International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFC

(06/2019)

ITU-T Focus Group Digital Currency including Digital Fiat Currency

Protection assurance use case for a payment transaction

Security Working Group Deliverable

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Currency Including Digital Fiat Currency (FG DFC) at its meeting in May 2017. TSAG is the parent group of FG DFC.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Protection assurance use case for a payment transaction

About this report

This report was written by Jacques Francoeur, Co-chair of the Security Working group of the ITU-T Focus Group Digital Currency including Digital Fiat Currency.

The author acknowledges the contributions and feedback received from members of the Security working group.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfc@itu.int

Table of Contents

List of Figures

1 Scope & Objectives

The objective of this report is to describe how the Protection Assurance framework can be applied for a payment use case. The systematic approach outlined can form the basis of a standard on conducting a unified Threat-to-Target and to Security-to-Target analysis that is modular, repeatable and most importantly reusable.

The scope of this document is all matters

- cyber threats, attacks and exploits;
- digital targets
- security countermeasures

2 Payment Pattern Target Model

The Protection Assurance report outlined a unified security method to conduct a risk and threat analysis of a Digital Currency Ecosystem Target. The Target use case discussed in this document is a Payment Pattern ("Pattern"), illustrated in Figure 1 as the Target.

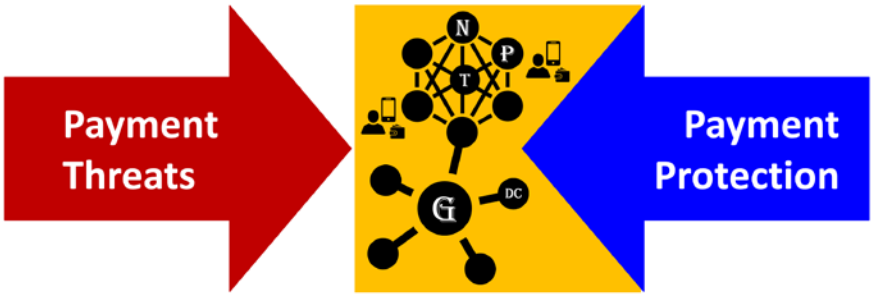


Figure 1: Unified Security Model Application to Payment Pattern Use Case

The Pattern selected was extracted from the Digital Currency Ecosystem Level 1 Target Model illustrated in Figure 2.

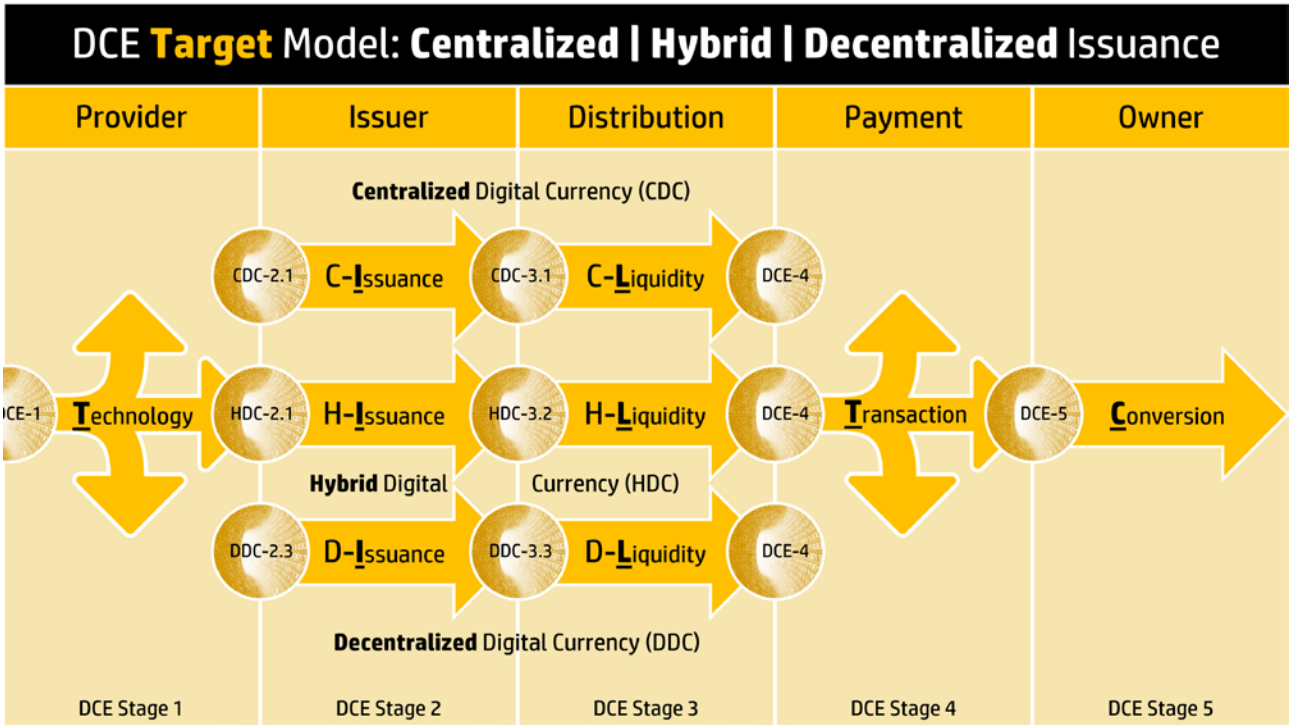


Figure 2: DCE Target Model Level 1

The Use Case Pattern selected is located in Stage 4 and 5 of the Digital Currency Ecosystem model, illustrated in Figure 3. The Pattern is agnostic to the type of Digital Currency issued.

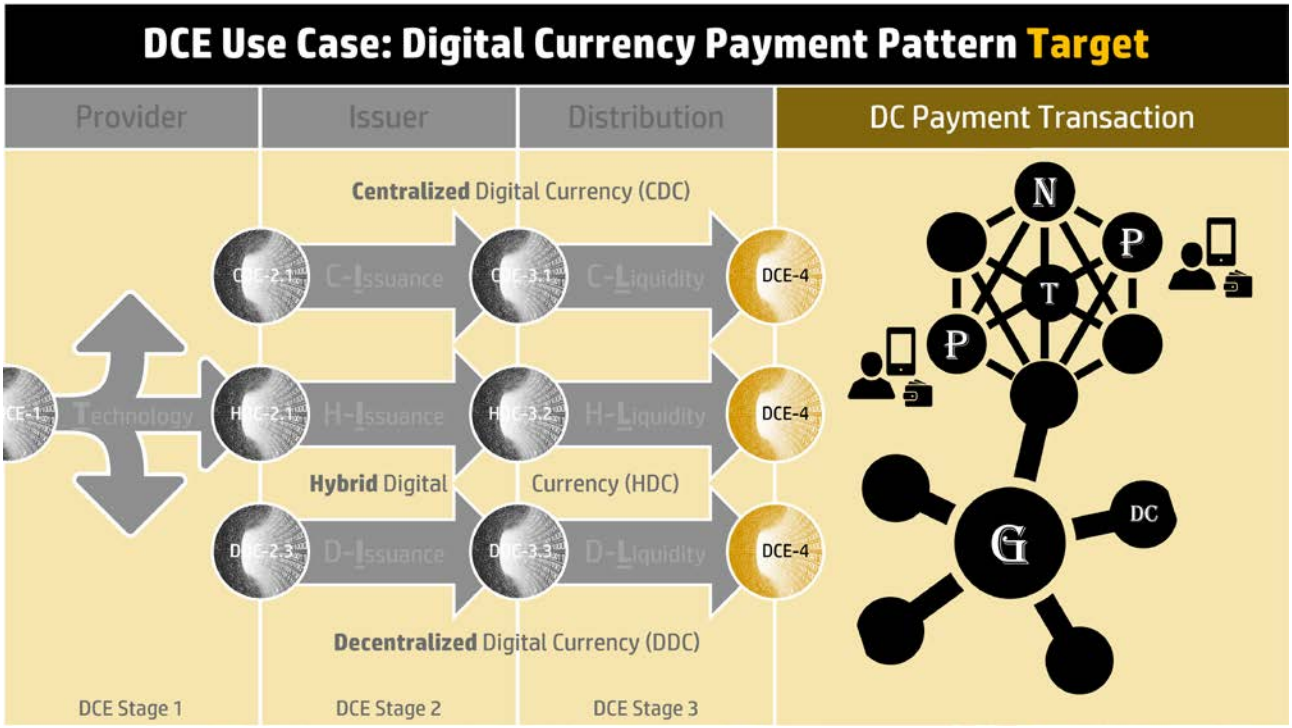


Figure 3: Payment Pattern Located in Stage 4 and 5 of DCE Level 1 Model

3 Target Sub-patterns

In order to conduct a systematic threat analysis and countermeasure design that is measurable, repeatable, and reuable the pattern should be decomposed into its elemental constituents, as illustrated in Figure 4

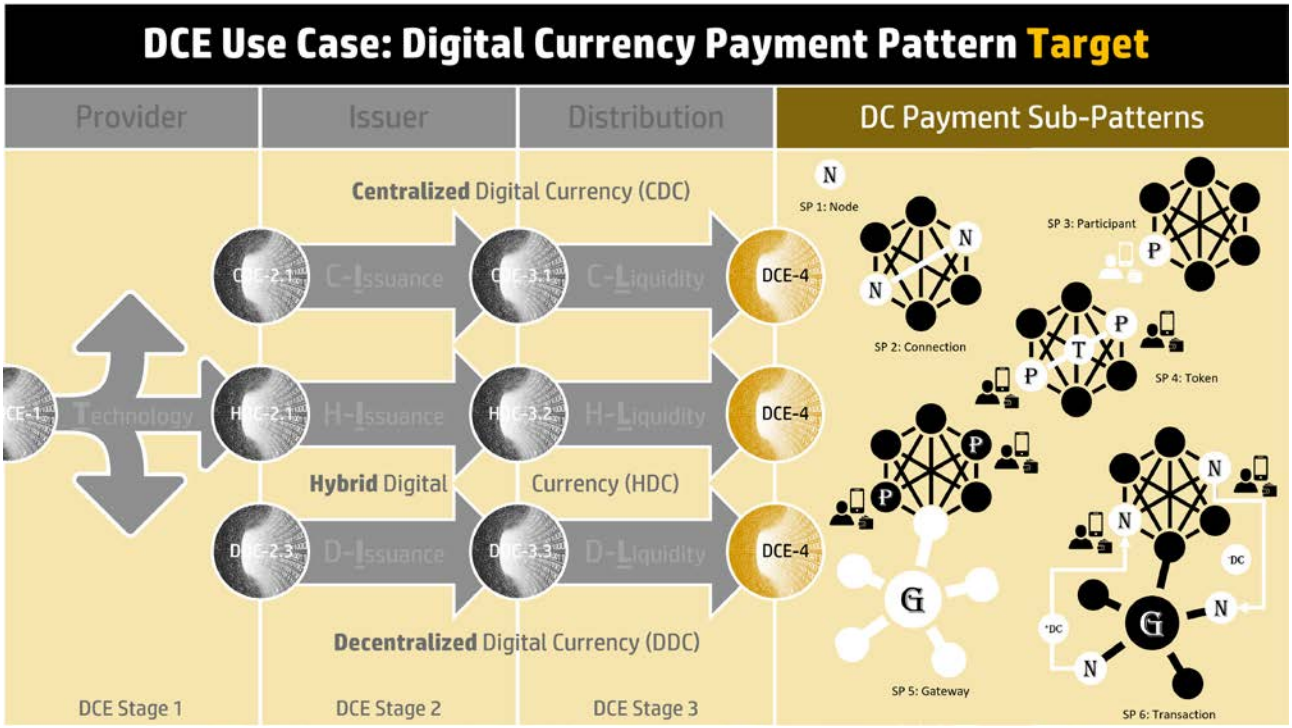


Figure 4: Payment Pattern Sub-Patterns

The decomposition process must be sequential and incremental from elements combined to form the complete Pattern.

The process starts with the smallest building block in the Pattern, in this use case a Node referred to as Sub-Pattern 1. The 2nd sub-pattern adds to the 1st to add attack surface for incremental consideration. Each sub-pattern forms a more completed Pattern each time but only the incremental is considered in the sub-pattern threat analysis. In this way, more complex patterns are created from less complex constituents that have already completed their Exploit | Vulnerability | Countermeasure analysis.

This approach allows a set of “building block” constructs to be completed once and reused by others. The six sub-patterns are listed below with the incremental elements in each case, illustrated in Figures 5 through 7.

- Sub-Pattern 1: Node
- Sub-Pattern 2: Connection: + TCP Connection yielding 2 Nodes and a connection.
- Sub-Pattern 3: Participant: + Person, Wallet application, Host Device yielding a connection to a Network Node.
- Sub-Pattern 4: Token: + Token in a transfer use case.
- Sub-Pattern 5: Gateway: + Payment Gateway Provider. Internal model not yet developed
- Sub-Pattern 6: Transaction: + a Digital Currency purchase of physical goods use case. DC already in existance.

