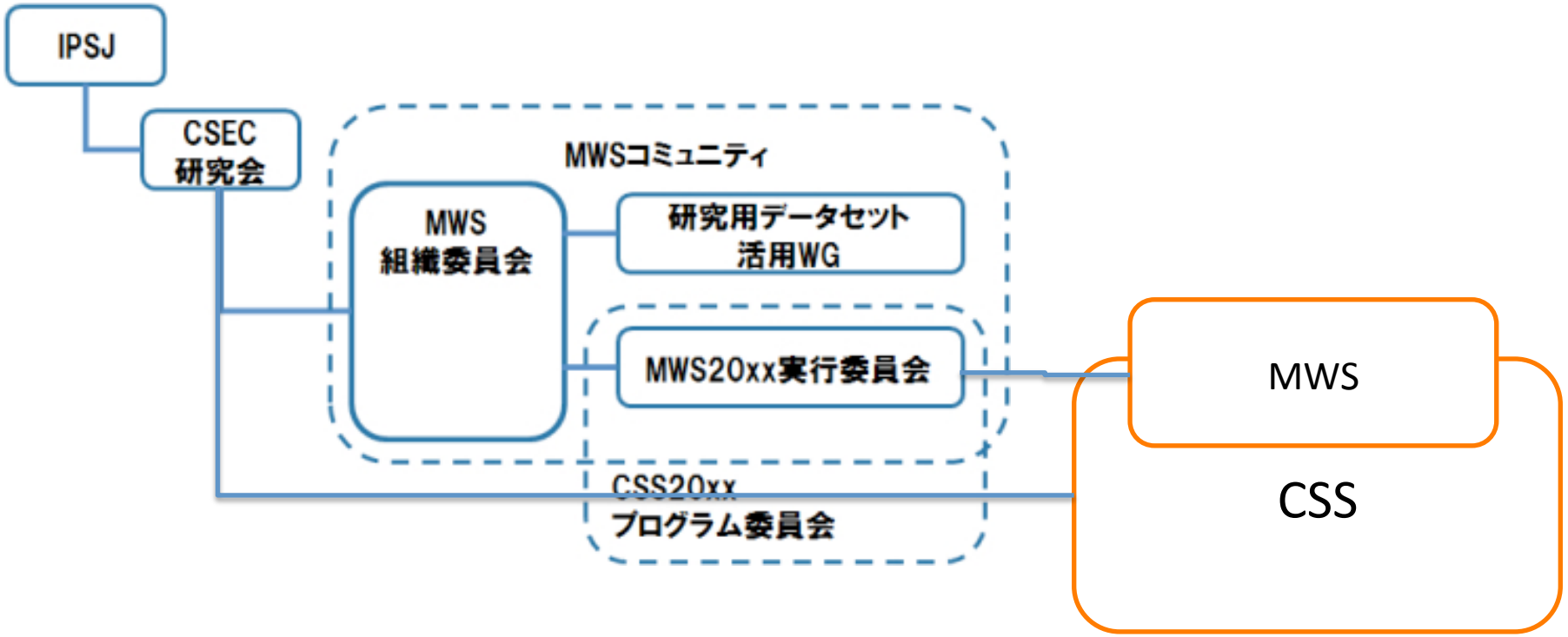
第9回マルウェア研究人材育成ワークショップの運営とCFP案

and some random thoughts

2016/5/30

MWS 2016プログラム委員長
早稲田大学　森　達哉

これまでのCSSとMWSの関係



ワークショップとしてのMWS はCSS に合同開催（内包）の形で運用

今年度（以降）のCSS運営（案）

マルウェア対策・サイバーセキュリティトラック (略称: MWS トラック)

プライバシー保護トラック (略称: PWS トラック)

暗号・認証トラック (略称: 暗号トラック)

システム・社会・ネットワークセキュリティトラック (略称: システムトラック)

ポイント:

- CSSの規模が大きくなったので、トラック制に以降
- これまでのMWSプログラム委員がMWSトラック運営委員となる
- MWSトラックは基本的にサイバーセキュリティ関連全般の受け皿となる（MWSデータセットの利用有無によらず）

