Vol.2019-CSEC-86 No.65
Vol.2019-SPT-34 No.65
2019/7/24

セキュリティやプライバシーに関するSoK論文やサーベイ論文をSoKする

金岡 晃[1,a)]

概要：特定の分野や技術要素について研究された論文の多くを調べ、アプローチなどの複数観点から研究開発の現状を整理しその先の研究の展望を考えるようなサーベイ論文は、セキュリティやプライバシーの研究分野においても多い。また近年の難関国際会議では、既存の研究を整理し体系化するような作業をSystematization of Knowledge（SoK）論文として受け入れることが始まっている。これらの論文は新たにこの分野の研究を始める研究者などを助けるなど意義が深い。本稿では、セキュリティとプライバシーに関するサーベイ論文やSoK論文を概観することで、どういった整理や体系化が行われているかなどサーベイ論文やSoK論文をメタな視点で体系化することに挑む。

Systematization of Knowledge of Security and Privacy SoK and Survey Papers

1. SoK論文の歴史と求められる要件

2010年、難関国際会議として知られるIEEE Symposium on Security and Privacy (以後S&P）がSoK論文の募集を開始した[1]。S&P 2010のCall for PapersにはSoK論文の説明として以下の記載がある。

> *The goal of this call is to encourage work that evaluates, systematizes, and contextualizes existing knowledge. These papers will provide a high value to our community but would otherwise not be accepted because they lack novel research contributions.*

既存の知識を「評価」「体系化（Systematize)」「文脈による解釈（Contexutualize)」する論文の募集とされ、具体的な論文の種類として以下の3つのパターンを挙げた。

(1) 主要研究領域に有用な視点を提供するサーベイ論文（*survey papers that provide useful perspectives on major research area*）
(2) 説得力のある証拠をもとに長年信じられてきたものに対する支持や意義を唱える論文（*papers that support or challenge long-held beliefs with compelling evidence*）
(3) 特定問題を解決するための競合するアプローチ群に対して広範囲かつ現実的な評価を与える論文（*papers that provide an extensive and realistic evaluation of competing approaches to solving specific problems*）

SoK論文は一般論文の査読とともに行われるが、評価は新規性ではなくコミュニティへの価値に重点を置くとされた。開始の当初はなぜこういった論文を募集するかという疑問に対してFAQが用意されていた。

S&P 2013では、既存研究状況の分析対象として「注目研究領域の特定」「未解決課題が存在するオープンな領域の指摘」「重要課題の解決に向けた優先順位の提示」があることがCFPに新たに示された。

S&P 2015になり、単なるサーベイではないということが強調されるようになり、上記3つのパターンが2つに絞られた。

(1) 確立された主要研究領域に関する重要な新しい洞察を提供する
(2) 説得力のある証拠をもとに長年信じられてきたものに対する支持や意義を唱える

S&P 2016ではその2つに加えて「主要研究領域に対する説得力のある包括的な新たな分類法」が示された。ややサーベイ論文寄りの論文も含まれるように戻った印象が感じられるものとなっている。その後、S&P 2020でもその

