A Holistic Approach to Security Attack Modeling and Analysis

Tong Li, Elda Paja,
and John Mylopoulos
University of Trento

Jennifer Horkoff
City University London

Kristian Beckers
Technische Universität
München

8th International i* Workshop (iStar'15),
Ottawa, Canada

August 24th, 2015

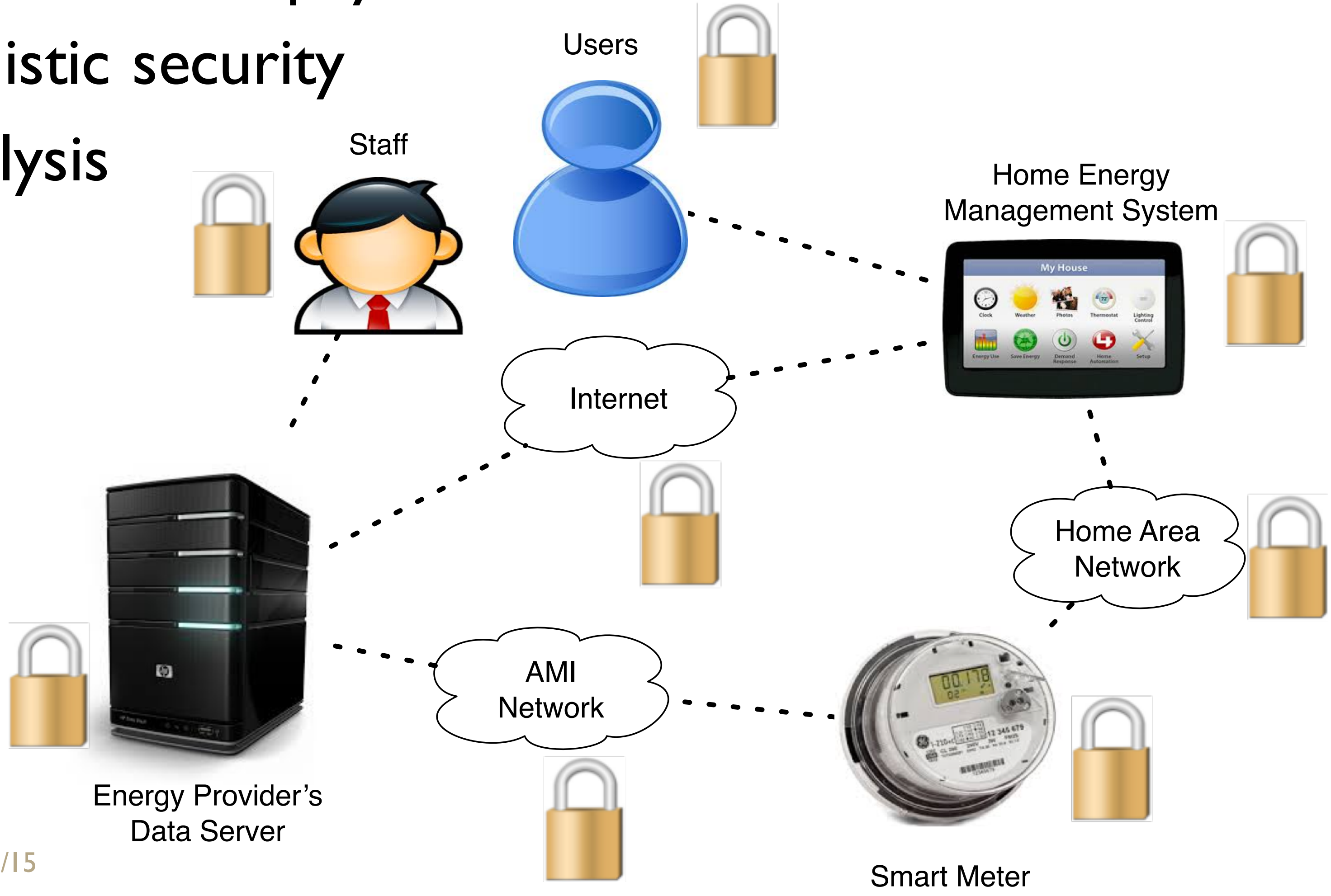
i* '15 EIGHTH
INTERNATIONAL
i* WORKSHOP

Outline

- Background
  - Motivation
    - Holistic security requirements analysis
  - Research outline
  - Challenges
    - Security attack analysis
- Proposal
  - A holistic security attack analysis framework
- Future Work
- Summaries

Motivation

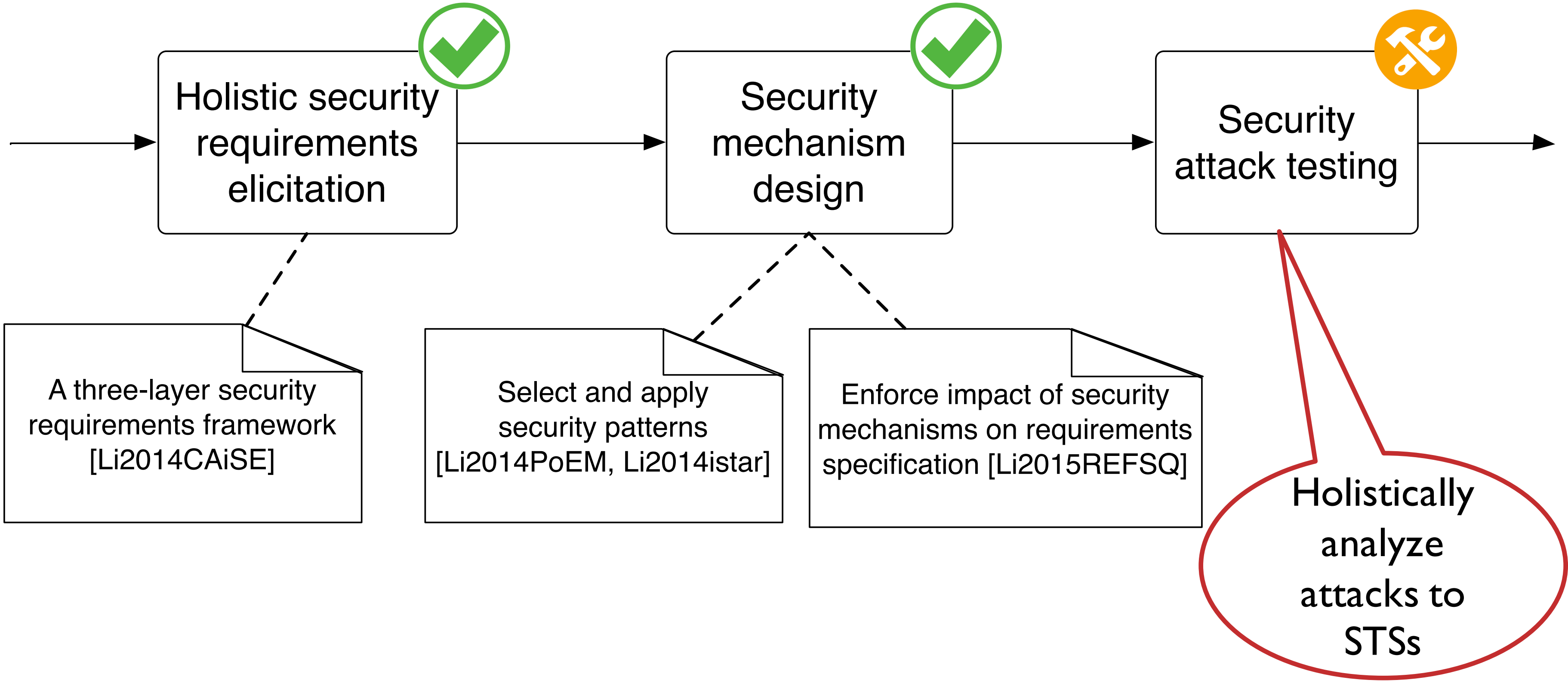
- Socio-Technical Systems (STSs) consist of human, software, and physical infrastructure
- Holistic security analysis



