SECURITY OF SMART GRID

Weichao Wang (UNCC), Yi Pan (Georgia State), Wenzhan Song (Georgia State) and Le Xie (Texas A&M)

NSF SFS Project Team on "Integrated Learning Environment for Smart Grid Security".

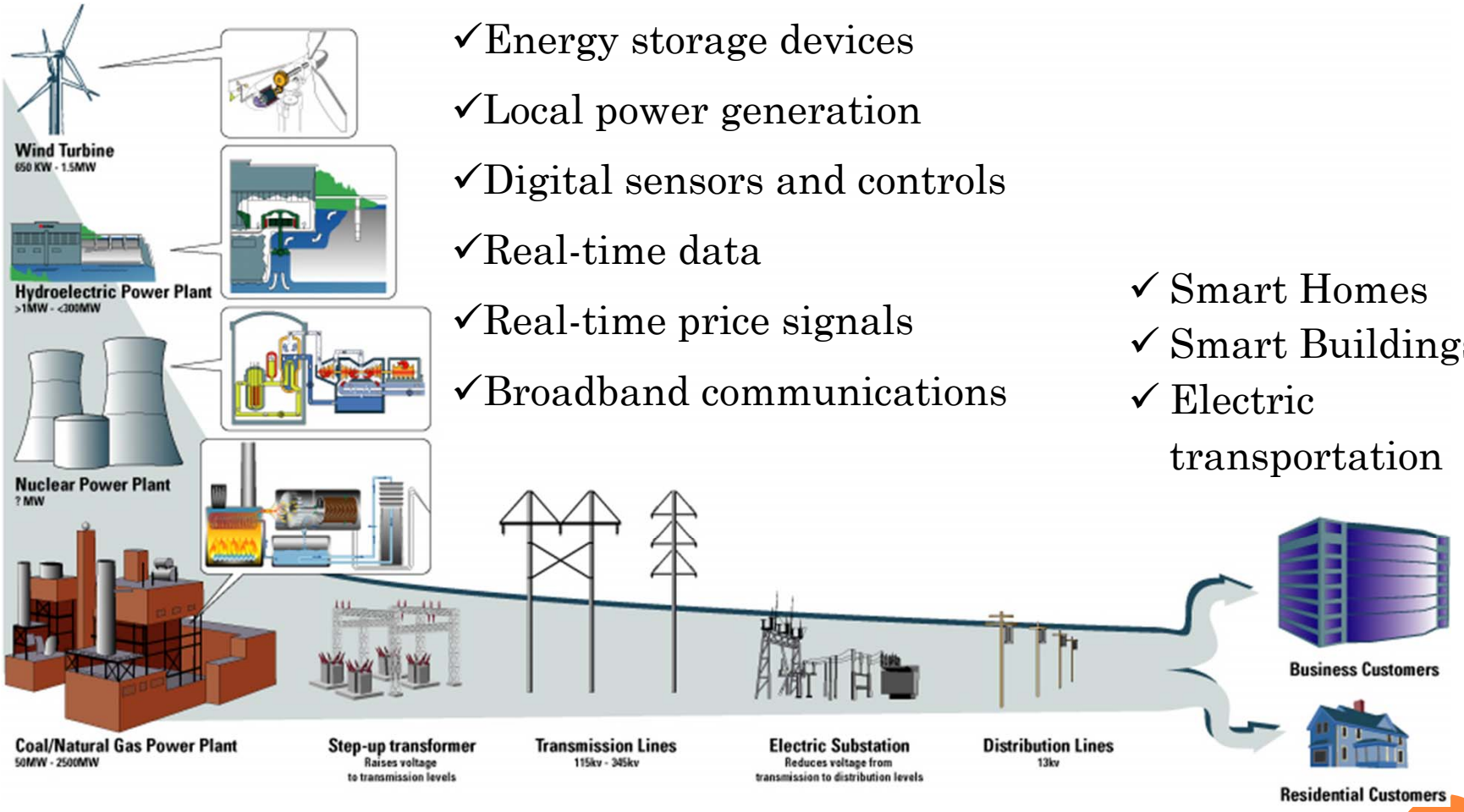
Organization of the Presentation

- Introduction to Smart Grid
- Security requirements
- Security challenges
- Security of Industrial Control Systems
- Security of AMI

