Workshop 01/07/2019

Tithnara Nicolas SUN

Philippe Dhaussy (Lab-STICC)
Lionel Van Aertryck (DGA-MI)
Ciprian Teodorov (Lab-STICC)

Table of contents

Introduction
Context

- Executable attack modeling on industrial control systems
- Some characteristics :
  - Cyber-physical interfaces
  - Dynamical systems
  - Semantic heterogeneity
  - Large number of specification and implementation languages
  - Large number of execution platforms
- Attack modeling
  - Attack trees, DAGs, graphs
  - Embedded attack strategies (embedded malicious code)
  - Either very abstract -> decoupled from the technical domain
  - Or very concrete -> coupled with the technical domain but low-level
  - Difficult to perform « execution-based » analysis

Introduction
Research questions

- How to capture an abstract operational semantics of the targeted system and compose it with executable attack modeling ?
- How to steer the focus towards architecture independent attack modeling ?
- How to capture the attack surface of the system-under attack (SUA) ?
- How to handle the semantic heterogeneity in the targeted system.

Introduction
Research questions

- **Opportunism** – The modeling language should allow an opportunism-based iterative refinement approach. The user should be able to detail only the points of interest, and provide very abstract (generic) implementation for the other parts.
- **Cyber-separation** – Ideally, the functional system model should be decoupled from the attack/defense actor modeling aspects. Which will enable focused reasoning both on the system aspects, and attack/defense models
- **Attack surface reification** – The attack surface should be exposed explicitly to ease the specification of attack/defense strategies
- **Incomplete knowledge** – The attack/defense actors act on the system having a limited knowledge. As opposed to specification languages which strive to provide an omniscient view on the system, attack discovery and modeling formalism should enable restricting the access to the « system model » to the attack surface.
- **Execution support** -- The formalism should provide the mechanisms for representing the system dynamics, even in the presence of partial behavior specification.
- **Multi-level abstraction** : mix abstraction levels
- **Semantic heterogeneity** : mix different languages

Introduction
Approach

- Methodology based on the integration of two correlated processes :
  - Target system modeling process – TSM - (captures the « situation »)
  - Executable attack modeling process – EAM
- The TSM process enables capturing the semantics of the SUA
- The EAM process focuses on the specification of attack scenarios

- The TSM and EAM link is established at the semantic level through the formal definition of **attack surface operations** (operations exposed from the TSM semantics).

Introduction
Approach

1. Target System Modeling Language *[30/06/19]*
2. Attack surface operations *[1/09/19]*
3. Attack modeling language *[15/09/19]*
4. OBP2 adapter, or hand-made simulator *[30/09/19]*
5. Case-study I - *[30/10/19]*

	Mai	Juin	Juillet	Aout	Septembre	Octobre
Target System Modeling (TSM) Language						
Attack Surface operations						
Attack Modeling Language (AML)						
OBP2 adapter						
Case-study I						

Target System Modeling Requirements

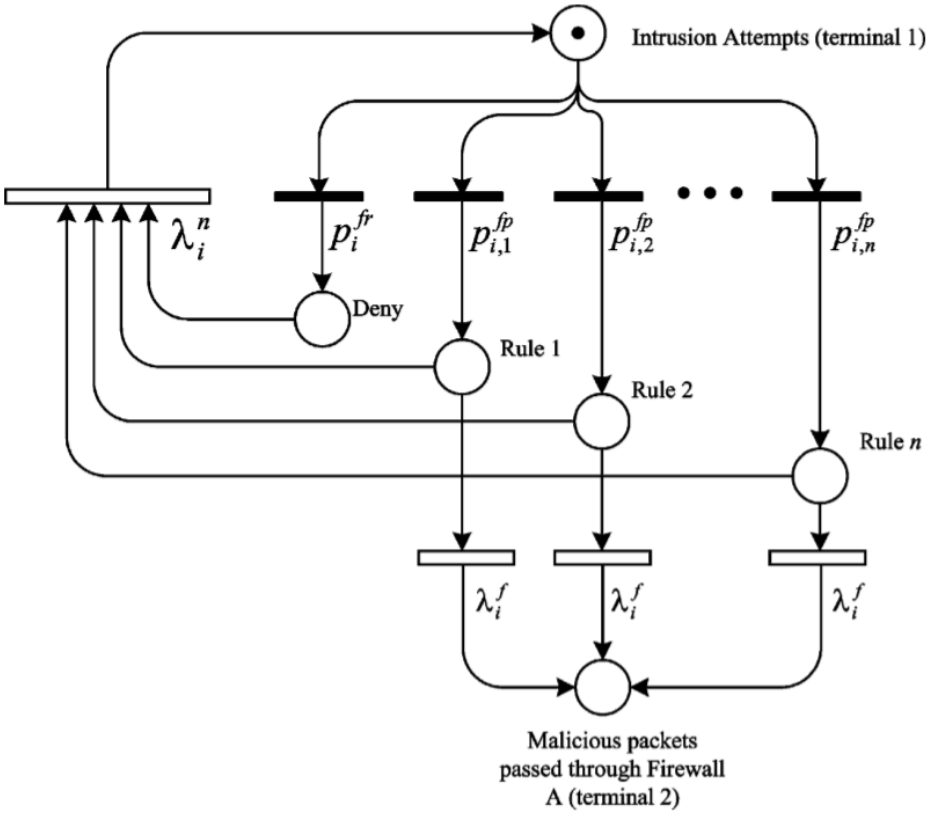
System modeling for cybersecurity purposes:

- Based on PimCA
- Step-by-step attack scenario execution
- Along with cases study