24/08/15

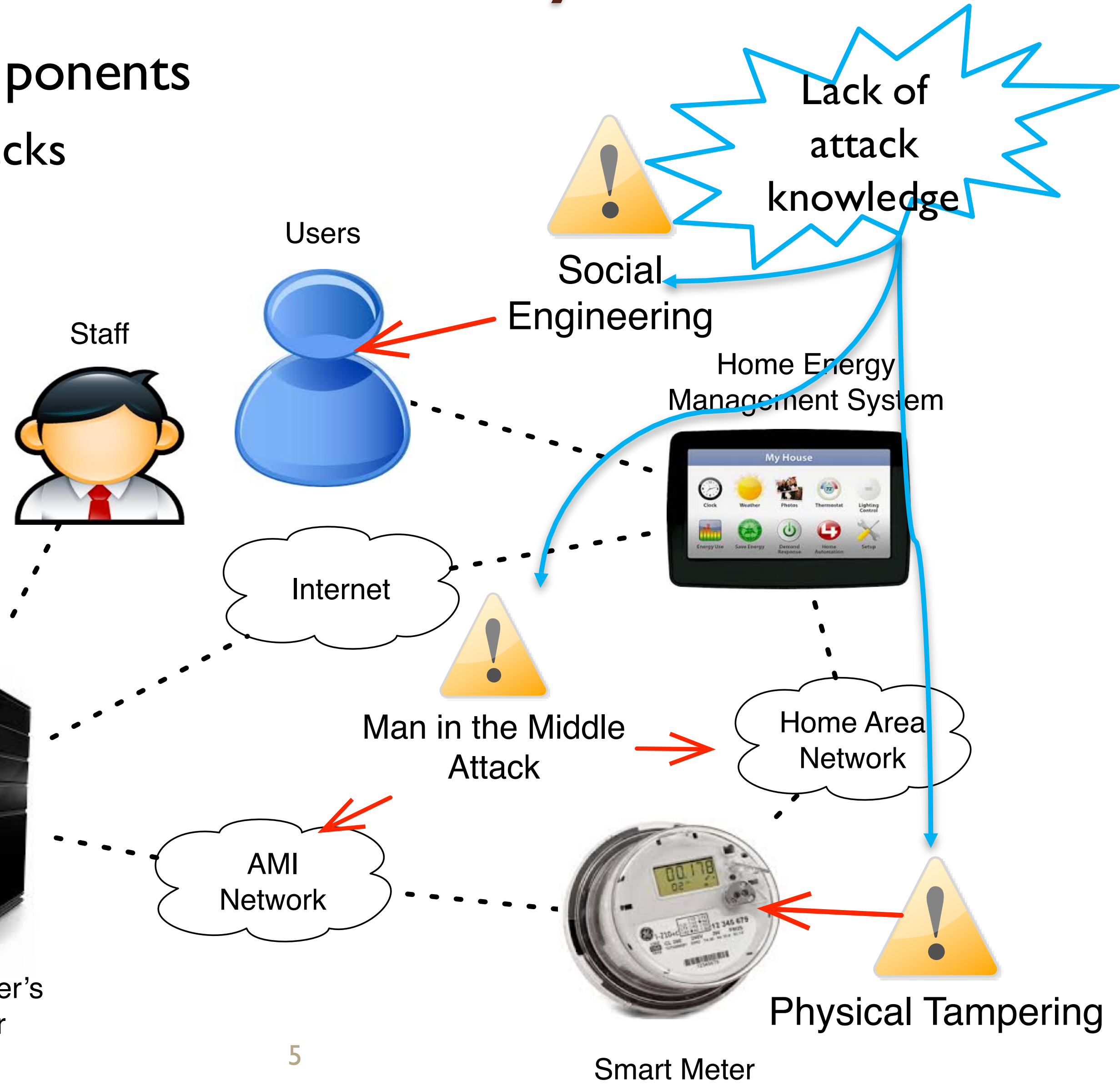
Research outline

- A Holistic security requirements analysis framework


Holistic security requirements elicitation
✓
Security mechanism design
✓
Security attack testing
A three-layer security requirements framework [Li2014CAiSE]
Select and apply security patterns [Li2014PoEM, Li2014istar]
Enforce impact of security mechanisms on requirements specification [Li2015REFSQ]
Holistically analyze attacks to STSs

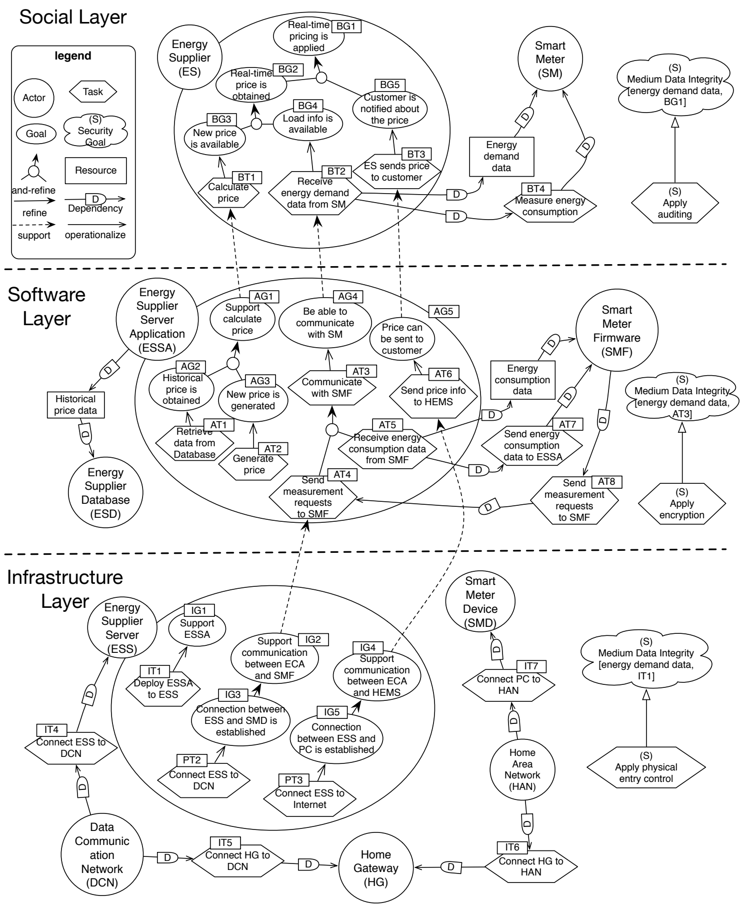
Challenges for attack analysis of STSs

- Heterogeneous components
  - A broad scope of attacks
- Multistage attacks
  - Difficult to detect
- Lack of attack knowledge



