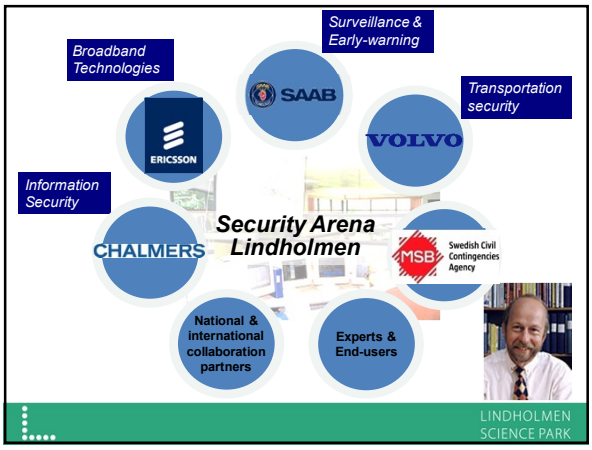
syssec

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet

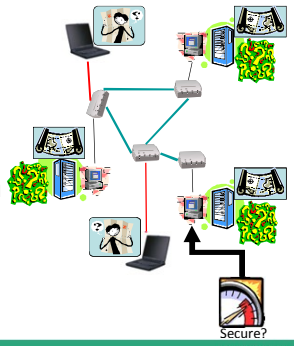
- Network of Excellence (2010-2014)
- Work towards solutions and collaborate
  - At a European level:
    - Poli. di Milano (IT)
    - Vrije Uniivesriteit (NL)
    - Institute Eurecom (FR)
    - IPP (Bulgaria)
    - TU Vienna (Austria)
    - Chalmers U (Sweden)
    - UEKAE (Turkey)
    - FORTH – ICS (Greece)
  - and with international colleagues around the world
- Focus
  - Research into malware & fraud, smart environments, and cyber attacks
  - Develop a curriculum for system security, and
  - Report and describe large threats in a yearly report

http://www.syssec-project.eu/



Research projects

- Protection against Denial-of-Service attacks
- Intelligent security logging
- Quantitative modelling and evaluation of security
- Decision support systems
- Secure sensor networks



LINDHOLMEN SCIENCE PARK

Communication and security projects

- Securing the connected car
- Security Metrics and Modeling
- IDS Systems
- Mitigating Distributed Denial of Service (DDoS) attacks
- Network defense against Spam
- SITS – Secure Intermodal Transport Systems
- Smart Grids
- Secure and Fault-tolerant Sensor Networks

CHALMERS

Secure Intermodal Transport System

Erland Jonsson

Tomas Olovsson

sits
Secure Intermodal Transport System

sits
Secure Intermodal Transport System

- Security Arena Project (MSB)
- Volvo Technology, Chalmers, SAAB and transport/shipping partners
- Goals:
  - Enable supply chain visibility: deviation management, security threat identification
  - Develop a goods transport framework for intermodal communication
  - Develop a proposed standard for information exchange for

VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

Short project description

sits
Secure Intermodal Transport System

MSB and other authorities want to track dangerous goods and other sensitive transports:

- Full control and surveillance of transports
- Risk planning
- Accident prevention – limiting damage and consequences
- Planning of rescue operations
- Prevention of antagonistic threats (security)

MSB Myndigheten för samhällsskydd och beredskap

VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

Allt för enkelt att stjäla transportgods i Sverige

Stölder av transportgods är ett stort problem som i Sverige beräknas omsätta över en miljard kronor årligen.

Den 18 oktober tillägnade SecurityUser en halvdagskonferens på Rica Talk Hotel i Älvsjö kring just denna problematik.

Det är för enkelt att stjäla transportgods idag, hävdade Luca Urciuoli, teknologie doktor i teknisk logistik vid Lunds tekniska högskola och fick medhåll av kriminalkommissarie Per-Arne Nilsson.