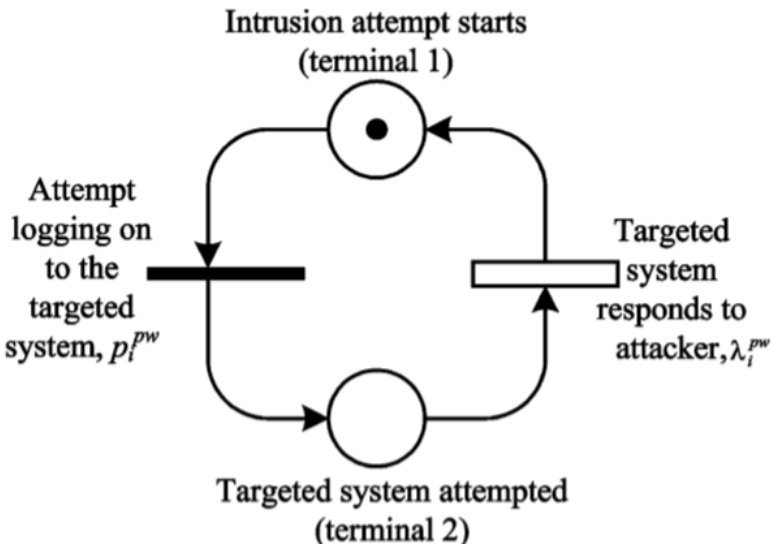
Target System Modeling Progress

SCADA Systems Cybersecurity

- Firewall



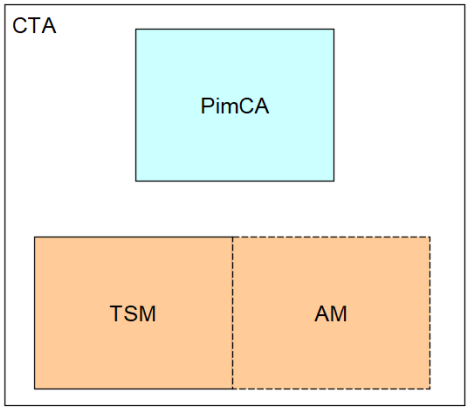
- Password



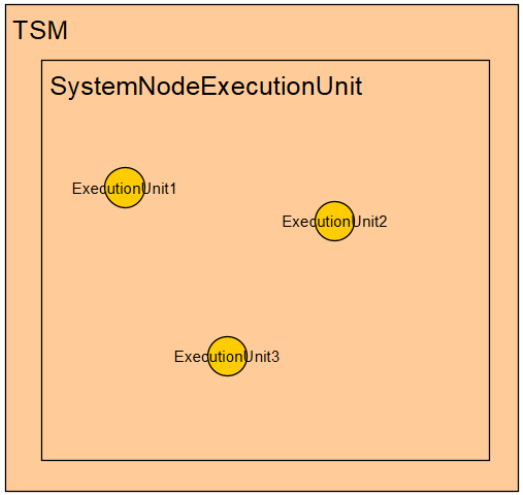
"Vulnerability Assessment of Cybersecurity for SCADA Systems" C. Ten, C. Liu and G. Manimaran : https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4652578&isnumber=4652575

Conclusion

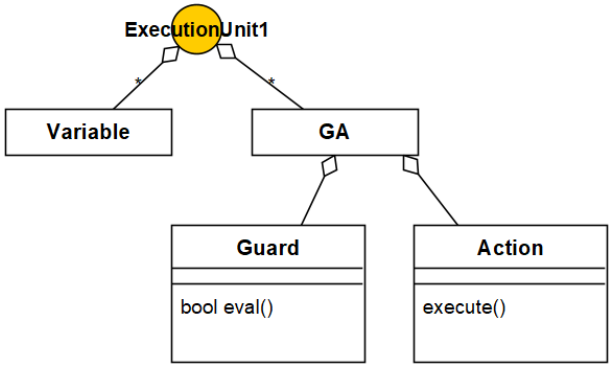
- OpenFlexo



- ExecutionUnit



- Guard\Action



Conclusion

- To do (short-term)
  - Objectives?
    - Attack scenario showcase
  - Market manipulation scenario/ Openflexo

- To do (mid-term)
  - Objectives?
    - New attack scenario discovery
  - System nominal behavior
  - Market manipulation scenario/ Openflexo

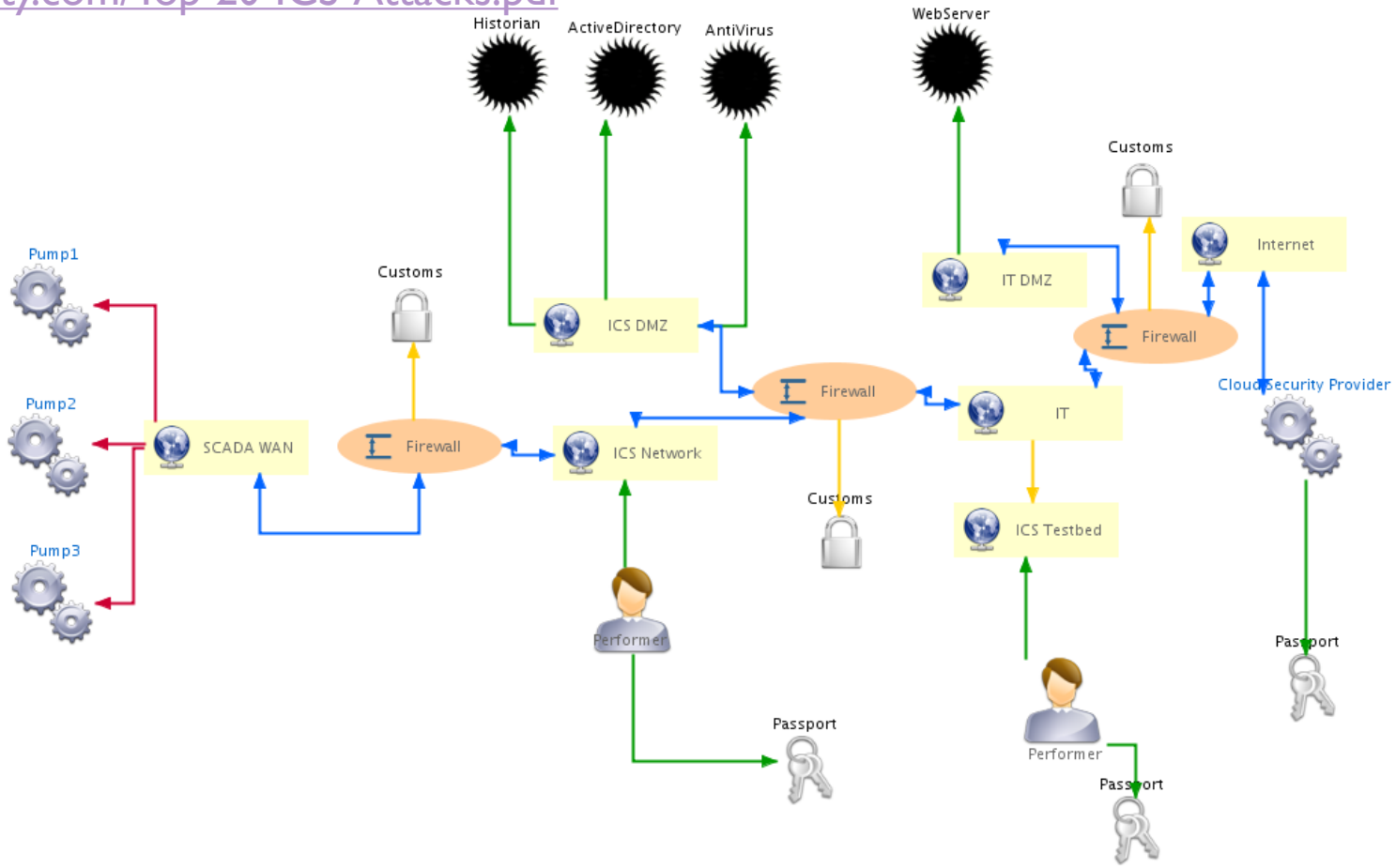
Target System Modeling PimCA/Openflexo

Icône-Concept	Description
Machinery	**Machinerie** : système manipulant des Ressources (regroupement particulier) : voiture, animal, PC, processus
Performer	**Exécutant (spécialise Machinerie)** : ce qui transforme la Ressource, e.g. UC/Programme, cerveau, régulateur.
Network	**Réseau (spécialise Machinerie)** : zone d'échange de matière, d'information, d'énergie, etc. : câblage, tuyauterie, IPC Engine.
Customs	**Douane (spécialise Machinerie)** : fonctionnalité particulière mise en place par une Machinerie pour identifier & autoriser une autre Machinerie : cadenas, garde, login, crypto
Interface	**Interface (spécialise Machinerie)** : permet de passer d'une Machinerie à une autre, du monde physique au monde virtuel et inversement : NIC, caméra, clavier, écran.
Gathering (non réifié)	**Regroupement** : ensemble logique d'objets de tout type, entrepôt sans Ressource. Un regroupement ne possède pas les infos propres à une machinerie, c.-à-d. executant, configuration, mémoire.
Repository	**Entrepôt** : zone de stockage de Ressource : armoire, bâtiment, disquette, database, file system

