案

資料6

実践的なサイバーセキュリティの研究分野　　産学共同研究構想の具体例

＜サービスの安全性に関する評価手法の確立＞

概略

共同研究先: インターネット企業、ユーザ企業
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト: （例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
電子決済サービスの利用が普及している。これらサービスは、多様なサービスと連携し、利便性を高めることでシェアを伸ばし、収集した情報をもとにサービスに活かすことでビジネスを発展させている。一方、これらのサービスを経由した金銭の窃盗や収集した情報の漏えい、不正利用等の事件も顕在化しており、このような問題は、損害賠償による経済的打撃だけでなく、企業の信頼にも影響を及ぼす大きな問題となりえる。サービス提供企業は、これらリスクを適切に分析・対処することが求められるが、利便性も重要なため安全性とのバランスをとることが難しい。そのため、サービスのモデリングやフォーマルメソッド等の科学的基礎に基づき定量的に安全性を証明できるようになることや、人間の心理的側面からの研究等により利便性も考慮した安全性の分析・評価手法を確立することは、電子決済サービス事業者および金融機関の関心が高いと想定される。

概要

共同研究により期待される成果:
大学による科学的基礎に基づくアプローチによりサービス全体の安全性の評価手法を確立し、定量的にシステムの安全性を証明できるようにする。また、安全なシステム実現の一環として、データの流れを可視化し、安全に保存・活用できるような手法を確立する。さらに、人の特性に基づく分析により、システムのインタフェースに対する安全性と利便性のバランスに関する評価手法を検討し、提案する。

共同研究の概要:
- 大学等においてフォーマルメソッド等を用いた情報セキュリティシステムの安全性評価で培われた理論、原理に基づき、サービス間の認証を含む処理や流通するデータのモデル化や定式化による評価手法を確立し、リスクを定量的に見える化することで、論理的に安全性を評価する手法を提供する。
- 大学等において秘密分散を用いた秘匿計算等の暗号技術で培われた技術的知見を活かし、データを安全に保有し、活用する手法を提案し、プロトタイプを開発する
- 大学等においてユーザビリティとセキュリティ・プライバシーに関する研究で培われた知見により、安全性と利便性が両立したシステムとなっているかを分析し評価する。

共同研究の形態: 企業からは、資金及び自社のサービス・システムと研究グループをつなぐことができる人材を提供し、大学にて研究員を雇用して研究を実施する
共同研究に想定する期間および規模: 3～4年、2400～4000万円/年、4～6名
想定される研究分野: セキュリティ評価・リスク評価、データセキュリティ、ユーザブルセキュリティ

案

実践的なサイバーセキュリティの研究分野　　産学共同研究構想の具体例

＜商用ソフトウェアの脆弱性対策と堅牢化手法の有効性研究＞

概略

共同研究先: ITベンダー企業（ソフトウェア開発企業（特にセキュリティソフトの開発を行う企業））
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
ウイルス対策ソフトや資産管理ソフトなど、日本で利用される商用ソフトウェアの脆弱性がサイバー攻撃者によって悪用されている。ソフトウェアベンダーもコストをかけて脆弱性対策をしているが、より高度な攻撃対策を実装することが求められる。特に業務・サービスを止めずに運用することが求められる重要インフラにおいては、導入するソフトウェアの堅牢性や万が一の侵害時の悪用検知は重要視される傾向にあり、重要インフラ市場でも有効性が認められる対策であれば、製品の価値向上につながり、売り上げに貢献できると想定される。

概要

共同研究により期待される成果:
ソフトウェアの脆弱性調査や対策の研究を行っている大学研究者との共同研究により、通常の市場サービスでは見つからないソフトウェアの脆弱性（ソフトウェアの動作等に係るもので例えば認証の不備で成立してしまう悪用など）を洗い出し、 対策手法を検討する。プロトタイピングにより実装への道筋を得、製品の堅牢性を高めることに資する。さらに、攻撃者による製品機能の悪用検知や攻撃検知といった、よりプロアクティブな対策手法も検討する。なお、実施した脆弱性対策や悪用検知対策等に関する研究発表を可能とすることで大学側へのインセンティブを与えることも考えられる。（ただし、攻撃者に有益となる防御の工夫等、機微な部分については秘匿）。

共同研究の概要:
- 大学等においてマルウェアの動作特性の解析とそれを活用した対策の研究で培われた攻撃手法の分析能力と対策手法を使って、ダミーファイルを利用した悪用検知などのプロアクティブな対策手法を発案しプロトタイプ実装を試みる。
  （可能な限り実環境にて、攻撃研究を行っている研究者に攻撃演習を実施し、有効性を評価する。）
- 大学等においてファイルシステムやOSの仕組みに深くかかわる攻撃や対策といったハードニングにつながる技術研究で培われた知見を活かして、マルウェア等によるソフトウェアの悪用を監視したり、悪用から保護する対策機能（プロセスの保護、設定ファイル含めた関連ファイルの保護強化など）のプロトタイプ実装を試みる。

共同研究の形態: 企業からは、資金および共同研究要員を提供し、大学の研究員と合同で研究を実施する
共同研究に想定する期間および規模: 3年、 ～2000万円/年、 2～3名
想定される研究分野: ソフトウェア脆弱性、攻撃手法、マルウェア

案

実践的なサイバーセキュリティの研究分野　　産学共同研究構想の具体例

＜端末側での利用者のセキュリティリスク低減に向けた分析・把握に係る研究＞

概略

共同研究先: セキュリティベンダー企業
実現の方向性: 企業保有のデータを共有して学理に基づく分析を行うもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト: （例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
COVID-19を受け、テレワークの普及とともにクラウドサービス利用が増え、端末におけるセキュリティ対策が重要視されるとともに、端末の利用状況の把握・分析の需要が高まっている。そこで、セキュリテイベンダー企業が提供しているソフトウェア製品のPC端末の証跡ログを活用することで、端末側でのセキュリティリスクの高い行動や、端末を操作する者が心理的にリスクの高い状況にあることを分析・把握できるようにし、顧客に提供する。これにより、ソフトウェア製品の機能が強化され、競合製品との差別化や新規サービス提供の機会に繋がりうると想定される。

概要

共同研究により期待される成果:
セキュリティベンダーより実際の環境にある各PC端末から収取した証跡ログを提供することで、セキュリティ心理学的知見を有する大学にてセキュリティリスクの高い行動や、メンタルヘルス的にリスクの高い状況を検知する条件を調査し、証跡ログの分析手法を確立する。プロトタイピングにより製品の機能強化に繋がる実装への道筋を得るとともに、試行に協力してくれるユーザをセキュリティベンダーと共に獲得し、実環境での検証を行うことで精度を向上する。

共同研究の概要:
- 大学等において取り組まれているサイバーセキュリティ状況認識の研究で培われた行動分析的知見を使って、PC端末の証跡ログからセキュリティリスクの高い行動に繋がると判断できる分析手法を発案しプロトタイプ実装と検証を試みる。
- 大学等において取り組まれているメンタル負荷などの研究で培われた心理学的知見を使って、PC端末の証跡ログから心理的にリスクの高い状況と判断できる分析手法を発案しプロトタイプ実装と検証を試みる。

共同研究の形態: 企業からは、研究費およびデータを提供し、大学にて研究員を雇用して研究を実施する
共同研究に想定する期間および規模: 2年、 ～2000万円/年、 2名
想定される研究分野: セキュリティ心理学、OSセキュリティ