Security Impacting the Physical World

Fear the Reaper: Characterization and Fast Detection of Card Skimmers ............................................. 1
Nolen Scaife, Christian Peeters, and Patrick Traynor, University of Florida

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid ............................................ 15
Saleh Soltan, Prateek Mittal, and H. Vincent Poor, Princeton University

Skill Squatting Attacks on Amazon Alexa ................................................................. 33
Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey, University of Illinois, Urbana-Champaign

CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition .......................... 49
Xuejing Yuan, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences; Yuxuan Chen, Florida Institute of Technology; Yue Zhao, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences; Yunhui Long, University of Illinois at Urbana-Champaign; Xiaokang Liu and Kai Chen, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, School of Cyber Security, University of Chinese Academy of Sciences; Shengzhi Zhang, Florida Institute of Technology, Department of Computer Science, Metropolitan College, Boston University, USA; Heqing Huang, unaffiliated; Xiaofeng Wang, Indiana University Bloomington; Carl A. Gunter, University of Illinois at Urbana-Champaign

Memory Defenses

ACES: Automatic Compartments for Embedded Systems ................................................................. 65
Abraham A Clements, Purdue University and Sandia National Labs; Naif Saleh Almakhdhub, Saurabh Bagchi, and Mathias Payer, Purdue University

IMIX: In-Process Memory Isolation Extension .................................................................................. 83
Tommaso Frassetto, Patrick Jauernig, Christopher Liebchen, and Ahmad-Reza Sadeghi, Technische Universität Darmstadt

HeapHopper: Bringing Bounded Model Checking to Heap Implementation Security ......................... 99
Moritz Eckert, University of California, Santa Barbara; Antonio Bianchi, University of California, Santa Barbara and The University of Iowa; Ruoyu Wang, University of California, Santa Barbara and Arizona State University; Yan Shoshitaishvili, Arizona State University; Christopher Kruegel and Giovanni Vigna, University of California, Santa Barbara

Guarder: A Tunable Secure Allocator ....................................................................................... 117
Sam Silvestro, Hongyu Liu, and Tianyi Liu, University of Texas at San Antonio; Zhiqiang Lin, Ohio State University; Tongping Liu, University of Texas at San Antonio

Censorship and Web Privacy

Fp-Scanner: The Privacy Implications of Browser Fingerprint Inconsistencies ..................................... 135
Antoine Vastel, Univ. Lille / Inria / Inria; Pierre Laperdrix, Stony Brook University; Walter Rudometkin, Univ. Lille / Inria / Inria; Romain Rouvoy, Univ. Lille / Inria / IUf

Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies ............... 151
Gertjan Franken, Tom Van Goethem, and Wouter Joosen, imec-DistriNet, KU Leuven
Effective Detection of Multimedia Protocol Tunneling using Machine Learning .......................... 169
Diogo Barradas, Nuno Santos, and Luís Rodrigues, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa

Quack: Scalable Remote Measurement of Application-Layer Censorship ........................................ 187
Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi, University of Michigan

Understanding How Humans Authenticate

Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse .... 203
Sanam Ghorbani Lyastani, CISPA, Saarland University; Michael Schilling, Saarland University; Sascha Fahl, Ruhr-University Bochum; Michael Backes and Sven Bugiel, CISPA Helmholtz Center i.G.

Forgetting of Passwords: Ecological Theory and Data ............................................................... 221
Xianyi Gao, Yulong Yang, Can Liu, Christos Mitropoulos, and Janne Lindqvist, Rutgers University; Antti Oulasvirta, Aalto University

The Rewards and Costs of Stronger Passwords in a University: Linking Password Lifetime to Strength .... 239
Ingolf Becker, Simon Parkin, and M. Angela Sasse, University College London

Rethinking Access Control and Authentication for the Home Internet of Things (IoT) .................... 255
Weijia He, University of Chicago; Maximilian Golla, Ruhr-University Bochum; Roshni Padhi and Jordan Ofek, University of Chicago; Markus Dürmuth, Ruhr-University Bochum; Earlence Fernandes, University of Washington; Blase Ur, University of Chicago

Vulnerability Discovery

ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem ................................................................. 273
Dave (Jing) Tian, Grant Hernandez, Joseph I. Choi, Vanessa Frost, Christie Ruales, and Patrick Traynor, University of Florida; Hayawardh Vijayakumar and Lee Harrison, Samsung Research America; Amir Rahmati, Samsung Research America and Stony Brook University; Michael Grace, Samsung Research America; Kevin R. B. Butler, University of Florida

