Security and Privacy in Smart-Grids: Challenges and Issues

RK Shyamasundar

Indian Institute of Technology, Bombay

rkss@cse.iitb.ac.in

The Distinguished Speakers Program is made possible by

Association for
Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/

About ACM

ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence.

ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

With over 100,000 members from over 100 countries, ACM works to advance computing as a science and a profession. www.acm.org

Agenda

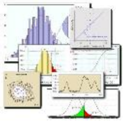
- Securing SCADA
- Stuxnet- A complex malware with Nation-State Support
  - Cyberwar
- SCADA in Electric Grid
- Smart Grid
  - Security and Privacy Challenges
- Summary

Computing for Societal Impact

Cloud computing infrastructure

Robust computing at low-cost , “pay-as-you-go”

- **Analysis**



- **Integration**

- **HMI**

Assuring security and safety of the nations

Global vigilance and Reach

Large volume of data

Phones, Sensors

Smart cars

Intelligent Eco Systems:

Trustworthy, Cost effective

Environment friendly

Benefits to individuals & society

Modern health care

Adaptive Power Grid

Efficient transportation (air, ground, sea)

Preservation of water

New age agriculture

Individuals & enterprises

Human expertise

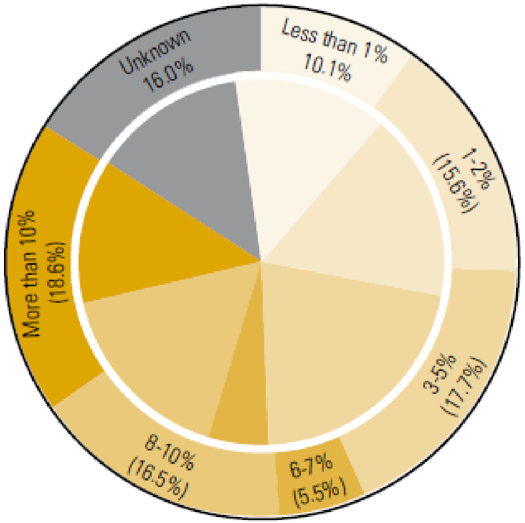
Innovations

Education

Research

Percentage of IT Budget Spent on Security

2010 Figures on Outside, 2009 Figures on Inside

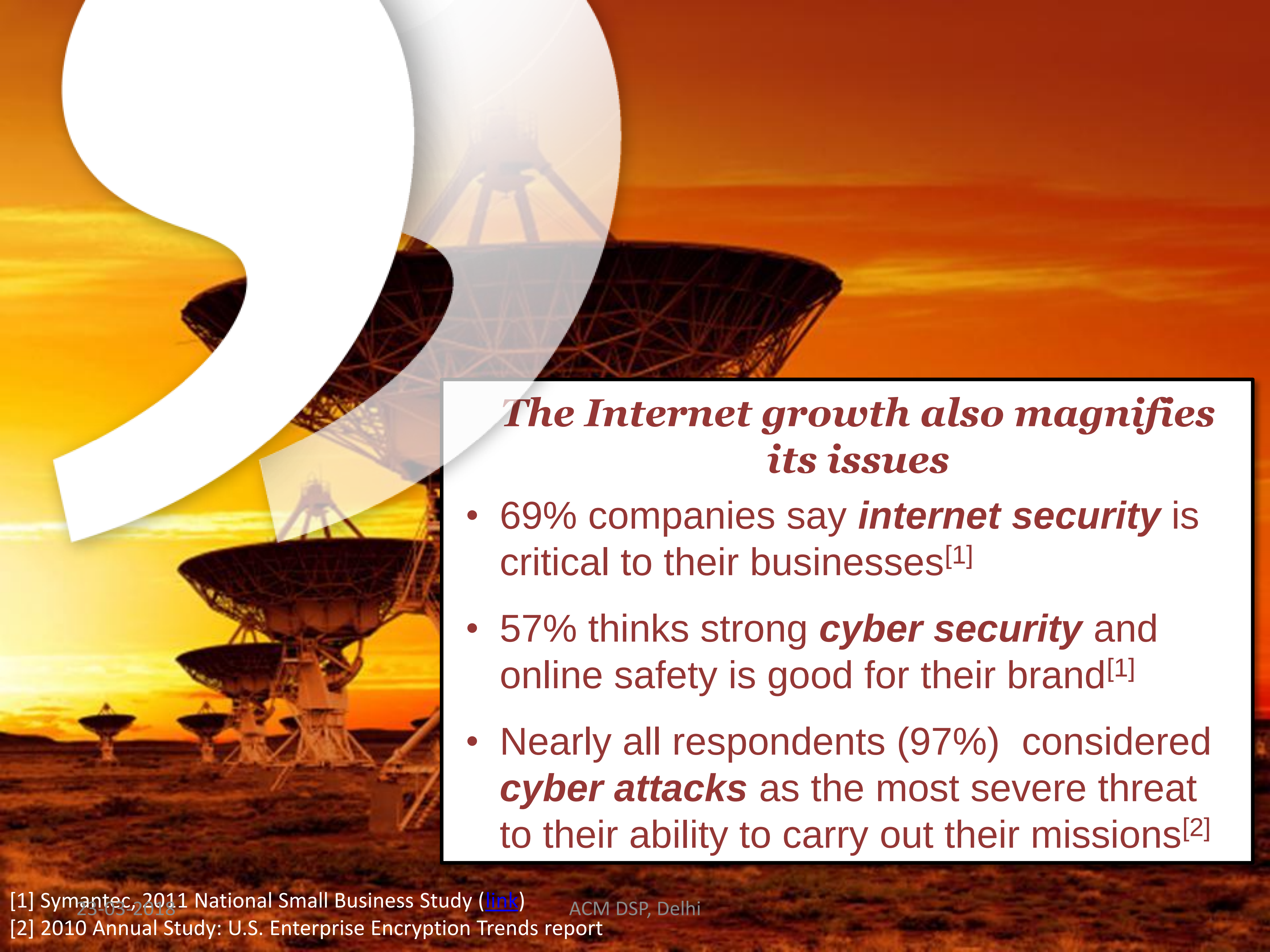


2010 CSI Computer Crime and Security Survey

2010 Respondents: 237

U.S. Federal
Cybersecurity
Market
$65.5 Billion
in 2013-2018
CAGR 6.2%

Information security and resilience critically important to many businesses



The Internet growth also magnifies its issues

- 69% companies say ***internet security*** is critical to their businesses[1]
- 57% thinks strong ***cyber security*** and online safety is good for their brand[1]
- Nearly all respondents (97%) considered ***cyber attacks*** as the most severe threat to their ability to carry out their missions[2]

[1] Symantec, 2011 National Small Business Study (link)

[2] 2010 Annual Study: U.S. Enterprise Encryption Trends report

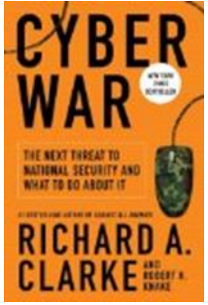
Scada (Supervisory Control And Data Acquisition): Risks

- Control Systems
  - Now at a higher risks to computer attacks because their vulnerabilities are increasingly becoming exposed and available to an ever-growing set of motivated and highly-skilled attacker
- Miscreants tailor their attacks with the aim of damaging the physical systems under control
- Essentially **Cyberwar**

SCADA Attacks

- March 1997: Worcester Air Traffic Communications Attack
- January 2000: Maroochy Shire Sewage Spill
- 2000 and 1982: Gas Pipelines in Russia (and the former Soviet Union)

Cyber War


CYBER
WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
RICHARD A.
CLARKE

- Cyber warfare has been defined by government security expert Richard A. Clarke, in his book Cyber War (May 2010), as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- All “big” nations are currently preparing for Cyber War
  - Cyber Defense Centers established in all these nations within their military structure & NATO
  - Cyber Defense Centre of Excellence in Estonia
  - Cyber Defense part of new NATO Strategy (Article 5 excluded)
  - Military and government networks are currently being hardened against attacks
  - All nations and, to and unbelievable large scale, China are training offensive cyber war personnel and are preparing for offensive an defensive cyber war
- **Information Superiority:** the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (US Army Vision 2010)

Some Cyber Wars

- **Titan Rain** was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003
- **Estonia 2007** Cyberattacks on Estonia refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters
- **Israel attack on Syria** During the night, an Israeli transport helicopter entered Syrian airspace and dropped a team of Shaldag Unit commandos into the area. The commandos took up positions close to the nuclear site. Israeli Air Force F-15I Ra'am fighter jets armed with laser-guided bombs, escorted by F-16I Sufa fighter jets and an ELINT aircraft, took off from Hatzerim Airbase. The ELINT aircraft successfully obscured the attacking aircraft from detection by Syrian radars.

STUXNET

- Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment
- it is the first discovered malware that spies on and subverts industrial systems
- Kaspersky Labs concluded that the sophisticated attack could only have been conducted "with nation-state support”
- Stuxnet attacked Windows systems using an unprecedented four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm)

Stuxnet

- Astonished by the complexity of the program and the quantity of zero day exploits used in this worm.
  - Zero day exploits are those that have no work around or patch.
- Another unique aspect of Stuxnet is that it contained components that were digitally signed with stolen certificates.
- a root kit was found for the programmable logic controller (PLC) which allows the manipulation of sensitive equipment.

