Security Group

University of Strathclyde

Selected peer-reviewed publications in cybersecurity

Shishir Nagaraja

Publication: S. Nagaraja. Botyacc: Unified p2p botnet detection using behavioural analysis and graph analysis. In *19th European Symposium on Research in Computer Security - Volume 8713*, ESORICS 2014, pages 439–456. Springer-Verlag New York, Inc., 2014.

Description: This paper unifies behavioural analysis and graph analysis approaches to detect malware C&C traffic. Behavioural analysis deals with the statistics of traffic i.e how endpoints communicate. Graph analysis considers who talks to whom without considering how. This work proposes a new technique that integrates and extends both these approaches. Botyacc defines a diffusion process applied on SIEM data to construct a feedback loop into conventional behavioural analysis. A second feedback loop from the output of behavioural analysis is input to the diffusion process. This work is significant because it unifies two previously different lines of inquiry.
Citations: 12
Areas: Traffic analysis, behavioural analysis, botnet detection, graph theory
URL: `http://personal.strath.ac.uk/shishir.nagaraja/papers/botyacc.pdf`

Publication: J. Gardiner and S. Nagaraja. On the security of machine learning in malware c&c detection. *ACM Comput. Surv. Journal*, 49(3):59:1–59:39, Dec. 2016.

Description: This paper studies the evasion resilience of malware detection algorithms. A significant line of inquiry has been on detecting the command and control(C&C) channel which a compromised system establishes to communicate with its controller. A major oversight with many of these detection techniques is the designs resilience to evasion attempts by the well-motivated attacker. C&C detection techniques make widespread use of a machine learning (ML) component. Therefore, to analyse the evasion resilience of these detection techniques we systematize works in the field of C&C detection, and then, using existing models from the literature, go on to systematize attacks against the machine learning components used in these approaches
Citations: 15
Areas: Command and control channels, botnets, data mining, machine learning, network intrusion
URL: `http://personal.strath.ac.uk/shishir.nagaraja/papers/secml-survey.pdf`

Publication: A. Biswas, D. Ghosal, and S. Nagaraja. A survey of timing channels and countermeasures. *ACM Comput. Surv. Journal*, 50(1):6:1–6:39, 2017.

Description: This paper presents a novel analysis of covert timing channels and countermeasures. It's significance lies in the systematization of the theoretical foundations, the implementation, and the various detection and prevention techniques in the area. Rigour: the paper analyzes 64 different timing-channel communication mechanisms.
Citations: 9
Areas: Network Timing Channels, Subliminal Channels, Inter-router communication, Network Steganography
URL: `http://personal.strath.ac.uk/shishir.nagaraja/papers/timing-survey.pdf`

Publication: B. Venkatesh, S. Choudhury, S. Nagaraja, and N. Balakrishnan. Botspot: fast graph based identification of structured p2p bots. *Journal of Computer Virology and Hackbing Techniques*, 11(4):247–261, 2015.

Description: Detecting malware C&C traffic is a needle-in-a-haystack search problem across distributed vantage points. This paper focuses on efficient algorithms for C&C detection. We have subsequently productised the technique to for online C&C detection in core routers at traffic speeds of up to 80Gbps. Experimental results on real Internet traffic traces from an ISPs backbone network indicate that our techniques, (i) have time complexity linear in the volume of traffic, (ii) are robust to measurement inaccuracies arising from partial visibility and dynamics of background traffic.
Citations: 6
Areas: malware, botnets, network security
URL: `http://personal.strath.ac.uk/shishir.nagaraja/papers/botspot.pdf`

Robert Atkinson

Publication: E. Hodo, X. Bellekens, A. Hamilton, P. L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson.

Threat analysis of iot networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6, May 2016.

