Removing Conditional Independent Relationships From the Belief Network - Only for Article

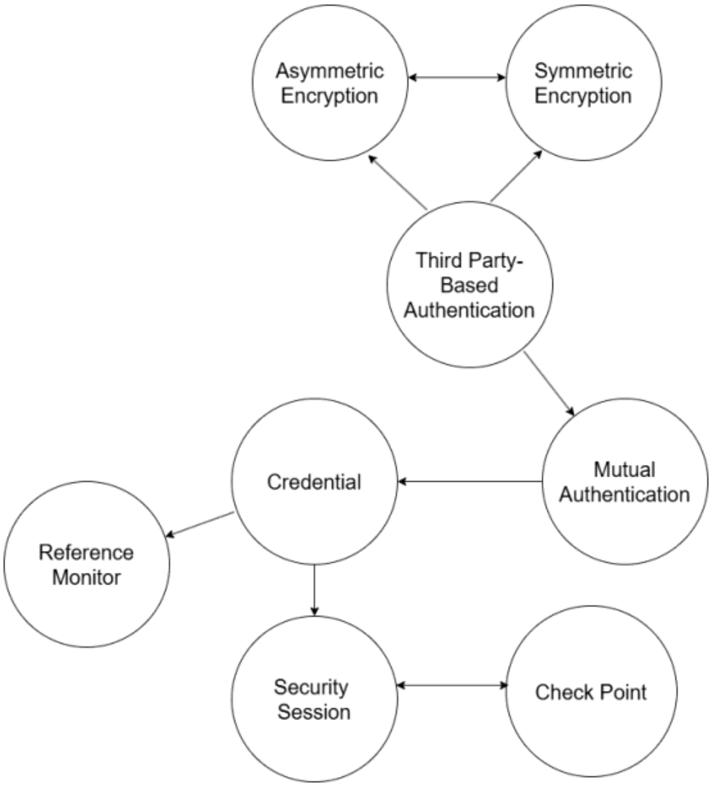
Thursday, August 1, 2024 8:12 PM

The following graph of the Bayesian belief network models a pattern sequence established using explicit relationships if patterns were allowed to be applied one after another. We extracted these explicit relationships from text descriptions of patterns.

Consider the following start-up pattern sequence:

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

This pattern sequence is meaningful, and we described it in a pattern story. We use the Bayesian belief network to find conditionally dependent and independent patterns in the start-up pattern sequence.
After we identify conditionally dependent patterns, we color edges between conditionally independent patterns with green color. Bayesian belief network will identify the pattern sequence that is expected because of conditionally dependent relationships between patterns.



Premenne pravdepodobnostneho modelu su:

- Asymmetric Encryption ∈ {0, 1} Asymmetric Encryption = 1 meaning pattern would be used, Asymmetric Encryption = 0 otherwise
- Symmetric Encryption ∈ {0, 1} Symmetric Encryption = 1 meaning pattern would be used, Symmetric Encryption = 0 otherwise
- Third Party-Based Authentication ∈ {0, 1} Third Party-Based Authentication = 1 meaning pattern would be used, Third Party-Based Authentication = 0 otherwise
- Mutual Authentication ∈ {0, 1} Mutual Authentication = 1 meaning pattern would be used, Authentication = 0 otherwise
- Credential ∈ {0, 1} Credential = 1 meaning pattern would be used, Credential = 0 otherwise
- Reference Monitor ∈ {0, 1} Reference Monitor = 1 meaning pattern would be used, Reference Monitor = 0 otherwise
- Security Session ∈ {0, 1} Security Session = 1 meaning pattern would be used, Security Session = 0 otherwise
- Check Point ∈ {0, 1} Check Point = 1 meaning pattern would be used, Check Point = 0 otherwise

Probability model of the Bayesian belief network is:

*p(Check Point | Secuity Session) * p(Security Session | Credential, Reference Monitor) * p(Credential | Mutual Authentication, Reference Monitor) * p(Mutual Authentication | Third Party-Based Authentication, Asymmetric Encryption) * p(Third Party-Based Authentication | Asymmetric Encryption)*p(Asymmetric Encryption)*

We decomposed identifying conditionally dependent patterns in the network into answering the following questions:

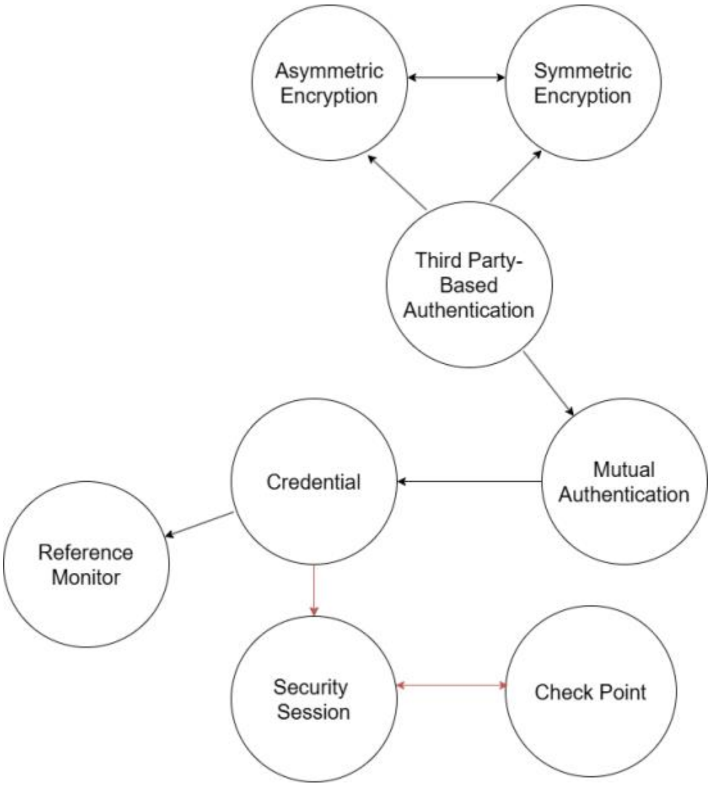
1. **Can we leave nodes for patterns Credential, Security Session, a Check Point connected as they are?** We can answer this question through answering a different question:

   Is Credential conditionally independent of Check Point, given the precondition for applying Check Point is to apply Security Session? We are searching for an answer to the question of whether the following equality applies p(Check Point, Credential | Security Session) = p(Check Point | Security Session)*p(Credential | Security Session). After looking at the graph, we can see this equality does not apply because p(Check Point, Credential | Security Session) ∝p(Security Session | Credential)*p(Credential)*p(Check Point | Security Session).

   Only one path between Credential and Check Point is not blocked because Security Session is a collider and is in a conditioning set. Patterns Credential and Check Point are not d-separated. Patterns Credential and Check Point are conditionally dependent, given the Security Session can be applied between them.

   Nodes for patterns Credential, Security Session, and Check Point can be left connected because the Credential and Check Point are conditionally dependent, given Security Session can be used between them. Given this conditional dependence, pattern sequence Credential → Security Session → Check Point is expected.

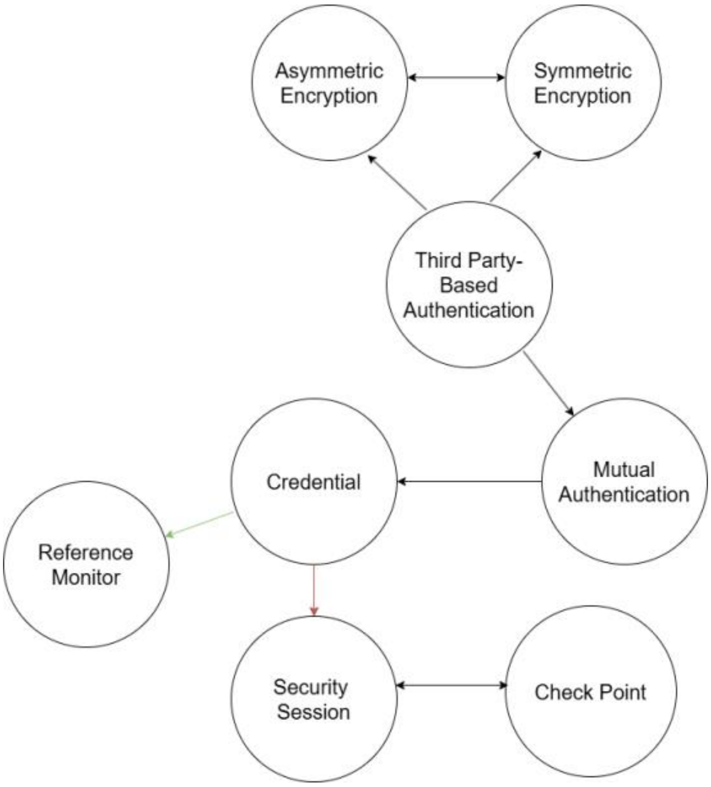
   Conditional dependence is shown with a red line.



2. **Can we leave nodes for patterns Credential, Security Session, a Reference Monitor connected as they are?** We can answer this question through answering a different question:

   Are Reference Monitor and Security Session conditionally independent if the Reference Monitor and Security Session patterns are applicable after the Credential pattern? In other words, we are asking if the following equation applies p(Reference Monitor, Security Session | Credential) = p(Reference Monitor | Credential)*p(Security Session | Credential). After looking at the graph, this equation is true. Because of this, we have simplified the model's component p(Security Session | Credential, Reference Monitor) to p(Security Session | Credential).