- Expected to have been created by a team of as many as 30 individuals. – STATE SUPPORT
- indicates a level of organization and funding that probably has not been seen before
- What was Stuxnet designed to do?
  - While there is no direct evidence, the code suggests that Stuxnet looks for a setup that is used in processing facilities that handle uranium used in nuclear devices
  - Thus the ultimate goal is to sabotage that facility by reprogramming to controllers to operate

Stuxnet

- The Stuxnet malware itself contained many different components and took advantage of four of the then unpatched vulnerabilities in Windows systems. Two of the vulnerabilities were used to spread Stuxnet—the LNK vulnerability
  - the Printer Spooler vulnerability
  - The other two vulnerabilities were used to elevate privileges on already infected machines—
    - the Win32k.sys keyboard layout vulnerability (CVE-2010-2743) and
    - the Task Scheduler vulnerability (CVE-2010-3888).
- Since the detection of Stuxnet, each of these vulnerabilities has been patched by the vendor.
- Stuxnet takes advantage of a default password in the Siemens WinCC software's database server as well as infect Siemens Step7 project files.

- There are rootkit components that have been signed with stolen certificates which make it difficult to fully clean an infected system.
- The certificates used have since been revoked, but it is still possible for Stuxnet to infect a system
- If stuxnet does not find Wincc/step 7, it does nothing
- Other wise, it infect the PLC without zero-day exploit and then reprograms it; attempts to hide changes through a root kit
- Reprogramming is done changing parts of the code overwriting process variables every 5 secs and inserting rouge ladder logic – hence impossible to detect

What should be the strategy to deal with these kinds of attacks?

- Should it go along the lines of IT security?
- How about Defense-in-depth mechanisms analogous to anomaly detection?
- What about false-alarms in anomaly detection?
- Should the focus be on Physical systems rather than software/network models?

Control Systems Security

- Control systems not suitable for patching and frequent updates
- While current tools from Information security can give necessary mechanisms for securing control systems, these alone are not sufficient for defense-in-depth of control systems
- **When attackers bypass even basic defenses they may succeed in damaging the physical world**

Consequences of an Attack

Risk Assessment

- While studies exist on cyber security of SCADA there are very few studies to identify attack strategy of an adversary once it gains access (existing studies pertain to data injection for power grids, electricity markets etc.)
- Need to understand threat model to design appropriate defenses and take measures to secure the most critical sensors and actuators

New Attack detection Patterns

- Dynamic system models for specifying Intrusion detection Systems
  - Current studies pertain false data injection attacks in control systems

Attack Resilient Algorithms and Architectures

- Design to withstand cyber assault

- Reconfigure and adapt control systems when under attack

Control Systems Security: Summary

- Understand the consequences of attacks
  - Do a thorough risk analysis
- Find Attack patterns
  - Design detections
- Design new attack-resilient algorithms and architectures
- Automatic response measures

Multi Disciplinary: Control Engineers + CS + Domain of Application …

Risk Management

- Process of shifting the odds in your favor by finding among all possible alternatives, the one that minimizes the impact of uncertain events

- Process Control Systems usually will have a network of sensors
  - Examples of impact of attack on sensor network on the process control system

New Scenario of Attacks

- Sensor Measurement: Y (k) ={y1(k), . . . , yp(k)},
  - yi(k) denotes measures by sensor i at time k.
  - ∀k, yi(k) ∈ [ymin, ymax] in the DOM (Y)
- Each sensor has a unique Crypto identity key
- Zi(k)s signals recd. by process controller (Val in domain – else gets det.).
- Zi(k)= aik if in attack slot

  = yik other wise

- **Integrity Check:**

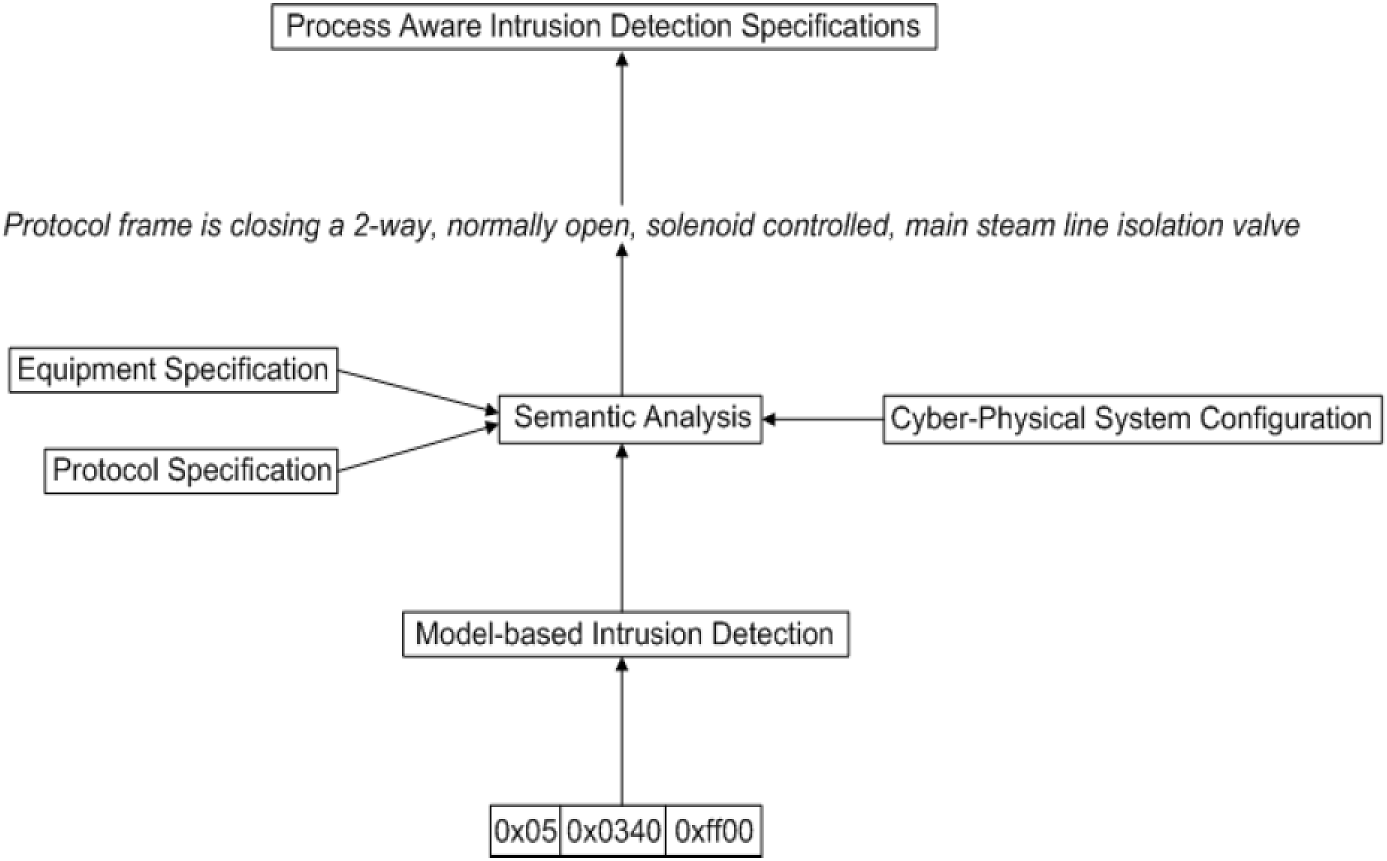
If attackers have compromised a sensor they can inject any value aik – an arbitrary value in the domain

- **DOS Attack**
  - Notices lack of measurements
  - A solution is to use the last value

Intrusion Detection

- Misuse detection
  - Based on signatures of known attacks
- Anomaly detection
  - Based on learning profiles of normal behaviour
    - Could detect unknown attacks but suffers from high false alarm rates
- Specification-based Detection
  - Manually developing specification of legitimate behaviour and hence has less false alarm rates
  - But ability to detect new attacks is also less.

Process Aware Intrusion



Process Aware Intrusion Detection Specifications

Protocol frame is closing a 2-way, normally open, solenoid controlled, main steam line isolation valve

Equipment Specification

Protocol Specification

Semantic Analysis

Cyber-Physical System Configuration

Model-based Intrusion Detection

0x05 | 0x0340 | 0xff00

Mirage Theory for Deception-Based Detection

- Military Deception (MILDEC): those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission.
- Relies on DISPLAYs: simulation, disguising, and/or portrayal of friendly objects, units, or capabilities that may not exist but are made to appear so.
- Eg. (physical means): dummy and decoy equipment and devices, tactical actions, movement of military forces, etc.
- Eg (technical means) include emission of chemical or biological odors, emission of radiation, reflection of energy, computers, etc.,
- Eg (administrative means) techniques to convey or deny physical evidence.