Icône-Concept	Description
Resource	**Ressource** : ce qui est transformé, manipulé par une Machinerie : matière, électricité, document, log, data
Instructions	**Consigne (spécialise Ressource)** : La direction, les paramètres que l'exécutant suit : Fichier de configuration, ordre, politique de sécurité
Passeport	**Passeport (spécialise Ressource)** : élément à fournir à la Douane pour être identifié / autorisé : clef, carte d'identité, badge, login/password, clef de chiffrement

Target System Modeling Top 20

The Top 20 Cyber Attacks Against Industrial Control Systems, https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf



Target System Modeling
Top 20

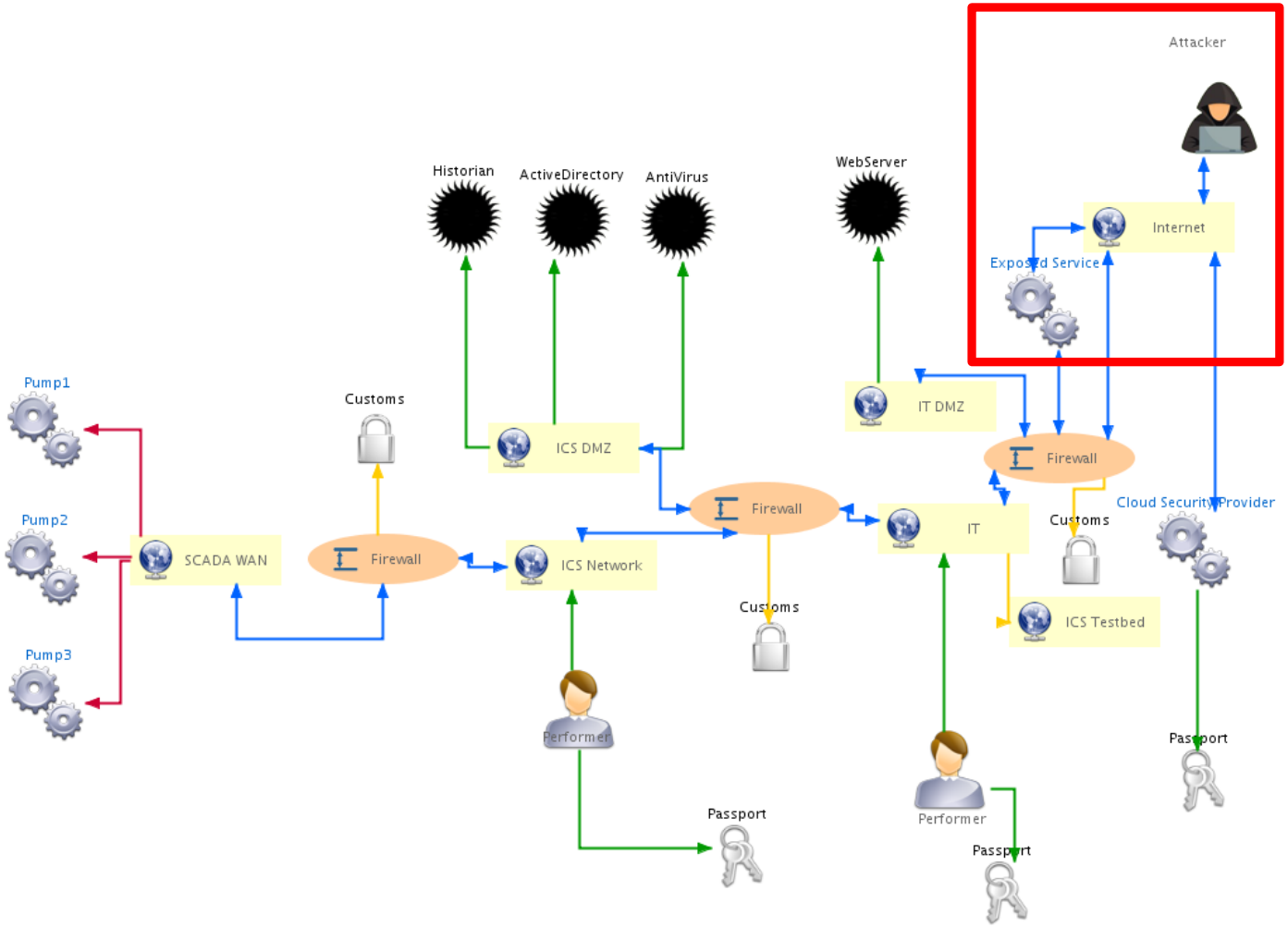
The Top 20 Cyber Attacks Against Industrial Control Systems, https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf

	Attack Name	Steps
1	ICS Insider	
2	IT Insider	
3	Common Ransomware	
4	Targeted Ransomware	
5	Zero-Day Ransomware	
6	Ukrainian Attack	
7	Sophisticated Ukrainian Attack	
8	Market Manipulation	
9	Sophisticated Market Manipulation	
10	Cell-Phone WIFI	
11	Hijacked Two-Factor	
12	Industrial Internet of Things Pivot	
13	Malicious Outsourcing	
14	Compromised Vendor Website	
15	Compromised Remote Site	
16	Vendor Back Door	
17	Stuxnet	
18	Hardware Supply Chain	
19	Nation-State Crypto Compromise	
20	Sophisticated Credentialed ICS Insider	

- Première approche (à raffiner/faire évoluer)
- Chaque type implique des guards/actions différentes