[1] 東邦大学, Toho University
[a)] akira.kanaoka@is.sci.toho-u.ac.jp

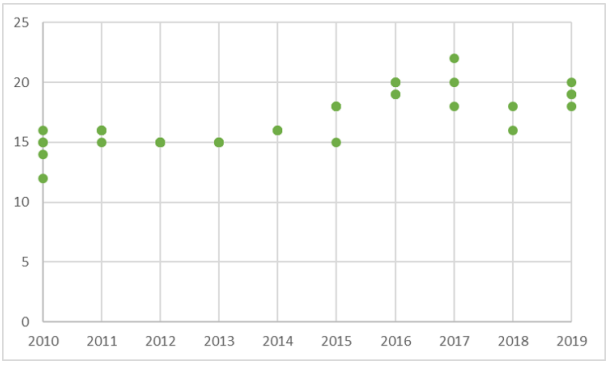

図 1　S&P で発表された SoK 論文のページ数推移

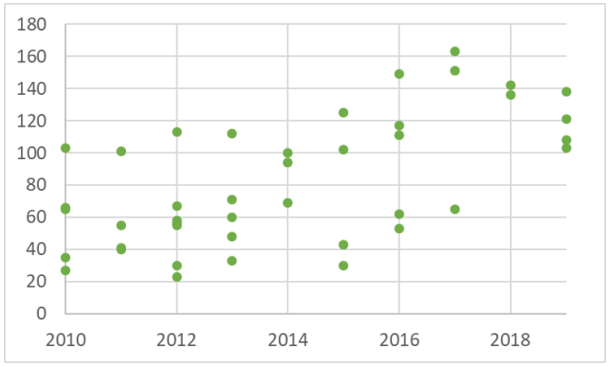

図 2　S&P で発表された SoK 論文の参考文献数数推移

CFP 記載は変わっていない。

S&P 2012、2013 ではそれぞれの SoK 論文のテーマとは関係なく、SoK セッションとして独立して発表されていた。S&P 2014 からは一般論文と合わせてそのテーマごとのセッションで発表されるようになった。この年より一般論文との違いを明確にするために論文タイトルの先頭に SoK の文字が入るように変えられた。これは他の国際会議でも踏襲されている（EuroS&P、PETS、HASP、CT-RSA、ASHES、ROOTS、AsiaCCS、AsiaPKC）。

その他の SoK 論文を募集する国際会議も S&P と類似した要件を記載しており、S&P が定める SoK 論文の要件が共通した要件として受け入れられていると考えられる。

2. SoK 論文を受け入れる国際会議

SoK 論文を Call For Papers に明示して含んでいるものは多くある。著者の調べた限りでは 13 の会議が募集を行っていた。表 1 にその情報を示す。

3. SoK 論文発表の外形傾向

SoK 論文が発表された数の推移を表 2 に示す。表中の空白は未募集あるいは未開催を示す。S&P が突出して多く、他の国際会議は募集はしているものの発表自体は少ないことがわかる。

図 1 と図 2 は S&P で発表された SoK 論文におけるページ数と参考文献数を示したものである。ページ数は平均 16.7 ページ、参考文献数は平均 81.9 件となっている。グラフからいずれも緩やかに増加の傾向があることがわかる。

4. SoK 論文の傾向分析

S&P で発表された SoK 論文は 2010 年から 2019 年までの間に 42 件あり、これは著者の調査によって得られた SoK 論文の総計 54 件のうち 77.8%を占める。S&P で発表された SoK 論文の傾向をとらえることで、全体の傾向がとらえられると仮定し、ここでは S&P で発表された 42 件の論文の傾向を調べる。

4.1 多数の対象を複数の視点で網羅的に評価

これはサーベイ論文としては一般的なこととなるが、SoK 論文においても同様の傾向がある。特に、図表を用いて視覚的にも伝わるように工夫されているものが多い [2], [12], [13], [24], [25], [27], [28], [30], [32], [33], [35], [36], [41], [42], [43]。

4.2 実際の評価や再実験の実施

サーベイ論文では文献の情報をもとに分類や分析を行うことが一般的であるが、SoK 論文では対象となる文献や手法、ソフトウェアに対して共通した環境を用意して実際に比較評価を行うことや、著者らの環境で再実験をすることが多い [5], [13], [20], [21], [26], [30], [34], [35], [40], [42]。これは SoK 論文が掲げる要件の 1 つが色濃く反映された結果と言えよう。

4.3 ツールやデータセットの公開

評価に利用したツールやデータセットを公開することがこの数年の SoK 論文にいくつか見られる [35], [40], [42]。これも今後続く傾向となる可能性がある。

