ヒューマンクリプトに基づく
超ディペンダブル暗号系に関する研究

今井秀樹　　松浦幹太
生産技術研究所

概要

人とコンピュータシステムをセキュリティの面から総合的に最適化するヒューマンクリプトの手法によって，安心感を飛躍的に高めた暗号系を構築すること．とりわけその際，人の立場から見た安全性の検証可能性を重視して，ディペンダビリティのブレークスルーを達成することが本研究の目的である．平成１５年度は，アルゴリズムだけでなくプロトコルレベルの暗号学的評価，応用範囲の拡大，個人だけでなく社会との調和をもつセキュリティとそれによってもたらされるディペンダビリティにまで研究が発展した．

1. はじめに

電子申請，電子投票，電子商取引，コンテンツ流通など，政治，経済，文化活動の多くの局面でネットワークを介してサービスが提供されつつある．そこで当然重要となる情報セキュリティ技術を「人が安心してサービスを利用できる」というディペンダビリティの観点で詳しく考えれば，人とコンピュータやネットワークとの接点がとりわけ問題である．ヒューマンクリプトとはそこに焦点を当てたアプローチであり，狭義には，人とコンピュータやネットワークとの関わりの部分における暗号技術，広義には，このような部分と密接に関連したプロトコルや運用・社会基盤も含めた情報セキュリティ全般である．

本報告では，2.1 節～2.3 節のように分類される３つのアプローチをベースにディペンダブル情報セキュリティ技術を構築した成果を報告する．

2. 研究の経緯と成果

2.1 人間的要素と直接関わる技術

Password-Authenticated Key Exchange

オンライン認証技術に関して，システムが人を認証する技術は活発に研究されてきた．しかし，人がシステムを認証する手段の研究は，不十分であった．そこで本研究では，その不備による脅威に対処すべく，エントロピーの小さな秘密情報（パスワード）に基づいてエントロピーの大きな秘密情報（鍵長の長い秘密鍵）を人とシステムとの間で共有するための研究を行っている．

人が IC カードや PDA のような道具を何も持たない場合の認証手法で最も基本的なパスワードを用いる方法に対しては，様々な攻撃が可能である．中でも大きな脅威であるオフライン辞書攻撃などを実際上不可能とする工夫がなされた暗号学的プロトコルとして，Password-Authenticated Key Exchange (PAKE)がある（図 1）．我々の先駆的研究[1]では評価方法が未成熟であったので，昨年度は評価の完成度を高めた[2],[3].

今年度は，PAKE を，(I)ユーザが複数のサーバと安全に通信でき，(II)脅威発生時の影響を最小限度に抑え，しかも(III)その安全性を暗号学的に評価できる手法 (Leakage-Resilient AKE: LR-AKE)へと拡張することに成功した[i],[ii]．従来は，サーバに保存されている秘密情報が漏洩するとその影響が他のサーバにも及ぶ，という問題点があったが，提案方式ではこれを克服した．