Av Henrik Paulsson

Peter Jeppsson, vd för TransportGruppen, inledde konferensen om säkra godstransporter.

www.securityuser.com

Nr 6, 2011

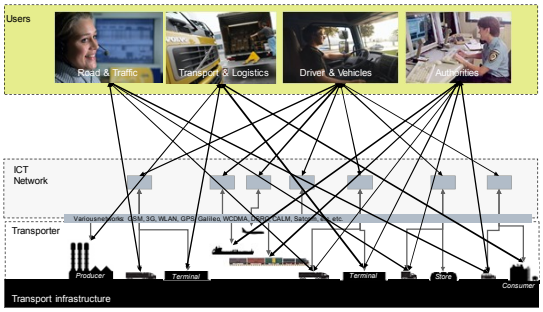
VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

Goals

- **Increase safety, security, visibility and effectiveness** within the transport supply chain
- **Protect society** from safety and security threats related to transportation of goods
- Work together with, and monitor, international standardization and harmonization projects within Intelligent Transport Systems (ITS), e.g. e-Freight
- Try to influence new standards to address safety and security threats and to satisfy all parties' need for integrity
- Develop methods for anomaly detection in ITS
- Develop a framework for increased and improved communication between involved parties
- Implement field tests with services based on the proposed framework (scenarios)

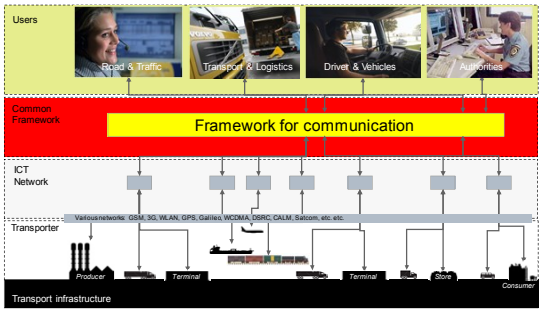
VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

Current situation



VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

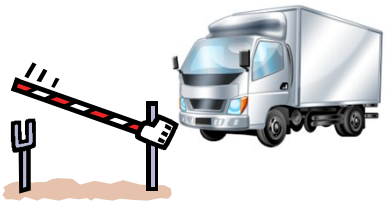
Communication with SITS framework



VOLVO CHALMERS SAAB Stena Line DSV DHL DB SCHENKER

Scenario in SITS

Automatic check-in



The vehicle automatically sends the necessary information needed to get access to the terminal area.

Minimizes need for manual administration, minimizes risk for erroneous or missing information and makes check-in more efficient.

VOLVO CHALMERS SAAB StenaLine DSV DHL DB SCHENKER

Smart Grids

Magnus Almgren
Marina Papatriantafilou

The Smart Grid: Overview

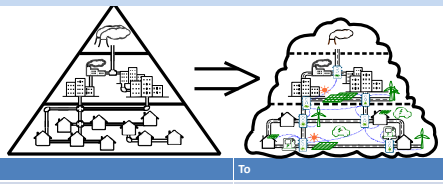
- The Smart Grid – a modernization of the electric delivery system
- Two-way flow of electricity and information with "intelligent nodes" to gain advantages from distributed computing
- But – nobody knows what it will become.
  - "like the Internet ~1990 – before Mosaic and Netscape"
- Different phases:
  - First phase: Advanced Metering Infrastructure
  - Future: Important to curb greenhouse gas emissions

Why The Smart Grid?

- New requirements on electrical systems, climate crisis driving new green technology
- New challenges:
  - Green power such as wind, ***available only at certain times***
  - Generation / load no longer fixed geographically, ***but may move*** (typically the electrical car)
- Solution: Add ICT to upgrade the grid
  - People talk about the "smart grid" but what it will entail?
  - First step is the "Smart meters," then
  - Upgrading components in the field, then
  - "apps" to control home appliances etc.