5. サーベイ論文に関する調査

S&P は当初 SoK 論文として考えられる種類の 1 つとしてサーベイ論文を挙げていた。サーベイ論文は古くから歴史のある研究報告スタイルであり、多くのサーベイがさまざまな分野で行われてきた。セキュリティやプライバシーに関する論文も多い。ここではセキュリティやプライバシーに関するサーベイ論文の傾向について外形的に簡単にまとめ、SoK 論文と比較をする。

ACM はサーベイを専門に扱う論文誌 ACM Computing Surveys（CSUR) を刊行しており、毎年多くのサーベイ論文が発表されている。Author Guidline に新規性についての評価基準は記載されていない一方で、Reviewer Guidline に 4 つの視点での評価をすることが示されており、そこにも新規性についての言及はなかった。SoK 論文の要件と比較すると、より緩やかな制限となっていることがわかる。

表 1　SoK 論文を募集している国際会議

会議名	開始年
IEEE S&P	2010
USENIX Workshop on Offensive Technologies (WOOT)	2011
ACM Workshop on Artificial Intelligence and Security (AISEC)	2012
Hardware and Architectural Support for Security and Privacy (HASP)	2015
Privacy Enhancing Technologies Symposium (PETS)	2016
Security Standardisation Research (SSR)	2017
IEEE European Symposium on Security and Privacy (EuroS&P)	2017
Workshop on Attacks and Solutions in Hardware Security (ASHES)	2017
Reversing and Offensive-oriented Trends Symposium (ROOTS)	2017
Fast Software Encryption (FSE)	2017
ACM ASIA Public-Key Cryptography Workshop (AsiaPKC)	2018
RSA Conference Cryptographers' Track (CT-RSA)	2018
ACM ASIA Conference on Computer and Communications Security (AsiaCCS)	2019

表 2　SoK 論文発表数

会議	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	計
S&P	5	4	7	5	3	4	5	3	2	4	42
HASP						0	0	0	0	0	0
PETS							2	0	0	1	3
EuroS&P								2	1	1	4
ASHES								1	0		1
ROOTS								0	0		0
CT-RSA									0	0	0
AsiaPKC									2	0	2
AsiaCCS										2	2

- 技術的な品質が高い (Technical quality is high.)
- 研究や実践における重要分野との関連性が高い (Relevance to significant areas of research or practice is high.)
- 一般の関心度が高い (The level of general interest is high.)
- プレゼンテーションが効果的である (The presentation is effective.)

次に、2018、2019 年に CSUR に発表された論文のうち、セキュリティとプライバシーに関係すると思われるものを選び、そのページ数や参考文献数調べた。

その結果、2018 年中に CSUR で発表されたセキュリティやプライバシーに関するサーベイ論文は 20 件 [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83]、2019 年中は 21 件であることがわかった [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62]。

平均ページ数は 35.2 ページと SoK 論文の 16.7 ページを大きく超える量となっている。参考文献についても平均 131.7 件と SoK 論文の 81.9 件を大きく超えている。SoK 論文は対象を絞り深く分析・考察していることに比べ、サーベイ論文は広い視点で分類がされている様子がうかがえる。

6. まとめ

SoK 論文は、これまでのサーベイ論文よりも調査対象の粒度がより細かく、調査の質も奥の深いものとなっている。スピード感が速いかつ裾野の急速な広まりを見せているセキュリティとプライバシー分野にとって、SoK 論文は研究者が着実な研究を行うために重要な意味を持つ。とくに近年では SoK 論文の傾向として、文献や手法の整理や分類法・モデル化にとどまらず、同一条件で比較実験を実際に行うことやその実験に用いるデータセットやツールが公開されるなど、再現性の高い評価が可能なことに加え、その分野で行われる今後の研究に対して有用な評価プラットフォームの提供が行われている。これらは研究歴の浅い研究者だけではなく、すでに一定の研究成果を上げているベテラン研究者が他のテーマに挑むときにその研究フォーカスのブレを少なくする効果があると考えられる。

参考文献

[1] Ieee symposium on security and privacy 2010 - call for papers.
[2] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pp.

553–567, May 2012.

