Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems

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

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-06852-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3

Library of Congress Cataloging-in-Publication Data
Anderson, Ross, 1956-
Security engineering : a guide to building dependable distributed systems / Ross J Anderson. — 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-06852-6 (cloth)
1. Computer security. 2. Electronic data processing–Distributed processing. I. Title.
QA76.9.A25A54 2008
005.1–dc22 2008006392

won the Nobel Prize in economics in 2002 for launching this field (along with the late Amos Tversky). One of his insights was that the heuristics we use in everyday judgement and decision making lie somewhere between rational thought and the unmediated input from the senses [679].

Kahneman and Tversky did extensive experimental work on how people made decisions faced with uncertainty. They developed *prospect theory* which models risk aversion, among other things: in many circumstances, people dislike losing $100 they already have more than they value winning $100. That's why marketers talk in terms of 'discount' and 'saving' — by *framing* an action as a gain rather than as a loss makes people more likely to take it. We're also bad at calculating probabilities, and use all sorts of heuristics to help us make decisions: we base inferences on familiar or easily-imagined analogies (the *availability heuristic* whereby easily-remembered data have more weight in mental processing), and by comparison with recent experiences (the *anchoring effect* whereby we base a judgement on an initial guess or comparison and then adjust it if need be). We also worry too much about unlikely events.

The channels through which we experience things also matter (we're more likely to be sceptical about things we've heard than about things we've seen). Another factor is that we evolved in small social groups, and the behaviour appropriate here isn't the same as in markets; indeed, many frauds work by appealing to our atavistic instincts to trust people more in certain situations or over certain types of decision. Other traditional vices now studied by behavioural economists range from our tendency to procrastinate to our imperfect self-control.

This tradition is not just relevant to working out how likely people are to click on links in phishing emails, but to the much deeper problem of the public perception of risk. Many people perceive terrorism to be a much worse threat than food poisoning or road traffic accidents: this is irrational, but hardly surprising to a behavioural economist, as we overestimate the small risk of dying in a terrorist attack not just because it's small but because of the visual effect of the 9/11 TV coverage and the ease of remembering the event. (There are further factors, which I'll discuss in Chapter 24 when we discuss terrorism.)

The misperception of risk underlies many other public-policy problems. The psychologist Daniel Gilbert, in an article provocatively entitled 'If only gay sex caused global warming', discusses why we are much more afraid of terrorism than of climate change. First, we evolved to be much more wary of hostile intent than of nature; 100,000 years ago, a man with a club (or a hungry lion) was a much worse threat than a thunderstorm. Second, global warming doesn't violate anyone's moral sensibilities; third, it's a long-term threat rather than a clear and present danger; and fourth, we're sensitive to rapid changes in the environment rather than slow ones [526].

Bruce Schneier lists more biases: we are less afraid when we're in control, such as when driving a car, as opposed to being a passenger in a car or

airplane; we are more afraid of risks to which we've been sensitised, for example by gruesome news coverage; and we are more afraid of uncertainty, that is, when the magnitude of the risk is unknown (even when it's small). And a lot is known on the specific mistakes we're likely to make when working out probabilities and doing mental accounting [1129, 1133].

Most of us are not just more afraid of losing something we have, than of not making a gain of equivalent value, as prospect theory models. We're also risk-averse in that most people opt for a bird in the hand rather than two in the bush. This is thought to be an aspect of *satisficing* — as situations are often too hard to assess accurately, we have a tendency to plump for the alternative that's 'good enough' rather than face the cognitive strain of trying to work out the odds perfectly, especially when faced with a small transaction. Another aspect of this is that many people just plump for the standard configuration of a system, as they assume it will be good enough. This is one reason why secure defaults matter[1].

There is a vast amount of material here that can be exploited by the fraudster and the terrorist, as well as by politicians and other marketers. And as behavioural psychology gets better understood, the practice of marketing gets sharper too, and the fraudsters are never far behind. And the costs to business come not just from crime directly, but even more from the fear of crime. For example, many people don't use electronic banking because of a fear of fraud that is exaggerated (at least in the USA with its tough consumer-protection laws): so banks pay a fortune for the time of branch and call-center staff. So it's not enough for the security engineer to stop bad things happening; you also have to reassure people. The appearance of protection can matter just as much as the reality.

2.3.3 Different Aspects of Mental Processing

Many psychologists see the mind as composed of interacting rational and emotional components — 'heart' and 'head', or 'affective' and 'cognitive' systems. Studies of developmental biology have shown that, from an early age, we have different mental processing systems for social phenomena (such as recognising parents and siblings) and physical phenomena. Paul Bloom has written a provocative book arguing that the tension between them explains why many people are natural dualists — that is, they believe that mind and body are basically different [194]. Children try to explain what they see using their understanding of physics, but when this falls short, they explain phenomena in terms of deliberate action. This tendency to look for affective

[1] In fact, behavioral economics has fostered a streak of libertarian paternalism in the policy world that aims at setting good defaults in many spheres. An example is the attempt to reduce poverty in old age by making pension plans opt-out rather than opt-in.

explanations in the absence of material ones has survival value to the young, as it disposes them to get advice from parents or other adults about novel natural phenomena. According to Bloom, it has a significant side-effect: it predisposes humans to believe that body and soul are different, and thus lays the ground for religious belief. This argument may not overwhelm the faithful (who can retort that Bloom simply stumbled across a mechanism created by the Intelligent Designer to cause us to have faith in Him). But it may have relevance for the security engineer.

First, it goes some way to explaining the *fundamental attribution error* — people often err by trying to explain things by intentionality rather than by situation. Second, attempts to curb phishing by teaching users about the gory design details of the Internet — for example, by telling them to parse URLs in emails that seem to come from a bank — will be of limited value if users get bewildered. If the emotional is programmed take over whenever the rational runs out, then engaging in a war of technical measures and countermeasures with the phishermen is fundamentally unsound. Safe defaults would be better — such as 'Our bank will never, ever send you email. Any email that purports to come from us is fraudulent.'

It has spilled over recently into behavioural economics via the *affect heuristic*, explored by Paul Slovic and colleagues [1189]. The idea is that by asking an emotional question (such as 'How many dates did you have last month?') you can get people to answer subsequent questions using their hearts more than their minds, which can make people insensitive to probability. This work starts to give us a handle on issues from people's risky behaviour with porn websites to the use of celebrities in marketing (and indeed in malware). Cognitive overload also increases reliance on affect: so a bank that builds a busy website may be able to sell more life insurance, but it's also likely to make its customers more vulnerable to phishing. In the other direction, events that evoke a feeling of dread — from cancer to terrorism — scare people more than the naked probabilities justify.

Our tendency to explain things by intent rather than by situation is reinforced by a tendency to frame decisions in social contexts; for example, we're more likely to trust people against whom we can take vengeance. (I'll discuss evolutionary game theory, which underlies this, in the chapter on Economics.)

2.3.4 Differences Between People

Most information systems are designed by men, and yet over half their users may be women. Recently people have realised that software can create barriers to females, and this has led to research work on 'gender HCI' — on how software should be designed so that women as well as men can use it effectively. For example, it's known that women navigate differently from men in the real world, using peripheral vision more, and it duly turns

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.