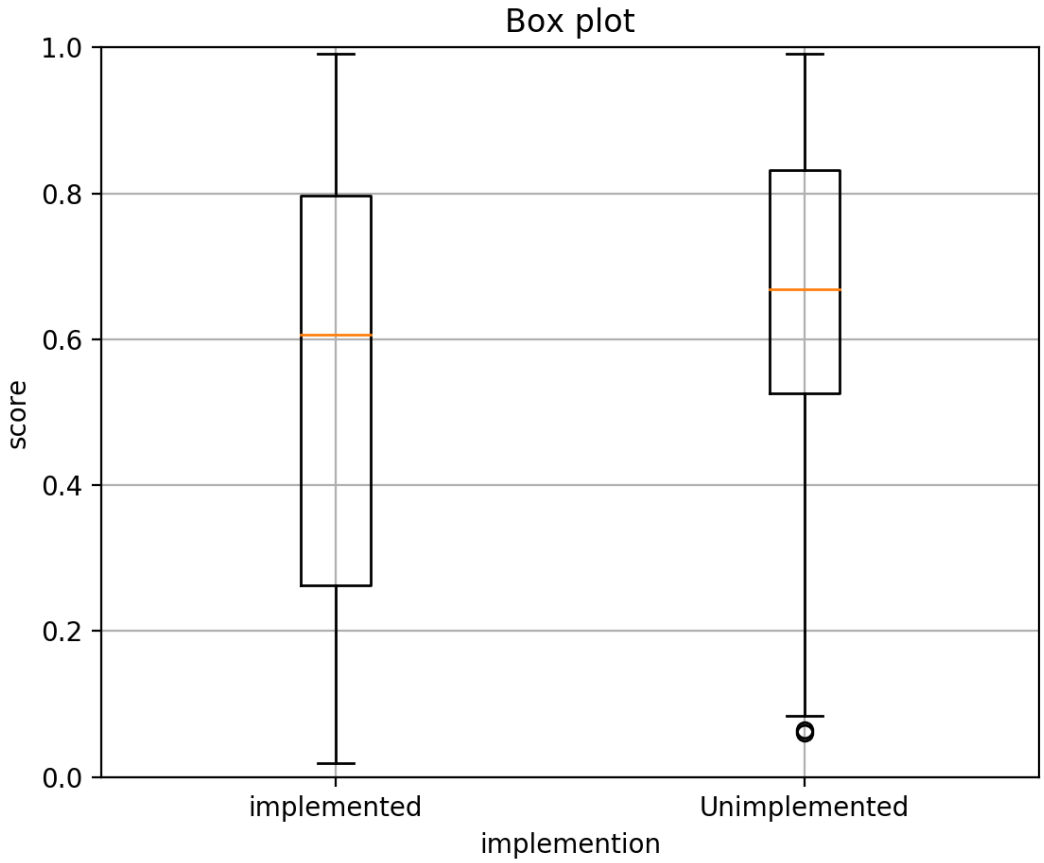


図 6.1: 純正の Cowrie と修正済の Cowrie のスコアリングによる比較

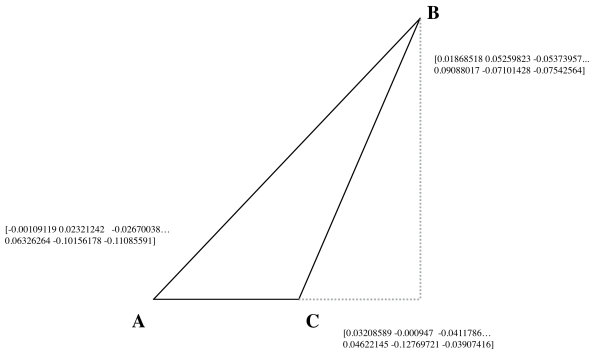
6.2 評価手法

本研究の仮説の検証手法としての評価として，3.2 節で述べた要件に対して評価を行う．予備実験では，素の低対話型 Honeypot よりも，コマンドを拡張した Honeypot の方がコマンドパターンが多く収集できることを示した．本研究では拡張した Honeypot で収集したコマンドログが，どれほど一般的な UNIX ユーザーの実行するコマンド [22] から離れたのかを評価した．

本研究では，以下の三種類の Honeypot を設置する．

1. 広く利用されている SSH の低対話型 Honeypot
2. 実際の Shell には実装されているが，1. の Honeypot で未実装のコマンドを実装した Honeypot
3. 広く利用されている高対話型 Honeypot

本研究の評価として上記の 3 つの Honeypot でのコマンドログの収集したが，高対話型 Honeypot のコマンドログの収集数が極端に少なかったため，今回の評価では純正の低対話型 Honeypot と，修正済の低対話型 Honeypot を比較する形での評価を行なった．高対話型 Honeypot ののコマンドログの収集量が少なかった考察については 6.3 で述べる．



ベクトル空間上において一般ユーザーのコマンドログの文章ベクトルの座標を原点 O とし，素の Honeypot コマンドログの文章ベクトルの座標を A，修正済の Honeypot コマンドログの文章ベクトルの座標を B とした時に，$|\vec{OA}| < |\vec{AB}| < |\vec{OB}|$ であり，なす角 $\angle AOB$ は鋭角である．
したがって，$0 < n$ を満たす n と任意のベクトル $\vec{\alpha}$ を使うと，$\vec{OB}$ は $\vec{OB} = (1+n)\vec{OA} + \vec{\alpha}$ と表すことができる．したがって，修正済の Honeypot のコマンドログは一般ユーザーのコマンドログを始点とすると，素の Honeypot のコマンドログのベクトル方向よりも正の向きに遠くに位置することが分かった．
また，SCDV によって獲得した各々の Honeypot の攻撃ログにおける文章ベクトルを，t-SNE で次元削減することで可視化を行なった結果を図 6.4，図 6.5，図 6.6 に示す．

図 6.4: 修正前と後の honeypot のコマンドログの文章ベクトルの可視化

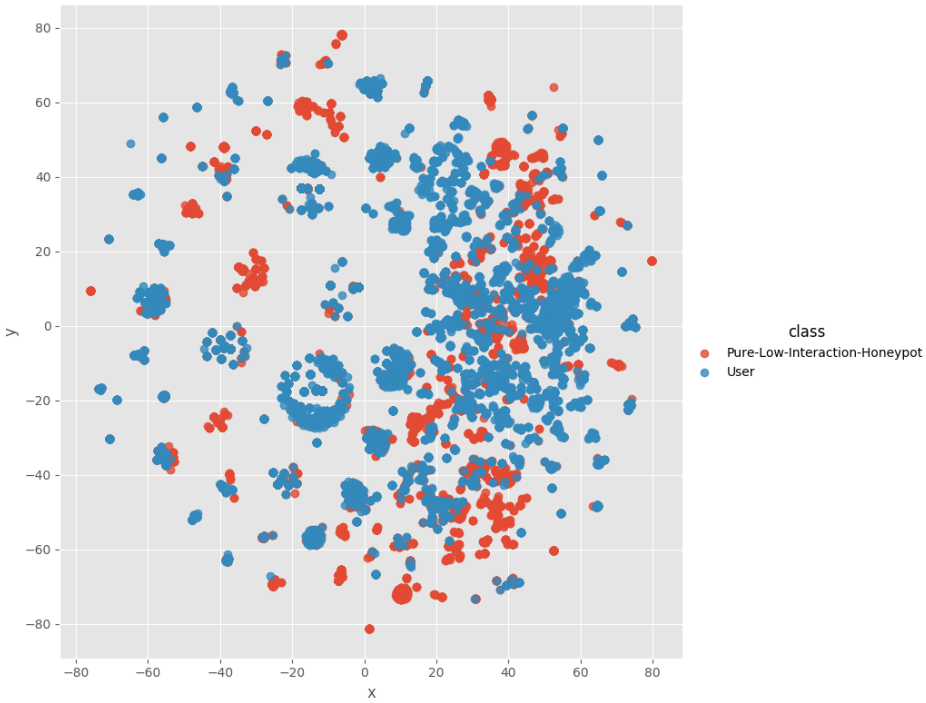


図 6.5: 修正前の honeypot と一般 UNIX ユーザーのコマンドログの文章ベクトルの可視化

図 6.6: 修正後の honeypot と一般 UNIX ユーザーのコマンドログの文章ベクトルの可視化