

建议读的论文

总体要求

1. 需和安全与隐私相关
2. 建议从顶级会议上寻找论文
3. 需要有一定的深度
4. 演讲时间为 20 分钟
5. 根据演讲内容、表现、技术性指标，评分为 0-50 分

推荐会议：

安全方面的会议：IEEE S&P, ACM CCS, USENIX Security, NDSS

数据、库数据挖掘、信息检索：KDD, WWW, SIGIR, SIGMOD, VLDB, ICDE

网络：ACM SIGCOMM, ACM MOBICOM, IEEE INFOCOM

其他领域请参见“中国计算机学会推荐国际学术会议和期刊目录”

(<http://www.ccf.org.cn/c/2016-12-27/569124.shtml>) 中的 A 类会议。

论文检索办法（以 USENIX Security 为例）：

1. 上述会议一般每年召开一次，但召开的月份可能不同，USENIX Security 通常于每年 8 月份召开，地点一般在美国的某个城市
2. 以检索 2016 年（也可以是 2015、2014 等）的 USENIX Security 会议论文为例：在 Google 中输入 USENIX Security 2016, 如下图：

Google

USENIX Security 2016

All Videos News Shopping Maps More Settings Tools

About 152,000 results (0.53 seconds)

USENIX Security '16 | USENIX
<https://www.usenix.org/conference/usenixsecurity16> ▼
Thanks to everyone who joined us in Austin, TX, for **USENIX Security '16**. ... **2016** USENIX Advances in Security Education Workshop; HotSec '16: **2016** USENIX ...
You've visited this page many times. Last visit: 1/5/17

Technical Sessions | USENIX
7:30 am–9:00 am, Wednesday.
Continental Breakfast. Zilker ...

Call for Papers
Call for Papers ... to submit papers
covering novel and scientifically ...
[More results from usenix.org »](#)

Important Dates
Important Dates. Paper submissions
due: Thursday ...

Co-located Workshops
Workshops will be held in conjunction
with the main ...

3. 点击进入 USENIX Security' 16, 会看到:

25TH USENIX SECURITY SYMPOSIUM
AUGUST 10–12, 2016 • AUSTIN, TX

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

HOME ATTEND **PROGRAM** ACTIVITIES SPONSORSHIP PARTICIPATE ABOUT

Thanks to everyone who joined us in Austin, TX, for USENIX Security '16. We hope you enjoyed the event. As part of our commitment to open access to research, the full proceedings are free and open to the public. The video, audio, and slides are being posted on the [technical sessions page](#) as we receive them. Paper PDFs are available to everyone now.

SPONSORS
Silver Sponsor
 Microsoft

HELP PROMOTE

AUGUST 10–12, 2016
AUSTIN, TX
www.usenix.org/sec16
Get more
Help Promote graphics!

Save the Date:
USENIX Security '17
August 16–18, 2017
Vancouver, BC, Canada

The following co-located workshops preceded the Symposium:

- [WOOT '16](#): 10th USENIX Workshop on Offensive Technologies
- [CSET '16](#): 9th Workshop on Cyber Security Experimentation and Test
- [FOCI '16](#): 6th USENIX Workshop on Free and Open Communications on the Internet
- [ASE '16](#): 2016 USENIX Advances in Security Education Workshop
- [HotSec '16](#): 2016 USENIX Summit on Hot Topics in Security

USENIX Security '16 Media Coverage

Symposium Organizers
Program Co-Chairs
Thorsten Holz, *Ruhr-Universität Bochum*

4. 点击 Program, 选择 Technical Sessions

-12, 2016 • AUSTIN, T

D PROGRAM ACTIVITIES

At a Glance

Technical Sessions

All events will take place at the Hyatt F

5. 你会看到:


Technical Sessions

The full Proceedings published by USENIX for the conference are available for download below. Individual papers can also be downloaded from the presentation page. Copyright to the individual works is retained by the author[s].

Proceedings Front Matter

[Proceedings Cover](#) | [Title Page and List of Organizers](#) | [Table of Contents](#) | [Message from the Program Co-Chairs](#)

Full Proceedings PDFs

-  [USENIX Security '16 Full Proceedings \(PDF\)](#)
-  [USENIX Security '16 Proceedings Interior \(PDF, best for mobile devices\)](#)
-  [USENIX Security '16 Proceedings Errata Slip \(PDF\)](#)
-  [USENIX Security '16 Proceedings Errata Slip 2 \(PDF\) \(11/17/16\)](#)




Full Proceedings ePub (for iPad and most eReaders)

-  [USENIX Security '16 Full Proceedings \(ePub\)](#)

Full Proceedings Mobi (for Kindle)

-  [USENIX Security '16 Full Proceedings \(Mobi\)](#)

Downloads for Registered Attendees

-   [USENIX Security '16 Attendee List \(PDF\)](#)
-  [USENIX Security '16 Proceedings Archive \(7z\)](#)

All sessions will take place at the [Hyatt Regency Austin](#).