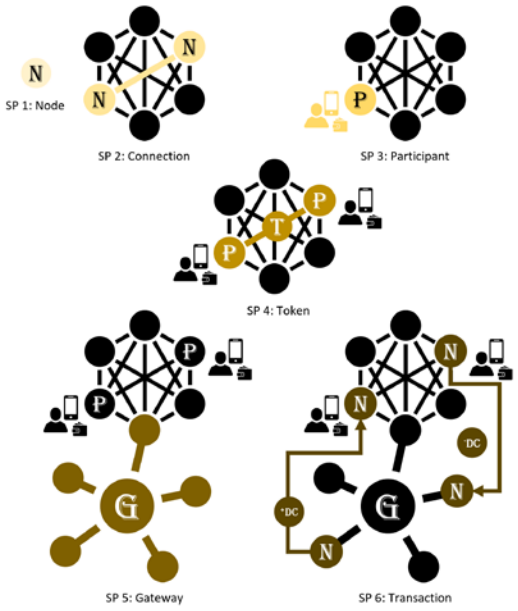
All DCE Target elements illustrated on the left of Figure 7 are sub-divided into a consistent “backbone” of target Classes as follows:

- Application Targets
- Service Targets
- Protocol Targets
- Network Targets
- Data Targets
- Physical Targets

Each sub-pattern is made up of one or more Target Classes, as illustrated in Figure 5.

Sub-Pattern 1: **Node**
Sub-Pattern 2: **Connection**
Sub-Pattern 2: **Participate**

ID	Sub-Pattern 1: **Node**
4	Network
4.1	**Node**
4.2	**IP Routing Table**
4.3	**Network Device**
5	Data
5.1	**IP Address**
6	Physical
6.1	**Operational Zone**
ID	**Sub-Pattern 2: Connection**
1	Application
1.1	**Decentralized Coordination**
2	Service
2.1	**TCP Connection**
3	Protocol
3.1	**P2P Network**
ID	**Sub-Pattern 3: Participant**
1	Application
1.2	**Wallet**
1.3	**Browser**
3	Protocol
3.2	**Participant – Wallet - Device**
4	Network
4.4	**Participant Interface Device**
5	Data
5.2	**Identity**
5.3	**Account**
5.4	**Private Key**
6	Physical
6.2	**Participant**



Sub-Pattern 4: P2P Token **Transfer**
Sub-Pattern 5: Payment **Gateway**
Sub-Pattern 6: P2P DC **Transaction**

ID	Sub-Pattern 4: **Token**
1	Application
1.4	**P2P Token Transfer**
1.5	**Digital Asset - Token**
2	Service
2.2	**Timestamp**
3	Protocol
3.3	**Token Transfer Protocol**
5	Data
5.5	**Token Transfer Data**
5.6	**Session Log Data**
ID	**Sub-Pattern 5: Gateway**
2	Service
2.3	**Interface/Session**
3	Protocol
3.4	**Participant – Wallet – Payment Gate**
5	Data
5.7	**Payment Gateway Identity**
ID	**Sub-Pattern 6: Transaction**
1	Application
1.6	**P2P DC Payment**
2	Service
2.4	**DC Transaction Service**
3	Protocol
3.5	**Participant/Wallet/Gateway/Payment**
5	Data
5.8	**Transaction Data**

Figure 5: Sub-Pattern Target Classes

Each Target Class is made up of sub-patterns, as illustrated in Figure 6. It is interesting to note how each sub-pattern contributes to what Target Classes. The network aspects get created 1st followed by applications and where data a protocol exists in all patterns.

Target Class by Sub-Pattern

	Target Class	SP #	SP Name
1	**Application Targets**		
1.1	Decentralized Coordination	2	Connection
1.2	Wallet	3	Participant
1.3	Browser	3	Participant
1.4	P2P Token Transfer	4	Token
1.5	Digital Asset – Token	4	Token
1.6	P2P DC Payment	6	Transaction
2	**Service Targets**		
2.1	TCP Connection	2	Connection
2.2	Timestamp	4	Token
2.3	Interface/Session	5	Gateway
2.4	DC Transaction Service	6	Transaction
3	**Protocol Targets**		
3.1	P2P Network	2	Connection
3.2	Participant|Wallet|Device	3	Participant
3.3	Token Transfer Protocol	4	Token
3.4	Participant|Wallet|Payment Gateway	5	Gateway
3.5	Participant|Wallet|Gateway|Payment	6	Transaction
4	**Network Targets**		
4.1	Node	1	Node
4.2	IP Routing Table	1	Node
4.3	Network Device	1	Node
4.4	Participant Interface Device	3	Participant
5	**Data Targets**		
5.1	IP Address	1	Node
5.2	Identity	3	Participant
5.3	Account	3	Participant
5.4	Private Key	3	Participant
5.5	Token Transfer Data	4	Token
5.6	Session Log Data	4	Token
5.7	Payment Gateway Identity	5	Gateway
5.8	Transaction Data	6	Transaction
6	**Physical Targets**		
6.1	Operational Zone	1	Node
6.1	Participant	3	Participant

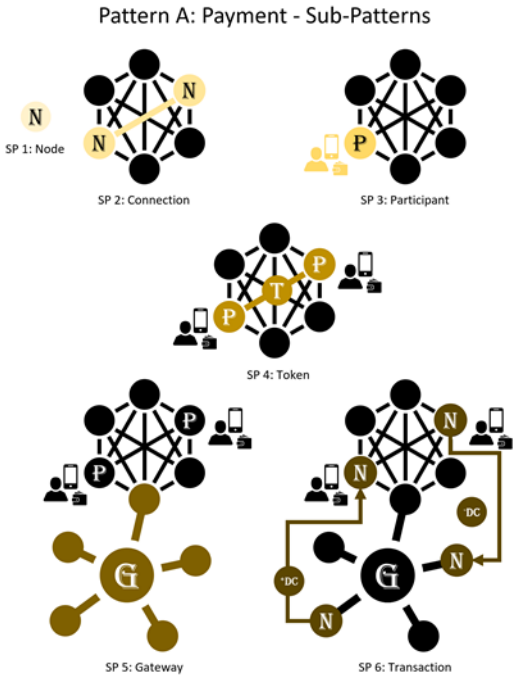


Figure 6: Target Class Sub-patterns

Patterns are formed by the association of various elements and components to deliver a function or service. Different use case patterns can be derived by the same library of Target elements illustrated in Figure 7.

DCE Targets List

#	Payment Targets by Target Class
1	**Application Targets**
1.1	Decentralized Coordination
1.2	Wallet
1.3	Browser
1.4	P2P Token Transfer
1.5	Digital Asset – Token
1.6	P2P DC Payment
2	**Service Targets**
2.1	TCP Connection
2.2	Timestamp
2.3	Interface/Session
2.4	DC Transaction Service
3	**Protocol Targets**
3.1	P2P Network
3.2	Participant|Wallet|Device
3.3	Token Transfer Protocol
3.4	Participant|Wallet|Payment Gateway
3.5	Participant|Wallet|Gateway|Payment
4	**Network Targets**
4.1	Node
4.2	IP Routing Table
4.3	Network Device
4.4	Participant Interface Device
5	**Data Targets**
5.1	IP Address
5.2	Identity
5.3	Account
5.4	Private Key
5.5	Token Transfer Data
5.6	Session Log Data
5.7	Payment Gateway Identity
5.8	Transaction Data
6	**Physical Targets**
6.1	Operational Zone
6.1	Participant

Figure 7: Payment Pattern Elements by Target Class (Right) as a Sub-set of DCE Target Elements

4 Threats to Target Sub-Patterns

The previous section discussed an extensive process to define the Target based on a limited and repeatable number of target elements. This section outlines the next step of the USM process, a Threat-to-Target analysis.

The six sub-patterns under a threat environment are illustrated in Figure 8 and 9. Each sub-pattern adds incremental “Attack Surface.” Each subsequent sub-pattern only considers the additional elements making up the sub-pattern. No previously considered elements can be part of more than one sub-pattern.

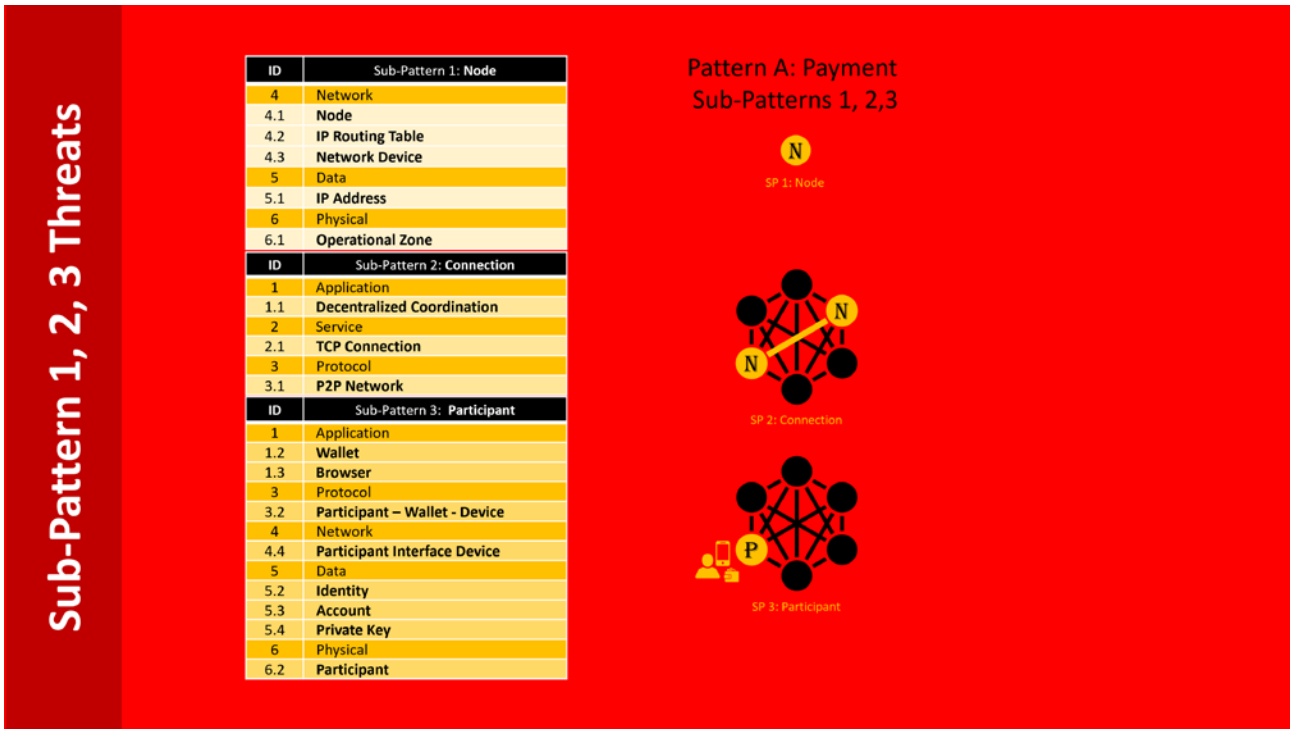


Figure 8: Incremental Target Threat Analysis, Sub-pattern 1, 2, 3

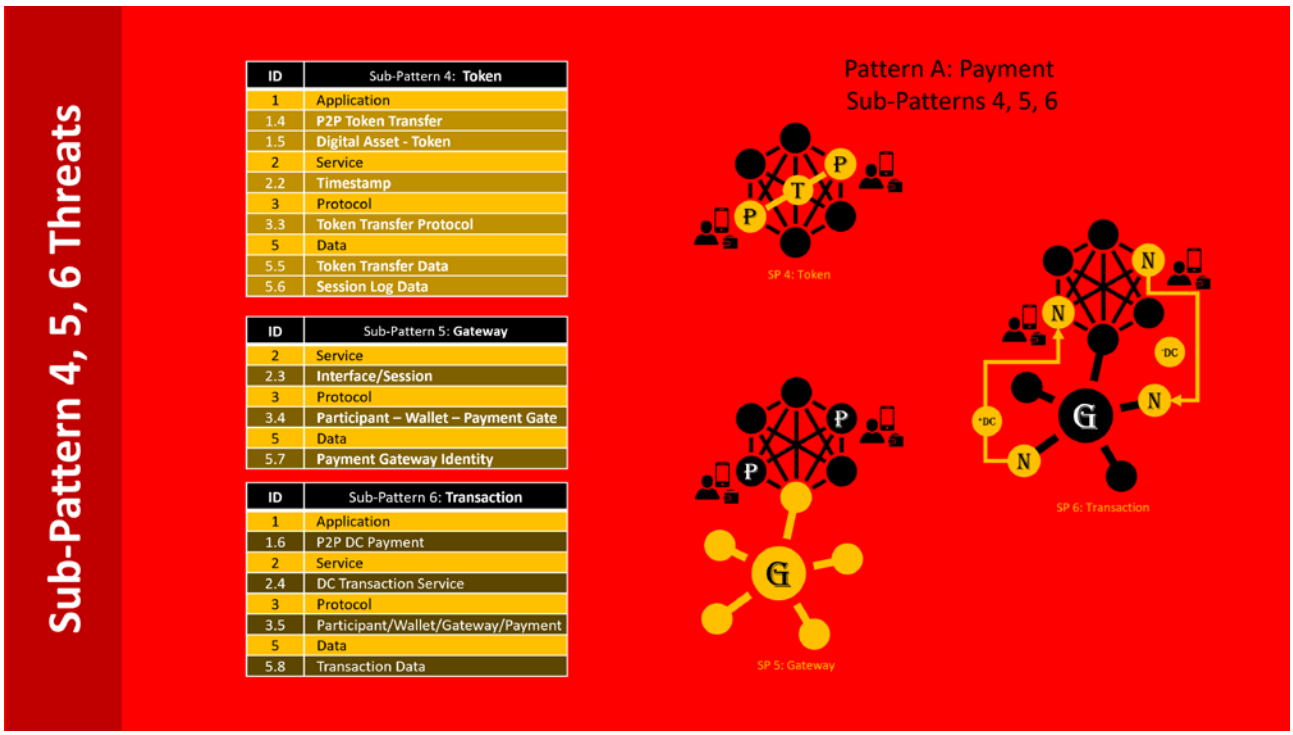


Figure 9: Incremental Target Threat Analysis: Sub-pattern 4, 5,6

The Threat-to-Target analysis has two perspectives consistent with the two target perspectives. Figure 10 illustrates the sub-pattern threats by Target Class which now convert to Target Threat Classes as follows:

- Application Target Threats
- Service Target Threats
- Protocol Target Threats
- Network Target Threats

- Data Target Threats
- Physical Target Threats

Figure 10: Target Threat Classes

The following sub-sections addresses each Target Threat Class individually across all sub-patterns. For each Target Threat Class, the existance of the target in each sub-pattern is highlighted in white. For a constant Target Type, one will investigate how it can be attacked and that attack be mitigated.

Note the work is incomplete and is a work in progress.

4.1 Application Threats Across All Sub-Patterns

The Application targets to each sub-pattern are highlighted in white, if any. For each Application in each sub-pattern, an Application threat vector analysis is now possible.

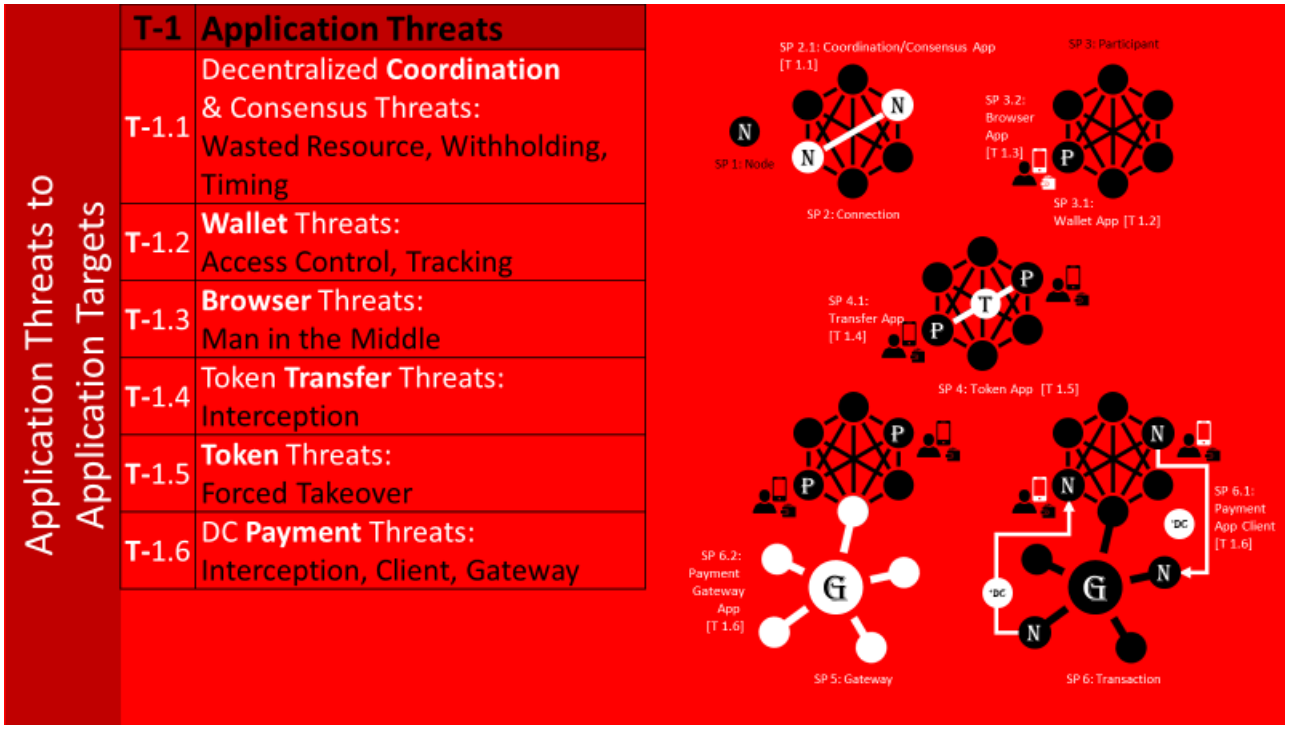


Figure 11: Application Target Threat Class Threats Across all Sub-Patterns

4.2 Network Threats Across All Sub-Patterns

The Network targets to each sub-pattern are highlighted in white, if any. For each Network element in each sub-pattern, an Network threat vector analysis is now possible.

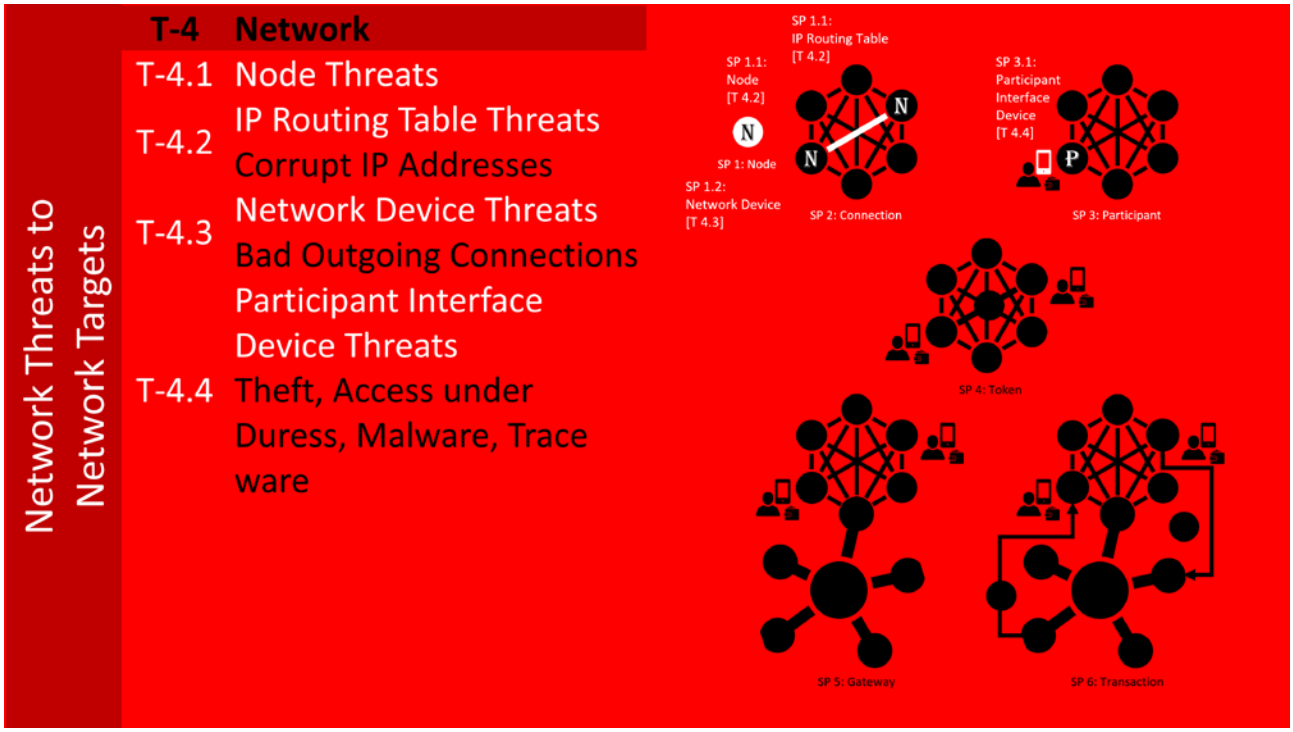


Figure 12: Network Target Threat Class Threats Across all Sub-Patterns

4.3 Protocol Threats Across All Sub-Patterns

The Protocol targets to each sub-pattern are highlighted in white, if any. For each protocol involved in each sub-pattern, a Protocol threat vector analysis is now possible.

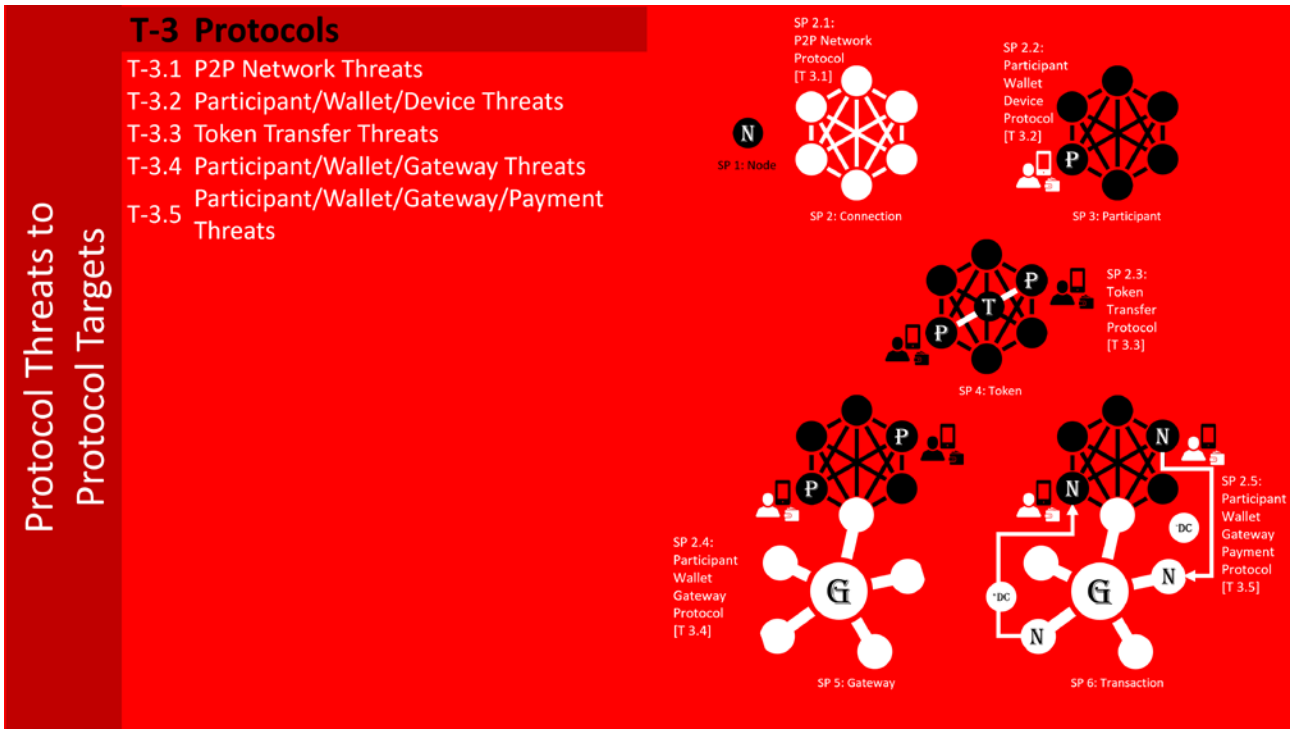


Figure 13: Protocol Target Threat Class Threats Across all Sub-Patterns

4.4 Data Threats Across All Sub-Patterns

The Data targets to each sub-pattern are highlighted in white, if any. It is assumed there is data involved in all activity. The data in each sub-pattern, a Data threat vector analysis is now possible.