Description: This paper presents a threat analysis of the IoT and uses an Artificial Neural Network (ANN) to combat these threats. A multi-level perceptron, a type of supervised ANN, is trained using internet packet traces, then is assessed on its ability to thwart Distributed Denial of Service (DDoS/DoS) attacks. This paper focuses on the classification of normal and threat patterns on an IoT Network. The ANN procedure is validated against a simulated IoT network. The experimental results demonstrate 99.4% accuracy and can successfully detect various DDoS/DoS attacks.
Citations: 21
Areas: IoT security, network security, DoS attack, intrusion detection
URL: `http://personal.strath.ac.uk/robert.c.atkinson/papers/isncc2016.pdf`

Publication: X. Bellekens, C. Tachtatzis, R. Atkinson, C. Renfrew, and T. Kirkham. A highly-efficient memory-compression scheme for gpu-accelerated intrusion detection systems. In R. Poet and M. Rajarajan, editors, *Proceedings of the 7th International Conference on Security of Information and Networks*, page 302. ACM, 2014.

Description: Pattern Matching is a computationally intensive task used in many research fields and real world applications. This paper explores the parallel capabilities of modern General Purpose Graphics Processing Units (GPGPU) applications for high speed pattern matching. A highly compressed failure-less Aho-Corasick algorithm is presented for Intrusion Detection Systems on off-the-shelf hardware. The work also explores the performance impact of adequate prefix matching for alphabet sizes and varying pattern numbers achieving speeds up to 8Gbps and low memory consumption for intrusion detection
Citations: 13
Areas: network security, intrusion detection
URL: `https://arxiv.org/pdf/1704.02272`

Publication: E. Hodo, X. Bellekens, E. Iorkyase, A. Hamilton, C. Tachtatzis, and R. Atkinson. Machine learning approach for detection of nontor traffic. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, pages 85:1–85:6, New York, NY, USA, 2017. ACM.

Description: This work focuses on the classification of Tor traffic and nonTor traffic to expose the activities within Tor traffic that minimizes the protection of users. A study to compare the reliability and efficiency of Artificial Neural Network and Support vector machine in detecting nonTor traffic in UNB-CIC Tor Network Traffic dataset is presented in this paper. The results are analysed based on the overall accuracy, detection rate and false positive rate of the two algorithms. Experimental results show that both algorithms could detect nonTor traffic in the dataset.
Citations: 2
Areas: Intrusion detection, Traffic Analysis, Anonymous Communication
URL: `https://arxiv.org/pdf/1708.08725`

Publication: X. Bellekens, G. Paul, C. Tachtatzis, J. Irvine, and R. Atkinson. Strategies for protecting intellectual property when using cuda applications on graphics processing units. In *Proc. of the 9th International Conference on Security of Information and Networks*, SIN '16, pages 166–173, New York, NY, USA, 2016. ACM.

Description: Advances in the massively parallel computational abilities of (GPUs) has given rise to the potential for GPU malware. Due to the complexity of the Nvidia CUDA (Compute Unified Device Architecture) framework, conventional reverse engineering techniques are unusable. This paper shows that the Nvidia compiler, using default settings, leaks information. We leverge this to develop analysis techniques for forensic investigation including carrying out black-box disassembly and reverse engineering of CUDA binaries.
Citations: 4
Areas: Reverse Engineering
URL: `http://xavierbellekens.com/publications/SIN16.pdf`

James Irvine

Publication: G. Paul and J. Irvine. Privacy implications of wearable health devices. In *Proc. of the 7th International Conference on Security of Information and Networks*, SIN '14, pages 117–121, New York, NY, USA, 2014.

Description: This paper investigates the privacy policies of four services for wearable personal health monitoring devices, and the extent to which these services protect user privacy. We find these services do not fall within the scope of existing legislation regarding the privacy of health data. We then present a set of criteria which would preserve user privacy, and redress the concerns identified within the policies of the services investigated.
Citations: 25
Areas: Privacy, IoT security
URL: `https://strathprints.strath.ac.uk/49510`

Publication: G. Paul and J. Irvine. Practical attacks on security and privacy through a low-cost android device. *Journal of Cyber Security and Mobility*, 4(2):33–52, January 2016.

