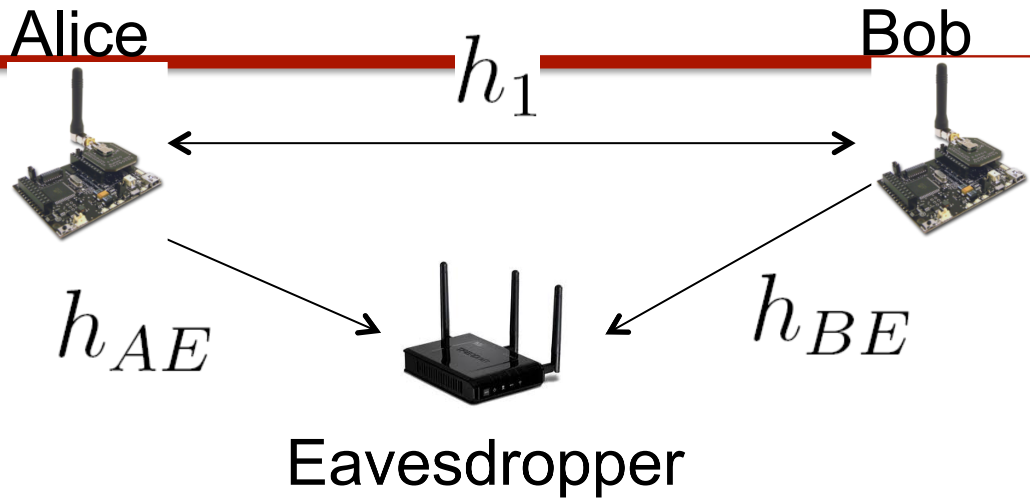
↓

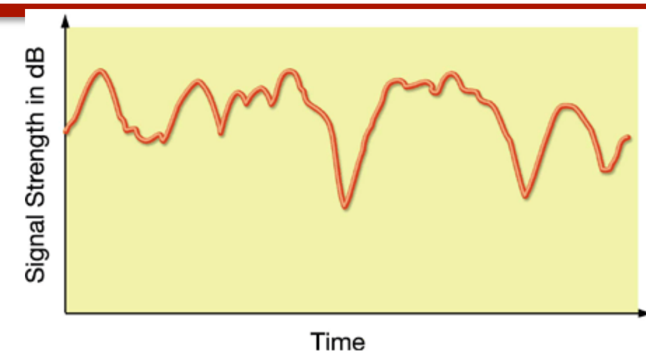
View physical layer phenomena as opportunities, and tries to exploit them

Topics:

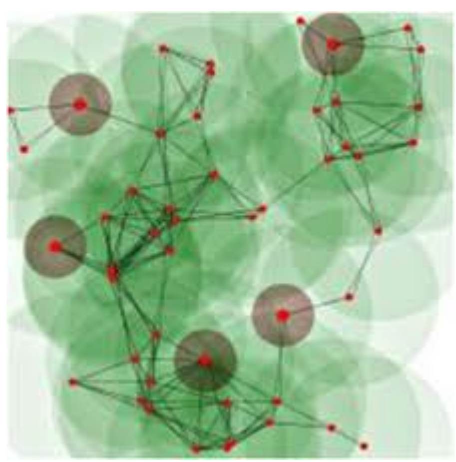
1. Secret key generation
2. Keyless secure wireless transmission
3. Applications in cyber physical systems such as networked control system, smart grid etc.

Online Secret Key Generation

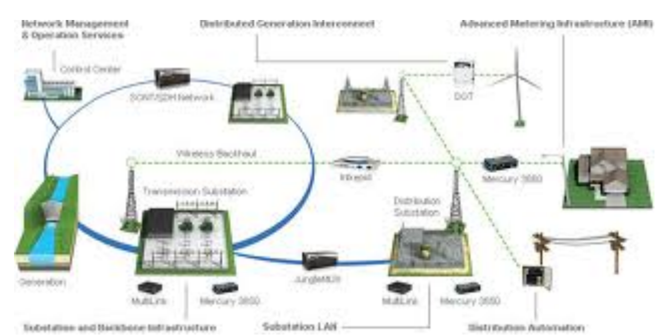




To exploit the time-varying channel as the common random source for the key generation