PRIMARY OBJECTIVES OF SMART GRIDS

- National integration;
- Self healing and adaptive: improve distribution and transmission system operation;
- Allow customers freedom to purchase power based on dynamic pricing;
- Improved quality of power: less wastage;
- Integration of large variety of generation options;

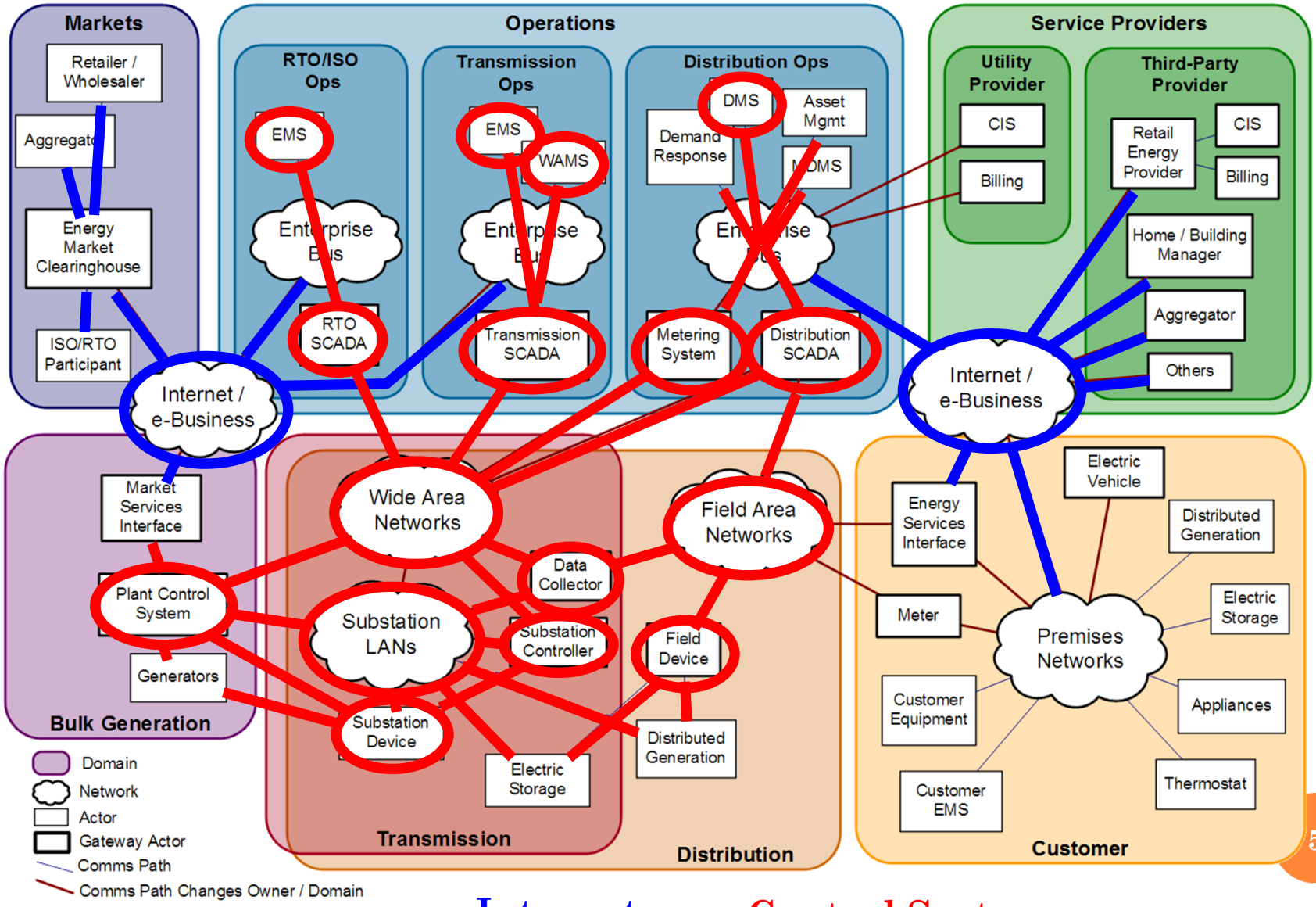
SMART GRID ARCHITECTURE



- ✓Energy storage devices
- ✓Local power generation
- ✓Digital sensors and controls
- ✓Real-time data
- ✓Real-time price signals
- ✓Broadband communications

