Simplifying Bayesian belief network to reveal expected pattern sequence based on conditionally dependent patterns

Thursday, August 1, 2024 8:12 PM

The following Bayesian belief network graph reflects the relationships between patterns in one considered sequence of patterns. These relationships between patterns are extracted from their textual descriptions. So, for example, if the Secure Channels pattern refers to the Asymmetric Encryption pattern as a pattern that can be used further, then an oriented edge pointing to the Asymmetric Encryption node is drawn between them. If the Asymmetric Encryption pattern also refers to the Secure Channels pattern, a two-way oriented edge is drawn between the patterns.

The considered sequence of patterns is:

Secure Channels → Asymmetric Encryption → Third Party-Based Authentication → Mutual Authentication → Credential → Security Session → Check Point

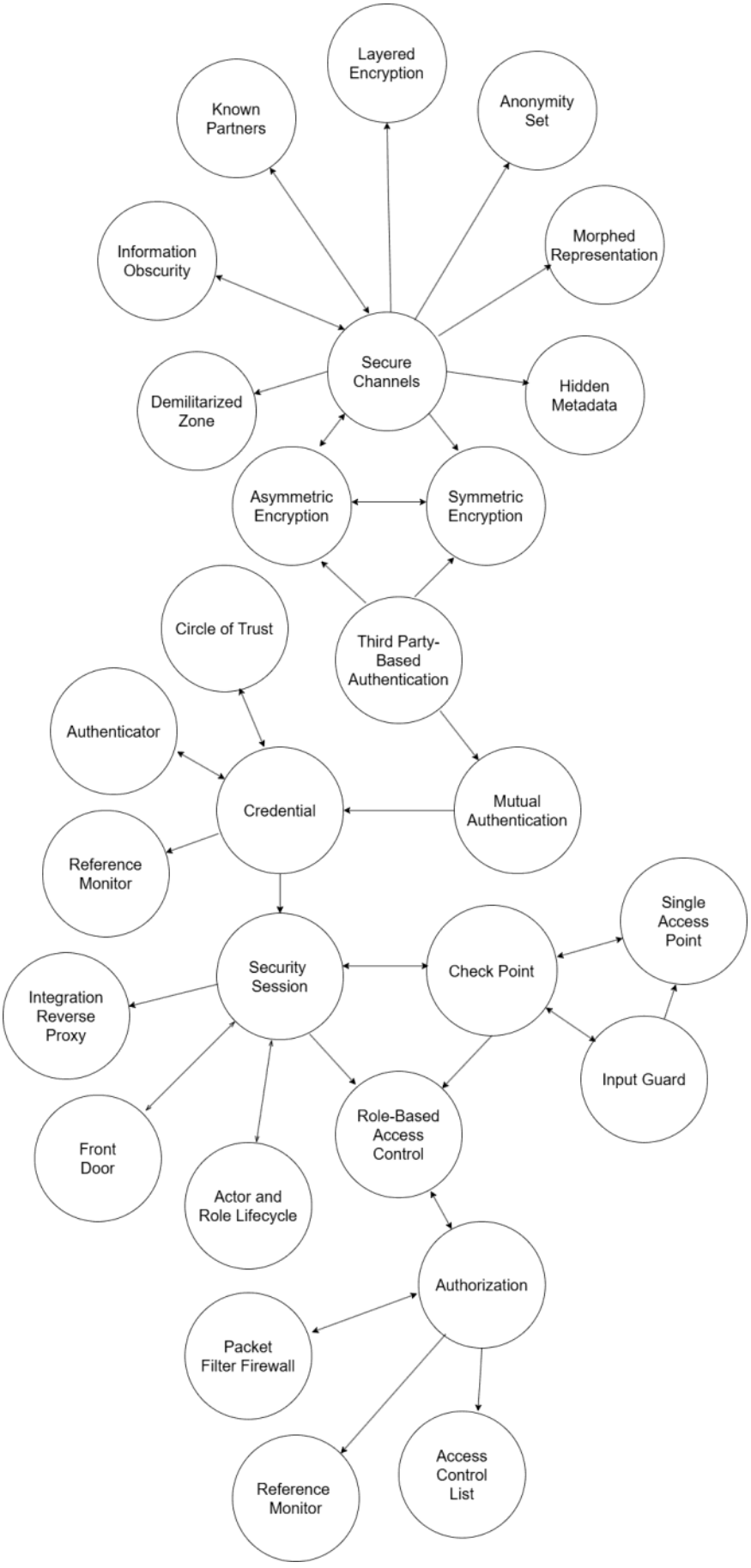
and it was established by authors of this article. This sequence of patterns is meaningful and can be described by a story about the use of patterns (standard technique). Patterns from this sequence are highlighted by a bold edge in the Bayesian belief network.

The goal behind simplifying Bayesian belief network is to find which patterns are conditionally independent and conditionally dependent on each other. I leave the conditionally dependent patterns connected by an edge (highlighted in red), between the conditionally independent patterns the edge is colored green (green indicates the edge that must be removed).

For example, after the Secure Channels pattern, it is possible to use the Asymmetric Encryption or Symmetric Encryption pattern, and therefore the question is which pattern from the pair of patterns (Asymmetric Encryption, Symmetric Encryption) should be used after the Secure Channels pattern. I expect that the Bayesian belief network will help me find answers to such questions.

The assumption is that the Bayesian belief network, after removing the edges between conditionally independent patterns, reveals a sequence that is more expected than the one at the beginning, after taking into account the conditional dependencies between the patterns.

The Bayesian belief network has 28 nodes.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Front Door
Role-Based Access Control
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

The variables of the probabilistic model are:

- Secure Channels ∈ {0, 1} Secure Channels = 1 means that the pattern is used, Secure Channels = 0 means that it is not used.
- Demilitarized Zone ∈ {0, 1} Demilitarized Zone = 1 means that the pattern is used, Demilitarized Zone = 0 means that it is not used.
- Information Obscurity ∈ {0, 1} Information Obscurity = 1 means that the pattern is used, Information Obscurity = 0 means that it is not used.
- Known Partners ∈ {0, 1} Known Partners = 1 means that the pattern is used, Known Partners = 0 means that it is not used.
- Layered Encryption ∈ {0, 1} Layered Encryption = 1 means that the pattern is used, Layered Encryption = 0 means that it is not used.
- Anonymity Set ∈ {0, 1} Anonymity Set = 1 means that the pattern is used, Anonymity Set = 0 means that it is not used.
- Morphed Representation ∈ {0, 1} Morphed Representation = 1 means that the pattern is used, Morphed Representation = 0 means that it is not used.
- Hidden Metadata ∈ {0, 1} Hidden Metadata = 1 means that the pattern is used, Hidden Metadata = 0 means that it is not used.
- Asymmetric Encryption ∈ {0, 1} Asymmetric Encryption = 1 means that the pattern is used, Asymmetric Encryption = 0 means that it is not used.
- Symmetric Encryption ∈ {0, 1} Symmetric Encryption = 1 means that the pattern is used, Symmetric Encryption = 0 means that it is not used.
- Third Party-Based Authentication ∈ {0, 1} Third Party-Based Authentication = 1 means that the pattern is used, Third Party-Based Authentication = 0 means that it is not used.
- Mutual Authentication ∈ {0, 1} Mutual Authentication = 1 means that the pattern is used, Mutual Authentication = 0 means that it is not used.
- Credential ∈ {0, 1} Credential = 1 means that the pattern is used, Credential = 0 means that it is not used.
- Circle of Trust ∈ {0, 1} Circle of Trust = 1 means that the pattern is used, Circle of Trust = 0 means that it is not used.
- Authenticator ∈ {0, 1} Authenticator = 1 means that the pattern is used, Authenticator = 0 means that it is not used.
- Reference Monitor ∈ {0, 1} Reference Monitor = 1 means that the pattern is used, Reference Monitor = 0 means that it is not used.
- Security Session ∈ {0, 1} Security Session = 1 means that the pattern is used, Security Session = 0 means that it is not used.
- Integration Reverse Proxy ∈ {0, 1} Integration Reverse Proxy = 1 means that the pattern is used, Integration Reverse Proxy = 0 means that it is not used.
- Front Door ∈ {0, 1} Front Door = 1 means that the pattern is used, Front Door = 0 means that it is not used.
- Actor and Role Lifecycle ∈ {0, 1} Actor and Role Lifecycle = 1 means that the pattern is used, Actor and Role Lifecycle = 0 means that it is not used.
- Check Point ∈ {0, 1} Check Point = 1 means that the pattern is used, Check Point = 0 means that it is not used.
- Single Access Point ∈ {0, 1} Single Access Point = 1 means that the pattern is used, Single Access Point = 0 means that it is not used.
- Input Guard ∈ {0, 1} Input Guard = 1 means that the pattern is used, Input Guard = 0 means that it is not used.
- Role-Based Access Control ∈ {0, 1} Role-Based Access Control = 1 means that the pattern is used, Role-Based Access Control = 0 means that it is not used.
- Authorization ∈ {0, 1} Authorization = 1 means that the pattern is used, Authorization = 0 means that it is not used.

- Packet Filter Firewall ∈ {0, 1} Packet Filter Firewall = 1 means that the pattern is used, Packet Filter Firewall = 0 means that it is not used.
- Reference Monitor ∈ {0, 1} Reference Monitor = 1 means that the pattern is used, Reference Monitor = 0 means that it is not used.
- Access Control List ∈ {0, 1} Access Control List = 1 means that the pattern is used, Access Control List = 0 means that it is not used.

The probability model of the Bayesian belief network of such a sequence if we read the graph from top to bottom is:

*p(Check Point | Security Session) * p(Security Session | Credential) **
*p(Credential | Mutual Authentication, Circle of Trust, Authenticator, Reference Monitor) **
*p(Mutual Authentication | Third Party-Based Authentication) **
*p(Third Party-Based Authentication | Asymmetric Encryption, Symmetric Encryption)**
*p(Symmetric Encryption | Secure Channels)*p(Asymmetric Encryption | Secure Channels)*

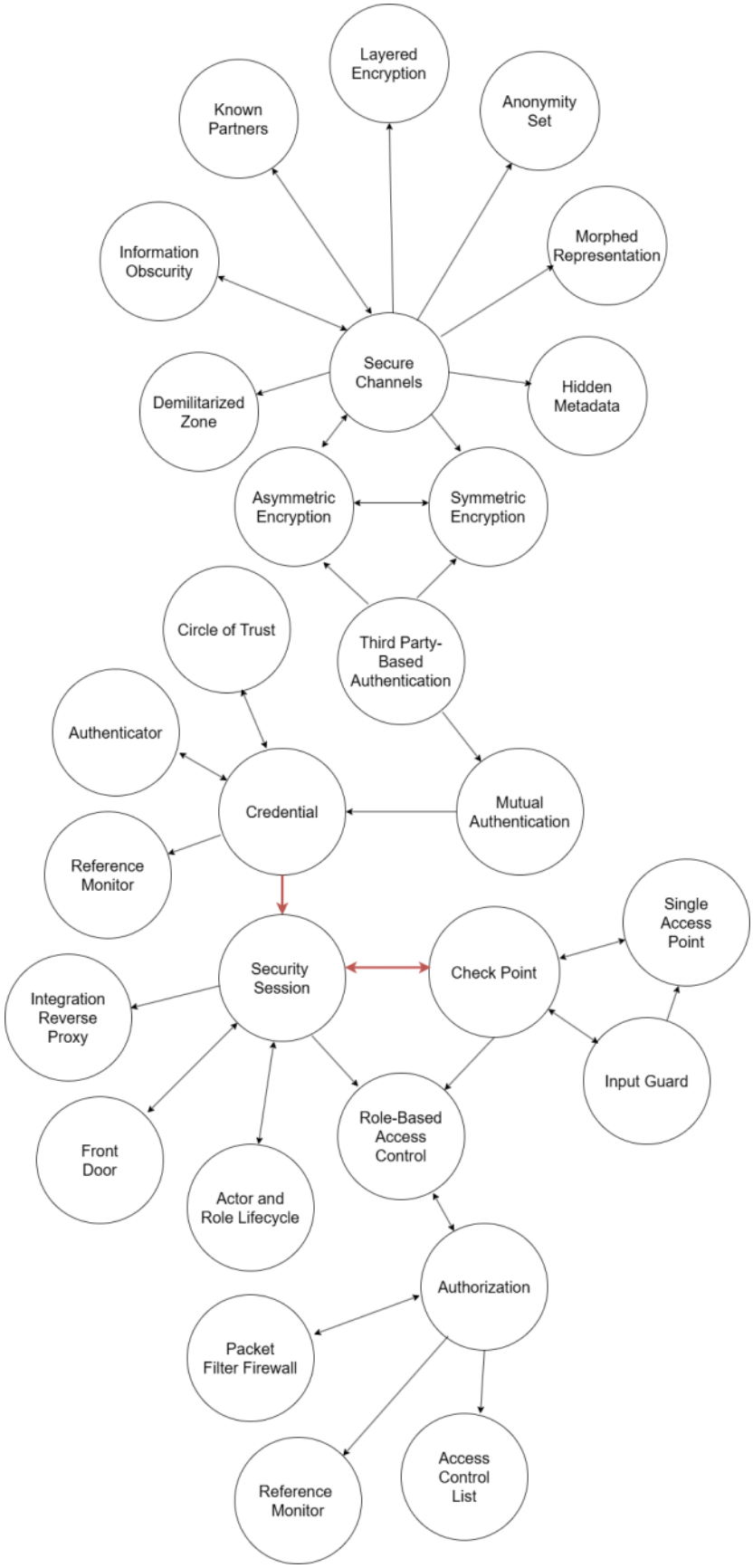
I divided the simplification of the Bayesian belief network into the following points:

1. **Is it possible to keep the Credential, Security Session, and Check Point nodes connected in the network?** Answering this question requires:

   Is the Check Point pattern conditionally independent of the Credential pattern, if the use of the Check Point pattern requires the use of a Security Session? In other words, we are asking whether the equality p(Check Point, Credential | Security Session) = p(Check Point | Security Session)*p(Credential | Security Session) holds. This equality does not apply when looking at the graph, because p(Check Point, Credential | Security Session) ∝ p(Security Session | Credential)*p(Credential)*p(Check Point | Security Session).

   There is only one path between the Credential, Security Session, and Check Point nodes. On that path is the node Security Session collider which is in condition p(Credential, Check Point | Security Session). The path between Credential and Check Point is not blocked and these nodes are not d-separated. Therefore, the Credential pattern and Check Point patterns are conditionally dependent on each other, knowing that Security Session can be used between them.

   The Credential, Security Session, and Check Point nodes remain connected as they are, because the Credential and Check Point patterns are conditionally dependent on each other, provided that the use of the Security Session pattern is considered between them. Conditional dependence in the graph is shown by a red edge. For the following sequence, this means that, based on conditional dependencies, the use of the sub-sequence Credential → Security Session → Check Point is expected.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Front Door
Role-Based Access Control
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

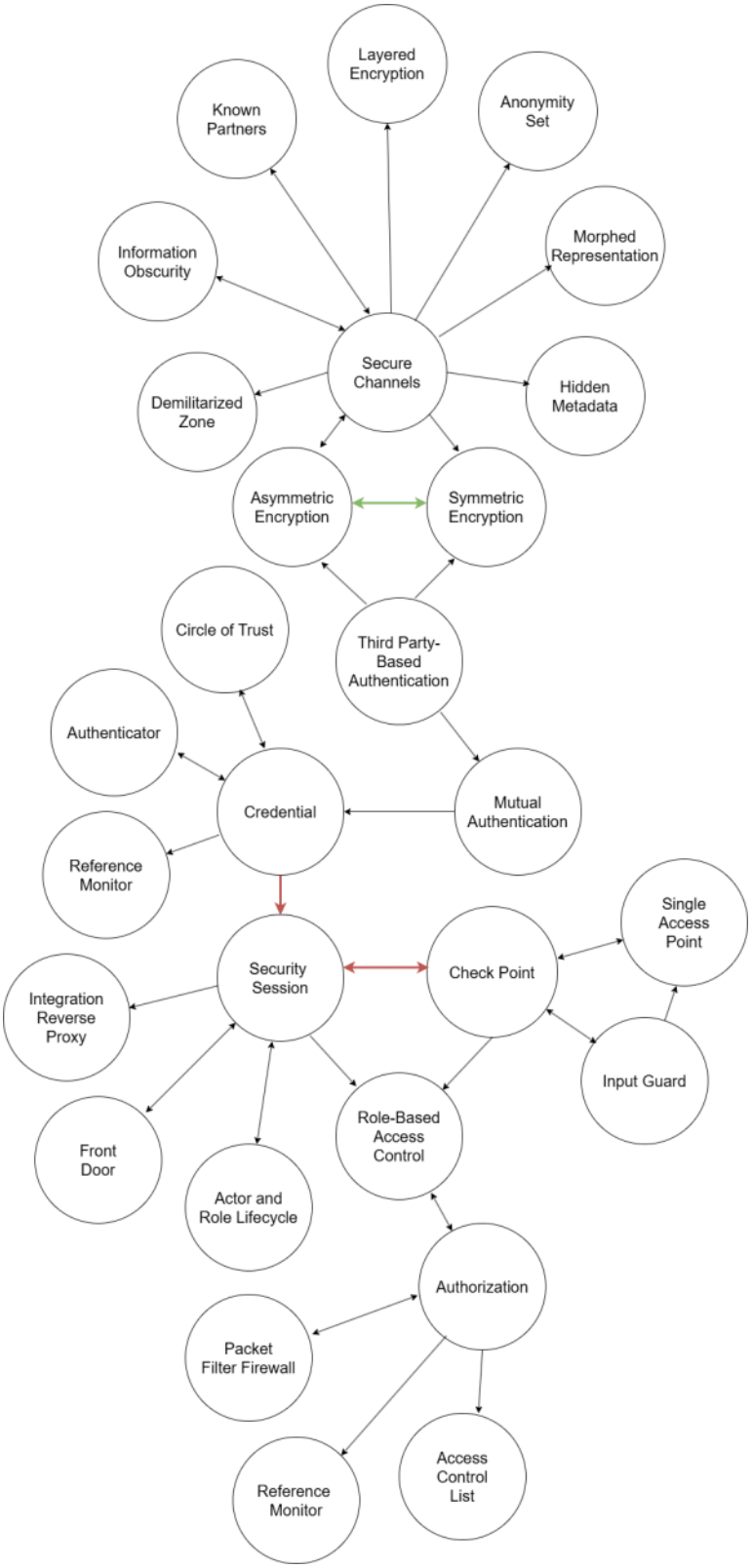
2. **Is it possible to keep the Asymmetric Encryption and Symmetric Encryption nodes connected in the network?** Answering this question requires:

   Is the Asymmetric Encryption pattern conditionally independent of the Symmetric Encryption pattern if they are to be used to implement Third Party-Based Authentication? In other words, we are asking whether the following equality p(Asymmetric Encryption, Symmetric Encryption | Third Party-Based Authentication) = p(Asymmetric Encryption | Third Party-Based Authentication)*p(Symmetric Encryption | Third Party-Based Authentication) holds. The Third Party-Based Authentication pattern is expected to be implemented through the Asymmetric Encryption or Symmetric Encryption pattern. This equality applies and the Asymmetric Encryption and Symmetric Encryption patterns are conditionally independent if their use is assumed to implement the Third Party-Based Authentication pattern.

   There is no collider on the path between Asymmetric Encryption and Symmetric Encryption nodes. The Third Party-Based Authentication node is in condition p(Asymmetric Encryption, Symmetric Encryption | Third Party-Based Authentication) and therefore the path between Asymmetric Encryption and Symmetric Encryption is blocked. The Asymmetric Encryption and Symmetric Encryption nodes are d-separated by the Third Party-Based Authentication node and therefore the Asymmetric Encryption and Symmetric Encryption patterns are conditionally independent knowing that they can be used to implement Third Party-Based Authentication.

   The arrow between the Asymmetric Encryption and Symmetric Encryption patterns is therefore highlighted in green.