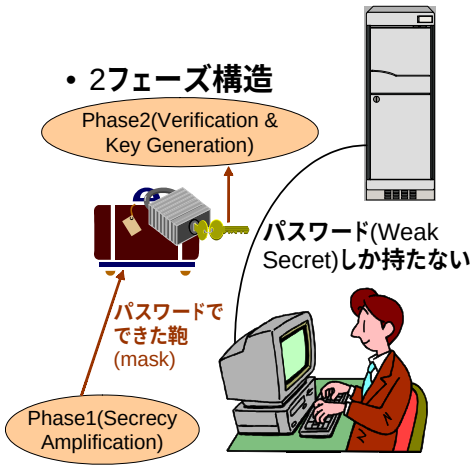

図 1：PAKE の概観

パーソナルエントロピー（バイオメトリクス情報）を利用した鍵生成および鍵更新方式

バイオメトリクス技術を利用した情報セキュリティの研究報告は多数あるが，大部分は単なる個人認証への応用である．これに対して近年，バイオメトリクス情報から公開鍵暗号系における秘密鍵を生成する方法がいくつか提案されている[4]．しかし，（１）得られる秘密鍵のビット長が短い（40bit 程度），（２）指紋のように固定的なバイオメトリクス情報を利用すると運用が難しい，といった問題が存在し，結局適当な長さの乱数がさらに必要になっていた．我々は昨年度，この問題を解決するために，パーソナルエントロピー，具体的には動的な手書き文字情報を利用する方法を考案した[5],[6],[7]．その手法では，手書き文字情報採取機器を用いて，利用者にある決まったパターンの文字・記号などを入力してもらう．そして，入力された文字の筆跡情報に加えて，筆圧情報，さらにはペンの傾き情報をも利用し，長いビット長(160bit 程度)の秘密鍵を生成することに成功した．また，従来の個人認証技術で広く用いられてきたテンプレート情報（認証フェーズで照合に利用する情報）は，その漏洩がプライバシー問題に直結している．我々の手法では，テンプレート情報を一切作成しないので，このような問題点も考慮する必要がない．そして，自分のバイオメトリクス情報を利用して秘密鍵を生成しているので，既存の公開鍵基盤（PKI : Public Key Infrastructure）と比較しても，本人と秘密鍵とのつながりがより緊密である．さらにまた昨年度は，同技術を利用して PKI 用 IC カードの対面取引における本人確認の安全性が保証されれば，PKI の秘密鍵漏洩後も本来の所有者が経済的不利益を被らないようなセキュリティプロトコルと運用方式を構成できることも示した[8]．

そして今年度は，提案方式の安全性に関する定量的評価に成功した[iii],[iv]．具体的には，バイオメトリクスから生成される秘密情報の複雑さを，情報量（エントロピー）を利用して評価した．

本プロジェクトでは検証可能性を重視しているので，我々はバイオメトリクスを評価可能な枠組みで情報セキュリティ分野に適用するための新たな暗号理論的概念[7]を提案した．現在の公開鍵暗号系において，秘密鍵漏洩は，秘密鍵所有者（正当なユーザ）にとって，もっとも重大な脅威の一つである．この鍵漏洩問題に対処する従来の復号用秘密鍵更新手法[3], [4]のいずれも，信頼できるストレージ機器を仮定していた．そのような機器が攻撃を受けて秘密情報が漏洩すると安全性が低下してしまうことは明らかである．われわれはこの問題を排除した「バイオメトリクス情報を利用した鍵更新方式 (bio-key-insulated encryption scheme)」を提案した．その方式[7]では，鍵漏洩が他の期間の安全性に影響を与えない．

今年度は，特に実装方式設計開発とそのプロトコル評価を行い，次の３点を明らかにした．

1. バイオメトリクス秘密鍵 K_{bio} が漏洩しない場合，ユーザの復号用秘密鍵がある閾値以上漏洩しない限り，すべての暗号文が解読されることはない．
2. たとえ K_{bio} が漏洩したとしても，ユーザの復号用秘密鍵が漏洩しない間は，暗号文が解読されることはない．
3. K_{bio} が漏洩し，さらにある期間($t = i$)のユーザの復号用秘密鍵が漏洩しても，それ以前の暗号文($t < i$)が解読されることはない．

こうして，提案手法は従来方式では達成できなかった鍵漏洩耐性を有することが検証できた．

2.2 システム構築技術と事後解決技術

ネットワークセキュリティで人が関与する重要なシステムの１つは，侵入検知システム(IDS)である．単独の IDS には，出力される膨大な量のアラートを容易には有効利用できないという限界がある．本研究では，全国の拠点に配置した多数の IDS のアラートログをデータマイニングで系統的に分析した[v]．その結果，オフラインで管理者に有効な知識（前述の限界を改善する知識）を提供できることを実証した．IDS は管理者も含めて１つのシステムと見るべきであること，および，広域協調が運用面のセキュリティ向上に役立つことを実証した啓蒙的意義が大きく，Telecom-ISAC における議論にも影響を与えると考えられる．