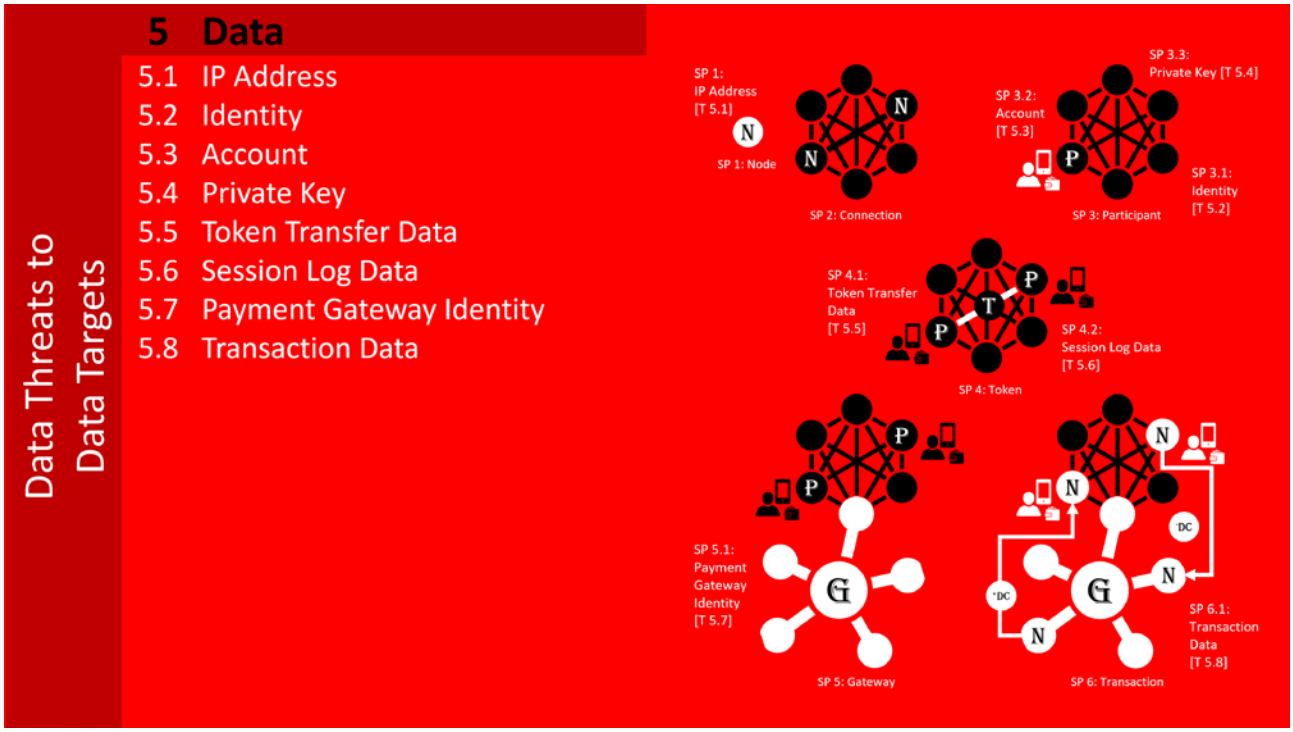


Figure 14: Data Target Threat Class Threats Across all Sub-Patterns

4.5 Service Threats Across All Sub-Patterns

The Service targets to each sub-pattern are highlighted in white, if any. For each Service in each sub-pattern, if any an Service threat vector analysis is now possible.

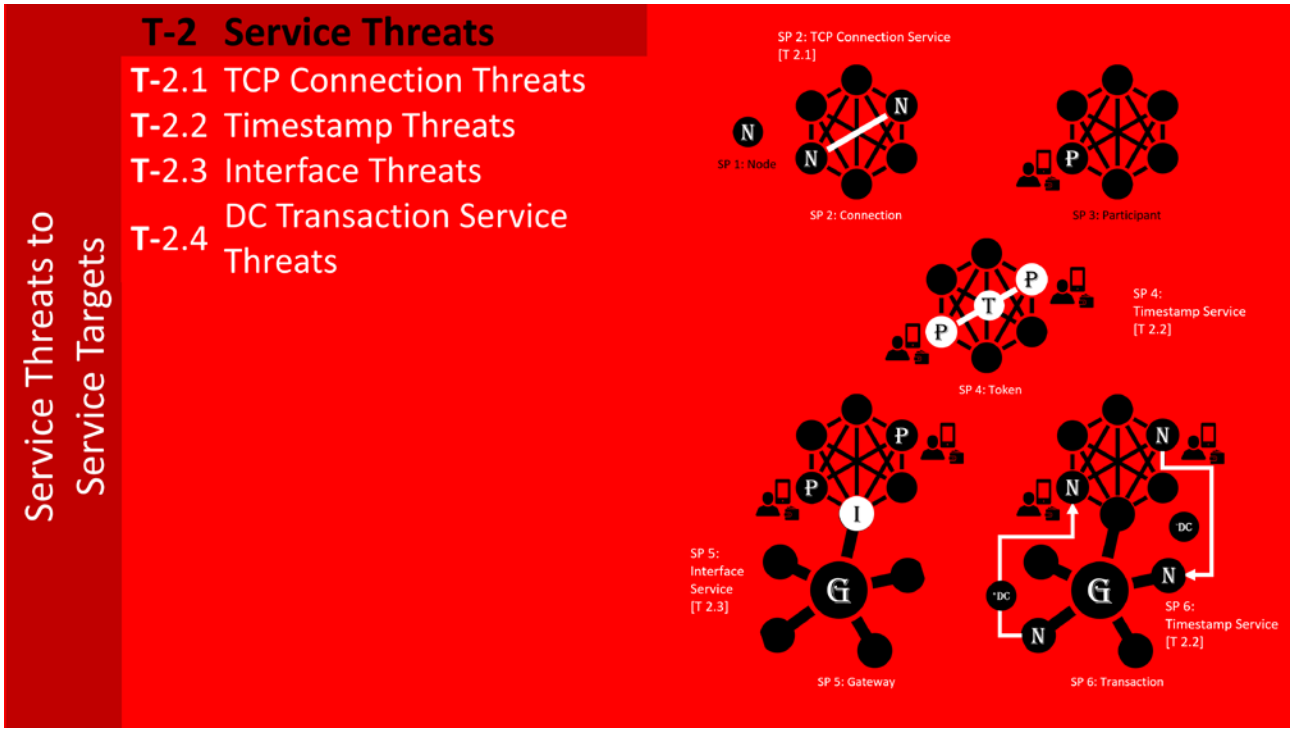


Figure 15: Service Target Threat Class Threats Across all Sub-Patterns

5 Security to Target Countermeasures

The previous sections defined the Target in detail and look at possible threat vectors for each incremental addition of attack surface. The Security-to-Target analysis builds on the previous Target model and Threat analysis. It builds on the same Target architecture on which the threat architecture was also founded.

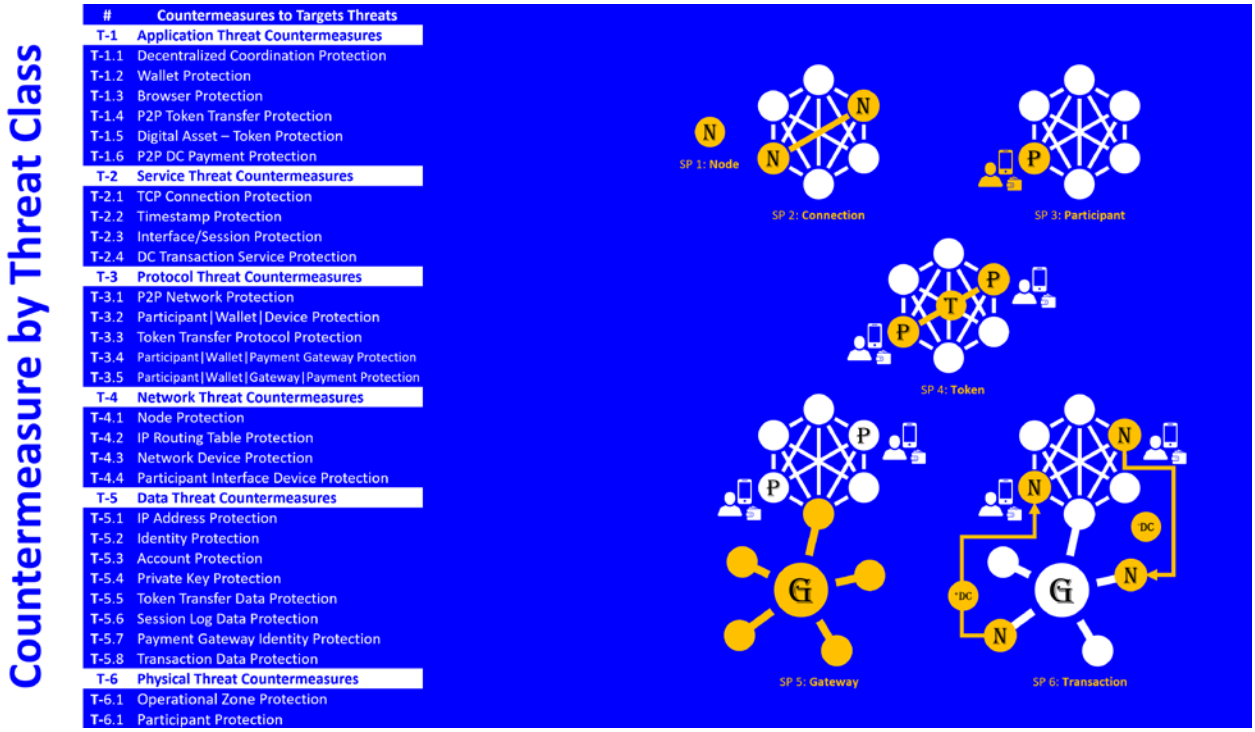


Figure 16: Target Threat Countermeasure by Threat Class

The consistency of the naming nomenclature is critical to improving the communication clarity between Threat, Target and Countermeasure.

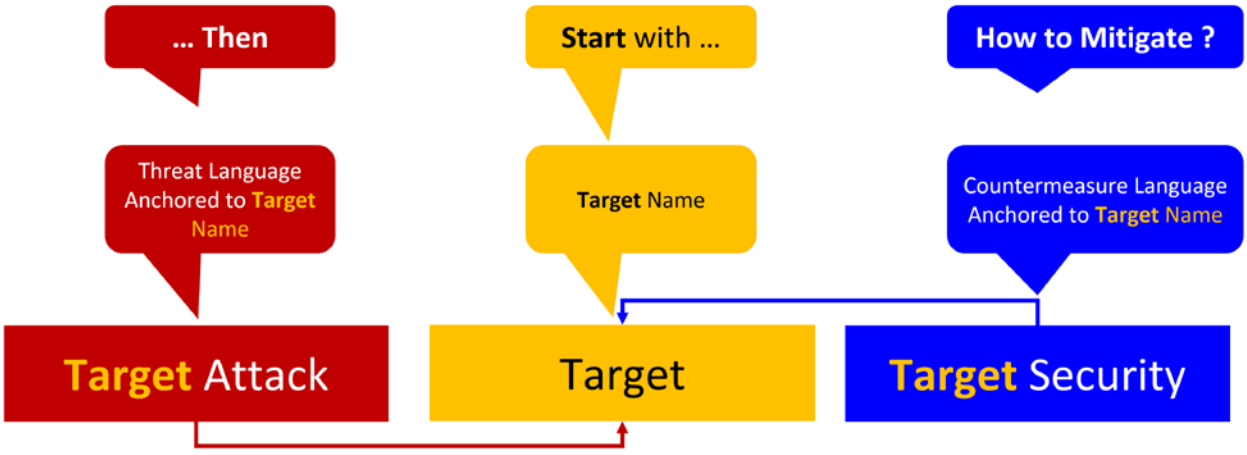


Figure 17: Threat | Target | Security Terminology Nomenclature

As illustrated in Figure 17, it starts with the Target and its formal name. Node, Server, Database, Application, Wallet, Device, Private Key, Account, etc. Since a threat is always executed on some form or target, the name of the threat should always include same Target name. For example, an Eclipse Node Attack, a Routing Table IP Address Corruption attack. Finally, the countermeasure either operates on the attack to detect or deny, for example, or on the Target itself, for example data encryption. Consequently, the name of the Countermeasure should always include the Target and Threat exploit name. For example, Eclipse Node Attack Corrupt IP Address Countermeasure. The result is a clear understanding across the end to end spectrum.

6 Sub-Pattern Threat & Countermeasure Analysis

Figure 18 provides a target template to define patterns and sub-pattern elements. The target is defined as either an application, data or device.