Charm: Facilitating Dynamic Analysis of Device Drivers of Mobile Systems ......................................... 291
Seyed Mohammadjavad Seyed Talebi and Hamid Tavakoli, UC Irvine; Hang Zhang and Zheng Zhang, UC Riverside; Ardalan Amiri Sani, UC Irvine; Zhiyun Qian, UC Riverside

Nassim Corteggiani, EURECOM, Maxim Integrated; Giovanni Camurati and Aurélien Francillon, EURECOM

Acquisitional Rule-based Engine for Discovering Internet-of-Thing Devices .................................... 327
Xuan Feng, Beijing Key Laboratory of IOT Information Security Technology, IIE, CAS, China, and School of Cyber Security, University of Chinese Academy of Sciences, China; Qiang Li, School of Computer and Information Technology, Beijing Jiaotong University, China; Haining Wang, Department of Electrical and Computer Engineering, University of Delaware, USA; Limin Sun, Beijing Key Laboratory of IOT Information Security Technology, IIE, CAS, China, and School of Cyber Security, University of Chinese Academy of Sciences, China

Web Applications

A Sense of Time for JavaScript and Node.js: First-Class Timeouts as a Cure for Event Handler Poisoning .... 343
James C. Davis, Eric R. Williamson, and Dongyoon Lee, Virginia Tech

Freezing the Web: A Study of ReDoS Vulnerabilities in JavaScript-based Web Servers ....................... 361
Cristian-Alexandru Staicu and Michael Pradel, TU Darmstadt

NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications ................................. 377
Abeer Alhuzali, Rigel Gjomemo, Birhanu Eshete, and V.N. Venkatakrishnan, University of Illinois at Chicago
Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks ..................393
Wei Meng, Chinese University of Hong Kong; Chenxiong Qian, Georgia Institute of Technology; Shuang Hao, University of Texas at Dallas; Kevin Borgolte, Giovanni Vigna, and Christopher Kruegel, University of California, Santa Barbara; Wenke Lee, Georgia Institute of Technology

Anonymity
How Do Tor Users Interact With Onion Services? ..................411
Philipp Winter, Anne Edmundson, and Laura M. Roberts, Princeton University; Agnieszka Dutkowska-Zuk, Independent; Marshini Chetty and Nick Feamster, Princeton University

Towards Predicting Efficient and Anonymous Tor Circuits ..................429
Armon Barton, Mohsen Imani, and Jiang Ming, University of Texas at Arlington; Matthew Wright, Rochester Institute of Technology

BurnBox: Self-Revocable Encryption in a World Of Compelled Access ..................445
Nirvan Tyagi, Cornell University; Muhammad Haris Mughees, UIUC; Thomas Ristenpart and Ian Miers, Cornell Tech

An Empirical Analysis of Anonymity in Zcash ..................463
George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn, University College London

Privacy in a Digital World
Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes . .479
José González Cabañas, Ángel Cuevas, and Rubén Cuevas, Department of Telematic Engineering, Universidad Carlos III de Madrid

Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide? . .497
Wajih Ul Hassan, Saad Hussain, and Adam Bates, University Of Illinois Urbana-Champaign

AttriGuard: A Practical Defense Against Attribute Inference Attacks via Adversarial Machine Learning . .513
Jinyuan Jia and Neil Zhenqiang Gong, Iowa State University

Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning ..................531

Attacks on Crypto & Crypto Libraries
Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels ..................549
Damian Poddebniak and Christian Dresen, Münster University of Applied Sciences; Jens Müller, Ruhr University Bochum; Fabian Ising and Sebastian Schinzel, Münster University of Applied Sciences; Simon Friedberger, NXP Semiconductors, Belgium; Juraj Somorovsky and Jörg Schwenk, Ruhr University Bochum

The Dangers of Key Reuse: Practical Attacks on IPsec IKE ..................567
Dennis Felsch, Martin Grothe, and Jörg Schwenk, Ruhr-University Bochum; Adam Czubak and Marcin Szymaran, University of Opole

One&Done: A Single-Decryption EM-Based Attack on OpenSSL’s Constant-Time Blinded RSA ..................585
Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic, Georgia Tech

DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries ..................603
Samuel Weiser, Graz University of Technology; Andreas Zankl, Fraunhofer AISEC; Raphael Spreitzer, Graz University of Technology; Katja Miller, Fraunhofer AISEC; Stefan Mangard, Graz University of Technology; Georg Sigl, Fraunhofer AISEC; Technical University of Munich
Enterprise Security