Description: In many regions, banking and other important services can be accessed from mobile connected devices, expanding the reach of these services. This paper highlights the practical risks of one such lowcost computing device, highlighting the ease with which Android-based internet tablets, designed for the developing world, can be completely compromised by an attacker. The weaknesses identified allow an attacker to gain full root access and persistent malicious code execution capabilities. We consider the implications of these attacks, and the ease with which these attacks may be carried out, and highlight the difficulty in effectively mitigating these weaknesses as a user, even on a recently manufactured device.
Citations: 4
Areas: Mobile security, privacy
URL: `https://strathprints.strath.ac.uk/54877/`

Publication: G. Paul and J. Irvine. Automating identification of potentially problematic privacy policies. *Nordic and Baltic Journal of Information and Communications Technologies*, February 2016.

Description: GDPR has increased focus on the privacy policies of companies. While the intent of legislation such as this is to put the user in control of their data, privacy policies are still difficult for users to understand. Approaches such as P3P allow the user to specify what they are willing to accept, which can then be checked against the given policy in an automated fashion. However, P3P is inflexible, and does not deal with a number of issues such are modification of policies or user anonymisation. This paper reviews policies amongst a number of major providers, and identifies a number of recommendations to improve current state-of-the-art.
Citations: 4
Areas: privacy, security policy
URL: `https://strathprints.strath.ac.uk/56209/`

Publication: X. Bellekens, G. Paul, J. Irvine, C. Tachtatzis, R. Atkinson, T. Kirkham, and C. Renfrew. Data remanence and digital forensic investigation for CUDA graphics processing units. In R. B. et. al, editor, *IFIP/IEEE International Symposium on Integrated Network Management*, pages 1345–1350, 2015.

Description: This paper investigates the practicality of memory attacks on commercial GPUs. We show that unscrupulous software running on the same GPU, either by another user may be able to gain access to the contents of the GPU memory. This contains data from previous program executions containing privileged data, which would ordinarily be inaccessible to an unprivileged application. Further, a novel methodology for digital forensic examination of GPU memory for remanent data is proposed along with considerations towards anti-forensic countermeasures.
Citations: 2
Areas: digital forensics, GPU security
URL: `https://strathprints.strath.ac.uk/53209`

Sotirios Terzis

Publication: A. Abadi, S. Terzis, R. Metere, and C. Dong. Efficient delegated private set intersection on outsourced private datasets. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2017.

Description: The work makes a significant contribution to the problem of efficient secure processing of data outsourced to the cloud by proposing the first PSI protocol for verifiable data storage and computation in the context of a malicious cloud, which provides the security properties necessary for cloud outsourcing with strong security guarantees and linear verification complexity using much more efficient additive rather than fully homomorphic encryption. The protocol security is rigorously analysed by providing a formal proof of its security properties in the standard model.
Citations: 1
Areas: Cloud security;Private Set Intersection;Secure Computation
URL: `https://strathprints.strath.ac.uk/60721/`

Publication: A. Abadi, S. Terzis, and C. Dong. VD-PSI: verifiable delegated private set intersection on outsourced private datasets. In *Proceedings of Financial Cryptography and Data Security - 20th International Conference.*

Description: The work makes a significant contribution to the problem of secure processing of data outsourced to the cloud by proposing two protocols. The work provides a rigorous study of the protocols that combines formal proofs of security properties and implementation-based performance analysis. The significance of the contribution is, first, the protocols preserve data privacy from the cloud provider, offering stronger security properties than earlier work; second, they are efficient, do not use homomorphic encryption, while the more efficient protocol is also shown to scale well and be more efficient to earlier similar state-of-the-art protocols for large dataset sizes.
Citations: 9
Areas: cloud security, security protocols
URL: `https://fc16.ifca.ai/preproceedings/09_Abadi.pdf`

Publication: A. Abadi, S. Terzis, and C. Dong. O-PSI: delegated private set intersection on outsourced datasets. In H. Federrath and D. Gollmann, editors, *Proceedings of ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings*, volume 455 of *IFIP Advances in Information and Communication Technology*, pages 3–17. Springer, 2015.