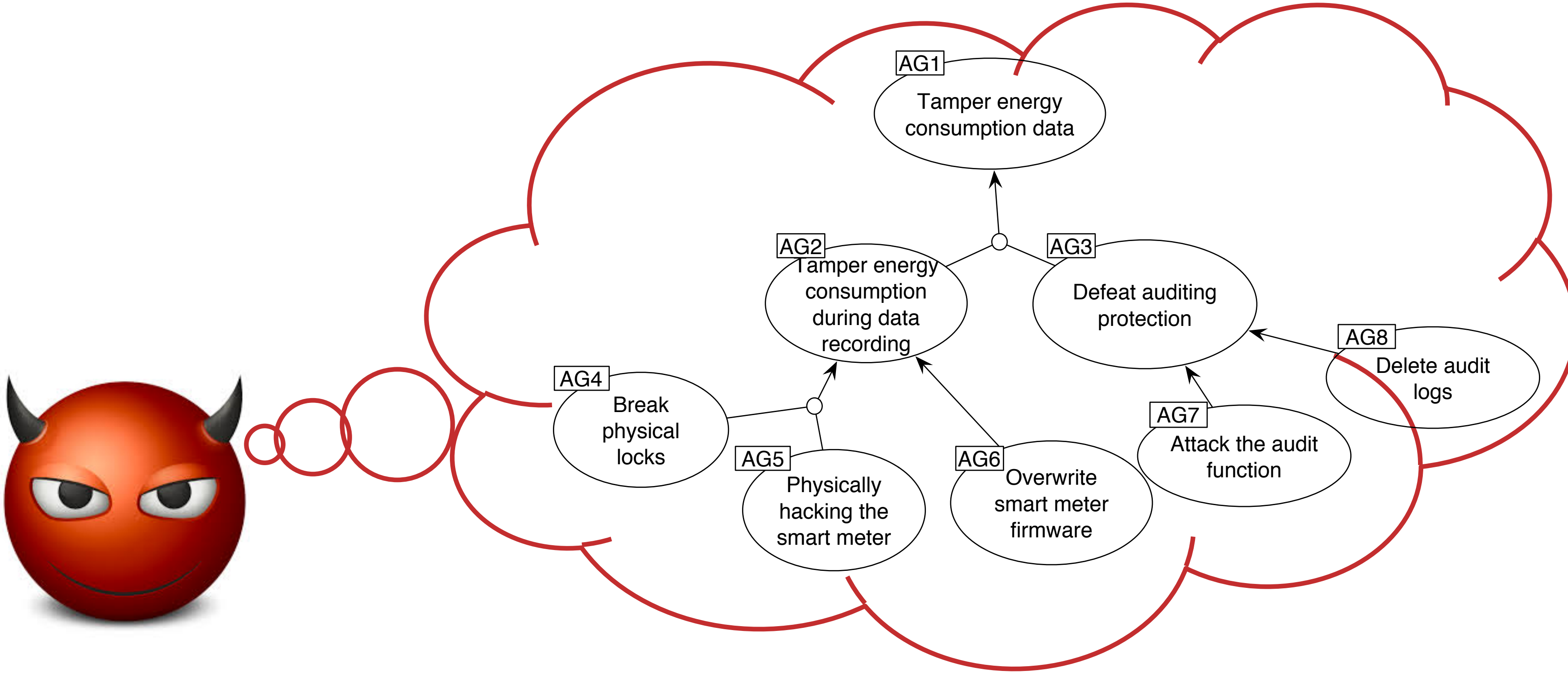
Solutions

Challenges	Solutions
Heterogeneous components	**Based on a three-layer requirements framework [Li2014CAiSE]**: • Business processes • software applications • physical infrastructure


Social Layer
legend
Actor
Task
Goal
(S) Security Goal
Resource
and-refine
refine
D
Dependency
support
operationalize
Energy Supplier (ES)
Real-time pricing is applied
BG1
Real-time price is obtained
BG2
BG3
New price is available
BG4
Load info is available
BG5
Customer is notified about the price
BT1
Calculate price
BT2
Receive energy demand data from SM
BT3
ES sends price to customer
D
D
Energy demand data
Smart Meter (SM)
D
D
BT4
Measure energy consumption
(S) Medium Data Integrity [energy demand data, BG1]
(S) Apply auditing
Software Layer
Energy Supplier Server Application (ESSA)
AG1
Support calculate price
AG4
Be able to communicate with SM
AG5
Price can be sent to customer
AG2
Historical price is obtained
AG3
New price is generated
AT3
Communicate with SMF
AT6
Send price info to HEMS
AT1
Retrieve data from Database
AT2
Generate price
AT5
Receive energy consumption data from SMF
AT4
Send measurement requests to SMF
D
Historical price data
D
Energy Supplier Database (ESD)
Energy consumption data
D
D
Smart Meter Firmware (SMF)
D
D
AT7
Send energy consumption data to ESSA
D
D
AT8
Send measurement requests to SMF
(S) Medium Data Integrity [energy demand data, AT3]
(S) Apply encryption
Infrastructure Layer
Energy Supplier Server (ESS)
IG1
Support ESSA
IT1
Deploy ESSA to ESS
IG2
Support communication between ECA and SMF
IG3
Connection between ESS and SMD is established
IG4
Support communication between ECA and HEMS
IG5
Connection between ESS and PC is established
PT2
Connect ESS to DCN
PT3
Connect ESS to Internet
D
IT4
Connect ESS to DCN
D
Data Communication Network (DCN)
D
IT5
Connect HG to DCN
D
Home Gateway (HG)
D
IT6
Connect HG to HAN
D
Home Area Network (HAN)
D
IT7
Connect PC to HAN
D
Smart Meter Device (SMD)
(S) Medium Data Integrity [energy demand data, IT1]
(S) Apply physical entry control

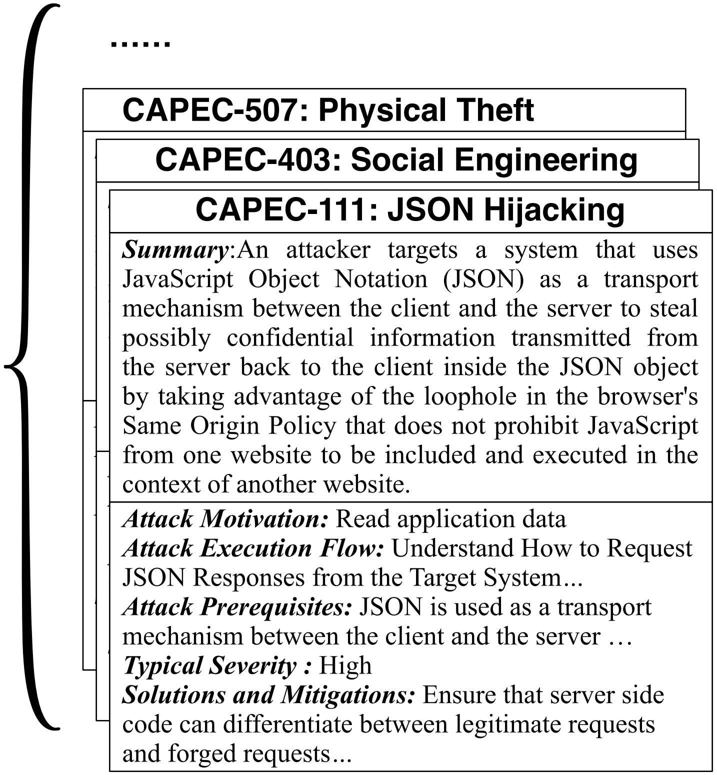
Solutions

Challenges	Solutions
Multistage attacks	**Takes an attacker's perspective**: Systematically capture and refine the attacker's anti-goals


AG1
Tamper energy consumption data
AG2
Tamper energy consumption during data recording
AG3
Defeat auditing protection
AG4
Break physical locks
AG5
Physically hacking the smart meter
AG6
Overwrite smart meter firmware
AG7
Attack the audit function
AG8
Delete audit logs

Solutions

Challenges	Solutions
Lack of attack knowledge	**Leverage attack patterns**: CAPEC (Common Attack Pattern Enumeration and Classification) • 463 patterns • Broad coverage • Detailed specification



......