The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level . . . . . . 621
Rock Stevens, Daniel Votipka, and Elissa M. Redmiles, University of Maryland; Colin Ahern, NYC Cyber Command; Patrick Sweeney, Wake Forest University; Michelle L. Mazurek, University of Maryland

Zero-Knowledge

Practical Accountability of Secret Processes .......................................................... 657
Jonathan Frankle, Sunoo Park, Daniel Shaar, Shafi Goldwasser, and Daniel Weitzen, Massachusetts Institute of Technology

DIZK: A Distributed Zero Knowledge Proof System .................................................. 675
Howard Wu, Wenting Zheng, Alessandro Chiesa, Raluca Ada Popa, and Ion Stoica, UC Berkeley

Network Defenses

NetHide: Secure and Practical Network Topology Obfuscation ................................ 693
Roland Meier and Petar Tsankov, ETH Zurich; Vincent Lenders, armasuisse; Laurent Vanbever and Martin Vechev, ETH Zurich

Towards a Secure Zero-rating Framework with Three Parties ................................ 711
Zhiheng Liu and Zhen Zhang, Lehigh University; Yinzhi Cao, The Johns Hopkins University/Lehigh University; Zhaohan Xi and Shihao Jing, Lehigh University; Humberto La Roche, Cisco Systems

Fuzzing and Exploit Generation

MoonShine: Optimizing OS Fuzzer Seed Selection with Trace Distillation .................. 729
Shankara Pailoor, Andrew Aday, and Suman Jana, Columbia University

Qsym: A Practical Concolic Execution Engine Tailored for Hybrid Fuzzing ................. 745
Insu Yun, Sangho Lee, and Meng Xu, Georgia Institute of Technology; Yeongjin Jang, Oregon State University; Taesoo Kim, Georgia Institute of Technology

Automatic Heap Layout Manipulation for Exploitation ........................................... 763
Sean Heelan, Tom Melham, and Daniel Kroening, University of Oxford

FUZE: Towards Facilitating Exploit Generation for Kernel Use-After-Free Vulnerabilities . 781
Wei Wu, University of Chinese Academy of Sciences; Pennsylvania State University; Institute of Information Engineering, Chinese Academy of Sciences; Yueqi Chen, Jun Xu, and Xinyu Xing, Pennsylvania State University; Xiaorui Gong and Wei Zou, University of Chinese Academy of Sciences; Institute of Information Engineering, Chinese Academy of Sciences

TLS and PKI

The Secure Socket API: TLS as an Operating System Service ................................. 799

Return Of Bleichenbacher’s Oracle Threat (ROBOT) .................................................. 817
Hanno Böck, unaffiliated; Juraj Somorovsky, Ruhr University Bochum, Hackmanit GmbH; Craig Young, Tripwire VERT

