# Building Networked Systems Security

EP2520 (MSc), EP3250 (PhD)

Period 3, 2022

Panos Papadimitratos

Networked Systems Security Group

www.eecs.kth.se/nss

# Building?

# Networked Systems?

Search Engines

E-Commerce

File Sharing

Email

Voice-over-IP

Video Streaming

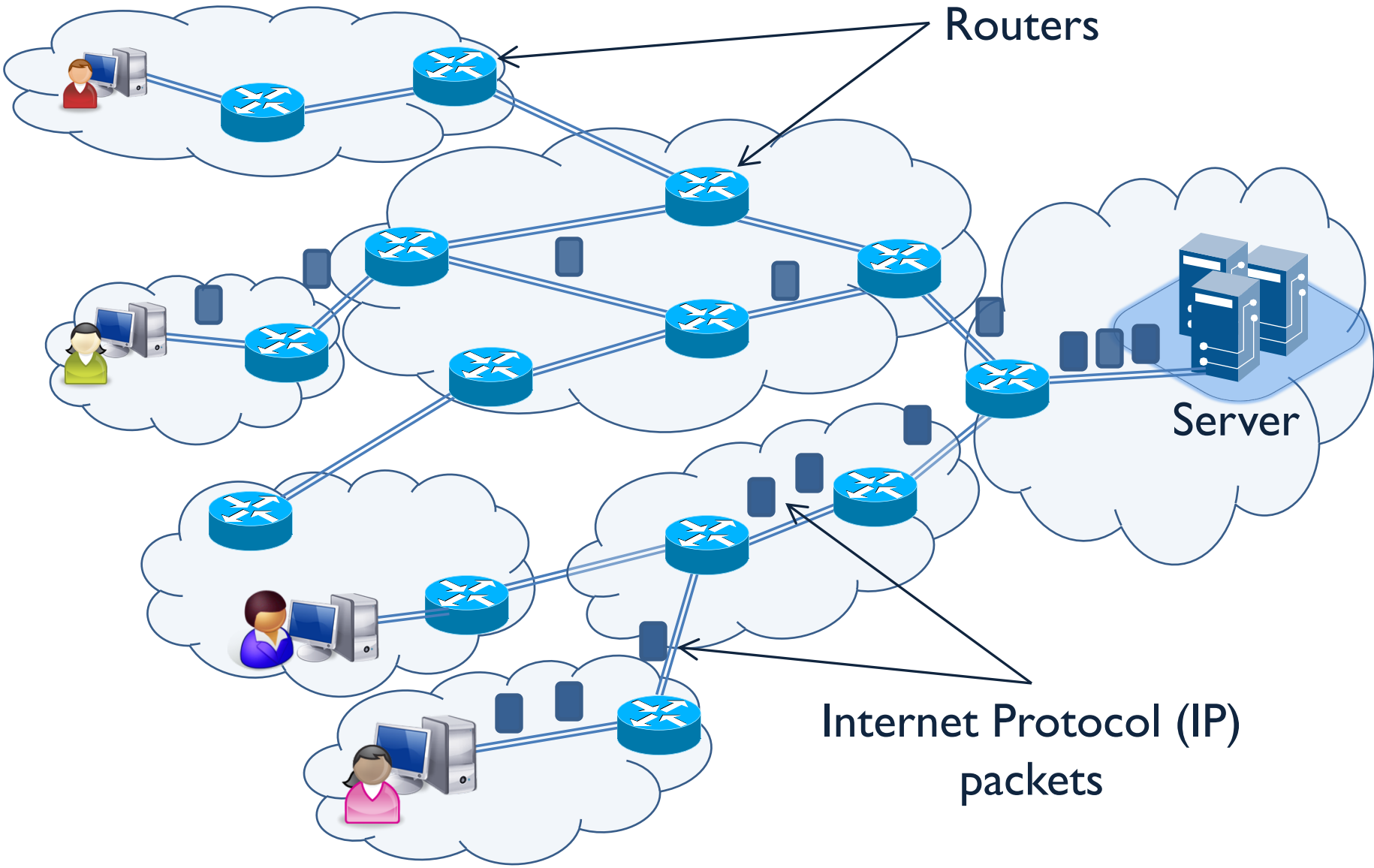
TCP/IP

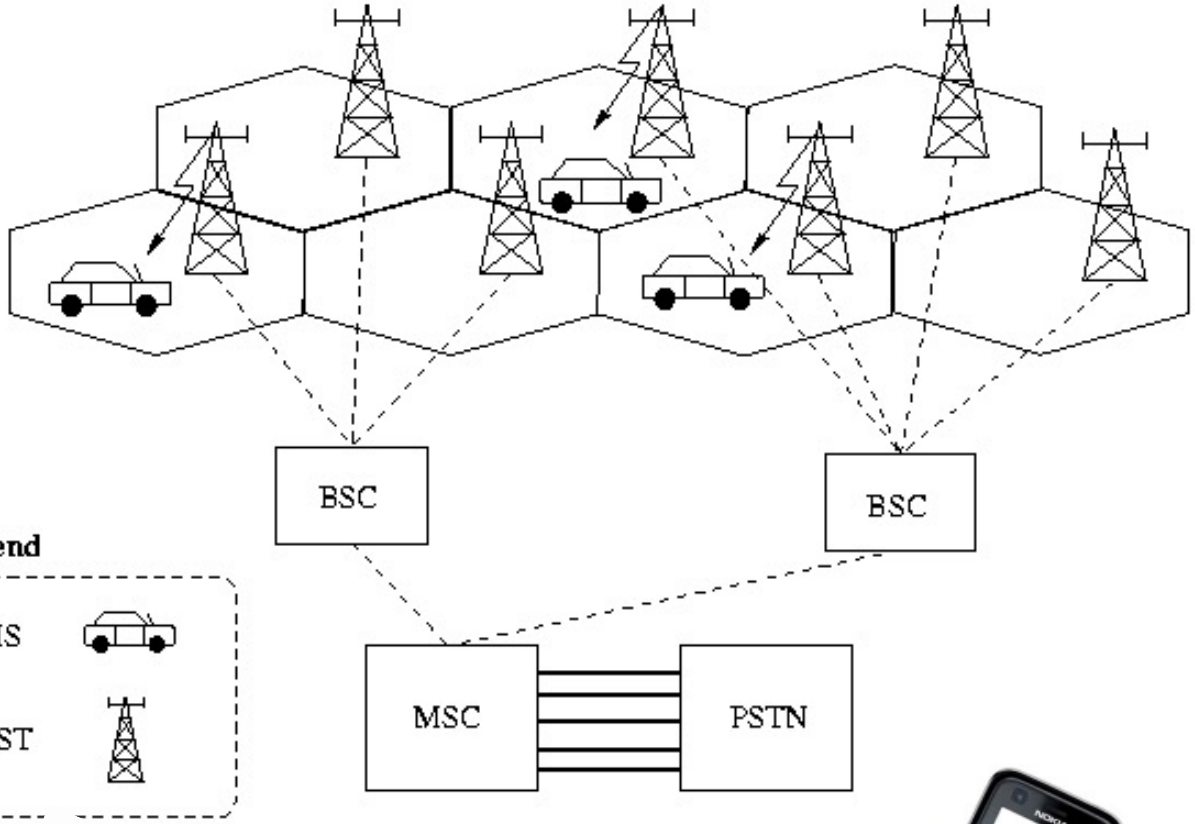
HTTP

SMTP

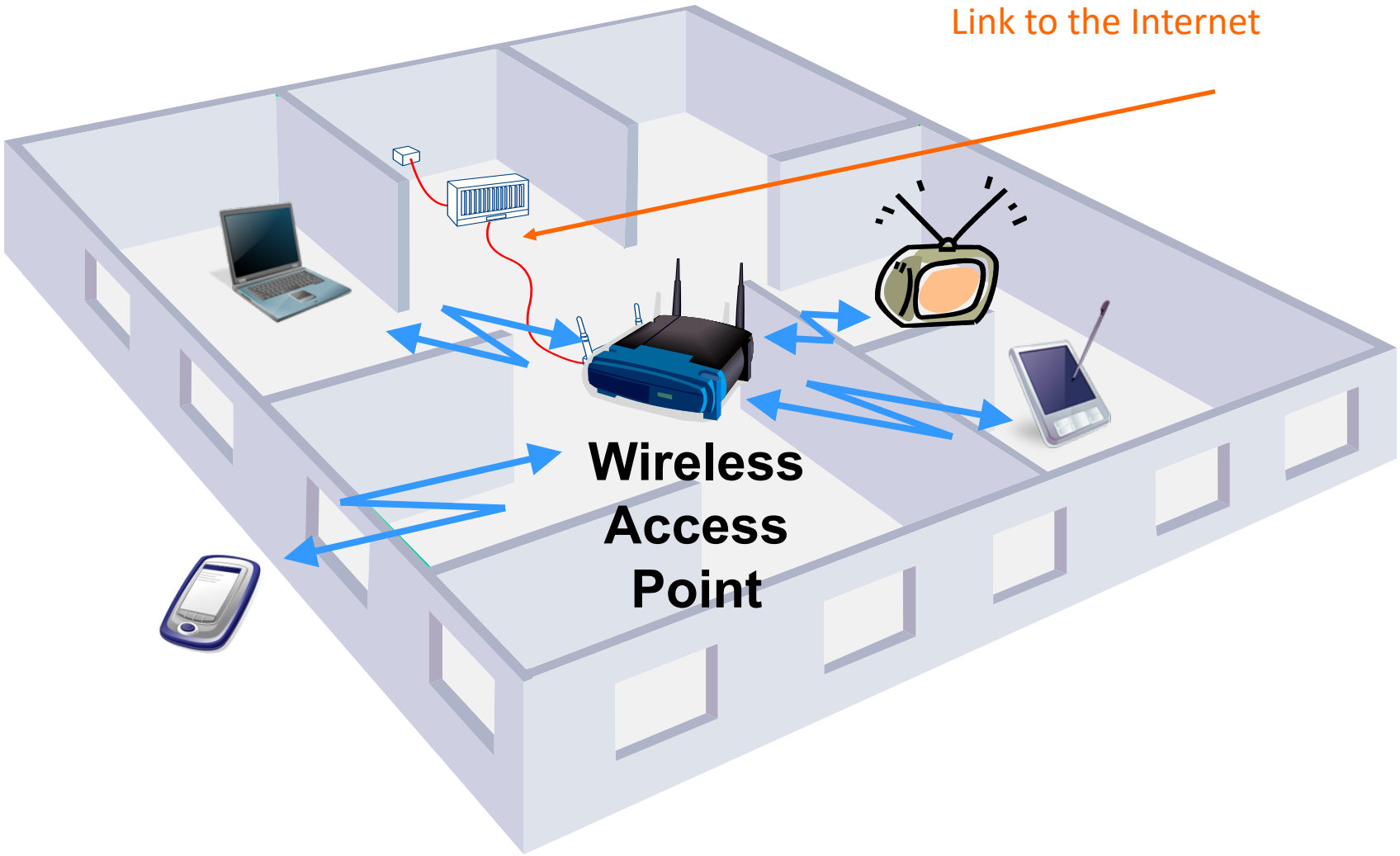
FTP

