

Trends in Cyber Security at CSE@UB

Professor S. Upadhyaya

Department of Computer Science and Engineering
SUNY at Buffalo

Colloquium Talk
September 24, 2009



Outline

- Overview of Cyber Security Center at UB
 - Research and Education
- Motivation – Why Cyber Security?
- Types of Research Projects – Hot Topics



Acknowledgments

- Graduate students

- Sunu Mathew (Ph.D.)
- Duc Ha (Ph.D.)
- Madhu Chandrasekaran (Ph.D.)
- Mohit Virendra (Ph.D.)
- S. Vidyaraman (Ph.D.)
- Chris Crawford (MS)



- Colleagues

- Prof. Hung Ngo
- Dr. Kevin Kwiat



- Funding agencies

- NSA, NSF, DARPA



- Google Images

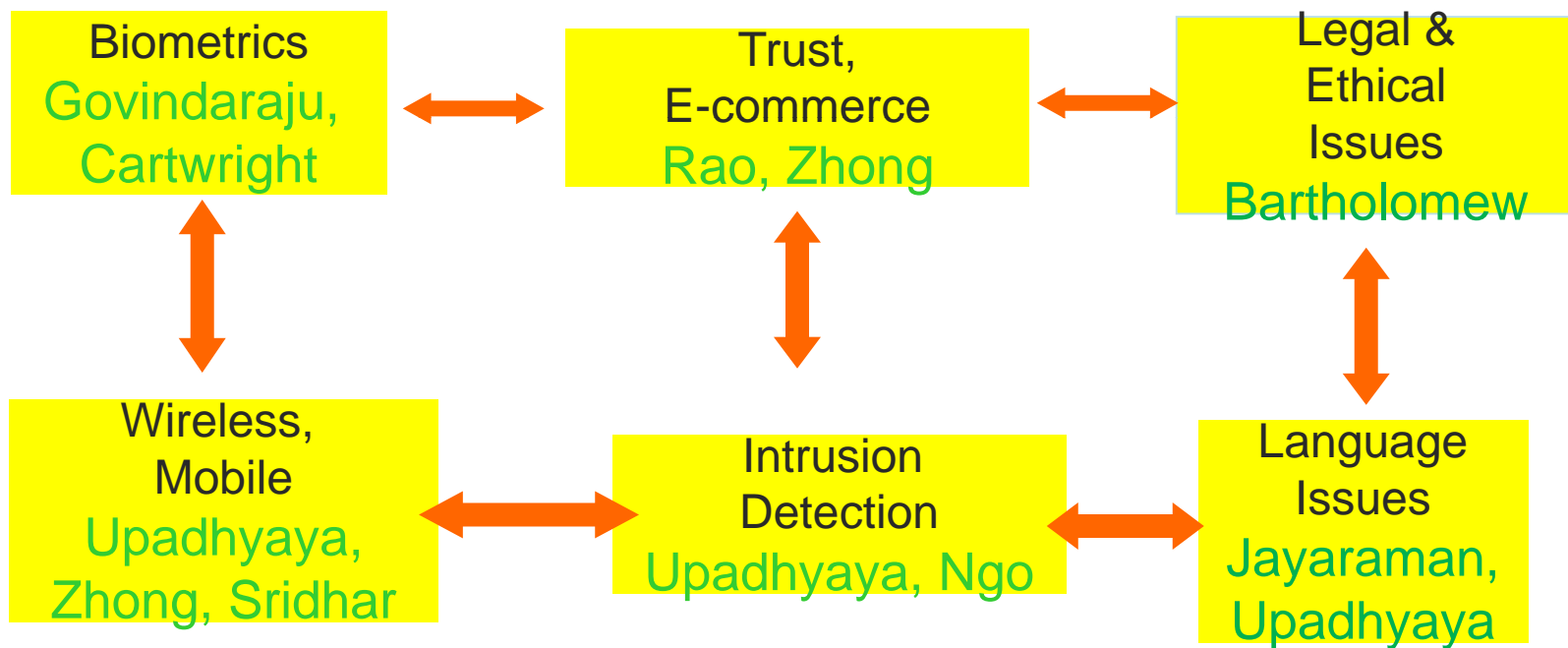


CEISARE

- CEISARE designated as a National Center of Excellence in 2002 by NSA, DHS
 - Through a competitive process
 - We were one of 13 centers designated that year (36 across the country)
 - Today, there are 100+ centers



