MWS2022 トラックチェアからの講評

MWS2022 プログラム委員長
内田 真人

目次

MWS2022プログラム委員のみなさま

市野 将嗣	電気通信大学	佐々木 貴之	横浜国立大学
岩本 一樹	株式会社セキュアブレイン	佐藤 将也	岡山県立大学
内田 真人	早稲田大学	高田 雄太	デロイト トーマツ サイバー合同会社
海野 由紀	富士通研究所	田中 恭之	NTTセキュリティ・ジャパン株式会社
岡本 剛	神奈川工科大学	田辺 瑠偉	横浜国立大学
沖野 浩二	富山大学	千葉 大紀	NTTセキュリティ・ジャパン株式会社
折田 彰	株式会社日立システムズ	羽田 大樹	NTTセキュリティ・ジャパン株式会社
加藤 雅彦	長崎県立大学	牧田 大佑	情報通信研究機構
川口 信隆	日立製作所	村上 洸介	株式会社KDDI総合研究所

みなさま、ご協力ありがとうございます！

MWSトラックのセッション編成

MWS① 10/24(月)	CSIRT・脆弱性分析	MWS② 10/24(月)	IoTセキュリティ
MWS③ 10/26(水)	脅威インテリジェンス	MWS④ 10/26(水)	機械学習による検知と分類
MWS⑤ 10/26(水)	マルウェア解析・プログラム解析	MWS⑥ 10/26(水)	マルウェア対策
MWS⑦ 10/27(木)	悪性Webサイト	MWS⑧ 10/27(木)	ネットワークセキュリティ

- トピックの全体傾向は昨年から変わらず、多様な論文が集まりました
- 最終的に34件の研究発表があり、8件のセッションを編成しました

数字でわかるMWS2022

	セッション数	論文総数	学生論文数	データセット活用論文
2015	10	32	-	23
2016	17	67	-	11
2017	17	67	-	16
2018	14	55	-	13
2019	13	53	29	9
2020	10	36	26	9
2021	9	35	21	8
2022	**8**	**34**	**23**	**2**

- 論文総数・学生論文数は近年と同等程度
- データセット活用論文が減少傾向
  - 従来のデータセットのスコープから、研究分野が広がりつつある
  - 自らデータセットを用意したり、公開データセットを利用したりする論文が増えた
  - MWS以外での発表や、測定できてはいない卒修論などもあるかもしれない

目次

- MWSトラックについて
- **表彰の選考について**
- 表彰の結果について

表彰の種類

- MWS実行委員会では、マルウェア対策研究において優秀な論文の発表を行い、MWSの盛会に寄与した講演者ならびに著者らを表彰することを目的とした論文賞を設けております。
- MWSプログラム委員会は以下の観点に基づいた厳正な審査を行い、表彰対象論文を選出します。
  1. マルウェア/サイバー攻撃対策に有効かつ新規性があるか
  2. 新たな技術の研究・開発を喚起する研究成果であるか
  3. 他の研究の参考になる研究成果であるか
  4. マルウェア/サイバー攻撃・対策の現状・実態を明らかにする実験・調査であるか

表彰の種類

https://www.iwsec.org/mws/2022/
https://www.iwsec.org/css/2022/award.html

CSS論文賞

CSS(最)優秀論文賞

すべての論文が審査対象

MWS優秀論文賞

MWSプログラム委員会で選考

- 著者全員を表彰対象とする。
- 過去の受賞経歴を問わない。

CSS学生論文賞

学生が講演者の論文が審査対象

MWS学生論文賞

MWSプログラム委員会で選考

- 著者全員を表彰対象とする。
- 過去に学生論文賞を受賞した者が講演する論文は審査対象とならない。
- 学生には社会人特別選抜またはそれに類似する制度で入学した者を含めない。
- MWSデータセットを使用した研究は積極的に評価する。

CSS奨励賞

すべての論文が審査対象

MWS ベストプラクティカル研究賞

MWSプログラム委員会で選考

- MWSトラックのすべての論文が審査対象
- 著者全員を表彰対象とする。
- 実用性の高さやサイバーセキュリティに関する研究コミュニティとしての有用性を評価する。

