All software is political. Technology shapes the course of our world and lines of code are votes for a particular future.

*Working on Signal iOS, 2013*
Tuesday, September 22
3:29
Signal 2m ago
New Message!
slide to view
Bruce Schneier is an internationally renowned security technologist, called a "security guru" by The Economist. He is the author of twelve books—including his seminal work, Applied Cryptography: Protocols, Algorithms, and Source Code in C—and Secrets and Lies: Digital Security in a Networked World as well as hundreds of articles, essays, and academic papers. His influential newsletter, "Schneier on Security," is read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation’s Open Technology Institute, a board member of the Electronic Frontier Foundation, and an advisory board member of the Berkow Information Center. He is also the Chief Technology Officer of Rapid7 Systems, Inc. You can read his blog, essays, and academic papers at www.schneier.com. He tweets at @schneiers.

**Preface for**

**APPLIED CRYPTOGRAPHY**

"This book should be on the shelf of any computer professional involved in the use or implementation of cryptography."

— IEEE Software

"An encyclopedic survey...could well have been subtitled 'The Joy of Encrypting'...a useful addition to the library of any active or would-be security practitioners."

— Cryptologia

"...the best introduction to cryptography I’ve ever seen...The book the National Security Agency wanted never to be published..."

— Wired Magazine

"...easily ranks as one of the most authoritative in its field..."

— PC magazine

"...monumental...fascinating...comprehensive...the definitive work on cryptography for computer programmers..."

— Dr. Dobb’s Journal

Written by the world’s most renowned security technologist, this 20th Anniversary Edition celebrates 20 years for the most definitive reference on cryptography ever published, **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. World-class security experts will find a compelling introduction for author Bruce Schneier and then specific tools for the professional edition.

Included in this edition:

- Exclusive forward by Bruce Schneier
- Ways to defeat the key exchange mechanism
- Encryption algorithms, including algorithms from the former Soviet Union and South Africa, and the RC4 stream cipher
- Protocols for digital signatures, authentication, secure negotiations, digital cash, and more
- Detailed information on key management and cryptographic implementations

This smart, relevant guide is a must for all those committed to computer and cyber security. Bruce Schneier covers general classes of cryptographic protocols and their specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems.

This book includes source-code listings and extensive advice on the practical aspects of cryptographic implementation, such as the importance of generating truly random numbers and keeping keys secure. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems.
AXOLOTL PROTOCOL
AN ILLUSTRATED PRIMER
<table>
<thead>
<tr>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0040</td>
<td>86</td>
</tr>
<tr>
<td>0050</td>
<td>d0</td>
</tr>
<tr>
<td>0060</td>
<td>67 69</td>
</tr>
<tr>
<td>0070</td>
<td>76 65 63 65 73 73 5f 74 6f 6b 65 6e 3d</td>
</tr>
</tbody>
</table>
Open Source

- Open Content
- Open Data
- Open Research
- Open Knowledge
- Open Education
- Open Health
- Open Innovation
- Open Music
- Open Standards
- Open Space
- Open Hardware
- Open Government
- Open Access
- Open Cloud
- Open Business
we need more people to participate in the technological “do-ocracy.” we cannot afford to gerrymander.

Working on Signal iOS, 2013
APPS THAT FIGHT RAPE

Move over, Mace, there’s a new high-tech way to protect women from sexual violence

Unwilling to tolerate rampant sexual attacks in the Indian capital of Delhi, where one of every four rapes in the country occurs, a local nonprofit has devised an ingenious way to keep women safe: the “Fight Back” phone app. Acting as an SOS device, the program sends a text with the user’s GPS location to up to five people, including the police, and as a post on Facebook and Twitter. “Even if the fear is that police are apathetic toward the problems of the people, your own friends and family will respond immediately,” says Hindol Sengupta, cofounder of Whypoli, the “citizen networking” organization that designed the app.

For women in the U.S., the Department of Health and Human Services announced the development of two antiviolence apps: Circle of 6 will allow the user to alert six emergency contacts, and OnWatch will give women immediate access to 911 and campus police and dispatch their exact locations through GPS. Both are expected to be available as free downloads at the App Store in early 2012. —Lauren N. Williams
A New App You Must Download Now

Called Circle of 6, this free app—it won first place in a contest sponsored by Vice President Joe Biden—helps you out of tricky social area and need a ride. Tap the car icon and a text goes out to six people you’ve previously chosen, asking for a lift and pulling your whereabouts from your phone’s GPS. Or suppose you’re desperate for a quick way out of talking to a creeper who’s cornered you at a party. A tap on the phone icon asks the same six names for a phone call pretending they need you.

It’s not for life-threatening scenarios; that’s where 911 comes in.
MAY THE SOURCE BE WITH YOU!
more evidence of #immigration turmoil in science: Prof unable to close hire of French Postdoc with Iranian heritage b/c they had other opt

4:34 PM - 3 Mar 2017
more evidence of #immigration turmoil in science: postdoc at Caltech choosing to leave US for another job early b/c immigration uncertainty
4:34 PM - 3 Mar 2017
Culture is more important than code, but code shapes culture.

November, 2016
Choosing not to be political is not a choice everyone can make.

November, 2016
<table>
<thead>
<tr>
<th>Purpose</th>
<th>OS X</th>
<th>Ubuntu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit text files</td>
<td>TextMate</td>
<td>Sublime</td>
</tr>
<tr>
<td>Organize Research papers</td>
<td>Papers.app</td>
<td>Mendeley</td>
</tr>
<tr>
<td>Resize windows on grid</td>
<td>SizeUp</td>
<td>CompizConfig Settings Manager</td>
</tr>
<tr>
<td>Site specific browser (standalone web apps)</td>
<td>Fluid</td>
<td>Google Chrome Shortcuts</td>
</tr>
<tr>
<td>Multiple desktops</td>
<td>Native</td>
<td>Unity tweak tool</td>
</tr>
</tbody>
</table>
After being away for 1 year, so exciting to see how many more friends I can talk to on #Signal @whispersystems
We are in a post-truth society. If every scientist/engineer behaved like this? Truth is not a function of number of views. It exists.

1:29 AM - 9 Nov 2016
I have not yet developed my position on @wikileaks. I have the cables, the internet, now where to start? where to finish?

5:31 AM - 4 Dec 2010
I like things thorough btw. before taking positions on Middle East affairs, I spent 4 years reading, studied Arabic, Hebrew, moved there 2x
A week ago I hatched a plan to educate myself in a more structured manner on what exactly Wikileaks stands for, its history, and its possible futures with the idea of developing a more concrete and informed opinion (and since I have a habit of taking action with respect to my opinions, thereby guiding my future actions). After seeking some advice about what to read via twitter and starting with this Julian Assange essay as a basis—a very good one for some philosophical background of the larger aims, I spent awhile digesting the Wikipedia page on Wikileaks before deciding I wanted to fact check its assertions and that its references might serve as a springboard the next step in my studies.
inclusive empowering in open source will positively shape our social landscape moving forward and change our political landscape

11:00 AM - 4 Mar 2017