IA Faculty Collaborators



Research & Other Synergistic Activities

- Funding
 - Over 4M from NSF, DARPA, NSA/ARDA, AFRL, DoD (since 2002)
 - Research, education, infrastructure
- Curriculum
 - Cyber security at Ph.D. level
 - Advanced Certificate in IA
 - IASP scholarships (DoD and NSF)
- Workshops
 - SKM 2004, SKM 2006, SKM 2008
 - Local Joint IA Awareness Workshops with FBI, ECC, Local industries
- Outreach Activities
 - High school workshops
 - Minority training



Graduate Certificate in IA

- Effort started with funds from DoD, 2003
 - Funding was to create a new integrative course in IA
- Two tracks – technical and managerial
- Requirements
 - 6 credits of core courses in the track
 - 5-6 credits of elective in the dept.
 - 3 credits of required integrative course
- Technical track
 - Core – Intro. to Crypto, Computer security, Wireless networks security (choose two courses)
- Managerial track
 - Core – Network management, E-Commerce security

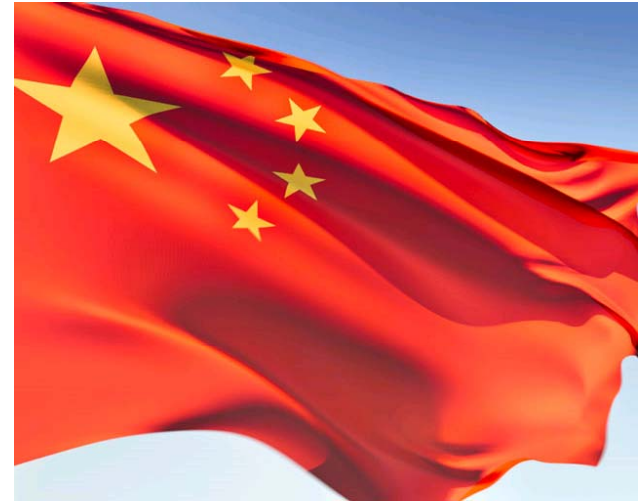


CEISARE Courses

- Courses with IA Content
 - CSE 565 Computer Security (currently teaching in fall 2009)
 - CSE 566 Wireless Networks Security (to be taught in spring 2010)
 - CSE 512 Applied Crypto and Computer Security
 - CSE 671 Security in Wireless Ad Hoc and Sensor Networks
 - LAW 629 Computers, Law, Technology and Society
 - LAW 645 Copyright
 - Law 956 E-Commerce Law
 - MGA 615 Fraud Examination
 - MGS 650 Information Assurance
 - MGS 651 Network Management
 - MGS 659 E-Commerce Security
 - MGT 681 Intellectual Property
 - MHI 512 Ethical, Social & Human Factors in Medical/Health Informatics
 - MTH 529/530 Introduction to the Theory of Numbers I/II
 - MTH 535 Introduction to Cryptography
 - MTH 567 Stream Ciphers
- Other Technical Electives
 - http://www.cse.buffalo.edu/caeia/advanced_certificate_program.htm



Computer Security Incident 1



Wall Street Journal, April 21, 2009

- Computer Spies Breach Pentagon's Fighter-Jet Project
- Hackers broke into DoD computers and downloaded terabytes of data containing design information about the Joint Strike Fighter, a \$300 billion stealth fighter currently under development