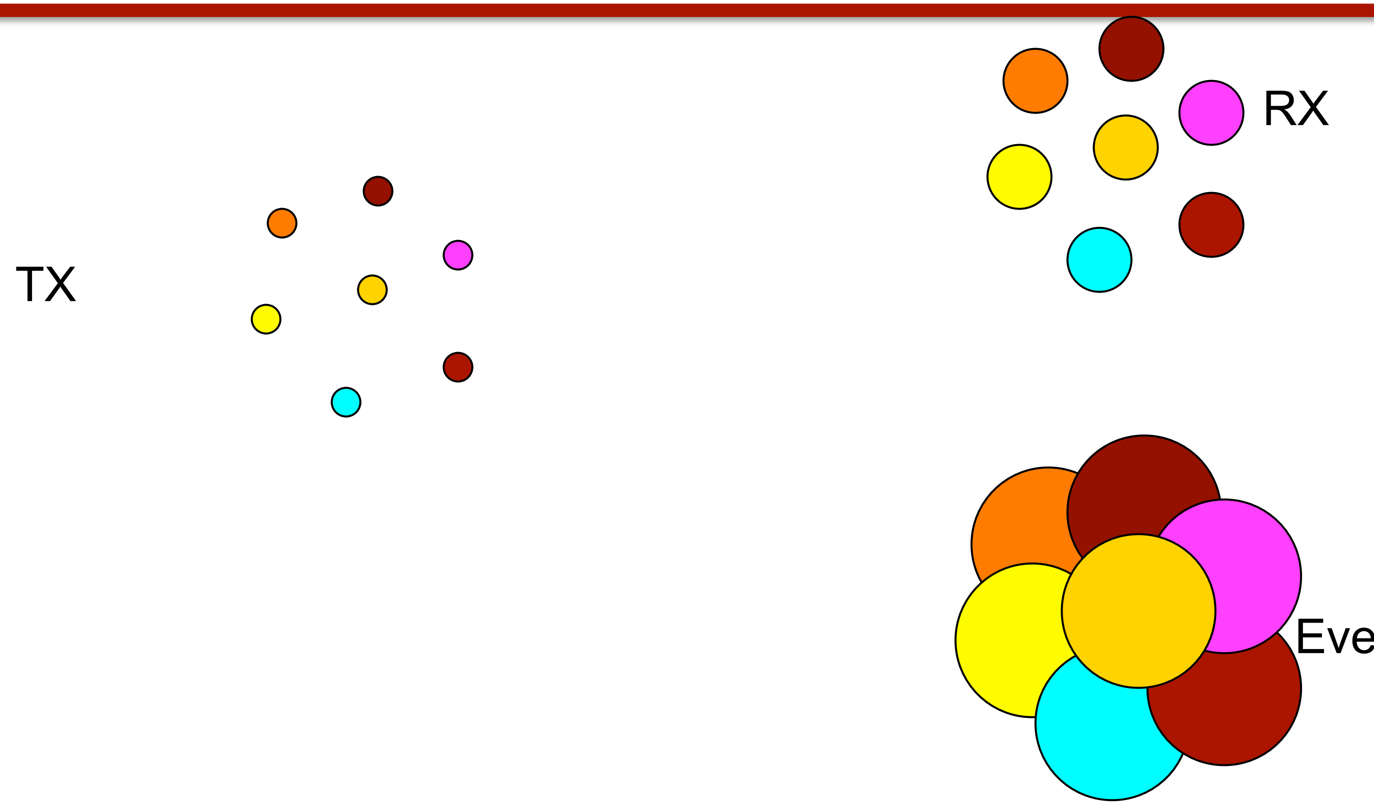


Large scale networks



Applications in Cyber-Physical Systems

Keyless Secure Wireless Transmission



Rx can decode message

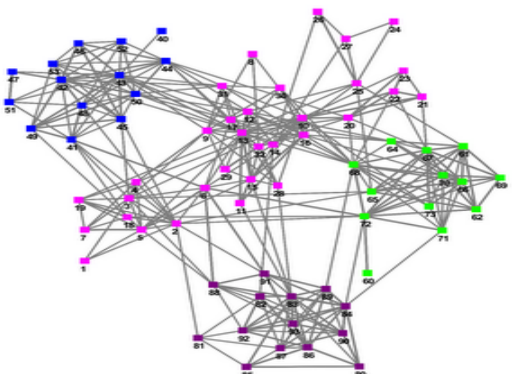
Attackers cannot decode because of noise

Utilize noise and fading to achieve secure transmission without any key

High Dimensional Signal Processing and Inference and Their Applications

How to extract useful information from huge amount of data quickly?