[3] Bryan Parno, Jonathan M. McCune, and Adrian Perrig. Bootstrapping trust in commodity computers. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pp. 414–429, Washington, DC, USA, 2010. IEEE Computer Society.

[4] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell. State of the art: Automated black-box web application vulnerability testing. In *2010 IEEE Symposium on Security and Privacy*, pp. 332–345, May 2010.

[5] Elie Bursztein, Steven Bethard, Celine Fabry, John C. Mitchell, and Dan Jurafsky. How good are humans at solving captchas? a large scale evaluation. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pp. 399–413, Washington, DC, USA, 2010. IEEE Computer Society.

[6] E. J. Schwartz, T. Avgerinos, and D. Brumley. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In *2010 IEEE Symposium on Security and Privacy*, pp. 317–331, May 2010.

[7] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy*, pp. 305–316, May 2010.

[8] V. Kashyap, B. Wiedermann, and B. Hardekopf. Timing- and termination-sensitive secure information flow: Exploring a new approach. In *2011 IEEE Symposium on Security and Privacy*, pp. 413–428, May 2011.

[9] F. Armknecht, R. Maes, A. Sadeghi, F. Standaert, and C. Wachsmann. A formalization of the security features of physical functions. In *2011 IEEE Symposium on Security and Privacy*, pp. 397–412, May 2011.

[10] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy*, pp. 96–111, May 2011.

[11] R. Henry and I. Goldberg. Formalizing anonymous blacklisting systems. In *2011 IEEE Symposium on Security and Privacy*, pp. 81–95, May 2011.

[12] C. Rossow, C. J. Dietrich, C. Grier, C. Kreibich, V. Paxson, N. Pohlmann, H. Bos, and M. v. Steen. Prudent practices for designing malware experiments: Status quo and outlook. In *2012 IEEE Symposium on Security and Privacy*, pp. 65–79, May 2012.

[13] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *2012 IEEE Symposium on Security and Privacy*, pp. 95–109, May 2012.

[14] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*, pp. 209–223, May 2012.

[15] K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton. Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. In *2012 IEEE Symposium on Security and Privacy*, pp. 332–346, May 2012.

[16] J. R. Mayer and J. C. Mitchell. Third-party web tracking: Policy and technology. In *2012 IEEE Symposium on Security and Privacy*, pp. 413–427, May 2012.

[17] E. Balsa, C. Troncoso, and C. Diaz. Ob-pws: Obfuscation-based private web search. In *2012 IEEE Symposium on Security and Privacy*, pp. 491–505, May 2012.

[18] J. Clark and P. C. van Oorschot. Sok: Ssl and https: Revisiting past challenges and evaluating certificate trust model enhancements. In *2013 IEEE Symposium on Security and Privacy*, pp. 511–525, May 2013.

[19] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi. Sok: The evolution of sybil defense via social networks. In *2013 IEEE Symposium on Security and Privacy*, pp. 382–396, May 2013.

[20] J. Reardon, D. Basin, and S. Capkun. Sok: Secure data deletion. In *2013 IEEE Symposium on Security and Privacy*, pp. 301–315, May 2013.

[21] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos. Sok: P2pwned - modeling and evaluating the resilience of peer-to-peer botnets. In *2013 IEEE Symposium on Security and Privacy*, pp. 97–111, May 2013.

[22] L. Szekeres, M. Payer, T. Wei, and D. Song. Sok: Eternal war in memory. In *2013 IEEE Symposium on Security and Privacy*, pp. 48–62, May 2013.

[23] B. Jain, M. B. Baig, D. Zhang, D. E. Porter, and R. Sion. Sok: Introspections on trust and the semantic gap. In *2014 IEEE Symposium on Security and Privacy*, pp. 605–620, May 2014.

[24] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE Symposium on Security and Privacy*, pp. 524–539, May 2014.

[25] P. Larsen, A. Homescu, S. Brunthaler, and M. Franz. Sok: Automated software diversity. In *2014 IEEE Symposium on Security and Privacy*, pp. 276–291, May 2014.