   We colored the edge between Credential and Reference Monitor in green to show conditional independence between Reference Monitor and Security Session if Credential is applicable after them.



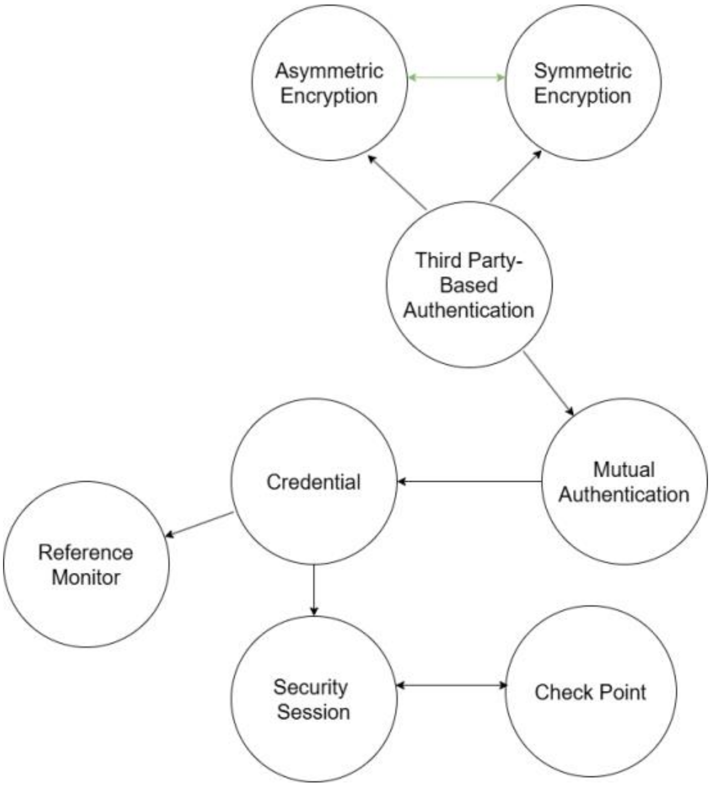
3. **Can we leave nodes for patterns Asymmetric Encryption a Symmetric Encryption connected as they are?** We can answer this question through answering a different question:

   Is Asymmetric Encryption conditionally independent of Symmetric Encryption, given an Asymmetric Encryption or Symmetric Encryption will implement Third Party-Based Authentication? We are searching for an answer to the question of whether the following equality applies p(Asymmetric Encryption, Symmetric Encryption | Third Party-Based Authentication) = p(Asymmetric Encryption | Third Party-Based Authentication)*p(Symmetric Encryption | Third Party-Based Authentication). This equality applies. Asymmetric Encryption and Symmetric Encryption are conditionally independent, given an Asymmetric Encryption or Symmetric Encryption will implement Third Party-Based Authentication.

   There is no collider along the path between Asymmetric Encryption and Symmetric Encryption. Node Third Party-Based Authentication is in a condition of p(Asymmetric Encryption, Symmetric Encryption | Third Party-Based Authentication). The path between Asymmetric Encryption and Symmetric Encryption is blocked. Nodes Asymmetric Encryption and Symmetric Encryption are d-separated by Third Party-Based Authentication. Patterns Asymmetric Encryption and Symmetric Encryption are conditionally independent, given the pattern Asymmetric Encryption or Symmetric Encryption is to be used to implement Third Party-Based Authentication.

   We can color the edge between Asymmetric Encryption and Symmetric Encryption in green to show conditional independence.

