NECOMA

視線追跡装置を用いた フィッシング対策技術の開発

- 日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発（NECOMA）プロジェクトでは、ユーザをサイバー脅威から保護する技術開発に取り組んでいます。
- ユーザを狙ったフィッシング攻撃の対策技術として、ウェブサイトの真贋判定を行う際にブラウジングの正しい習慣を身につけさせるアプリケーションの実装を行っています。
- 各ユーザのスキルやブラウジング環境ごとに最適なサイバー脅威対策技術の研究開発をおこなうとともに、国際標準化活動を通じた普及活動を行います。

フィッシングの被害

セキュリティ企業によると、フィッシング攻撃の平成 25 年の被害総額は全世界で 7,000 億円と試算されています。平成 26 年度も毎月 10,000 を超えるフィッシングサイトが報告されており、脅威の規模は拡大していると言えるでしょう。

EV SSL 証明書

厳格な審査のもと発行される SSL 証明書です。近年の主要ブラウザでは、EV SSL 証明書を用いたウェブサイトを表示する際に、アドレスバーを緑色に変更するなど、サイトの安全性を認識させやすくなっています。

フィッシング攻撃とは

フィッシング攻撃とは、インターネットを利用するエンドユーザを騙すことにより、ユーザの個人情報を盗むサイバー攻撃です。攻撃者は、本物そっくりに作成した偽のウェブサイトにユーザをおびき寄せ、個人情報を入力させるよう促します。この偽のウェブサイトがフィッシングサイトと呼ばれています。

フィッシングサイトの対策は、大きく 3 通りに分けることができます。

ユーザの教育による対策

ユーザにウェブサイトの URL やドメイン、EV SSL 証明書などからフィッシングサイトの識別が行えるような知識を啓蒙します。

インタフェースの改善による対策

ユーザがウェブサイトの安全性や危険性を認識しやすくなるようにインタフェースを改善します。

フィッシングサイトの検知による対策

フィッシングサイトの URL をパターンマッチで照合する、あるいは、フィッシングサイトらしさを計算することにより検知を行います。検知結果をユーザに通知することにより、ユーザの意思決定をサポートします。

視線追跡に基づくフィッシング対策

NECOMA では平成 25～26 年度に被験者実験を行い、エンドユーザがフィッシングサイトを見た際に、ブラウザのどこを見ているかについて調査を行いました。フィッシングサイトを見分ける力が優れているユーザの視線が下の図の通りです。ウェブコンテンツではなく、ブラウザのアドレスバーに表示される URL や SSL 証明書を見て判断する傾向が観測されました。

これに対して、フィッシングサイトを見分けられなかったユーザは、アドレスバーではなくコンテンツから判断しようとする傾向があります。

フィッシングサイトは正規サイトと全く同じ外見をしていることが多く、表示されたコンテンツで判定を行うことは難しいため、フィッシングサイトを正しく判定できなかったと推測されます。

NECOMA

視線追跡装置を用いた フィッシング対策技術の開発

視線追跡装置

視線追跡装置は、人間の視線方向の測定を行う装置です。人間の眼球に近赤外線を照射し、角膜表面からの反射光と瞳孔中心位置などから眼球運動の測定を行う角膜反射法や、角膜部の電位を調べる EOG 法などの測定法があります。

認知心理学

人間に内在する精神状態を、その人間から観測される情報に基づいて分析する学際領域です。NECOMA では、視線情報に基づいて、エンドユーザがウェブサイトを閲覧する際の意図を推測する技術開発を行っています。

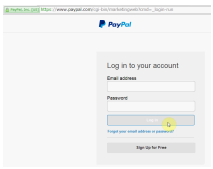
EyeBit のドキュメント

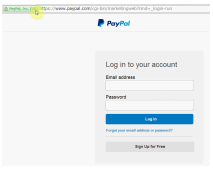
EyeBit については、分かりやすい解説がブログ記事として、詳細な解説が論文として、いずれも NECOMA プロジェクトのウェブサイトに掲載されています。

NECOMA の研究活動ならびに成果についての詳細は、Web サイト www.necoma-project.jp をご覧ください。

視線追跡による対策: EyeBit

EyeBit は視線追跡を行い、ユーザがブラウザのアドレスバーを確認するまでは、表示されるウェブフォームへの入力ができなくなるブラウザ拡張です。





左の図がコンテンツを表示した際の画面です。ユーザがアドレスバーを見た場合、視線追跡カメラとブラウザ拡張が連携し、右の図のように入力が可能なようになります。

ユーザは EyeBit の利用によりアドレスバーを確認する習慣が身につきます。フィッシング攻撃下においても、無意識に URL や SSL 証明書を確認するようになれば、騙されて個人情報を盗まれる危険性を減らすことができます。

NECOMA プロジェクトでは、EyeBit の技術を普及させるため、教育・国際標準化・オープンソース化の 3 本柱を掲げ取り組んでいます。

教育

国内・海外を問わず高等教育機関においてフィッシング対策の授業を行い、NECOMA の成果を説明しています。平成 27 年度は小学生を対象とした授業を行いました。

国際標準化

国際標準化団体 ITU-T の SG17 に参加し、サイバーセキュリティの分科会において勧告案を提案し、本分野の研究開発を促しています。

オープンソース

EyeBit を試験しやすくするため、実装をオープンソースにより公開しています。商用・非商用問わず、どなたでも自由に改変して利用することが可能です。

※ダウンロード先
https://github.com/necoma/

視線分析によるフィッシング予防

NECOMA プロジェクトでは、エンドユーザの視線を計測することで、エンドユーザがフィッシングサイトに騙されてしまう状況を未然に検知する技術開発を行いました。

この技術では、認知心理学の先行研究を活用しています。アドレスバーやセキュリティ情報を凝視した時間と回数を調べることで、エンドユーザが「漠然と眺めている」のか「意図をもって眺めているのか」を判定し、ウェブサイトの真贋判定の意図を分析しています。

スマートフォンユーザへの応用

スマートフォンは画面の表示領域が狭く、セキュリティ情報の提示が十分でない状況があります。NECOMA プロジェクトでは、小型のタブレット端末を用いて実験を行い、開発したサイバー防御技術の評価を行いました。この結果、ユーザの安全性の向上が見込め、かつ利便性の低下は限定的であることが示唆されました。

未来のセキュリティ技術開発へ

コンピュータシステムではなく、システムを利用するユーザへの攻撃が増加しています。NECOMA プロジェクトはユーザを守るためにはユーザが何を考えているかを知る必要があると考え、視線分析と認知心理学に着目しました。

プロジェクト終了以降も、他の生体情報を用い、多種多様なサイバー脅威に対する技術開発を行っていく予定です。

【お問い合わせ先】
奈良先端科学技術大学院大学　情報科学研究科
インターネット工学研究室内
NECOMA プロジェクト事務局
Mail: fp7-necoma-pr@is.naist.jp
Web: http://www.necoma-project.jp

NECOMA
Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis