Kevin P. Dyer

www: https://kpdyer.com **email:** kpdyer@gmail.com **github:** https://github.com/kpdyer

KEVIN IS...

- A Software Engineer at Google working in Security and Privacy.
- A pragmatic, experienced (10 years in industry) engineer that embraces complex technical/business challenges.
- Proud to be a core member of projects featured in high-profile venues (e.g., MIT Tech Review, TEDx) and deployed to millions of users.

INDUSTRY

CURRENT ROLE

2015 - now **Software Engineer**, Google, Mountain View, CA, USA
I build/deploy secure infrastructure and cryptography at the scale of Google.

PREVIOUS ROLES

2014 (intern) **Software Engineer**, Google / University of Washington
Peer-to-peer networking, nodejs, C++, Cryptography, JavaScript

2013 (intern) **Research Scientist**, RedJack, Silver Spring, MD, USA
Network security, Python, Cryptography, Multi-threaded programming

2010 - 2015 [Ph.D. Student]

2008 - 2010 **Software Engineer**, NDS, Staines, UK
- *Web app with 1M+ users*, PHP, Oracle, CSS, JavaScript, Java
- *In-browser DRM*, C++, Python, DRM, DirectX
- *Backend Crypto Infrastructure*, Java, XML

2007 - 2008 **Software Engineer**, Imagineer Systems, Guildford, UK
VFX Suite for Film/TV Post Production, C++, Qt, PostgreSQL

2006 - 2007 **Software Engineer**, Connect Express Consultants, Staines, UK
Various projects, C++, MySQL, Telephony/SMS, Asterisk PBX

2002 - 2007 [B.S., M.Sc. Student]

OPEN SOURCE

PROJECT MAINTAINER

- **libfte**, Python, C++, JavaScript APIs, https://github.com/kpdyer/libfte
  A library for constructing format-abiding encryption schemes, using regular expressions.
- **regex2dfa**, C++, JavaScript APIs, https://github.com/kpdyer/regex2dfa
  A C++ API and command-line tool for converting a regular expression into a DFA.
- **fteproxy**, Python, https://fteproxy.org
  A TCP proxy that transmits messages that conform to a user-specified regular expression.
- **marionette**, Python, https://github.com/kpdyer/marionette
  A TCP proxy that allows users to have fine-grained control over traffic features such as connection duration, number of messages sent, and message format using libfte.

PREVIOUS ROLES

- **The Tor Project**, (2013-2015) Developer of the FTE pluggable transport. QA of pluggable transport and bridge features.

Academia

Degrees

2015 **Ph.D., Computer Science**
Portland State University

2007 **M.Sc. with Distinction, Mathematics of Cryptography and Communications**
Royal Holloway, University of London

2006 **B.S., Computer Science with Mathematics**
Santa Clara University

Impact

I pursue research that has important, practical applications. As an example, I'm one of the creators behind Format-Transforming Encryption, a new type of encryption that's being used for **censorship circumvention** in countries like Iran and China.

In addition, I have also done research on traffic analysis of encrypted communications. This work focuses on applications such as Apple's iMessage and WhatsApp, and analyzes the information they leak via encrypted communications — this work was featured in the **MIT Technology Review**.

Accolades

- Awarded a surprise gift of **$100,000** from Google Chairman Eric Schmidt to Portland State University, for the creation of Format-Transforming Encryption.
- Awarded a grant of **$16,000** for fteproxy, the Format-Transforming Encryption open-source proxy system.

Publications

7. Wang, L., **Dyer K.P.**, Aditya A., Ristenpart T., Shrimpton T. *Seeing through Network-Protocol Obfuscation*, In proceedings of the ACM Conference on Computer and Communications Security (CCS), 2015.
(Acceptance rate: 20%)
6. **Dyer K.P.**, Coull S.E., Shrimpton T. *Marionette: A Programmable Network Traffic Obfuscation System*, USENIX Security 2015.
(Acceptance rate: 15%)
5. Coull, S.E. and **Dyer K.P.** *Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond*, SIGCOMM Computer Communications Review, October 2014.
(Acceptance rate: $<$15%)
4. Luchaup D., **Dyer K.P.**, Jha S., Ristenpart T., Shrimpton T. *LibFTE: A Toolkit for Constructing Practical, Format-Abiding Encryption Schemes*, USENIX Security 2014.
(Acceptance rate: 19%)
3. **Dyer K.P.**, Coull S.E., Ristenpart T., Shrimpton T. *Protocol Misidentification Made Easy with Format-Transforming Encryption*, In proceedings of the ACM Conference on Computer and Communications Security (CCS), 2013.
(Acceptance rate: 20%)
2. **Dyer K.P.**, Coull S.E., Ristenpart T., Shrimpton T. *Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail*, In Proceedings of the 33rd IEEE Symposium on Security and Privacy, 2012.
(Acceptance rate: 13%)
1. **Dyer K.P.** and Schaefer, E.F. *Linear cryptanalysis of two round 16 step MD5 over the rationals*, In Proceedings of the Southern African Mathematical Sciences Association, 2005.
(Acceptance rate: unknown)