このように，管理者と相互に補助し合うセキュリティ技術開発も，本プロジェクトの特徴的な成果である．この視点は，ある暗号処理を施す際に必ず所望の必須処理を施す（例えば，あるデータベースの暗号化データを更新すると，暗号化だけでなく必ず証明書付きの署名を付し，かつ，セキュア・タイムスタンプサーバに送信する等）ことを保証するシステムの開発にも反映させた[vi]．

トラストメトリックとプライバシー保護に関わる研究

公開鍵暗号系のためのインフラは，信頼の形態に応じて大きく PKI モデルと PGP メールのような Web of Trust モデルに二分される．トラストメトリックスとは，特に Web of Trust モデルにおける，相手やその鍵に対する信頼度の定量化方法を探究する研究である．我々は近年，とりわけ人の協力が必要な Web of Trust モデルにおいて，協力者の信頼性が必ずしも高くない場合に頑健な信頼度計算方式を研究している[11]. 昨年度のプロジェクトでは，その方式に協力者のプライバシー保護の概念を導入し[12], 協力を得やすくするという社会心理学的にも有効なシステムを考案した．さらに，発表論文[13]では，協力内容に関する検算機能を加えるという拡張を行った．これにより，個人情報を保護しながらもより確かな計算結果を得られることが可能となった.

今年度は，基盤となるネットワークに対して汎用性を持たせるために，ネットワーク構造が静的でない場合を仮定した[vii]．具体的には，既知の匿名通信方式である Onion routing と提案方式である Sliced Onion との比較を行った．そして，ネットワーク構成を変化させた場合のメッセージ到達確率，およびメッセージを転送するノードが結託した場合に匿名性が暴かれる可能性について暗号学的考察･評価を行い, 有効性を検証した[viii].

また，紙面の関係で詳細は割愛するが，ユビキタスシステムで近年重要視されている RFID のセキュリティに関して，その動作モード切替を巧みに利用したプライバシー保護技術の基礎的成果を出している[ix].

2.3 社会的要素

情報セキュリティ技術が実世界で有効に機能して十分なディペンダビリティを提供するためには，人の集合体である社会が提供する迅速なイノベーションが肝要である．本研究では，文献計量分析と特許調査，さらにそれらの相関分析に基づき，イノベーションを支える社会基盤の１つである産学連携の現況と課題を明らかにした．すなわち，分野の成長に見合った連携拡大はなく，しかもその飽和レベルが明らかに低い．一方で，わが国の情報セキュリティ分野に有効な知的成果共有の場が存在すること，および，突出して有効に機能している研究ネットワークが存在することも実証された[x]．これらの強みを活かして飽和レベルを上げるためには，異種セクタ間の同化を求めるのではなく異質なものに橋を架けるような施策が重要であることを, 併せて論証した[xi],[xii].

3. むすび

以上のように，ヒューマンクリプトのアプローチで高度なディペンダビリティを達成する要素技術およびプロトコル研究で平成 14 年度に築いた基礎を，平成 15 年度は主に(I)プロトコルレベルの暗号学的評価, (II)応用範囲の拡大, (III)個人だけでなく社会との調和の観点で大きく発展させた．重要なことは，暗号学的評価や学際情報学的実証研究によって,「検証可能性を重視する」というプロジェクトのポリシーを貫徹したことである.

参考文献

[1] K. Kobara and H. Imai, ``Pretty simple password authenticated key exchange protocol,'' In 24th Symp. Inform. Theory and Its Applications, (SITA '01), pages 561—563, December 2001.

[2] K. Kobara and H. Imai. ``Pretty-simple password-authenticated key-exchange protocol proven to be secure in the standard model". IEICE Trans., E85-A(10):2229--2237, October 2002.

[3] K. Kobara and H. Imai. ``PAKE vs. password-based authentications in wireless standards". In Proc. of The 3rd International Workshop on ITS Telecommunications, pp.135--138, 2002.

