

# JOSEPH C. BONNEAU

PO Box 234, Ross, CA, 94957

www.jbonneau.com

(650) 804-6934; jbonneau@gmail.com

## EDUCATION

### **University of Cambridge**—Cambridge, UK

*Doctor of Philosophy, Expected 2011, Computer Laboratory, Department of Computer Science*

- 2008 Gates Cambridge Scholar
- Member of Churchill College

### **Stanford University**—Stanford, CA

*Master of Science, March 2007, Computer Science, Specialization in Cryptography and Computer Security*

- GPA: 4.19/4.00
- GRE General Test: 800/800 Quantitative 720/800 Verbal 6.0/6.0 Writing
- GRE Computer Science Test: 880 (99<sup>th</sup> percentile)
- Teaching Assistant: Discrete Mathematics, Introductory Programming, Software Project

### **Stanford University**—Stanford, CA

*Bachelor of Science, degree conferred with distinction on June 2006, Computer Science Major*

- Frederick E. Terman Engineering Scholastic Award (top 5% of School of Engineering)
- Major GPA: 4.14/4.00 Overall GPA: 4.03/4.00
- Relevant coursework: cryptography, security, finite-state model checking, operating systems, compilers, databases, algorithms, complexity theory, AI, computer architecture, physics, multivariable calculus, differential equations, number theory, group theory.

## RESEARCH

### **Cache-Collision Timing Attacks Against AES**

- Published in *2006 Workshop on Cryptographic Hardware and Embedded Systems*
- Presented to conference October 12, 2006 in Yokohama, Japan
- Improvement over previous best known AES timing attacks by  $\sim 1,000$  times

### **Robust Final Round Cache-Trace Attacks Against AES**

- Published in IACR Cryptology ePrint Archive, Report # 374, 2006
- Improved robustness of previous attacks to noise and proved optimality

### **Finite State Security Analysis of “Off The Record” Messaging**

- Discovered multiple security flaws in instant messaging encryption protocol

## WORK EXPERIENCE

### **Cryptography Research, Inc.**—San Francisco, CA

*Cryptographic Scientist, April 2007–May 2008*

- Researched differential power analysis attacks and countermeasures.
- Experience with cryptographic algorithms, embedded devices, and electronics.
- Developed obfuscation techniques for Blu-Ray discs
- Performed security evaluations of consumer electronics products
- Developed training materials and tutorials.
- Contributed to other designs and consulting projects.

**Microsoft Corporation**—Redmond, WA  
*Software Development Intern, June 2006–September 2006*

- Integrated smart card support into binary obfuscation tool.
- Performed security analysis of existing tool.

**Federal Bureau of Investigation**—Washington, DC  
*Honors Intern, June 2005–August 2005*

- Designed and developed secure software for document management application.

**Integration Appliance, Inc. (formerly Tsunami Software)**—Palo Alto, CA  
*Intern, Software Development, June 2004–August 2004*

- Developed GUI for database management application using Java, Swing.

## SKILLS & MISCELLANEOUS

**Programming Languages:** BASIC, C, C++, Java, SQL, LISP, MIPS Assembly, HTML

**Tools:** CVS, Make, gdb, Sun Cryptographic Extensions, Bash scripting

**Operating Systems:** Windows NT/98/2000/XP, Unix, Linux

**Software:** Word, Excel, Powerpoint, LaTeX, 70 WPM typing

**Security Clearance:** U.S. Government Top Secret (FBI, April 2005)

**Foreign Language:** Proficient in French

**Aviation:** FAA Private Pilot's Certificate, High Performance Aircraft Rated

## ATHLETICS

Stanford Ice Hockey 2002-2005

Stanford Intramural Football champion, 2005

Stanford Intramural Dodgeball champion, 2005

Redwood High School Varsity Water Polo

Redwood High School Varsity Swimming

Tamalpais Union Rugby

## HIGH SCHOOL ACADEMICS

Redwood High School Class of 2002, Larkspur, CA

GPA: 4.42/4.00 (ranked 2<sup>nd</sup> of 417)

SAT: 1530 (800 Math, 730 Verbal)

SATII: 800 Math IIC, 800 US History, 780 Writing, 770 Chemistry

AP Computer Science, Physics, Calculus, European History, US History

2002 National Merit Scholar

2002 Robert C. Byrd Scholar

North Coast Scholar Athlete 1998-2002

California State Scholarship Federation-Lifetime Member

Redwood Honor Society-Lifetime Member

American High School Math Exam-school top score, 2001

High Honors, Golden State Exam-Biology, Geometry, Algebra, US History

National Latin Examination "Magna Cum Laude," 1999-2001