Bamboozling Certificate Authorities with BGP ....................................................... 833
Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal, Princeton University
<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI</td>
<td>851</td>
<td>Doowon Kim and Bum Jun Kwon, University of Maryland, College Park; Kristián Kozák, Masaryk University, Czech Republic; Christopher Gates, Symantec; Tudor Dumitras, University of Maryland, College Park</td>
</tr>
<tr>
<td>Vulnerability Mitigations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debolating Software through Piece-Wise Compilation and Loading</td>
<td>869</td>
<td>Anh Quach and Aravind Prakash, Binghamton University; Lok Yan, Air Force Research Laboratory</td>
</tr>
<tr>
<td>Precise and Accurate Patch Presence Test for Binaries</td>
<td>887</td>
<td>Hang Zhang and Zhiyun Qian, University of California, Riverside</td>
</tr>
<tr>
<td>From Patching Delays to Infection Symptoms: Using Risk Profiles for an Early Discovery of Vulnerabilities Exploited in the Wild</td>
<td>903</td>
<td>Chaowei Xiao and Armin Sarabi, University of Michigan; Yang Liu, Harvard University / UC Santa Cruz; Bo Li, UIUC; Mingyan Liu, University of Michigan; Tudor Dumitras, University of Maryland, College Park</td>
</tr>
<tr>
<td>Understanding the Reproducibility of Crowd-reported Security Vulnerabilities</td>
<td>919</td>
<td>Dongliang Mu, Nanjing University; Alejandro Cuevas, The Pennsylvania State University; Limin Yang and Hang Hu, Virginia Tech; Xinyu Xing, The Pennsylvania State University; Bing Mao, Nanjing University; Gang Wang, Virginia Tech</td>
</tr>
<tr>
<td>Side Channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder Than You Think</td>
<td>937</td>
<td>Stephan van Schaik, Cristiano Giuffrida, Herbert Bos, and Kaveh Razavi, Vrije Universiteit Amsterdam</td>
</tr>
<tr>
<td>Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks</td>
<td>955</td>
<td>Ben Gras, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida, Vrije Universiteit</td>
</tr>
<tr>
<td>Meltdown: Reading Kernel Memory from User Space</td>
<td>973</td>
<td>Moritz Lipp, Michael Schwarz, and Daniel Gruss, Graz University of Technology; Thomas Prescher and Werner Haas, Cyberus Technology; Anders Fogh, G DATA Advanced Analytics; Jann Horn, Google Project Zero; Stefan Mangard, Graz University of Technology; Paul Kocher, Independent; Daniel Genkin, University of Michigan; Yuval Yarom, University of Adelaide and Data61; Mike Hamburg, Rambus, Cryptography Research Division</td>
</tr>
<tr>
<td>Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution</td>
<td>991</td>
<td>Jo Van Bulck, imec-DistriNet, KU Leuven; Marina Minkin, Technion; Ofir Weisse, Daniel Genkin, and Baris Kasikci, University of Michigan; Frank Piessens, imec-DistriNet, KU Leuven; Mark Silberstein, Technion; Thomas F. Wenisch, University of Michigan; Yuval Yarom, University of Adelaide and Data61; Raoul Strackx, imec-DistriNet, KU Leuven</td>
</tr>
<tr>
<td>Cybercrime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets</td>
<td>1009</td>
<td>Rolf van Wegberg and Samaneh Tajalizadehkoob, Delft University of Technology; Kyle Soska, Carnegie Mellon University; Uğur Akyazi, Carlos Hernandez Ganan, and Bram Klievink, Delft University of Technology; Nicolas Christin, Carnegie Mellon University; Michel van Eeten, Delft University of Technology</td>
</tr>
<tr>
<td>Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces</td>
<td>1027</td>
<td>Kan Yuan, Haoran Lu, Xiaojing Liao, and Xiaofeng Wang, Indiana University Bloomington</td>
</tr>
<tr>
<td>Schrödinger's RAT: Profiling the Stakeholders in the Remote Access Trojan Ecosystem</td>
<td>1043</td>
<td>Mohammad Rezaeiad, George Mason University; Brown Farinholt, University of California, San Diego; Hitesh Dharmdasani, Informant Networks; Paul Pearce, University of California, Berkeley; Kirill Levchenko, University of California, San Diego; Damon McCoy, New York University</td>
</tr>
</tbody>
</table>
The aftermath of a crypto-ransomware attack at a large academic institution
Leah Zhang-Kennedy, University of Waterloo, Stratford Campus; Hala Assal, Jessica Rocheleau, Reham Mohamed, Khadija Baig, and Sonia Chiasson, Carleton University

Web and Network Measurement
We Still Don’t Have Secure Cross-Domain Requests: an Empirical Study of CORS
Jianjun Chen, Tsinghua University; Jian Jiang, Shape Security; Haixin Duan, Tsinghua University; Tao Wan, Huawei Canada; Shuo Chen, Microsoft Research; Vern Paxson, UC Berkeley, ICSI; Min Yang, Fudan University

End-to-End Measurements of Email Spoofing Attacks
Hang Hu and Gang Wang, Virginia Tech

Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path
Baojun Liu, Chaoyi Lu, Haixin Duan, and Ying Liu, Tsinghua University; Zhou Li, IEEE member; Shuang Hao, University of Texas at Dallas; Min Yang, Fudan University

End-Users Get Maneuvered: Empirical Analysis of Redirection Hijacking in Content Delivery Networks
Shuai Hao, Yubao Zhang, and Haining Wang, University of Delaware; Angelos Stavrou, George Mason University

Malware
SAD THUG: Structural Anomaly Detection for Transmissions of High-value Information Using Graphics
Jonathan P. Chapman, Fraunhofer FKIE

FANCI: Feature-based Automated NXDomain Classification and Intelligence
Samuel Schüppen, RWTH Aachen University; Dominik Teubert, Siemens CERT; Patrick Herrmann and Ulrike Meyer, RWTH Aachen University