Mirage Theory Applications: Ideas

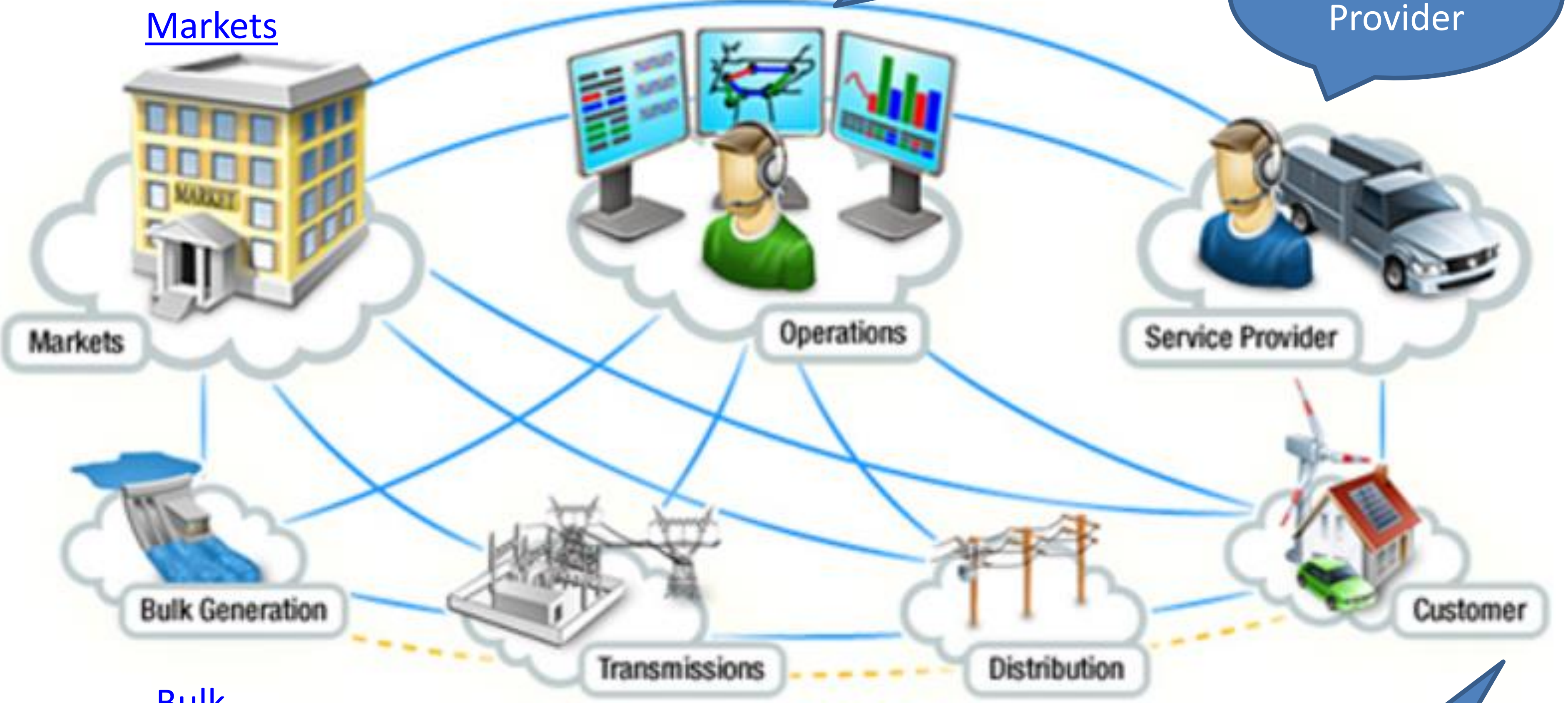
- **Basis:** leverage of the boundary between continuous and discrete spaces, leverage of how the presence of a continuous space is redirected on a corresponding discrete space, and simulation or emulation of physical processes and physical equipment.
- A computer network attack provides an adversary with access that may extend to a whole discrete space.
- Nevertheless, due to physical limits there are no feasible ways for an adversary to gain visibility over a continuous space through a computer network attack.
- In other words, a computer network attack won't enable an adversary to virtually move beyond the analog-to-digital and digital-to-analog conversion integrated circuits.
- Consequently an adversary cannot verify whether input electrical signals are indeed applied by existing sensing devices, nor can he/she verify whether output electrical signals indeed reach an existing actuating device.

Challenges

- Intrusion detection approaches devised for operation in process control networks are required to be highly effective in terms of probability of detection and false alarms rate due to the sensitivity of the tasks that those special purpose networks conduct in industrial environments.
- More specifically, no single attack on process control networks can be left undetected due to permanent physical damage that those attacks have potential to cause on the digitally controlled physical system.
- False positives may also prove more costly in process control networks when compared to general purpose computer networks.
- **Challenge is to arrive at techniques that would correct the limitations of the three intrusion detection approaches .**

