NTTソフトウェア

IETF89報告会
PERPASS-related WG Report

笠松 宏平

2014.4.11

NTT Software Corporation

http://www.ntts.co.jp/

http://www.nttsoft.com/

自己紹介

- 名前: 笠松 宏平 (かさまつ こうへい)
- 所属: NTTソフトウェア
  セキュリティ事業部
- メールアドレス: kasamatsu.kohei@po.ntts.co.jp
- 業務領域
  - IETFでの標準化活動
    - NTT研究所の暗号技術
    - セキュアプロトコルの動向監視

暗号技術の標準化に対する
PERPASSの影響大

- 高機能な楕円曲線 (BN-curves)を投稿中☺
  - draft-kasamatsu-bncurves-01
    - URL: http://tools.ietf.org/html/draft-kasamatsu-bncurves-01

発表の流れ

PM に関連する動向について
IETF88会合からIETF89会合へのアップデート

- 導入
  - Pervasive Monitoring (PM)とは
  - PMの発端であるIETF88の復習
- Pervasive Monitoring対策技術の動向
  - PERPASS Lunch Meeting
  - 各WGに対する検討
  - 今後の動向予想
- IETF89のSTRINT Workshop報告状況

導入

- Pervasive Monitoring (PM)とは
  - 潤沢なリソースを持った組織が行う広範囲な盗聴行為
  - 通信監視プログラム PRISMの運営発覚 (2013/6/6)後, IETF88 (2013/11/3)から議論開始

- IETF88会合の復習
  - Technical Plenariesで次のコンセンサスが取れた
    - PMは攻撃であり, IETFはPMに積極的に対処する
    - **PMを考慮した脅威モデルを検討し, 脅威モデルを考慮してStandards Track Specificationの提案を受け入れるか判断すべき**
    - **認証がない場合でも, 暗号化すべき**
  - PERPASS BoF
    - Handling Pervasive Monitoring in the IETF
    - Technical Plenariesのコンセンサスを受け, IETFで実施する活動や計画について議論された (活発な議論すぎてまとまらず…)

二つを軸に
動向をまとめます

IETF89: Pervasive Monitoring対策技術の動向

脅威モデルとRFCのレビュー

PERPASS

暗号化の推進

プロトコルでの利用促進

UTA　DNSE

強い暗号技術への移行

SAAG　TLS　CFRG

UTA: Using TLS in Applications

PERPASS: Handling Pervasive Monitoring in the IETF

PERPASS (Handling Pervasive Monitoring in the IETF)

- 目的
  - IETFで扱うプロトコルでPervasive Monitoringに対してどのように対処するか議論するための

    non-working group mailing list
- 経緯
  - IETF88
    - BoFが開催
  - IETF89
    - Lunch Meeting 開催
      - 2014年3月3日 (月) 11:30 – 13:00

アジェンダ

- Discuss goals and scope (10 min)
  - Privacy including PM
  - Just PM
- Which effort (10 min)
  - Existing RFC
  - IDs at IETF last call
- Brief look at existing examples of such reviews (20 min)
- A look at possible criteria for Privacy or PM reviews (15 min)
- How to organize the draft review process for maximum benefit. (15 min)
- where to go from here. (10 min)

サマリ (1/2)

- ゴールおよびスコープ
  - ゴール
    - 決定事項
      - PMの観点で**Standards track RFCs**をレビュー＆ドキュメント化
    - 今後の課題
      - I-Dをレビュー対象にするかどうか
  - スコープ
    - Privacyもスコープに含む
      - RFC6973: Privacy Considerations for Internet Protocols がベース
    - PMに関するレビューを優先

サマリ (2/2)

- レビューのための基準作りを進める
  - PMおよびPrivacyのconcern
    - 分類
    - 優先順位づけ
- レビューの進め方
  - Wikiを用いたIssuesの共有
    - http://trac.tools.ietf.org/group/ppm-legacy-review/wiki
  - 議論を行うMLの変更
    - perpass ⇒ ietf-privacy
    - ietf-privacy:
      - http://www.ietf.org/mail-archive/web/ietf-privacy/current/maillist.html