- ✓ Smart Homes
- ✓ Smart Buildings
- ✓ Electric transportation

Power Grid Comm. & Control: a Close View



borrowed from NIST Smart Grid Twiki

- Security Requirements of Smart Grid
  - Hardware:
    - Define Critical Cyber Assets
    - Define & Create Electronic Security Perimeters
  - Software:
    - Support control and Wide Area Networks
    - Malicious Software Prevention
    - Disable Unused Ports And Services
  - Human Factors and Accountability:
    - Track and Report Access by User with Audit Trail
    - Remove User Access (in 24 hours) for Termination
    - Provide for User Access Rights – Gateway
    - Strong Two Factor User Authentication for Interactive Access
    - Appropriate Use Banner

- Security Challenges
  - Diversity of protocols being used;
  - Special topology and devices in Smart Grid;
  - Human factor;
  - Legacy devices;
  - Third party software and hardware;
  - Lack of details on attacks;

Security Risks to Modern Industrial Control Systems (ICS)

- COTS[a] + IP + connectivity = many security risks (COTS: Commercial off-the-shelf)
- All of those of Enterprise networks and more

Worms and Viruses	Legacy OSes and applications
DOS and DDOS attacks	Inability to limit access
Unauthorized access	Inability to revoke access
Unauthorized applications	Unexamined system logs
Unpatched systems	Accidental mis-configuration
Little or no use of anti-virus	Improperly secured devices
Limited use of firewalls	Improperly secured wireless
Improper use of ICS networks	Unencrypted links

When ICS Security Fails

- Loss of production
- Penalties
- Loss of market value
- Physical damage
- Environmental damage
- Injury
- Loss of life

$$$.$$

- USSR pipeline explosion, 1982
- Bellingham pipeline rupture, 1999
- Queensland sewage release, 2000
- Davis Besse nuclear plant infection, 2003
- Northeast USA blackout, 2003
- Browns Ferry nuclear plant scram, 2006

Availability, Integrity and Confidentiality

- Enterprise networks require C-I-A
  - Confidentiality of intellectual property matters most
- ICS requires A-I-C
  - Availability and integrity of control matters most
  - control data has relatively low entropy
  - Many ICS vendors provide six 9's of availability
- Ensuring availability is hard
  - Cryptography does not help (directly)
  - DOS protection, rate limiting, resource management, QoS, redundancy, robust hardware
- Security must not reduce availability!

DoS and DDoS Attacks

- Denial of Service (DoS) attack overwhelms a system with too many packets/requests
  - Exhausts TCP stack or application resources
  - Defenses include connection limits in firewall
- Distributed Denial of Service (DDoS) attack coordinates many machines to overwhelm a target system
  - No single point of attack
  - Requires sophisticated, coordinated defenses
  - Weapon of choice for hackers and cyber-extortionists
- DoS, DDoS particularly effective when Availability is critical, i.e. against ICS

Fragile ICS Devices

- Many IP stack implementations are fragile
  - Some devices lockup on ping sweep or NMAP scan
  - Numerous incidents of ICS shut down by uninformed IT staff running a well-intentioned vulnerability scan
- Modern ICS devices are much more complex
  - Some IEDs (Intelligent Electronic device) include web server for configuration and status
  - More lines of code leads to more bugs
  - Modern IEDs require patching just like servers

Unpatched Systems

- Many ICS systems are not patched current
  - Particularly Windows servers
  - No patches available for older versions of windows
- OS and application patches can break ICS
  - OS patches are tested for enterprise apps
- Uncertified patches can invalidate warranty
- Patching often requires system reboot
- Before installation of a patch:
  - Vendor certification—typically one week
  - Lab testing by operator
  - Staged deployment on less critical systems first
  - Avoid interrupting any critical process phases

Limited use of Host Anti-Virus

- Anti-Virus operations can cause significant system disruption at inopportune times
  - 3am is no better than any other time for a full disk scan on a system that operates 24x7x365
- ICS vendors only beginning to support anti-virus
  - Anti-virus is only as good as the signature set
  - Signatures may require testing just like patches
- Anti-Virus may be losing ground in enterprise deployments
  - impact on hosts, endpoint security not getting better
  - virus writers have learned to test against dominant Anti-Virus
- application whitelisting can be a good alternative
  - enumerate goodness rather than badness