Power Grid is one of the 20th Century's Greatest Engineering feats

Smart- Grid Framework



Operations

Service Provider

Markets

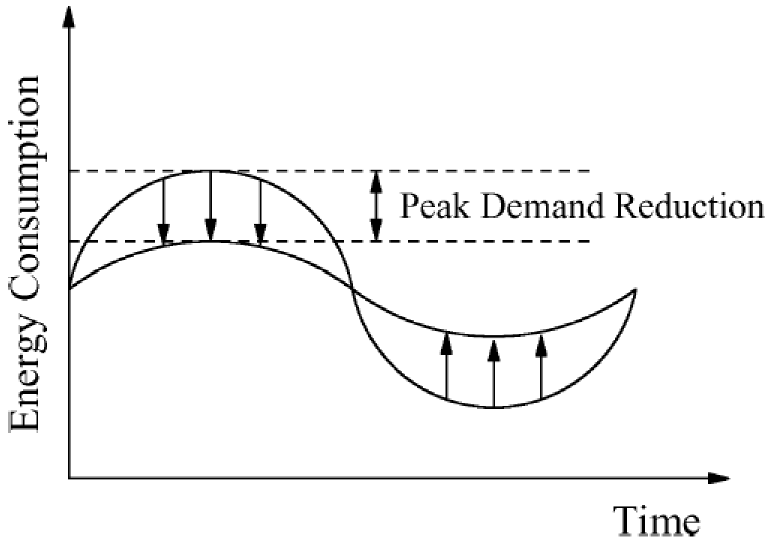
Bulk

Distribution

Customer

Smart Grid

Objective



- **Peak demand reduction**

- **Using smart meters -- cutting some appliances that could be scheduled later at off-peak schedules.**

Transformation

- Centralized producer controlled network to **a decentralized consumer-interactive network with fine-grained monitoring**
  - **Old meters collected data monthly (or hourly) while smart meters collect data every minute**
  - **While SCADA collects data every 1 to 2 secs, phasor measurement units (PMUs) collect 30-60 times a sec.**
  - **PMUs and Advanced Metering I nfrastructure (AMI) provide an MRI of the the grid as opposed to X-rays of SCADA**

Smart Grid Features & Vulnerabilities

- Smart-grid technology includes distributed control and monitoring systems that extend control to consumer equipment such as distributed generators, office and home appliances.
- Control and monitoring signals travel via different media networks to many end-use devices with various vulnerabilities.

- Question: Can Smart-Grid resist attacks and self-heal itself without causing infrastructure and equipment damage or large-scale blackouts?
- Problems: Massive use of low-cost communication/ electronics provides an explosion of information that bears different data formats and time stamps, with or without secured information interchange mechanisms.

Smart Grid: Pros and Cons

- Allows close interaction and inter-operation of T&D grid, building & house controllers, and distribution generation.

- Challenge: Devise a defense supervisory system that can efficiently process myriads of data to evaluate system status, identify failures, predict threats, and suggest remedials.

- Possibility of cyber attacks and cascade failures propagating from one system to another.
- Leads to power system blackouts, smart-grid IT infrastructure failures, energy market chaos, damaged consumer devices, human safety,
- Could have more frequent incidents such as smaller-scale outages.

Grid Security Challenges

- Numerous challenges will arise with the integration of cyber and physical systems, along with such factors as
  - human behavior, commercial interests, regulatory policy, and even political elements.
  - Some challenges will be quite similar to those of traditional networks, but involving more complex interactions.

Some select challenges

- Trust
- Communication and Device Security
- Privacy
- Security Management: Issues in Complexity and Scale

Trust

- Appropriate (authenticated) user is accessing valid consistent data created by the Right device at the expected location at the expected time, communicated using the expected protocol
- The data hasn’t been tampered with.

Classical

- Grid’s control systems are assumed to be operating in an environment of implicit trust, which has influenced design decisions.

  (like our Operating Systems)

Smart Grid

- Many stakeholders aren’t trustworthy,
- New methods are required for monitoring approaches

Communication and Device Security

Classical

- Electric-grid communications have relied largely on serial communication for monitoring and control. Serial comm. is reliable, & predictable,
- Due to the underlying communications protocols, provides some containment.
- Traditional communications involve devices that were in areas with physical access controls like fences and locked buildings

Smart Grid

- Use Internet technologies, broadband communication, & nondeterministic comm. Environments
- Compounded by the rapid deployment of smartgrid systems without adequate security and reliability planning.
- Two-way meters being deployed are accessible by consumers and adversaries.
  - Thus, automatic meter reading (AMR) environments are to be treated as hostile

Privacy

- Classical Electric grid’s security Objectives: availability, integrity, and confidentiality.
- **Smart Grid: Incorporates smart metering and load management**

- user and corporate privacy is increasingly becoming an issue.
- Electricity use patterns could lead to disclosure of not only how much energy customers use but also when they’re at home, at work, or traveling.
  - it might even be possible to deduce information about specific activities (for example, sleeping versus watching television).

- Also possible to discover what types of appliances and devices are present by compromising either the customer’s home area network or the AMR network.
- increases in power draw might suggest changes in business operations.
- Such energy-related information could support criminal targeting of homes or provide business intelligence to competitors.

- **Challenge: mitigating such threats.**

Security Management: Complexity & Scale (1)

- The classical Electric Grid communicates with thousands of devices.
- In Smart-Grid, the volume of data and the number of devices with which a utility communicates increases by several orders of magnitude.
- Thus, maintenance, managing trust, monitoring for cyberintrusion become challenges.