[26] X. Ugarte-Pedrero, D. Balzarotti, I. Santos, and P. G. Bringas. Sok: Deep packer inspection: A longitudinal study of the complexity of run-time packers. In *2015 IEEE Symposium on Security and Privacy*, pp. 659–673, May 2015.

[27] D. Bernhard, V. Cortier, D. Galindo, O. Pereira, and B. Warinschi. Sok: A comprehensive analysis of game-based ballot privacy definitions. In *2015 IEEE Symposium on Security and Privacy*, pp. 499–516, May 2015.

[28] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. Sok: Secure messaging. In *2015 IEEE Symposium on Security and Privacy*, pp. 232–249, May 2015.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*, pp. 104–121, May 2015.

[30] M. C. Tschantz, S. Afroz, Anonymous, and V. Paxson. Sok: Towards grounding censorship circumvention in empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 914–933, May 2016.

[31] V. Cortier, D. Galindo, R.Kusters, J.Muller, T. Truderung. Sok: Verifiability notions for e-voting protocols. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 779–798, May 2016.

[32] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith. Sok: Lessons learned from android security research for appified software platforms. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 433–451, May 2016.

[33] H. Tu, A.Doupe, Z. Zhao, G. Ahn. Sok: Everyone hates robocalls: A survey of techniques against telephone spam. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 320–338, May 2016.

[34] Y. Shoshitaishvili, R. Wang, C. Salls, N. Stephens, M. Polino, A. Dutcher, J. Grosen, S. Feng, C. Hauser, C. Kruegel, and G. Vigna. Sok: (state of) the art of war: Offensive techniques in binary analysis. In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 138–157, May 2016.

[35] J.Muller, V. Mladenov, J. Somorovsky, J. Schwenk. Sok: Exploiting network printers. In *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 213–230, May 2017.

[36] B. Fuller, M. Varia, A. Yerukhimovich, E. Shen, A. Hamlin, V. Gadepally, R. Shay, J. D. Mitchell, and R. K. Cunningham. Sok: Cryptographically protected database search. In *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 172–191, May 2017.

[37] C. Herley and P. C. v. Oorschot. Sok: Science, security and the elusive goal of security as a scientific pursuit. In *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 99–120, May 2017.

[38] J. Tian, N. Scaife, D. Kumar, M. Bailey, A. Bates, and K. Butler. Sok: "plug pray" today - understanding usb insecurity in versions 1 through c. In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 1032–1047, May 2018.

[39] J. V. Monaco. Sok: Keylogging side channels. In *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 211–228, May 2018.

[40] Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic. Sok: General purpose compilers for secure multi-party computation. In *SoK: General Purpose Compilers for Secure Multi-Party Computation*, p. 0. IEEE.

[41] Sanjeev Das, Jan Werner, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. Sok: The challenges, pitfalls, and perils of using hardware performance counters for security.

[42] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. Sok: Security evaluation of home-based iot deployments.

[43] Dokyung Song, Julian Lettner, Prabhu Rajasekaran, Yeoul Na, Stijn Volckaert, Per Larsen, and Michael Franz. Sok: sanitizing for security. *arXiv preprint arXiv:1806.04355*, 2018.

[44] Elisa Mannes and Carlos Maziero. Naming content on the network layer: A security analysis of the information-centric network model. *ACM Comput. Surv.*, Vol. 52, No. 3, pp. 44:1–44:28, June 2019.

[45] Tommi Gröndahl and N. Asokan. Text analysis in adversarial settings: Does deception leave a stylistic trace? *ACM Comput. Surv.*, Vol. 52, No. 3, pp. 45:1–45:36, June 2019.

[46] Hu Xiong, Yan Wu, and Zhenyu Lu. A survey of group key agreement protocols with constant rounds. *ACM Comput. Surv.*, Vol. 52, No. 3, pp. 57:1–57:32, June 2019.