Computer Security Incident 2



Wall Street Journal, April 8, 2009

- Electricity Grid in U.S. Penetrated By Spies
- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials



Types of Attacks

- Threats to national security
- Cognitive hacking
 - Manipulating user's perception
 - “Killing” of Britney Spears (Oct. 2001)
- Worm attacks
 - Sasser Worm (May 2004)
- Virus attacks
 - SoBig.F (Aug. 2003), > \$50M damage
 - NIMDA virus in Sept. 2001
- DoS attacks
 - Yahoo, Amazon, eBay, CNN (Feb. 2000)
- SQL injection attacks
 - UN Website defacing (8/12/07)



Cognitive Hacking

- On Oct. 7, 2001, CNN's top-ranked news story
- Example of a cognitive hacking where you manipulate a user's perception
- These attacks are "hoax" like hoax Virus notifications
- Refer to: IEEE Computer, August 2002 issue:
 - <http://computer.org/computer/co2002/r8toc.htm>
- It began with a spoof of CNN.com
- Through a bug in CNN's software, the article got spread when clicked on "email this article"
- Within 12 hours, more than 150,000 people viewed the spoofed page



Phishing Attacks

The screenshot shows an email titled "UPDATE YOUR PAYPAL ACCOUNT" in the Thunderbird interface. The email header includes a warning: "Thunderbird thinks this message might be an email scam." The header fields are: Subject: UPDATE YOUR PAYPAL ACCOUNT; From: security@paypal.com <account@paypal.com> (highlighted in red); Reply-To: security@paypal.com <security@paypal.com> (highlighted in red); Date: 02/19/2006 02:58 PM; To: kr45@cse.Buffalo.EDU, mtaneja@cse.Buffalo.EDU, mhwora@cse.Buffalo.EDU, mc79@cse.Buffalo.EDU (highlighted in red). The body of the email starts with "Dear Sir," (highlighted in red) and contains a message from the "PayPal Account Review Department" explaining account limitations and providing a link to "http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/accounts-outside" (highlighted in red). The email ends with "Sincerely, PayPal Account Review Department" and "PayPal Email ID PP576". Annotations in pink boxes point to various parts of the email: "Purported sender:" points to the From and Reply-To fields; "Sent to multiple users (4 users in the To: field)" points to the To field; "False emotion: The message body invokes a false sense of fear and concern in the users to immediately disclose their critical information in spoofed website to avoid account revocation" points to the main body text; "Mismatched visible and hidden URL" points to the link, with the visible URL being "http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/accounts-outside" and the hidden URL being "http://ns.softispb.ru/.us/webscr.php?cmd=Login".

UPDATE YOUR PAYPAL ACCOUNT - Thunderbird

Thunderbird thinks this message might be an email scam.

Subject: UPDATE YOUR PAYPAL ACCOUNT

From: security@paypal.com <account@paypal.com>

Reply-To: security@paypal.com <security@paypal.com>

Date: 02/19/2006 02:58 PM

To: kr45@cse.Buffalo.EDU, mtaneja@cse.Buffalo.EDU, mhwora@cse.Buffalo.EDU, mc79@cse.Buffalo.EDU

Dear Sir,

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. This is a fraud prevention measure meant to ensure that your account is not compromised.

In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason:

We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive PayPal account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

Case ID Number: PP-046-631-789
We encourage you to log in and restore full access as soon as possible. Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account or may result in eventual account closure.

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.

To keep your account active, click here:
<http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/accounts-outside>

Sincerely,
PayPal Account Review Department

PayPal Email ID PP576

Purported sender:
From: security@paypal.com <account@paypal.com>
Reply-To: security@paypal.com <security@paypal.com>

Sent to multiple users (4 users in the To: field)

False emotion:
The message body invokes a false sense of fear and concern in the users to immediately disclose their critical information in spoofed website to avoid account revocation

Mismatched visible and hidden URL
Visible URL: http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/accounts-outside
Hidden URL: http://ns.softispb.ru/.us/webscr.php?cmd=Login

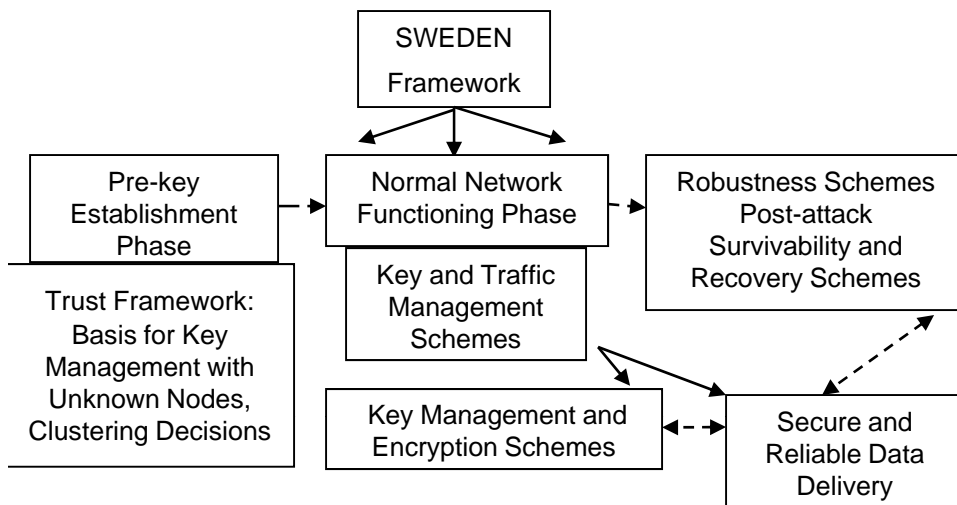


Research Projects

- Most federally funded
- Some industry funded
- Disciplines ranging from Systems Security to Networks Security



SWEDEN: A New Framework for Secure and Trusted Communications in Wireless Data Networks, Shambhu Upadhyaya, Funded by AFRL, NSF/Cisco, 2004-09



Goals

- Design decision making framework for nodes to establish keys with other unknown nodes
- Use this framework for cluster forming decisions in ad-hoc networks
- Improve on existing key management schemes and design secure data delivery schemes for enhanced reliability in data transfer
- Provide schemes for resiliency against attacks and post-failure recovery

Novel Ideas

- Trust between the nodes used as a metric for decision making
- Differential encryption (header and payload differently) scheme for ad-hoc networks, and hashing based lightweight techniques for sensor networks
- Evaluating security of paths and nodes based on their relative position in the network
- Building in survivability in the network architecture proactively for surviving potential attacks
- **Robustness, Recovery and Survivability Schemes**

Accomplishments

- ❑ **Setting up of the NSF and Cisco sponsored Wireless Security Lab**
- ❑ **Representative Publications:**
 - ❑ IEEE Conference on Local Computer Networks (LCN), Tampa, FL, Nov 2004
 - ❑ IEEE ACM IWIA, College Park, MD, Mar 2005
 - ❑ IEEE Conference on Knowledge Intensive Multi-agent Systems (KIMAS), Boston, MA, Apr 2005
 - ❑ Secure Knowledge Management (SKM), Sep 2004
 - ❑ MMM 2007, St. Petersburg, 2007
- ❑ **Future Plans**
 - ❑ Security Schemes for mesh networks
 - ❑ Performing hands-on experiments at the Wireless Security Lab