Applications:



Network attack detection

Chemical/biological/ nuclear attack detection

Structure monitoring

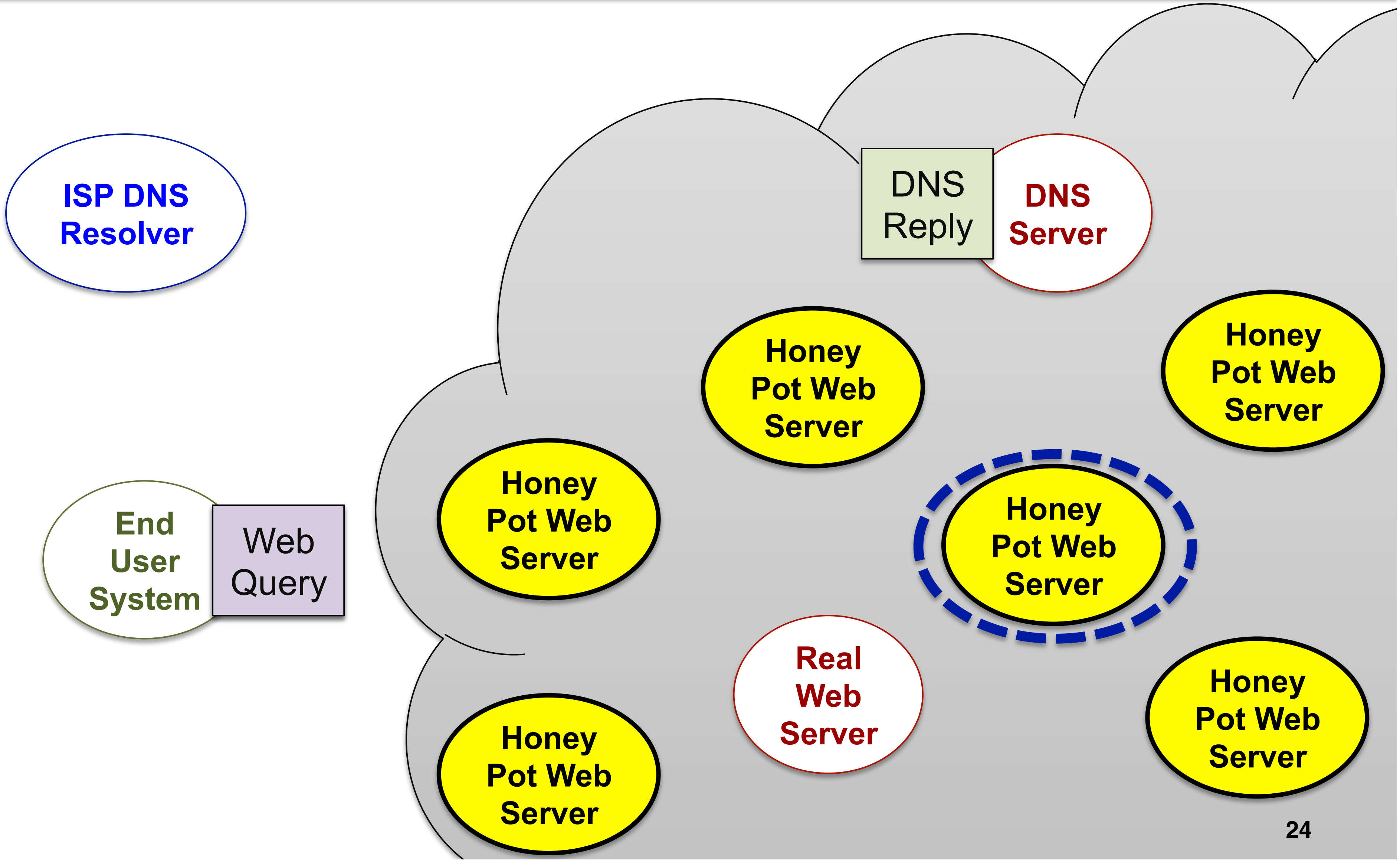
Research Interests – Craig Shue

- Computer Networking and Security
  - Internet-scale measurements
  - DNS infrastructure security
  - IP randomization for “Moving Targets” defenses
  - Precise physical geo-location from an IP address for law enforcement
- Operating and Distributed Systems
  - Virtualization and cloud systems for security