[4] F. Monrose, M.K.Reiter, Q.Li and S.Wetzel, ``Cryptographic key generation from voice," In Proceedings of the 2001 IEEE Symposium on Security and Privacy, May 2001.

[5] 赤尾雅人, 今井秀樹, ``バイオメトリックスを用いた暗号鍵生成,'' 第 25 回情報理論とその応用シンポジウム, (SITA '02), pages 339—342, December, 2002.

[6] 赤尾雅人, 山中晋爾, 花岡悟一郎, 今井秀樹, ``ペン入力を用いた暗号鍵生成手法,'' 2003 年 暗号と情報セキュリティシンポジウム(SCIS2003), pages 299—304, January, 2003

[7] 山中晋爾, 花岡悟一郎, 赤尾雅人, 花岡裕都子, 今井秀樹, ``バイオメトリックスを用いた鍵更新方式ーバイオメトリックスの効果的利用法ー," 2003 年 暗号と情報セキュリティシンポジウ

ム(SCIS2003), pages 375--380, 2003.
[8] 小森旭, 花岡悟一郎, 松浦幹太, 須藤修: ``署名鍵漏洩問題における電子証拠生成技術について", 2003 年暗号と情報セキュリティシンポジウム(SCIS2003)予稿集, Vol.II, pp.983-988, 2003.
[9] Boneh and M. Franklin, ``Identity-based encryption from the weil pairing, " CRYPTO'01, LNCS vol. 2139, Springer-Verlag, 2001.
[10] Y. Dodis, J. Katz, S. Xu and M. Yung. ``Key-insulated public key cryptosystems," EUROCRYPT'02, LNCS vol. 2332, Springer-Verlag, 2002.
[11] 田村 仁, 松浦幹太, 今井秀樹: ``審査能力について考慮した多次元トラストメトリックに関する考察", 2002 年暗号と情報セキュリティシンポジウム(SCIS2002)予稿集, Vol.I, pp.103-108, Jan. 2002.
[12] J. Tamura, K. Kobara and H. Imai, ``A Proposal of Trust-Metrics considering Privacy," 第 25 回情報理論とその応用シンポジウム, (SITA '02), pages 135—138, December, 2002.
[13] 田村仁, 古原和邦, 今井秀樹, ``個人情報の保護を考慮したトラストメトリックスの拡張および考察," 2003 年 暗号と情報セキュリティシンポジウム(SCIS2003), pages 995—1000, 2003.