CHALMERS

SmartGrid: From "broadcasting" to "routing" of power and non-centralized coordination



From	To
Central generation and control	Distributed and central generation and control
Flow by Kirchhoff's law	Flow control (routing) by power electronics
Power generation according to demand	Fluctuating generation and demand; need for equilibrium/storage
Manual trouble response	Automatic response/islanding, predictive avoidance; advanced monitoring, situational awareness
Security needs in the power system	New security needs in the information system: operation & administration domains, "openness" (e.g. malicious/misleading sources; trust)

The Smart Grid and Security: Interdisciplinary field

- Power Engineers
  - Safety is a priority
  - Know nothing about ICT, communication or security.
  - Attitude often: But we use encryption between the devices
  - Devices last for 20—50 years
- Security Experts
  - Know very little about the physical laws and the networks
  - Little comprehension for the need to keep systems running 24/7
  - Devices updated weekly, life expentancy 3—5 years
- Security problems already demonstrated in some widely deployed devices (smart meters)
  - Can be hacked but also come with privacy concerns

The Smart Grid & Security: Threats

forward

1. Wireless attacks
   - *Threat #8:* wireless communication
2. Physical access to device
   - *Threat #17:* sensors and RFID
   - *Threat #26:* targeted attacks
3. Problems with new firmware
   - *Threat #9:* unforeseen cascading effects
   - *Threat #3:* threats due to scale
4. Other problems
   - *Threat #25:* safety takes priority



19

The Smart Grid & Security: Consequences

forward

- Electric power important for many sectors of society.
- Dependence mapped in [KBM-2007]:
  - cash payments, credit payments,
  - food sector,
  - sewage,
  - transport,
  - fuel supply,
  - primary care and care of the elderly,
  - heating, lightning, access to news (longer term)
  - cell phone communication (longer term)
- Using cyber attacks in conjunction with normal crime.

KBM-2007:En sammanfattning av rapporten: faller en – faller då alla? ISBN: 978-91-85797-24-0 20

Threats to public infrastructure

forward

New York Times: 2012-04-14:

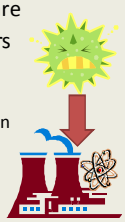
At a closed-door briefing, the senators were shown how a power company employee could derail the New York City electrical grid by clicking on an e-mail attachment sent by a hacker, and how an attack during a heat wave could have a cascading impact that would lead to deaths and cost the nation billions of dollars.

Why are these critical electrical grid computers connected to the public Internet???

http://www.nytimes.com/2012/03/14/us/new-interest-in-hacking-as-threat-to-us-security.html 21

New Era 2010: Stuxnet

- Advanced Malware
  - Target specifically Programmable Logic Controllers: Siemens SIMATIC Step 7 software
  - Lots of rumors of goal and who creators
    - designed and released by a government
      - the U.S. or Israel ???
    - **Target**: Bushehr nuclear power plant in Iran (60% of infected hosts in Iran)



Symantec oct-2010: W32.Stuxnet Dossier (http://goo.gl/pP7S)

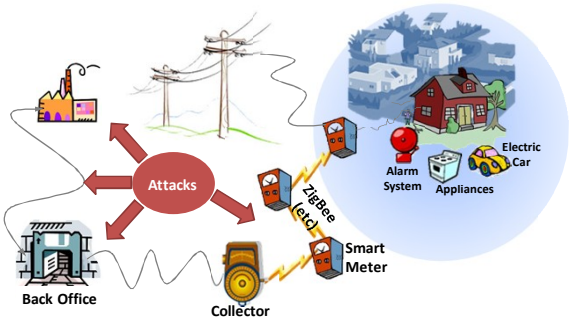
Stuxnet: Pandora's box ?

- Stuxnet is advanced and one of the first wild malware's targeting PLCs.
  - 6—8 people about 6 months to create.
- PLCs exists in many industries
  - factory assembly lines, amusement rides, or lighting fixtures.

