2011 年 11 月 22 日

博士学位論文審査報告書

大学名	早稲田大学
研究科名	人間科学研究科
申請者氏名	PARK Jong Hyuk（パク ジョンヒョク）
学位の種類	博士（人間科学）
論文題目	HUC-HISF: A Hybrid Intelligent Security Framework for Human-Centric Ubiquitous Computing 人間中心のユビキタスコンピューティングのためのハイブリッド・インテリジェント・セキュリティ・フレームワーク
論文審査員	主査　早稲田大学教授　金　群　博士（工学）（日本大学） 副査　早稲田大学教授　永岡　慶三　工学博士（慶應義塾大学） 副査　早稲田大学准教授　菊池　英明　博士（情報科学）（早稲田大学） 副査　早稲田大学教授　西村　昭治 副査　会津大学上級准教授　Vitaly Klyuev　物理学および数学博士（レニングラード大学）

近年、ユビキタスコンピューティングや人間中心のコンピューティングなど新しいコンピューティングパラダイムは、コンピュータとネットワーク技術の急速な進歩によって大変前途有望なものだと大きく期待されている。ユビキタスと人間中心のコンピューティング環境の統合によって、いつでもどこでも便利で快適な人間中心のサービスを提供することが可能となる。しかし、このような新しいコンピューティング環境においては、従来のコンピューティング環境に比べてセキュリティ上の脅威にさらされる可能性がより大きい。従来のコンピューティング環境内には存在しなかったより多くの脅威があらわれ、とくに人間に近いネットワーク環境において、さまざまな攻撃によって、個人のプライバシーが危険にさらされる。例えば、ユビキタスヘルスシステムにおける個人の健康情報、スマートホームにおける個人の生活情報などがハッキングされる可能性があり、それによって大きな問題を引き起こすこともありえる。こういったことを防ぐためには、人間中心のユビキタスコンピューティング環境に適した知的でダイナミックなセキュリティフレームワークが求められる。

本研究は、人間中心のユビキタスコンピューティング環境に対応したセキュリティを最大化することを目指して、人間中心のユビキタスコンピューティングのためのハイブリッド･インテリジェント･セキュリティ･フレームワーク (Hybrid Intelligent Security Framework for Human-centric Ubiquitous Computing , HUC-HISF)を提案するものである。

まず、提案のセキュリティフレームワークは、リソースに制約のあるアプリケーション（例えば、廉価な RFID タグやセンサー）におけるセキュリティを確保するための軽量暗号化アルゴリズムを提供し、ユビキタス・モバイル・デバイスといったリソースに制約のある環境においてもソフトウェアとハードウェアの性能向上をはかる。

次に、提案のセキュリティフレームワークは、人間中心のユビキタスコンピューティングのためのセキュリティプロトコルの改善を行っている。具体的には、

- ワイヤレス・モバイル・ネットワーク環境における高速で安全なハンドオーバを実現するためのセッション・キー・ディストリビューション・メカニズム (Session Key Distribution Mechanism)を提案している。このメカニズムはストリーム・コントロール・トランスミッション・プロトコル (Stream Control Transmission Protocol)に基づいて開発され、それによってモバイルノードが接続を切断することなく能動的に IP アドレスを変えることができるようになる。
- セキュリティが強化されたキー・リカバリー・プロトコル (Security-Enhanced Key Recovery Protocol)およびプライバシーが強化されたキー・リカバリー・プロトコル (Privacy-Enhanced Key Recovery Protocol)を提案している。これらのプロトコルはユーザのロケーションに関するプライバシーを保護するために改善されたものである。
- コントラクト・ネットワーク・プロトコル (Contract Network Protocol, CNP)に基づいたセキュリティ・シミュレーション・モデル (Security Simulation Model)を提案し、ネットワークへの不正侵入を効果的に検出するための汎用シミュレーション環境を設計し、構築している。

また、本研究で提案しているセキュリティフレームワークは、人間中心のユビキタスコンピューティングのための動的ヒューマンーコンテキスト・ロール・ベース・アクセス・メカニズム (Dynamic Human-Context Role Based Access Control Mechanism)を提供し、時空間情報などヒューマンーコンテキストを取り入れることによって既存の手法を大きく改善することができた。

本論文では、さらに、提案のセキュリティフレームワークが人間中心のユビキタスコンピューティングにおけるサーベイランス・サービスやモバイル IPTV サービスに適用することが可能であることを示すとともに、本研究で提案しているセキュリティフレームワークの有効性を検証するためのシミュレーション環境を構築し、パフォーマンスとセキュリティの両側面からシミュレーションと分析を行っている。

本研究で提案している人間中心のユビキタスコンピューティングのためのハイブリッド・インテリジェント・セキュリティ・フレームワークは、ヒューマン・ファクターや人間的な側面を考慮しながら、ワイヤレス・モバイル・ネットワーキング環境に応じたセキュリティを最大限に確保するためのプロトコル、アルゴリズム、メカニズムを含む統合パッケージを提供することが期待できる。

なお、本論文（一部を含む）が掲載された主な学術論文は以下の通りである。

[1] J.H. Park: “Privacy-Enhanced Key Recovery in Mobile Communication Environments,” The Journal of Supercomputing (Springer), Vol.54, No.1, pp.82-93 (Oct. 2010).

[2] J.H. Park: “Subscriber Authentication Technology of AAA Mechanism for Mobile IPTV Service Offer,” Telecommunication Systems (Springer), Vol.45, No.1, pp.37-45 (Sep. 2010).

[3] J.H. Park and Q. Jin: “Effective Session Key Distribution for Secure Fast Handover in Mobile Networks,” Telecommunication Systems (Springer), Vol.44, No.1-2, pp.97-107 (June 2010).

[4] J.H. Park: “Security Analysis of mCrypton Proper to Low-cost Ubiquitous Computing Devices and Applications,” International Journal of Communication Systems (Wiley), Vol.22, No.6, pp.959-969 (Aug. 2009).

[5] J.H. Park, S.J. Lee, J.G. Lim and L.T. Yang: “U-HMS: Hybrid System for Secure Intelligent Multimedia Data Services in Ubi-Home,” Journal of Intelligent Manufacturing (Springer), Vol.20, No.3, pp.337-346 (June 2009).

[6] J.H. Park: “USF-PAS: Study on Core Security Technologies for Ubiquitous Security Framework,” Journal of Universal Computer Science, Vol.15, No.5, pp.1065-1080 (Mar. 2009).

[7] J.H. Park and H.S. Seo: “Security Simulation Modeling using Contract Net Protocol,” Journal of Internet Technology, Vol.10, No.1, pp.23-28 (Jan. 2009).

本研究の成果は、ネットワークセキュリティに関する研究分野全般、とくに、ワイヤレス・モバイル・ネットワーク環境や人間中心のユビキタスコンピューティング統合環境におけるセキュリティの研究発展に大きく寄与するものとして高く評価することができる。

以上のことに鑑みて、本審査委員会は本論文が博士（人間科学）の学位の授与するに値する学術的な価値を有するものと認める。

以上