発表文献

[i] SeongHan Shin, Kazukuni Kobara, Hideki Imai, ``Leakage-Resilient Authenticated Key Establishment Protocols," Proc. of the ASIACRYPT 2003. LNCS 2894. pp.155-172. Springer-Verlag, (2003-12)
[ii] SeongHan Shin, Kazukuni Kobara, Hideki Imai, ``A New Password-based Authentication Protocol," Proc. of the Computer Security Symposium 2003 (CSS'03), IPSJ Symposium Series vol. 2003, No.15, pp.7-12 (2003-10)
[iii] Masato Akao, Shinji Yamanaka, Goichiro Hanaoka and Hideki Imai, ``On Evaluating the Entropy of Graphical Passwords," 第 26 回情報理論とその応用シンポジウム(SITA2003)予稿集, vol.II, pp.517-520, (2003-12)
[iv] Masato Akao, Shinji Yamanaka, Goichiro Hanaoka, Hideki Imai, ``A Simple Construction of Biometric-Based Key Generation Schemes," Proc. of the Symposium on Cryptography and Information Security (SCIS'04), pp.821-826 (2004-01)
[v] 田村研輔, 松浦幹太, 今井秀樹, ``データマイニングを用いた IDS ログ分析結果の活用," 2004 年暗号と情報セキュリティシンポジウム予稿集, pp.1155-1160, (2004-01)
[vi] Manabu Ando, Kanta Matsuura, Michiharu Kudo and Akira Baba, "An Architecture of a Secure Database for Networked Collaborative Activities," Proc. Of 5th International Conference on Enterprise Information Systems, ICEIS Press, Vol.I, pp.3-10 (2003-04)
[vii] Jin Tamura, Kazukuni Kobara, and Hideki Imai, ''A new anonymous routing scheme and its aptitude for ad-hoc networks,'' 第 26 回情報理論とその応用シンポジウム(SITA2003)予稿集, vol.II, pp.329-332, (2003-12)
[viii] Jin Tamura, Kazukuni Kobara, Hideki Imai, and Ramjee Prasad, "Application of Trust-Metrics for Evaluating Performance System in Ad-hoc Networks with Privacy," Proc. IEEE Wireless Communication and Networking Conference (to appear in March 2004)
[ix] Dingzhe Liu, Kazukuni Kobara and Hideki Imai, "Pretty-Simple Privacy Enhanced RFID and Its Application," Proc. Symposium on Cryptography and Information Security (SCIS'04), pp.707-712 (2004-01)
[x] Ken Ebato, Kenneth Pechter and Kanta Matsuura, "University-Industry Research Collaboration in the Information Security Field in Japan," Proc. 2003 IEEE International Engineering Management Conference (IEMC-2003) (2003-11)
[xi] 江波戸謙, 松浦幹太, "情報セキュリティ分野における産学連携の状況," Network Security Forum 2003 (2003-10)
[xii] 江波戸謙, 松浦幹太, "情報セキュリティ分野における産学連携研究," 2004 年暗号と情報セキュリティ・シンポジウム(SCIS2004)予稿集, Vol.I, pp.13-18 (2004-1)

受賞

[I]CSS2003 学生論文賞 (発表文献[ii]に対して)
[II] NSF2003 セキュリティ論文佳作(発表文献[xi]に対して)
[III] K. Kobara and H. Imai, "Pretty-Simple Password-Authenticated Key Exchange Under Standard Assumptions," 暗号と情報セキュリティシンポジウム 20 周年記念賞 (2003-10)

安全なソフトウェア基盤の構築

米澤 明憲
情報理工学系研究科 コンピュータ科学専攻

概 要

現代の計算機システムにおいて、不正アクセスによる個人情報流出、サービス拒否攻撃による業務妨害、金融機関のシステム障害、個人用計算機の不安定さといった問題は、ほぼすべてソフトウェアの欠陥が原因である。我々は、そのような欠陥を防止しやすい、安全なプログラミング言語等の技術について研究を推進している。本年度は、安全な C 言語処理系、ユーザプログラムをカーネルモードで実行可能な Linux、移動可能なファイアウォール、移動コードを実現するための言語およびミドルウェア、動的型付き言語のメモリ管理を効率化する手法、リファレンスモニタの実装技術に関して研究成果を得た。

1 はじめに

現代の計算機システムにおいて、不正アクセスによる個人情報流出、サービス拒否攻撃による業務妨害、金融機関のシステム障害、個人用計算機の不安定さといった問題は、ほぼすべてソフトウェアの欠陥が原因である。我々は、そのような欠陥を防止しやすい、安全なプログラミング言語等の技術について研究を推進している。特に、ML のような現代的な言語を様々な分野に適用するだけでなく、C, Java, Perl といった産業界で定着している古典的な言語や、移動コードの利用を強く意識した先進的な言語についても、最新の理論を応用するための研究・開発を行っている。それと並行して、オペレーティングシステムのカーネルやミドルウェア等のシステムソフトウェアを安全かつ効率的に実行する方式や、ネットワークを通じた攻撃から計算機を守るための方式の研究・開発も行っている。本年度の主要な成果を以下に挙げる。