Poor Authentication and Authorization

- Machine-to-machine communications involve no "user"
- Many ICS have poor authentication mechanisms and very limited authorization mechanisms
- Many protocols use cleartext passwords
- Many ICS devices lack crypto support
- Sometimes passwords left as vendor default
- Device passwords are hard to manage appropriately
  - Often one password is shared amongst all devices and all users and seldom if ever changed
  - This is happening AGAIN in Smart Meter deployments!

Poor Audit and Logging

- Many ICS have poor or non-existent support for logging security-related actions
  - Attempted or successful intrusions may go unnoticed
- Where IDS (Intrusion Detection Systems) logs are kept, they are often not reviewed
- Various regulatory requirements are driving some change in this area
  - NERC—North American Electric Reliability Corporation
  - FERC—Federal Energy Regulatory Commission
  - Sarbanes Oxley and PCAOB (Public Company Accounting Oversight Board)
  - FISMA—Federal Information Security Management Act

Legacy Equipment

- Much legacy equipment
- Usually impossible to update to add security features
- Difficult to protect legacy communications
- Password protection is weak
- Little or no audit and logging

Unauthorized Applications

- Unauthorized apps installed on ICS systems can interfere with ICS operation
- Many types of unauthorized apps have been found during security audits
  - Instant messaging
  - P2P file sharing
  - DVD and MPEG video players
  - Games, including Internet-based
  - Web browsers

Inappropriate Use of ICS Desktops

- Web browsing can infect ICS
  - Browser vulnerabilities
  - Downloads
  - Cross-site scripting
  - Spyware
- Email to/from control servers can infect ICS
  - Sendmail and outlook vulnerabilities
- Disk storage exhaustion can crash OS
  - Storage of music, videos

Little or No Cyber Security Monitoring

- internal monitoring is essential to detect low profile compromises
  - IDS
  - port scanning
  - vulnerability scanning
  - system audit
- without internal monitoring we don't know whether or not systems have been compromised