Description: The work describes the first protocol for Private Set Intersection that ensures data confidential under the semi-honest model for outsourced data sets. The work is rigorous including a sketch for a security proof.
Citations: 17
Areas: secure distributed computation, cloud security, distributed systems security
URL: `https://strathprints.strath.ac.uk/52407/`

Description: This paper studies how users perceive security of five authentication schemes: password, PKQ, WA, Go-Pass and GrIDSure. We found that user-perception of security has little to do with the actual strength of an authentication scheme. While brute-force resistance was a major contributing factor in ther security perception of something-you-know schemes, the awareness of the potential threats and effort involved also play a role.
Citations: 7
Areas: authentication, network security
URL: `https://strathprints.strath.ac.uk/50752/`

Lilian Edwards

Publication: L. Edwards. Privacy, security and data protection in smart cities : a critical eu law perspective. *European Data Protection Law Review*, 2(1):28–58, March 2016.

Description: The paper argues that a right to an explanation in the EU General Data Protection Regulation (GDPR) is unlikely to present a complete remedy to algorithmic harms, particularly in respect of privacy leakages due to ML algorithms. Additional concerns range from unfairness, discrimination, and opacity. We discuss approaches to redress the situation via (i) to the right to erasure ("right to be forgotten") and the right to data

portability; and (ii) to privacy by design, Data Protection Impact Assessments and certification and privacy seals, may have the seeds we can use to make algorithms more responsible, explicable, and human-centered.
Citations: 17
Areas: privacy law, machine learning, algorithms, data protection, privacy
URL: `https://ssrn.com/abstract=2972855`

Publication: L. Edwards and M. Veale. Slave to the algorithm? why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law and Technology Review*, 16(1):1–65, 12 2017.

Description: A key issue in Smart Cities is the lack of opportunity in an ambient or smart city environment for the giving of meaningful consent to processing of personal data; other crucial issues include the degree to which smart cities collect private data from inevitable public interactions. This paper, drawing on author engagement with smart city development in Glasgow as well as the results of an international conference in the area curated by the author, argues that smart cities combine the three greatest current threats to personal privacy, with which regulation has so far failed to deal effectively; the Internet of Things(IoT); and the Cloud. It seeks solutions both from legal institutions such as data protection law and from technological approaches, proposing in particular from the ethos of Privacy by Design, a new "social impact assessment" and new human:computer interactions to promote user autonomy in ambient environments.
Citations: 32
Areas: privacy, smart cities, data protection, internet of things, privacy by design
URL: `https://strathprints.strath.ac.uk/55917/`

Publication: L. Edwards. Privacy, security and data protection in smart cities : a critical eu law perspective. *European Data Protection Law Review*, 2(1):28–58, March 2016.

Description: In this paper we give an introduction to the transition in contemporary surveillance from top down traditional police surveillance to profiling and pre-crime methods. We then review in more detail the rise of open source (OSINT) and social media (SOCMINT) intelligence and its use by law enforcement and security authorities. Following this we consider what if any privacy protection is currently given in UK law to SOCMINT. Two factors are in particular argued to be supportive of a reasonable expectation of privacy in open public social media communications: first, the failure of many social network users to perceive the environment where they communicate as public; and secondly, the impact of search engines (and other automated analytics) on traditional conceptions of structured dossiers as most problematic for state surveillance. We conclude that existing laws provide adequate protection for open SOCMINT and that this will be increasingly significant as more and more personal data is disclosed and collected in public without well-defined expectations of privacy
Citations: 1
Areas: privacy in law, social media, open source intelligence, big data, predictive policing
URL: `https://ssrn.com/abstract=2702426`

Publication: L. Edwards and E. Harbinja. Protecting post-mortem privacy: reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts and Entertainment Law Journal*, 32(1):101–147, 2013.