   For the following sequence, this means that after using the Secure Channels pattern and before using Third Party-Based Authentication, either Asymmetric Encryption or Symmetric Encryption is used.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Front Door
Role-Based Access Control
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

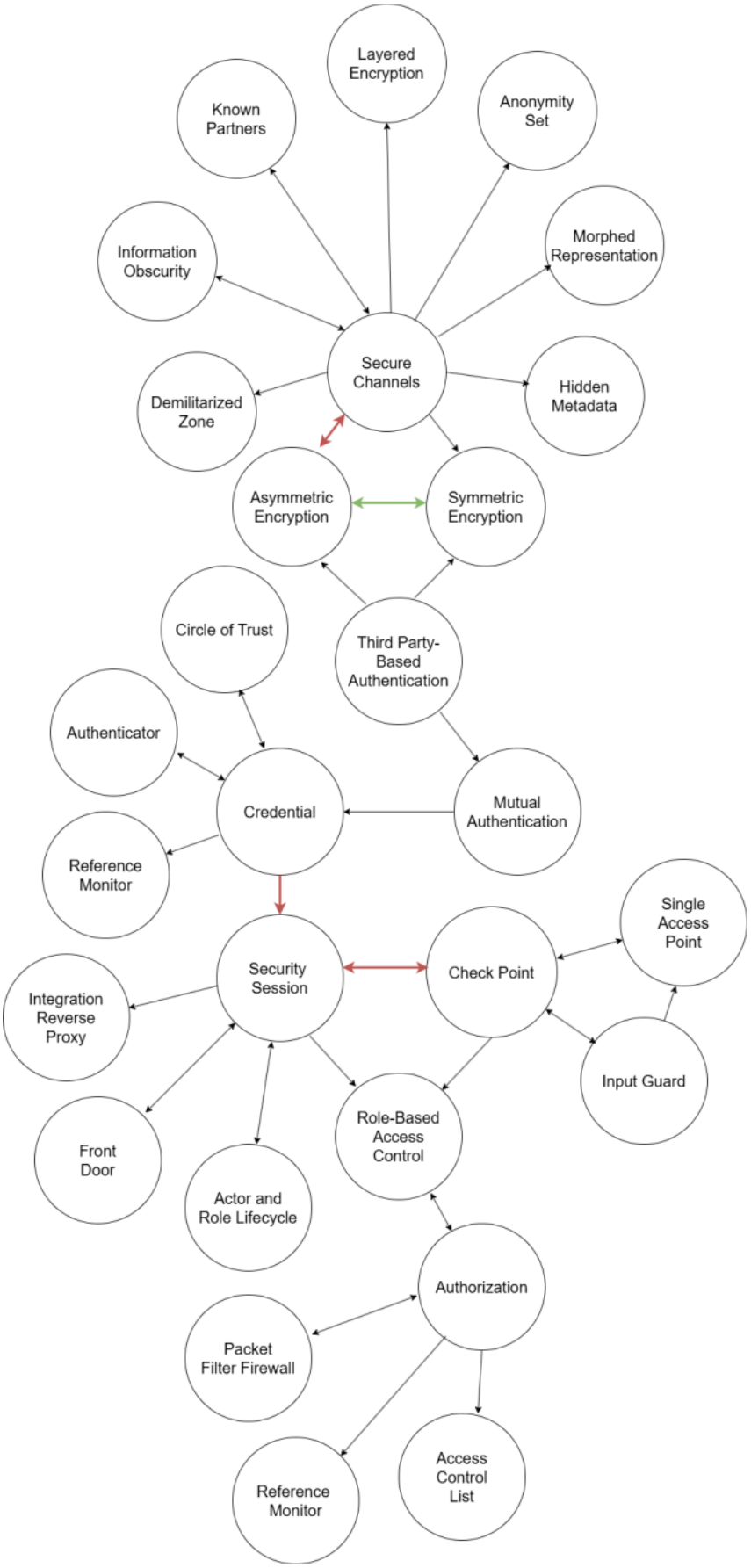
3. **Is it possible to keep the Secure Channels and Asymmetric Encryption nodes connected in the network?** Answering this question requires:

   Is the Asymmetric Encryption pattern conditionally independent of the Secure Channels pattern, if we know that after Secure Channels, the Symmetric Encryption pattern can be used instead of Asymmetric Encryption? In other words, we are asking whether the equality p(Asymmetric Encryption, Secure Channels | Symmetric Encryption) = p(Asymmetric Encryption | Symmetric Encryption)*p(Secure Channels | Symmetric Encryption) holds. This equality does not apply because the use of Asymmetric Encryption is not expected after Symmetric Encryption and also the use of Secure Channels is not expected after the use of the Symmetric Encryption pattern. The Secure Channels pattern and Asymmetric Encryption are therefore conditionally dependent.

   The conditional dependency in the graph between Secure Channels and Asymmetric Encryption is shown by a red edge.

   Yes, I can leave the Secure Channels and Asymmetric Encryption patterns connected in the graph as they are.

   For the following sequence, this means that, based on conditional dependencies, the use of the Secure Channels -> Asymmetric Encryption sub-sequence is expected.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Front Door
Role-Based Access Control
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

4. **Is it possible to keep the Secure Channels a Symmetric Encryption nodes connected in the network?**
   Answering this question requires:

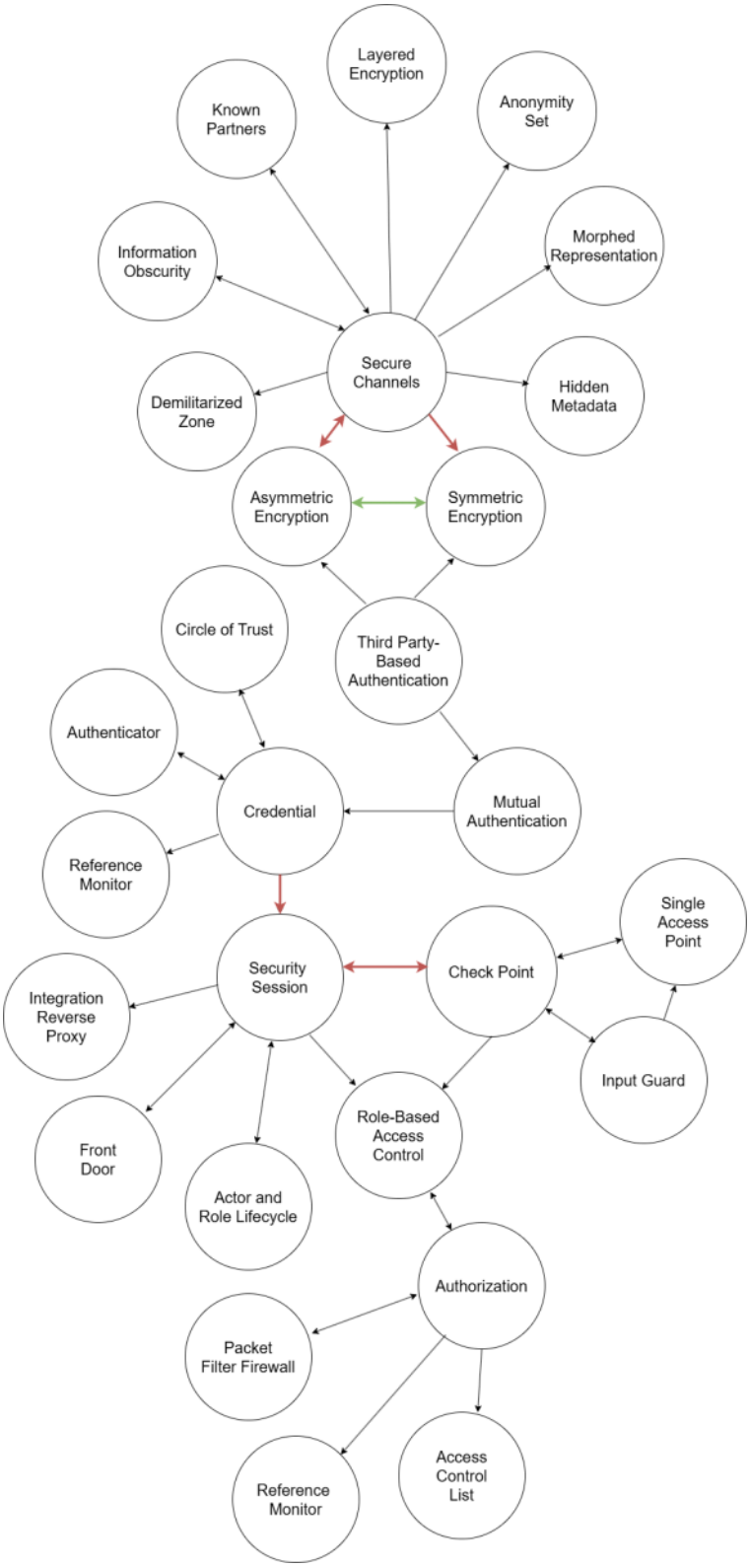
   Is the Symmetric Encryption pattern conditionally independent of the Secure Channels pattern, if we know that after Secure Channels, the Asymmetric Encryption pattern can be used instead of Symmetric Encryption? In other words, we are asking whether the equality p(Symmetric Encryption, Secure Channels | Asymmetric Encryption) = p(Symmetric Encryption | Asymmetric Encryption)*p(Secure Channels | Asymmetric Encryption) holds. This equality does not apply because the use of Symmetric Encryption is not expected after Asymmetric Encryption, even if Secure Channels can be used after Asymmetric Encryption. The Secure Channels and Symmetric Encryption patterns are therefore conditionally dependent, knowing that instead of Symmetric Encryption, Asymmetric Encryption can be used before and after Secure Channels.

   The conditional dependency in the graph between Secure Channels and Symmetric Encryption is shown by a red edge.

   Yes, I can leave the Secure Channels and Symmetric Encryption patterns connected in the graph as they are.

   For the sequence, this means that, based on conditional dependencies, the use of the Secure Channels -> Symmetric Encryption sub-sequence is expected.

   Either Asymmetric Encryption or Symmetric Encryption can be used after Secure Channels. Both options are equally expected.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Role-Based Access Control
Front Door
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

5. **Is it possible to keep the Third Party-Based Authentication, Mutual Authentication, and Credential nodes connected in the network?** Answering this question requires:

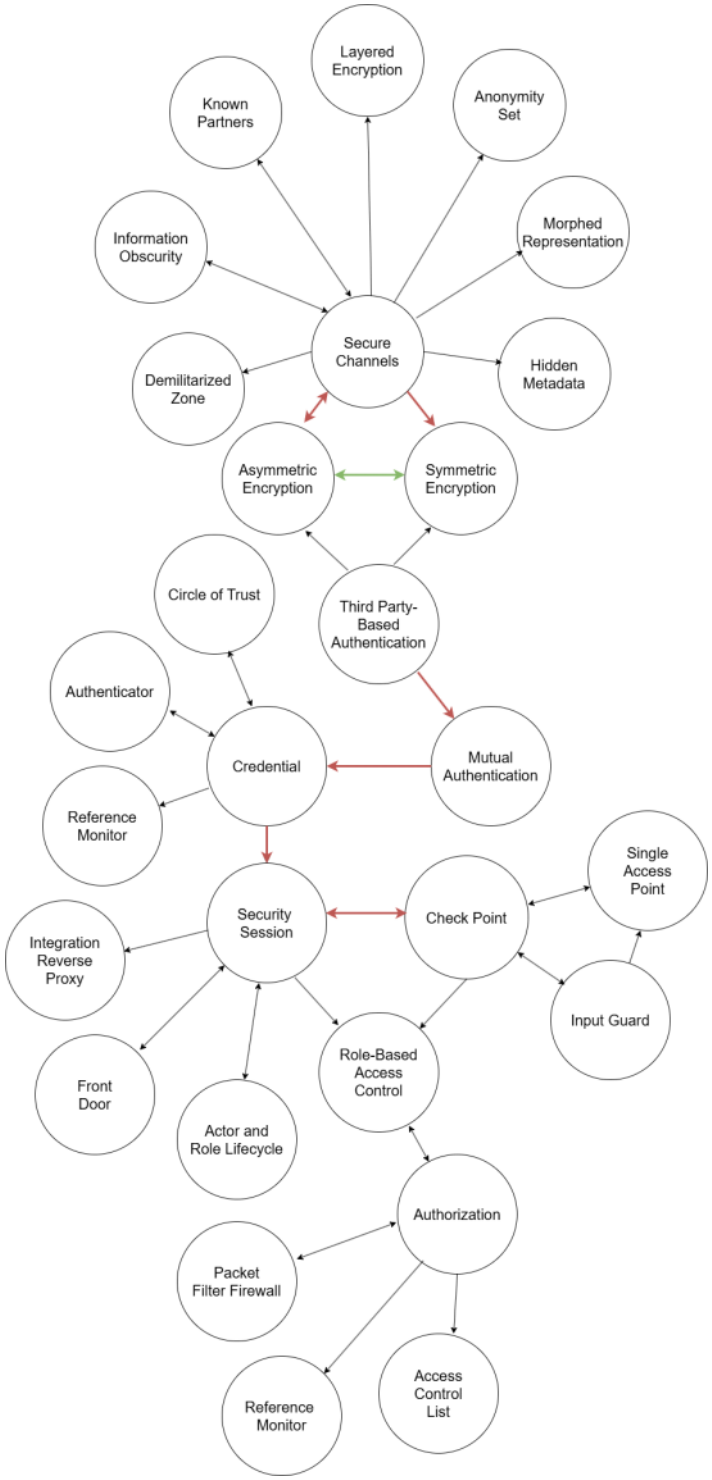
   Is the Third Party-Based Authentication pattern conditionally independent of the Credential pattern, if the use of Mutual Authentication is considered between them? The Mutual Authentication node is not a collider on the path between Third Party-Based Authentication and Credential, and the Mutual Authentication pattern is in condition of the probability p(Third Party-Based Authentication, Credential | Mutual Authentication) whose value we need to calculate. Therefore, Third Party-Based Authentication and Credential are conditionally independent, provided that Mutual Authentication is assumed to be used between them.

   On the only path between Third Party-Based Authentication and Credential nodes is a Mutual Authentication node that is not a collider and is in the condition p(Third Party-Based Authentication, Credential | Mutual Authentication). Therefore, this path is blocked. Third Party-Based Authentication and Credential nodes are d-separated and therefore the Third Party-Based Authentication and Credential patterns are conditionally independent knowing that Mutual Authentication can be used between them. Therefore, I can color the edge between the Third Party-Based Authentication, Mutual Authentication, and Credential patterns green.

   But at the same time, p(Asymmetric Encryption, Third Party-Based Authentication | Mutual Authentication) ≠ p(Asymmetric Encryption | Mutual Authentication)*p(Third Party-Based Authentication | Mutual Authentication). This means that the Asymmetric Encryption and Third Party-Based Authentication patterns are conditionally dependent knowing that they can be used before Mutual Authentication.

   It also applies that p(Credential, Mutual Authentication | Security Session) ≠ p(Credential | Security Session)*p(Mutual Authentication | Security Session) and therefore Mutual Authentication and Credential are conditionally dependent knowing that they are used to implement Secure Session.

   I can leave the Third Party-Based Authentication, Mutual Authentication, and Credential nodes connected and color their connections red.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Role-Based Access Control
Front Door
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

6. **Is it possible to keep the Circle of Trust, Authenticator, Credential, and Security Session nodes connected in the network?** Answering this question requires:

   Are the Circle Of Trust and Authenticator patterns conditionally independent if they are to be used to implement a Security Session? In other words, we ask whether the equality p(Circle of Trust, Authenticator | Security Session) = p(Circle of Trust | Security Session)*p(Authenticator | Security Session) holds

   This equality does not hold because:

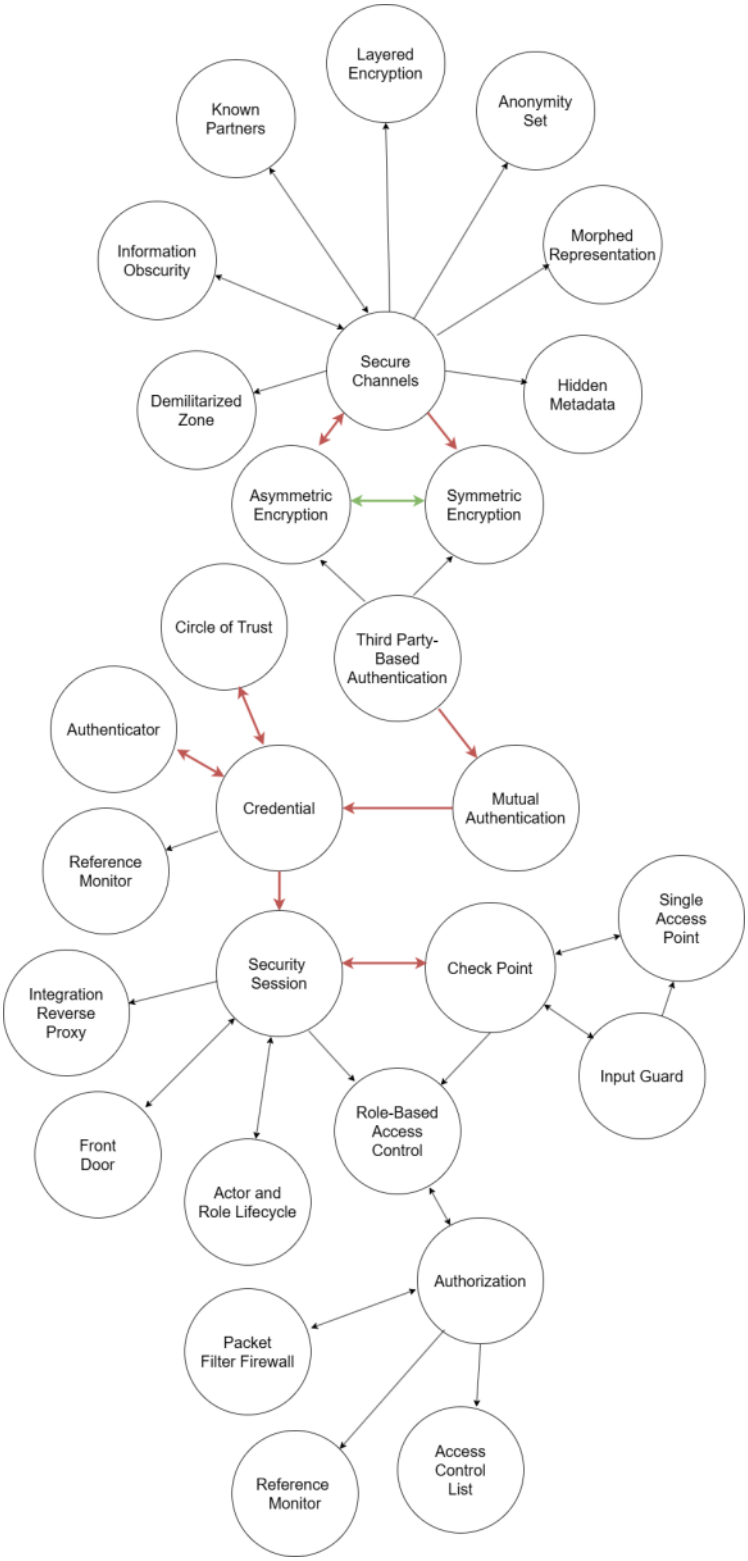
   p(Circle of Trust, Authenticator | Security Session) = p(Circle of Trust, Authenticator, Security Session) / p(Security Session) =

$$\frac{1}{p(Security\ Session)} * \sum_{Credential} \begin{matrix} p\big(Security\ Session \,\big|\, Credential\big) * p(Credential \mid Circle\ of\ Trust, Authenticator) * \\ p(Circle\ of\ Trust) \\ * p(Authenticator) \end{matrix} \neq p\big(Circle\ of\ Trust \,\big|\, Security\ Session\big) * p\big(Authenticator \,\big|\, Security\ Session\big)$$

   Therefore, the Circle of Trust and Authenticator patterns are conditionally dependent, knowing that they are used to implement the Security Session. I can leave the Circle of Trust, Authenticator, Credential, and Security Session patterns connected in the graph as they are (also through Credential).

   The conditional dependency in the graph between Circle of Trust, Credential, and Security Session is shown by a red edge.