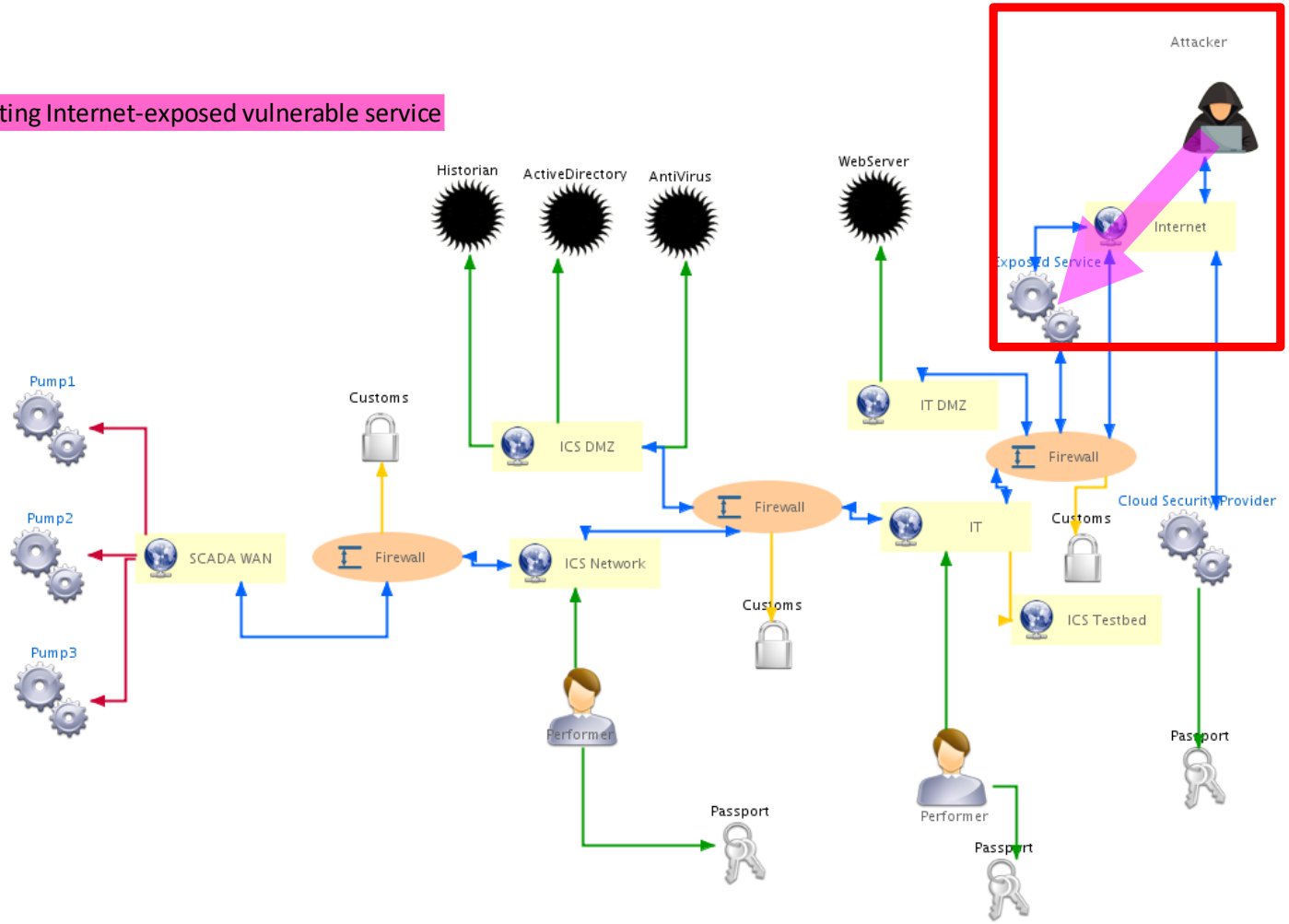
	Social engineering attack
	Malware injection
	Observation/Understanding/Design/Research
	Privilege elevation
	Pivoting
	Malware execution
	Trace erasure

Target System Modeling
Market Manipulation



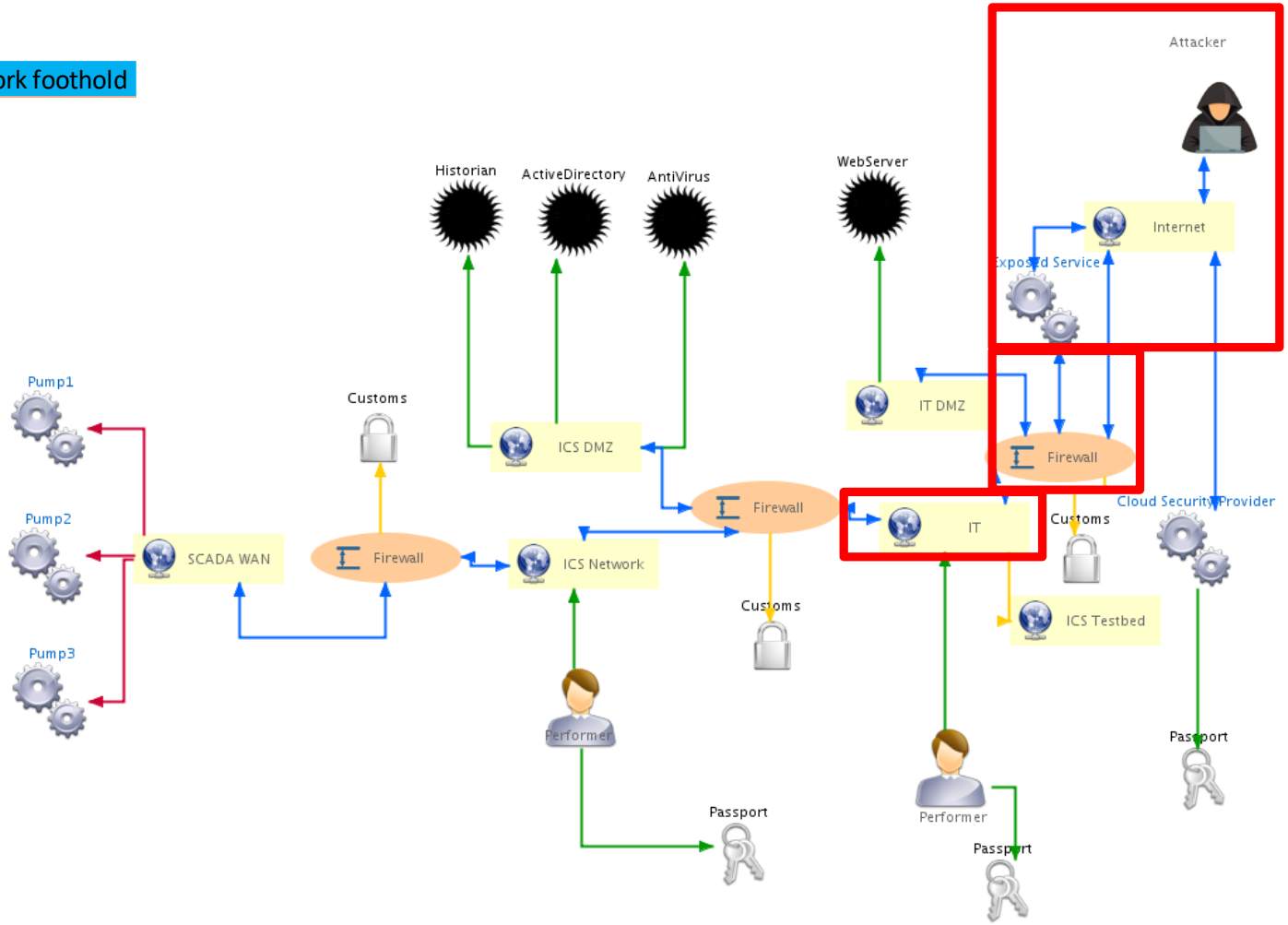
Target System Modeling
Market Manipulation