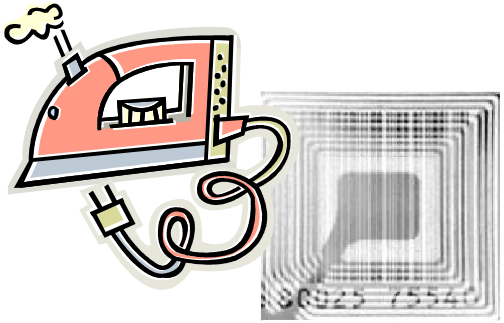
SSL


Routers
Server
Internet Protocol (IP)
packets


BSC
BSC
Legend
MS
BST
MSC
PSTN


NOKIA


Link to the Internet
Wireless
Access
Point



tagged object

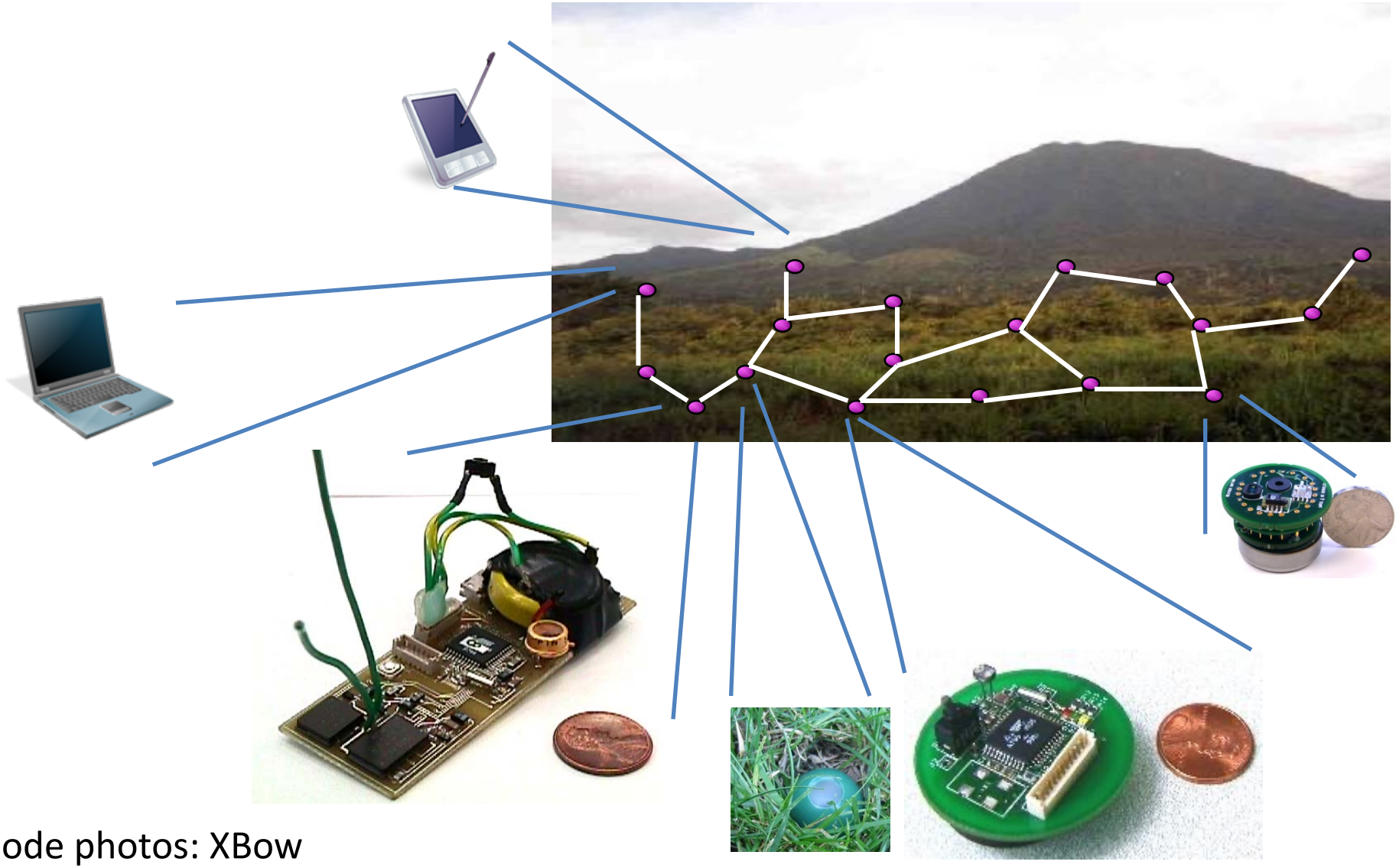