   For the sequence, this means that, based on conditional dependencies, a combination of Circle of Trust and Authenticator is expected to implement the Security Session.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Role-Based Access Control
Front Door
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

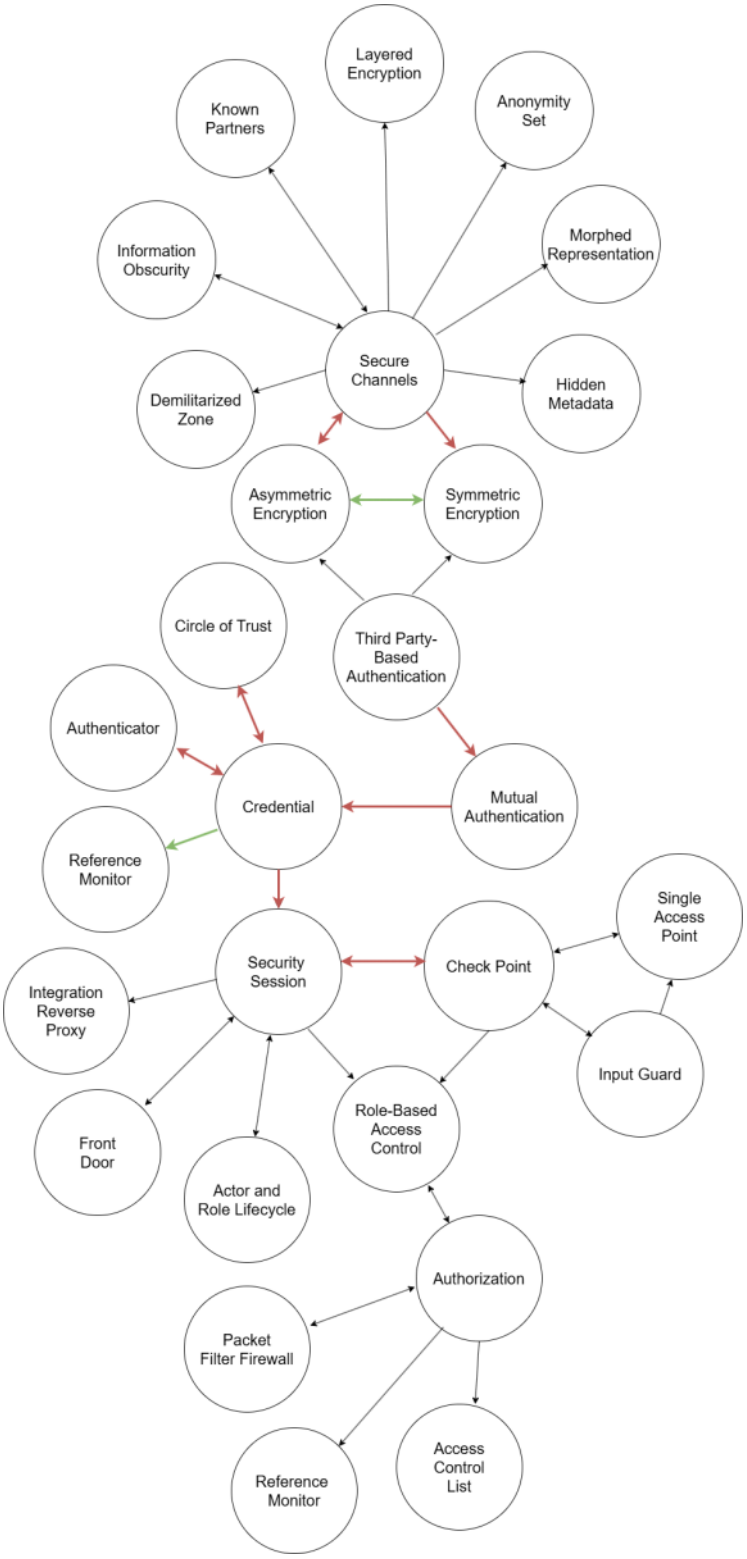
7. **Is it possible to keep the Credential, Reference Monitor, and Security Session nodes connected in the network?** Answering this question requires:

   Is the Reference Monitor pattern conditionally independent of the Security Session pattern, if the use of Credential is considered between them? In other words, we are asking whether the equality p(Reference Monitor, Security Session | Credential) = p(Reference Monitor | Credential)*p(Security Session | Credential) holds. This equality applies because after Credential it is possible to use the Reference Monitor pattern or the Security Session pattern.

   On the only path between the Reference Monitor and Security Session nodes, there is a Credential node that is not a collider and is in the condition p(Reference Monitor, Security Session | Credential). This path is blocked. Reference Monitor and Security Session nodes are d-separated and therefore the Reference Monitor and Security Session patterns are conditionally independent knowing that they can be used after the Credential pattern.

   I highlight the edge between the Reference Monitor and Credential patterns in green. However, I do not remove the edge between Credential and Security Session because here I am only testing the dependency between Reference Monitor and Security Session, but before the Security Session the use of Circle of Trust or Authenticator is still expected.

   Therefore, it cannot be identified from the Bayesian belief network that the sequence Reference Monitor -> Credential -> Security Session -> Check Point would be expected on the basis of conditional relationships. Also, the combination of the Circle of Trust, Authenticator, and Reference Monitor patterns is not expected for the Security Session implementation.


Layered Encryption
Known Partners
Anonymity Set
Information Obscurity
Morphed Representation
Secure Channels
Demilitarized Zone
Hidden Metadata
Asymmetric Encryption
Symmetric Encryption
Circle of Trust
Third Party-Based Authentication
Authenticator
Credential
Mutual Authentication
Reference Monitor
Single Access Point
Security Session
Check Point
Integration Reverse Proxy
Input Guard
Role-Based Access Control
Front Door
Actor and Role Lifecycle
Authorization
Packet Filter Firewall
Reference Monitor
Access Control List

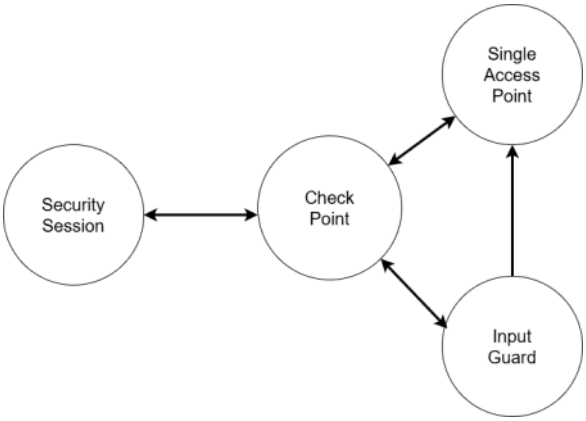
Use of the Jeffrey's Rule To Consider Uncertain Evidence and Further Simplify the Bayesian Belief Network

This section is divided into questions about the structure of the Bayesian belief network to simplify it.

Single Access Point is used after the Check Point pattern, e.g. when the implementation and configuration of the Check Point security component changes. Changes in Check Point therefore affect Single Access Point. Single Access Point can be used after Check Point to initialize the Check Point component. Input Guard is a specialization of Check Point.

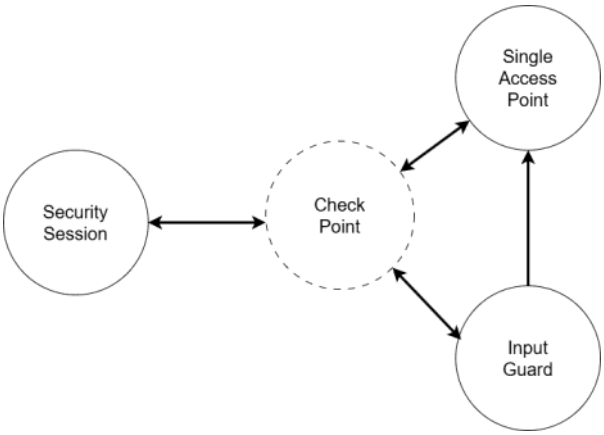
Let's have a following probability model of the Bayesian belief network:

p(Security Session, Check Point, Single Access Point, Input Guard) = p(Check Point | Security Session)*p(Security Session)*p(Input Guard | Check Point)*p(Single Access Point | Check Point)



Then we can simplify this network:

Calculating probability that Security Session would be used before Check Point

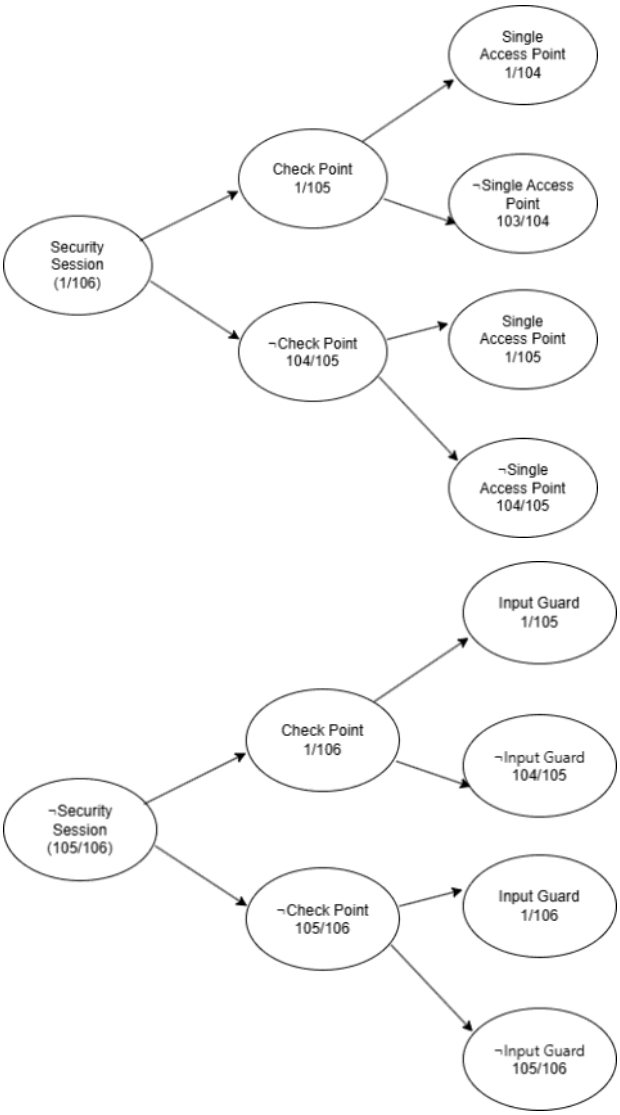


The probability that the Security Session pattern will be used before the Check Point pattern is used can be calculated using Jeffrey's rule procedure:

p(Security Session = 1 | Check Point$_{uncertain}$) = $\sum_{Check\ Point} p(Security\ Session = 1 \mid Check\ Point = 1) * (1/5) + p(Security\ Session = 1 \mid Check\ Point = 0) * (4/5)$ = ((0.00952295391)*(1/5))+((0.00943311464)*(4/5)) = 0.00945108249

When calculating according to Jeffrey's rule, I needed the probabilities p(Security Session = 1 | Check Point = 1) and p(Security Session = 1 | Check Point = 0), where second probability was calculated using the Bayes rule and both values are extracted from the stochastic tree:

p(Security Session = 1 | Check Point = 1) = (p(Check Point = 1 | Security Session = 1)*p(Security Session = 1)) / ((p(Check Point = 1 | Security Session = 1)*p(Security Session = 1))+(p(Check Point = 1 | ¬Security Session = 1)*p(¬Security Session = 1))) = ((1/105)*(1/106)) / (((1/105)*(1/106))+((1/106)*(105/106))) = 0.00952295391
p(Security Session = 1 | Check Point = 0) = (p(Check Point = 0 | Security Session = 1)*p(Security Session = 1)) / ((p(Check Point = 0 | Security Session = 1)*p(Security Session = 1))+(p(Check Point = 0 | ¬Security Session = 1)*p(¬Security Session = 1))) = ((104/105)*(1/106)) / (((104/105)*(1/106))+((105/106)*(105/106))) = 0.00943311464



I calculated the probability p(Check Point | Check Point$_{uncertain}$) = 1/5 that the Check Point will be used after the Security Session as 1/N, where N is the number of patterns that are listed in the text description of the Security Session pattern as those applicable further on. Following the Security Session pattern, the following patterns are considered (I consider only those for which there is a description in the same pattern catalog):

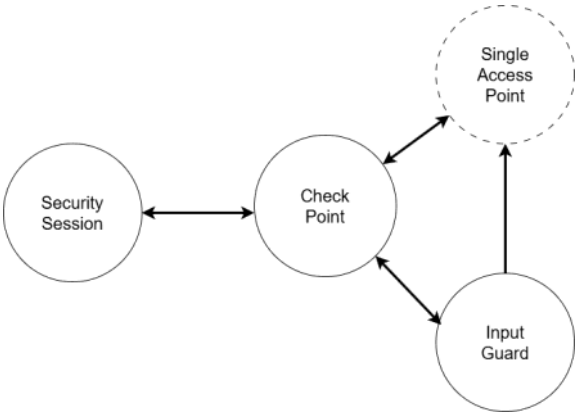
- Check Point
- Role-Based Access Control
- Integration Reverse Proxy
- Front Door
- Actor and Role Lifecycle

There are 5 of these patterns, so if the probability of using each pattern is the same, then the probability of using Check Point after the Security Session pattern is 1/5. Opposite probability p(Check Point | ¬Check

Point$_{uncertain}$) that the Check Point would not be used after Security Session is 4/5.

If we are not sure whether the Check Point pattern will be used after the Security Session (and not the others referred to by the Security Session), then the probability p(Security Session = 1 | Check Point = 1) = 1/105 = 0.0095 drops to p(Security Session = 1 | Check Point$_{uncertain}$) = 0.00945108249.

Calculating probability that the Security Session would be used before Input Guard

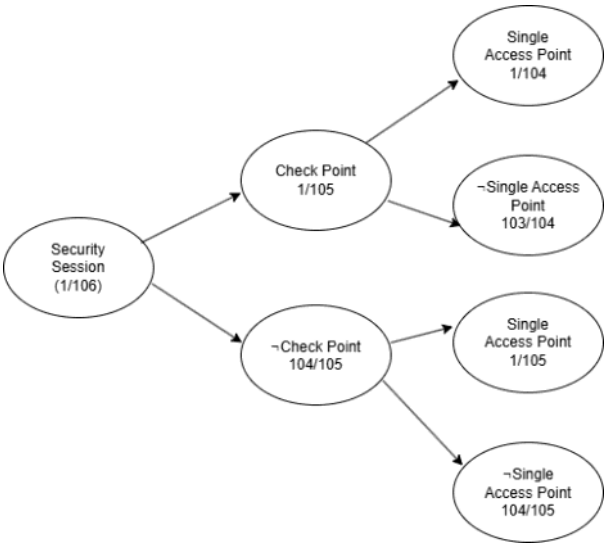


The probability that the Security Session will be used before the Input Guard, regardless of whether or not a Single Access Point$_{uncertain}$ will be used after the Check Point, can be calculated as:

p(Security Session = 1 | Input Guard = 1, Single Access Point$_{uncertain}$) = p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) *p(Single Access Point = 1 | Single Access Point$_{uncertain}$) + p(Security Session = 1 | Input Guard = 1, Single Access Point = 0)*p(Single Access Point = 0 | Single Access Point$_{uncertain}$) = p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) *(1/104)+ p(Security Session = 1 | Input Guard = 1, Single Access Point = 0)*(103/104) =

The probability that the Single Access Point will or will not be used after the Check Point is extracted from the stochastic tree (see below):

p(Single Access Point = 1 | Single Access Point$_{uncertain}$) = 1/104
p(Single Access Point = 0 | Single Access Point$_{uncertain}$) = 103/104



To calculate p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) I need to use the Bayes rule:

p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) =

$$\frac{p(Security\ Session = 1, Input\ Guard = 1, Single\ Access\ Point = 1)}{p(Input\ Guard = 1, Single\ Access\ Point = 1)}$$

$$= \frac{\sum_{Check\ Point} p(Single\ Access\ Point = 1 \mid Check\ Point) * p(Input\ Guard = 1 \mid Check\ Point) * p(Check\ Point \mid Security\ Session = 1) * p(Security\ Session = 1)}{\sum_{Security\ Session, Check\ Point} p(Single\ Access\ Point = 1 \mid Check\ Point) * p(Input\ Guard = 1 \mid Check\ Po * p(Check\ Point \mid Security\ Session) * p(Security\ Session)}$$

=

= where the values for calculating the numerator and denominator can be taken directly from the stochastic trees (see below)

numerator is:

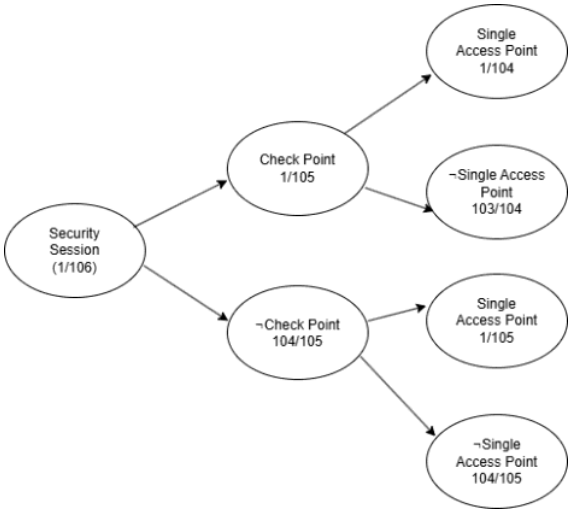
p(Single Access Point = 1 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)*
p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) + p(Single Access Point = 1 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) = (1/104)*(1/104)*(1/105)*(1/106) + (1/105)*(1/105)*(104/105)*(1/106) = 0.00000085584566

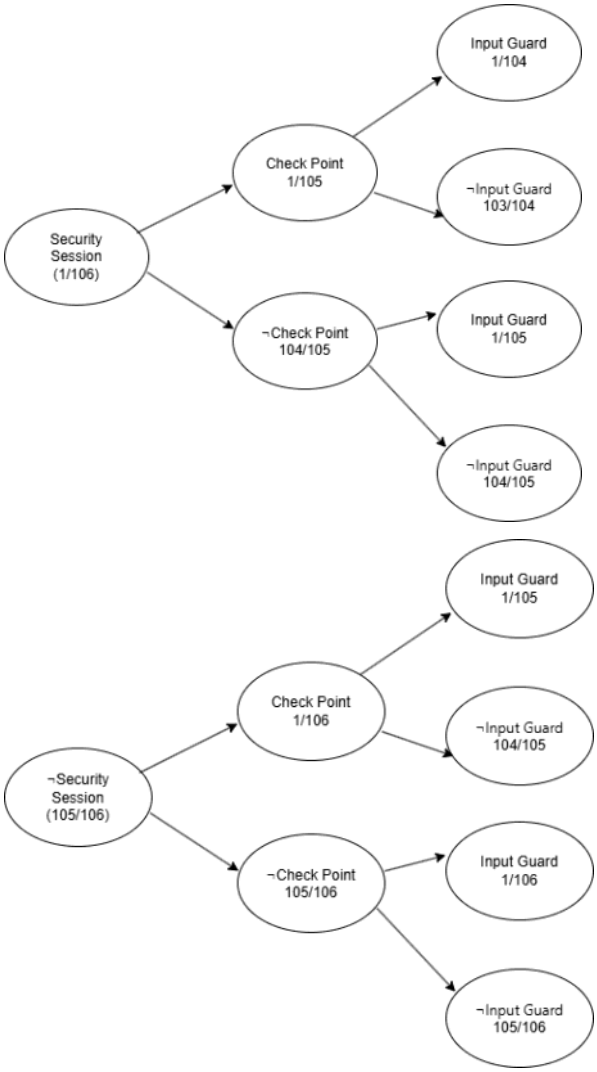
denominator needs to take into account these cases:

- Check Point = 0, Security Session = 0
- Check Point = 1, Security Session = 1
- Check Point = 1, Security Session = 0
- Check Point = 0, Security Session = 1

denominator is:
p(Single Access Point = 1 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 0)*p(Security Session = 0) +
p(Single Access Point = 1 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) +
p(Single Access Point = 1 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 0)*p(Security Session = 0) +
p(Single Access Point = 1 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(1/105)*(1/105)*(105/106)*(105/106)+(1/104)*(1/104)*(1/105)*(1/106)
+(1/104)*(1/104)*(1/106)*(105/106)+(1/105)*(1/105)*(104/105)*(1/106) = 0.00009071948

Probability p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889847





To calculate p(Security Session = 1 | Input Guard = 1, Single Access Point = 0) I need to use the Bayes rule:

p(Security Session = 1 | Input Guard = 1, Single Access Point = 0) =

$$\frac{p(Security\ Session = 1, Input\ Guard = 1, Single\ Access\ Point = 0)}{p(Input\ Guard = 1, Single\ Access\ Point = 0)}$$

$$= \frac{\sum_{Check\ Point} p\left(Single\ Access\ Point = 0 \mid Check\ Point\right) * p\left(Input\ Guard = 1 \mid Check\right.}{\sum_{Security\ Session, Check\ Point} p\left(Single\ Access\ Point = 0 \mid Check\ Point\right) * p\left(Input\ Guard = 1\right.}$$

$$= \frac{p(Check\ Point \mid Security\ Session = 1) * p(Security\ Session =}{* p(Check\ Point \mid Security\ Session) * p(Security\ Ses}$$

where the values for calculating the numerator and denominator can be taken directly from the stochastic trees (see above)

numerator is:
p(Single Access Point = 0 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)* p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) + p(Single Access Point = 0 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) = (103/104)*(1/105)*(1/105)*(1/106) + (104/105)*(105/106)*(104/105)*(1/106) = 0.0091686584

denominator needs to take into account these cases:

- Check Point = 0, Security Session = 0
- Check Point = 1, Security Session = 1
- Check Point = 1, Security Session = 0
- Check Point = 0, Security Session = 1

denominator is:

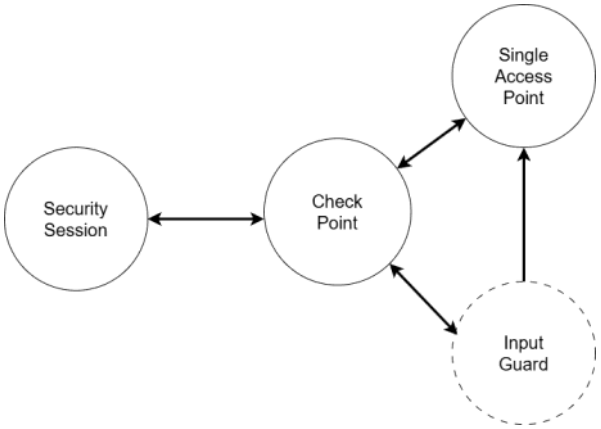
p(Single Access Point = 0 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 0)*p(Security Session = 0) +
p(Single Access Point = 0 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) +
p(Single Access Point = 0 | Check Point = 1)*p(Input Guard = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 0)*p(Security Session = 0) +
p(Single Access Point = 0 | Check Point = 0)*p(Input Guard = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(104/105)*(1/106)*(105/106)*(105/106)+(103/104)*(1/105)*(1/105)*(1/106)+(103/104)*(1/105)*(1/106)*(105/106)+(105/106)*(1/106)*(104/105)*(1/106) =
0.00934495431

Probability p(Security Session = 1 | Input Guard = 1, Single Access Point = 0) value is 0.0091686584 / 0.00934495431 = 0.98113464185

The probability that the Security Session will be used before the Input Guard, regardless of whether or not a Single Access Point will be used after the Check Point, can be calculated as:

p(Security Session = 1 | Input Guard = 1, Single Access $Point_{uncertain}$) = (0.00943397889847*(1/104))+ (0.98113464185*(103/104)) = 0.9717913662447 and it's a high probability.