RFC レビュー状況

ppm-legacy-review

Search

Login | About Trac | Preferences | Help/Guide

Wiki | Timeline | Roadmap | Browse Source | View Tickets | Search

wiki: WikiStart

Start Page | Index | History

Welcome to the privacy and pervasive monitoring RFC review page

This page is an anchor for reviews of existing RFCs (not new drafts) for privacy and pervasive monitoring issues.

We use a ticket system for reviews. Select "view tickets" above to see existing reviews or add material to them.

The ten most recently modified tickets are:

Ticket	Summary	Status	Owner	Priority	Component	Modified
#9	RFC 0793 Transmission Control Protocol (TCP) lacks privacy considerations	new	wes@mti-systems.com	major	TSV	34 hours
#8	RFC 1034 and many others: "DNS privacy considerations" work	new	bortzmeyer+ietf@nic.fr	major	INT	11 days
#7	RFC 3912 Whois has no security whatsoever	new	huitema@huitema.net	major	APP	11 days
#6	RFC 4578 DHCP UUID/GUID option for PXE enables client tracking	new	huitema@huitema.net	major	INT	11 days
#5	RFC 4702 DHCP Client FQDN Option enables client tracking	new	huitema@huitema.net	major	INT	11 days
#4	RFC 2132 Host Name option enable client tracking	new	huitema@huitema.net	major	INT	11 days
#3	RFC 4361 Unique client identifier option enables client tracking	new	huitema@huitema.net	major	INT	11 days
#2	RFC 2131 new request may leak previous IP address	new	huitema@huitema.net	major	INT	11 days
~~#1~~	test this	closed		trivial	Unassociated with Area	2 weeks

URL: http://trac.tools.ietf.org/group/ppmlegacy-review/wiki

暗号化を推進する理由 (1/2)

PMによって一般市民の情報も盗聴される
(Passive Attackのコスト < Active Attackのコスト)

潤沢なリソースを持った組織

IETF88, Technical PlenaryのBruce Schneier氏の発表より
(Technical Topic: Introduction)

暗号化を推進する理由 (1/2)

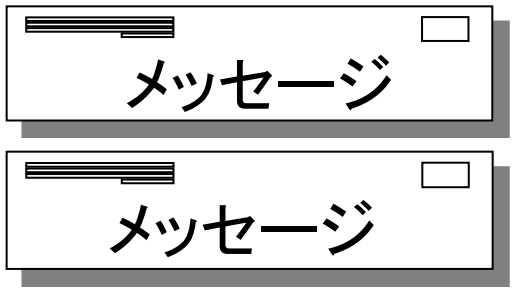
PMによって一般市民の情報も盗聴される
(Passive Attackのコスト < Active Attackのコスト)

