



# Smart Grid Security: Reliable Energy Services on a Trusted Information Infrastructure



leave it up to us

**albis**  
technologies

# Recent Security Threats

The image is a screenshot of a news website, likely the Wall Street Journal, displaying a security-related article. The main article is titled "Stuxnet malware threat continues, targets control systems" by Angela Moscaritolo, dated July 21, 2010. The article text discusses the Stuxnet malware, its use of a zero-day Microsoft Windows Shell vulnerability, and its targeting of industrial control systems (SCADA) in the United States. The website features several banners with the text "Align with stronger security..." and icons of a power button, a padlock, and a shield. A sidebar on the left shows "TOP STORIES IN Technology" with a headline "Electricity". The top navigation bar includes "Home", "News", "Products", "Blogs", "Buyers Guide", "Whitepapers", "Jobs", "Events", "Subscribe", "SC World Congress", and "Archive". The article page includes social media sharing options for Print, Email, Reprint, Permissions, and Font Size, as well as a "RELATED ARTICLES" section with links to "Flaw uses USB devices as vector to steal data", "Microsoft Security Advisory (2286198)", "Authorities charge 53 in N.J. identify theft/bank fraud ring", "Phish claims recipient's tax payment was rejected", "NBA star Shaquille O'Neal accused of hacking", and "IBM buys compliance software".

**THE WALL STREET JOURNAL**  
Digital Network  
WSJ.com MarketWatch BARRON'S FINANCIAL NEWS More

Thursday, April 9, 2009

**SC MAGAZINE**  
FOR IT SECURITY PROFESSIONALS

Align with stronger security...

Home World EU

TOP STORIES IN Technology

TECHNOLOGY | APR

**Electricity**

Article

Email Print

By SIOBHAN GORMAN

Home > News > Stuxnet malware threat continues, targets control systems

## Stuxnet malware threat continues, targets control systems

Angela Moscaritolo July 21, 2010

PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A A A A Tweet 2 Like

The recently discovered Stuxnet malware, which takes advantage of a zero-day Microsoft Windows Shell vulnerability, is being used in targeted attacks to penetrate industrial control systems, particularly in the United States, according to security researchers.

The malware has been active for several days, targeting supervisory control and data acquisition (SCADA) systems, which are used to manage operations at places such as power plants and gas and oil refineries, to obtain data. The United States, Iran and Russia have been hit the hardest, according to security firm ESET. Almost 58 percent of all infections have occurred in the United States.

The Stuxnet worm exploits a zero-day vulnerability present in Windows Shell that was disclosed by Microsoft on Friday. The bug exists because Windows incorrectly parses checks for Link files.

### RELATED ARTICLES

- Flaw uses USB devices as vector to steal data

### RELATED LINKS

- Microsoft Security Advisory (2286198)