Calculating probability that the Security Session would be used before the Single Access Point



In the previous calculation, I was able to calculate the probability that the Security Session will be used before the Input Guard pattern, regardless of the use of Single Access Point after the Check Point pattern. This probability was:

p(Security Session = 1 | Input Guard = 1, Single Access $Point_{uncertain}$) = 0.00943397889847*(1/104)+ 0.98113464185*(103/104) = 0.9717913662447

However, it is questionable whether this probability is higher, lower, or the same as the probability that the Security Session will be used before the Single Access Point pattern, regardless of the use of Input Guard after the Check Point pattern. In case:

- that the latter probability is lower than the probability of using the Input Guard pattern after the Check Point pattern (and also the Security Session), then the use of the sequence Security Session -> Check Point -> Input Guard will be more likely than the sequence Security Session -> Check Point -> Single Access Point. In this case, the relationship between Check Point and Single Access Point will be deleted.

- that the latter probability is higher than the probability of using Input Guard after Check Point (and also Security Session), then the sequence Security Session -> Check Point -> Single Access Point will be more likely to be used than the sequence Security Session -> Check Point -> Input Guard . In this case, the relationship between Check Point and Input Guard will be removed.

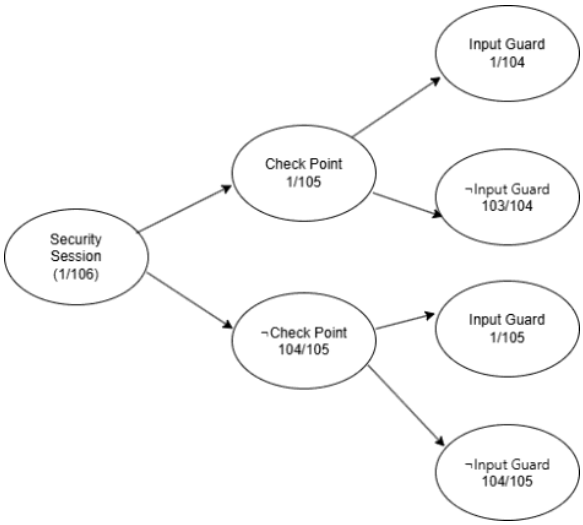
- that this second probability is the same as the probability of using Input Guard after Check Point (and also Security Session), the relations between Security Session, Check Point, Input Guard, and Single Access Point should be left. Such a situation will mean that, after the Check Point pattern, a combination of the Input Guard and Single Access Point patterns is expected to be used.

The probability that a Security Session will be used before a Single Access Point, regardless of whether or not Input Guard will be used after the Check Point pattern, can be calculated as:

$p(\text{Security Session} = 1 \mid \text{Input Guard}_{uncertain}, \text{Single Access Point} = 1) = p(\text{Security Session} = 1 \mid \text{Single Access Point} = 1, \text{Input Guard} = 1) * p(\text{Input Guard} = 1 \mid \text{Input Guard}_{uncertain}) + p(\text{Security Session} = 1 \mid \text{Single Access Point} = 1, \text{Input Guard} = 0) * p(\text{Input Guard} = 0 \mid \text{Input Guard}_{uncertain}) = p(\text{Security Session} = 1 \mid \text{Single Access Point} = 1, \text{Input Guard} = 1) * (1/104) + p(\text{Security Session} = 1 \mid \text{Single Access Point} = 1, \text{Input Guard} = 0) * (103/104) =$

The probability that Input Guard will be used or not after Check Point is extracted from the stochastic tree (see below):

$p(\text{Input Guard} = 1 \mid \text{Input Guard}_{uncertain}) = 1/104$
$p(\text{Input Guard} = 0 \mid \text{Input Guard}_{uncertain}) = 103/104$



To calculate p(Security Session = 1 | Single Access Point = 1, Input Guard = 1) I need to use the Bayes rule:

p(Security Session = 1 | Single Access Point = 1, Input Guard = 1) =

$$\frac{p(Security\ Session = 1,\ Single\ Access\ Point = 1,\ Input\ Guard = 1)}{p(Single\ Access\ Point = 1,\ Input\ Guard = 1)} =$$

$$\frac{\sum_{Check\ Point} \begin{matrix} p(Input\ Guard\ = 1 \mid Check\ Point) * \\ p(Single\ Access\ Point = 1 \mid Check\ Point) * \\ p(Check\ Point \mid Security\ Session = 1) * \\ p(Security\ Session = 1) \end{matrix}}{\sum_{Security\ Session, Check\ Point} \begin{matrix} p(Input\ Guard = 1 \mid Check\ Point) * \\ p(Single\ Access\ Point = 1 \mid Check\ Point) * \\ p(Check\ Point \mid Security\ Session) * \\ p(Security\ Session) \end{matrix}} =$$

= where the values for calculating the numerator and denominator can be taken directly from the stochastic trees (see below)

numerator is:
p(Inpunt Guard = 1 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)* p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) + p(Input Guard = 1 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(1/104)*(1/104)*(1/105)*(1/106)+(1/105)*(1/105)*(104/105)*(1/106) = 0.00000085584566

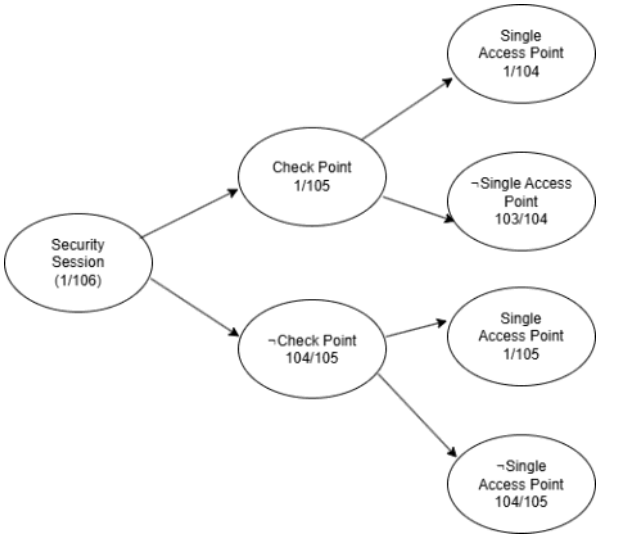
denominator needs to take into account these cases:

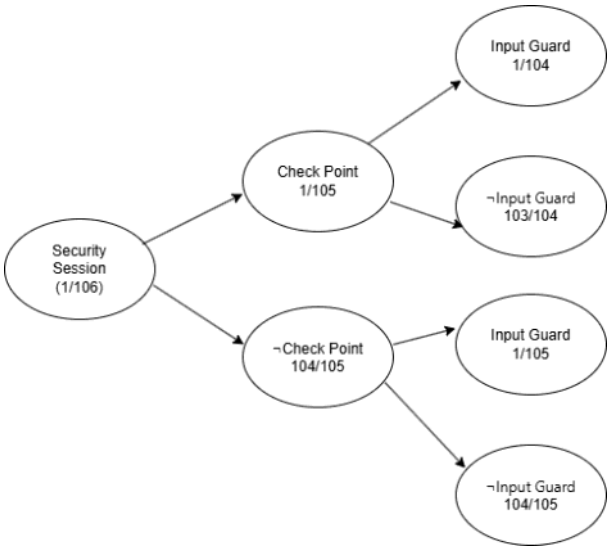
- Check Point = 0, Security Session = 0
- Check Point = 1, Security Session = 1
- Check Point = 1, Security Session = 0
- Check Point = 0, Security Session = 1

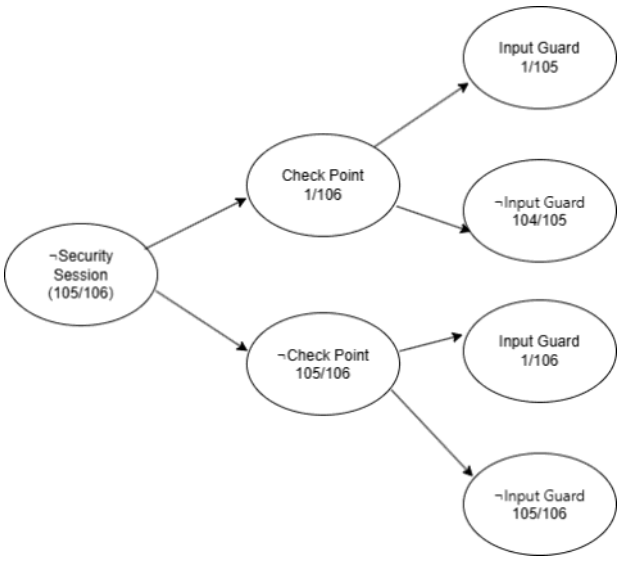
denominator is:

p(Input Guard = 1 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 0)*p(Security Session = 0) +
p(Input Guard = 1 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) +
p(Input Guard = 1 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 0)*p(Security Session = 0) +
p(Input Guard = 1 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(1/105)*(1/105)*(105/106)*(105/106)+(1/104)*(1/104)*(1/105)*(1/106)+(1/104)*(1/104)*(1/106)*(105/106)+(1/105)*(1/105)*(104/105)*(1/106)= 0.00009071948

Probability p(Security Session = 1 | Input Guard = 1, Single Access Point = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889


Security Session (1/106)
Check Point 1/105
¬Check Point 104/105
Single Access Point 1/104
¬Single Access Point 103/104
Single Access Point 1/105
¬Single Access Point 104/105


Security Session (1/106)
Check Point 1/105
¬Check Point 104/105
Input Guard 1/104
¬Input Guard 103/104
Input Guard 1/105
¬Input Guard 104/105


¬Security Session (105/106)
Check Point 1/106
¬Check Point 105/106
Input Guard 1/105
¬Input Guard 104/105
Input Guard 1/106
¬Input Guard 105/106

And again, to calculate p(Security Session = 1 | Single Access Point = 1, Input Guard = 0) I need to use the Bayes rule:

p(Security Session = 1 | Single Access Point = 1, Input Guard = 0) =

$$\frac{p(Security\ Session = 1, Single\ Access\ Point = 1,\ Input\ Guard = 0)}{p(Single\ Access\ Point = 1,\ Input\ Guard = 0)}$$

$$= \frac{\sum_{Check\ Point} \begin{matrix} p(Input\ Guard\ = 0 \mid Check\ Point) * \\ p(Single\ Access\ Point = 1 \mid Check\ Point) * \\ p(Check\ Point \mid Security\ Session = 1) * \\ p(Security\ Session = 1) \end{matrix}}{\sum_{Security\ Session, Check\ Point} \begin{matrix} p(Input\ Guard = 0 \mid Check\ Point) * \\ p(Single\ Access\ Point = 1 \mid Check\ Point) \\ * p(Check\ Point \mid Security\ Session) * \\ p(Security\ Session) \end{matrix}}$$

= where the values for calculating the numerator and denominator can be taken directly from the stochastic trees (see above)

numerator is:
p(Input Guard = 0 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)*
p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) + p(Input Guard = 0 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(104/105)*(1/104)*(1/105)*(1/106)+(105/106)*(1/105)*(104/105)*(1/106)=0.00008900771

denominator needs to take into account these cases:

- Check Point = 0, Security Session = 0
- Check Point = 1, Security Session = 1
- Check Point = 1, Security Session = 0
- Check Point = 0, Security Session = 1

denominator is:

p(Input Guard = 0 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 0)*p(Security Session = 0) +
p(Input Guard = 0 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 1)*p(Security Session = 1) +
p(Input Guard = 0 | Check Point = 1)*p(Single Access Point = 1 | Check Point = 1)*p(Check Point = 1 | Security Session = 0)*p(Security Session = 0) +
p(Input Guard = 0 | Check Point = 0)*p(Single Access Point = 1 | Check Point = 0)*p(Check Point = 0 | Security Session = 1)*p(Security Session = 1) =
(105/106)*(1/105)*(105/106)*(105/106)+(104/105)*(1/104)*(1/105)*(1/106)+(103/104)*(1/104)*(1/106)*(105/106)+(105/106)*(1/105)*(104/105)*(1/106) = 0.00943480172

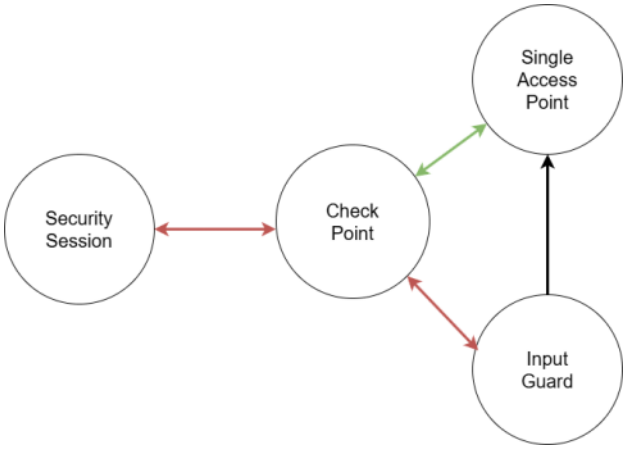
Probability p(Security Session = 1 | Single Access Point = 1, Input Guard = 0) value is 0.00008900771 / 0.00943480172 =
0.0094339778

The probability that Security Session will be used before Single Access Point regardless of whether or not Input Guard will be used after Check Point can therefore be calculated as:

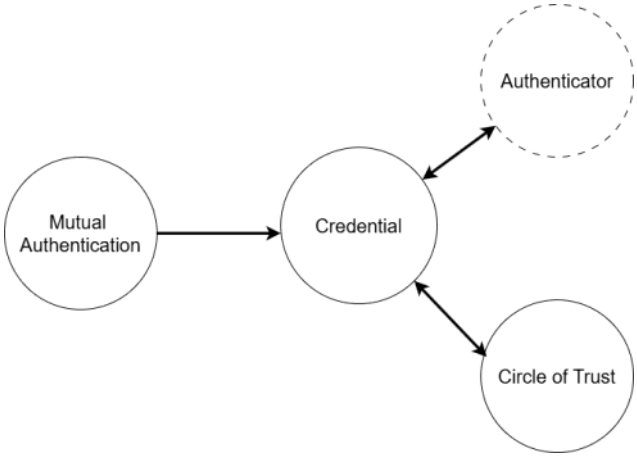
p(Security Session = 1 | Single Access Point = 1, Input $Guard_{uncertain}$) = (0.00943397889)*(1/104)+ (0.0094339778)*(103/104) =0.00943397781 and this probability is lower than the probability p(Security Session = 1

| Input Guard = 1, Single Access Point$_{uncertain}$) = 0.9717913662447 of the event that the Check Point would be used before the Input Guard.

It is therefore more likely that the sequence Security Session -> Check Point -> Input Guard is used than the sequence Security Session -> Check Point -> Single Access Point. The relationship between Check Point and Single Access Point can be removed.



Calculating probability that the Mutual Authentication would be used before the Circle of Trust

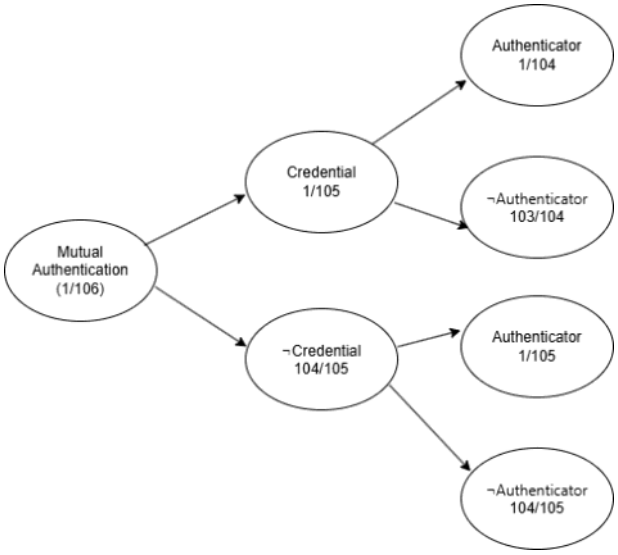


The probability that Mutual Authentication will be used before Circle of Trust regardless of whether or not Authenticator$_{uncertain}$ will be used after Credential can be calculated as:

p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator$_{uncertain}$) = p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) *p(Authenticator = 1 | Authenticator$_{uncertain}$)+ p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 0)*p(Authenticator = 0 | Authenticator$_{uncertain}$) = p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) *(1/104)+ p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 0)*(103/104) =

The probability that Credential is used or not before Authenticator is extracted from the stochastic tree (see below):

p(Authenticator = 1 | Authenticator$_{uncertain}$) = 1/104
p(Authenticator = 0 | Authenticator$_{uncertain}$) = 103/104



To calculate p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) I need to use the Bayes rule:

p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) =

$$\frac{p(Mutual\ Authentication = 1,\ Circle\ of\ Trust = 1,\ Authenticator = 1)}{p(Circle\ of\ Trust = 1,\ Authenticator = 1)} =$$

$$= \frac{\sum_{Credential} p(Authenticator\ = 1 \mid Credential) * p\big(Circle\ of\ Trust = 1 \mid Credential\big) * p(Credential \mid Mutual\ Authentication = 1) * p(Mutual\ Authentication = 1)}{\sum_{Mutual\ Authentication, Credential} p(Authenticator = 1 \mid Credential) * p\big(Circle\ of\ Trust = 1 \mid Credential\big) * p(Credential \mid Mutual\ Authentication) * p(Mutual\ Authentication)} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

numerator is:
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*
p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) = (1/104)*(1/104)*(1/105)*(1/106)+(1/105)*(1/105)*(104/105)*(1/106) = 0.00000085584566

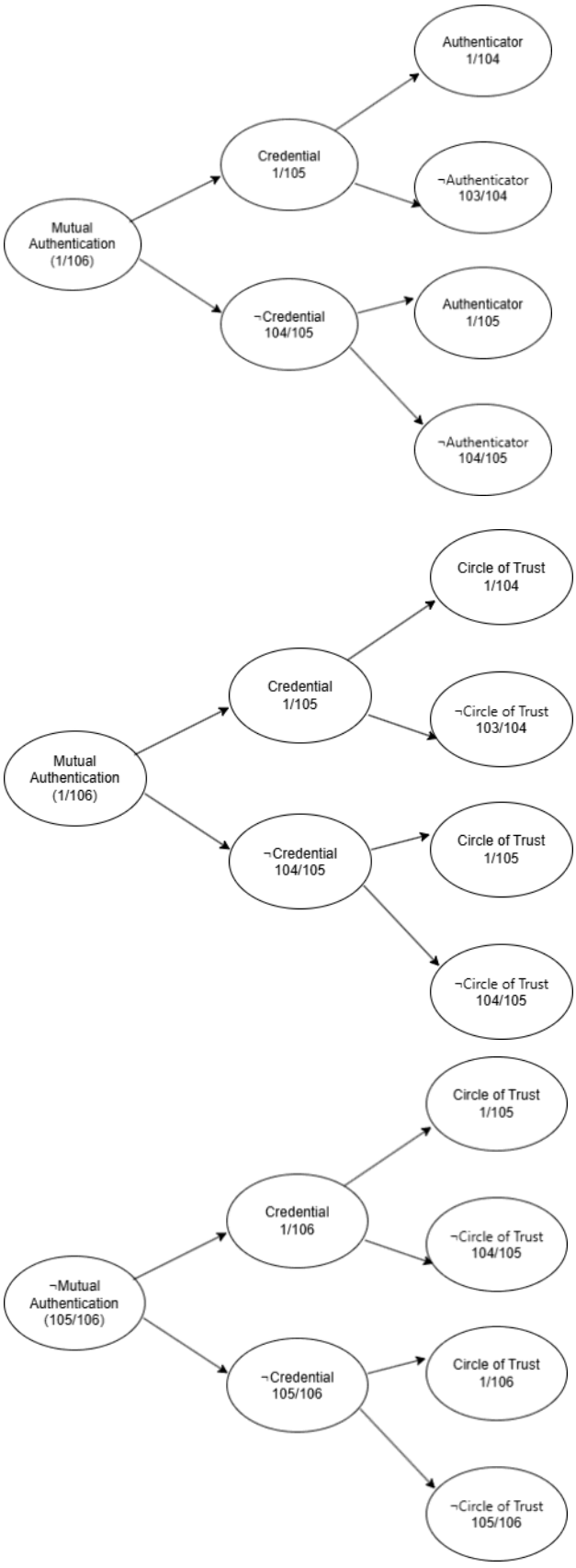
denominator needs to take into account these cases:

- Credential = 0, Mutual Authentication = 0
- Credential = 1, Mutual Authentication = 1
- Credential = 1, Mutual Authentication = 0
- Credential = 0, Mutual Authentication = 1

denominator is:

p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) =
(1/105)*(1/105)*(105/106)*(105/106)+(1/104)*(1/104)*(1/105)*(1/106)+(1/104)*(1/104)*(1/106)*(105/106)+(1/105)*(1/105)*(104/105)*(1/106)=

Probability p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889



To calculate p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 0) I need to use the Bayes rule:

p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 0) =

$$\frac{p(Mutual\ Authentication = 1,\ Circle\ of\ Trust = 1,\ Authenticator = 0)}{p(Circle\ of\ Trust = 1,\ Authenticator = 0)} =$$

$$= \frac{\sum_{Credential} p(Authenticator = 0 \mid Credential) * p\big(Circle\ of\ Trust = 1 \,\big|\, Credential\big) * p(Credential \mid Mutual\ Authentication = 1) * p(Mutual\ Authentication = 1)}{\sum_{Mutual\ Authentication, Credential} p(Authenticator = 0 \mid Credential) * p\big(Circle\ of\ Trust = 1 \,\big|\, Credential\big) * p(Credential \mid Mutual\ Authentication) * p(Mutual\ Authentication)} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see above)

numerator is:
p(Authenticator = 0 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*
p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) + p(Authenticator = 0 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) = (103/104)*(1/104)*(1/105)*(1/106)+(104/105)*(1/106)*(104/105)*(1/106) = 0.00008816809

denominator needs to take into account these cases:

- Credential = 0, Mutual Authentication = 0
- Credential = 1, Mutual Authentication = 1
- Credential = 1, Mutual Authentication = 0
- Credential = 0, Mutual Authentication = 1

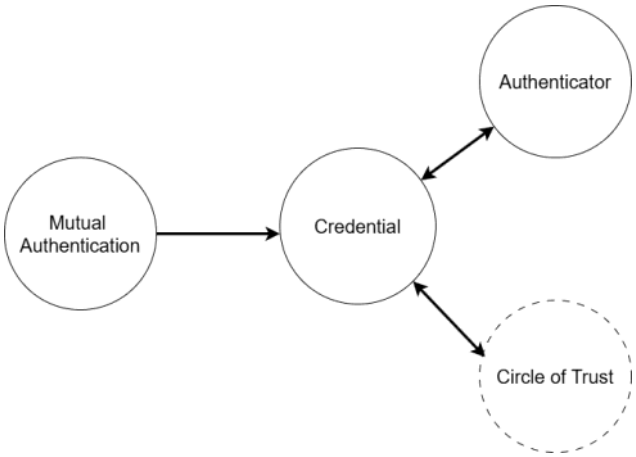
denominator is:
p(Authenticator = 0 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 0 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Authenticator = 0 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 0 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) =
(104/105)*(1/106)*(105/106)*(105/106)+(103/104)*(1/104)*(1/105)*(1/106) +
(103/104)*(1/104)*(1/106)*(105/106)+(104/105)*(1/106)*(104/105)*(1/106)=0.00934580208

Probability p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 0) value is 0.00008816809 / 0.00934580208 = 0.00943397786

The probability that Mutual Authentication will be used before Circle of Trust regardless of whether or not Authenticator will be used after Credential can therefore be calculated as:

p(Mutual Authentication = 1 | Circle of Trust = 1, $Authenticator_{uncertain}$) = (0.00943397889*(1/104))+
(0.00943397786*(103/104)) =
0.00943397786 and this is a low probability.

Calculating probability that the Mutual Authentication would be used before Authenticator



In the previous calculation, I was able to calculate the probability that the Mutual Authentication will be used before the Circle of Trust pattern, regardless of the use of Authenticator after the Credential pattern. This probability was:

p(Mutual Authentication = 1 | Circle of Trust = 1, $\text{Authenticator}_{\text{uncertain}}$) = (0.00943397889*(1/104))+ (0.00943397786*(103/104)) = 0.00943397786

However, it is questionable whether this probability is higher, lower, or the same as the probability that the Mutual Authentication will be used before the Authenticator pattern, regardless of the use of Circle of Trust after the Credential pattern. In case:

- that the latter probability is lower than the probability of using Circle of Trust after Credential (and also Mutual Authentication), the sequence Mutual Authentication -> Credential -> Circle of Trust will be more likely to be used than the sequence Mutual Authentication -> Credential -> Authenticator. In this case, the relationship between Credential and Authenticator will be removed.

- that the latter probability is higher than the probability of using Circle of Trust after Credential (and also Mutual Authentication), then the use of the sequence Mutual Authentication -> Credential -> Authenticator will be more likely than the sequence Mutual Authentication -> Credential -> Circle of Trust. In this case, the relationship between Credential and Circle of Trust will be removed.

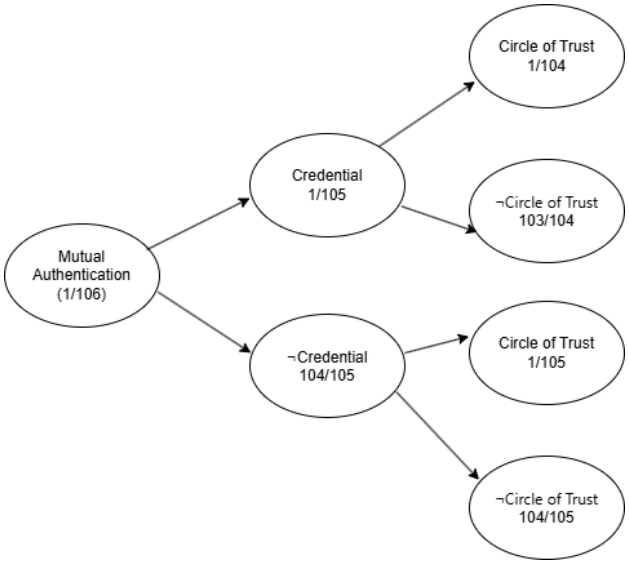
- that the second probability is the same as the probability of using Circle of Trust after Credential (and also Mutual Authentication), then the relations between Security Session, Credential, Circle of Trust, and Authenticator should be left. Such a situation will mean that a combination of the Circle of Trust and Authenticator patterns is expected to be used after the Credential pattern.

The probability that Mutual Authentication will be used before Authenticator regardless of whether or not Circle of Trust will be used after Credential can be calculated as:

p(Mutual Authentication = 1 | Circle of $\text{Trust}_{\text{uncertain}}$, Authenticator = 1) = p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 1)*p(Circle of Trust = 1 | Circle of $\text{Trust}_{\text{uncertain}}$) + p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 0)*p(Circle of Trust = 0 | Circle of $\text{Trust}_{\text{uncertain}}$) = p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 1) *(1/104)+ p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 0)*(103/104) =

The probability that the Credential will or will not be used before the Circle of Trust is extracted from the stochastic tree (see below):

p(Circle of Trust = 1 | Circle of $\text{Trust}_{\text{uncertain}}$) = 1/104
p(Circle of Trust = 0 | Circle of $\text{Trust}_{\text{uncertain}}$) = 103/104



To calculate p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) I need to use the Bayes rule:

p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) =

$$\frac{p(Mutual\ Authentication = 1,\ Authenticator = 1,\ Circle\ of\ Trust = 1)}{p(Authenticator = 1,\ Circle\ of\ Trust = 1)}$$

$$= \frac{\sum_{Credential} p(Cirlce\ of\ Trust\ = 1 \mid Credential) * p(Authenticator = 1 \mid Credential) * p(Credential \mid Mutual\ Authentication = 1) * p(Mutual\ Authentication = 1)}{\sum_{Mutual\ Authentication, Credential} p(Circle\ of\ Trust = 1 \mid Credential) * p(Authenticator = 1 \mid Credential) * p(Credential \mid Mutual\ Authentication) * p(Mutual\ Authentication)} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

Numerator is:
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*
p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) = (1/104)*(1/104)*(1/105)*(1/106)+(1/105)*(1/105)*(104/105)*(1/106) = 0.00000085584566

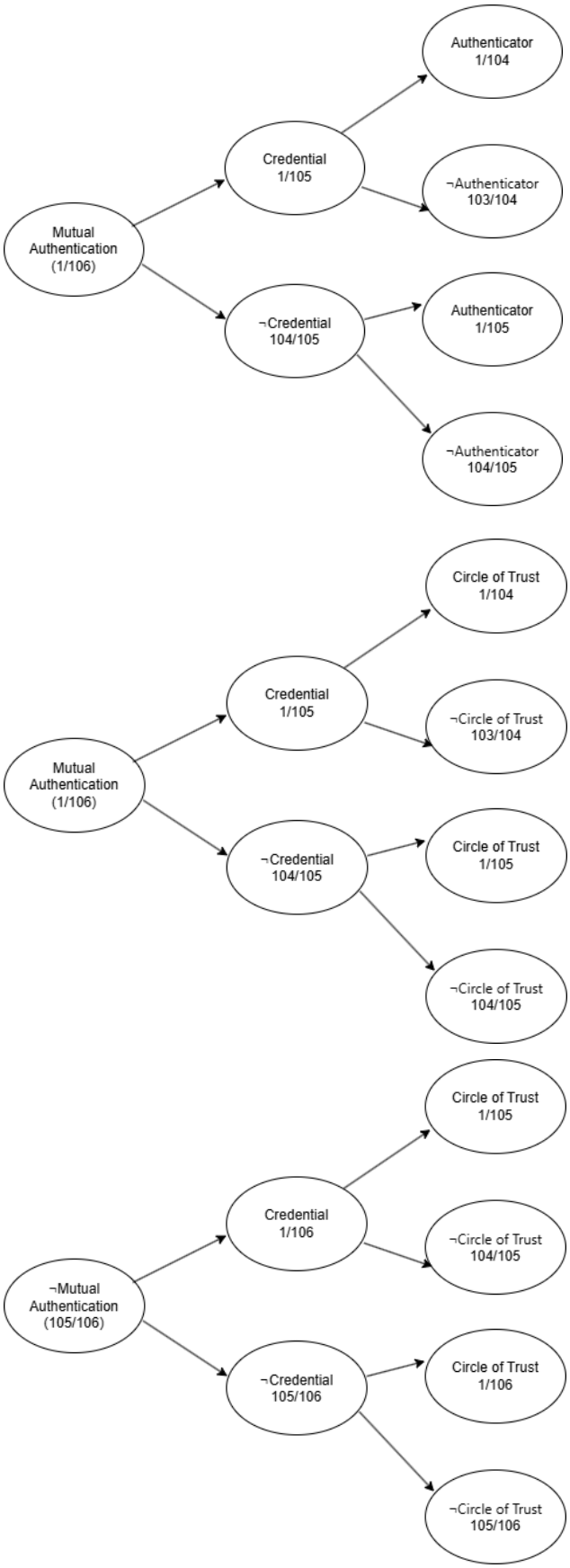
Denominator needs to take into account these cases:

- Credential = 0, Mutual Authentication = 0
- Credential = 1, Mutual Authentication = 1
- Credential = 1, Mutual Authentication = 0
- Credential = 0, Mutual Authentication = 1

Denominator is:

p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Authenticator = 1 | Credential = 1)*p(Circle of Trust = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Authenticator = 1 | Credential = 0)*p(Circle of Trust = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) =
(1/105)*(1/105)*(105/106)*(105/106)+(1/104)*(1/104)*(1/105)*(1/106)+(1/104)*(1/104)*(1/106)*(105/106)+(1/105)*(1/105)*(104/105)*(1/106)=

Probability p(Mutual Authentication = 1 | Circle of Trust = 1, Authenticator = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889



And again, to calculate p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 0) I need to use the Bayes rule:

p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 0) =

$$\frac{p(Mutual\ Authentication = 1,\ Authenticator = 1,\ Circle\ of\ Trust = 0)}{p(Authenticator = 1,\ Circle\ of\ Trust = 0)}$$

$$= \frac{\sum_{Credential} p(Circle\ of\ Trust\ = 0 \mid Credential) * p(Authenticator = 1 \mid Credential) * p(Credential \mid Mutual\ Authentication = 1) * p(Mutual\ Authentication = 1)}{\sum_{Mutual\ Authentication, Credential} p(Circle\ of\ Trust = 0 \mid Credential) * p(Authenticator = 1 \mid Credential) * p(Credential \mid Mutual\ Authentication) * p(Mutual\ Authentication)}$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (above)

numerator is:
p(Circle of Trust = 0 | Credential = 1)*p(Authenticator = 1 | Credential = 1)*
p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1)
+ p(Circle of Trust = 0 | Credential = 0)*p(Authenticator= 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) =
((104/105)*(1/104)*(1/105)*(1/106))+((104/105)*(1/105)*(104/105)*(1/106))=0.00008899972

denominator needs to take into account these cases:

- Credential = 0, Mutual Authentication = 0
- Credential = 1, Mutual Authentication = 1
- Credential = 1, Mutual Authentication = 0
- Credential = 0, Mutual Authentication = 1

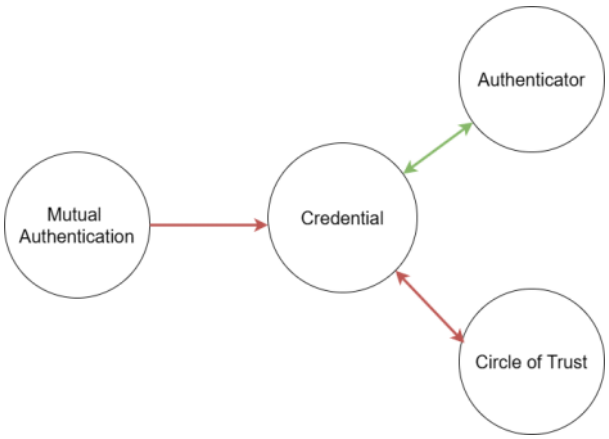
denominator is:
p(Circle of Trust = 0 | Credential = 0)*p(Authenticator = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Circle of Trust = 0 | Credential = 1)*p(Authenticator = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 1)*p(Mutual Authentication = 1) +
p(Circle of Trust = 0 | Credential = 1)*p(Authenticator = 1 | Credential = 1)*p(Credential = 1 | Mutual Authentication = 0)*p(Mutual Authentication = 0) +
p(Circle of Trust = 0 | Credential = 0)*p(Authenticator = 1 | Credential = 0)*p(Credential = 0 | Mutual Authentication = 1)*p(Mutual Authentication = 1) =
((104/105)*(1/105)*(105/106)*(105/106))+((104/105)*(1/104)*(1/105)*(1/106))+((104/105)*(1/104)*(1/106)*(105/106))+((105/106)*(1/105)*(104/105)*(1/106)) = 0.00943480172

Probability p(Mutual Authentication = 1 | Authenticator = 1, Circle of Trust = 0) value is 0.00008899972 / 0.00943397033 = 0.00943396225

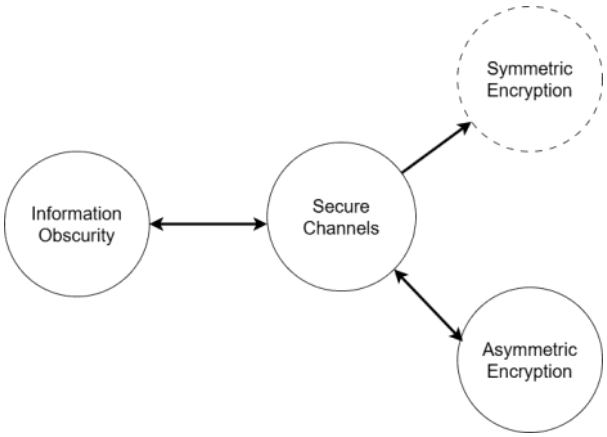
The probability that Mutual Authentication will be used before Authenticator regardless of whether or not the Circle of Trust pattern will be used after the Credential pattern can therefore be calculated as:

p(Mutual Authentication = 1 | Authenticator = 1, Circle of $Trust_{uncertain}$) = ((0.00943397889)*(1/104))+ ((0.00943396225)*(103/104)) = 0.00943396241 and this probability is lower than the probability p(Mutual Authentication = 1 | Circle of Trust = 1, $Authenticator_{uncertain}$) = 0.00943397786 of the event that the Credential would be used before the Circle of Trust.

It is therefore more likely that the sequence Mutual Authentication -> Credential -> Circle of Trust is used than the sequence Mutual Authentication -> Credential -> Authenticator. The relationship between Credential and Authenticator can be removed.



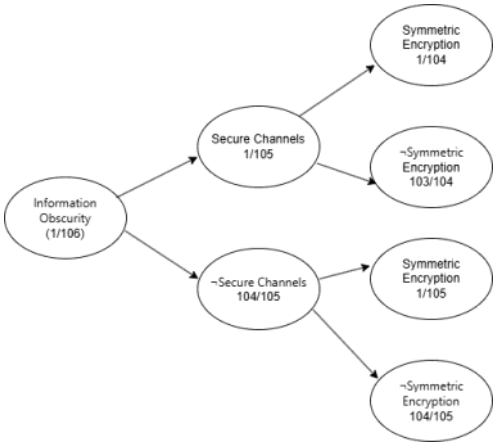
Calculating probability that the Information Obscurity would be used before the Asymmetric Encryption



The probability that Information Obscurity will be used before Asymmetric Encryption regardless of whether or not Symmetric Encryption$_{uncertain}$ will be used after Secure Channels can be calculated as:

p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption$_{uncertain}$) = p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) *p(Symmetric Encryption = 1 | Symmetric Encryption$_{uncertain}$) + p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 0)*p(Symmetric Encryption = 0 | Symmetric Encryption$_{uncertain}$) = p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) *(1/104)+ p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 0)*(103/104) =

The probability that Symmetric Encryption is used or not after Secure Channels is selected from the stochastic tree (see below):
p(Symmetric Encryption = 1 | Symmetric Encryption$_{uncertain}$) = 1/104
p(Symmetric Encryption = 0 | Symmetric Encryption$_{uncertain}$) = 103/104



To calculate p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) I need to use the Bayes rule:

p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) =

$$\frac{p(Information\ Obscurity = 1,\ Asymmetric\ Encryption = 1,\ Single\ Access\ Point = 1)}{p(Asymmetric\ Encryption = 1,\ Symmetric\ Encryption = 1)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p(Symmetric\ Encryption\ = 1 \mid Secure\ Channels) * \\ p(Asymmetric\ Encryption = 1 \mid Secure\ Channels) * \\ p(Secure\ Channels \mid Information\ Obscurity = 1) * \\ p(Information\ Obscurity = 1) \end{matrix}}{\sum_{Information\ Obscurity,\ Secure\ Channels} \begin{matrix} p(Symmetric\ Encryption = 1 \mid Secure\ Channels) * \\ p(Asymmetric\ Encryption = 1 \mid Secure\ Channels) \\ * p(Secure\ Channels \mid Information\ Obscurity) * \\ p(Information\ Obscurity) \end{matrix}} =$$

where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below):

numerator is:
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) + p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) = ((1/104)*(1/104)*(1/105)*(1/106)) + ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00000085584566

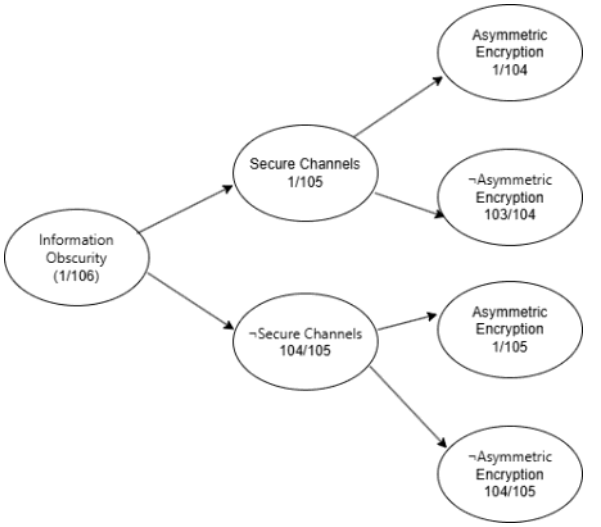
denominator needs to take into account these cases:

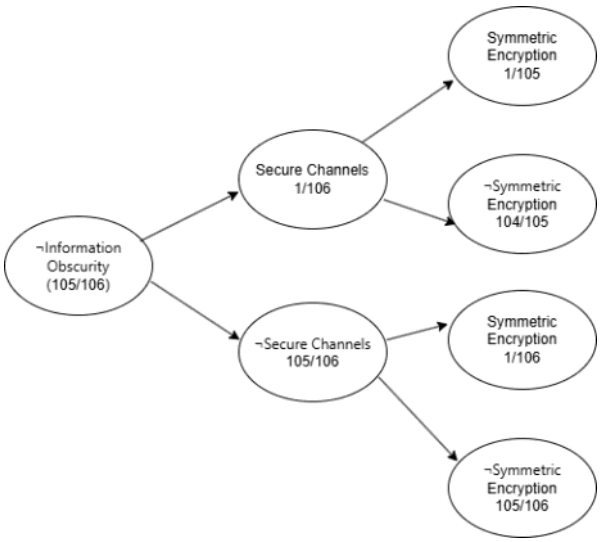
- Secure Channels = 0, Information Obscurity = 0
- Secure Channels = 1, Information Obscurity = 1
- Secure Channels = 1, Information Obscurity = 0
- Secure Channels = 0, Information Obscurity = 1

denominator is:

p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1) 1)*p(Information Obscurity = 1) =
((1/105)*(1/105)*(105/106)*(105/106))+((1/104)*(1/104)*(1/105)*(1/106))+((1/104)*(1/104)*(1/106)*(105/106))+ ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00009071948

Probability p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889





And again, to calculate probability p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 0) I need to use the Bayes rule:

p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 0) =

$$\frac{p(Information\ Obscurity = 1,\ Asymmetric\ Encryption = 1,\ Symmetric\ Encryption = 0)}{p(Asymmetric\ Encryption = 1,\ Symmetric\ Encryption = 0)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption = 0 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p(Secure\ Channels \,|\, Information\ Obscurity = 1) * \\ p(Information\ Obscurity = 1) \end{matrix}}{\sum_{Information\ Obscurity,\ Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption = 0 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) \\ * p(Secure\ Channels\ |Information\ Obscurity) * \\ p(Information\ Obscurity) \end{matrix}} =$$

= where I can take the values for calculating the numerator and denominator directly from stochastic trees (see above)

numerator is:
p(Symmetric Encryption = 0 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) + p(Symmetric Encryption = 0 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) = ((104/105)*(1/104)*(1/105)*(1/106)) + ((104/105)*(1/105)*(104/105)*(1/106)) = 0.00008899972

denominator needs to take into account these cases:

- Secure Channels = 0, Information Obscurity = 0
- Secure Channels = 1, Information Obscurity = 1
- Secure Channels = 1, Information Obscurity = 0
- Secure Channels = 0, Information Obscurity = 1

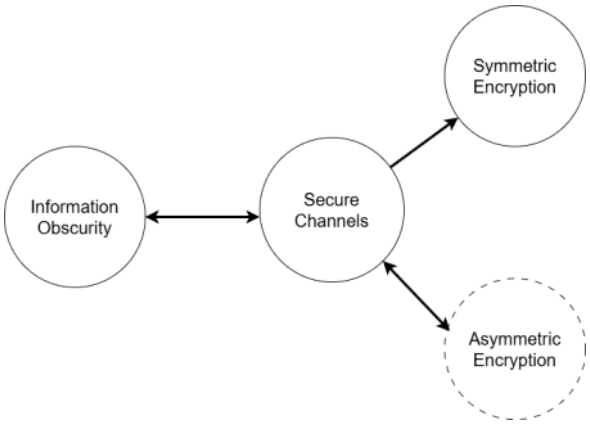
denominator is:
p(Symmetric Encryption = 0 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 0 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) +
p(Symmetric Encryption = 0 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 0 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) =
((105/106)*(1/105)*(105/106)*(105/106))+((103/104)*(1/104)*(1/105)*(1/106))+((103/104)*(1/104)*(1/106)*(105/106))+((105/106)*(1/105)*(104/105)*(1/106)) = 0.00943480164

Probability p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 0) value is 0.00008899972 / 0.00943480164 = 0.00943313101

The probability that Information Obscurity will be used before Asymmetric Encryption regardless of whether or not Symmetric Encryption will be used after Secure Channels can be calculated as:

p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+ ((0.00943313101)*(103/104)) = 0.00943313916 and it's a low probability.

Calculating probability that the Information Obscurity would be used before the Symmetric Encryption



In the previous calculation, I was able to calculate the probability that the Information Obscurity will be used before the Asymmetric Encryption pattern, regardless of the use of Symmetric Encryption after the Secure Channels pattern. This probability was:

p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+ ((0.00943313101)*(103/104)) = 0.00943313916

However, it is questionable whether this probability is higher, lower, or the same as the probability that Information Obscurity will be used before the Symmetric Encryption pattern, regardless of the use of Asymmetric Encryption after the Secure Channels pattern. In case:

- that the latter probability is lower than the probability of using Asymmetric Encryption after Secure Channels (and also Information Obscurity), the sequence Information Obscurity -> Secure Channels -> Asymmetric Encryption will be more likely to be used than the sequence Information Obscurity -> Secure Channels -> Symmetric Encryption. In this case, the relationship between Secure Channels and Symmetric Encryption will be removed.

- that the latter probability is higher than the probability of using Asymmetric Encryption after Secure Channels (and also Information Obscurity), the sequence Information Obscurity -> Secure Channels -> Symmetric Encryption will be more likely to be used than the sequence Information Obscurity -> Secure Channels -> Asymmetric Encryption. In this case, the relationship between Secure Channels and Asymmetric Encryption will be removed.

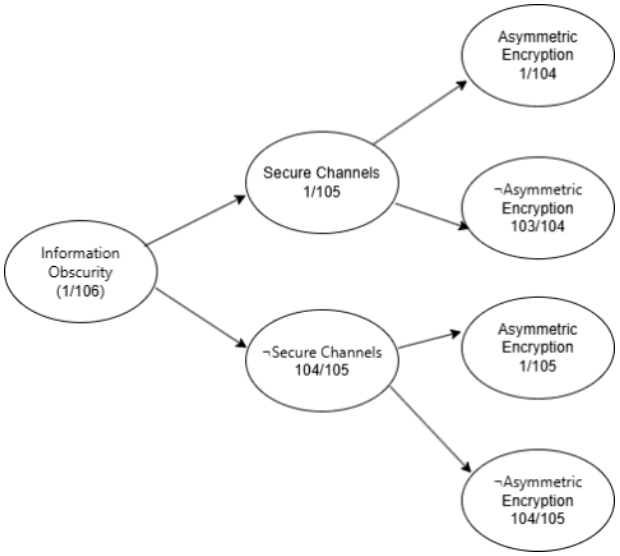
- That the latter probability is the same as the probability of using Asymmetric Encryption after Secure Channels (and also Information Obscurity), then the relationships between Information Obscurity, Secure Channels, Asymmetric Encryption, and Symmetric Encryption should be left. Such a situation will mean that a combination of Asymmetric Encryption and Symmetric Encryption patterns is expected to be used after the Secure Channels pattern.

The probability that Information Obscurity will be used before Symmetric Encryption regardless of whether or not Asymmetric Encryption will be used after Secure Channels can be calculated as:

p(Information Obscurity = 1 | Asymmetric Encryption$_{uncertain}$, Symmetric Encryption = 1) = p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 1)*p(Asymmetric Encryption = 1 | Asymmetric Encryption$_{uncertain}$) + p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0)*p(Asymmetric Encryption = 0 | Asymmetric Encryption$_{uncertain}$) = p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 1) *(1/104)+ p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0)*(103/104) =

The probability that Asymmetric Encryption is used or not after Secure Channels is selected from the stochastic tree (see below):

p(Asymmetric Encryption = 1 | Asymmetric Encryption$_{uncertain}$) = 1/104
p(Asymmetric Encryption = 0 | Asymmetric Encryption$_{uncertain}$) = 103/104



p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) =

$$\frac{p(Information\ Obscurity = 1,\ Asymmetric\ Encryption = 1,\ Single\ Access\ Point = 1)}{p(Asymmetric\ Encryption = 1,\ Symmetric\ Encryption = 1)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption\ = 1 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p\left(Secure\ Channels \,\middle|\, Information\ Obscurity = 1\right) * \\ p(Information\ Obscurity = 1) \end{matrix}}{\sum_{Information\ Obscurity,\ Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) \\ * p(Secure\ Channels\ |Information\ Obscurity) * \\ p(Information\ Obscurity) \end{matrix}} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

numerator is:
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) + p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) = ((1/104)*(1/104)*(1/105)*(1/106)) + ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00000085584566

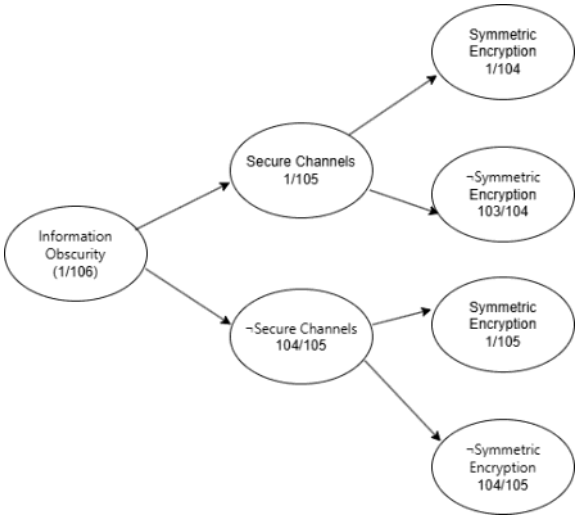
denominator needs to take into account these cases:

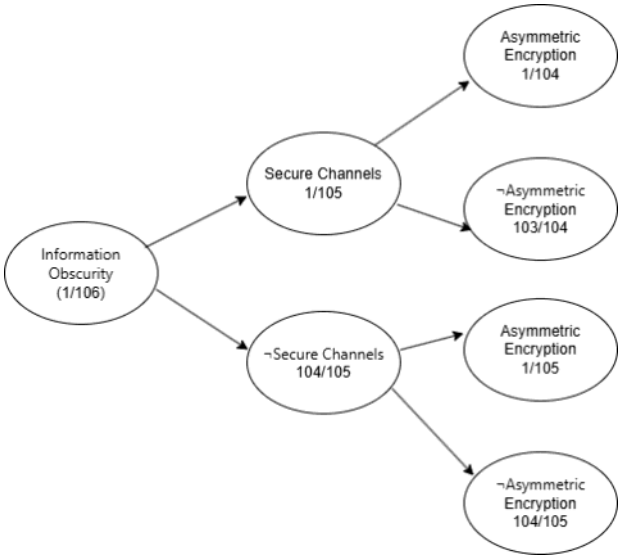
- Secure Channels = 0, Information Obscurity = 0
- Secure Channels = 1, Information Obscurity = 1
- Secure Channels = 1, Information Obscurity = 0
- Secure Channels = 0, Information Obscurity = 1

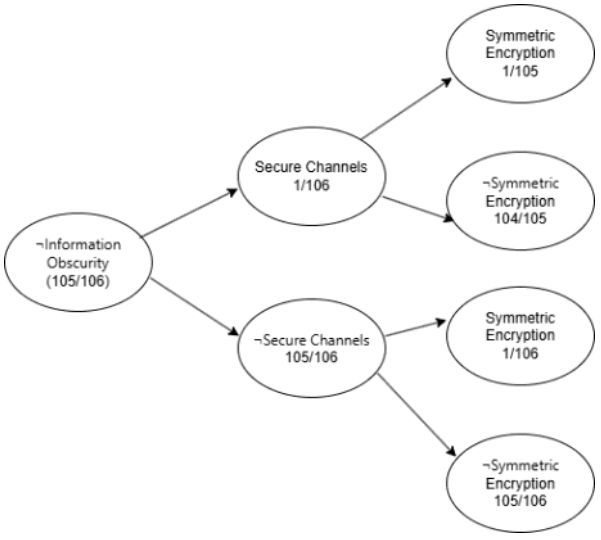
denominator is:

p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1) 1)*p(Information Obscurity = 1) =
((1/105)*(1/105)*(105/106)*(105/106))+((1/104)*(1/104)*(1/105)*(1/106))+((1/104)*(1/104)*(1/106)*(105/106))+ ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00009071948

Probability p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) value is 0.00000085584566 / 0.00009071948 = 0.00943397889


Information Obscurity (1/106)
Secure Channels 1/105
¬Secure Channels 104/105
Symmetric Encryption 1/104
¬Symmetric Encryption 103/104
Symmetric Encryption 1/105
¬Symmetric Encryption 104/105


Information Obscurity (1/106)
Secure Channels 1/105
¬Secure Channels 104/105
Asymmetric Encryption 1/104
¬Asymmetric Encryption 103/104
Asymmetric Encryption 1/105
¬Asymmetric Encryption 104/105


¬Information Obscurity (105/106)
Secure Channels 1/106
¬Secure Channels 105/106
Symmetric Encryption 1/105
¬Symmetric Encryption 104/105
Symmetric Encryption 1/106
¬Symmetric Encryption 105/106

And again, to calculate p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) I need to use the Bayes rule:

p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) =

$$\frac{p(Information\ Obscurity = 1,\ Symmetric\ Encryption = 1,\ Asymmetric\ Encryption = 0)}{p(Symmetric\ Encryption = 1,\ Asymmetric\ Encryption = 0)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p(Asymmetric\ Encryption\ = 0 \mid Secure\ Channels) * \\ p(Symmetric\ Encryption = 1 \mid Secure\ Channels) * \\ p(Secure\ Channels \mid Information\ Obscurity = 1) * \\ p(Information\ Obscurity\ = 1) \end{matrix}}{\sum_{Information\ Obscurity\ ,\ Secure\ Channels} \begin{matrix} p(Asymmetric\ Encryption = 0 \mid Secure\ Channels) * \\ p(Symmetric\ Encryption = 1 \mid Secure\ Channels) \\ * p(Secure\ Channels\ | Information\ Obscurity) * \\ p(Information\ Obscurity) \end{matrix}}$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see above)

numerator is:
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) + p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) =
((103/104)*(1/104)*(1/105)*(1/106))+((104/105)*(1/105)*(104/105)*(1/106)) = 0.00008899964

denominator needs to take into account these cases:

- Secure Channels = 0, Information Obscurity = 0
- Secure Channels = 1, Information Obscurity = 1
- Secure Channels = 1, Information Obscurity = 0
- Secure Channels = 0, Information Obscurity = 1

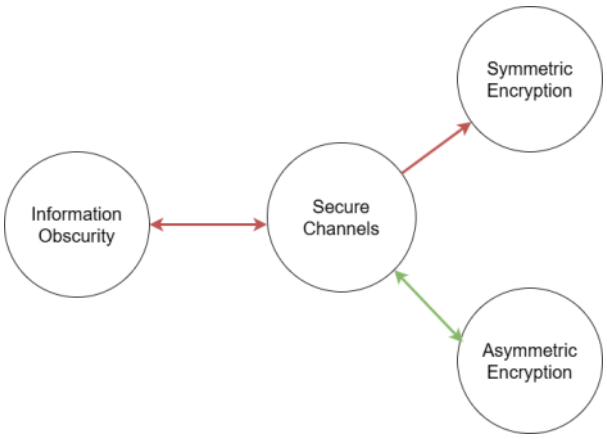
denominator is:
p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 1)*p(Information Obscurity = 1) +
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Information Obscurity = 0)*p(Information Obscurity = 0) +
p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Information Obscurity = 1)*p(Information Obscurity = 1) =
((104/105)*(1/105)*(105/106)*(105/106))+((103/104)*(1/104)*(1/105)*(1/106))+((103/104)*(1/104)*(1/106)*(105/106))+((104/105)*(1/105)*(104/105)*(1/106)) = 0.00943395403

Probability p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) value is 0.00008899964 / 0.00943395403 = 0.00943397007

The probability that Information Obscurity will be used before Symmetric Encryption regardless of whether or not Asymmetric Encryption will be used after Secure Channels can therefore be calculated as:

p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+ ((0.00943397007)*(103/104)) = 0.00943397015 and this probability is higher than the p(Information Obscurity = 1 | Asymmetric Encryption = 1, Symmetric Encryption$_{uncertain}$) = 0.00943313916 of the event that the Asymmetric Encryption would be used after Secure Channels.

It is therefore more likely that the sequence Information Obscurity -> Secure Channels -> Symmetric Encryption is used than the sequence Information Obscurity -> Secure Channels -> Asymmetric Encryption. The relationship between Secure Channels and Asymmetric Encryption can be removed.

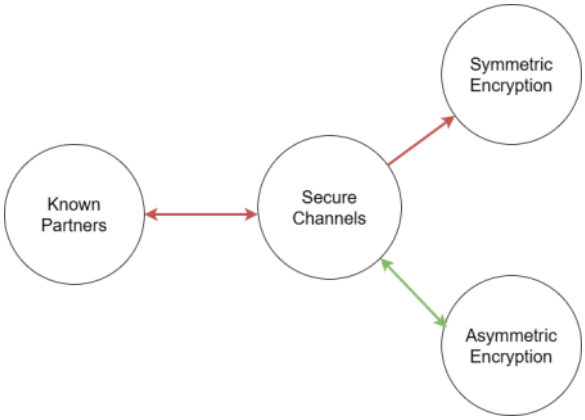


Calculating probability that the Known Partners would be used before Symmetric Encryption

In the previous calculation, I was able to calculate the probability of the use of pattern sequence Information Obscurity -> Secure Channels -> Symmetric Encryption. This probability was:

p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+ ((0.00943397007)*(103/104)) = 0.00943397015

However, before the Secure Channels pattern, in addition to Information Obscurity, the Known Partners pattern can also be used, and therefore it is necessary to compare this probability with the probability p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption$_{uncertain}$) in order to find out whether the use of the Information Obscurity - > Secure Channels -> Symmetric Encryption is the more likely than of the sequence Known Partners -> Secure Channels -> Symmetric Encryption.