プログラム運営上予想されること

- MWSとしての投稿数が増える
  - コミュニティとしては裾野が広がることは歓迎すべきこと
  - 投稿してきた人をコミュニティに巻き込みましょう（実質的な研究議論を増やしたい）
- 運営上、プログラム委員を増やす必要あり
  - 査読
  - 座長
  - 是非、ご協力をよろしくお願い致します。

MWSコミュニティの良さ

- MWS はいわば DEFCON コミュニティと Research コミュニティが渾然一体となっているコミュニティであり、世界的にも稀有な存在
  (松浦先生談)

- 実サービスに携わっている企業のテクニカルなコミットが大きい（協賛金だけでなくデータや知識・教育等）

共有価値観：プラクティカルな技術には価値がある

賞新設の提案

- *MWS Best practical paper award* (仮称)

- 研究論文としての完成度や新規性よりも、技術としての実用性の高さや、サイバーセキュリティの研究コミュニティとしての有用性を評価する
  - SoK 論文 (Systemization of Knowledge)
  - 社会的インパクトが大きかったマルウェアや脆弱性の解析事例
  - インパクトが大きい攻撃手法のPoC実装
  - その他、書き物としてはいまいちであるが、内容にキラリと光るものがある投稿全般。

ここ3年のPC長のご意見

2013年神薗さん

賞の新設、賛成です。以前、議論になったかと思われますが、特に企業からの論文は、内容は良いが論文の書き方に難があり、評価対象外となるものが多かったと認識しております。これらの論文を拾うという考え方も、ありかと思われます。

書き方には少し難があるが、今後の研究をリードするような論文を評価する価値基準を設けるのも良いかと思われます。

2014年吉岡先生

Best practice awardに賛成致します。
実用的、実務的な内容にも価値を見出すのは、この分野の研究活動を活発にすることに役に立つと思います。

2015年毛利先生

私のときは，賞を新設まではしませんでしたが，審査基準にいわゆる論文の新規性だけではなく，他の研究に刺激を与えるような実践的な開発・実験・報告等を評価するということを明記いたしました．今回先生のご提案される内容は，同様の意図かと思います．

先生からのご提案を伺って，確かにそれを賞にするというアイディアは良いなと感じました．・・・ということで，賛同いたします．

Call for papers（案）

本トラックはマルウェア研究人材育成ワークショップ(MWS)コミュニティのメンバーが運用しています。MWSトラックでは、MWSデータセットを利用した研究成果、及びマルウェア対策、サイバーセキュリティに関連する研究技術の論文を募集します。

MWSトラックでは従来の論文賞、学生論文賞に加え、今年度からプラクティカル論文賞を新設します。本賞は論文としての完成度ではなく、実用性に重点を置いた論文を評価するものです。本賞の設置はMWSコミュニティが実用的な技術や知識に高い価値を認めていることを反映しています。日頃実務的な業務に携わっている方々からの積極的なご投稿と会場でのご議論を大いに歓迎致します。

One more thing… (call for comments)

- Can we organize an English session(s) in the MWS track?
- It would provide foreign students who cannot write/discuss in Japanese with a nice opportunity to present their research outcomes in Japan.
- It might be a good opportunity to attract students from abroad, especially geographically close countries like China, Korea, and Taiwan.
- It would also be nice for us to make ourselves more "internationalized". For instance, a student who will talk at an International conference can use the English session for her/ his practice.
- This is *not* meant to create a new International conference in any sense. It is meant to enhance our diversities.