一般市民

一般市民

犯罪者

犯罪者

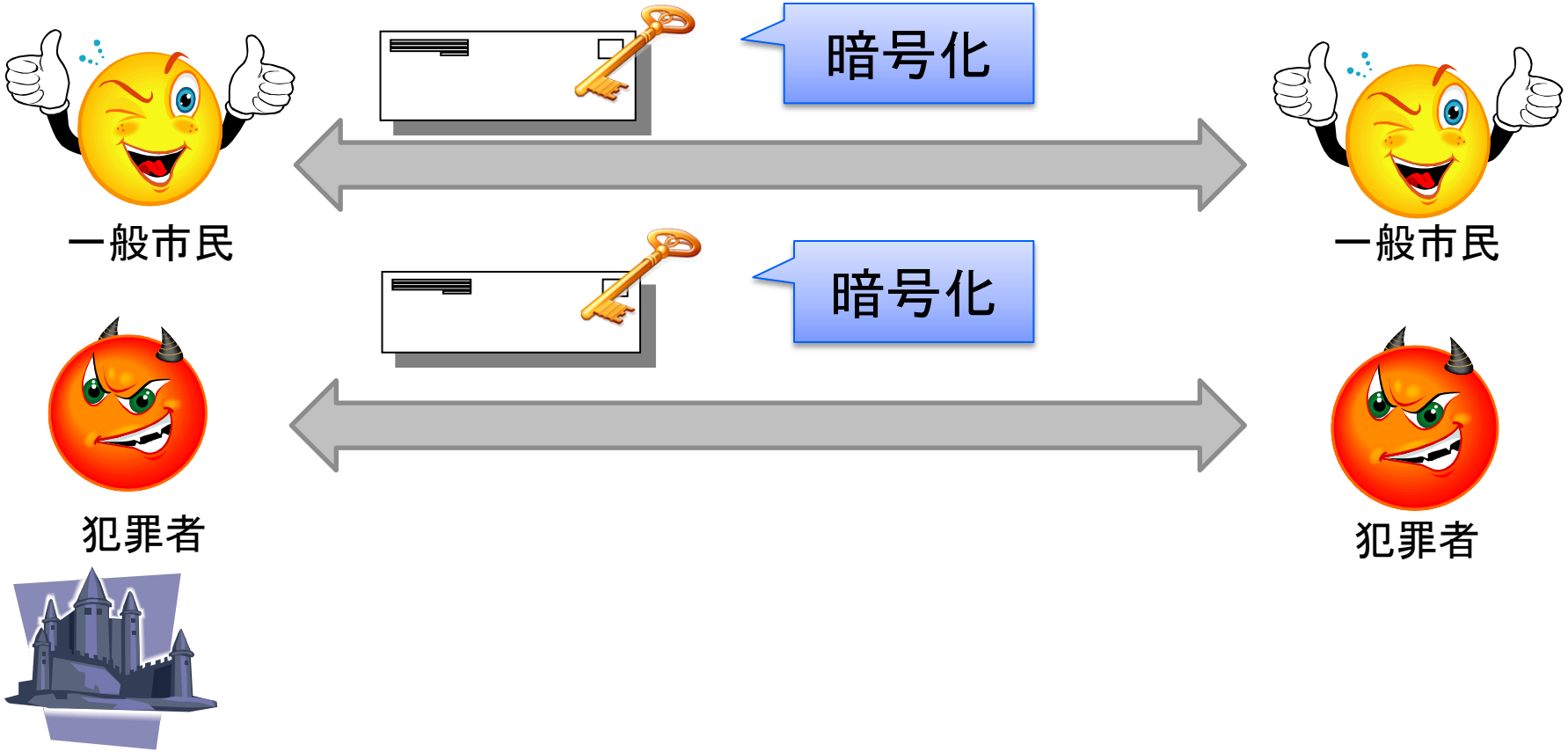


潤沢なリソースを持った組織

IETF88, Technical PlenaryのBruce Schneier氏の発表より
(Technical Topic: Introduction)

暗号化を推進する理由 (2/2)