Exploiting Internet-exposed vulnerable service



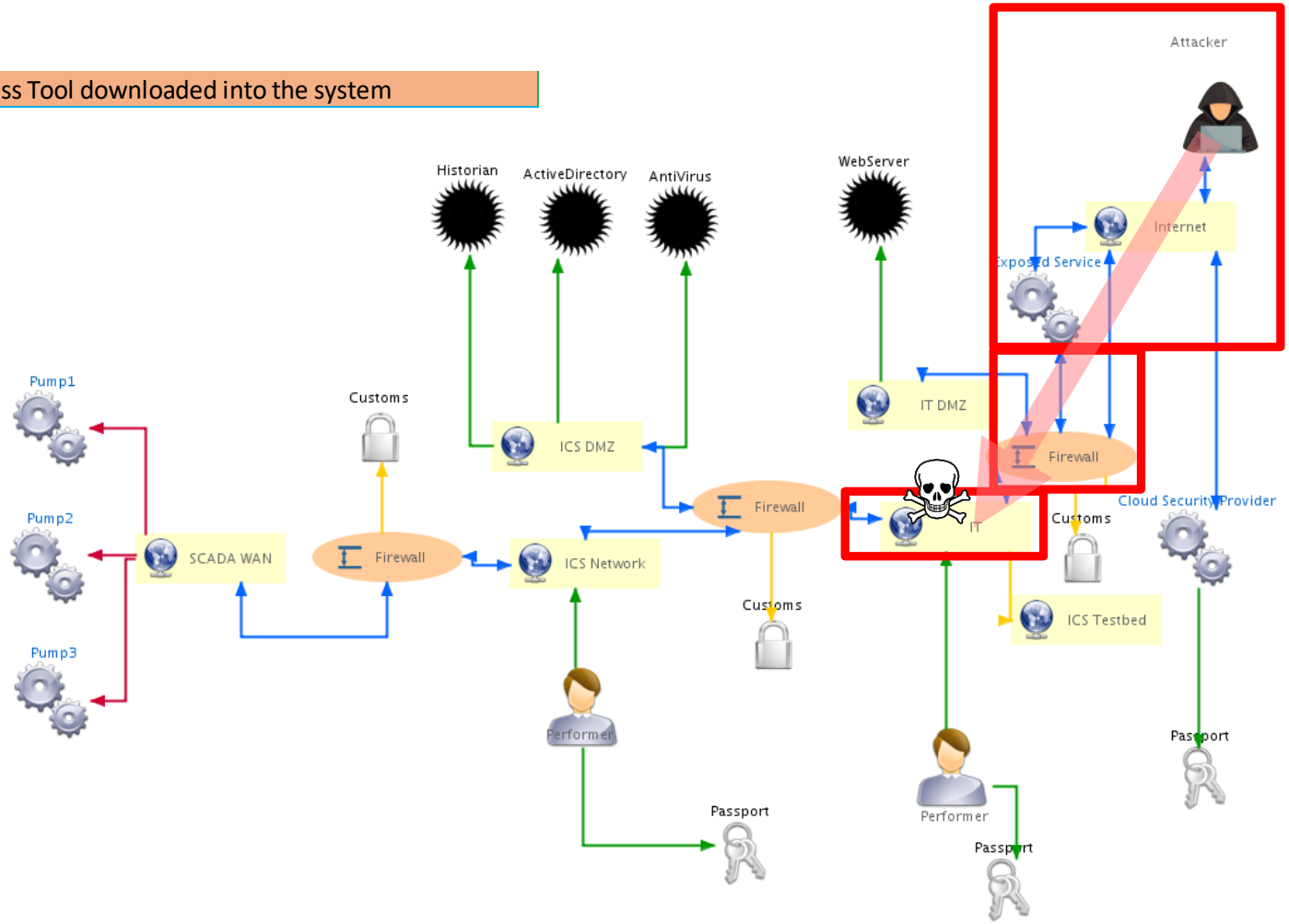
Target System Modeling
Market Manipulation

IT network foothold



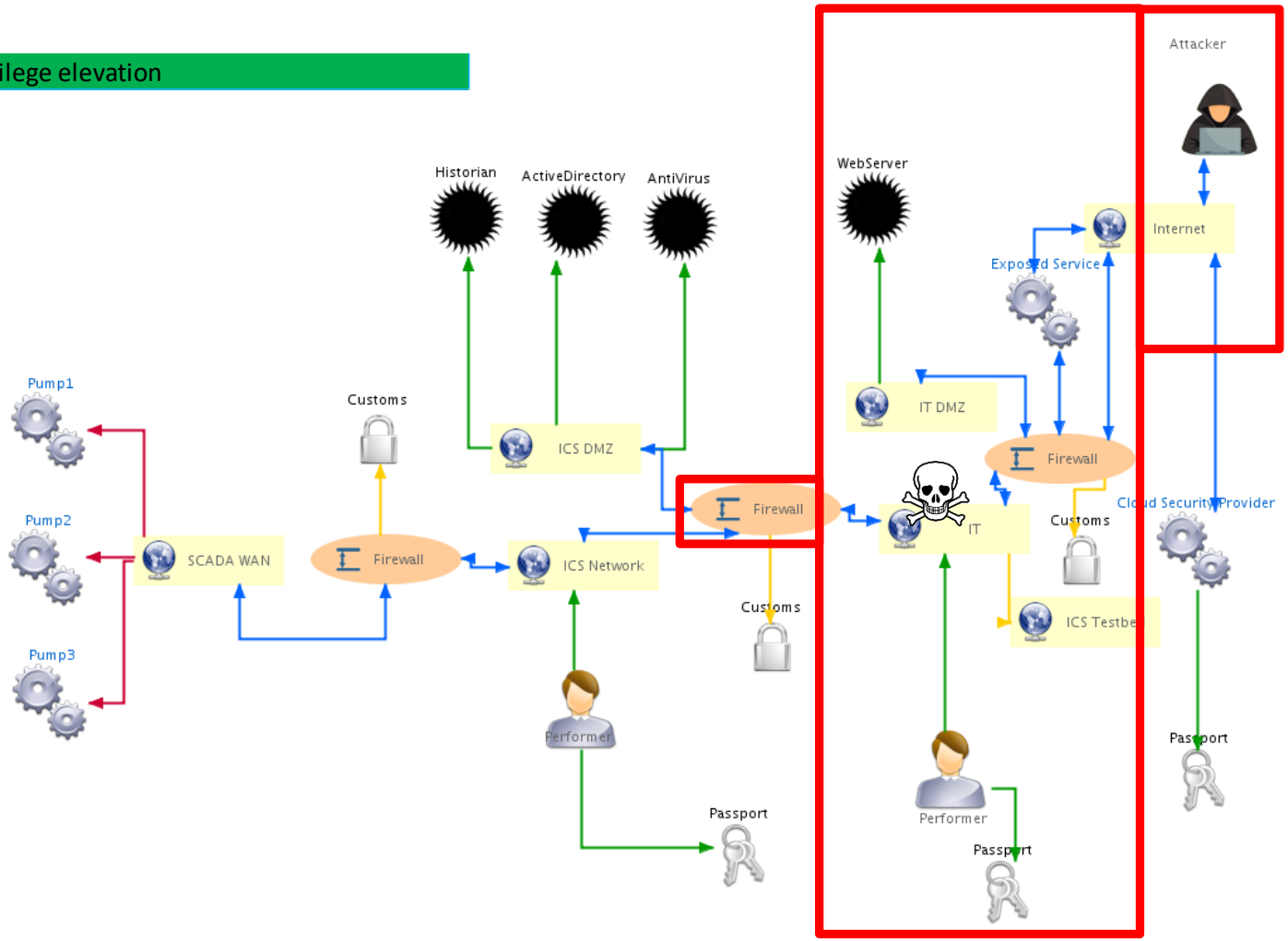
Target System Modeling
Market Manipulation