CAPEC-507: Physical Theft

CAPEC-403: Social Engineering

CAPEC-111: JSON Hijacking

Summary:An attacker targets a system that uses JavaScript Object Notation (JSON) as a transport mechanism between the client and the server to steal possibly confidential information transmitted from the server back to the client inside the JSON object by taking advantage of the loophole in the browser's Same Origin Policy that does not prohibit JavaScript from one website to be included and executed in the context of another website.

Attack Motivation: Read application data
Attack Execution Flow: Understand How to Request JSON Responses from the Target System...
Attack Prerequisites: JSON is used as a transport mechanism between the client and the server …
Typical Severity : High
Solutions and Mitigations: Ensure that server side code can differentiate between legitimate requests and forged requests...

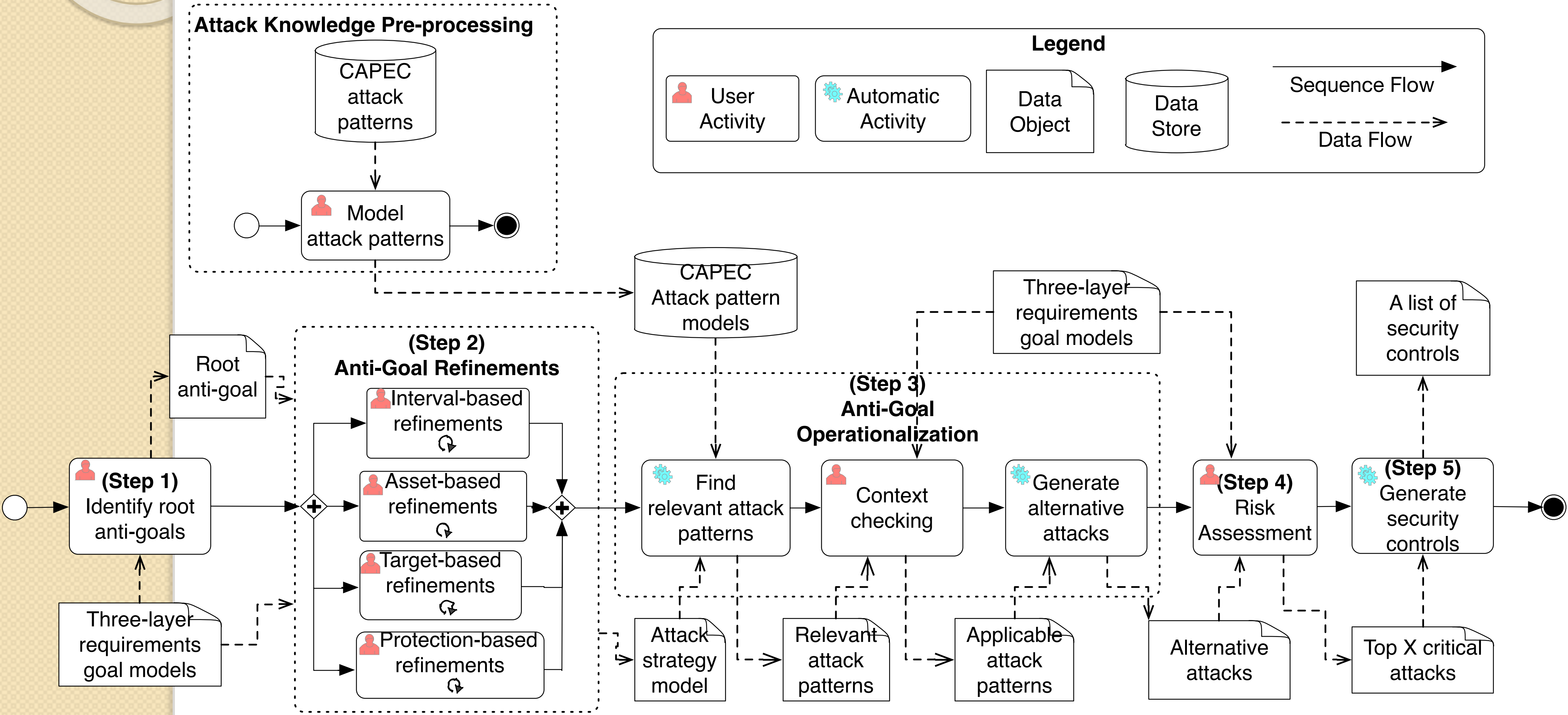
Proposal

- A holistic security attack analysis framework [Li2015REPoster]

Challenges	Solutions
Heterogeneous components	**Based on a three-layer requirements framework [Li2014CAiSE]**: Business processes, software applications, physical infrastructure
Multistage attacks	**Takes an attacker's perspective**: Systematically capture and refine the attacker's anti-goals
Lack of attack knowledge	**Leverage attack patterns**: CAPEC (Common Attack Pattern Enumeration and Classification)