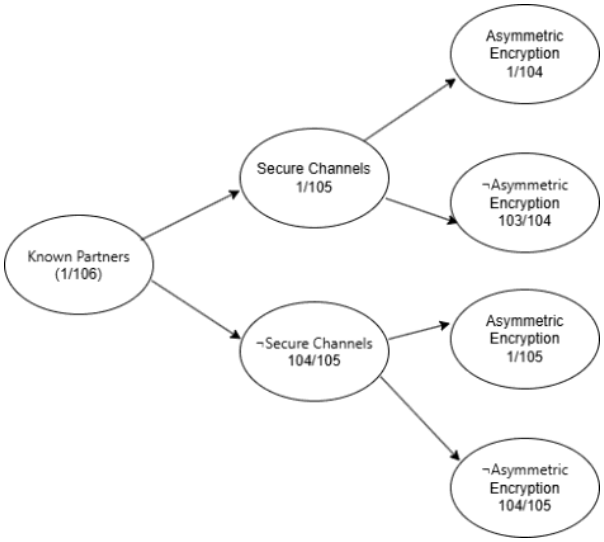


The probability that Known Partners will be used before Symmetric Encryption regardless of whether or not Asymmetric Encryption will be used after Secure Channels can be calculated as:

p(Known Partners = 1 | Asymmetric Encryption$_{uncertain}$, Symmetric Encryption = 1) = p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 1)*p(Asymmetric Encryption = 1 | Asymmetric Encryption$_{uncertain}$) + p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0)*p(Asymmetric Encryption = 0 | Asymmetric Encryption$_{uncertain}$) = p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 1) *(1/104)+ p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0)*(103/104) =

The probability that Asymmetric Encryption is used or not after Secure Channels is selected from the stochastic tree (see below):

p(Asymmetric Encryption = 1 | Asymmetric Encryption$_{uncertain}$) = 1/104
p(Asymmetric Encryption = 0 | Asymmetric Encryption$_{uncertain}$) = 103/104



p(Known Partners = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) =

$$\frac{p(Known\ Partners = 1,\ Asymmetric\ Encryption = 1,\ Single\ Access\ Point = 1)}{p(Asymmetric\ Encryption = 1,\ Symmetric\ Encryption = 1)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption\ = 1 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p(Secure\ Channels \mid Known\ Partners = 1) * \\ p(Known\ Partners = 1) \end{matrix}}{\sum_{Known\ Partners,\ Secure\ Channels} \begin{matrix} p\left(Symmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p\left(Asymmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) \\ * p(Secure\ Channels \mid Known\ Partners) * p(Known\ Partners) \end{matrix}} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

numerator is:
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Known Partners = 1)*p(Known Partners = 1) + p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 1)*p(Known Partners = 1) = ((1/104)*(1/104)*(1/105)*(1/106)) + ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00000085584566

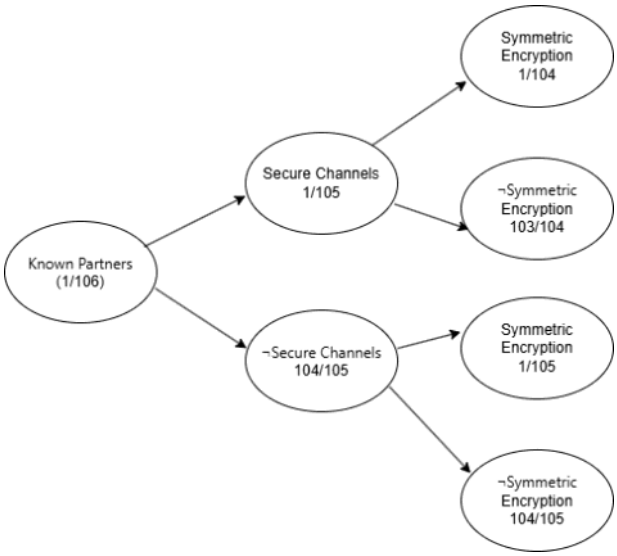
denominator needs to take into account these cases:

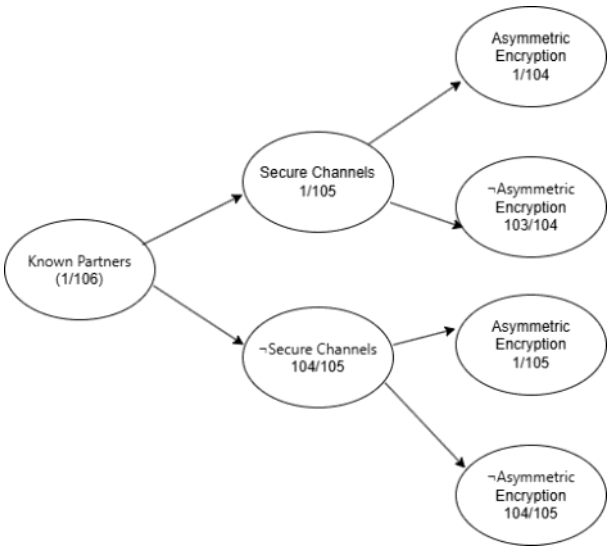
- Secure Channels = 0, Known Partners = 0
- Secure Channels = 1, Known Partners = 1
- Secure Channels = 1, Known Partners = 0
- Secure Channels = 0, Known Partners = 1

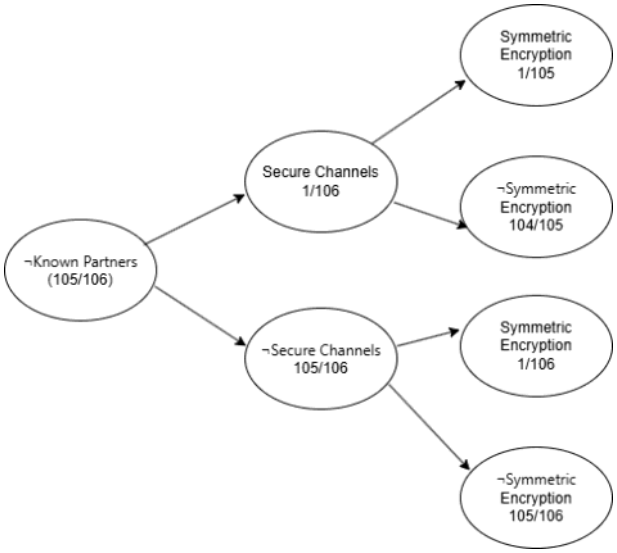
denominator is:

p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 0)*p(Known Partners = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Known Partners = 1)*p(Known Partners = 1) +
p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Asymmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Known Partners = 0)*p(Known Partners = 0) +
p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Asymmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 1) 1)*p(Known Partners = 1) =
((1/105)*(1/105)*(105/106)*(105/106))+((1/104)*(1/104)*(1/105)*(1/106))+((1/104)*(1/104)*(1/106)*(105/106))+
((1/105)*(1/105)*(104/105)*(1/106)) = 0.00009071948

Probability p(Known Partners = 1 | Asymmetric Encryption = 1, Symmetric Encryption = 1) value is
0.00000085584566 / 0.00009071948 = 0.00943397889







And again, to calculate p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) I need to use the Bayes rule:

p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) =

$$\frac{p(Known\ Partners = 1,\ Symmetric\ Encryption = 1,\ Asymmetric\ Encryption = 0)}{p(Symmetric\ Encryption = 1,\ Asymmetric\ Encryption = 0)}$$

$$= \frac{\sum_{Secure\ Channels} \begin{matrix} p\left(Asymmetric\ Encryption\ = 0 \,\middle|\, Secure\ Channels\right) * \\ p\left(Symmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) * \\ p(Secure\ Channels \mid Known\ Partners = 1) * \\ p(Known\ Partners\ = 1) \end{matrix}}{\sum_{Knwon\ Partners\ ,\ Secure\ Channels} \begin{matrix} p\left(Asymmetric\ Encryption = 0 \,\middle|\, Secure\ Channels\right) * \\ p\left(Symmetric\ Encryption = 1 \,\middle|\, Secure\ Channels\right) \\ * p(Secure\ Channels \mid Known\ Partners) * \\ p(Known\ Partners) \end{matrix}}$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see above):

numerator is:
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)* p(Secure Channels = 1 | Known Partners = 1)*p(Known Partners = 1) + p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 1)*p(Known Partners = 1) = ((103/104)*(1/104)*(1/105)*(1/106))+((104/105)*(1/105)*(104/105)*(1/106)) = 0.00008899964

denominator needs to take into account these cases:

- Secure Channels = 0, Known Partners = 0
- Secure Channels = 1, Known Partners = 1
- Secure Channels = 1, Known Partners = 0
- Secure Channels = 0, Known Partners = 1

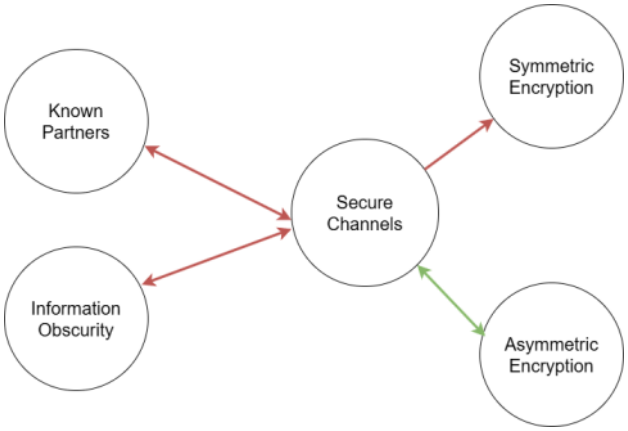
denominator is:
p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 0)*p(Known Partners = 0) +
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Known Partners = 1)*p(Known Partners = 1) +
p(Asymmetric Encryption = 0 | Secure Channels = 1)*p(Symmetric Encryption = 1 | Secure Channels = 1)*p(Secure Channels = 1 | Known Partners = 0)*p(Known Partners = 0) +
p(Asymmetric Encryption = 0 | Secure Channels = 0)*p(Symmetric Encryption = 1 | Secure Channels = 0)*p(Secure Channels = 0 | Known Partners = 1)*p(Known Partners = 1) =
((104/105)*(1/105)*(105/106)*(105/106))+((103/104)*(1/104)*(1/105)*(1/106))+((103/104)*(1/104)*(1/106)*(105/106))+((104/105)*(1/105)*(104/105)*(1/106)) = 0.00943395403

Probability p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption = 0) value is 0.00008899964 / 0.00943395403 = 0.00943397007

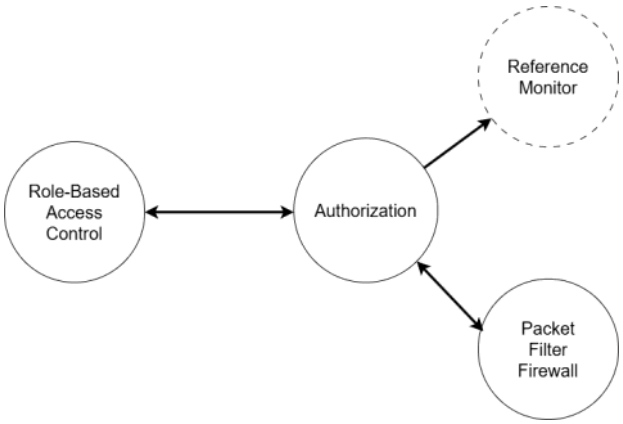
The probability that Known Partners will be used before Symmetric Encryption regardless of whether or not Asymmetric Encryption will be used after Secure Channels can therefore be calculated as:

p(Known Partners = 1 | Symmetric Encryption = 1, Asymmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+((0.00943397007)*(103/104)) = 0.00943397015 and this probability is equal to the probability p(Information Obscurity = 1 | Symmetric Encryption = 1, Asymmetric Encryption$_{uncertain}$) = ((0.00943397889)*(1/104))+((0.00943397007)*(103/104)) = 0.00943397015 that the pattern sequence Information Obscurity -> Secure Channels -> Symmetric Encryption will be used.

It is therefore likely that a combination of Information Obscurity and Known Partners patterns will be used before Secure Channels.



Calculating probability that the Role-Based Access Control would be used before the Packet Filter Firewall

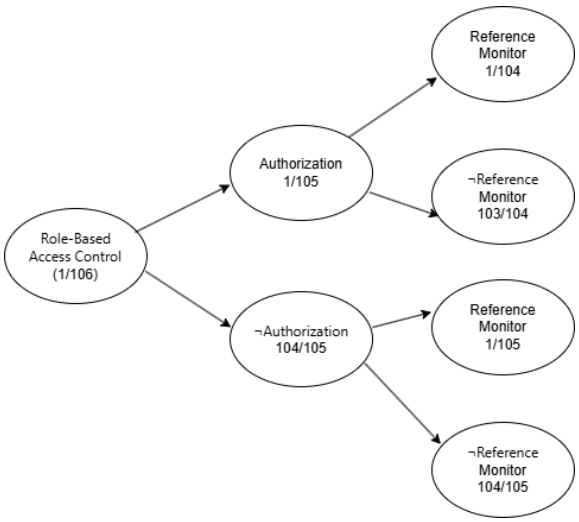


The probability that Role-Based Access Control will be used before Packet Filter Firewall regardless of whether or not Reference $Monitor_{uncertain}$ will be used after the Authorization pattern can be calculated as:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference $Monitor_{uncertain}$) = p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) *p(Reference Monitor= 1 | Reference $Monitor_{uncertain}$) + p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 0)*p(Reference Monitor = 0 | Reference $Monitor_{uncertain}$) = p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) *(1/104)+ p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 0)*(103/104) =

The probability that the Reference Monitor will or will not be used after Authorization is selected from the stochastic tree (see below):

p(Reference Monitor = 1 | Reference $Monitor_{uncertain}$) = 1/104
p(Reference Monitor = 0 | Reference $Monitor_{uncertain}$) = 103/104



To calculate p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) I need to use the Bayes rule:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) =

$$\frac{p(Role-Based\ Access\ Control=1,\ Packet\ Filter\ Firewall=1,\ Reference\ Monitor=1)}{p(Packet\ Filter\ Firewall=1,\ Reference\ Monitor=1)} =$$

$$= \frac{\sum_{Authorization} \begin{matrix} p(Reference\ Monitor\ =1 \mid Authorization) * \\ p(Packet\ Filter\ Firewall=1 \mid Authorization) * \\ p(Authorization \mid Role-Based\ Access\ Control=1) * \\ p(Role-Based\ Access\ Control=1) \end{matrix}}{\sum_{Role-Based\ Access\ Control,\ Authorization} \begin{matrix} p(Reference\ Monitor=1 \mid\ Authorization) * \\ p(Packet\ Filter\ Firewall=1 \mid Authorization) \\ * p(Authorization \mid Role-Based\ Access\ Control) * \\ p(Role-Based\ Access\ Control) \end{matrix}} =$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

numerator is:
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*
p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) + p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) = ((1/104)*(1/104)*(1/105)*(1/106)) + ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00000085584566

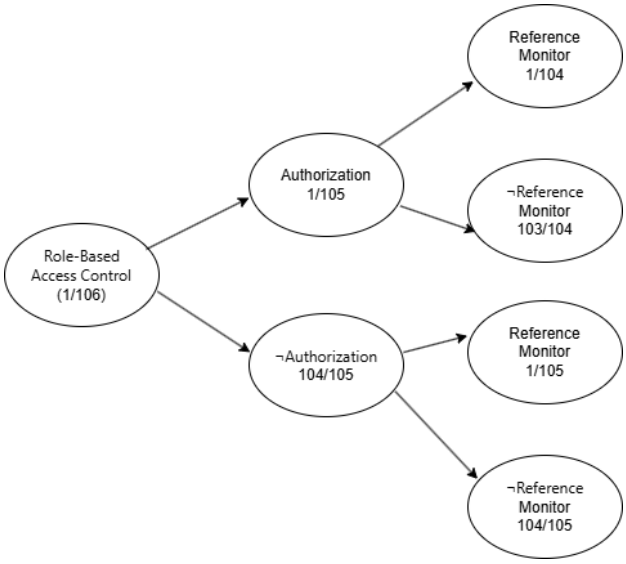
denominator needs to take into account these cases:

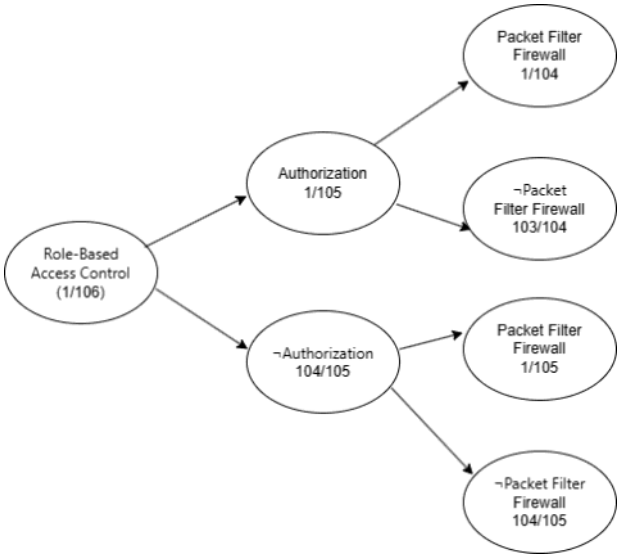
- Authorization = 0, Role-Based Access Control = 0
- Authorization = 1, Role-Based Access Control = 1
- Authorization = 1, Role-Based Access Control = 0
- Authorization = 0, Role-Based Access Control = 1

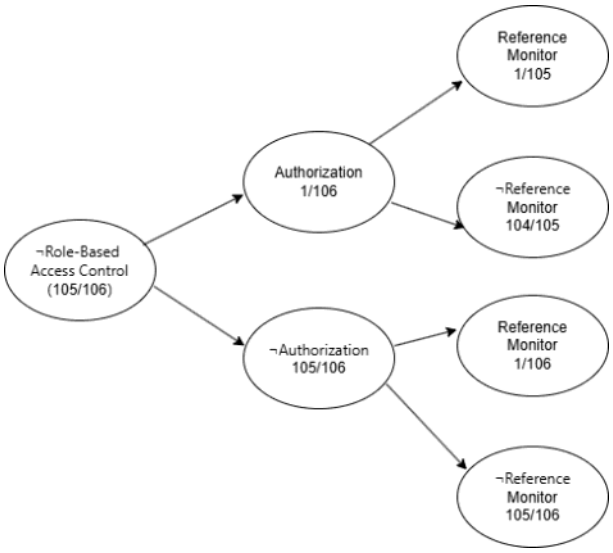
denominator is:

p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) +
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) =
((1/105)*(1/105)*(105/106)*(105/106))+((1/104)*(1/104)*(1/105)*(1/106))+((1/104)*(1/104)*(104/105)*(105/106))+((1/105)*(1/105)*(104/105)*(1/106)) =
0.00018056666

Probability p(Role-Based Access Contro = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) value is 0.00000085584566 / 0.00018056666 = 0.00473977676721


Role-Based Access Control (1/106)
Authorization 1/105
¬Authorization 104/105
Reference Monitor 1/104
¬Reference Monitor 103/104
Reference Monitor 1/105
¬Reference Monitor 104/105


Role-Based Access Control (1/106)
Authorization 1/105
¬Authorization 104/105
Packet Filter Firewall 1/104
¬Packet Filter Firewall 103/104
Packet Filter Firewall 1/105
¬Packet Filter Firewall 104/105


¬Role-Based Access Control (105/106)
Authorization 1/106
¬Authorization 105/106
Reference Monitor 1/105
¬Reference Monitor 104/105
Reference Monitor 1/106
¬Reference Monitor 105/106

And again, to calculate p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 0) I need to use the Bayes rule:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 0) =

$$\frac{p(Role-Based\ Access\ Control=1, Packet\ Filter\ Firewall=1,\ Reference\ Monitor=0)}{p(Packet\ Filter\ Firewall=1,\ Reference\ Monitor=0)}$$

$$= \frac{\sum_{Authorization} \begin{matrix} p(Reference\ Monitor=0 \mid Authorization) * \\ p(Packet\ Filter\ Firewall=1 \mid Authorization) * \\ p(Authorization \mid Role-Based\ Access\ Control=1) * \\ p(Role-Based\ Access\ Control=1) \end{matrix}}{\sum_{Role-Based\ Access\ Control,\ Authorization} \begin{matrix} p(Reference\ Monitor=0 \mid Authorization) * \\ p(Packet\ Filter\ Firewall=1 \mid Authorization) * \\ p(Authorization \mid Role-Based\ Access\ Control) * \\ p(Role-Based\ Access\ Control) \end{matrix}} =$$

= where I can take the values for calculating the numerator and denominator directly from stochastic trees (see above)

numerator is:
p(Reference Monitor = 0 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*
p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) + p(Reference Monitor = 0 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) = ((103/104)*(1/104)*(1/105)*(1/106)) +
((104/105)*(1/105)*(104/105)*(1/106)) =
0.00008899964

denominator needs to take into account these cases:

- Authorization = 0, Role-Based Access Control = 0
- Authorization = 1, Role-Based Access Control = 1
- Authorization = 1, Role-Based Access Control = 0
- Authorization = 0, Role-Based Access Control = 1

denominator is:

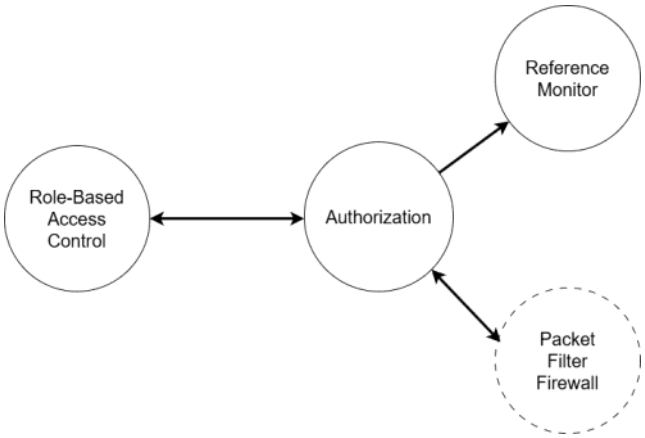
p(Reference Monitor = 0 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 0 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) +
p(Reference Monitor = 0 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 0 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) =
((104/105)*(1/105)*(105/106)*(105/106))+((103/104)*(1/104)*(1/105)*(1/106))+((103/104)*(1/104)*(1/106)*(105/106))+((105/106)*(1/105)*(104/105)*(1/106)) =
0.00943396202

Probability p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 0) value is
0.00008899964 / 0.00943396202 = 0.00943396208

The probability that Role-Based Access Control will be used before Packet Filter Firewall regardless of whether or not Reference Monitor will be used after Authorization can be calculated as:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor$_{uncertain}$) =
((0.00473977676721)*(1/104))+ ((0.00943396208)*(103/104)) =
0.00938882568 and this is a low probability.