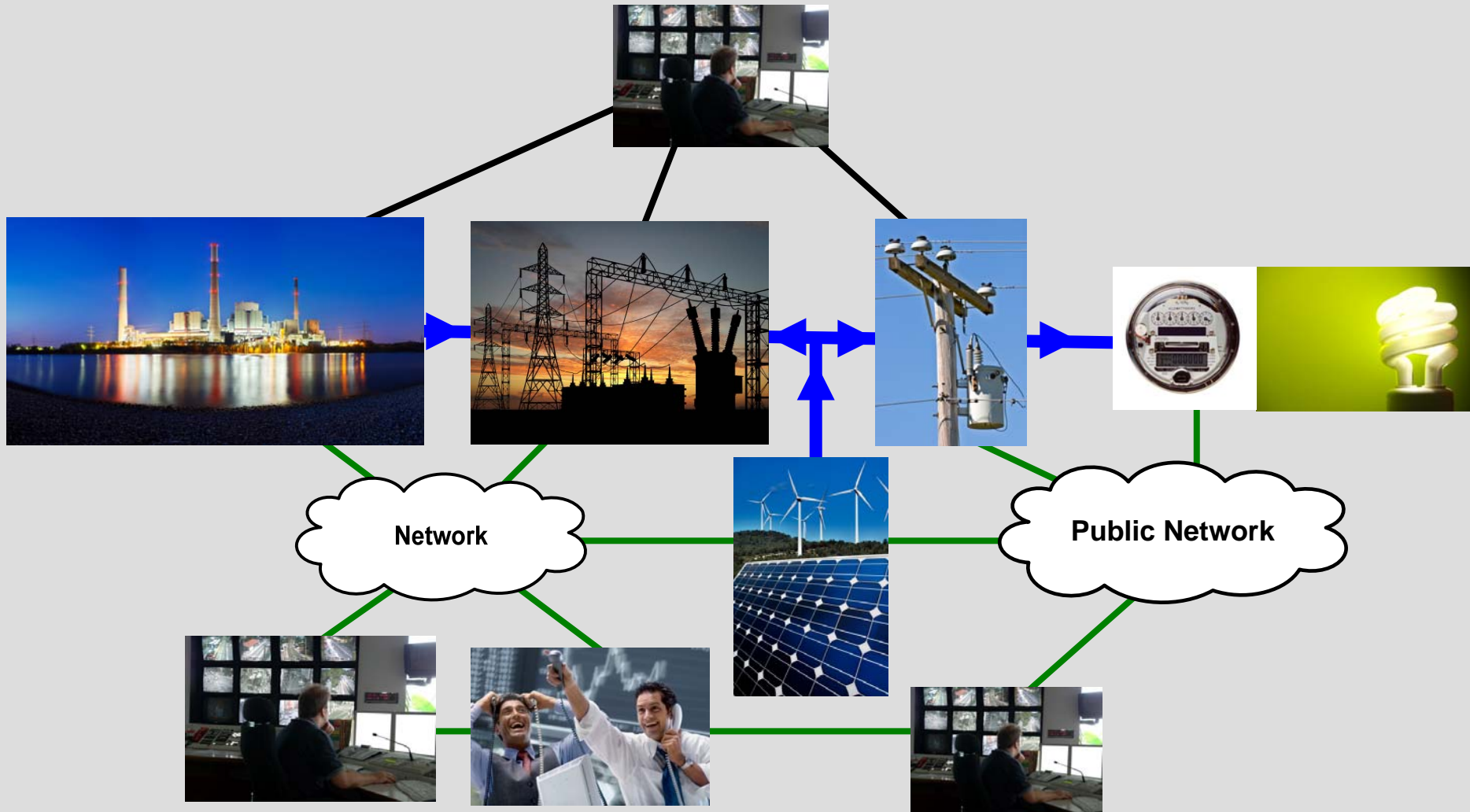
### MORE IN NEWS

- Authorities charge 53 in N.J. identify theft/bank fraud ring
- Phish claims recipient's tax payment was rejected
- NBA star Shaquille O'Neal accused of hacking
- IBM buys compliance software

Align with stronger security...

Align with stronger security...

# The Electric Grid – Yesterday and Tomorrow



# Securing the Electric Grid



New tech. feature	Decentralized generation	Switching and routing	<b>Two way communication</b>
Threat	Mix between office net and industrial plant	Eavesdropper, denial-of-service	<b>Achilles' heel of the Smart grid</b>
Security goals	Stability and availability	Confidentiality of data	<b>Privacy</b>
Security features	Physical security, firewalls	Data encryption, intrusion detection	<b>Access control, trusted devices</b>

# Emerging Standards

## ■ General

- Guidelines for Smart Grid Cyber Security – NIST:  
<http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>
- OASIS: Web service security for energy networks [http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=energyinterop](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=energyinterop)

## ■ Generation and Transmission

- NERC / FERC – mainly operational security
- IEC 62351 – Information Security for Power Control Systems Operations
  - Affects DNP, IEC 61850
  - TLS and challenge response mechanism
  - Role-base access control

## ■ Distribution and Metering

- AMI-SEC System Security Requirements  
[http://www.controlsystmsroadmap.net/pdfs/AMI\\_System\\_Security\\_Requirements-v1\\_01-1.pdf](http://www.controlsystmsroadmap.net/pdfs/AMI_System_Security_Requirements-v1_01-1.pdf)
- DLMS, COSEM: Security for narrow-band powerline communication