Reading signal

ID

ID

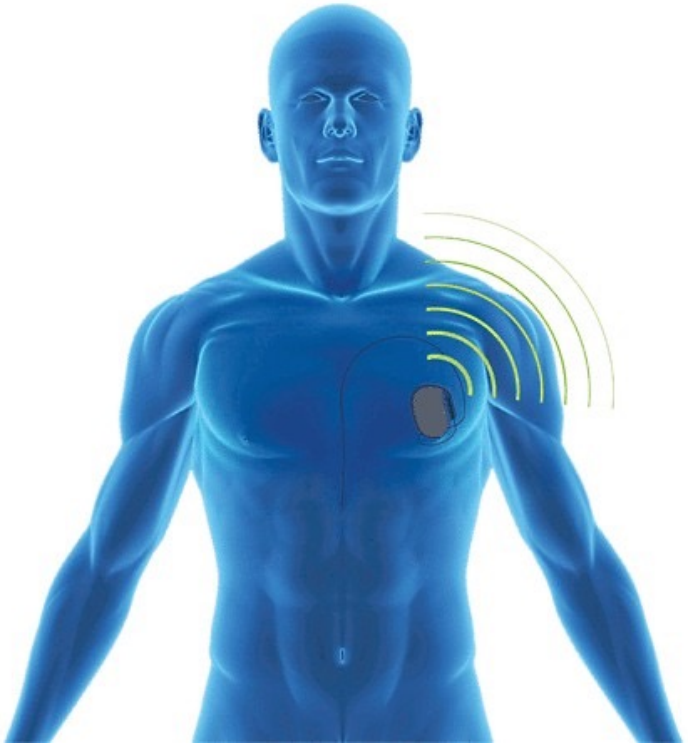
Detailed object information

Back-end database

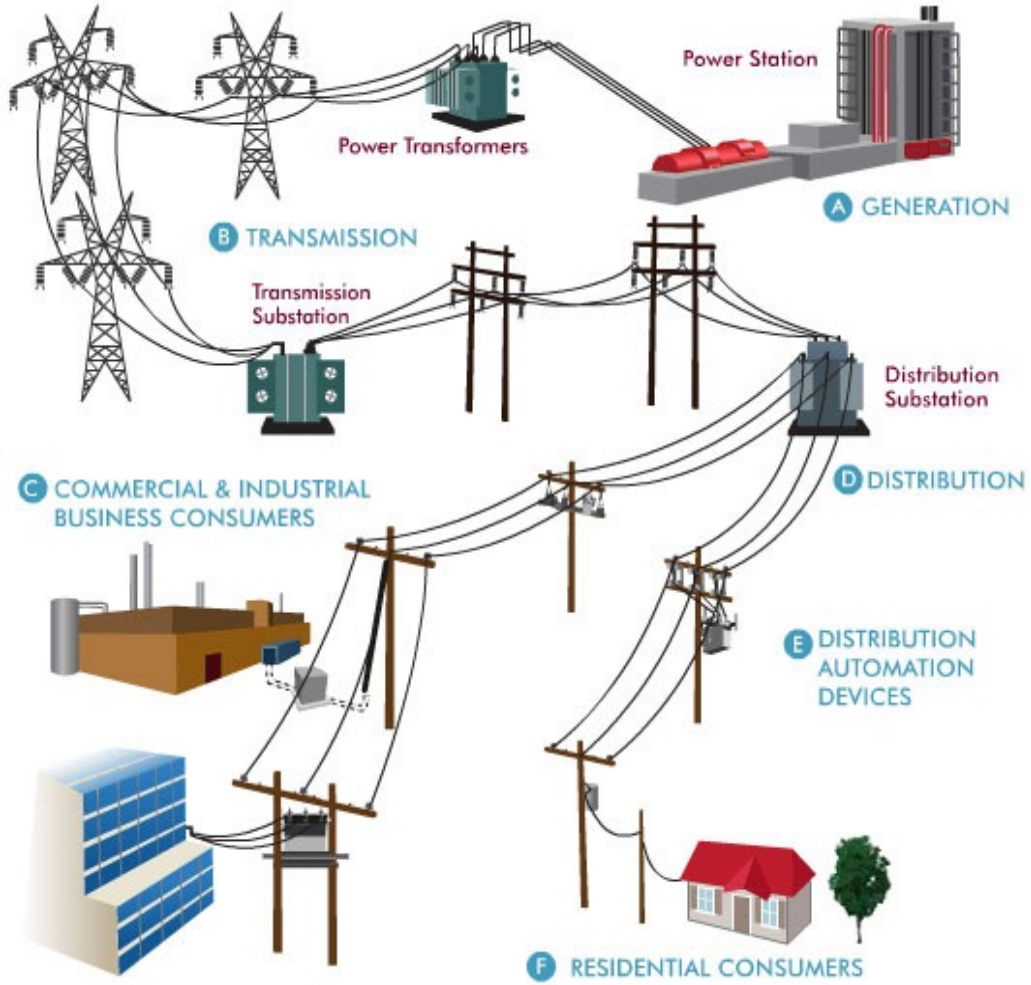


Node photos: XBow