Calculating probability that the Role-Based Access Control would be used before the Reference Monitor



Previously, I was able to calculate the probability that Role-Based Access Control will be used before the Packet Filter Firewall pattern regardless of the use of Reference Monitor after the Authorization pattern. This probability was:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor$_{uncertain}$) =
((0.00473977676721)*(1/104))+ ((0.00943396208)*(103/104)) = 0.00938882568

However, it is questionable whether this probability is higher, lower, or the same as the probability that Role-Based Access Control will be used before the Reference Monitor pattern, regardless of the use of Packet Filter Firewall after the Authorization pattern. In case:

- that the latter probability is lower than the probability of using Packet Filter Firewall after Authorization (and also Role-Based Access Control), then the sequence Role-Based Access Control -> Authorization -> Packet Filter Firewall will be more likely to be used than the sequence Role-Based Access Control -> Authorization -> Reference Monitor. In this case, the relationship between Authorization and Reference Monitor will be removed.

- that the latter probability is higher than the probability of using Packet Filter Firewall after Authorization (and also Role-Based Access Control), it will be more likely to use the sequence Role-Based Access Control -> Authorization -> Reference Monitor than the sequence Role-Based Access Control - > Authorization -> Packet Filter Firewall. In this case, the relationship between Authorization and Packet Filter Firewall will be removed.

- that this second probability is the same as the probability of using Packet Filter Firewall after Authorization (and also Role-Based Access Control), then the relationships between Role-Based Access Control, Authorization, Packet Filter Firewall, and Reference Monitor should be left. Such a situation will mean that after the Authorization pattern, a combination of the Packet Filter Firewall and Reference Monitor patterns is expected to be used.

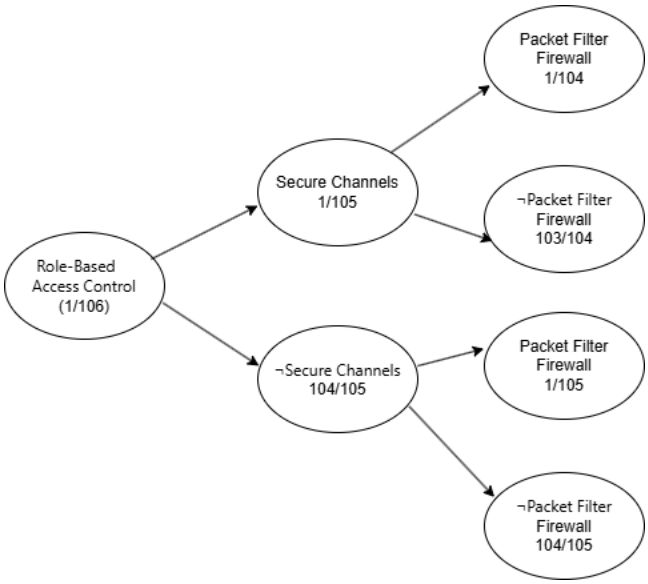
The probability that Role-Based Access Control will be used before Reference Monitor regardless of whether or not Packet Filter Firewall will be used after Authorization can be calculated as:

p(Role-Based Access Control = 1 | Packet Filter Firewall$_{uncertain}$, Reference Monitor = 1) = p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 1)*p(Packet Filter Firewall = 1 | Packet Filter Firewall$_{uncertain}$) + p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 0)*p(Packet Filter

Firewall = 0 | Packet Filter Firewall$_{uncertain}$) = p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 1) *(1/104)+ p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 0)*(103/104) =

The probability that the Packet Filter Firewall is used or not after Authorization is selected from the stochastic tree (see below):

p(Packet Filter Firewall = 1 | Packet Filter Firewall$_{uncertain}$) = 1/104
p(Packet Filter Firewall = 0 | Packet Filter Firewall$_{uncertain}$) = 103/104



To calculate p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) I need to use the Bayes rule:

p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) =

$$\frac{p(Role-Based\ Access\ Control=1,\ Packet\ Filter\ Firewall=1,\ Reference\ Monitor=1)}{p(Packet\ Filter\ Firewall=1,\ Reference\ Monitor=1)}=$$

$$=\frac{\sum_{Authorization}\begin{matrix}p(Reference\ Monitor\ =1\mid Authorization)*\\ p(Packet\ Filter\ Firewall=1\mid Authorization)*\\ p(Authorization\mid Role-Based\ Access\ Control=1)*\\ p(Role-Based\ Access\ Control=1)\end{matrix}}{\sum_{Role-Based\ Access\ Control,\ Authorization}\begin{matrix}p(Reference\ Monitor=1\mid\ Authorization)*\\ p(Packet\ Filter\ Firewall=1\mid Authorization)\\ *\ p(Authorization\mid Role-Based\ Access\ Control)*\\ p(Role-Based\ Access\ Control)\end{matrix}}=$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see below)

numerator is:
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)* p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) + p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) = ((1/104)*(1/104)*(1/105)*(1/106)) + ((1/105)*(1/105)*(104/105)*(1/106)) = 0.00000085584566

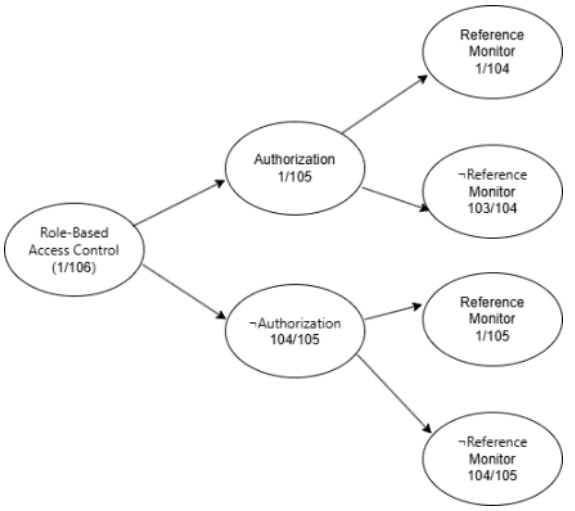
denominator needs to take into account these cases:

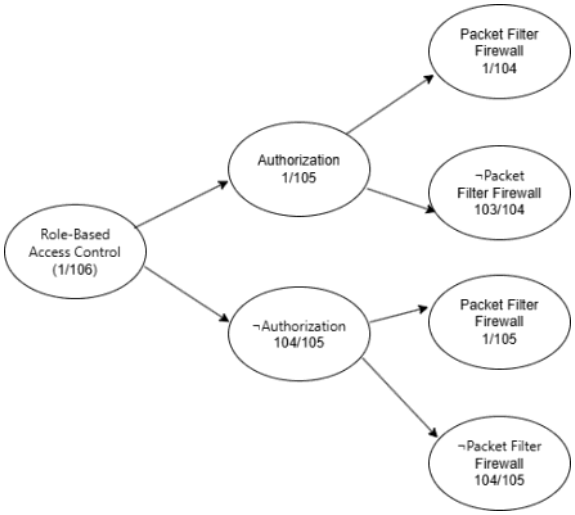
- Authorization = 0, Role-Based Access Control = 0
- Authorization = 1, Role-Based Access Control = 1
- Authorization = 1, Role-Based Access Control = 0
- Authorization = 0, Role-Based Access Control = 1

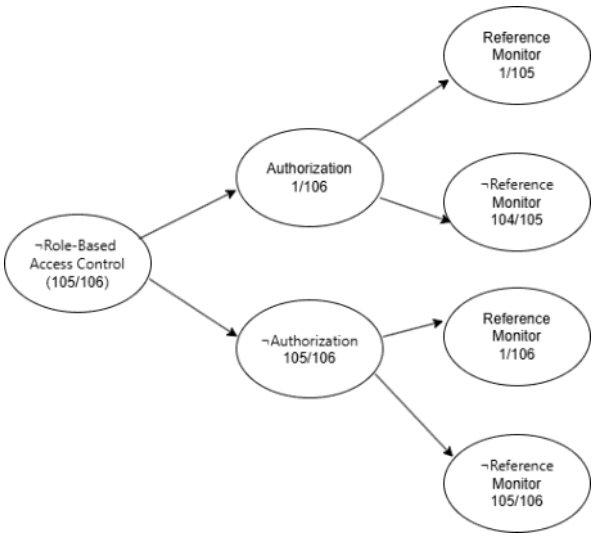
denominator is:

p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) +
p(Reference Monitor = 1 | Authorization = 1)*p(Packet Filter Firewall = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Reference Monitor = 1 | Authorization = 0)*p(Packet Filter Firewall = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) =
((1/105)*(1/105)*(105/106)*(105/106))+((1/104)*(1/104)*(1/105)*(1/106))+((1/104)*(1/104)*(104/105)*(105/106))+((1/105)*(1/105)*(104/105)*(1/106)) =
0.00018056666

Probability p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor = 1) value is
0.00000085584566 / 0.00018056666 = 0.00473977676721







And again, to calculate p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 0) I need to use the Bayes rule:

p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 0) =

$$\frac{p(Role-Based\ Access\ Control=1,\ Reference\ Monitor=1,\ Packet\ Filter\ Firewall=0)}{p(Packet\ Filter\ Firewall=1,\ Reference\ Monitor=0)}$$

$$= \frac{\sum_{Authorization} \begin{matrix} p(Packet\ Filter\ Firewall\ =0 \mid Authorization) * \\ p(Reference\ Monitor=1 \mid\ Authorization) * \\ p(Authorization \mid\ Role-Based\ Access\ Control=1) * \\ p(Role-Based\ Access\ Control\ =1) \end{matrix}}{\sum_{Role-Based\ Access\ Control\ ,\ Authorization} \begin{matrix} p(Packet\ Filter\ Firewall=0 \mid Authorization) * \\ p(Reference\ Monitor=1 \mid\ Authorization) \\ * p(Authorization \mid Role-Based\ Access\ Control) * \\ p(Role-Based\ Access\ Control) \end{matrix}}$$

= where the values for calculating the numerator and denominator can be taken directly from stochastic trees (see above):

numerator is:
p(Packet Filter Firewall = 0 | Authorization = 1)*p(Reference Monitor = 1 | Authorization = 1)*
p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) + p(Packet Filter Firewall = 0 | Authorization = 0)*p(Reference Monitor = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) =
((103/104)*(1/104)*(1/105)*(1/106))+((104/105)*(1/105)*(104/105)*(1/106)) =
0.00008899964

denominator needs to take into account these cases:

- Authorization = 0, Role-Based Access Control = 0
- Authorization = 1, Role-Based Access Control = 1
- Authorization = 1, Role-Based Access Control = 0
- Authorization = 0, Role-Based Access Control = 1

Denominator is:
p(Packet Filter Firewall = 0 | Authorization = 0)*p(Reference Monitor = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Packet Filter Firewall = 0 | Authorization = 1)*p(Reference Monitor = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) +
p(Packet Filter Firewall = 0 | Authorization = 1)*p(Reference Monitor = 1 | Authorization = 1)*p(Authorization = 1 | Role-Based Access Control = 0)*p(Role-Based Access Control = 0) +
p(Packet Filter Firewall = 0 | Authorization = 0)*p(Reference Monitor = 1 | Authorization = 0)*p(Authorization = 0 | Role-Based Access Control = 1)*p(Role-Based Access Control = 1) =
((104/105)*(1/105)*(105/106)*(105/106))+((103/104)*(1/104)*(1/105)*(1/106))+((103/104)*(1/104)*(1/106)*(105/106))+((105/106)*(1/105)*(104/105)*(1/106)) =
0.00943396202

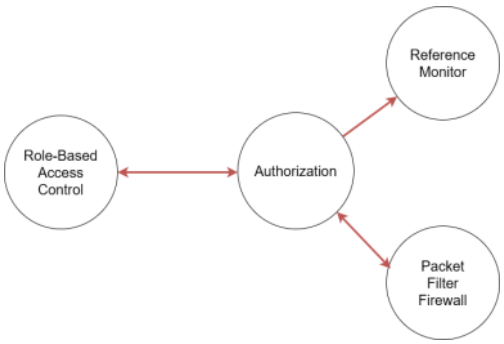
Probability p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall = 0) value is 0.00008899964 / 0.00943396202 = 0.00943396208

The probability that Role-Based Access Control will be used before Reference Monitor regardless of whether or not Packet Filter Firewall will be used after Authorization can therefore be calculated as:

p(Role-Based Access Control = 1 | Reference Monitor = 1, Packet Filter Firewall$_{uncertain}$) =
((0.00473977676721)*(1/104))+ ((0.00943396208)*(103/104)) =
0.00938882568

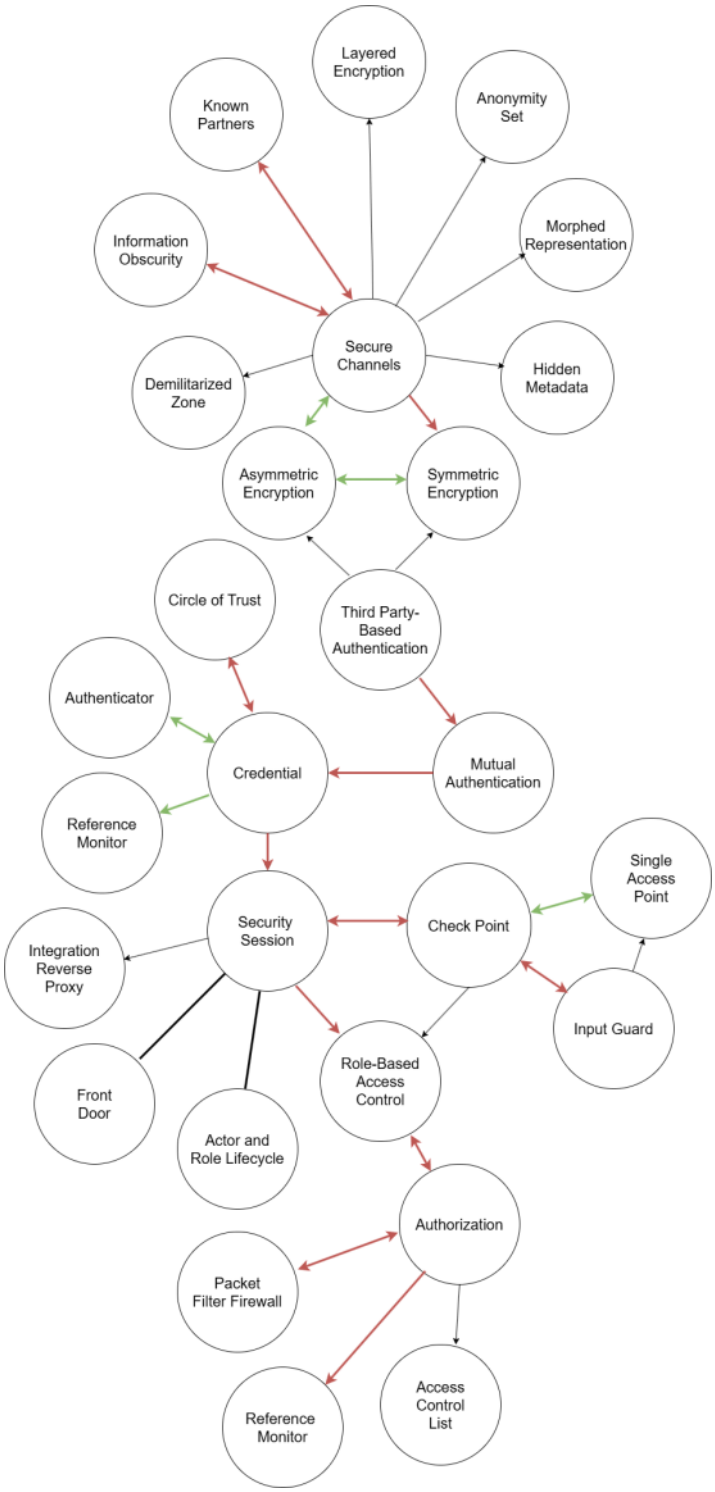
And this probability is the same as p(Role-Based Access Control = 1 | Packet Filter Firewall = 1, Reference Monitor$_{uncertain}$) = 0.00938882568 of the event that the Packet Filter Firewall would be used after Authorization.

It is therefore more likely that a combination of Packet Filter Firewall and Reference Monitor will be used after Authorization and all relationships should be kept.



This means that after the Security Session, either the Check Point -> Input Guard pattern sequence or the Role-Based Access Control -> Authorization -> (Packet Filter Firewall + Reference Monitor) pattern sequence is expected.

Simplified Bayesian Belief Network



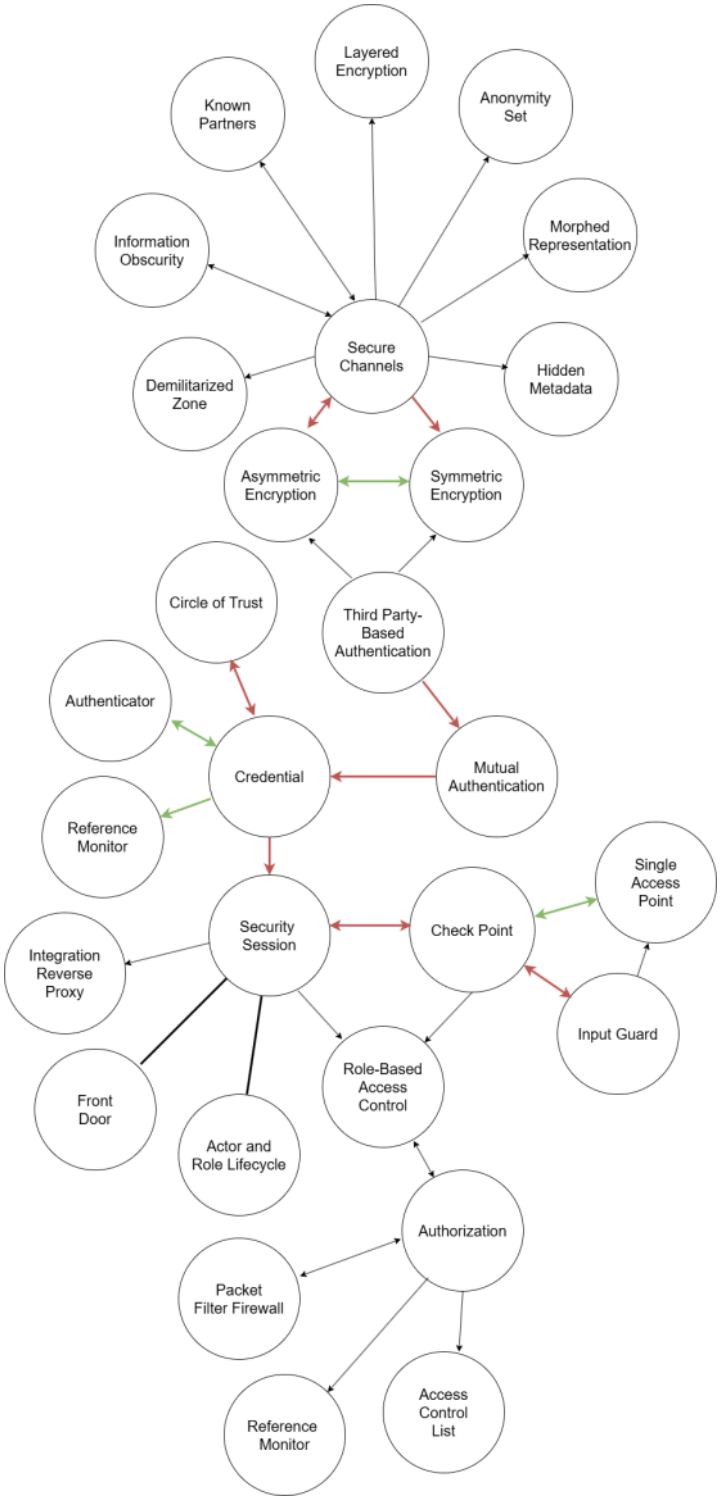
8. In order to maintain the continuity of the pattern sequence Secure Channels -> Asymmetric Encryption -> Third Party-Based Authentication -> Mutual Authentication -> Credential -> Security Session -> Check Point -> Input Guard I am also interested in how to simplify the Bayesian belief network so that it considers using the pattern Check Point after the Security Session without the sequence continuing in another direction using the Front Door or Actor and Role Lifecycle patterns.

   The problem is that the Front Door pattern and the Actor and Role Lifecycle pattern are conditionally dependent, because:

a) p(Front Door, Actor and Role Lifecycle | Security Session) ≠ p(Front Door | Security Session)*p(Actor and Role Lifecycle | Security Session)
b) There is only collider on the only path between Front Door and Actor and Role Lifecycle after Security Session. This collider is in the condition of the p(Front Door, Actor and Role Lifecycle | Security Session) and because of that this path is blocked.

Network can be simplified by transforming directed edges between patterns Security Session, Front Door, and Actor and Role Lifecycle to non-directed edges.

The Bayesian belief network looks like this after transformation:



Bibliography

Resources used to simplify the Bayesian belief network are:

- Barber, D. (2011). Bayesian Reasoning and Machine Learning. Cambridge University Press.