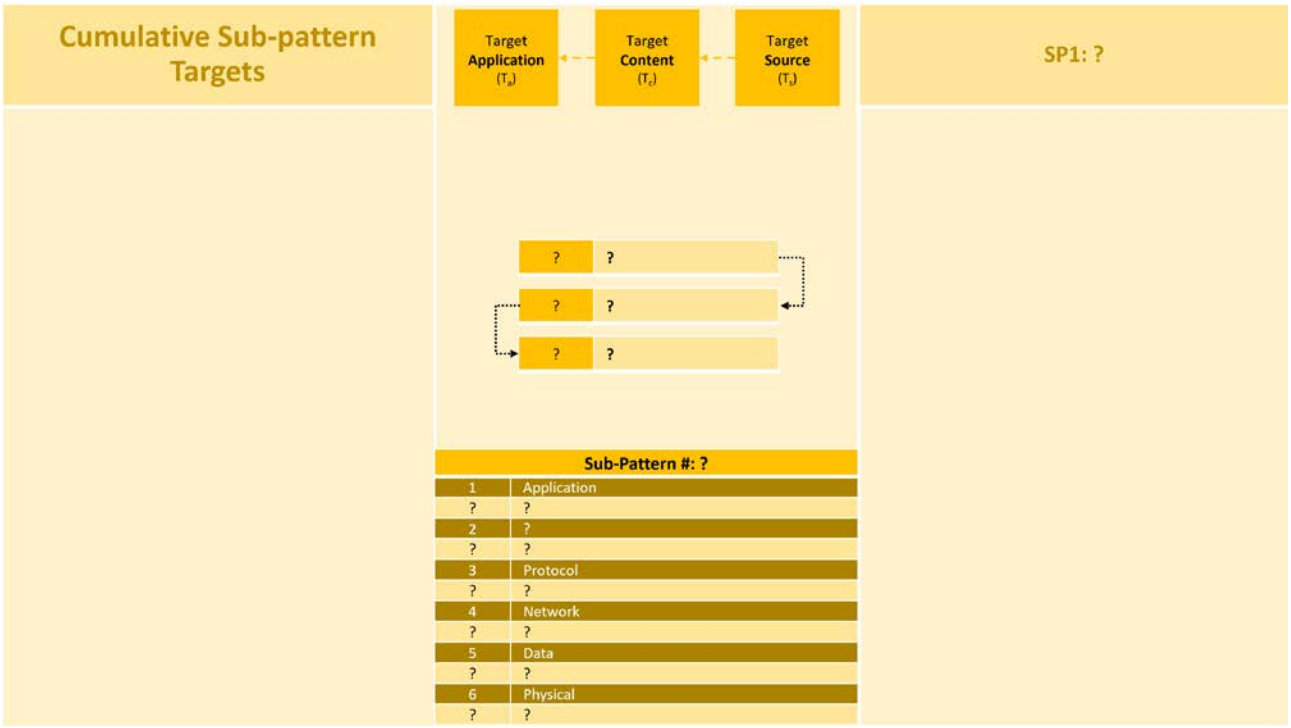


Figure 18: Sub-Pattern Target Element Template

Figure 19 builds on the Target template to provide an Exploit | Vulnerability | Countermeasure template (“EVC”) to identify threat vectors that apply to the Target elements and then to consider effective countermeasures. Note the “?” as they are required to specific the specific exploit on the specific vulnerability and the specific mitigating countermeasure required.

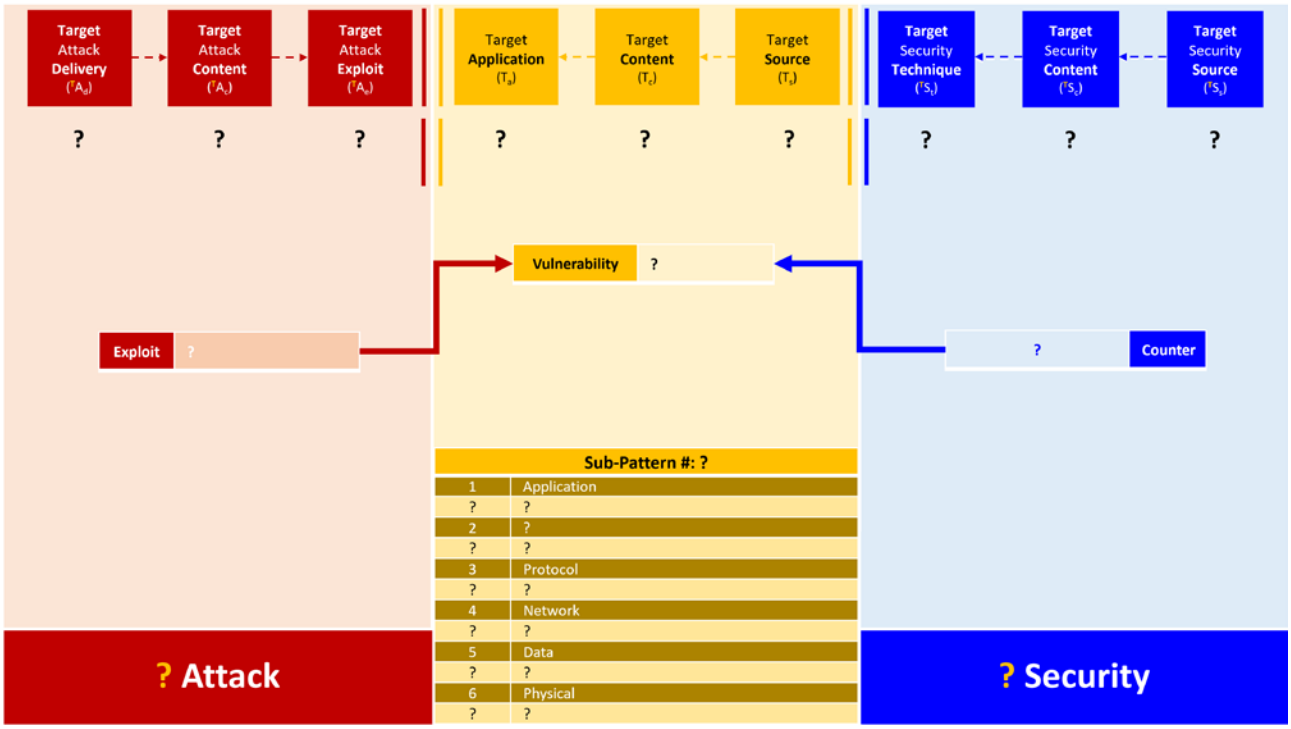


Figure 19: Exploit | Vulnerability | Countermeasure Template

The following sub-sections 5.1 through 5.7 demonstrate the process that was outlined in the previous sections applied to the Payment Pattern.

- The 1st figure of each sub-section is the Target Sub-Pattern with the incremental attack surface in the center and the cumulative sub-patterns off to the left and right of center. This is illustrated in Figure 20, 22, 24, 26, 28, 30 and 32
- The 2nd figure of each sub-section defines threat vectors and countermeasures on sub-pattern elements. This is illustrated in Figure 21, 23, 25, 27, 29, 31 and 32.