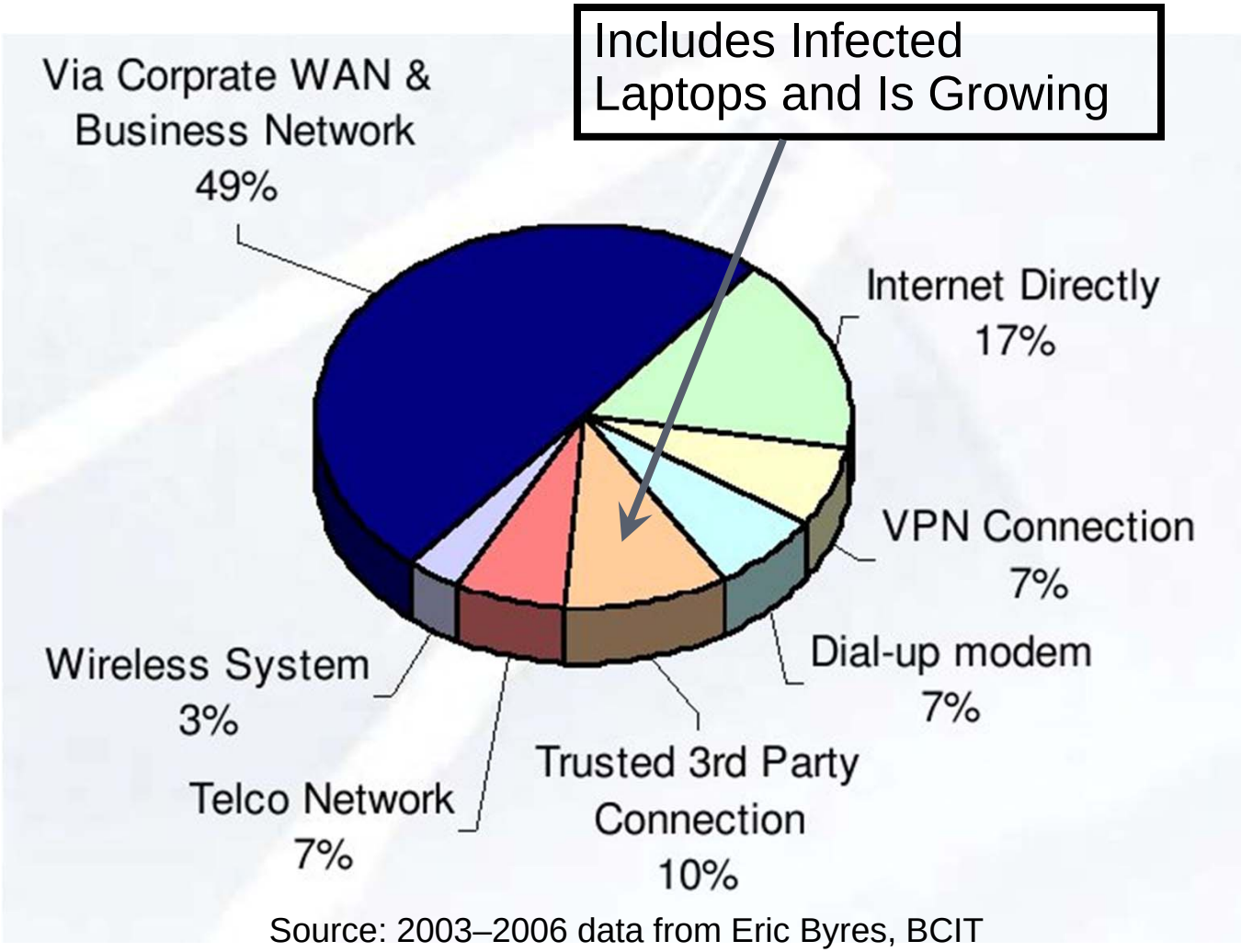
Requirement for 3rd Party Access

- Firmware updates and PLC, IED programming are sometimes done by vendor
  - Many ICS have open maintenance ports
  - Infected vendor laptops can bring down ICS
- Partners may require continuous status information
  - Partner access is often poorly secured
  - Partner channels can serve as backdoors

People Issues

- ICS network often managed by "Control Systems Department", distinct from "IT Department" running enterprise network
  - ICS personnel are not IT or networking experts
  - IT personnel are not ICS experts
- Majority of control systems workforce is older and nearing retirement
  - Few young people entering this field
  - Few academic programs

