【領域:】についての重要なプレゼンテーション報告

セッションコード(IS09) セッションタイトル(Security for Cooperative Mobility) プレゼンテーションのタイトル(V2X Security & Privacy: The Current State and ITS Future) 発表者(Andre Weimerskirch, ESCRYPT Inc., USA) 論文番号(1089)	取材担当 三菱電機株式会社 三澤 学

【概要】

「V2X Security & Privacy: The Current State and ITS Future (V2X のセキュリティとプライバシ:現状と ITS の将来)と題された、IS09 Security for Cooperative Mobility セッションの中で ESCRYPT 社 の Andre Weimerskirch 氏が発表した論文である。この発表では、V2X セキュリティの現状と未解決の問題について述べているおり、問題のある機器の検出方法、証明書の失効やその通知の仕方、またそれらを運用するためのセキュリティポリシーの必要性を述べている。

【特徴】

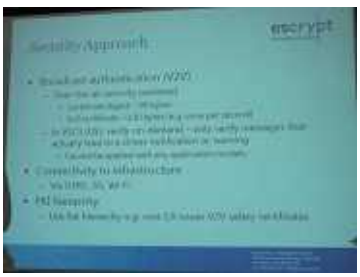
V2X セキュリティの現状と未解決の問題について述べているおり、問題のある機器の検出方法、証明書の失効やその通知の仕方、またそれらを運用するためのセキュリティポリシーの必要性を述べている。

【内容】

本発表では、V2X セキュリティの(1)現状と(2)未解決の問題について述べている。

(1) V2X セキュリティの現状

- 欧米では、V2X セキュリティのプロトコルである IEEE1609.2 の利用を前提としており、このプロトコルでは証明書と署名により送信者の正当性やメッセージの完全性の検証を行う。
- 署名検証は、処理負荷が大きいため、処理負荷を軽減するためのアプローチが検討されている。
  - −Verify-On-Demand*により署名検証の回数を軽減 (CAMP VSC3)。但し他のアプリケーションに適用できるかは不明である。
  - −Root CA が各車両の証明書を発行することで、証明書の検証負荷を軽減する。
- プライバシ保護の観点からは次の運用を検討している。
  - −定期的に証明書を変更する。
  - −証明書自体にプライバシに関わる情報を含めない。

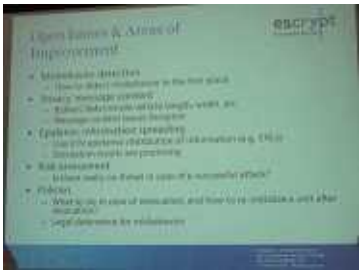


*ドライバに対する注意喚起が必要となるメッセージに対してのみ検証を行う方法。

(2) 未解決の問題

V2X における未解決の問題として次のものを挙げている。

- 問題のある動作、機器を初期段階で検出する方法。
- マルチホップを用いることで CRL を広めることは容易であるが、一方で通信回線が混雑する恐れがあること。
- 欧米では、安全安心のアプリケーションを中心にセキュリティが検討されているが、その他のアプリケーションでのセキュリティの検討が不十分であること。
- 運用(どのような条件で証明書を失効するのか等)に必要なセキュリティポリシーの策定。



【領域:】についての重要なプレゼンテーション報告

セッションコード(IS09) セッションタイトル(Security for Cooperative Mobility)
プレゼンテーションのタイトル(A Generic Public Key Infrastructure for Securing Car-to-X Communication)
発表者(Norbert Bissmeyer, Fraunhofer Institute for Secure Information Technology, Germany)
論文番号(1339)

取材担当
三菱電機株式会社
三澤 学

【概要】

「A Generic Public Key Infrastructure for Securing Car-to-X Communication (C2X のための一般的な PKI)と題された、IS09 Security for Cooperative Mobility セッションの中で Fraunhofer 社の Norbert Bissmeyer 氏が発表した論文である。この発表では、C2C-CC で検討されている、プライバシ保護やセンタとの非-常時接続を考慮した PKI のストラクチャについて述べている。

【特徴】

C2C-CC で検討されている、プライバシ保護やセンタとの非-常時接続を考慮した PKI のストラクチャについて述べている。車は、プライバシ情報を含まない、かる有効期限の短い証明書を複数持つことで、トラッキング等を含めたプライバシ保護を実現すること、証明書の有効期限を短くすることで車は CRL を取得する必要がなく、証明書発行時のみセンタと接続すればよいと提案している。

【内容】

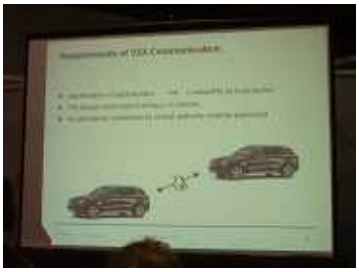
本発表では、C2C-CC で検討されている、プライバシ保護やセンタとの非-常時接続を考慮した PKI のストラクチャについて提案している。

(1) V2X におけるセキュリティ要求

発表では、V2X におけるセキュリティの要件を次のように定めている。

(a) 送信者の正当性を検証できること
(b) 車両、ドライバのプライバシを保護できること
(c) センタと常時接続する必要がないこと

(a)については、IEEE1609.2(PKI)を用いることで実現ができる。
この発表では、(b)、(c)を実現する方法について提案している。



(2) プライバシ保護やセンタとの非-常時接続を考慮した PKI のストラクチャ

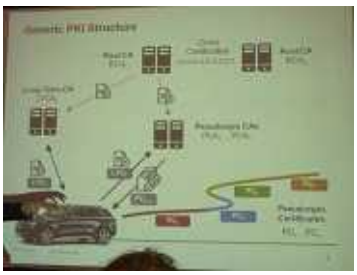
＜提案の概要＞提案のコンセプトは次の通りである。

- 車車間通信で用いる証明書(Pseudonym 証明書)や Pseudonym 証明書の発行要求に使用する証明書(Long-Term 証明書)には、プライバシに関する情報は含めない。
- トラッキング等も防止するため、車は、Pseudonym 証明書を複数持ち、定期的もしくはランダムに変えながら使用する。
- 車に対する CRL の発行は、センタとの常時接続が求められるため、Pseudonym 証明書の有効期限を短くし、Pseudonym 証明書を発行する際に、CA がその車に対して Pseudonym 証明書を発行してよいかを判定する。

＜提案の詳細＞

発表では、このコンセプトを実現するため、先述の Pseudonym 証明書、Long-Term 証明書に加え、Pseudonym CA と Long-Term-CA の導入を提案している。それぞれの役割は次の通りである。

- Pseudonym CA：車車間通信に用いる Pseudonym 証明書を発行する。
- Long-Term-CA：Pseudonym 証明書の発行要求に用いる証明書（Long-Term 証明書）を発行する。



PKI の階層としては、Root CA が、Pseudonym CA、Long-Term-CA の証明書を発行し、Pseudonym CA が Pseudonym 証明書を、Long-Term-CA が Long-Term 証明書を発行するというものになる。

証明書には、プライバシ情報が含まれないため、Pseudonym CA は、車に関する情報を得ることができない。一方、Long-Term-CA は、車や所有者等に関する情報を知った上で Long-Term 証明書を発行する。

Long-Term 証明書の CRL は Pseudonym CA は常に取得し、Pseudonym 証明書の発行要求が合った場合には、Long-Term 証明書の CRL を参照することで、Pseudonym 証明書を発行してよいかを判定できる。

Pseudonym 証明書の有効期限は短いため、車は CRL を取得する必要がなく、センタとの通信は Pseudonym 証明書の発行時に限られる。

なお、一つの車両あたりの Pseudonym 証明書の保有数や、有効期限の長さについては、システムに応じて自由に設定可能とのことであるが、C2C-CC 等で具体的にどのような値を用いるかは今後の検討課題である。