6.1 Sub-Pattern 1: Node

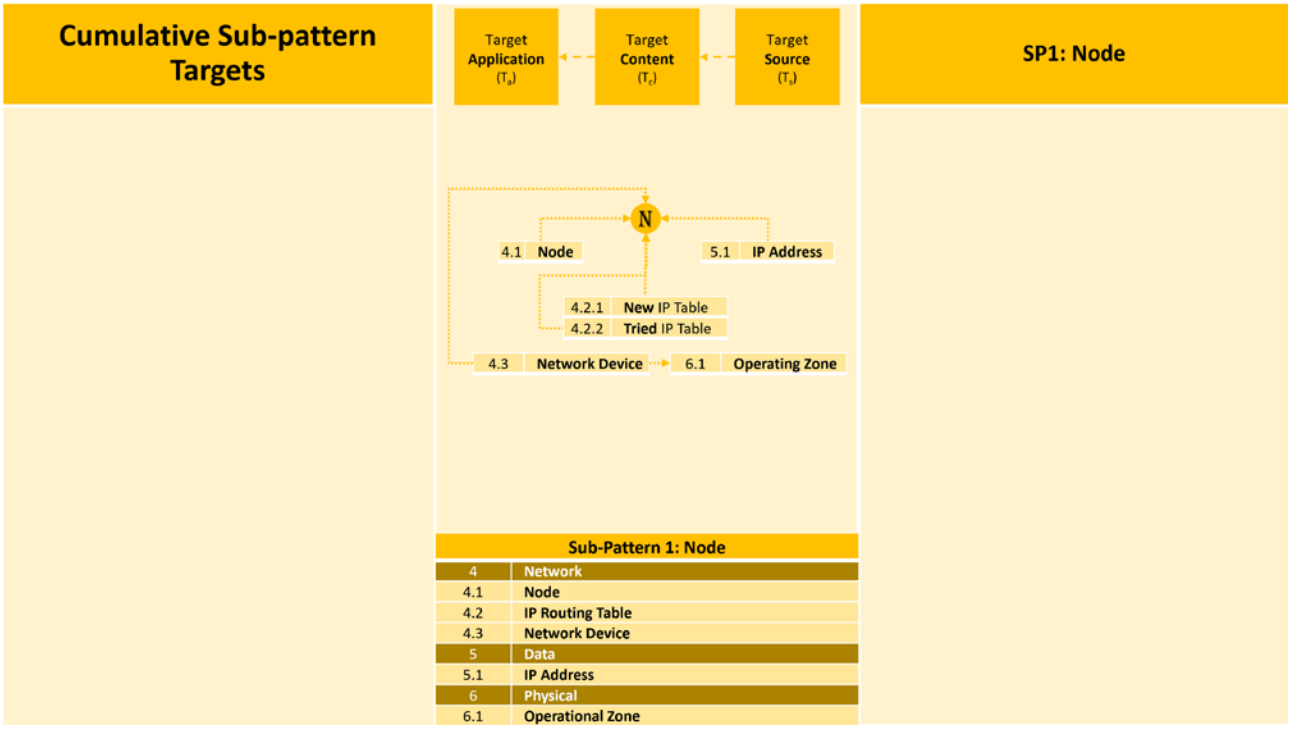


Figure 20: Payment Pattern Sub-Pattern 1: Node

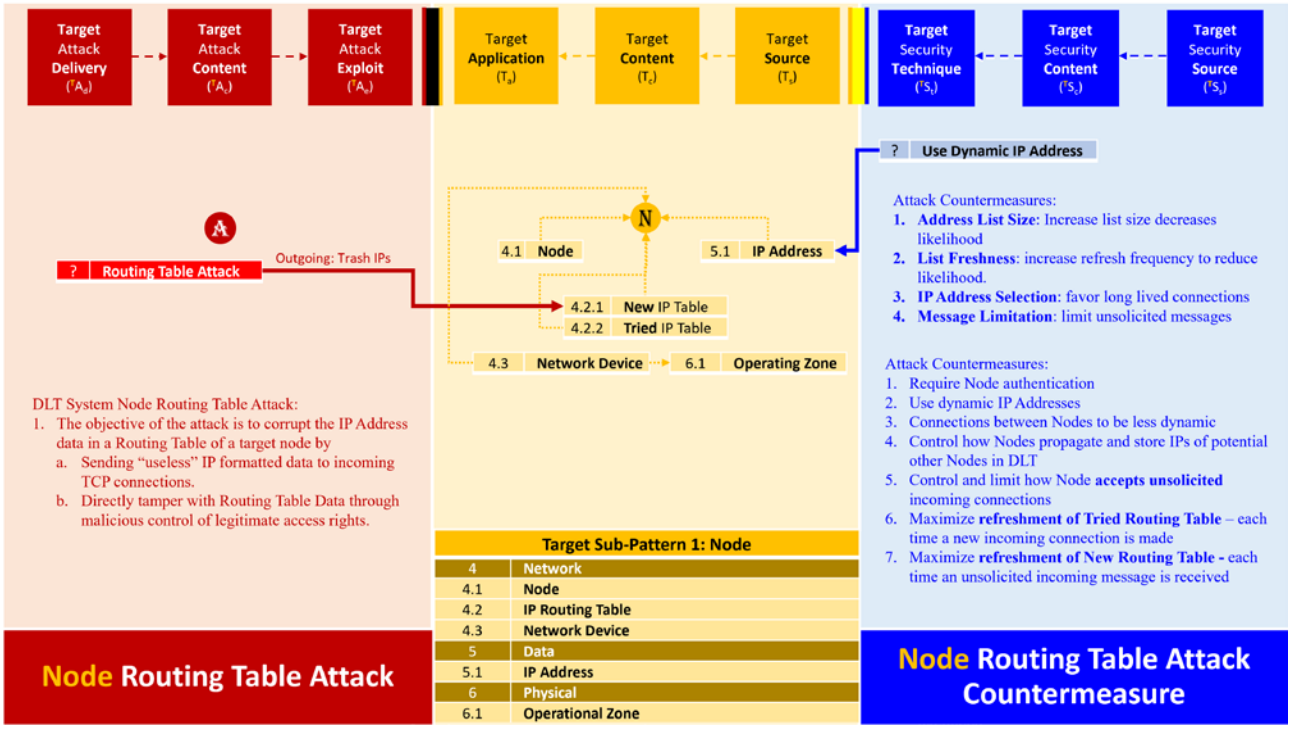


Figure 21: Payment Pattern Sub-Pattern 1: Node Threat and Countermeasures

6.2 Sub-Pattern 2: Connection

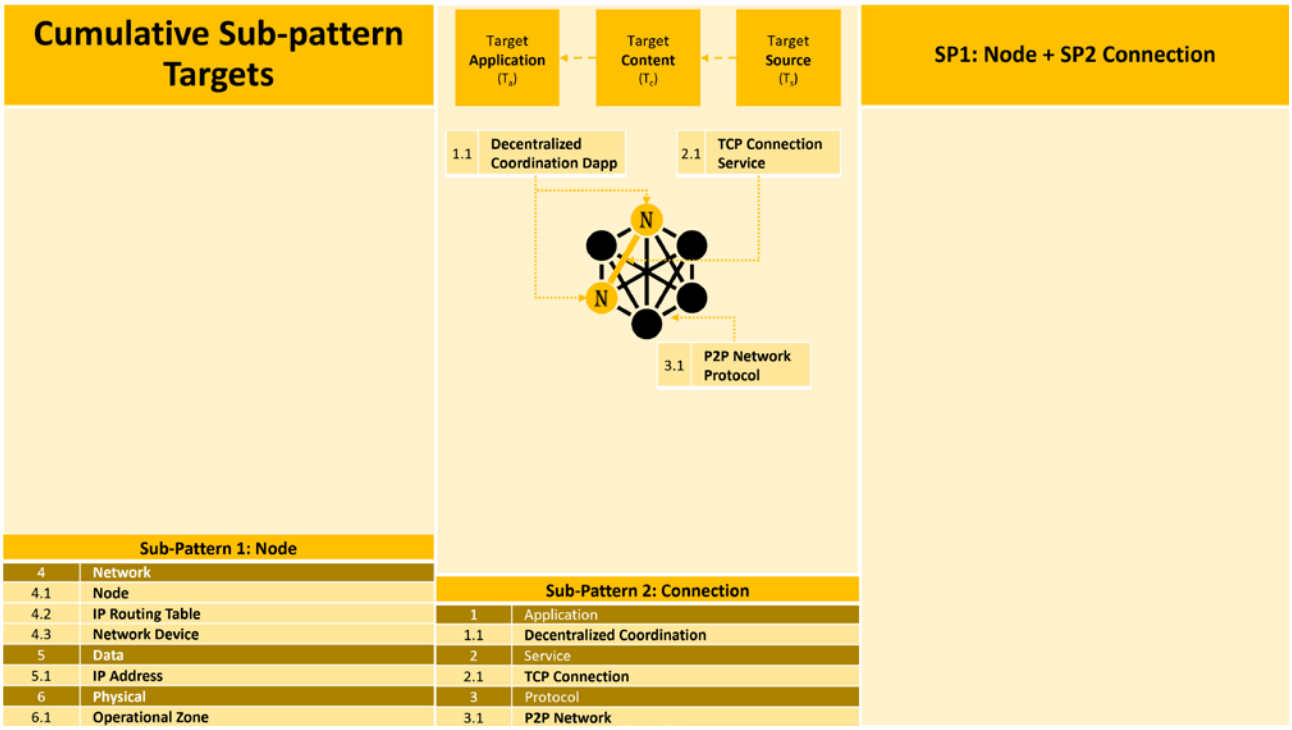


Figure 22: Payment Pattern Sub-Pattern 2: Connection

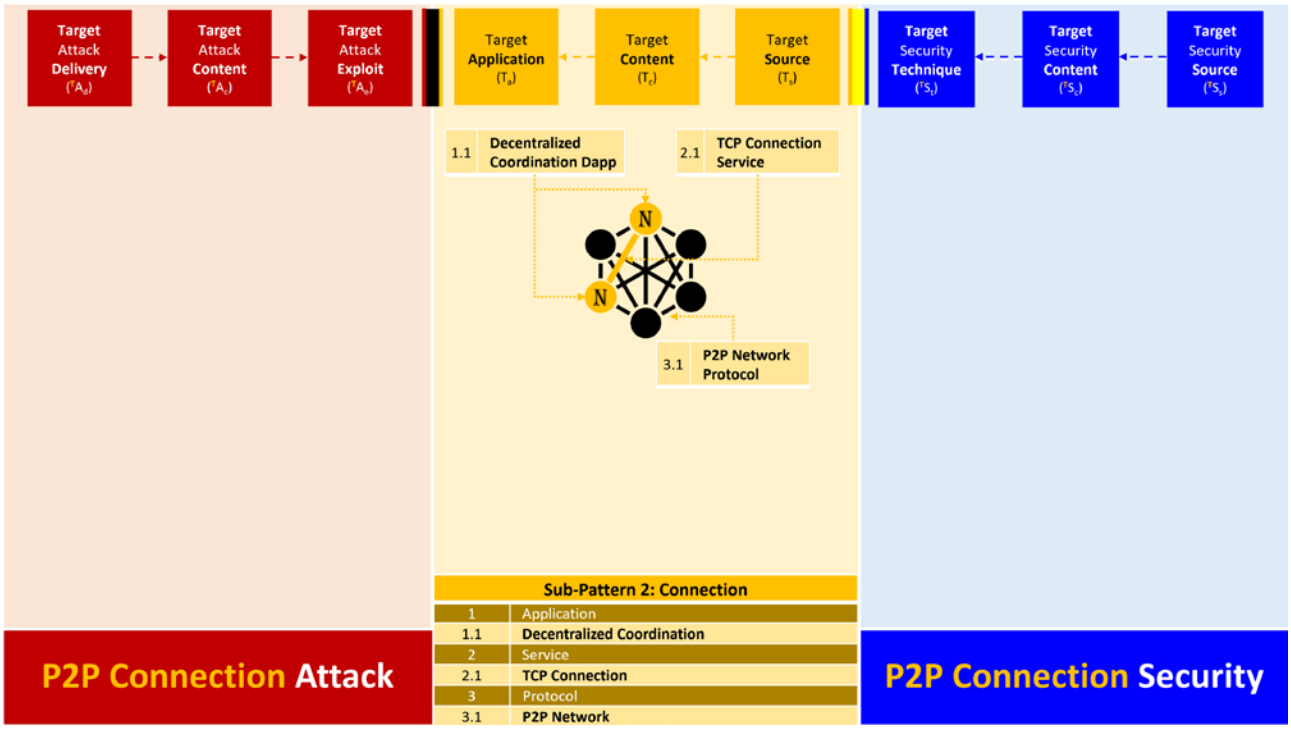


Figure 23: Payment Pattern Sub-Pattern 2: Connection Threat and Countermeasures

6.3 Sub-Pattern 2.1: P2P Network

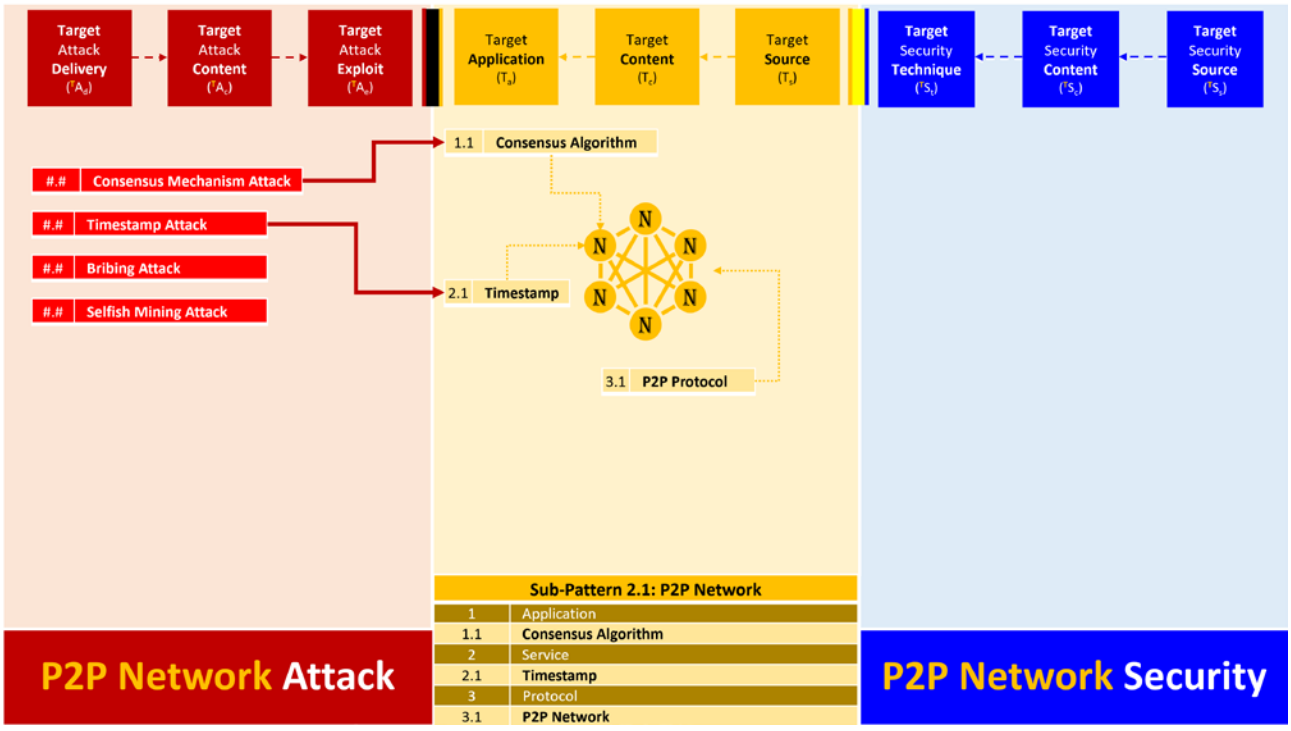


Figure 24 Payment Pattern Sub-Pattern 2.1: P2P Network Threat and Countermeasures

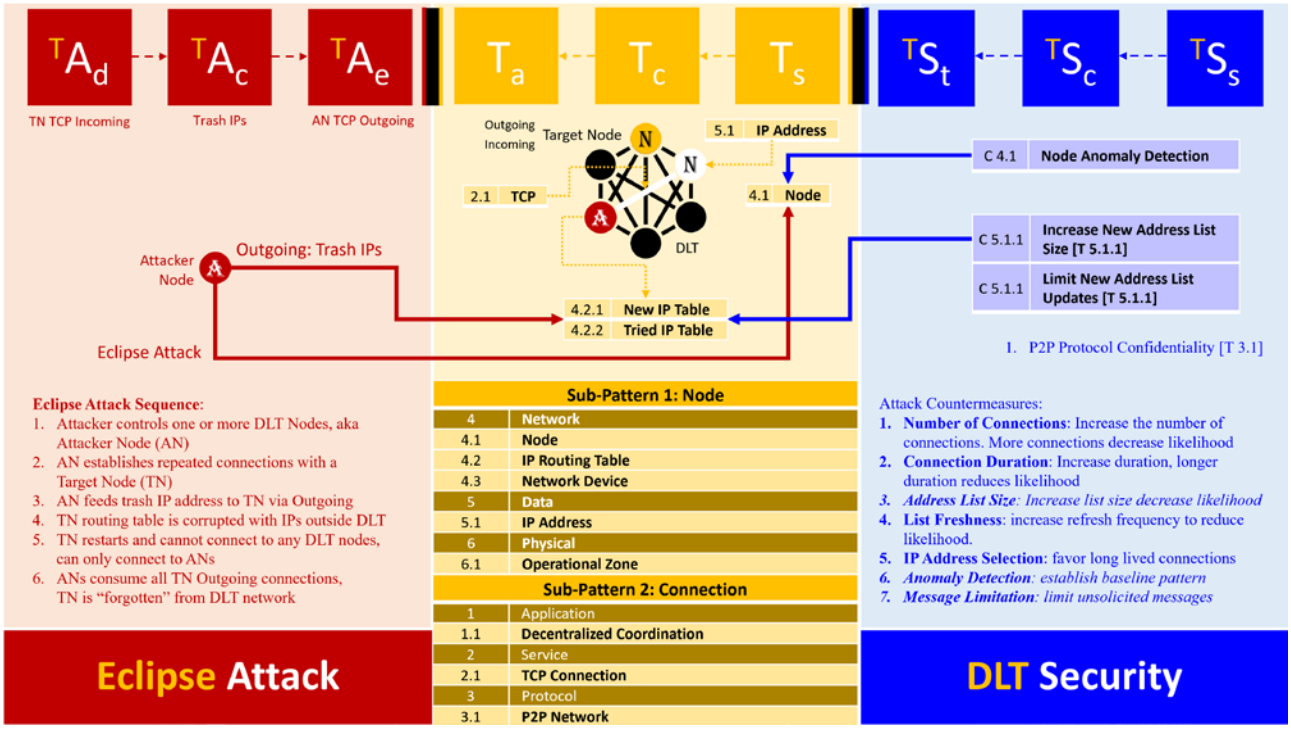


Figure 25: Payment Pattern Sub-Pattern 1 and 2: Eclipse Attack and Countermeasures