Attack Vectors into Control Systems

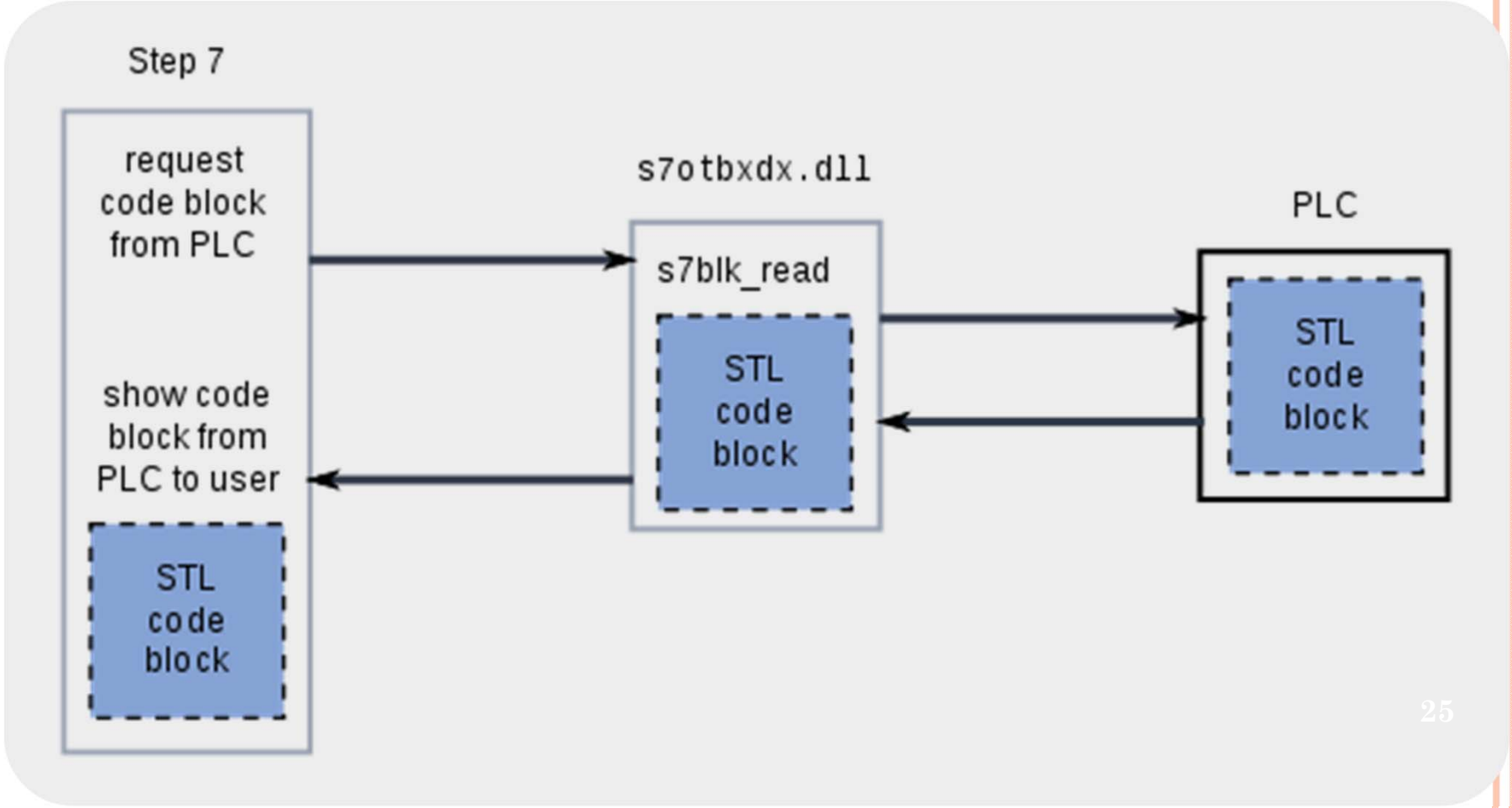


Source: 2003–2006 data from Eric Byres, BCIT

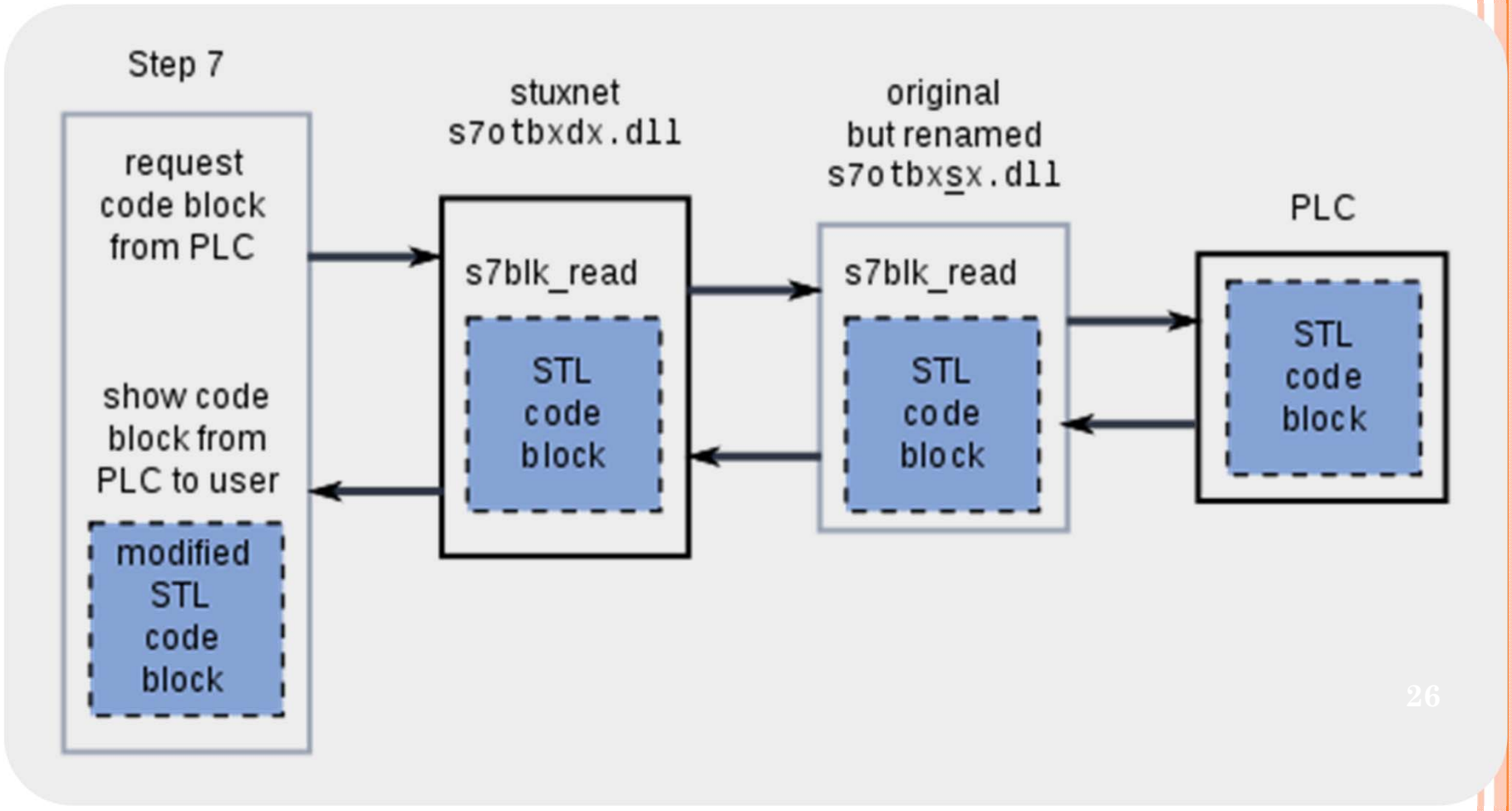
Component Based Attack Example - STUXNET