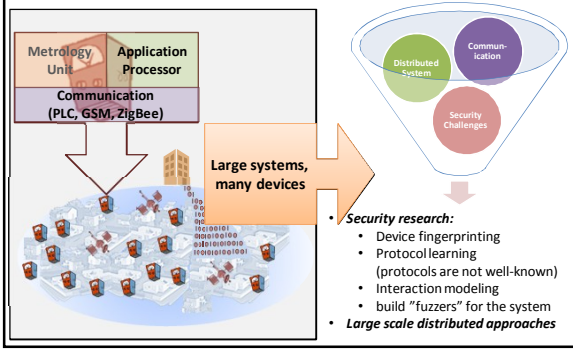
now blueprint to create malware targeting PLCs

- Compare this with the *Loveletter* virus (2000)
  - 2003/11 there existed 82 different variants of Loveletter.
  - Today: more than 5,000 attacks are carried out every day

AMI – Advanced Meter Infrastructure



AMI from an ICT Perspective



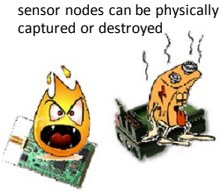
- ***Security research:***
  - Device fingerprinting
  - Protocol learning (protocols are not well-known)
  - Interaction modeling
  - build "fuzzers" for the system
- ***Large scale distributed approaches***

Secure and Fault-tolerant Sensor Networks

Andreas Larsson
Philippas Tsigas
Elad Schiller

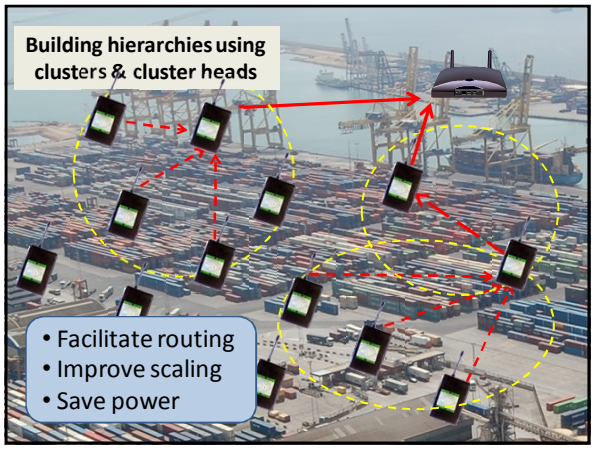
Secure and Fault-tolerant Sensor Networks

- Nodes get lost (unattended environments)
- Harsh environments
- Batteries run out
- Adversarial attacks
  sensor nodes can be physically captured or destroyed

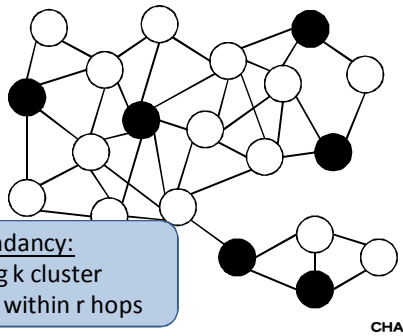


- Forging/modifying messages
- Denial of Service (DoS)
- Pulse-delay attacks
- Sybil attacks
  - Multiple identities

CHALMERS



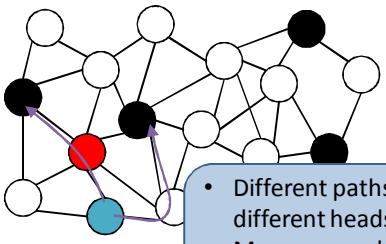
Routing through (k,r)-clustering



Redundancy:
Having k cluster heads within r hops

CHALMERS

Redundancy for security



- Different paths to different heads
- Message reaches some head
- Resilient routing

Thank you!

- Securing the connected car
- Security Metrics and Modeling
- IDS Systems
- Mitigating Distributed Denial of Service (DDoS) attacks
- Network defense against Spam
- SITS – Secure Intermodal Transport Systems
- Smart Grids
- Secure and Fault-tolerant Sensor Networks

CHALMERS