6.4 Sub-Pattern 3: Participant

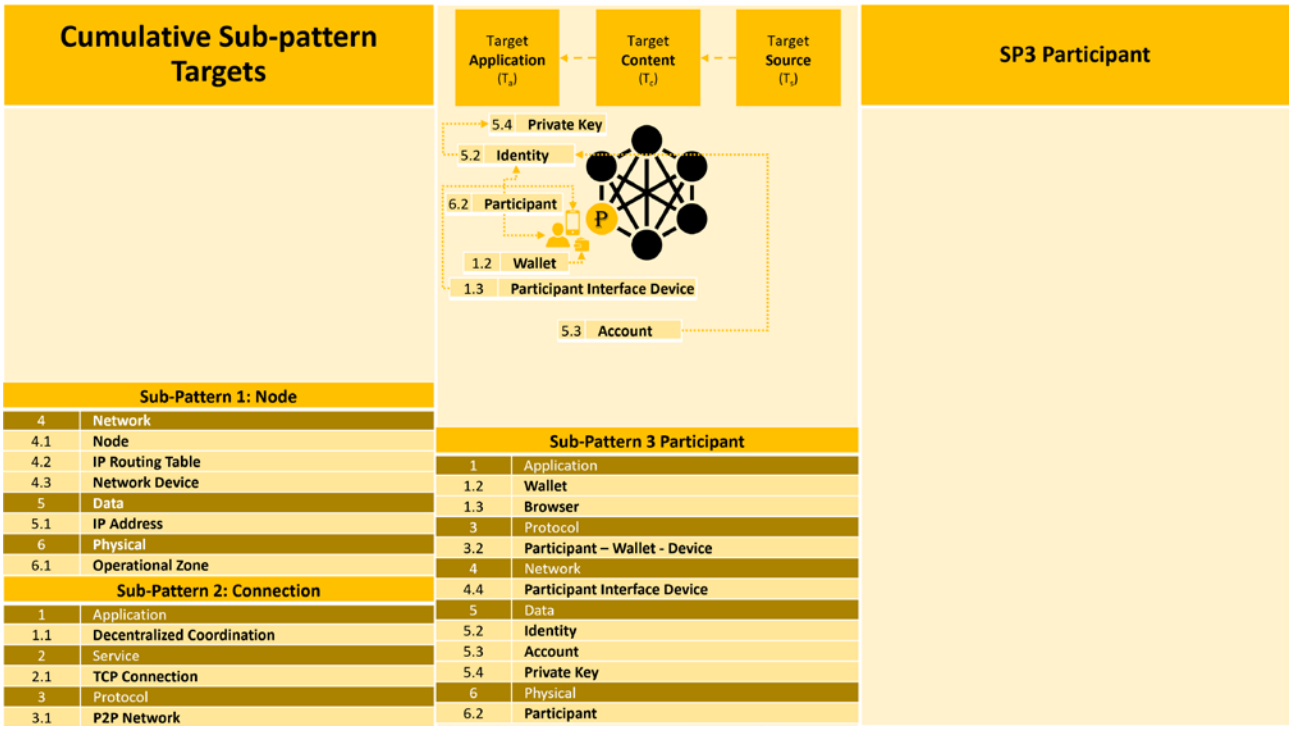


Figure 26 Payment Pattern Sub-Pattern 3: Participant

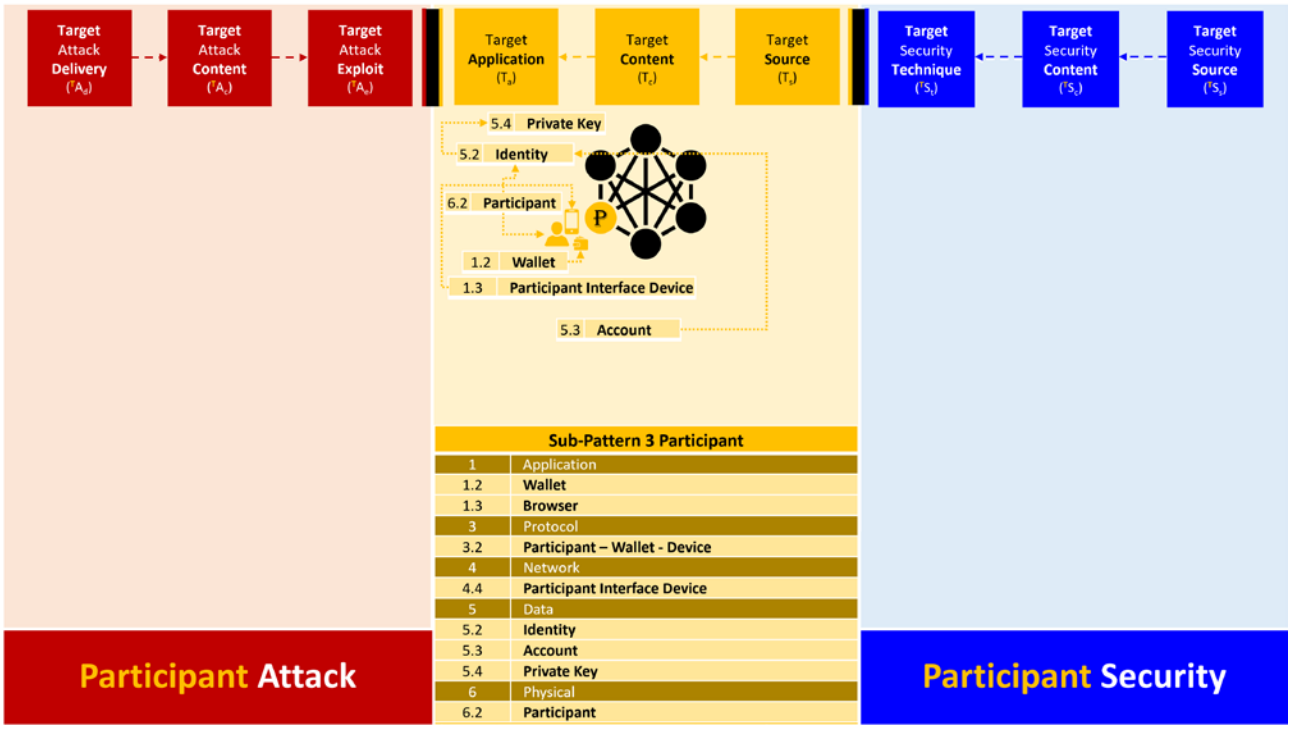


Figure 27: Payment Pattern Sub-Pattern 3: Participant Threat and Countermeasures

6.5 Sub-Pattern 4: Token

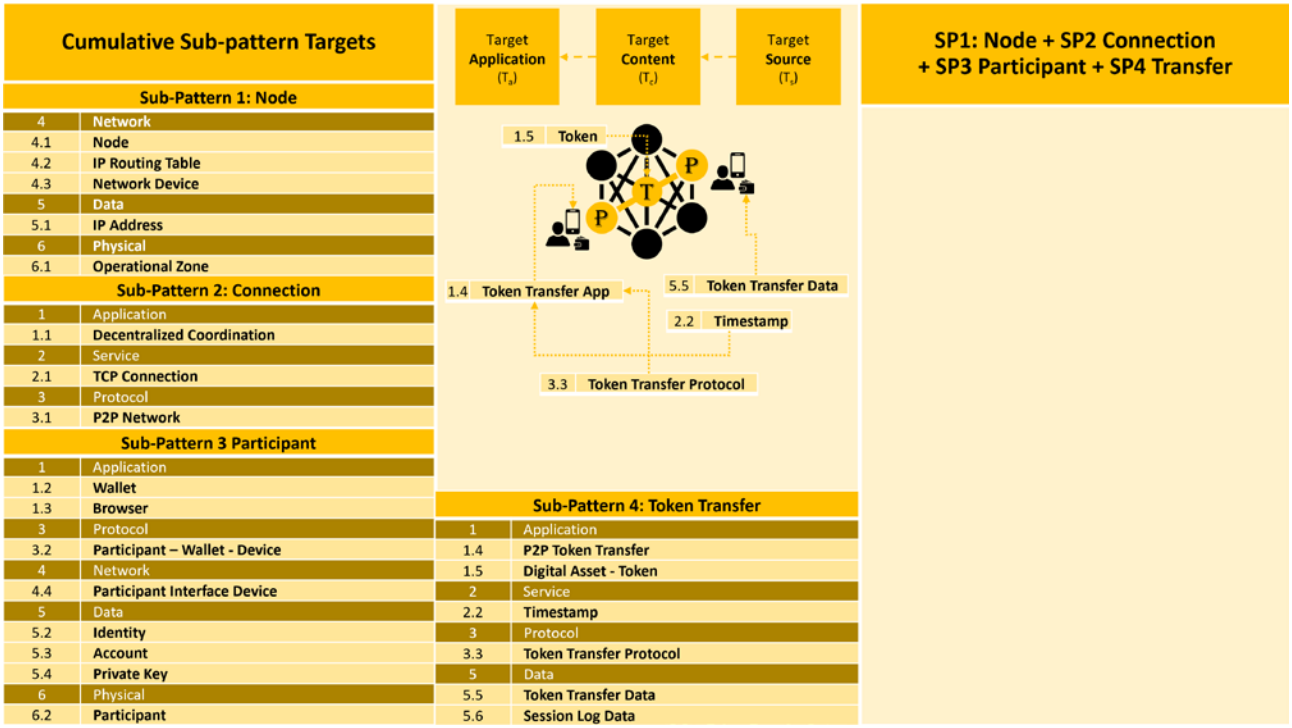


Figure 28: Payment Pattern Sub-Pattern 4: Token

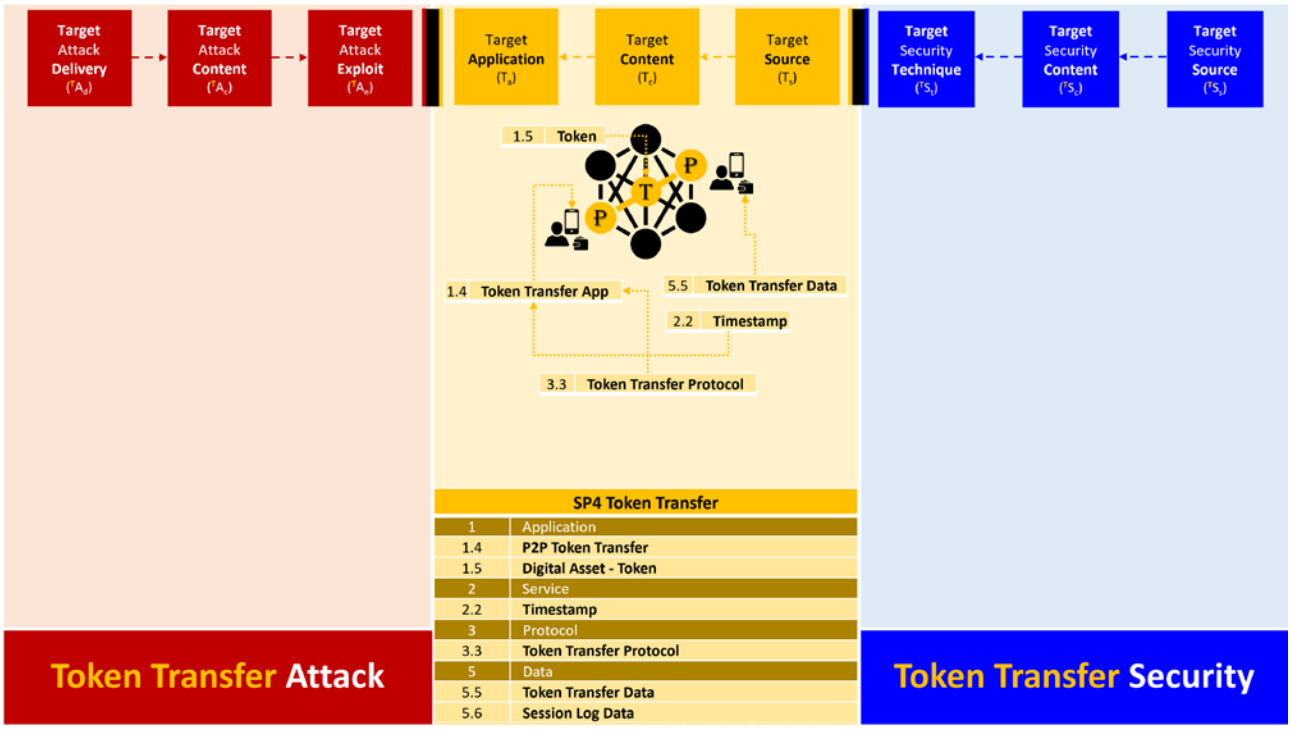


Figure 29: Payment Pattern Sub-Pattern 4: Token Transfer Threat and Countermeasures