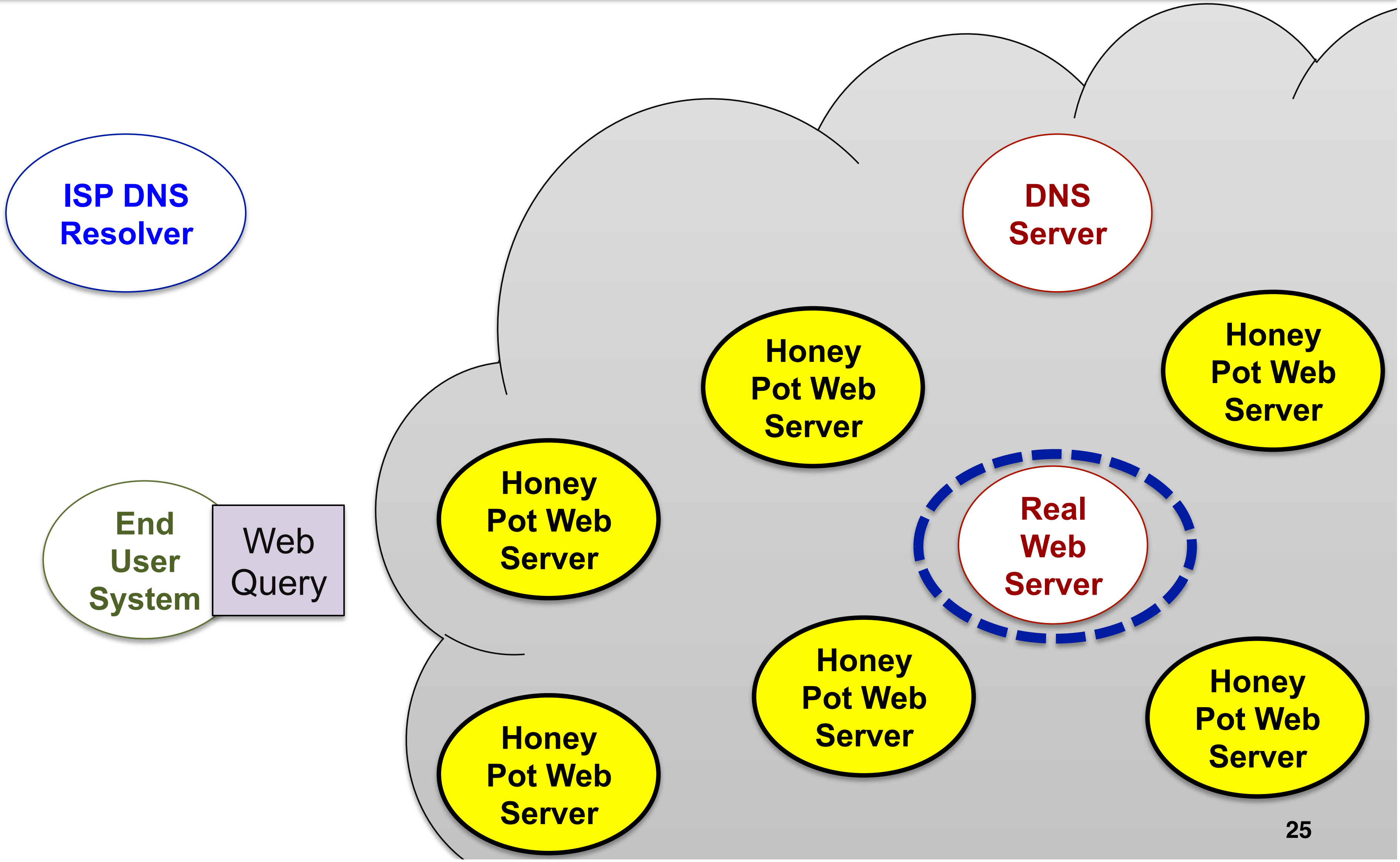
Protecting Enterprise Servers

- Servers are largely sitting ducks
  - Agile attackers, but servers static
  - Attackers can probe, discover network
- Organizations have limited tools to block malicious activity
  - Networks designed to allow communication
- Goal: create a gatekeeper
  - Use network to deny unwanted traffic
  - DNS can serve this function

