

# **4th USENIX Workshop on Offensive Technologies (WOOT'10)**

Washington, DC, USA  
9 August 2010

ISBN: 978-1-7138-1787-1

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571



**Some format issues inherent in the e-media version may also appear in this print version.**

Copyright© (2010) by Usenix Association  
All rights reserved.

Printed with permission by Curran Associates, Inc. (2020)

For permission requests, please contact Usenix Association  
at the address below.

Usenix Association  
2560 Ninth Street, Suite 215  
Berkeley, California, 94710

<https://www.usenix.org/>

**Additional copies of this publication are available from:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: 845-758-0400  
Fax: 845-758-2633  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# TABLE OF CONTENTS

SMUDGE ATTACKS ON SMARTPHONE TOUCH SCREENS .....	1
<i>A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, J.M. Smith</i>	
INTERPRETER EXPLOITATION .....	11
<i>D. Blazakis</i>	
RECOVERING WINDOWS SECRETS AND EFS CERTIFICATES OFFLINE .....	19
<i>E. Burzstein, J.M. Picod</i>	
A FRAMEWORK FOR AUTOMATED ARCHITECTURE-INDEPENDENT GADGET SEARCH .....	28
<i>T. Dullien, T. Kornau, R.P. Weinmann</i>	
PRACTICAL PADDING ORACLE ATTACKS .....	38
<i>J. Rizzo, T. Duong</i>	
FRAMING ATTACKS ON SMART PHONES AND DUMB ROUTERS: TAP-JACKING AND GEO-LOCALIZATION ATTACKS .....	47
<i>G. Rydstedt, B. Gourdin, E. Bursztein, D. Boneh</i>	
ZERO-SIZED HEAP ALLOCATIONS VULNERABILITY ANALYSIS .....	55
<i>J. Vanegue</i>	
CRAWLING BITTORRENT DHTS FOR FUN AND PROFIT .....	66
<i>S. Wolchok, J.A. Halderman</i>	

## **Author Index**