# Wireless Sensors

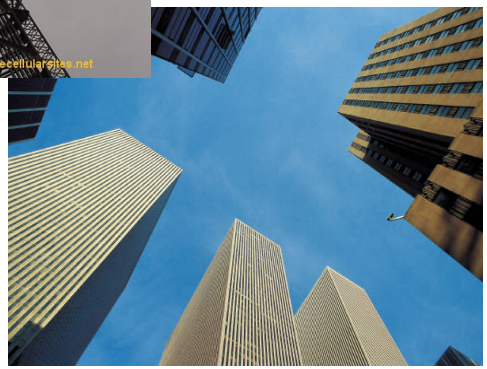


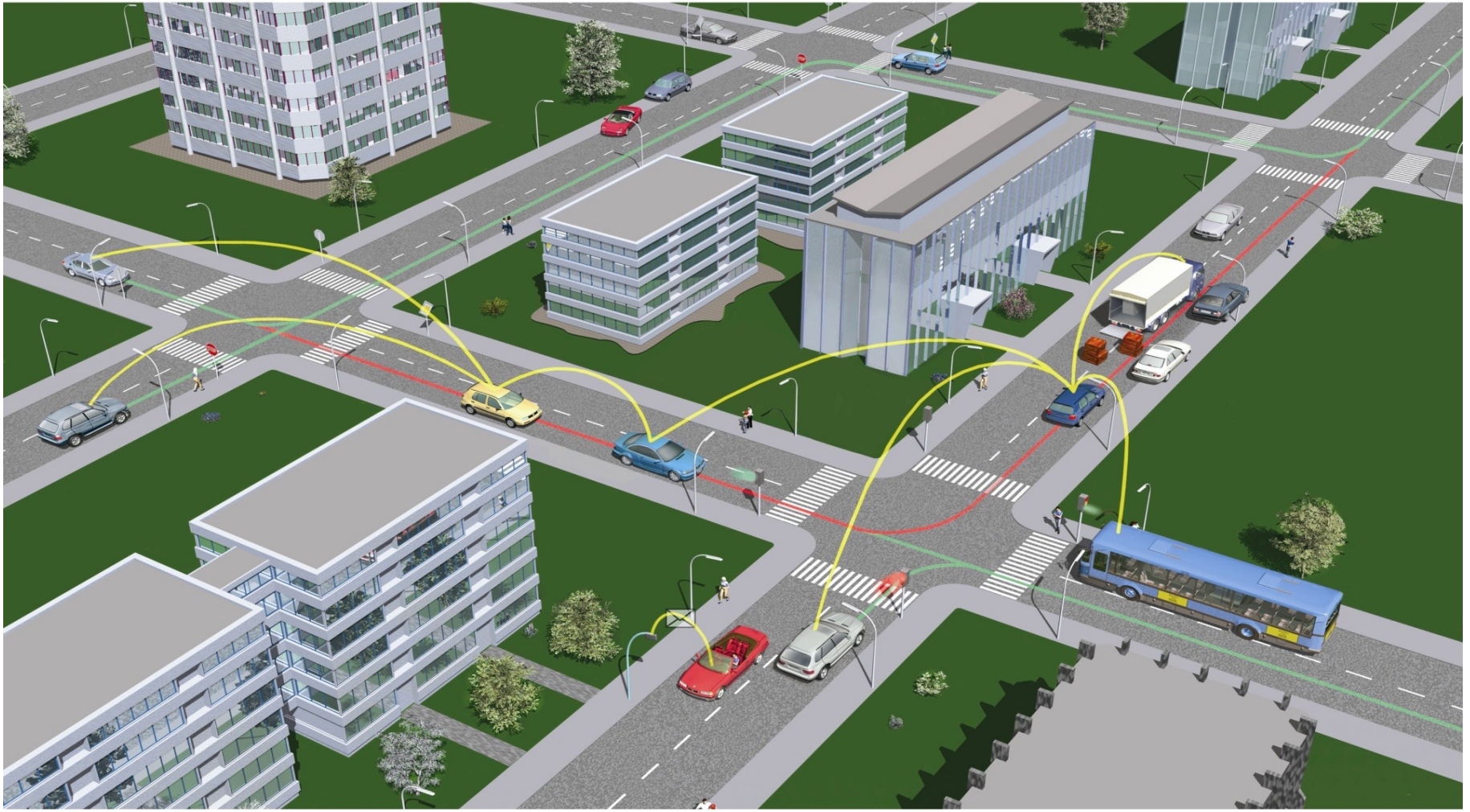

Online health record Connected device Medical device


Power Station
Power Transformers
A GENERATION
B TRANSMISSION
Transmission Substation
Distribution Substation
C COMMERCIAL & INDUSTRIAL BUSINESS CONSUMERS
D DISTRIBUTION
E DISTRIBUTION AUTOMATION DEVICES
F RESIDENTIAL CONSUMERS


SMARTHOME


THALES






Security?


Log in
Username:
password:

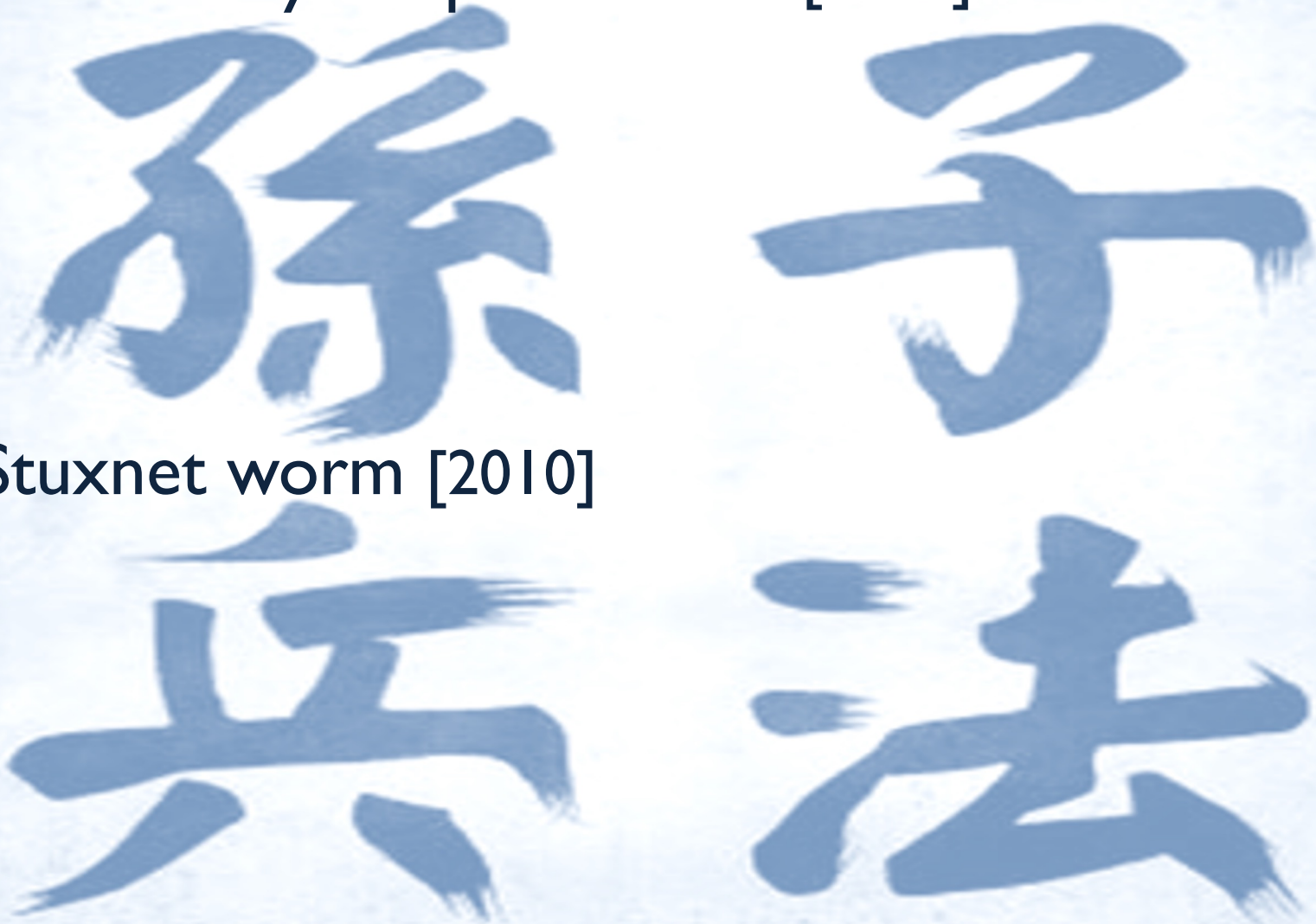

eset
AhnLab
McAfee
avast!
PANDA
SECURITY
G DATA
Quick Heal
Norton
from symantec
RISING
LION STRONG SECURITY
F-SECURE
TREND
MICRO
webroot
ca
bitdefender
Sunbelt Software
KASPERSKY lab
AVG
AntiVirus


SPAM
SPAM
SPAM
SPAM


SPAM

Estonian cyberspace attack [2007]

Stuxnet worm [2010]



# Networked Systems Security

# Networked Systems Security

- How to secure networked systems?

- Emphasis on concepts across technologies
- Contemporary and emerging technologies

# Networked Systems Security (cont'd)

- Attacks - adversarial behavior
  - Adversary
    - Has/introduces own devices/nodes in the system
    - Compromises devices/nodes already in the system
  - Adversarial devices
    - Do not do what they were supposed to do
    - Do not do what benign, correct devices do

# Networked Systems Security (cont'd)

- The legitimate user(s) may
  - Loose part or all of their data
  - Get meaningless/fake data
  - Loose control of the networked system operation
  - …

**Disruption, manipulation, destruction: Unacceptable!**

**Prevent and manage adversarial behavior!**

# Networked Systems Security (cont'd)

- Decide what adversary you fight against
- Bring in new tools, e.g., cryptography

**Security is much more than cryptography!**

# Networked Systems Security (cont'd)

- Decide 'who' can trust 'who'
- Design new protocols
- Re-design your existing protocols
  - Add security
  - Possibly disable functionality

# Networked Systems Security (cont'd)

- Make sure that the secure(d) protocols work
  - Do applications still do what they are supposed to?
  - Why? Because security can always add complexity
- Prove they are secure

# Building Networked Systems Security (BNSS)

- All the above steps to design a secure solution

AND

- Implement your solutions
- Verify
- Evaluate

# BNSS (cont'd)

- Wireless and wire-line security
- Real-world technologies
- Real-world problems
- Real-world solutions
  - Implemented and demonstrated by you

# BNSS (cont'd)

- Fully project-based course
- [Weeks 3-4] Lectures/meetings on the necessary elements, material online earlier
- [Week 5-10] Project work exclusively

# BNSS (cont'd)

- [Week 10] Finalization of your work
- [Week 11] Presentation/demonstration of your work
- [Weeks 3-11]
  - Flexible schedule
  - Team-work
  - Meetings with the teaching team
    - Get support
    - Post questions on CANVAS (per group, closed or the whole class)
    - Meet by appointment

# BNSS (cont'd)

- Grading
  - MSc: Letter grade
  - PhD: Pass/Fail
- Project deliverables
  - Reports
  - Implementation
  - Documentation
  - Demonstration/Presentation