Recent progress

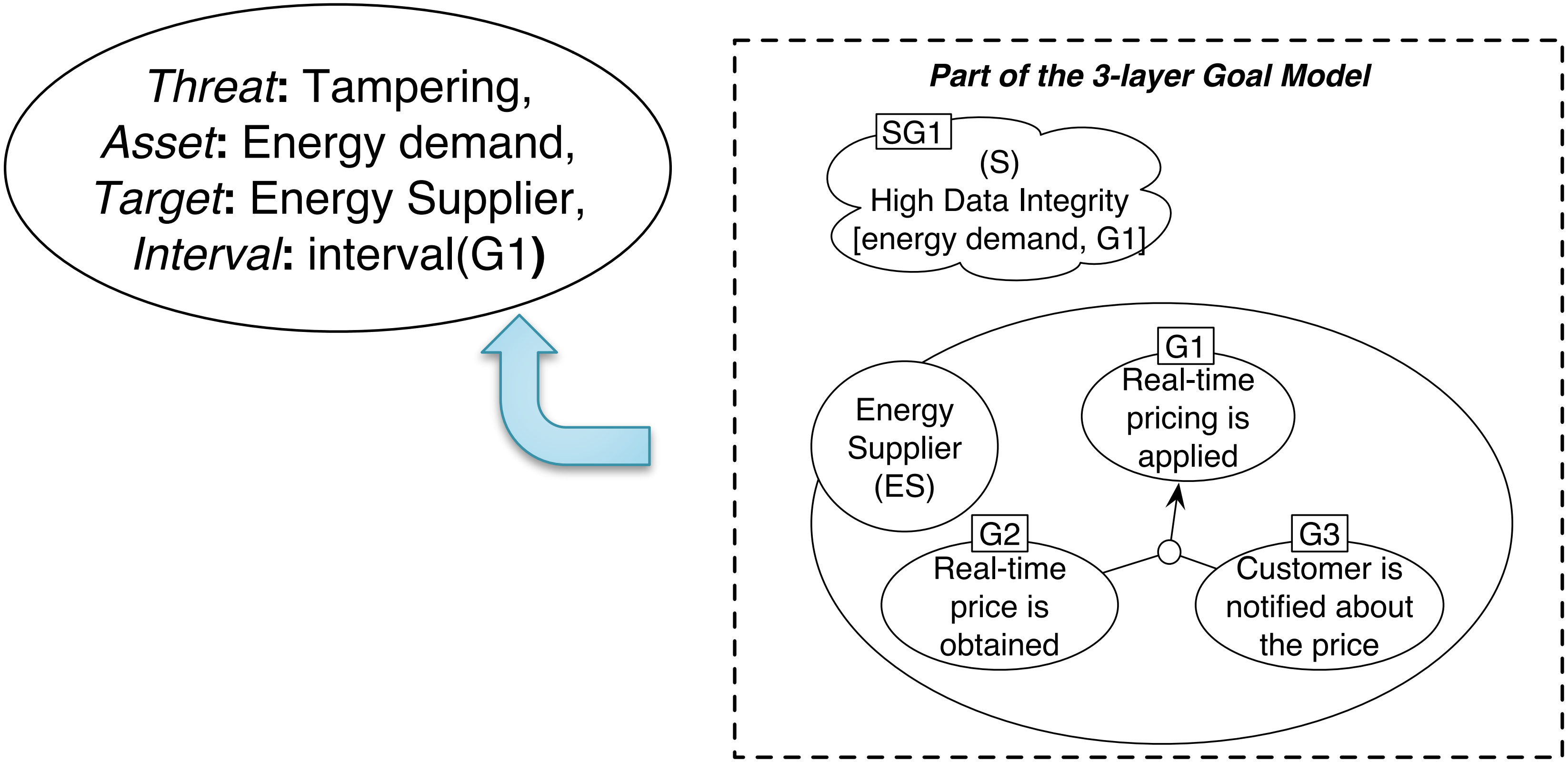
- A refined attack modeling and analysis process



Attack Knowledge Pre-processing
CAPEC attack patterns
Model attack patterns
Legend
User Activity
Automatic Activity
Data Object
Data Store
Sequence Flow
Data Flow
CAPEC Attack pattern models
Three-layer requirements goal models
A list of security controls
Root anti-goal
(Step 2) Anti-Goal Refinements
Interval-based refinements
Asset-based refinements
Target-based refinements
Protection-based refinements
(Step 3) Anti-Goal Operationalization
(Step 1) Identify root anti-goals
Find relevant attack patterns
Context checking
Generate alternative attacks
(Step 4) Risk Assessment
(Step 5) Generate security controls
Three-layer requirements goal models
Attack strategy model
Relevant attack patterns
Applicable attack patterns
Alternative attacks
Top X critical attacks

Step 1: Identify root anti-goals

- Structured anti-goals:

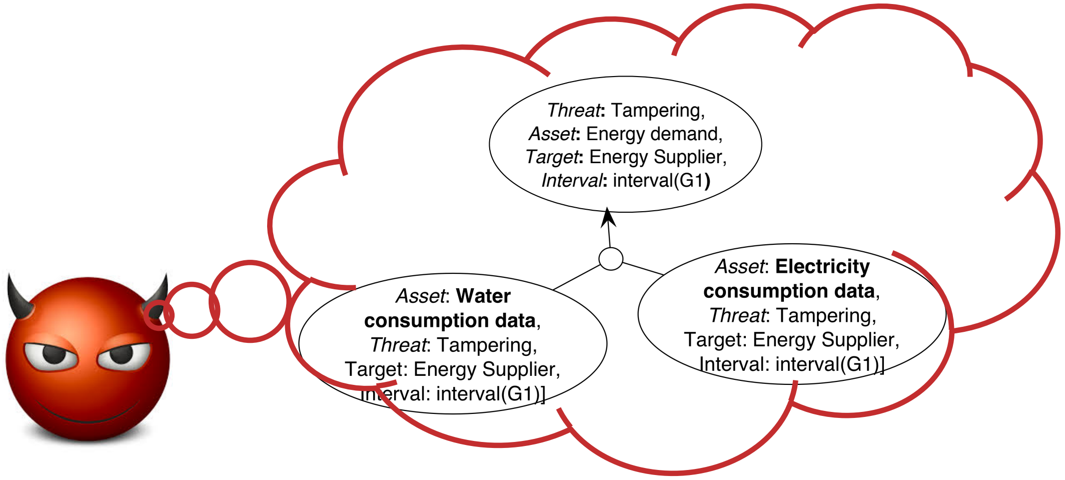


Threat: Tampering,
Asset: Energy demand,
Target: Energy Supplier,
Interval: interval(G1)

Part of the 3-layer Goal Model

SG1
(S)
High Data Integrity
[energy demand, G1]
Energy Supplier (ES)
G1
Real-time pricing is applied
G2
Real-time price is obtained
G3
Customer is notified about the price

Step 2: Anti-goal refinement



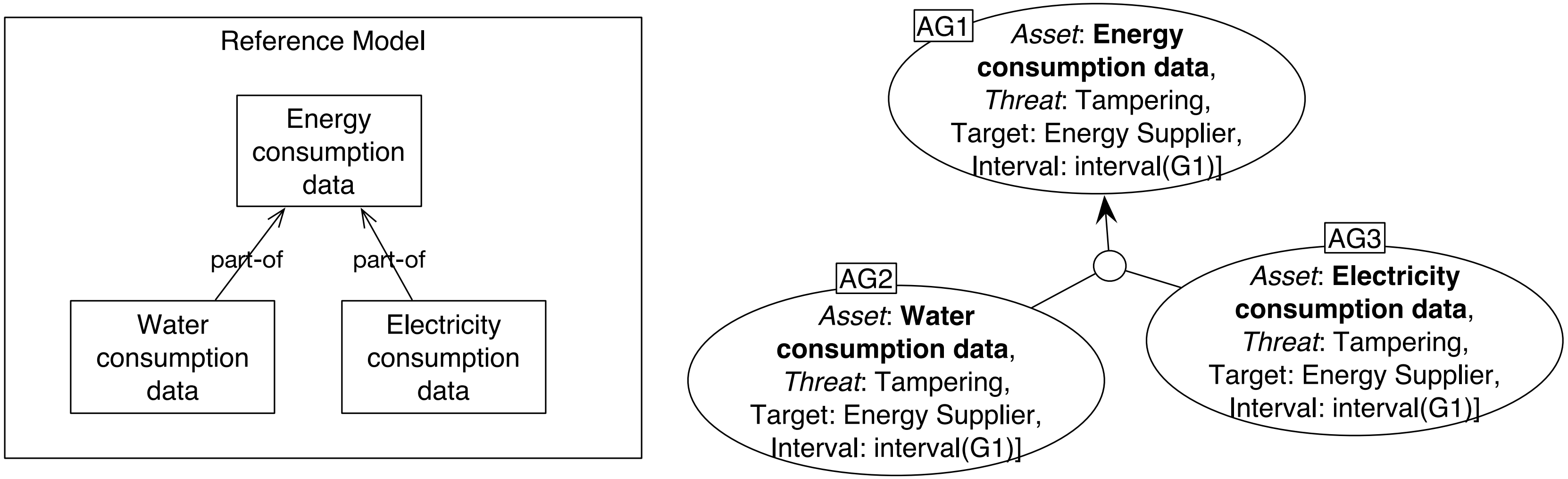
Threat: Tampering,
Asset: Energy demand,
Target: Energy Supplier,
Interval: interval(G1)