余談：MWS/CSSへの投稿状況（個人的な経験）

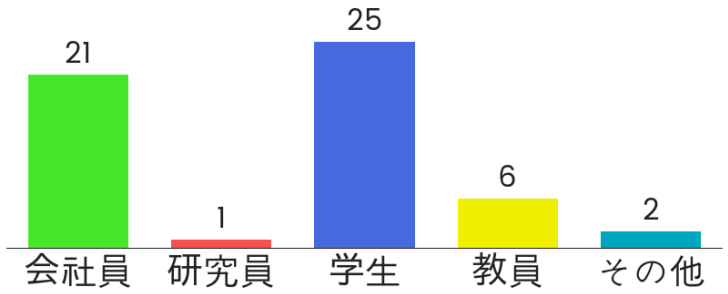
年	タイトル	分野	著者	MWS データ	国際会議、ジャーナル	備考
2009	TCPフィンガープリントによる悪意のある通信の分析	ネットワーク	木佐森他	CCC	情報処理学会論文誌	推薦論文
2010	実行ファイルに含まれる文字列の学習に基づくマルウェア検出方法	マルウェア	戸部他	CCC/D3M		
2011	多種多様な攻撃に用いられるIPアドレス間の相関解析	ネットワーク	千葉他	CCC・D3M		
	OpenFlowスイッチによる悪意のある通信の集約	ネットワーク	山田他			
2012	悪性Webサイト探索のための優先巡回順序の選定法	ネットワーク	千葉他	D3M	IEEE/IPSJ SAINT2012, 情報処理学会論文誌	
2013	自動化されたマルウェア動的解析システムで収集した 大量APIコールログの分析	マルウェア	藤野他	FFRI	IEEE CCNC 2015 IWSEC 2015(招待)	優秀論文賞
	通信源ホストの分類を利用したダークネット通信解析	ネットワーク	笹生他	NICTER		
2014	既知の悪性URL群と類似した特徴を持つURLの検索	Web	孫他	D3M	IEEE ISCC 2015, 信学会論文誌(EB)	
	リフレクター攻撃における増幅器探索通信の解析	ネットワーク	芳賀他	NICTER	IEEE GLOBECOM 2015	
	Androidアプリの説明文とプライバシー情報アクセスの相関分析	Android	渡邉他		ASIACCS15ポスター、 SOUPS 2015, IWSEC 2015(招待)	学生論文賞
	機械学習によるマルウェア検出　リローデッド	マルウェア	笹生他	FFRI		
2015	Androidクローンアプリの大規模分析	Android	石井他		RAID 2015ポスター、 ACM IWSPA 2016	学生論文賞
	未知マルウェア検知に向けたマルウェア通信の実態調査	マルウェア	畑田他		投稿中	
	Android アプリストアにおける不自然なレーティング・レビューの解析	Android	孫他		RAID 2015ポスター、 投稿中	
	Canvas Fingerprintingを用いたWebトラッキングの検証と実態調査	Web	芳賀他		RAID 2015ポスター	
	エキスパートによるマルウェア解析レポートと動的解析ログの相関分析	マルウェア	藤野他	FFRI		
	その無線アクセスポイント安全ですか？～不正な無線APの分類とフィールド調査～	ネットワーク	原田他		RAID 2015ポスター	
	RouteDetector: 9軸センサ情報を用いた位置情報追跡攻撃	Android	渡邉他		USENIX WOOT 2015	PWS論文賞
	スパムトラップを用いたマルウェア添付スパムメールの分析	ネットワーク	志村他		RAID 2015ポスター	

余談：データセットに関して

- サイバーセキュリティの研究を始めるとっかかりとしてデータセットを使えるのは非常にありがたい
  - 技術的障壁、倫理上の問題から解放される
  - 過去の研究事例もある研究キット
- 慣れてきたら自分でもデータを収集したくなる
  - MWSデータセットだけでは物足りなくなるケース
    - 規模、時間、一貫性、網羅性、一般性、etc.
- されに慣れてきたら研究コミュニティに還元することで、研究のインパクトを高める
  - 生のデータ (AmpPot, ACODE)
  - データ収集のノウハウ
  - こういうデータがほしいという要望

