MWSプレミーティグ
研究分野でも注目され始めた現場の課題

2022年7月12日

秋山 満昭

データドリブンアプローチの重要性

- 実データの観測・分析に基づく研究**

  攻撃状況や被害状況を含む実データの観測と分析を基にしたデータドリブンアプローチの研究。サイバー空間の脅威状況を正しく理解し対策する研究に資するため、重点的に振興を図るべきと考えられる。

NISCサイバーセキュリティ研究・産学連携戦略WG最終報告
https://www.nisc.go.jp/pdf/council/cs/kenkyuwg-saishu.pdf

産業界と学術界のジレンマ

産業界

- 学術界で提案されている技術が**「現場」**で使い物にならず、目の前の問題にマンパワーで対処することで忙しい
- **課題整理や根本的な課題に取り組む**ような**研究稼働はない**

学術界

- **研究稼働はある**
- **「現場」**を持っていないので、**現場の本当の課題がわからず**、作った技術が本当に使い物になるのかもわからない

「現場」を研究対象にする研究の増加

- サイバーセキュリティのトップ会議やユーザブルセキュリティの難関会議SOUPSにおいて、専門家（セキュリティエンジニア、システム管理者、プログラマ）や専門組織（開発プロジェクト、SOC、CSIRT等）を対象にした研究が増加中
- 「現場」の実際の課題を把握して整理することで、研究開発する技術をより良いものにできる
- 「現場」に技術を持ち込んで検証することで、本来の効果やさらなる課題を把握できる

（注）研究用データセットは必ずしも「現場」のデータではない

受動的かつ不完全なセキュリティログ情報を用いたネットワーク構成情報検証手法（CSS2020）

- SOC（セキュリティオペレーションセンタ）における課題の発見と、それを解決する技術を提案
- 方法
  - フィールドワーク（組織へ入り込んで調査）
    - 三ヶ月以上かけて、国内外のSOCでエンジニアと一緒に業務をすることで、課題を明らかにした
  - 課題を解決する技術の提案
    - 不完全なログしかない状況で監視対象ネットワークの構成を自動的に推測して検証する技術

SOC	拠点	内容	期間・人数
SOC-A	国内	脅威分析業務の補助	3 カ月
		分析官へのヒアリング	4 人
SOC-B	海外	脅威分析作業	2 週間
		分析官へのヒアリング	3 人

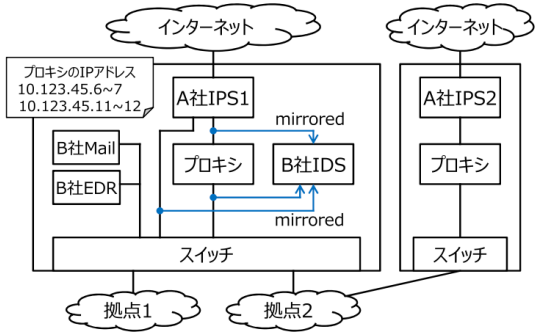

図 1　分析官が作成するネットワーク図のイメージ

「現場」の調査方法

調査方法	詳細	特徴
アンケート	質問紙に回答してもらう	• 大規模に実施可能（数百人規模） • 配布/回収はオンラインでできるため時間はほとんどかからない • 表層的な回答しか得られない
インタビュー	面接（オンライン/オフライン）で回答してもらう	• 時間がかかる（一人当たり数十分） • 小規模でしか実施できない（数人～数十人が限界） • 詳細を聞くことができる
フィールドワーク	組織に入り込んで観測する	• 非常に時間がかかる • 非常に詳細な情報が手に入る • ごく少数の組織しか把握できない

関連する論文（ほんの一部です）

- システム管理者
  - Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines (SOUPS 2019)
  - “Anyone Else Seeing this Error?”: Community, System Administrators, and Patch Information (EuroS&P2020)
- 開発者
  - Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security (S&P2017)
  - Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs (CHI2020)
- セキュリティエンジニア
  - Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues (CCS 2019)
  - How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks (CHI 2022)
- その他
  - Security Obstacles and Motivations for Small Businesses from a CISO's Perspective (USENIX Security 2021)

まとめ

- 「現場」を理解することでよりよい研究対象の設定ができる
- 「現場」を理解すること自体が研究になる
- 研究を始める段階から「学術界と産業界の橋渡し」を考えたい。研究コミュニティとして何ができるか？
  - 世界的な潮流を考えると、研究用データセットの ”次” を考えるべき時期ではないか