Impact

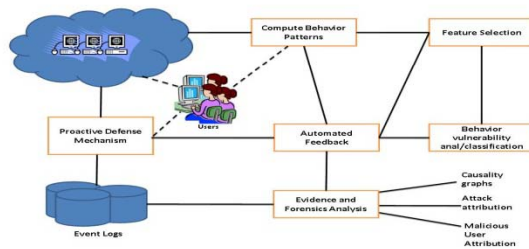
- Graduate Students
 - M. Virendra (Ph.D., June 2008), M. Jadliwala (Sept. 2009), Ameya Sanzgiri (stated June 2009), Chris Crawford (M.S., June 2009)
- Publications
 - KIMAS 2005, SKM 2006, IEEE ICC 2007, MMM-ACNS 2007, IEEE SRDS 2007, Infocom 2008, WiSec 2009
- Funding Agency
 - Air Force Research Laboratory (2007-09)



Objective

A unified behavior based framework for mitigating threats and damaging attacks on the Internet

- Address phishing, zero-day exploits, spyware, email authorship attribution, information leak in documents
- Hardware acceleration to support scalability



The approach

- Behavior Capture and Analysis (feature selection, simulated annealing)
- Behavior Based Monitoring and Detection (support vector machines)
- Attack Attribution and Forensics (causality graphs)
- Attack-Agnostic Framework (component based approach, implementing theories in hardware on modern CPUs)
- Validation (user studies)

State of the art in the area

- Malware on the Internet is rampant
- Behavior-based defense used successfully in real-world
- Extended to cyber-world by researchers at Columbia U.
- Behavior capture and correlation of applications using programming languages
- Behavior based monitoring for attack detection using statistical and rule-based algorithms
- Behavior based techniques for network forensics using causality graphs
- Designing new hardware for content processing and cryptography

Novel ideas

- Attack-agnostic framework to address all facets of security
 - attack protection, detection, response and forensics
- A holistic approach
- Proof-of-concept prototypes for anti-phishing, handling zero-day exploits, malicious email attribution, anti-spyware, information leak detection
- Hardware acceleration techniques to handle “pump and dump” malware
 - Grounded in theory and preliminary investigation
 - “Spycon: Emulating user activities to detect evasive Spyware”, IEEE Malware 2007 (Best paper award)



Impact

- Graduate Students
 - M. Chandrasekaran (Ph.D., June 2009), N. Pulera (M.S., June 2008), H. Alkebulan, (M.S., Dec. 2008), N. Campbell (B.S., Dec. 2008)
- Publications
 - Ubisafe 2006, Malware 2007 (Best Paper Award), Albany IA Conference 2007, 2008
- Funding Agency
 - DoD (2007-08)



Accelerating Techniques for Rapid Mitigation of Phishing and Spam Emails

- Phishing scams pose a serious threat to end-users and commercial institutions
- Current software based solutions cannot be implemented on end-user's local computers due to the computation overhead involved with the associated feature selection and data mining algorithms
- We aim at detecting phishing attacks based on the **semantic and structural properties** present in the **content of the phishing emails** at the end-user level
- **Our solution is hardware based**
 - We are implementing some basic theories such as Simulated Annealing, Bayesian Learning, and Associative Rule Mining in the hardware
 - Exploit the inbuilt pipelining, scheduling and other accelerator capabilities and the micro engines of the Intel Tolapai processor

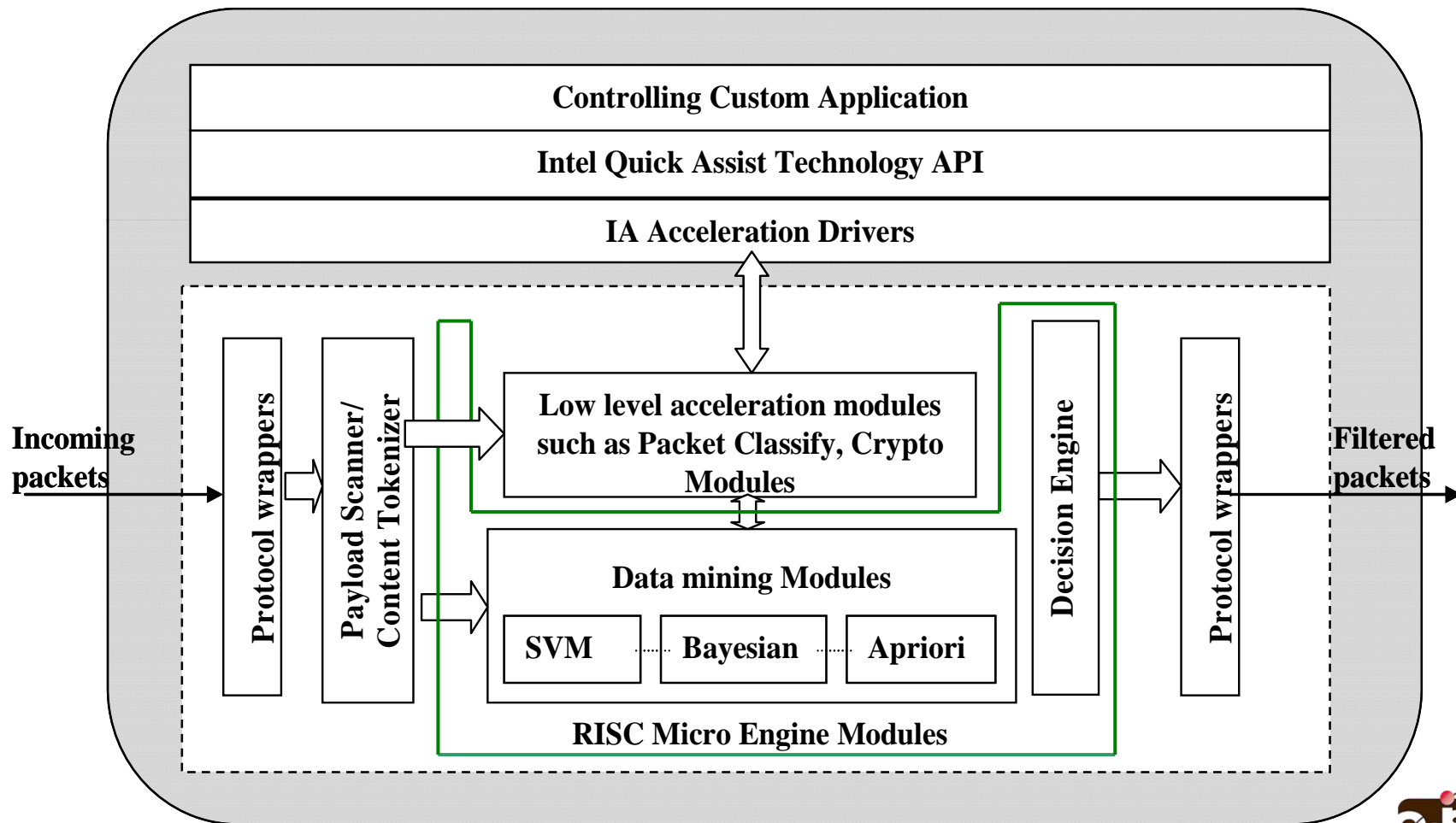


Impact

- Graduate Students
 - M. Chandrasekaran (Ph.D., June 2009), Ajay Nagrale (M.S., June 2010), Pranil Gupta (M.S., June 2010)
- Publications
 - Intel Summit, Feb. 2009
- Funding Agency
 - Intel Corporation (2008-10)



Integrating with Tolapai



Hot Topics in Security

- Design for Information Security
- Writing Secure Code
- Phishing Prevention (Using Machine Learning Algo.)
- Sensor Networks Security
 - U.S. President Obama calls for installation of 40 million smart meters for better management of electricity and energy (Smart meters use WSN technology)
- Trust, Privacy, Healthcare
- Useful sites
 - SANS Institute
 - SecurityFocus
 - DHS – US-CERT (US Computer Emergency Readiness Team)