Description: Post-mortem privacy is the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after their death. While of established concern in disciplines such as psychology, counselling and anthropology, this notion has till now has received relatively little attention in cybersecurity and law. An analysis of comparative common and civilian law institutions, focusing on personality rights, defamation, moral rights and freedom of testation, confirms that there is little support for post-mortem privacy in common law, and while personality rights in general have greater traction in civilian law, including their survival after death, the primary role taken by contract regulation may still mean that users of US-based cloud platforms, are deprived of post mortem privacy rights. We suggest future protection may need to come from legislation, contract or privacy-enhancing-technologies, of which the first emergent into the market is Google Inactive Account Manager.
Citations: 19
Areas: personality rights, privacy law, rights of the deceased
URL: `https://ssrn.com/abstract=2267388`

George Weir

Publication: S. Albladi and G. Weir. User characteristics that influence judgment of social engineering attacks in social networks. *Hum.-centric Comput. Inf. Sci.*, 8(1):128:1–128:24, Dec. 2018.

Description: Often, attackers access victims' information on online social networks before launching targeted attacks. This paper proposes techniques for proactive identification of gullible individuals who are likely to be vulnerable to social engineering and spear-phishing attacks. We propose a *unified* user-centric framework to measure gullibility based on the following class of attributes: socio-psychological, habitual, socio-emotional, and perceptual. We are closely working with the Scottish Police to carry out a wider study to validate our findings.
Citations: 0
Areas: Deception, Information security, Phishing, Social engineering, Social network
URL: `https://strathprints.strath.ac.uk/63669`

Publication: Y. Alkhurayyif and G. Weir. Readability as a basis for information security policy assessment. In *2017 Seventh International Conference on Emerging Security Technologies (EST)*, pages 114–121, Sept 2017.

Description: This security usability paper examines the comprehensibility of information security policies from eight different ISPs. As widely suspected, this user study found that information security policies are largely found to be opaque and incomprehensible, both using automated approaches and by humans. We developed a framework for security-policy readability using nine metrics from natural language literature. Our results reveal that traditional readability metrics are ineffective in predicting the human estimation. We proposed a new readability metric which accurately predicts human estimation thus providing a new quantitative measure that organisations can rely upon. We are closely working with eight different organisations to adopt our new readability metric into their organisational policy evolution workflow.
Citations: 0
Areas: Information security policy
URL: `https://strathprints.strath.ac.uk/63070/`

Publication: N. Etaher, G. Weir, and M. Alazab. From zeus to zitmo: Trends in banking malware. In *2015 IEEE TrustCom, Helsinki, August 20-22, 2015, Volume 1*, pages 1386–1391, 2015.

Description: This paper details a survey of Android users in an attempt to shed light on how users perceive the risks associated with app permissions and in-built adware. A series of questions was presented in a Web survey, with results suggesting interesting differences between males and females in installation behaviour and attitudes toward security.
Citations: 8
Areas: malware,
URL: `https://strathprints.strath.ac.uk/54485/`

Publication: G. Robinson and G. Weir. Understanding android security. In *Global Security, Safety and Sustainability - 10th International Conference, ICGS3 2015, London, UK, September 15-17, 2015. Proceedings*, volume 534, pages 189–199. Springer, 2015.

Description: This paper details a survey of Android users in an attempt to shed light on how users perceive the risks associated with app pe rmissions and in-built ad- ware. A series of questions was presented in a Web su rvey, with results suggest- ing interesting differences between males and females in installation behaviour and attitudes toward security
Citations: 7
Areas: Mobile security, security usability
URL: `https://strathprints.strath.ac.uk/54575/`