6.6 Sub-Pattern 5: Payment Gateway

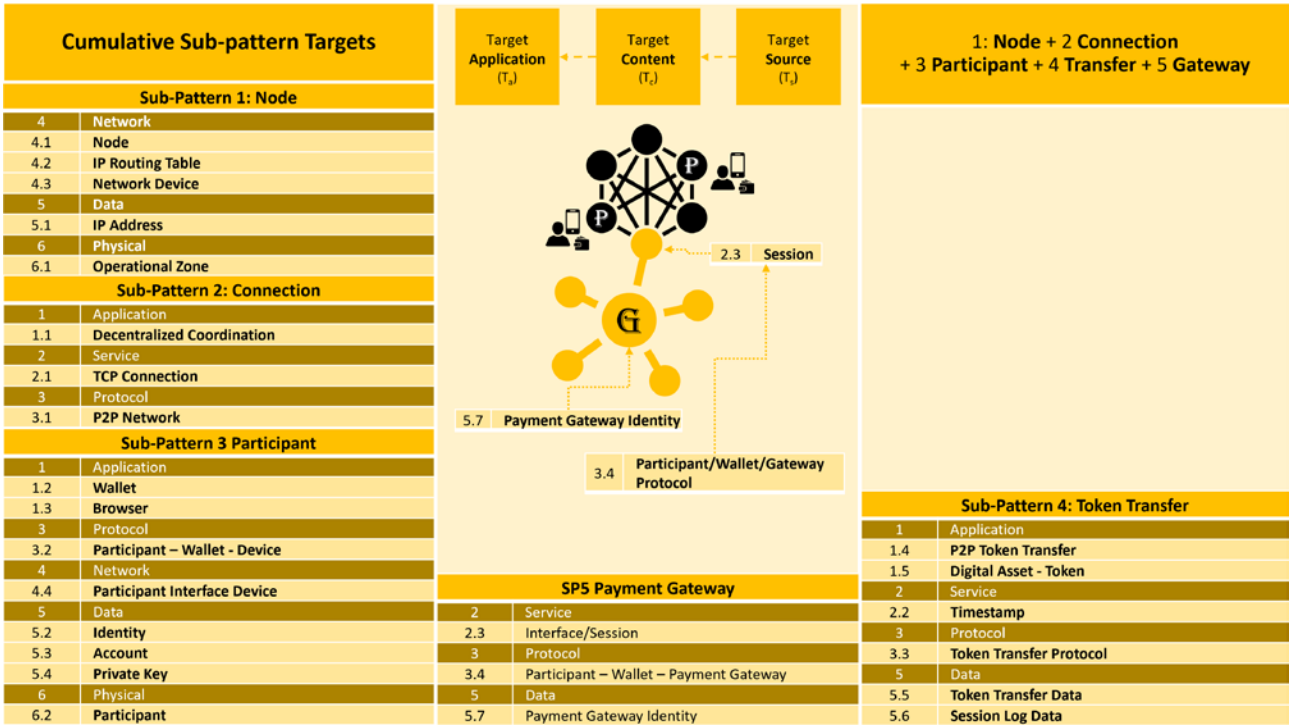


Figure 30: Payment Pattern Sub-Pattern 5: Payment Gateway

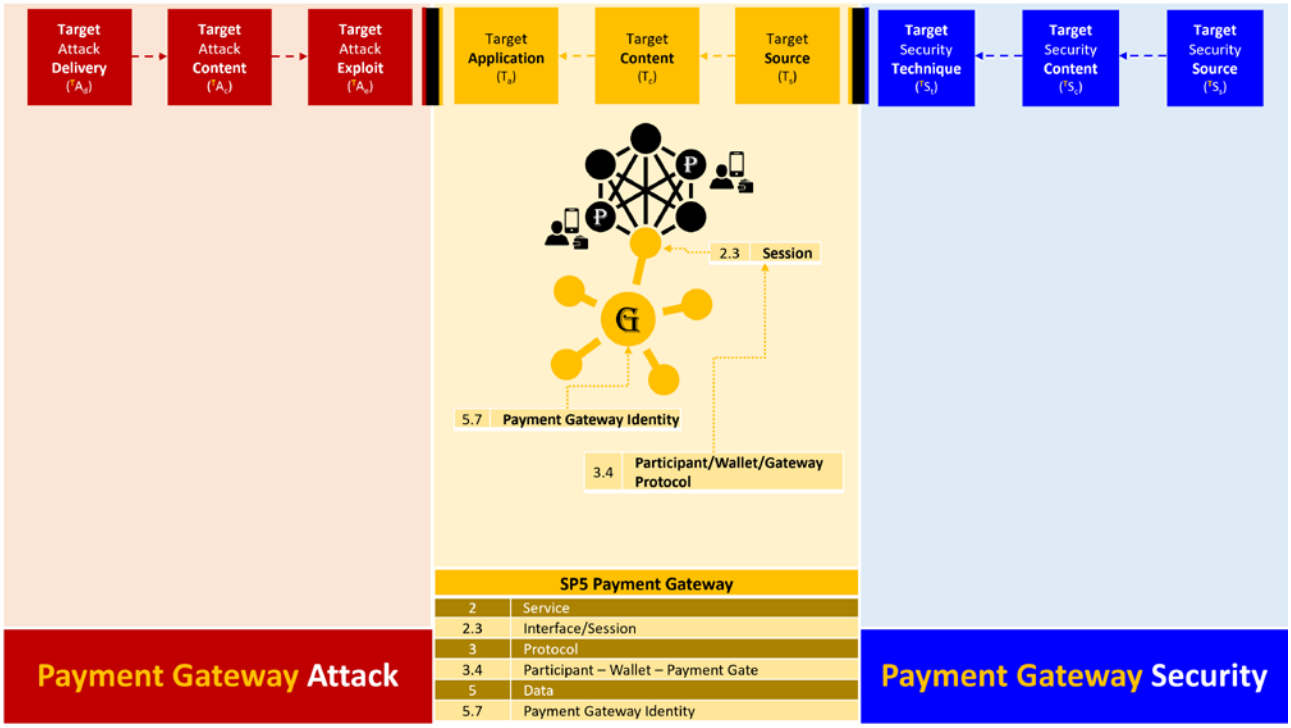


Figure 31: Payment Pattern Sub-Pattern 5: Payment Gateway Threat and Countermeasures

6.7 Sub-Pattern 6: DC Transaction

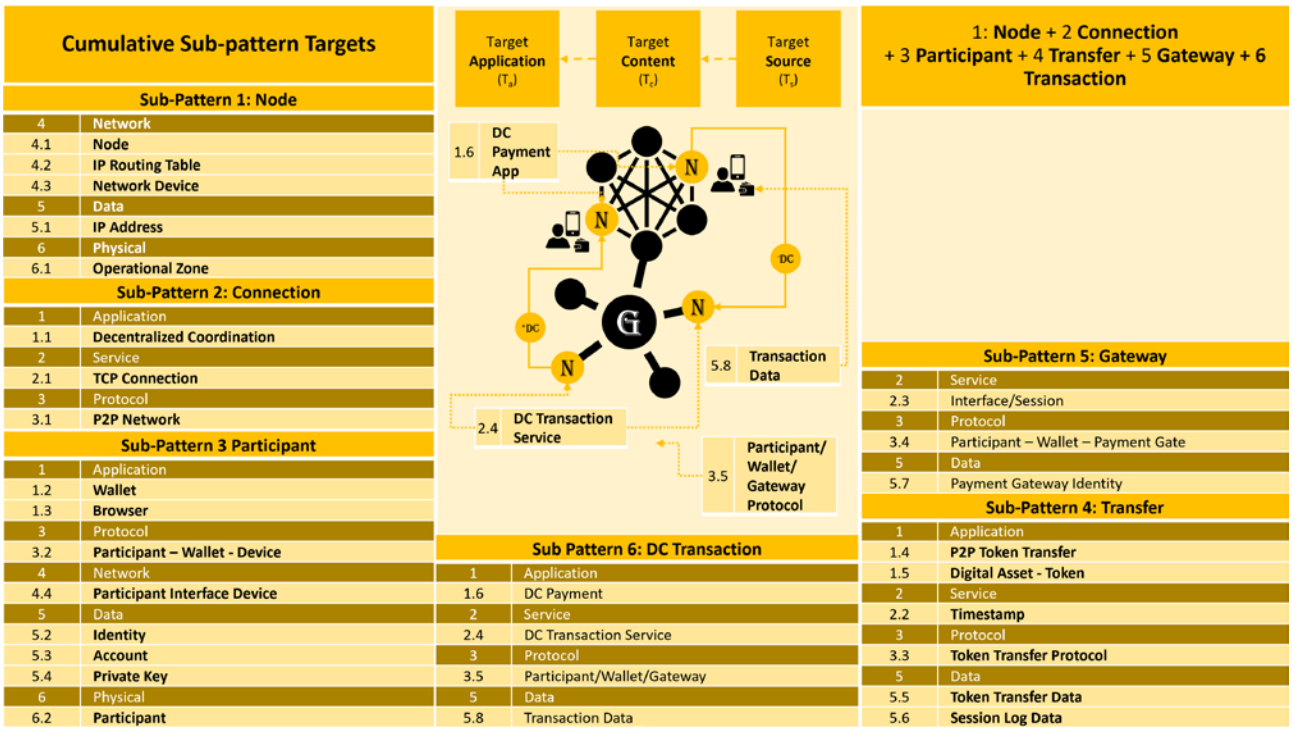


Figure 32: Payment Pattern Sub-Pattern 6: Transaction

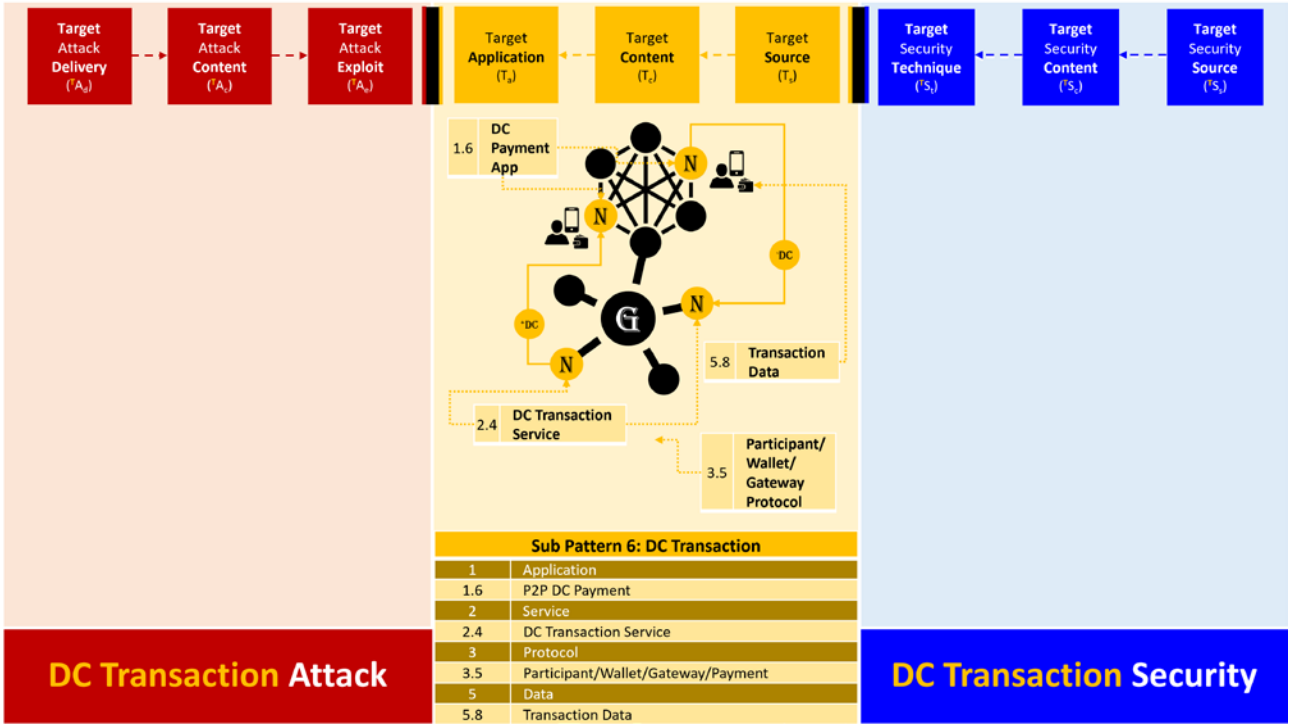


Figure 33: Payment Pattern Sub-Pattern 6: DC Transaction Threat and Countermeasures