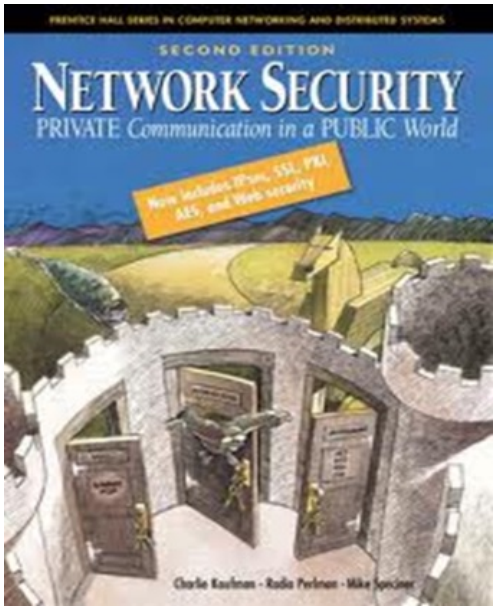
# BNSS (cont'd)

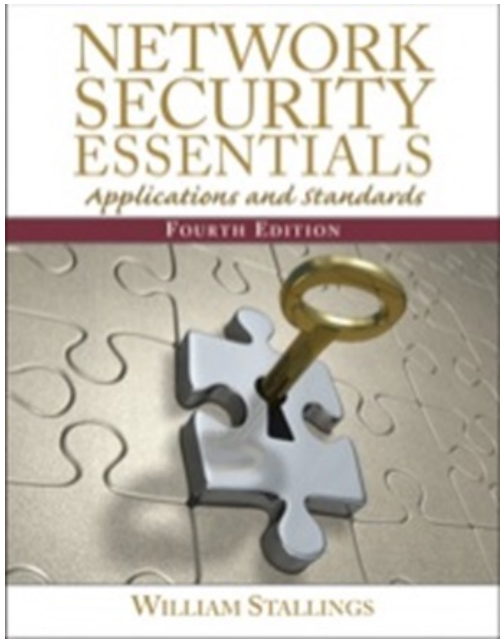
- Teaching team
  - Cihan Eryonucu
  - Hongyu Jin
  - Iraklis Symeonidis
  - Marco Spanghero
  - Di Wu

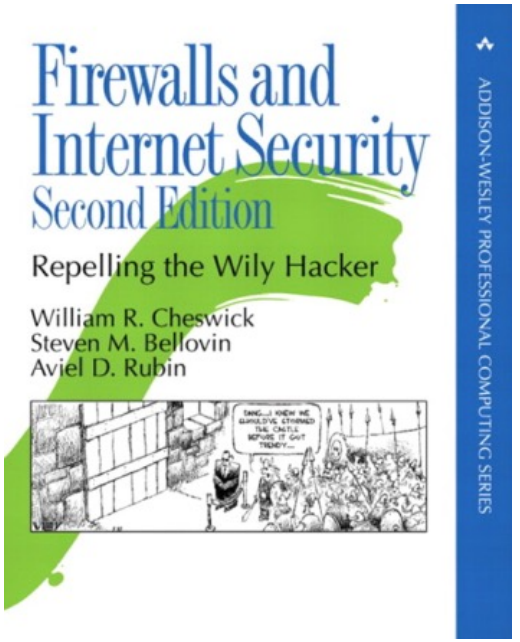
# BNSS (cont'd)

- Course material
  - Slides
  - Reading material
  - Three optional text books
    - You probably have from previous courses

# BNSS (cont'd)




- Feel free to buy 0-3 books

# BNSS (cont'd)

- Canvas: https://canvas.kth.se/courses/31545

Let's look at the project!

# BNSS (cont'd)

- Choose the default topic or
  - You can make your own proposal
    - Instead of the course-defined project
    - Or in addition to the project
  - Proposed design due at the same time as the initial design
    - Could be an ANSS continuation
  - Review and revision shortly after
  - Present/defend at the end of the term

# BNSS (cont'd)

- Next steps
  - Sign up and pick your team: *Now*
  - Form your teams: ASAP, latest by end of week 4
  - Project description: default project available!
  - Propose your own project: Week 4
    - Conclude on the topic early in Week 5
  - Attend lectures/meetings
  - Use the bookings as you wish through the period
  - Sign out your equipment: *Week 5 or 6*
    - *Note: access to VMs will be available to you once you have your team ready!*
  - *Start diving into the details and the implementation as early as possible!*

# Building Networked Systems Security

EP2520 (MSc), EP3250 (PhD)

Period 3, 2022

Panos Papadimitratos
Networked Systems Security Group
www.eecs.kth.se/nss