2 本年度の成果

2.1 安全な C 言語処理系のためのインタフェース記述言語

バッファ溢れ等のセキュリティホールを悪用する攻撃を防止するための、安全な C 言語処理系の研究・開発を進めた。安全な C 言語処理系はディペンダブルなシステムを作る用途に大変有用である。対外的には、安全な C 言語処理系のためのインタフェース記述言語についての研究に関する論文を国際会議 [6] および国内の会議 [8] で発表した。その論文では、外部のソフトウェアと安全な C 言語処理系との相互運用性を向上するためのインターフェース記述言語 (IDL) の設計・開発について述べられている。プログラマは IDL によってオペレーティングシステムのシステムコールや標準ライブラリ関数との相互運用に関する仕様を記述する。IDL の処理系はその仕様にしたがい、データ表現の変換や事前条件の検査を行うコード (stub) を半自動的に生成する。この IDL はメールサーバ (sendmail ないし qmail) や Web サーバ (apache) といった

大規模なアプリケーションプログラムを安全なC言語処理系で処理して実行するための基盤となる仕組みである。上記の論文中ではIDLの処理系の性能評価を行った結果も報告されている。

2.2 我々の安全なC言語処理系による攻撃防御の実証実験

安全なC言語処理系が攻撃を効果的に防御することを示す実証実験を行った。実験では広く普及しているメールサーバソフトウェアであるsendmailを用いた。まず、sendmail 8.11.0からsendmail 8.11.5までに実在した脆弱性を利用してsendmailを乗っ取る攻撃コードを記述した。その攻撃コードはメモリアクセスの誤りを巧妙に悪用するものであり、スタックフレームに印をつけるだけのような単純なバッファ溢れ攻撃対策では防御できない。次に、脆弱性を有する部分のコードを切り出し、既存のC言語処理系と安全なC言語処理系でコンパイルして二つのバージョンのプログラムを作成した。既存のC言語処理系によって作られたプログラムでは、上記の攻撃コードによる乗っ取りが成功し、攻撃者が危険な操作を実行することができた。一方、我々の安全なC言語処理系によって作られたプログラムは攻撃コードによる乗っ取りを許さなかった。

2.3 ユーザプログラムをカーネルモードで実行可能なLinux

型検査等の実行前検証により安全性が事前に保証されているユーザプログラムを、カーネルモードで実行できるLinux（オープンソースのUNIXの一種）の構築方式等についての研究成果を国際会議で発表した[2]。この方式では、一般にハードウェアによる実行時検査の大半が不要となり、システムコールのオーバーヘッドが大幅に軽減する。基礎的な実験によれば、システムコール自体にかかるオーバーヘッドは、約1ミリ秒から30ナノ秒程度に減少した。これにより、データベースやネットワークサーバといった、入出力の頻繁なアプリケーションを高速化できる。本年度は、大規模なプログラムを用いて性能評価やシステムの最適化を行うことに注力した。その結果、多くの有用な実験データを収集することができ、その一部は上記の論文に反映されている。大規模な実験を行うためには標準ライブラリの実装が必要であったが、その問題は既存の標準ライブラリを少ない手間で我々のLinux用に移植するための方式を発見・考案することにより解決した。本研究はディペンダブルなオペレーティングシステムを構築するための基盤となるものである。

2.4 移動可能なファイアウォール

DDoS攻撃からサーバを防御するMoving Firewallシステムについての研究を行い、そのシステムの設計･実装･評価および複数ISP間の導入方式についての論文を国際会議で発表した[1]。サーバがDDoS攻撃を受けた際には、Moving Firewallができるだけ攻撃元の近くまで遡って攻撃トラフィックを局所的に閉じ込める。被害サーバ側で攻撃パケットを遮断する従来の「点」での防御方法に比べて、インターネットを流れる攻撃パケットの帯域を全体の「面」で制限することで攻撃被害を局所化する利点をもつ。今年度は、実際の日常業務に利用されている計算機サーバの通信トラフィックを収集し、DDoS攻撃などの不正通信トラフィックを複数回にわたり発見し、それの分析を行った。実世界のサーバに対する実際の攻撃の挙動データを収集したことは、今後ネットワーク攻撃に対するディペンダブルな防御システムの研究をさらに発展させていく上で大きな価値がある。