An Empirical Study of Web Resource Manipulation in Real-world Mobile Applications
Xiaohan Zhang, Yuan Zhang, Qianqian Mo, Hao Xia, Zhemin Yang, and Min Yang, Fudan University; Xiaofeng Wang, Indiana University, Bloomington; Long Lu, Northeastern University; Haixin Duan, Tsinghua University

Fast and Service-preserving Recovery from Malware Infections Using CRIU
Ashton Webster, Ryan Eckenrod, and James Purtilo, University of Maryland

Subverting Hardware Protections
The Guard’s Dilemma: Efficient Code-Reuse Attacks Against Intel SGX
Andrea Biondo and Mauro Conti, University of Padua; Lucas Davi, University of Duisburg-Essen; Tommaso Frasetto and Ahmad-Reza Sadeghi, Technische Universität Darmstadt

A Bad Dream: Subverting Trusted Platform Module While You Are Sleeping
Seunghun Han, Wook Shin, Jun-Hyeok Park, and Hyeong Chun Kim, National Security Research Institute

More Malware
Tackling runtime-based obfuscation in Android with Tiro
Michelle Y. Wong and David Lie, University of Toronto

Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation
Richard Bonett, Kaushal Kafle, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk, William & Mary
Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer .......................... 1511
Thanh Bui and Siddharth Prakash Rao, Aalto University; Markku Antikainen, University of Helsinki; Viswanathan Manihatty Bojan and Tuomas Aura, Aalto University

Wireless Attacks
All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems .......... 1527
Kexiong (Curtis) Zeng, Virginia Tech; Shiniun Liu, University of Electronic Science and Technology of China; Yuanchao Shu, Microsoft Research; Dong Wang, Hao Yu Li, Yanzhi Dou, Gang Wang, and Yaling Yang, Virginia Tech

Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors . . 1545
Yazhou Tu, University of Louisiana at Lafayette; Zhiqiang Lin, Ohio State University; Insup Lee, University of Pennsylvania; Xiali Hei, University of Louisiana at Lafayette

Modelling and Analysis of a Hierarchy of Distance Bounding Attacks ............................................. 1563
Tom Chothia, Univ. of Birmingham; Joeri de Ruiter, Radboud University Nijmegen; Ben Smyth, University of Luxembourg

Off-Path TCP Exploit: How Wireless Routers Can Jeopardize Your Secrets ................................. 1581
Weiteng Chen and Zhiyun Qian, University of California, Riverside

Neural Networks
Formal Security Analysis of Neural Networks using Symbolic Intervals ........................................... 1599
Shiqi Wang, Kexin Pei, Justin Whitehouse, Junfeng Yang, and Suman Jana, Columbia University

Turning Your Weakness Into a Strength: Watermarking Deep Neural Networks by Backdooring ........ 1615
Yossi Adi and Carsten Baum, Bar Ilan University; Moustapha Cisse, Google Inc; Benny Pinkas and Joseph Keshet, Bar Ilan University

A4NT: Author Attribute Anonymity by Adversarial Training of Neural Machine Translation .............. 1633
Rakshith Shetty, Bernt Schiele, and Mario Fritz, Max Planck Institute for Informatics

GAZELLE: A Low Latency Framework for Secure Neural Network Inference ................................. 1651
Chiraag Juvekar, MIT MTL; Vinod Vaikuntanathan, MIT CSAIL; Anantha Chandrakasan, MIT MTL

Information Tracking
FlowCog: Context-aware Semantics Extraction and Analysis of Information Flow Leaks in Android Apps .............................................................. 1669
Xiang Pan, Google Inc./Northwestern University; Yinzhi Cao, The Johns Hopkins University/Lehigh University; Xuechao Du and Boyuan He, Zhejiang University; Gan Fang, Palo Alto Networks; Yan Chen, Zhejiang University/Northwestern University

Sensitive Information Tracking in Commodity IoT ................................................................. 1687

Enabling Refinable Cross-Host Attack Investigation with Efficient Data Flow Tagging and Tracking .... 1705
Yang Ji, Sangho Lee, Mattia Fazzini, Joey Allen, Evan Downing, Taesoo Kim, Alessandro Orso, and Wenke Lee, Georgia Institute of Technology

Dependence-Preserving Data Compaction for Scalable Forensic Analysis .................................... 1723
Md Nahid Hossain, Junao Wang, R. Sekar, and Scott D. Stoller, Stony Brook University