研究紹介

PRESS RELEASE

岡山大学
OKAYAMA UNIVERSITY

平成 30 年 5 月 31 日

低リソース・高速での処理が可能な暗号化技術の研究
～IoT 時代を支える情報セキュリティ～

◆発表のポイント

・IoT（モノのインターネット）時代を支えるセキュリティ技術を開発しています。
・デバイスが発する電磁波を解読し、AI（人工知能）を用いて解析することでパスワードなどを割り出す攻撃について、脅威を評価する実証研究を行っています。
・データを暗号化する際のアルゴリズムの複雑化など、対策技術の研究も進めています。

あらゆるものがインターネットにつながる IoT 時代。大学院自然科学研究科（工）の野上保之教授の研究室では、その安全性を支える情報セキュリティに関し、データを守る暗号技術の開発や、その脅威となる攻撃法の実験検証と対策技術の開発を行っています。特に、暗号計算中に発生する電磁的なノイズを AI を用いて解析し、パスワードなどを割り出す攻撃の検証と、暗号データのかく乱や暗号計算アルゴリズム自身の複雑化といった対策技術の開発を進めています。

■発表内容

＜導入＞

あらゆるものがインターネットにつながる「IoT 時代」が到来したといわれています。家電や工業機械など無数の物品が、IoT デバイスとその周辺機器を介して絶えず情報をやりとりすることで、自動・遠隔操作や無人での動作最適化などが可能になり、私たちの生活の質は飛躍的に向上しました。しかしその一方で、それらのデバイスを起点として悪意ある攻撃者からデータの不正取得、改ざんといった攻撃を受けるリスクも増大しています。本研究室では、暗号数学や計算アルゴリズムを駆使し、IoT デバイスの情報セキュリティを高めるための研究を続けています。

＜背景＞

末端のデータから守る（データセキュリティ）においてはこれまで、その情報の発信源はパソコンやスマホなど十分な計算リソースをもつデバイスであり、情報セキュリティに関する研究・技術開発はこれらを中心に進められてきました。しかしながら、少し目線を変えると、IC カードの集積回路のように目に見えて小さなデバイスから、無線 LAN 機器、自動車の中の制御マイコン、自宅のスマートスピーカーなど、その中ではやはり小さな通信デバイスが重要な情報を生成・仲介しています。それらの中には、暗号化・復号してデータをしっかり守っているものもあれば、生データをそのまま送受信しているものもあります。また、ロボットの動作処理など重要な処理をリアルタイムで行う場合には、計算時間のかかる暗号化・復号処理を行っている場合ではない状況もあります。そのような状況に対する情報セキュリティに関する研究・技術開発は、必ずしもこれまで十分

なものではありませんでした。特にこの IoT 時代、攻撃者が簡単に攻撃対象となるデバイスを入手でき、さまざまな攻撃実験を行えるという状況に対しては、その対策についても多様な視点から検討する必要があります。

＜研究内容、業績＞

IoT 時代の情報セキュリティの脅威として、特に懸念が高まっているのが、デバイスの発する電磁波を読み取るといった物理的手段を用いた手法です。リソースが限られたデバイスに暗号化・復号機能を搭載すると、暗号計算中に発生する電磁的なノイズの中に、パスワードなどの機密情報が漏洩してしまうことがあります。漏洩した情報がごく断片的なものであっても、AI を用いた解析によって完全な情報を推定されるおそれがあります。

本研究室では、そのような攻撃と対策に関する一連の実験や研究開発を行っています。例えば、IoT デバイスに楕円曲線暗号 [1)]や AES 暗号 [2)]など最先端の暗号アルゴリズムを搭載し、その暗号化中に発生する電磁的なノイズの観測波形から、パスワード情報が漏洩しないかを調べています。それらの波形データを多数解析し、AI を用いてパスワードを推定できないか検証する実験も併せて行っています。また、このような手法による攻撃の対策として、極めて長い周期で予測が困難な乱数を準備し、その乱数を用いた暗号データのかく乱や、暗号計算アルゴリズム自身の複雑化を行うと同時に、そのために必要となる処理時間の軽減など効率化の研究も進めています。そうして開発した技術を実際にロボットなどに搭載し、リアルタイム処理へ及ぼす影響などについても検証をしています。

＜展望＞

これからの情報セキュリティ技術開発において、AI 技術がどのように取り入れられるかが重要になると考えています。本研究室でも、AI による攻撃・脅威への対策技術開発について、さまざまな視点から研究開発していきたいと考えています。

新たなセキュリティ技術による対策と新たな攻撃法の発見は、短いサイクルで進んでしまいます。しかしこれに対応せず、脆弱性が内在するような製品を開発するようでは、安全・安心な ICT 社会の形成は進みません。セキュリティ対策や仕組みについては、これを広く知っている若手の技術者が求められていますし、またすでに一線で活躍している技術者の学び直しも必要になってきています。本研究室の成果が、産業界における研究開発に直結することだけでなく、そのような工学教育の視点からも還元できるよう、岡山大学として enPiT2-Security BasicSecCap[3)]の取り組みを実施しています。

＜略歴＞

野上　保之（のがみ　やすゆき）

1972 年生まれ。信州大学大学院・博士課程を修了、博士（工学）。

専門は離散数学、情報セキュリティ（暗号）。

＜語句説明・用語解説＞

1)　楕円曲線暗号

　従来の 10 倍以上短いパスワードで強力な安全性を実現できる暗号であり、とりわけ IoT デバイス向けとして活用が進んでいます。

2)　AES 暗号

　データを高速に暗号化・復号する世界標準の共通鍵暗号です。

3)　enPiT2-Security BasicSecCap

　岡山大学も連携校となっている「実践的なセキュリティ人材を育成する」学部生向け教育プログラムです。

　https://www.seccap.jp/basic/seccap.html

＜お問い合わせ＞
岡山大学大学院自然科学研究科（工）
教授　野上保之
（電話番号）086-251-8127
（メール）yasuyuki.nogami@okayama-u.ac.jp