Remote Access Tool downloaded into the system



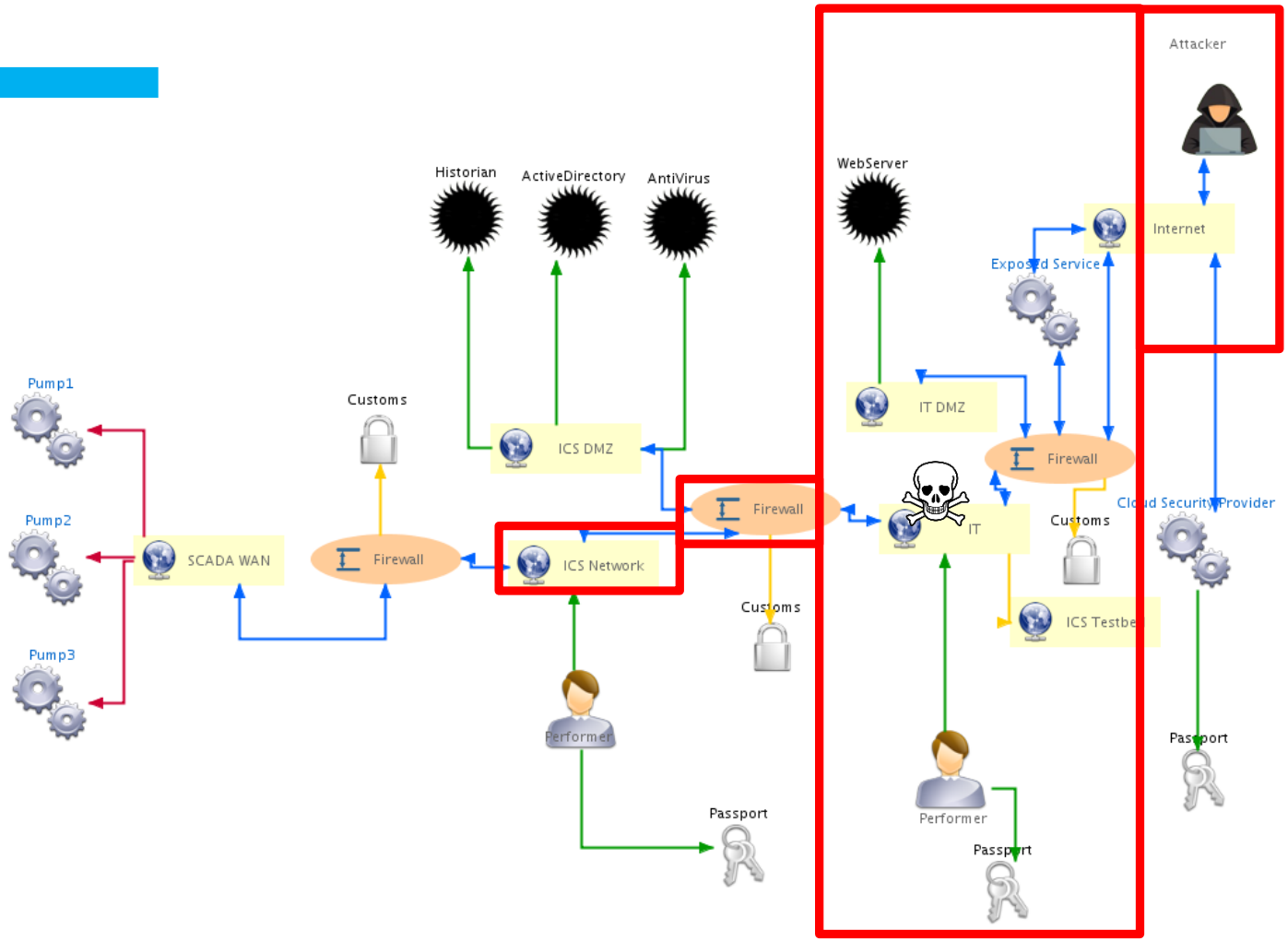
Target System Modeling
Market Manipulation

IT Domain Privilege elevation



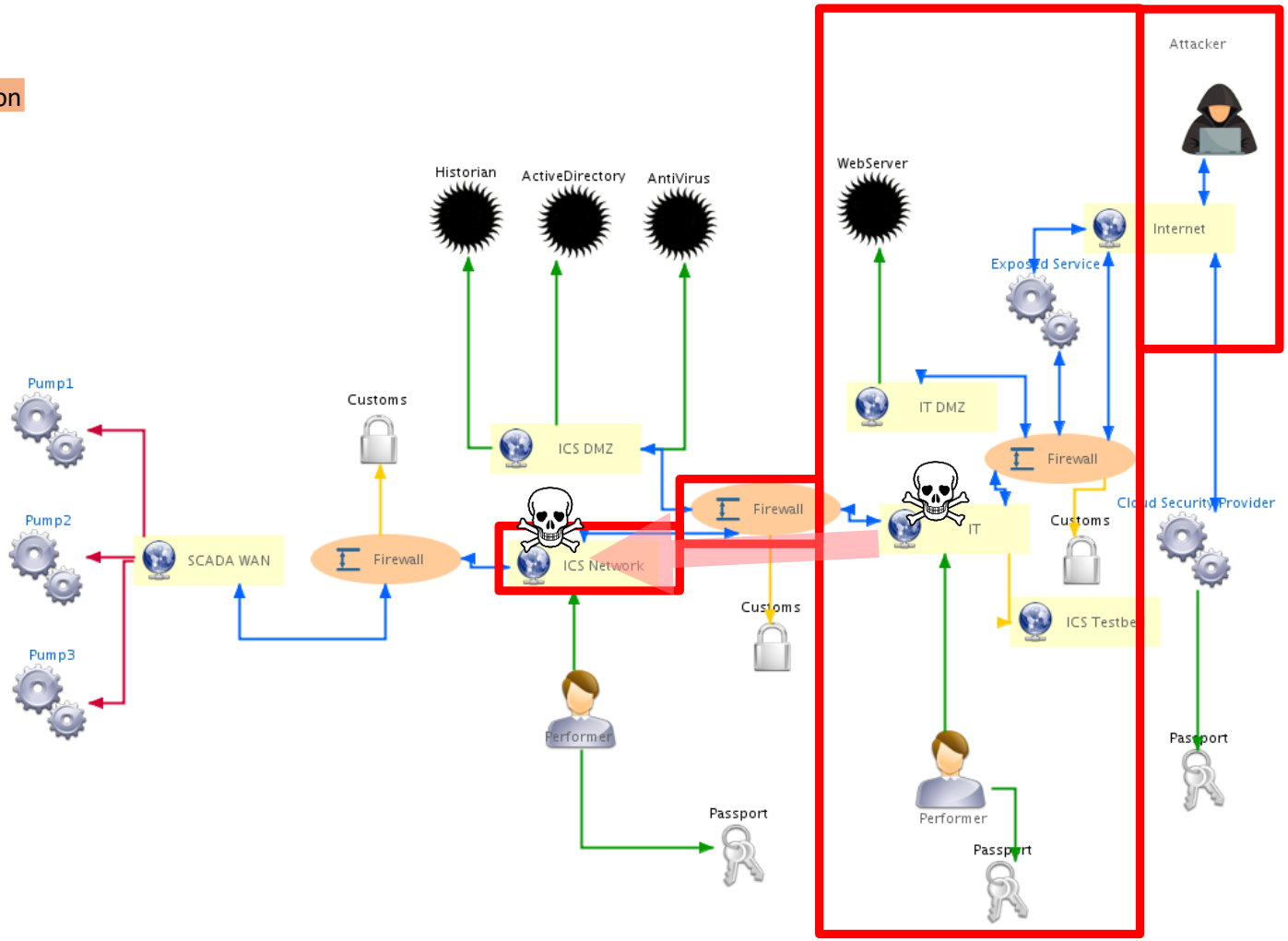
Target System Modeling
Market Manipulation

Pivoting to ICS



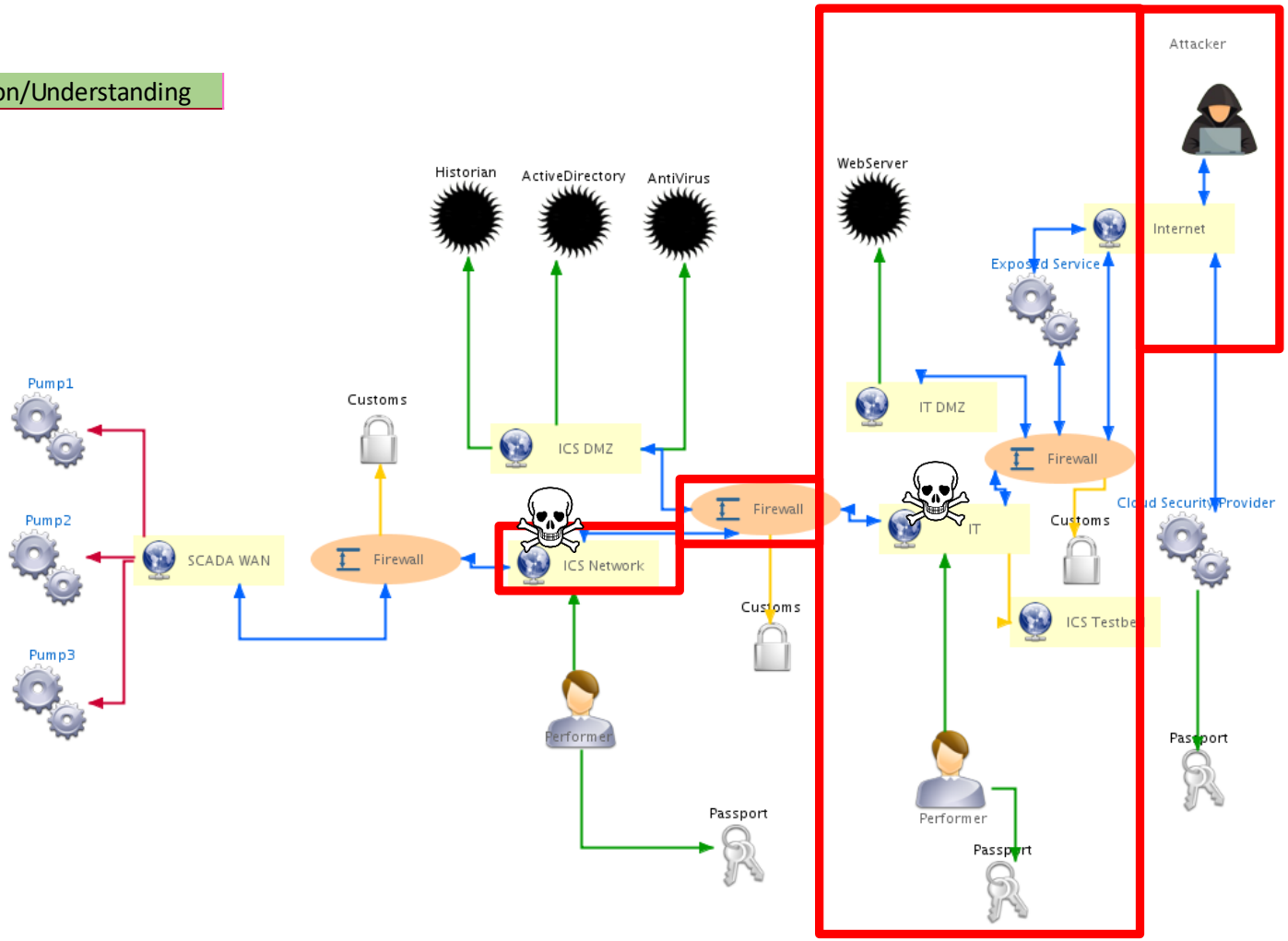
Target System Modeling
Market Manipulation