Asset: **Water consumption data**,
Threat: Tampering,
Target: Energy Supplier,
Interval: interval(G1)]

Asset: **Electricity consumption data**,
Threat: Tampering,
Target: Energy Supplier,
Interval: interval(G1)]

- Define four refinement patterns
  - Asset-based refinement
  - Target-based refinement
  - Interval-based refinement
  - protection-based refinement

Asset-based refinement



Reference Model

Energy consumption data

part-of

part-of

Water consumption data

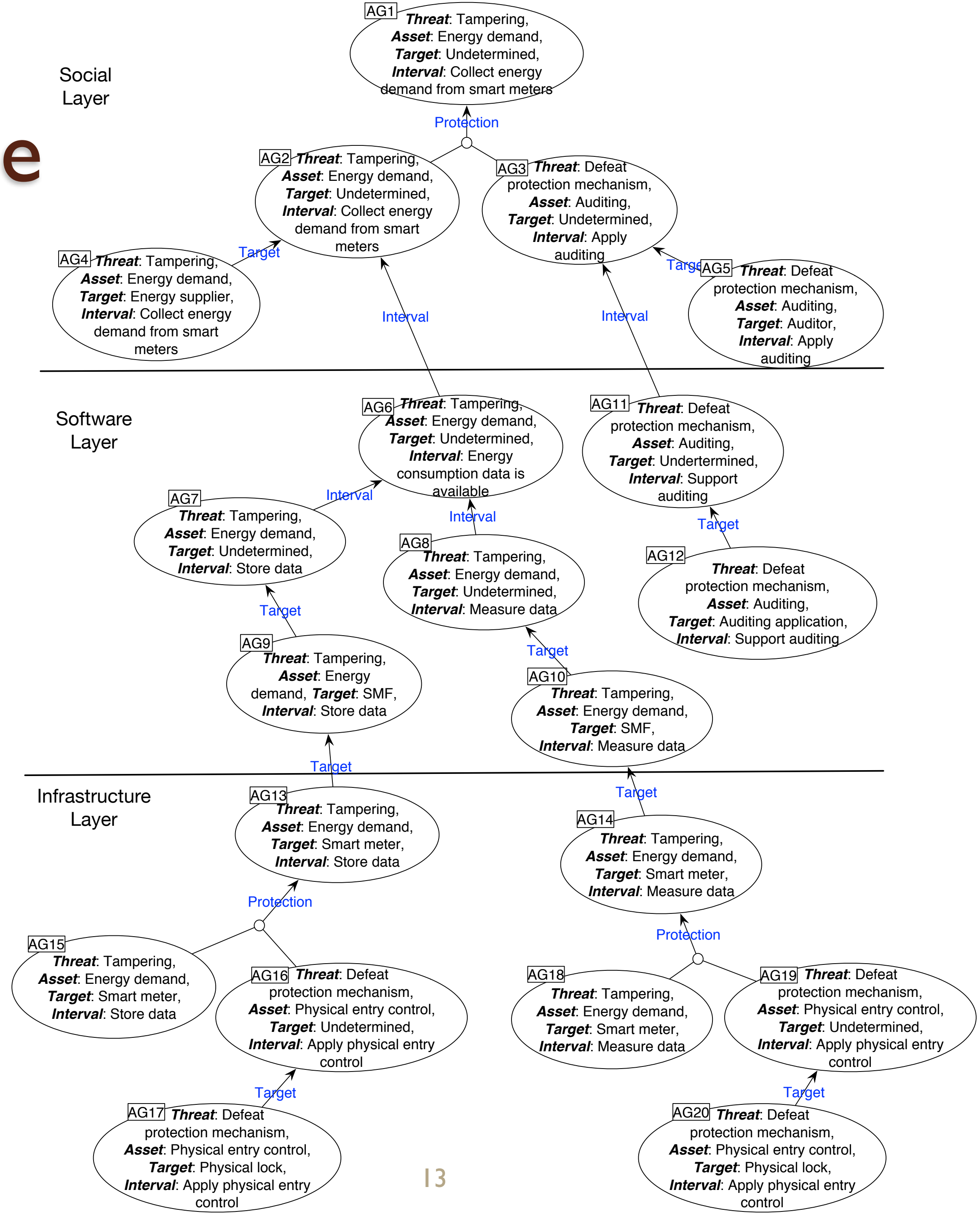
Electricity consumption data

AG1
Asset: **Energy consumption data**,
Threat: Tampering,
Target: Energy Supplier,
Interval: interval(G1)]

AG2
Asset: **Water consumption data**,
Threat: Tampering,
Target: Energy Supplier,
Interval: interval(G1)]

AG3
Asset: **Electricity consumption data**,
Threat: Tampering,
Target: Energy Supplier,
Interval: interval(G1)]

Example



Social Layer

AG1 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Undetermined, ***Interval***: Collect energy demand from smart meters

AG2 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Undetermined, ***Interval***: Collect energy demand from smart meters

AG3 ***Threat***: Defeat protection mechanism, ***Asset***: Auditing, ***Target***: Undetermined, ***Interval***: Apply auditing

AG4 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Energy supplier, ***Interval***: Collect energy demand from smart meters

AG5 ***Threat***: Defeat protection mechanism, ***Asset***: Auditing, ***Target***: Auditor, ***Interval***: Apply auditing

Software Layer

AG6 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Undetermined, ***Interval***: Energy consumption data is available

AG11 ***Threat***: Defeat protection mechanism, ***Asset***: Auditing, ***Target***: Undertermined, ***Interval***: Support auditing

AG7 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Undetermined, ***Interval***: Store data

AG8 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Undetermined, ***Interval***: Measure data

AG12 ***Threat***: Defeat protection mechanism, ***Asset***: Auditing, ***Target***: Auditing application, ***Interval***: Support auditing

AG9 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: SMF, ***Interval***: Store data

AG10 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: SMF, ***Interval***: Measure data

Infrastructure Layer

AG13 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Smart meter, ***Interval***: Store data

AG14 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Smart meter, ***Interval***: Measure data

AG15 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Smart meter, ***Interval***: Store data

AG16 ***Threat***: Defeat protection mechanism, ***Asset***: Physical entry control, ***Target***: Undetermined, ***Interval***: Apply physical entry control

AG18 ***Threat***: Tampering, ***Asset***: Energy demand, ***Target***: Smart meter, ***Interval***: Measure data