# Physical Security not sufficient – Information Security needed

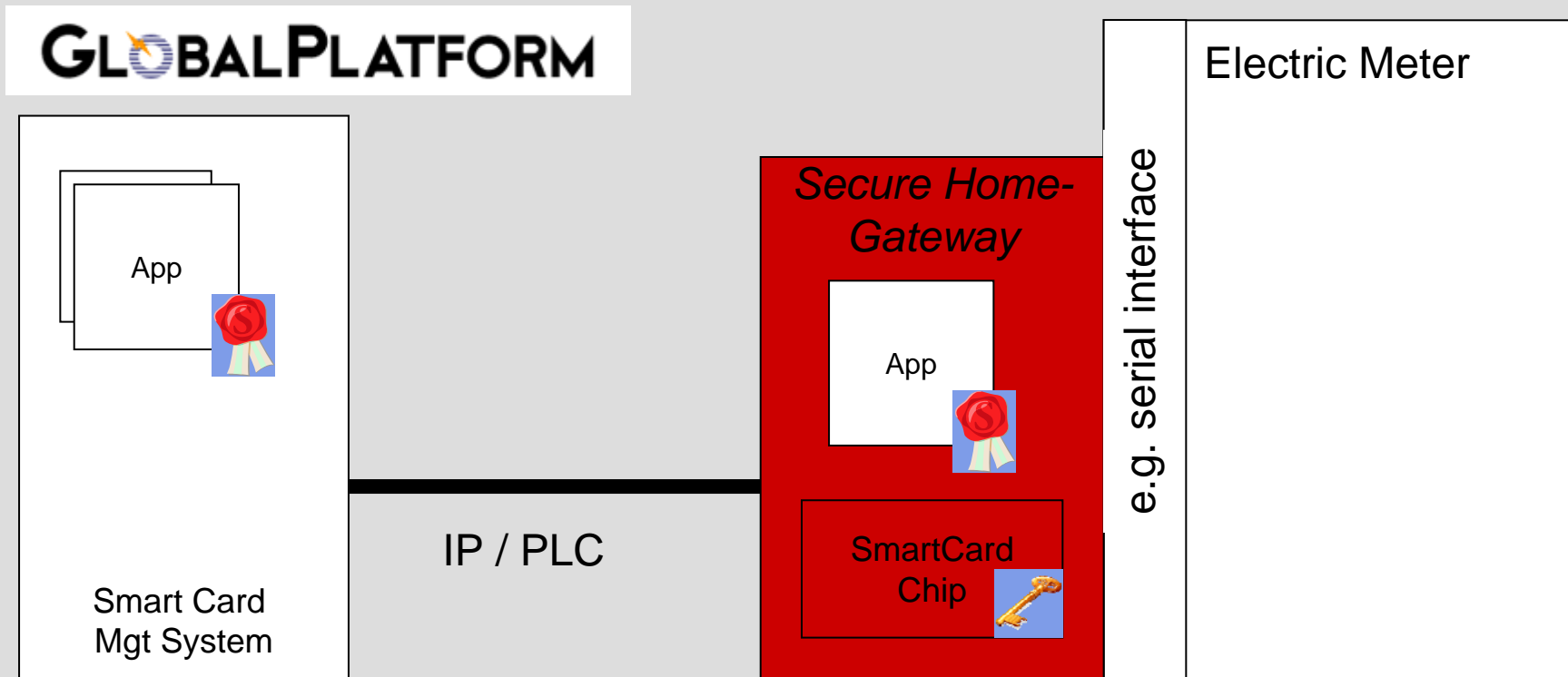


Critical infrastructures are exposed to the Internet

The availability of the power distribution network depends on the reliability of the information infrastructure