Defending with Fast Flux IP Address Randomization



Defending with Fast Flux IP Address Randomization



Benefits

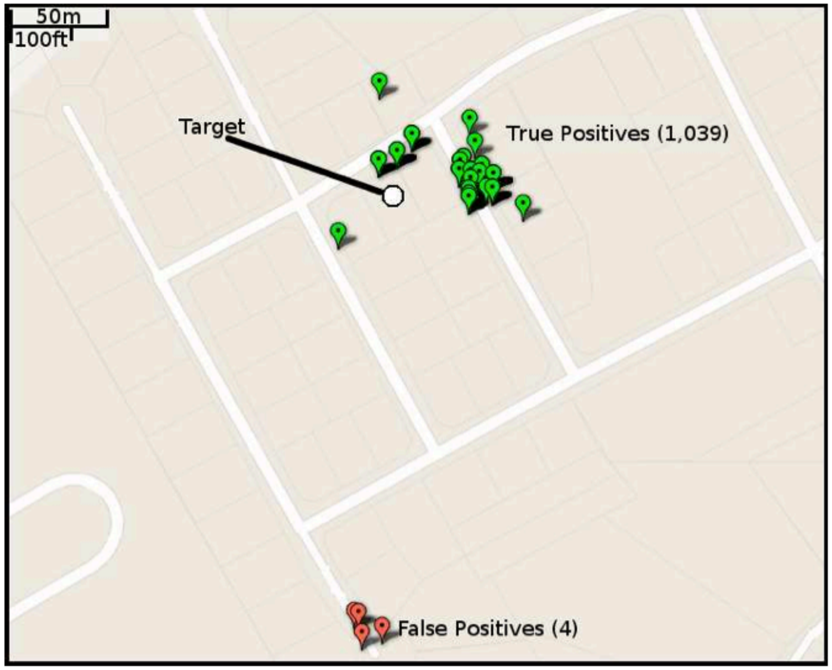
- Allows access control before connection
  - Allow, deny, or direct to honey pot
- Effectively blocks scanning/network discovery
- Extendable to allow source network filtering
- Implemented via NAT in iptables
  - Low overheads at DNS/iptables systems
- Next steps: selected for commercialization under DHS Transition to Practice Program

Geolocating Wireless Targets

- Geolocating Internet users common
  - Advertising, demographic studies, research
- Granularity: about neighborhood-scale
  - 690m radius circle using landmark latency
- A tighter granularity would be useful
  - Law enforcement bypassing ISP subpoenas
  - Prosecution of copyright infringement
- Research question: Can we locate a target user’s home?

Geolocating Target Machines

- Tested in Worcester
  - 35 minutes of driving
  - Only 4 false positives
  - Narrowed down to 3 houses
- Low bandwidth
- Resistant to countermeasures



Research Interests-
Krishna Venkatasubramanian

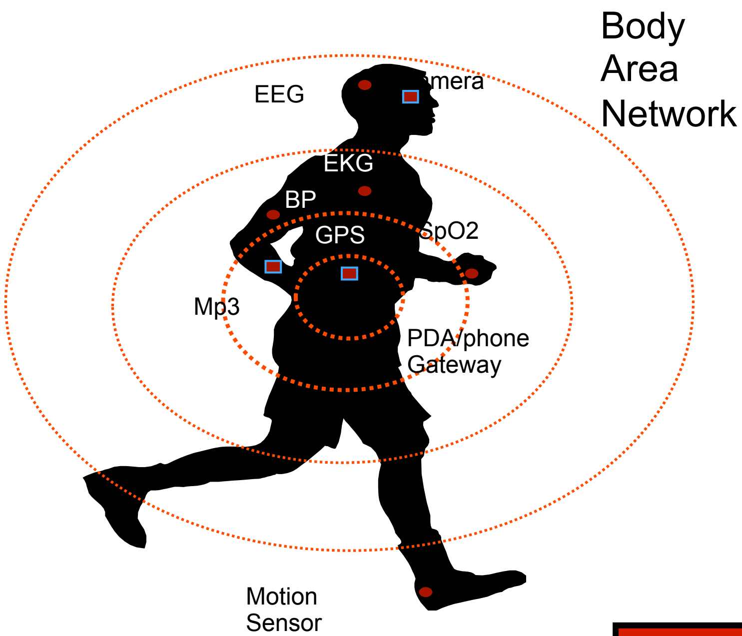
Secure Medical
Cyber-Physical Systems

Overview

- Medical Cyber Physical System Security
  - Environment-coupled Security for Body Area Networks
    - Transparent key distribution for information security
  - Secure Interoperability for Medical Devices
    - Analysis of information security threats on interoperability systems

Secure Body Area Networks

Body Area Networks: Tiny low-power networked sensing systems for monitoring health in a pervasive manner