選奨の方法（１）

- **基本方針：『石を拾うことはあっても玉を捨てることなかれ』**
  - なるべく多くの人が受賞となるように幅広く選定する
  - MWS データセットを使用した研究は積極的に評価する
  - ただし、賞の価値を毀損しないようにする
- **評価基準：各１～６点の２４点満点で評価**
  - **新規性：**
    - 類似の研究がこれまでに無く独創的なものであるか、
      または、類似の研究と比較して進歩改善の度合が大きいかどうか。
  - **妥当性および信頼性：**
    - 著者の主張に対する的確な証拠、証明、評価が示されているかどうか、
      および、評価検証の結果は一貫しており安定しているか。
  - **実用性：**
    - 現在の計算機環境で実装が容易かどうか、
      または、既に実装済でその完成度が高いかどうか。
  - **総合評価：**
    - 上記３つの平均点ではなく、論文の良い面があればそれを総合的に反映する。

選奨の方法（２）

- **選奨の大まかな手順**
  - **一次査読**：1本の論文を2人の査読者で評価
  - **二次査読**：一次査読上位の論文について、MWSプログラム委員全員で評価
  - **最終審査**：MWSトラックの点数上位の論文をCSSへ推薦
- **論文評価のべからず集**
  - ライバルの研究成果に低い点数をつけるべからず
  - 知り合いの研究成果に高い点数をつけるべからず
  - 自分の好みで判断するべからず
  - 一律に同じ点数をつけるべからず
- **論文著者へのフィードバック**
  - 推薦したい論文は「なぜ良かったのか」に関するコメントを残しました
  - 二次査読対象の論文著者に対しコメントをフィードバックします

目次

- MWSトラックについて
- 表彰の選考について
- **表彰の結果について**

二次審査対象論文（34件中11件を選出）

- VirusTotalとWebアクセスログを用いたURLブロックリストの作成・管理手法の改良
- 悪用された脆弱性に関する情報源の比較調査
- am I infected? IoTセキュリティ診断Webサービスを用いたエンドユーザへの注意喚起の実証実験
- IoTマルウェアの感染処理に着目したアクセス制御手法の提案
- AndroidアプリのURL自動リンクにおけるフィッシングリスクの分析と対策の実装
- ハニーポットで観測されたエクスプロイトのライフサイクルに関する実態調査
- アジャイル型のサイバー攻撃解析用模擬ICT環境構築・管理システム
- xltrace: クロスアーキテクチャに対応したライブラリ関数のトレース手法
- UEFIモジュールのパッキングによる難読化
- Androidマルウェア検知器に対するSHAP値を用いた学習による回避攻撃
- スクリプト実行環境に対する動的バイトコード計装機能の自動付与手法

各賞受賞論文

MWS優秀論文賞 CSS最優秀論文賞	xltrace: クロスアーキテクチャに対応したライブラリ関数のトレース手法
CSS優秀論文賞	IoTマルウェアの感染処理に着目したアクセス制御手法の提案
MWS学生論文賞 CSS学生論文賞	UEFIモジュールのパッキングによる難読化
CSS学生論文賞	Androidマルウェア検知器に対するSHAP値を用いた学習による回避攻撃
CSS奨励賞	スクリプト実行環境に対する動的バイトコード計装機能の自動付与手法
CSS奨励賞	am I infected? IoTセキュリティ診断Webサービスを用いたエンドユーザへの注意喚起の実証実験

各賞受賞論文

MWSベストプラクティカル研究賞	悪用された脆弱性に関する情報源の比較調査

- 本論文では、KEV、Symantec Signature、公開文書の3つの情報源について、カバレッジ、含む脆弱性の特性、公開のスピードの観点で分析を行っている。
- その結果、情報源のカバレッジは低く複数の情報源の監視が必要なこと、一般にGround Truthとして用いられるSymantec Signatureは網羅性が低いこと、公開速度の面ではNVDは遅く公開情報を収集する必要があることを示している。
- 既知の悪用された脆弱性に関しての比較調査は非常にプラクティカルである。
- また、得られた知見は、インシデント対応を行うセキュリティ技術者や研究者に有益であり、資料的価値も高く、全CSIRTが知っておいて欲しいものである。
- さらに、アノテーションガイドラインを作り2人の作業者でアノテーションを行っており分析の信頼性が高い。
- 以上より、本論文はMWSベストプラクティカル研究賞に相応しいと判断する。