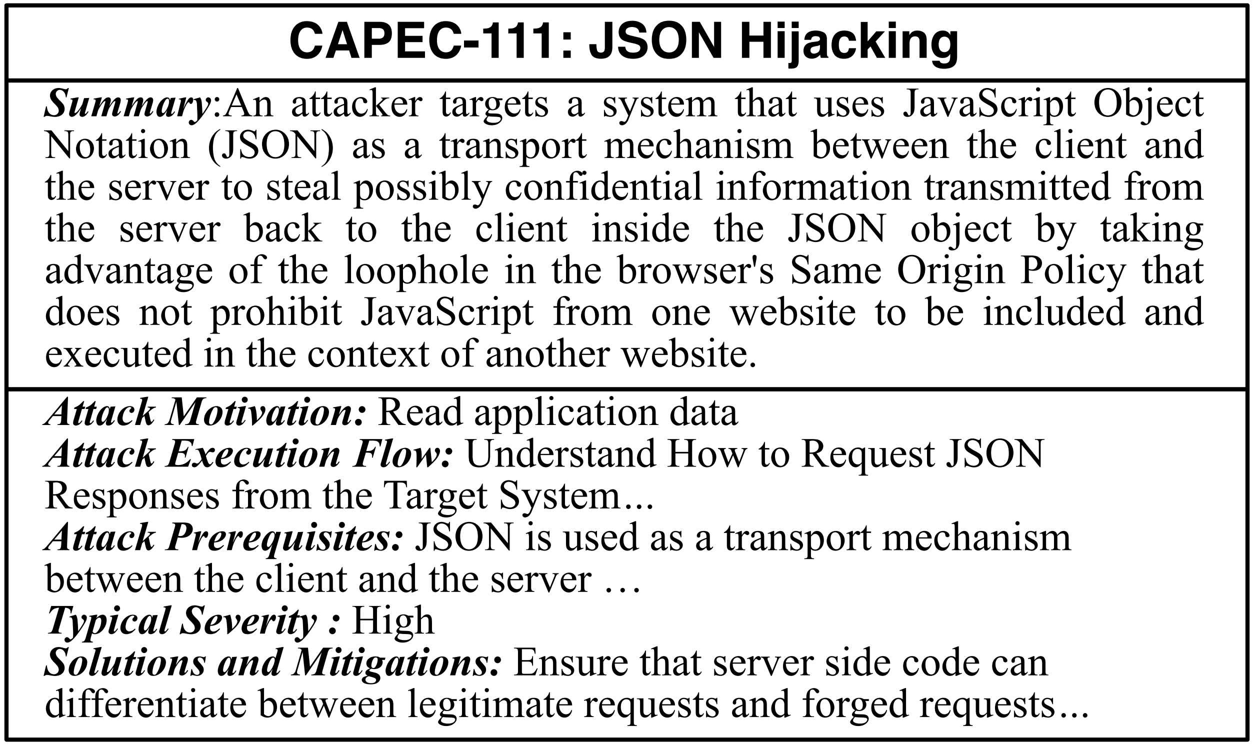
AG19 ***Threat***: Defeat protection mechanism, ***Asset***: Physical entry control, ***Target***: Undetermined, ***Interval***: Apply physical entry control

AG17 ***Threat***: Defeat protection mechanism, ***Asset***: Physical entry control, ***Target***: Physical lock, ***Interval***: Apply physical entry control

AG20 ***Threat***: Defeat protection mechanism, ***Asset***: Physical entry control, ***Target***: Physical lock, ***Interval***: Apply physical entry control

Step 3: Anti-goal operationalization

- Using CAPEC attack pattern repository
  - Includes 463 attack patterns
  - Example:



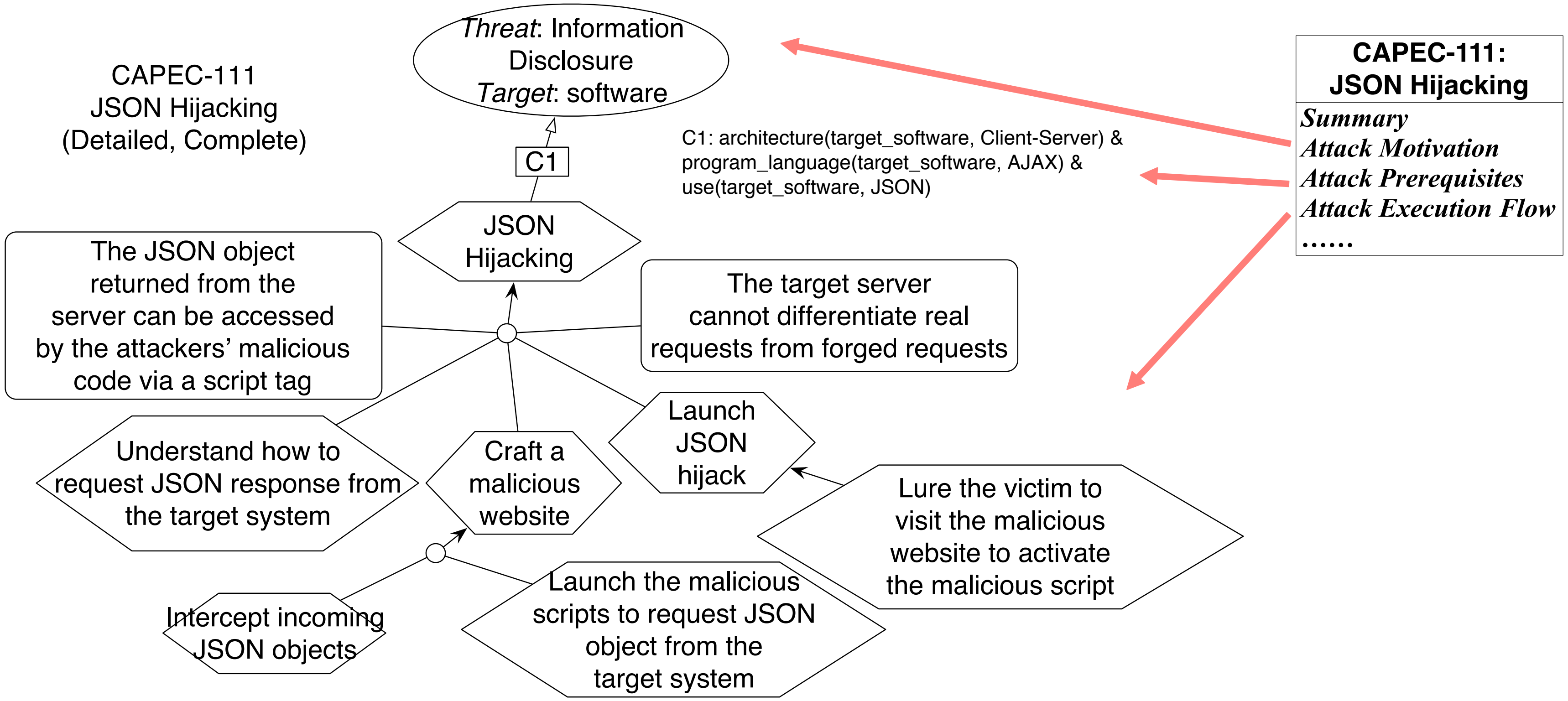
CAPEC-111: JSON Hijacking

Summary:An attacker targets a system that uses JavaScript Object Notation (JSON) as a transport mechanism between the client and the server to steal possibly confidential information transmitted from the server back to the client inside the JSON object by taking advantage of the loophole in the browser's Same Origin Policy that does not prohibit JavaScript from one website to be included and executed in the context of another website.