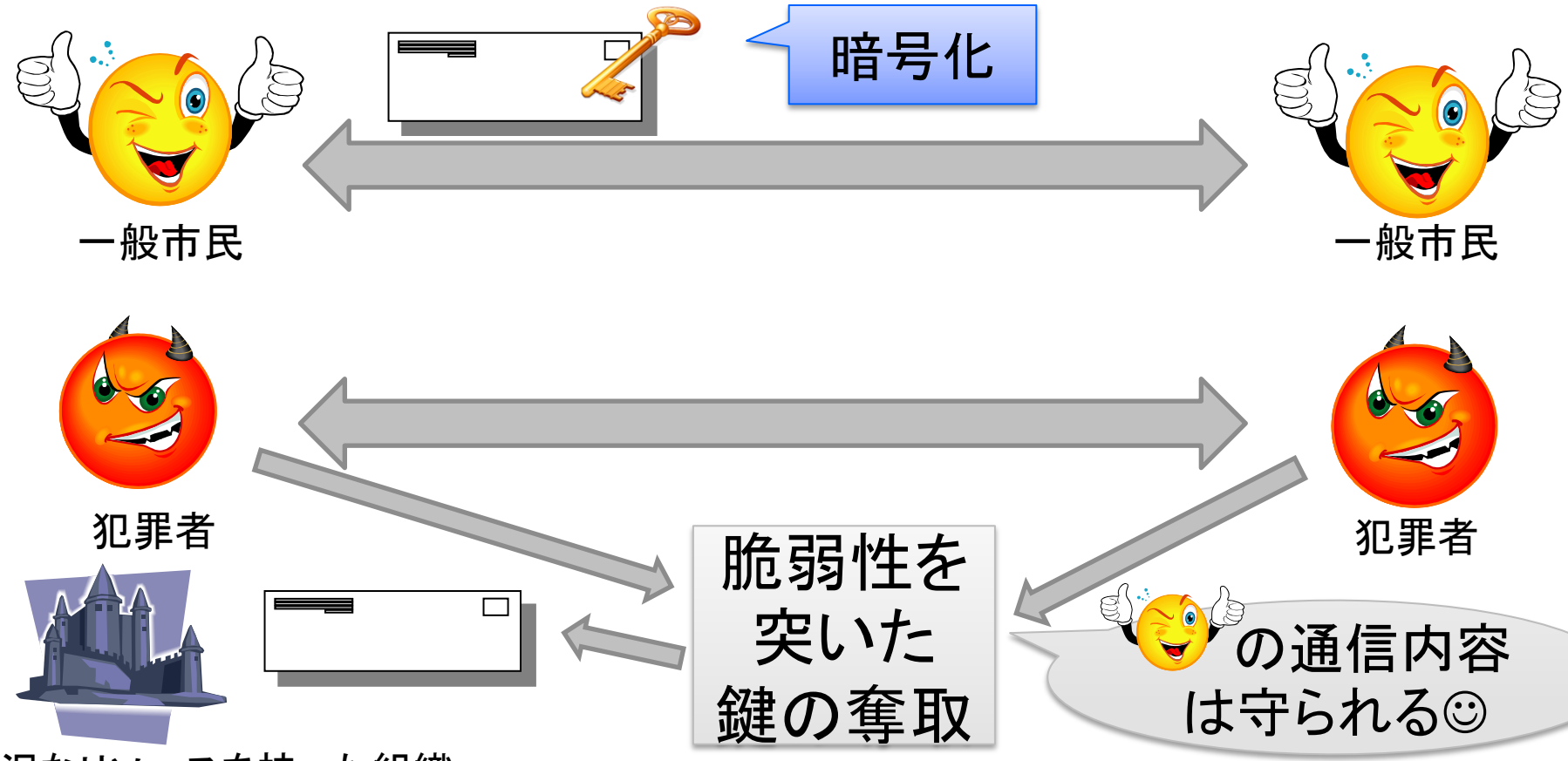
全ての通信を暗号化することでターゲットを絞った盗聴へ
（Passive Attackのコスト > Active Attackのコスト）



IETF88, Technical PlenaryのBruce Schneier氏の発表より(Technical Topic: Introduction)

暗号化を推進する理由 (2/2)

全ての通信を暗号化することでターゲットを絞った盗聴へ
（Passive Attackのコスト > Active Attackのコスト）



IETF88, Technical PlenaryのBruce Schneier氏の発表より(Technical Topic: Introduction)

補足:暗号化を推進する理由(1/2)

- IETF88でのコンセンサスが取れた“**無認証の暗号化**”を説明
  - IETF88 Technical PlenaryでのBruce Schneier氏の講演がベース
  - 「補足:暗号化を推進する理由(2/2) 」に Bruce Schneier氏の発言を抜粋
- 「暗号化を推進する理由」に関する注意事項
  - IETF88時点の考え方をベースに説明を実施
  - 盗聴対象(犯罪者)を発見する方法は講演では説明がされていない
  - PMとしてActive Attackerもスコープに入っている
    - 本報告会の中島氏のSTRINT workshopの講演資料を参照
  - 全ての通信を暗号化することに全ての人が賛成しているワケではない
    - ウィルススキャン等, 暗号化されたトラフィックではできない処理が存在
    - IETF88のTechnical Plenaryではコンセンサスが取れていない
    - IETF89でも結論は出ていない

補足:暗号化を推進する理由(2/2)

IETF88, Technical Plenary, Bruce Schneier氏の講演抜粋

- The goal is to make eavesdropping expensive. That's the way to think of it. **To force the NSA to abandon wholesale collection in favor of targeted collection.** So ubiquitous encryption on the Internet backbone, that will do an enormous amount of good, provide some real security, right, cover traffic for those who need to use encryption. But the more you can encrypt data as it flows around the Internet, the better we'll do.

各WGに対する暗号化の推進

✓各プロトコルに対する検討

初会合

- Using Applications with TLS (UTA)
  - **Over TLSによるアプリケーション間のトラフィックの保護**を増加させることを目的としたWG
    - SMTP, POP, IMAP, XMPP, HTTP1.1, ….
  - 認証なしの暗号化に関する定義 (**Opportunistic Encryption**)についても議論
    - 定義についてコンセンサスは取れていない

初会合

- Encryption of DNS requests for confidentiality (DNSE)
  - DNSのクエリ, レスポンスのデータ保護を目的としたWG

各WGに対する暗号化の推進

✓強い暗号技術への移行

- SAAG
  - IAB Russ Housleyによる暗号技術のagilityのガイドライン策定に関する発表
    - http://tools.ietf.org/html/draft-iab-crypto-alg-agility-00
- CFRG, TLS
  - 新しい楕円曲線の選定 (Non-NIST Approved)
    - Curve25519 vs Brainpool curve vs other
  - Ciphersuitesに対する（Perfect）Forward Secrecyの要請
    - DH, ECDH > RSA

今後の動向予想

- PM対策の観点からRFCに対するレビューの継続
  - 優先順位の高いStandard track RFCsを選定＆レビュー
    - 対象はDNS, DHCP, SIP, SDP, RTCP, RADIUS, Diameterなど
    - すでにDNS, DHCPはレビューが進んでいる
- 暗号技術の推進
  - 各プロトコルに対する検討は範囲を広げながら推進
    - IETF89後, tcpcrypt (Discussion list for adding encryption to TCP) mailing listが開設された.
  - 強い暗号技術への移行も加速
    - **安全な楕円曲線**については7月IETFを待たずに電話会議開催
    - **（Perfect）Forward Secrecy**の需要は**今後も増加傾向**

STRINT Workshopとの関連

脅威モデルとRFCのレビュー

PERPASS*

暗号化の推進

各プロトコルに対するOEの検討

UTA

DNSE

強い暗号技術への移行

SAAG

TLS

CFRG

暗号技術に関する議論
by Orit Levin
- ✓ Opportunistic Encryption,
- ✓ Perfect Forward Secrecy
- ✓ passive attack model

全体のサマリ報告
by Stephen Farrell

Research breakoutの報告
by Kenny Paterson

まとめ

- PERPASSの動向
  - PERPASS lunch meeting
    - Standards Track RFCsをPMの観点でレビュー開始
  - 各WGに対するOEの影響
    - 各プロトコルに対するOEの検討
    - 暗号技術の強化
  - IETF89におけるSTRINT Workshop報告状況
    - SAAG, CFRG, UTA