[47] Samia Oukemeni, Helena Rifà-Pous, and Joan Manuel Marquès Puig. Privacy analysis on microblogging online social networks: A survey. *ACM Comput. Surv.*, Vol. 52, No. 3, pp. 60:1–60:36, June 2019.

[48] Rochak Swami, Mayank Dave, and Virender Ranga. Software-defined networking-based ddos defense mechanisms. *ACM Comput. Surv.*, Vol. 52, No. 2, pp. 28:1–28:36, April 2019.

[49] Athira Nambiar, Alexandre Bernardino, and Jacinto C. Nascimento. Gait-based person re-identification: A survey. *ACM Comput. Surv.*, Vol. 52, No. 2, pp. 33:1–33:34, April 2019.

[50] Azzedine Boukerche and Qi Zhang. Countermeasures against worm spreading: A new challenge for vehicular networks. *ACM Comput. Surv.*, Vol. 52, No. 2, pp. 34:1–34:25, May 2019.

[51] Chadni Islam, Muhammad Ali Babar, and Surya Nepal. A multi-vocal review of security orchestration. *ACM Comput. Surv.*, Vol. 52, No. 2, pp. 37:1–37:45, April 2019.

[52] Ayman Taha and Ali S. Hadi. Anomaly detection methods for categorical data: A review. *ACM Comput. Surv.*, Vol. 52, No. 2, pp. 38:1–38:35, May 2019.

[53] Usama Ahmed, Imran Raza, and Syed Asad Hussain. Trust evaluation in cross-cloud federation: Survey and requirement analysis. *ACM Comput. Surv.*, Vol. 52, No. 1, pp. 19:1–19:37, February 2019.

[54] Parnika Bhat and Kamlesh Dutta. A survey on various threats and current state of security in android platform. *ACM Comput. Surv.*, Vol. 52, No. 1, pp. 21:1–21:35, February 2019.

[55] Marco Patrignani, Amal Ahmed, and Dave Clarke. Formal approaches to secure compilation: A survey of fully abstract compilation and related work. *ACM Comput. Surv.*, Vol. 51, No. 6, pp. 125:1–125:36, February 2019.

[56] Jin-Hee Cho, Shouhuai Xu, Patrick M. Hurley, Matthew Mackay, Trevor Benjamin, and Mark Beaumont. Stram: Measuring the trustworthiness of computer-based systems. *ACM Comput. Surv.*, Vol. 51, No. 6, pp. 128:1–128:47, February 2019.

[57] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations: A survey. *ACM Comput. Surv.*, Vol. 51, No. 6, pp. 129:1–129:41, January 2019.

[58] Sandro Pinto and Nuno Santos. Demystifying arm trustzone: A comprehensive survey. *ACM Comput. Surv.*, Vol. 51, No. 6, pp. 130:1–130:36, January 2019.

[59] Diego De Siqueira Braga, Marco Niemann, Bernd Hellingrath, and Fernando Buarque De Lima Neto. Survey on computational trust and reputation models. *ACM Comput. Surv.*, Vol. 51, No. 5, pp. 101:1–101:40, November 2018.

[60] Giannis Tziakouris, Rami Bahsoon, and Muhammad Ali Babar. A survey on self-adaptive security for large-scale open environments. *ACM Comput. Surv.*, Vol. 51, No. 5, pp. 100:1–100:42, October 2018.

[61] Ming Liu, Zhi Xue, Xianghua Xu, Changmin Zhong, and Jinjun Chen. Host-based intrusion detection system with system calls: Review and future trends. *ACM Comput. Surv.*, Vol. 51, No. 5, pp. 98:1–98:36, November 2018.

[62] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan čapkun, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. Security of distance-bounding: A survey. *ACM Comput. Surv.*, Vol. 51, No. 5, pp. 94:1–94:33, September 2018.

[63] Christophe Kiennert, Ziad Ismail, Herve Debar, and Jean Leneutre. A survey on game-theoretic approaches for intrusion detection and response optimization. *ACM Comput. Surv.*, Vol. 51, No. 5, pp. 90:1–90:31, August 2018.