付録：MWS意見交換会での皆様からのフィードバック（Web投票システムを利用）

あなたのご身分を教えて下さい（一番近いものを選択してください） Mentimeter



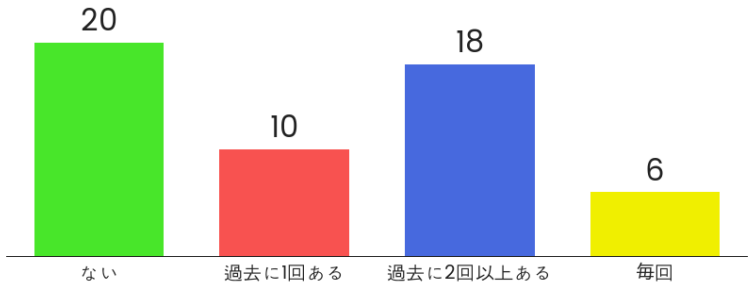
Votes: 55

あなたの所属組織名を教えて下さい（任意回答） Mentimeter

Votes: 48

これまでにMWS に参加したことは

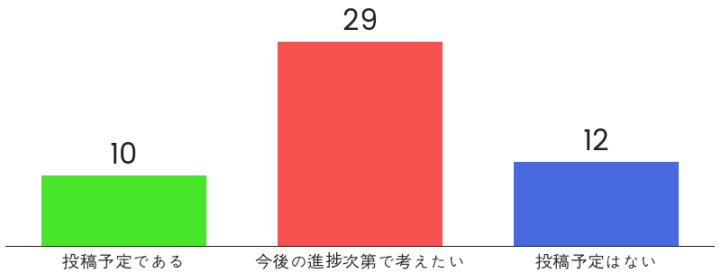
Mentimeter



Votes: 54

今年はMWS に投稿予定ですか？

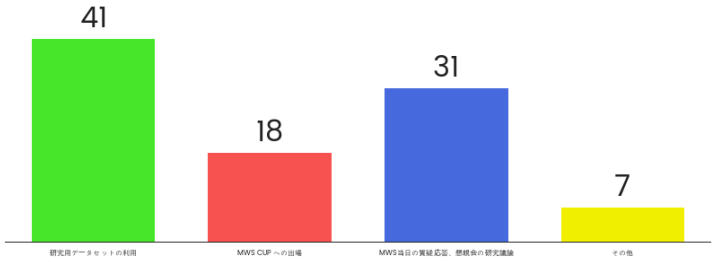
Mentimeter



Votes: 51

MWSに期待するものはなんですか？

Mentimeter

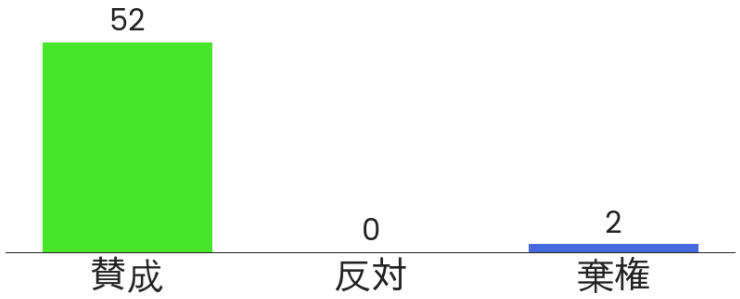


データ　CUP　議論　その他

Votes: 55

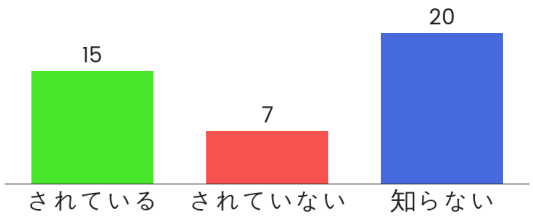
プラクティカル論文賞の新設に

Mentimeter



Votes: 54

あなたの所属組織に倫理委員会は設置されていますか？ Mentimeter



なんでもご意見お聞かせください

Mentimeter

医療研究の倫理規定はとても厳しいです。（特定の企業からお金をもらっていないことを明言するなど）

意見交換会での資料は、 参加メンバに、pdf等で、 配布して欲しい。

このツール気に入りました！ 意見収集にも合意形成にも両方に活用できますね。

ダークネット分析に興味があります。

Fake conferenceとか、scam journalの延長線上に、commercial IRB サービスとかあるかも？ お墨付きしんどろーむ！w

倫理のパネルディスカッションやりましょう

Practical賞とても良いと思います。ユーザの可用性やサービス化した際の運用コストなどが立証されていないと当然実用まで至れない現状といつも格闘しています。また倫理の件はマルウェアをインターネットにつないで動かすこと、またそれを促進することへの倫理を考えたいです。

意見交換会に参加して、今まで知らなかった知識やおもしろい論文の話などを聞けて良かった。またこのような意見交換会に参加したい。できれば、勉強会なども開いてほしい。

意見を"交換"するために、各発表に対して匿名コメントできる govote のような仕組みがあると良いかもしれませんね。