Wednesday, August 10, 2016

7:30 am–9:00 am	Wednesday
-----------------	-----------

Continental Breakfast

Zilker Ballroom Foyer

8:25 am–8:45 am	Wednesday
-----------------	-----------

Daily Lightning Talks

Zilker Ballroom 2–4


We begin each day with a lightning talks session, offering a 60-second preview of the papers to be presented on the day. For authors, it's an opportunity to provide more reasons why people should come to your talk. For attendees, it's an opportunity to hear an elevator pitch for the papers you will have to miss today.

8:45 am–9:00 am	Wednesday
-----------------	-----------

Opening Remarks and Awards

Zilker Ballroom 2–4

6. 往下拖动鼠标，你会看到如下。其中红框里是 Session 的主题（也就是这个 Session 里的文章的主题，方便你选择和参考），蓝框里是论文题目和作者。

10:30 am–11:00 am			Wednesday
Break with Refreshments			
Zilker Ballroom Foyer			
11:00 am–12:30 pm			Wednesday
Low-Level Attacks	Verification and Timing	Panel	
Refereed Papers I	Refereed Papers II	Zilker Ballroom 4	
Zilker Ballroom 2	Zilker Ballroom 3	2016 Test of Time Award Panel	
Session Chair: Dan Boneh, <i>Stanford University</i>	Session Chair: Deian Stefan, <i>University of California, San Diego</i>	Moderator: Matt Blaze, <i>University of Pennsylvania</i>	
Flip Feng Shui: Hammering a Needle in the Software Stack	Verifying Constant-Time Implementations	Panelists: Peter Honeyman, <i>University of Michigan</i> , and Niels Provos, <i>Google</i>	
Kaveh Razavi, Ben Gras, and Erik Bosman, <i>Vrije Universiteit Amsterdam</i> ; Bart Preneel, <i>Katholieke Universiteit Leuven</i> ; Cristiano Giuffrida and Herbert Bos, <i>Vrije Universiteit Amsterdam</i>	José Bacelar Almeida, <i>HASLab/INESC TEC and University of Minho</i> ; Manuel Barbosa, <i>HASLab/INESC TEC and DCC FCUP</i> ; Gilles Barthe and François Dupressoir, <i>IMDEA Software Institute</i> ; Michael Emmi, <i>Bell Labs and Nokia</i>	Available Media	
Available Media	Available Media		
One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation	Secure, Precise, and Fast Floating-Point Operations on x86 Processors		
Yuan Xiao, Xiaokuan Zhang, Yinqian Zhang, and Radu Teodorescu, <i>The Ohio State University</i>	Ashay Rane, Calvin Lin, and Mohit Tiwari, <i>The University of Texas at Austin</i>	Available Media	

7. 点击每篇文章，你会看到具体的细节如下：论文题目、摘要等。
- 有的会议还题目了论文下载链接、Slides、演讲视频等。如果未提供论文下载链接，请自行搜索下载。通常，也可到作者主页里去下载论文和 Slides。建议经常看论文作者主页，通常里面有很多相关论文及资源。


Flip Feng Shui: Hammering a Needle in the Software Stack

Authors:

Kaveh Razavi, Ben Gras, and Erik Bosman, *Vrije Universiteit Amsterdam*; Bart Preneel, *Katholieke Universiteit Leuven*; Cristiano Giuffrida and Herbert Bos, *Vrije Universiteit Amsterdam*

Open Access Content

USENIX is committed to Open Access to the research presented at our events. Papers and proceedings are freely available to everyone once the event begins. Any video, audio, and/or slides that are posted after the event are also free and open to everyone. [Support USENIX](#) and our commitment to Open Access.

 [Razavi PDF](#)

 [View the slides](#)

 [BibTeX](#)

Abstract:

We introduce Flip Feng Shui (FFS), a new exploitation vector which allows an attacker to induce bit flips over *arbitrary* physical memory in a *fully controlled way*. FFS relies on hardware bugs to induce bit flips over memory and on the ability to surgically control the physical memory layout to corrupt attacker-targeted data anywhere in the software stack. We show FFS is possible today with very few constraints on the target data, by implementing an instance using the *Rowhammer bug* and *memory deduplication* (an OS feature widely deployed in production). Memory deduplication allows an attacker to reverse-map any physical page into a virtual page she owns as long as the page's contents are known. Rowhammer, in turn, allows an attacker to flip bits in controlled (initially unknown) locations in the target page.

We show FFS is extremely powerful: a malicious VM in a practical cloud setting can gain unauthorized access to a co-hosted victim VM running OpenSSH. Using FFS, we exemplify end-to-end attacks breaking OpenSSH public-key authentication, and forging GPG signatures from trusted keys, thereby compromising the Ubuntu/Debian update mechanism. We conclude by discussing mitigations and future directions for FFS attacks.

Presentation Video