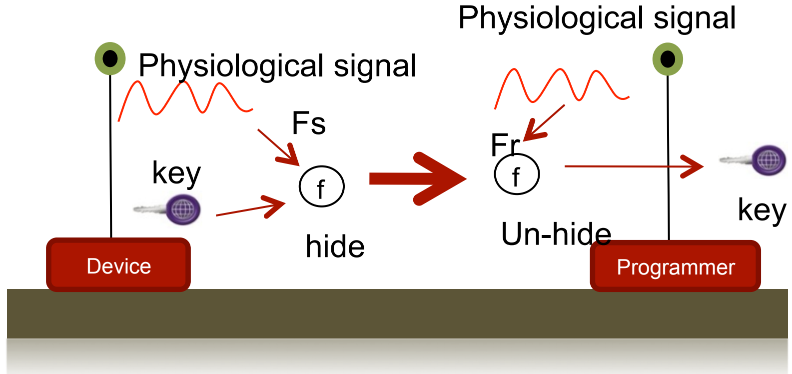
Features

- Wireless nodes with limited computation capabilities
- No time & space restrictions for health management
- Better quality of care
- Early detection/treatment of ailments
- Mission Critical: Ideal for emergency care

Security is essential for BANs because (1) sensitive information they collect and (2) potential harm they can cause by unauthorized acutation

Information Security: Physiological Signal based Key Agreement

- Uses commonly measured physiological signals for key agreement. Example
  - Photoplethysmogram (PPG)
  - Electrocardiogram (EKG)
- Two step process
  - Generate signal features at the sender and receiver (Fs and Fr)
  - Use Fs and Fr for secret key transport:
    - Generate a key at one sensor Hide it using Fs
    - Transport it to other sensor Unhide it at the Fr
- Benefits
  - Usability – no initialization/setup
  - Authenticated key distribution



- Extension
  - Enable BAN-to-Cloud Secure Communication
  - Use parameterized **generative models** of physiological signals to obtain features **at the receiver** and opening the the vault.

- K. K. Venkatasubramanian, Ayan Banerjee, and Sandeep K. S. Gupta, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", In IEEE Transactions on Information Technology in Biomedicine (Special Issue on Wireless Health), vol. 14 (1), Jan. 2010.
- A. Banerjee, S. K. S. Gupta, K. K. Venkatasubramanian, "PEES: Physiology-based End-to-End Security for mHealth", In Proc. 4th Annual Wireless Health Conference, Baltimore, MD,

Medical-Device Interoperability

Characteristics

- Medical devices gaining communication capabilities
- Devices still operate independently
- Standardized interaction between devices non existent
- Full benefit of communication capabilities not being realized

Current

Future

Advantages

- Improve Patient safety
- Safety interlocks
- Complete, accurate medical records
- Reduce errors
- Context awareness
- Rapid deployment

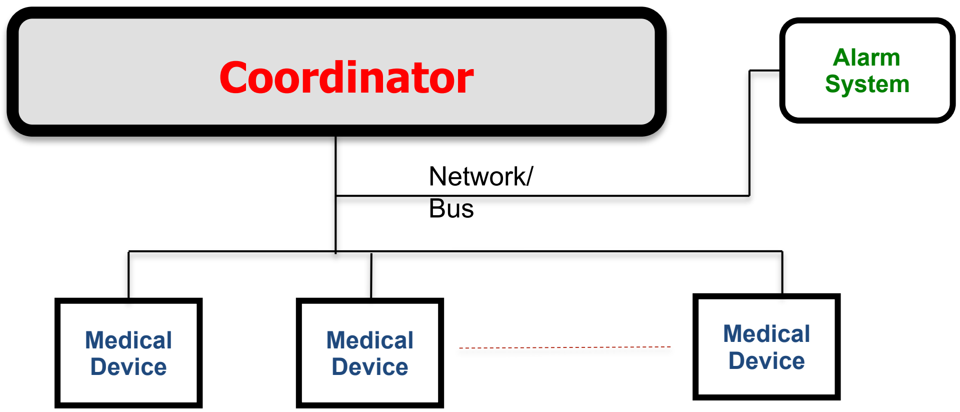
MD PnP: Interoperable medical devices based on plug-n-play!

Vendor neutrality based on open medical device interfaces

www.mdpnp.org

System Model for Medical Device Interoperability

- One Coordinator
  - For managing devices on a patients
- Multiple medical devices
  - Monitoring patient vital signs
  - Actuating treatment to patient
  - Devices have a “fail-safe” mode
- One Alarm System
  - For both medical and functional problems
  - Supervised by the Coordinator, but independent
- One Network/Bus
  - That interconnects the aforementioned entities
  - Could be wired or wireless



- Based on the ASTM Standard F2761-2009 called Integrated Clinical Environment.
- Defines a high-level architecture and functional concept