[64] Yury Zhauniarovich, Issa Khalil, Ting Yu, and Marc Dacier. A survey on malicious domains detection through

dns data analysis. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 67:1–67:36, July 2018.

[65] Marcus Botacin, Paulo Lício De Geus, and André grégio. Who watches the watchmen: A security-focused review on current state-of-the-art techniques, tools, and methods for systems and binary analysis on modern platforms. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 69:1–69:34, July 2018.

[66] Keman Huang, Michael Siegel, and Stuart Madnick. Systematically understanding the cyber attack business: A survey. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 70:1–70:36, July 2018.

[67] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. A survey of physics-based attack detection in cyber-physical systems. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 76:1–76:36, July 2018.

[68] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 79:1–79:35, July 2018.

[69] Xiao Han, Nizar Kheir, and Davide Balzarotti. Deception techniques in computer security: A research perspective. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 80:1–80:36, July 2018.

[70] Adam Czajka and Kevin W. Bowyer. Presentation attack detection for iris recognition: An assessment of the state-of-the-art. *ACM Comput. Surv.*, Vol. 51, No. 4, pp. 86:1–86:35, July 2018.

[71] Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. Current and future trends in mobile device forensics: A survey. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 46:1–46:31, May 2018.

[72] Paulo Angelo Alves Resende and André Costa Drummond. A survey of random forest based methods for intrusion detection systems. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 48:1–48:36, May 2018.

[73] Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, and Claudia Diaz. A survey on routing in anonymous communication protocols. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 51:1–51:39, June 2018.

[74] Niels Van Dijkhuizen and Jeroen Van Der Ham. A survey of network traffic anonymisation techniques and implementations. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 52:1–52:27, May 2018.

[75] Ali Ahmadian Ramaki, Abbas Rasoolzadegan, and Abbas Ghaemi Bafghi. A systematic mapping study on intrusion alert analysis in intrusion detection systems. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 55:1–55:41, June 2018.

[76] Isabel Wagner and David Eckhoff. Technical privacy metrics: A systematic survey. *ACM Comput. Surv.*, Vol. 51, No. 3, pp. 57:1–57:38, June 2018.

[77] Zihao Shan, Kui Ren, Marina Blanton, and Cong Wang. Practical secure computation outsourcing: A survey. *ACM Comput. Surv.*, Vol. 51, No. 2, pp. 31:1–31:40, February 2018.

[78] Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri. The privacy implications of cyber security systems: A technological survey. *ACM Comput. Surv.*, Vol. 51, No. 2, pp. 36:1–36:27, February 2018.

[79] Dimitris Gritzalis, Giulia Iseppi, Alexios Mylonas, and Vasilis Stavrou. Exiting the risk assessment maze: A meta-survey. *ACM Comput. Surv.*, Vol. 51, No. 1, pp. 11:1–11:30, January 2018.

[80] Paulo Martins, Leonel Sousa, and Artur Mariano. A survey on fully homomorphic encryption: An engineering perspective. *ACM Comput. Surv.*, Vol. 50, No. 6, pp. 83:1–83:33, December 2017.

[81] Artem Voronkov, Leonardo Horn Iwaya, Leonardo A. Martucci, and Stefan Lindskog. Systematic literature review on usability of firewall configuration. *ACM Comput. Surv.*, Vol. 50, No. 6, pp. 87:1–87:35, December 2017.

[82] Elif Bilge Kavun, Hristina Mihajloska, and Tolga Yalçin. A survey on authenticated encryption–asic designer’s perspective. *ACM Comput. Surv.*, Vol. 50, No. 6, pp. 88:1–88:21, December 2017.

[83] Prakash Shrestha and Nitesh Saxena. An offensive and defensive exposition of wearable computing. *ACM Comput. Surv.*, Vol. 50, No. 6, pp. 92:1–92:39, November 2017.