- Specifically programmed to attack SCADA and could reprogram PLC's
- Zero day attack
- Highly complex
- 0.5 Mb file transferred able to multiply
- Targets- Iran nuclear plants ,Process plants in Germany and ISRO India

Normal Communication between Step 7 Software and Siemens Programmable Logic Controller



Stuxnet Hijacking Communication Between Step 7 and Siemens PLC



Defending ICS

- Separate control network from enterprise network
  - Harden connection to enterprise network
  - Protect all points of entry with strong authentication
  - Make reconnaissance difficult from outside
- Harden interior of control network
  - Make reconnaissance difficult from inside
  - Avoid single points of vulnerability
  - Frustrate opportunities to expand a compromise
- Harden field sites and partner connections
  - mutual distrust
- Monitor both perimeter and inside events
- Periodically scan for changes in security posture

Smart Meter Security

- Meters may suffer from physical attacks such as battery change, removal, and modification.
- Functions like remote connect/disconnect meters and outage reporting may be used by unwarranted third parties.
- Customer usage varies on individuals, and thus, breaches of the metering database may lead to alternated bills.

Possible Solution

- Ensure the integrity of meter data.
- Detect unauthorized changes on meter.
- Authorize all accesses to/from AMI networks.
- Secure meter maintenance.

Personal Information

- NIST guidelines provide a list of personal information that is available on smart grid:
  - Name: responsible for the account
  - Address: location to which service is being taken
  - Account number: unique identifier for the account
  - Meter IP, Meter reading, current bill, billing history
  - Lifestyle; when the home is occupied and it is unoccupied, when occupants are awake and when they are asleep, how many various appliances are used, etc.
  - Service Provider: identity of the party supplying this account, relevant only in retail access markets.

30

Privacy Concerns

- Energy consumption data may disclose personal information.
  - Data in the smart meter and HAN could reveal certain activities of home smart appliances, e.g., appliance vendors may want this kind of data to know both how and why individuals used their products in certain ways.
  - Near real-time data regarding energy consumption may infer whether a residence or facility is occupied.
  - Personal lifestyle information can be derived from energy use data.

CONCLUSION

- Security of smart grid is of top priority before any such systems can be deployed;
- Connectivity and information access through smart meters open new doors to attacks;
- New technique is required to enforce information security;
- Education of end users plays an essential role in future power grid safety