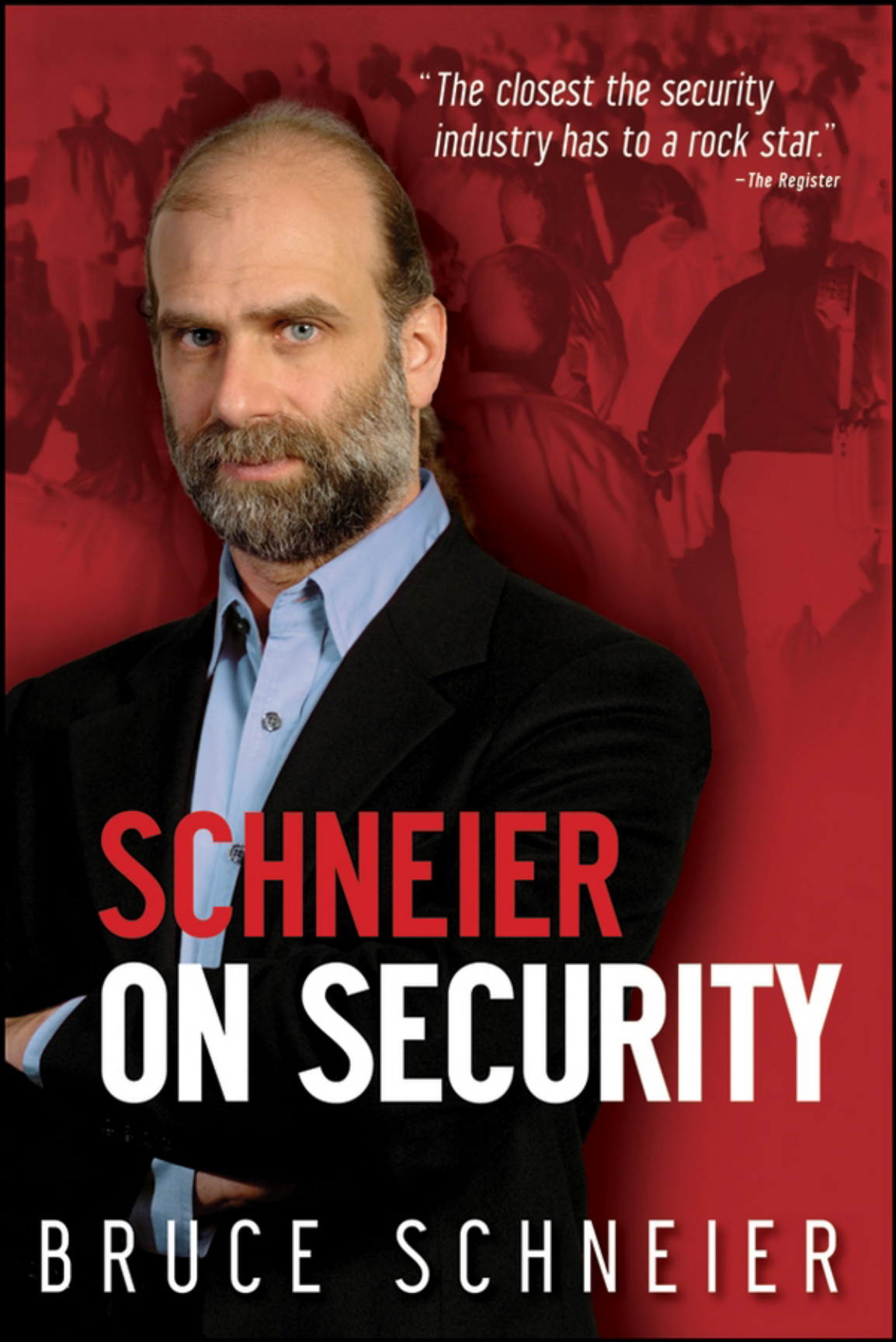
"The closest the security industry has to a rock star."
–The Register
SCHNEIER
ON SECURITY
BRUCE SCHNEIER

Schneier on Security

Bruce Schneier

Wiley Publishing, Inc.

Schneier on Security

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-39535-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

To Beth

Credits

Executive Editor
Carol Long

Senior Development Editor
Tom Dinse

Production Editor
Elizabeth Ginns Britten

Copy Editor
Kim Cofer

Editorial Manager
Mary Beth Wakefield

Production Manager
Tim Tate

Vice President and Executive Group Publisher
Richard Swadley

Vice President and Executive Publisher
Joseph B. Wikert

Project Coordinator, Cover
Lynsey Stanford

Compositor
Maureen Forys, Happenstance Type-O-Rama

Proofreader
C.M. Jones

Indexer
Jack Lewis

Cover Designer
Michael Trent

Cover Photo
© Steve Woit

Contents

Introduction

This book is a collection of essays on security: on security technology, on security policy, on how security works in the real world. Some are about specific technologies, like voting machines or national ID cards. Some are about specific targets, like airplanes or the Olympics. And some are about general trends, like increasing complexity or human behavior.

All have been published before—between June 2002 and June 2008—in newspapers, magazines, websites, and my own monthly e-mail newsletter *Crypto-Gram*.

Although I have grouped them by topic and have arranged them within those topics, they all stand alone and can be read in any order. (There is some overlap of material because it appeared in different locations for different audiences.) You don't even have to read this introduction first. Actually, it might be better if you read a few essays first, then returned once you started wondering who in the world I am and what authority I have to write this broadly about security.

I'm a security technologist. I've worked for many companies, small and large, both as an employee and as a consultant. Over the years, my career has been a series of generalizations: from cryptography and mathematical security to computer and network security, and from there to more general security technology. More recently, I've been researching and writing about the interaction between security technology and people: the economics of security and, most recently, the psychology of security.

It turns out that these human issues are the most important of all. Security is often about technology, but it's always about people. People are the reason security exists in the first place, and people are at the core of any security breach. Technology helps—both the attacker and defender, actually, although in different ways—but security is fundamentally about people.

There are four points I want to make in this introduction, points you should keep in mind as you read the essays in this book and whenever you encounter anything security-related:

1. **Security is a trade-off.** There's no such thing as absolute security. Life entails risk, and all security involves trade-offs. We get security by

giving something up: money, time, convenience, capabilities, liberties, etc. Sometimes we make these trade-offs consciously, and sometimes we make them unconsciously.

2. **You are a security consumer.** You get to make these trade-offs, whether they be personal, corporate, national, or whatever. "Is this security measure effective?" is not a good question. It's much better to ask: "Is this a good trade-off?" These trade-offs are subjective. There's not always one answer, because not all costs are objective. Costs like inconvenience, time, and a feeling of security are subjective. Just as different consumers choose different cleaning products, different television shows, and different vacation destinations, different people will make different security trade-offs.
3. **Security is a system.** People often think of security in terms of specific attacks and defenses. But it's not that simple. Security is always part of a system, and that system is always more complex than the individual components. Identification systems are much more than the ID card. Bank vault security is more than the metal box. Whatever the system is, security should always be analyzed in the context of the broader system.
4. **Technology causes security imbalances.** The thing about technology is that it changes trade-offs. It makes something cheaper, or more expensive; faster, or more time-consuming. Technological advances can make some attacks easier, or it can make some defenses easier. In today's rapidly changing technological world, it is important to watch for new security imbalances.

Much of this book consists of common-sense, although often uncommon, application of these four principles.

If you're done and want to read more, I have two recommendations. The first is my previous book, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World,* first published in 2003. The second is to subscribe to my free monthly e-mail newsletter, *Crypto-Gram.* You can also visit my blog and wander through my pages of essays. The newsletter, the blog, and information about my books are all at `http://www.schneier.com/`.

1 Terrorism and Security

What the Terrorists Want

Originally published in Wired, *24 August 2006*

On August 16, two men were escorted off a plane headed for Manchester, England, because some passengers thought they looked either Asian or Middle Eastern, might have been talking Arabic, wore leather jackets, and looked at their watches—and the passengers refused to fly with them on board. The men were questioned for several hours and then released.

On August 15, an entire airport terminal was evacuated because someone's cosmetics triggered a false positive for explosives. The same day, a Muslim man was removed from an airplane in Denver for reciting prayers. The Transportation Security Administration decided that the flight crew overreacted, but he still had to spend the night in Denver before flying home the next day. The next day, a Port of Seattle terminal was evacuated because a couple of dogs gave a false alarm for explosives.

On August 19, a plane made an emergency landing in Tampa, Florida, after the crew became suspicious because two of the lavatory doors were locked. The plane was searched, but nothing was found. Meanwhile, a man who tampered with a bathroom smoke detector on a flight to San Antonio was cleared of terrorism, but only after having his house searched.

On August 16, a woman suffered a panic attack and became violent on a flight from London to Washington, so the plane was escorted to Boston's Logan Airport by fighter jets. "The woman was carrying hand cream and matches but was not a terrorist threat," said the TSA spokesman after the incident.

And on August 18, a plane flying from London to Egypt made an emergency landing in Italy when someone found a bomb threat scrawled on an air

sickness bag. Nothing was found on the plane, and no one knows how long the note was on board.

I'd like everyone to take a deep breath and listen for a minute.

The point of terrorism is to cause terror—sometimes to further a political goal, and sometimes out of sheer hatred. The people terrorists kill are not the targets; they are collateral damage. And blowing up planes, trains, markets, or buses is not the goal; those are just tactics. The real targets of terrorism are the rest of us: the billions of us who are not killed but are terrorized because of the killing. The real point of terrorism is not the act itself, but our reaction to the act.

And we're doing exactly what the terrorists want.

We're all a little jumpy after the recent arrest of 23 terror suspects in Great Britain. The men were reportedly plotting a liquid-explosive attack on airplanes, and both the press and politicians have been trumpeting the story ever since.

In truth, it's doubtful that their plan would have succeeded; chemists have been debunking the idea since it became public. Certainly the suspects were a long way off from trying: None had bought airline tickets, and some didn't even have passports.

Regardless of the threat, from the would-be bombers' perspective, the explosives and planes were merely tactics. Their goal was to cause terror, and in that they've succeeded.

Imagine for a moment what would have happened if they had blown up ten planes. There would be canceled flights, chaos at airports, bans on carry-on luggage, world leaders talking tough new security measures, political posturing and all sorts of false alarms as jittery people panicked. To a lesser degree, that's basically what's happening right now.

Our politicians help the terrorists every time they use fear as a campaign tactic. The press helps every time it writes scare stories about the plot and the threat. And if we're terrified, and we share that fear, we help. All of these actions intensify and repeat the terrorists' actions, and increase the effects of their terror.

(I am not saying that the politicians and press are terrorists, or that they share any of the blame for terrorist attacks. I'm not that stupid. But the subject of terrorism is more complex than it appears, and understanding its various causes and effects are vital for understanding how to best deal with it.)

The implausible plots and false alarms actually hurt us in two ways. Not only do they increase the level of fear, but they also waste time and resources

that could be better spent fighting the real threats and increasing actual security. I'll bet the terrorists are laughing at us.

Another thought experiment: Imagine for a moment that the British government had arrested the 23 suspects without fanfare. Imagine that the TSA and its European counterparts didn't engage in pointless airline security measures like banning liquids. And imagine that the press didn't write about it endlessly, and that the politicians didn't use the event to remind us all how scared we should be. If we'd reacted that way, then the terrorists would have truly failed.

It's time we calm down and fight terror with anti-terror. This does not mean that we simply roll over and accept terrorism. There are things our government can and should do to fight terrorism, most of them involving intelligence and investigation—and not focusing on specific plots.

But our job is to remain steadfast in the face of terror, to refuse to be terrorized. Our job is to not panic every time two Muslims stand together checking their watches. There are approximately 1 billion Muslims in the world, a large percentage of them not Arab, and about 320 million Arabs in the Middle East, the overwhelming majority of them not terrorists. Our job is to think critically and rationally, and to ignore the cacophony of other interests trying to use terrorism to advance political careers or increase a television show's viewership.

The surest defense against terrorism is to refuse to be terrorized. Our job is to recognize that terrorism is just one of the risks we face, and not a particularly common one at that. And our job is to fight those politicians who use fear as an excuse to take away our liberties and promote security theater that wastes money and doesn't make us any safer.

Movie-Plot Threats

Originally published in Wired, *8 September 2005*

Sometimes it seems like the people in charge of homeland security spend too much time watching action movies. They defend against specific movie plots instead of against the broad threats of terrorism.

We all do it. Our imaginations run wild with detailed and specific threats. We imagine anthrax spread from crop dusters. Or a contaminated milk supply. Or terrorist scuba divers armed with almanacs. Before long, we're envisioning an entire movie plot—without Bruce Willis to save the day. And we're scared.

Psychologically, this all makes sense. Humans have good imaginations. Box cutters and shoe bombs conjure vivid mental images. "We must protect the Super Bowl" packs more emotional punch than the vague "we should defend ourselves against terrorism."

The 9/11 terrorists used small pointy things to take over airplanes, so we ban small pointy things from airplanes. Richard Reid tried to hide a bomb in his shoes, so now we all have to take off our shoes. Recently, the Department of Homeland Security said that it might relax airplane security rules. It's not that there's a lessened risk of shoes, or that small pointy things are suddenly less dangerous. It's that those movie plots no longer capture the imagination like they did in the months after 9/11, and everyone is beginning to see how silly (or pointless) they always were.

Commuter terrorism is the new movie plot. The London bombers carried bombs into the subway, so now we search people entering the subways. They used cell phones, so we're talking about ways to shut down the cell-phone network.

It's too early to tell if hurricanes are the next movie-plot threat that captures the imagination.

The problem with movie-plot security is that it only works if we guess right. If we spend billions defending our subways, and the terrorists bomb a bus, we've wasted our money. To be sure, defending the subways makes commuting safer. But focusing on subways also has the effect of shifting attacks toward less-defended targets, and the result is that we're no safer overall.

Terrorists don't care if they blow up subways, buses, stadiums, theaters, restaurants, nightclubs, schools, churches, crowded markets or busy intersections. Reasonable arguments can be made that some targets are more attractive than others: airplanes because a small bomb can result in the death of everyone aboard, monuments because of their national significance, national events because of television coverage, and transportation because most people commute daily. But the United States is a big country; we can't defend everything.

One problem is that our nation's leaders are giving us what we want. Party affiliation notwithstanding, appearing tough on terrorism is important. Voting for missile defense makes for better campaigning than increasing intelligence funding. Elected officials want to do something visible, even if it turns out to be ineffective.

The other problem is that many security decisions are made at too low a level. The decision to turn off cell phones in some tunnels was made by those

in charge of the tunnels. Even if terrorists then bomb a different tunnel elsewhere in the country, that person did his job.

And anyone in charge of security knows that he'll be judged in hindsight. If the next terrorist attack targets a chemical plant, we'll demand to know why more wasn't done to protect chemical plants. If it targets schoolchildren, we'll demand to know why that threat was ignored. We won't accept "we didn't know the target" as an answer. Defending particular targets protects reputations and careers.

We need to defend against the broad threat of terrorism, not against specific movie plots. Security is most effective when it doesn't make arbitrary assumptions about the next terrorist act. We need to spend more money on intelligence and investigation: identifying the terrorists themselves, cutting off their funding, and stopping them regardless of what their plans are. We need to spend more money on emergency response: lessening the impact of a terrorist attack, regardless of what it is. And we need to face the geopolitical consequences of our foreign policy and how it helps or hinders terrorism.

These vague things are less visible, and don't make for good political grandstanding. But they will make us safer. Throwing money at this year's movie plot threat won't.

Fixing Intelligence Failures

Originally published in Crypto-Gram*, 15 June 2002*

Could the intelligence community have connected the dots? Why didn't anyone connect the dots? How can we make sure we connect the dots next time? Dot connecting is the metaphor of the moment in Washington, as the various politicians scramble to make sure that 1) their pet ideas for improving domestic security are adopted, and 2) they don't get blamed for any dot connection failures that could have prevented 9/11.

Unfortunately, it's the wrong metaphor. We all know how to connect the dots. They're right there on the page, and they're all numbered. All you have to do is move your crayon from one dot to another, and when you're done you've drawn a lion. It's so easy a three-year-old could do it; what's wrong with the FBI and the CIA?

The problem is that the dots can only be numbered after the fact. With the benefit of hindsight, it's easy to draw lines from people in flight school here,