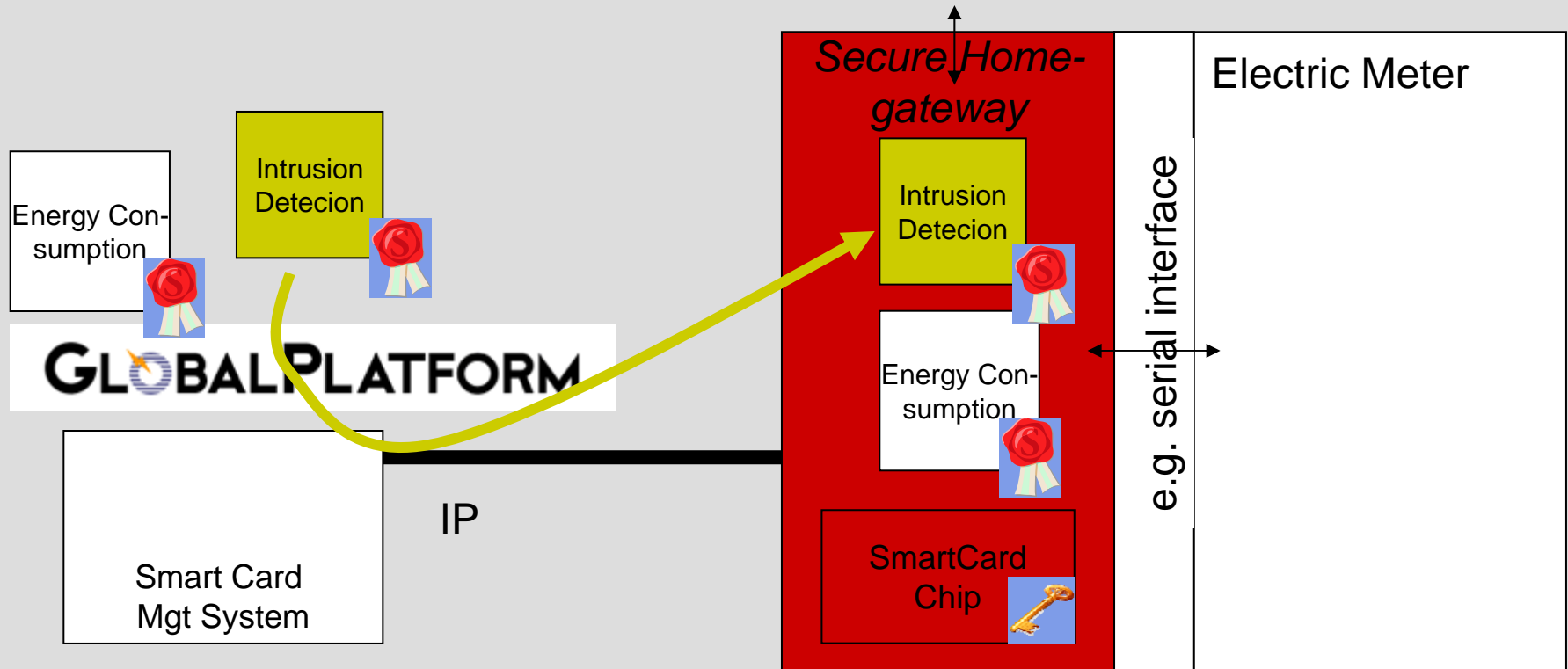
# Smartcard Technologies for Meters



## Goals

- Leverage on of existing security and network mgt technologies
- Allow upgrade of security in infrastructures with long lifetime
- Enable valued-added services securely on new metering infrastructure

# Smartcard Technology: Service Enabler in Metering Industry ?!



## Goal

Securing Smart Meters with value-added secure building-gateway.

# Summary

- The Smart Grid transforms physical assets to information assets
- Reliable energy services require a trusted infrastructure
  - Implement the security features provided by system vendors
    - Certification
  - Defence-in-depth realized for smart meters with trusted architecture
    - No real security without hardware
  - Role-based access control (RBAC)
    - End-to-end security to protect information assets
- Propositions
  - Protect privacy of customers and secure access to the electric grid with a gateway
  - Reap the benefits of established mechanisms in Smartcard Industry to protect novel smart metering infrastructure

# Leave it up to us



## Albis Technologies Ltd – Your partner for the Internet of Energy

Swiss quality with longstanding expertise in

- Embedded Security;
  - Wireless and High-frequency; and
  - Accredited certification for EMC & Safety
- located in the heart of Europe.

### Contact for R&D

Albis Technologies Ltd  
Marco Tölle  
8047 Zurich  
Switzerland  
Phone +41 58 252 4777

### Contact for Smart Grid Security

Albis Technologies Ltd  
Dr. Dieter M. Arnold  
8047 Zurich  
Switzerland  
Phone +41 58 252 4290

[development@albistechnologies.com](mailto:development@albistechnologies.com)

[http://www.albistechnologies.com/services/research/competence\\_center/trusted\\_en.php](http://www.albistechnologies.com/services/research/competence_center/trusted_en.php)