RAT propagation



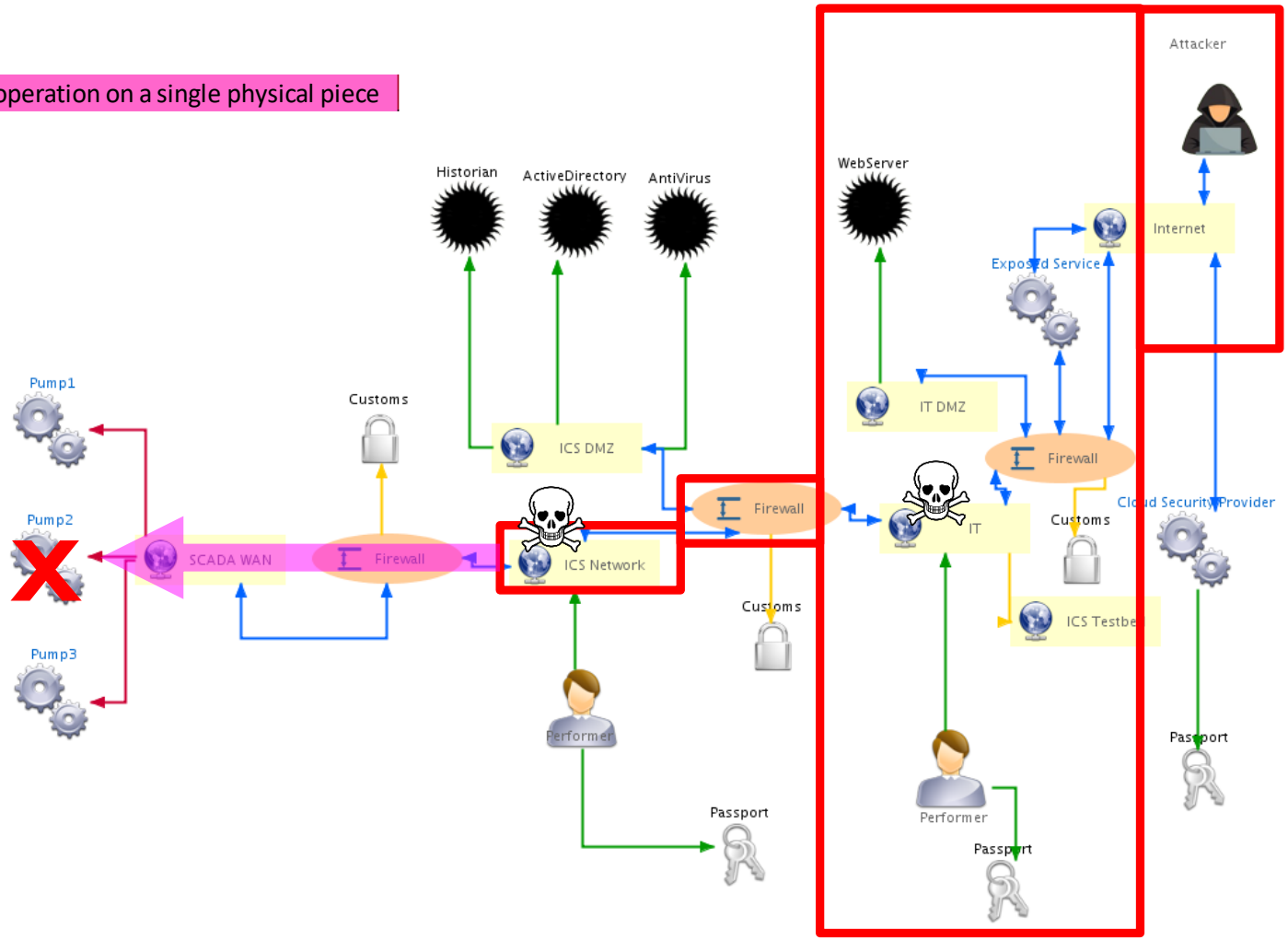
Target System Modeling
Market Manipulation

ICS Observation/Understanding



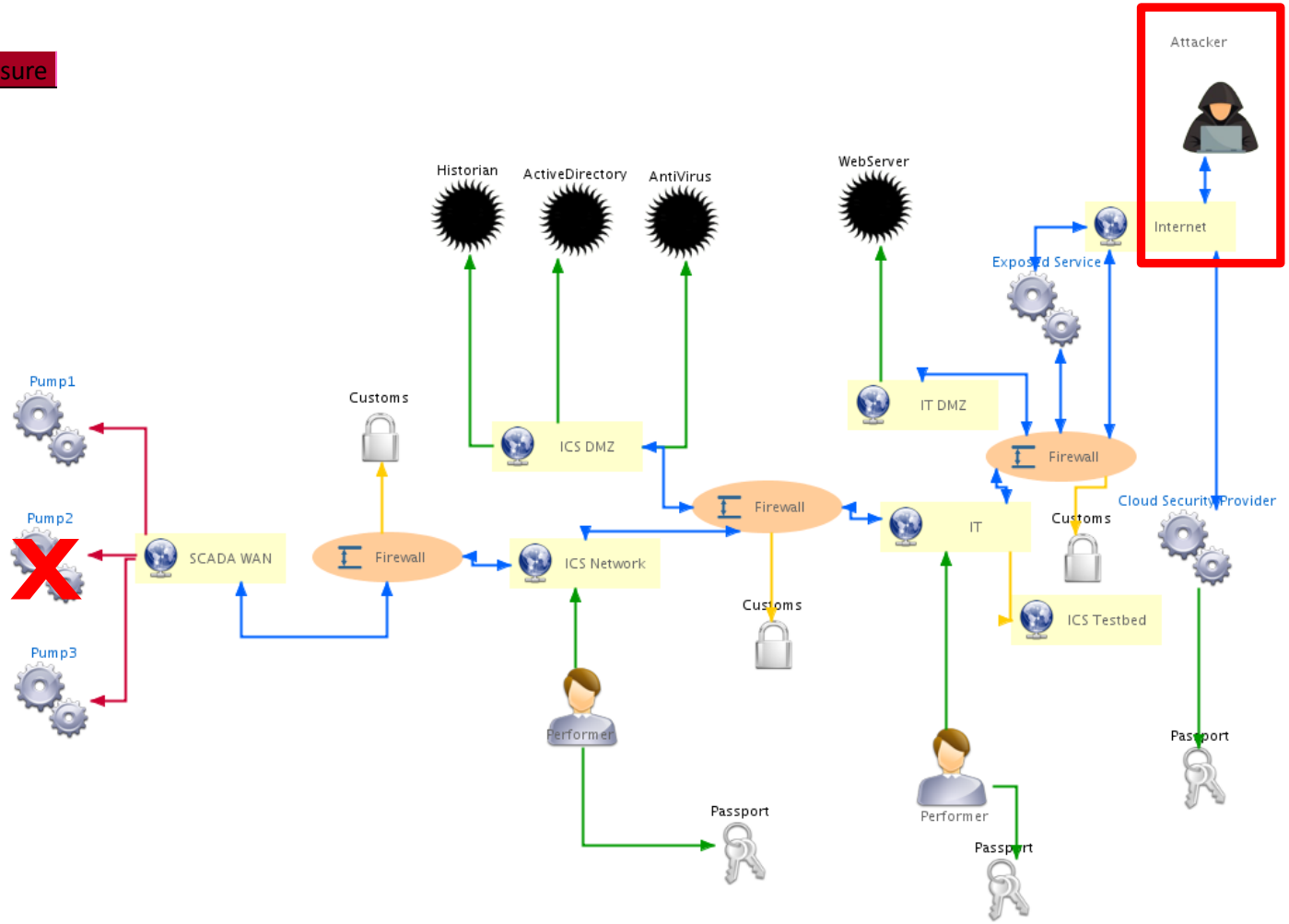
Target System Modeling
Market Manipulation

Targeted mis-operation on a single physical piece



Target System Modeling
Market Manipulation

Trace erasure



Target System Modeling
Market Manipulation

Sell single physical piece at high price