NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2017-230 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
ROBERT L. KAMINSKI
Work Unit Manager

/ S /
WARREN H. DEBANY JR.
Technical Advisor, Information
Exploitation and Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
NOV 2017	FINAL TECHNICAL REPORT	FEB 2016 – MAY 2017

4. TITLE AND SUBTITLE

PRiFi NETWORKING FOR TRACKING-RESISTANT MOBILE COMPUTING

5a. CONTRACT NUMBER
FA8750-16-2-0034

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Joan Feigenbaum

5d. PROJECT NUMBER
DHS1

5e. TASK NUMBER
4Y

5f. WORK UNIT NUMBER
AL

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Yale University
51 Prospect St
New Haven CT 06511-8937

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIG
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2017-230

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As the most serious cyber-attack threats rapidly shift from untargeted toward increasingly targeted methods, it is becoming correspondingly more crucial for organizations to protect the identity and location-privacy of their members against malicious tracking and surveillance. We propose to develop PriFi, an anti-tracking and location-private network access mechanism to protect members of an organization both while on-site (via privacy-protected WiFi networking) and while off-site (via privacy-protected Virtual Private Networking or VPN).

15. SUBJECT TERMS
Anonymity; Location privacy; Tracking resistance

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**ROBERT L. KAMINSKI**
U	U	U	SAR	15	19b. TELEPHONE NUMBER (*Include area code*)

TABLE OF CONTENTS

Section **Page**

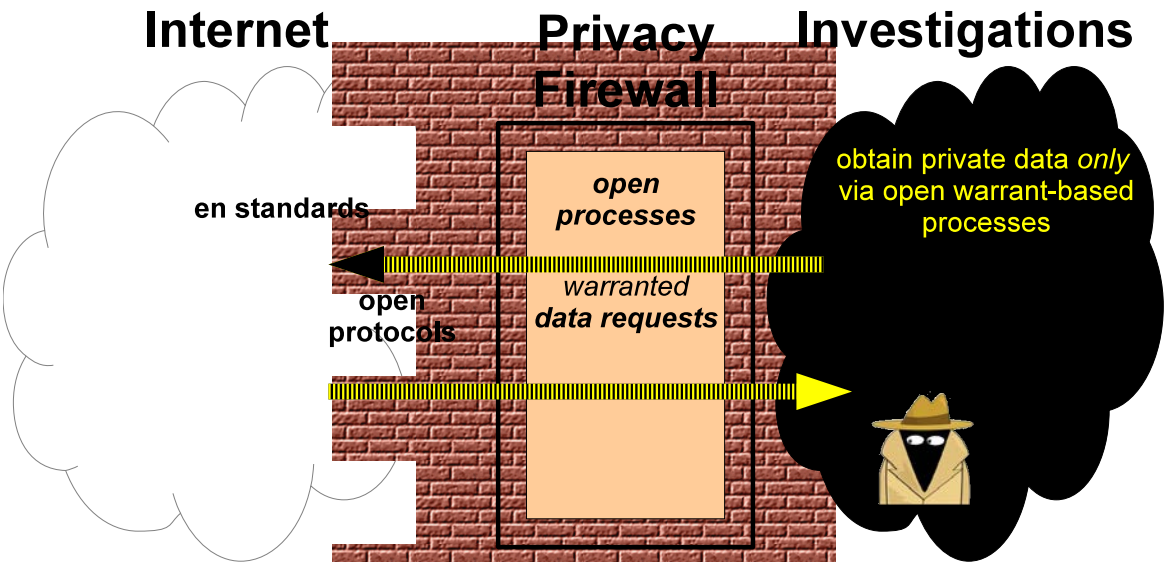

Figure 3: What We Require: Open Warrant-Based Processes for Lawful Electronic Surveillance, Creating a "Privacy Firewall"

Since beginning the PriFi project, we have expanded this work to include an investigation of *contact chaining*, which is also a standard tool of law enforcement and intelligence. The goal is to use the topology of a communication graph (*e.g.*, a phone-call graph, email graph, or social network) to identify associates (or "contacts") of lawfully targeted users. Agencies can then investigate those associates to determine whether they deserve further attention. It is useful to consider both direct contacts, *i.e.*, users who are neighbors in the communication graph, and extended contacts, *i.e.*, users who are at distance k in the communication graph, for an appropriate constant k. Without mechanisms to limit an investigation's scope, contact chaining in a mass-communication network can sweep in a huge number of untargeted users.

We present an accountable contact-chaining protocol that bounds the scope of the search, uses encryption to protect untargeted users, and is efficient, with time and communication complexity linear in the size of the output. Experiments show that a three-hop, privacy-preserving graph traversal producing 27,000 ciphertexts can be done in under two minutes.

For a more detailed account, please refer to [10].

5.0 CONCLUSIONS

PriFi is a very promising approach to low-latency, tracking-resistant, local-area networking and could be a critical component of a next-generation communications infrastructure that supports both personal privacy and national security. Preliminary experiments indicate that its performance is good enough to be used in real-life applications, with reasonably high throughput. PriFi's novel client/relay/server architecture and demanding use of DC-nets are interesting system features.

6.0 REFERENCES

[1] R. Dingledine, N. Mathewson, and P. Syverson. **Tor: The Second-Generation Onion Router.** 13th USENIX Security Symposium, 2004.

[2] D. Wolinsky, H. Corrigan-Gibbs, B. Ford, and A. Johnson. **Dissent in Numbers: Making Strong Anonymity Scale.** 10th USENIX Symposium on Operating Systems Design and Implementation, 2012.

[3] L. Barman, M. Zamani, I. Dacosta, J. Feigenbaum, B. Ford, J.-P. Hubaux, and D. Wolinsky. **PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication.** 15th ACM Workshop on Privacy in the Electronic Society, 2016.

[4] J. Weber. **Analysis of Scheduling Algorithms for PriFi.** Thesis: Master in Communication Systems, EPFL, 2017.

[5] Analysis of the PriFi Protocol. Unpublished manuscript, 2017.
URL: http://www.cs.yale.edu/homes/jf/xxAnalysisxx.pdf. Accessed June 29, 2017.

[6] Shadow: Real Applications, Simulated Networks. URL: http://shadow.github.io/. Accessed June 29, 2017.

[7] A. Johnson, R. Jansen, A. Jaggard, J. Feigenbaum, and P. Syverson. **Avoiding the Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection.** 24th Symposium on Network and Distributed System Security, 2017.

[8] E. Syta, P. Jovanovic, E. Kogias, N. Gailly, L. Gasser, I. Khoffi, M. Fischer, and B. Ford. **Scalable Bias-Resistant Distributed Randomness.** 38th IEEE Symposium on Security and Privacy, 2017.

[9] A. Segal, B. Ford, and J. Feigenbaum. **Catching Bandits and *Only* Bandits: Privacy-Preserving Intersection Warrants for Lawful Surveillance.** 4th USENIX Workshop on Free and Open Communications on the Internet, 2014.

[10] A. Segal, J. Feigenbaum, and B. Ford. **Privacy-Preserving Lawful Contact Chaining.** 15th ACM Workshop on Privacy in the Electronic Society, 2016.

7.0 APPENDIX AND BIBLIOGRAPHY

Published Papers, MS Thesis, and Unpublished Manuscript (Each Included Below)

Analysis of the PriFi Protocol. Unpublished manuscript, 2017.
URL: http://www.cs.yale.edu/homes/jf/xxAnalysisxx.pdf. Accessed June 29, 2017.

L. Barman, M. Zamani, I. Dacosta, J. Feigenbaum, B. Ford, J.-P. Hubaux, and D. Wolinsky. **PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication.** 15th ACM Workshop on Privacy in the Electronic Society, 2016.

A. Johnson, R. Jansen, A. Jaggard, J. Feigenbaum, and P. Syverson. **Avoiding the Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection.** 24th Symposium on Network and Distributed System Security, 2017.

A. Segal, J. Feigenbaum, and B. Ford. **Privacy-Preserving Lawful Contact Chaining.** 15th ACM Workshop on Privacy in the Electronic Society, 2016.

E. Syta, P. Jovanovic, E. Kogias, N. Gailly, L. Gasser, I. Khoffi, M. Fischer, and B. Ford. **Scalable Bias-Resistant Distributed Randomness.** 38th IEEE Symposium on Security and Privacy, 2017.

J. Weber. **Analysis of Scheduling Algorithms for PriFi.** Thesis: Master in Communication Systems, EPFL, 2017.

LIST OF ACRONYMS

BFT	Byzantine Fault Tolerance
DARPA	Defense Advanced Research Projects Agency
DC-nets	Dining-Cryptographers Networks
EPFL	Ecole Polytechnique Federale de Lausanne
UT	University of Texas
VPN	Virtual Private Network