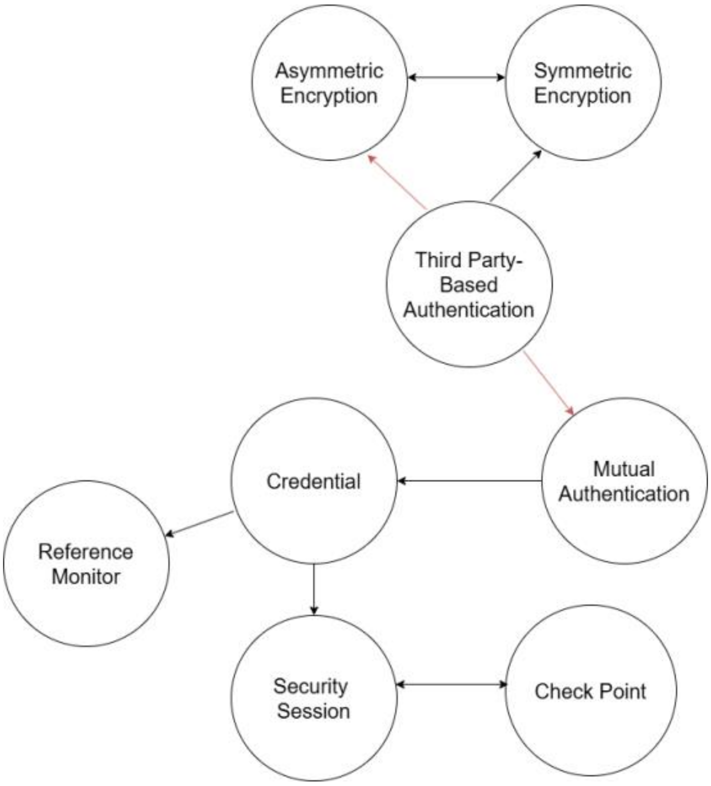
   This conditional independence is important to use the model's component p(Third Party-Based Authentication | Asymmetric Encryption) and p(Third Party-Based Authentication | Symmetric Encryption) later in the article.



4. **Can we leave nodes for patterns Mutual Authentication, Third Party-Based Authentication a Asymmetric Encryption connected as they are?** We can answer this question through answering a different question:

Are Asymmetric Encryption and Third Party-Based Authentication patterns conditionally independent, knowing we can use Mutual Authentication after Third Party-Based Authentication? In other words, we are asking if the following equation applies p(Asymmetric Encryption, Third Party-Based Authentication | Mutual Authentication) =p(Asymmetric Encryption | Mutual Authentication)*p(Third Party-Based Authentication | Mutual Authentication). This equation is not true, and because of that, we can use this conditional dependence to use the model's component p(Mutual Authentication | Third Party-Based Authentication, Asymmetric Encryption).

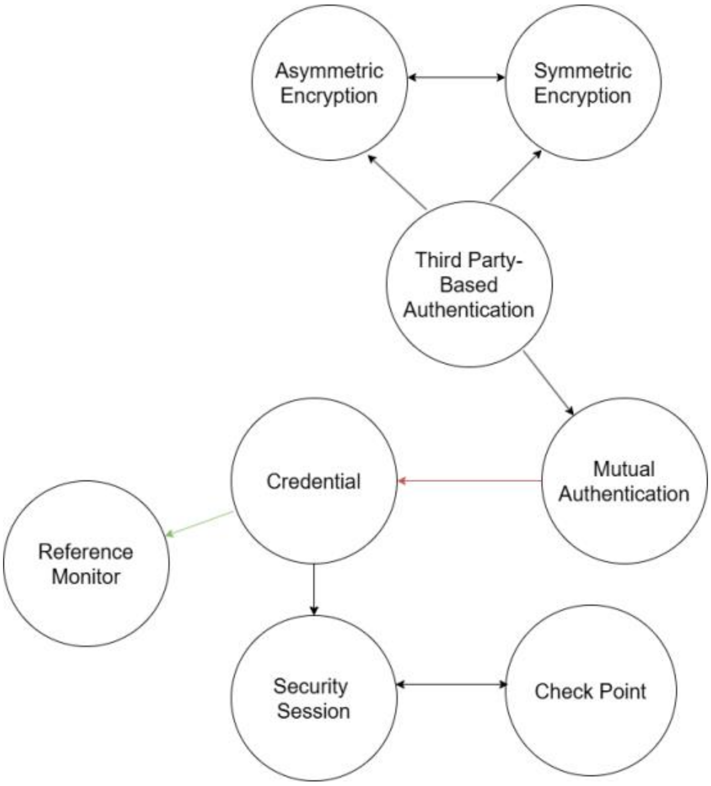
We are displaying this conditional dependence with red color.



5. **Can we leave nodes for patterns Credential a Mutual Authentication spojene?** We can answer this question through answering a different question:

Are Credential and Mutual Authentication conditionally independent, knowing that we can use Reference Monitor after Credential? In other words, we are asking if the following equation applies p(Credential, Mutual Authentication| Reference Monitor) = p(Credential | Reference Monitor)*p(Mutual Authentication | Reference Monitor). This equation is not true.

We also know Reference Monitor and Security Session are conditionally independent, knowing we can use both after Credential. We can use both characteristics to simplify the model's component *p(Credential | Mutual Authentication, Reference Monitor) to p(Credential | Mutual Authentication).*



Simplified Belief network we work with looks like this:

*p(Check Point | Secuity Session) * p(Security Session | Credential) * p(Credential | Mutual Authentication) * p(Mutual Authentication | Third Party-Based Authentication, Asymmetric Encryption) * p(Third Party-Based Authentication | Asymmetric Encryption)*p(Asymmetric Encryption)*