Attack Motivation: Read application data
Attack Execution Flow: Understand How to Request JSON Responses from the Target System...
Attack Prerequisites: JSON is used as a transport mechanism between the client and the server …
Typical Severity : High
Solutions and Mitigations: Ensure that server side code can differentiate between legitimate requests and forged requests...

Step 3: Anti-goal operationalization

- Model and analyze CAPEC attack patterns
  - Selection step 1: Identify relevant patterns
  - Selection step 2: Identify applicable patterns



CAPEC-111
JSON Hijacking
(Detailed, Complete)

Threat: Information Disclosure
Target: software

C1

C1: architecture(target_software, Client-Server) & program_language(target_software, AJAX) & use(target_software, JSON)

JSON Hijacking

The JSON object returned from the server can be accessed by the attackers' malicious code via a script tag

The target server cannot differentiate real requests from forged requests

Understand how to request JSON response from the target system

Craft a malicious website

Launch JSON hijack

Lure the victim to visit the malicious website to activate the malicious script

Intercept incoming JSON objects

Launch the malicious scripts to request JSON object from the target system

CAPEC-111:
JSON Hijacking

Summary
Attack Motivation
Attack Prerequisites
Attack Execution Flow
……

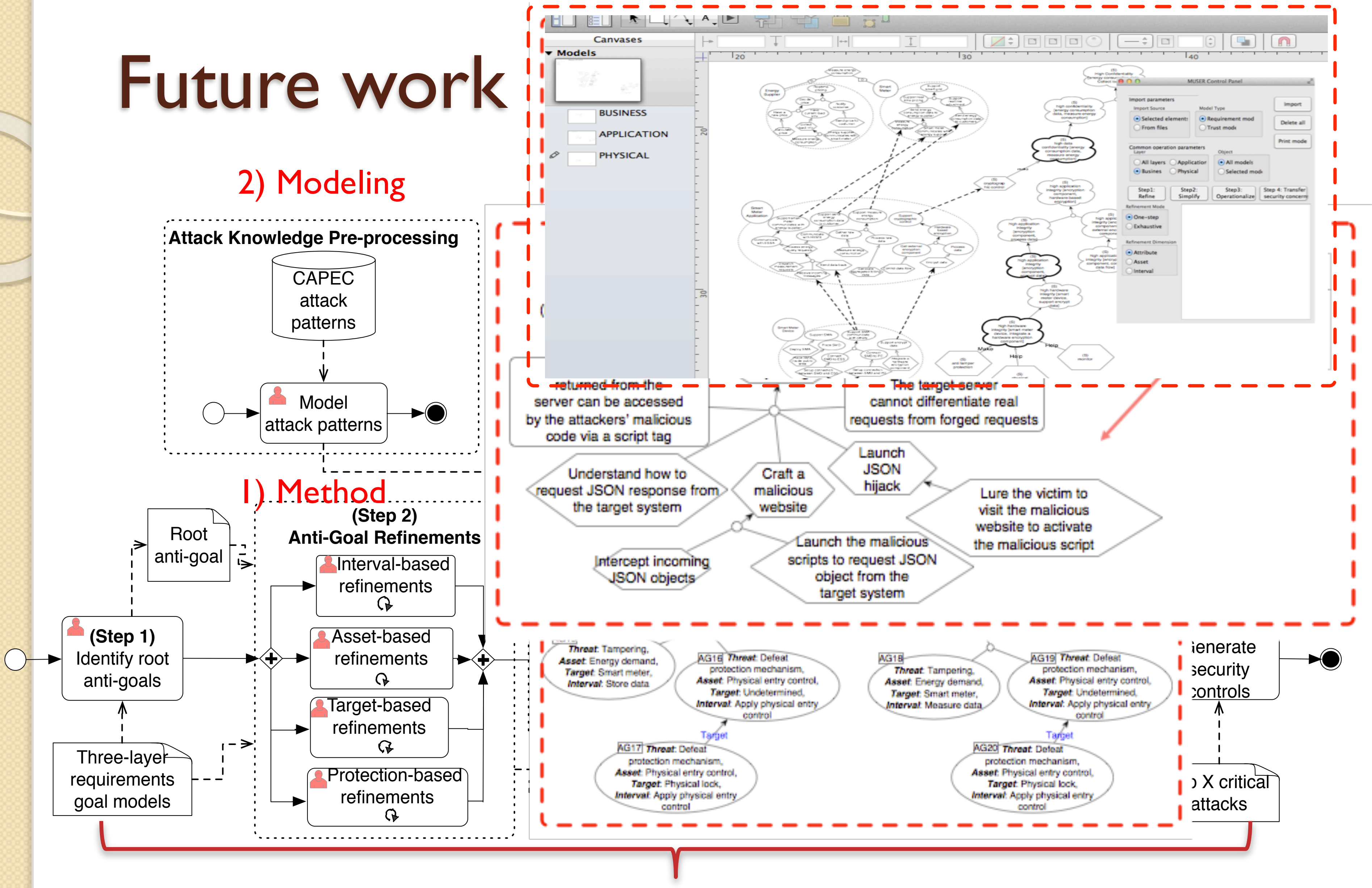
Attack assessments and treatments

- Step 4: Risk assessments
  - Analyze severity and likelihood of each attack (CAPEC)
- Step 5: Attack treatments
  - Prioritize attacks
  - Design security controls (CAPEC)

Future work

2) Modeling

1) Method


Attack Knowledge Pre-processing
CAPEC attack patterns
Model attack patterns
(Step 2)
Anti-Goal Refinements
Root anti-goal
Interval-based refinements
Asset-based refinements
Target-based refinements
Protection-based refinements
(Step 1) Identify root anti-goals
Three-layer requirements goal models
ienerate security controls
X critical attacks
Canvases
Models
BUSINESS
APPLICATION
PHYSICAL
MUSER Control Panel
returned from the server can be accessed by the attackers' malicious code via a script tag
The target server cannot differentiate real requests from forged requests
Understand how to request JSON response from the target system
Craft a malicious website
Launch JSON hijack
Lure the victim to visit the malicious website to activate the malicious script
Intercept incoming JSON objects
Launch the malicious scripts to request JSON object from the target system
Threat: Tampering, Asset: Energy demand, Target: Smart meter, Interval: Store data
AG16 Threat: Defeat protection mechanism, Asset: Physical entry control, Target: Undetermined, Interval: Apply physical entry control
AG18 Threat: Tampering, Asset: Energy demand, Target: Smart meter, Interval: Measure data
AG19 Threat: Defeat protection mechanism, Asset: Physical entry control, Target: Undetermined, Interval: Apply physical entry control
Target
AG17 Threat: Defeat protection mechanism, Asset: Physical entry control, Target: Physical lock, Interval: Apply physical entry control
Target
AG20 Threat: Defeat protection mechanism, Asset: Physical entry control, Target: Physical lock, Interval: Apply physical entry control

3) Tool

Summaries

- Holistically analyze security of STSs
    - Ongoing work: Identify potential attacks to test system security
- Propose a holistic security attack analysis framework
- Present and illustrate a refined process and discuss subsequent research objectives

Thank You!

Contact: tong.li@disi.unitn.it