- Cryptographic key management: Smart meters use X.509 certificate for device identification and cryptographic-session establishment.
- However, a certificate's cryptographic keys are static for each device
  - Thus, providing a key lifetime equivalent to the meter's useful life (5 to 15 years). Cryptographic solutions in this context should include a key management solution to periodically update keys, or at least to revoke them.
  - Support staff required to maintain PKI management becomes very formidable (cost etc)

Security Management (2)

- The time and processing required to update cryptographic keys.
- Devices currently planned for monitoring and controlling the smart grid might not have the processor cycles and memory to adequately support fast and high-volume cryptographic computations.

Architecture-Based Requirements & Solutions

- Grid’s hierarchical physical and cyberinfrastructure layers :
- Generation, Transmission, Distribution
  - In transmission systems, SCADA components enable balancing authorities (BAs) to exchange command and data information with substations for sensing and actuation of grid parameters.
  - At higher layers, BAs communicate regularly with reliability coordinators (RCs), and entities engage in market transactions with independent system operators (ISOs).
- The time frame granularity for operations varies depending on the kind of activity involved.

- Eg., protection and control mechanisms at substations operate at the granularity of milliseconds.
- State estimators and contingency analyses in BAs and RCs operate at the granularity of minutes.
- Hourly and day-ahead power markets run by RCs operate at the granularity of hours and days, respectively.

- Distribution side: less structured

Requirements for Effective Cybersecurity Solutions

- Cybersecurity properties: confidentiality, integrity, availability,
- **Availability**: Highest Priority as it has to manage continuous power flow in the physical infrastructure
- Efficiency and scalability
- Adaptability & evolvability

- Great opportunities for Designing effective cybersecurity solutions taking into account specified power flows, presence of trusted third parties, and inherent redundancy for contingencies.

Transmission Substations

- Authentication technologies for transmission substation networks face short, strict real-time constraints.
  - In certain cases, multicast messages must be delivered in less than 4 milliseconds.
  - Addressing this challenge requires not only efficient authentication algorithms minimizing computational cost
    - **but also** avoidance of buffering packets so that presented data can be processed immediately.
- Multicast authentication schemes should also have small communication overhead, packet-loss tolerance, and resistance against malicious attacks.

An example of Authentication (Qan Wang et al): Using one-time-signature and one-way hash chain cryptographic constructs

It has features like: fast signing, verification and buffering-free data processing.

Constrained SCADA networks (Patrick Tsang and Sean Smith)

- "bump in the wire" solution for authentication for legacy SCADA devices.
- first apply Hash-Base Message Authentication Code to byte streams with minimal buffering.
- They then convert the random-error detection available on legacy systems into a mechanism that guarantees data authenticityand freshness.
- This solution achieves very low latency.

Policy-based data sharing (1)

- Aim to use GPS-clock-synchronized fine-grained power grid measurements to provide increased grid stability and reliability.
- Key to achieving this is securely sharing the measurements (synchrophasor measurements gathered by PMUs) among power grid entities over wide area networks.
- Typically, such sharing follows policies that depend on data generator and consumer preferences and on time-sensitive contexts; for example, entities will more likely share information during an emergency.

Policy-based data sharing (2)

- **Example** (Rakesh Bobba et al): Leverage presence of trusted third parties to design a mediated policy-based encryption system that protects the secrecy of data and policies while releasing them to authorized entities.

- Extends key encapsulation mechanism/data encapsulation mechanism encryption framework and leverages RCs and ISOs for policy enforcement.

- **Shows how power grid offers opportunities (in this case, trusted third parties with regulatory oversight that might not exist in other environments) for designing solutions. Attestation for constrained smart meters – that are a key element of the smart grid and represent a constrained embedded platform.**

- **A key challenge** : **ensuring the devices' software is authentic,** to prevent energy theft and other attacks.
  - These devices' cost, power, memory, and computational limitations restrict the ability to deploy standard trusted platform modules on them.

- **Cumulative Attestation Kernel**(Michael LeMay , Carl Gunter's) : an architecture implemented at a low level in the embedded system.
  - **provides cryptographically secure audit data for an unbroken sequence of firmware revisions installed on the system, including the current firmware.**

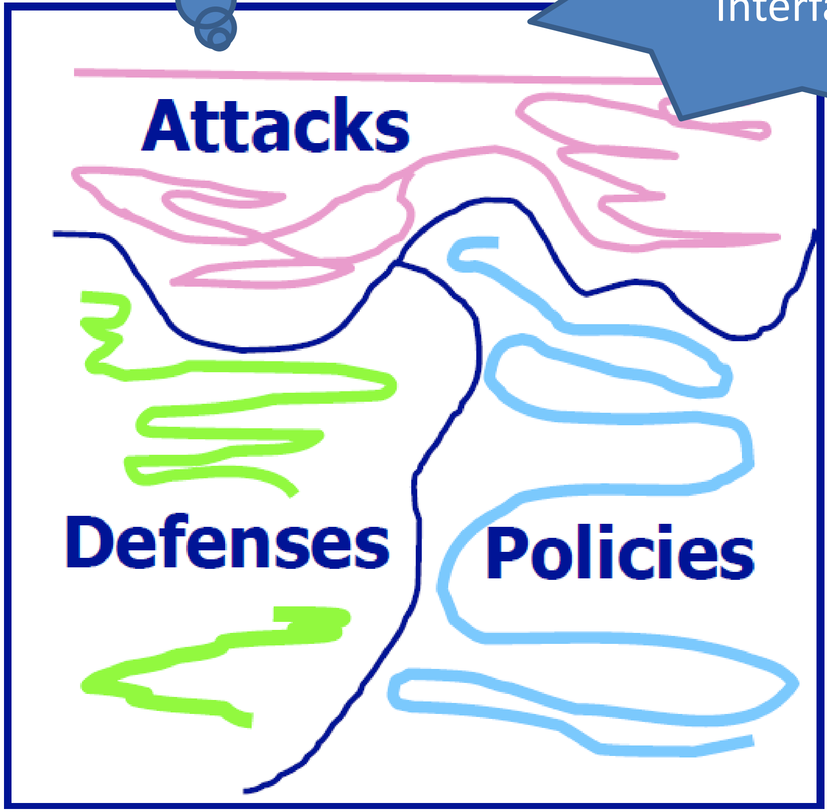
- LeMay and Gunter: Developed a prototype that employs microcontrollers typically used in smart meters and formally verifies the remote-attestation protocol.

Cost

Theories About

Cyber Interface

System



Features:

- Classes of policies
- Classes of attacks
- Classes of defenses

Relationships:

"Defense class D enforces policy class P despite attacks from class A."

"Defense D + Defense D' = …"

Summary

- Attack Models:
  - An integrated approach for Cyber and System attack model
- Security of system (stability, safety, performance, **availability**)
- Security Cybersystem – Confidentiality, integrity, availability
- Scalable Key Management
- Countermeasures of Cyber-oriented and System-oriented
  - Contingencies
- Devise a defense supervisory system that can efficiently process myriads of data to evaluate system status, identify failures, predict threats, and suggest remedials.
- Privacy
- Effective Cyber Security Solutions

References

SCADA

- Attacks Against Process Control Systems: Risk Assessment, Detection, and Response, Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang and Shankar Sastry, ACM ASIACCS 2012
- Composite Intrusion Detection in Process Control Networks by Julian L. Rrushi, Ph.D. Dissertation, University of Milano, 2008

Specification Based Intrusion Detection

NV Narendra Kumar & RK Shyamasundar, ICSE 2010, EICAR 2010, 2011,

Smart Grids

- Smart-Grid Security Issues, H Khurana et al., IEEE Security and Privacy Jan/Feb 2010
- Cyber–Physical Security of a Smart Grid Infrastructure, Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli, Proceedings IEEE, Jan 2012.

PKI for Security Management:

Access control for a Distributive Business Approach, Vishwas Patil, RKS, Alesandro Mei, Sept 2012, Lambert Academic Pub

Access control for a collaborative business environment not only needs to manage resources of individual collaborator but also needs to integrate, dissociate collaborating domains' users & resources, on-demand. As inter-domain transactions are carried out over the Internet, the transactions need security & privacy. Interoperability mechanisms fall short to comprehensively achieve security & privacy in a manner that is scalable, dynamic, autonomy-preserving, and tractable in ephemeral collaborations; thus risking the manageability and security of overall environment in practice. This book delves into all the practical aspects of access control for a distributed environment. Fundamental concepts are explained with the help of practical scenarios. A spectrum of PKIs & their effects on resulting access control frameworks have been extensively studied. The role of cryptography & its relevance is advocated through our analysis & solutions. This book shall help security architects & consultants in arriving at better design decisions. The investigative scenarios & corresponding solutions presented in this book should help security practitioners to engineer their approaches judiciously.

Vishwas Patil

Vishwas Patil is a Scientist at Institute for Infocomm Research, Singapore. He pursued his PhD from Sapienza University of Rome. RK Shyamasundar is JC Bose National Fellow & Senior Professor at TIFR. He is a fellow of ACM, IEEE, IAS, INSA, INAE, NAS, TWAS. Alessandro Mei is a Professor at Sapienza University of Rome. He is a Marie Curie fellow.

978-3-659-17508-4

Access Control - A PKI Approach

Patil, Shyamasundar, Mei

Vishwas Patil
Rudrapatna Shyamasundar
Alessandro Mei

Access Control for a Collaborative, Distributed Business Environment

A PKI Approach

LAP LAMBERT Academic Publishing

THANK YOU

QUESTIONS?