When Gadgets Betray Us: The Dark Side of Our Infatuation With New Technologies

Robert Vamosi

When Gadgets Betray Us: The Dark Side of Our Infatuation With New Technologies

Robert Vamosi

When Gadgets Betray Us: The Dark Side of Our Infatuation With New Technologies Robert Vamosi Technology is evolving faster than we are. As our mobile phones, mp3 players, cars, and digital cameras become more and more complex, we understand less and less about how they actually work and what personal details these gadgets might reveal about us.

Robert Vamosi, an award-winning journalist and analyst who has been covering digital security issues for more than a decade, shows us the dark side of all that digital capability and convenience. Hotel-room TV remotes can be used to steal our account information and spy on what we've been watching, toll-booth transponders receive unencrypted EZ Pass or FasTrak info that can be stolen and cloned, and our cars monitor and store data about our driving habits that can be used in court against us.

When Gadgets Betray Us gives us a glimpse into the secret lives of our gadgets and helps us to better understand - and manage - these very real risks.

When Gadgets Betray Us: The Dark Side of Our Infatuation With New Technologies Details

Date	:	Published March 29th 2011 by Basic Books
ISBN	:	9780465019588
Author	:	Robert Vamosi
Format	:	Hardcover 222 pages
Genre	:	Science, Technology, Nonfiction, Business, Adult

From Reader Review When Gadgets Betray Us: The Dark Side of Our Infatuation With New Technologies for online ebook

Phoenix says

De Bugs in Da Infrastructure

Vamosi presents a number of interesting examples of how different systems, including emergency broadcast signals, parking meters, cell phones, photocopiers (your potentially sensitive documents are now digitized and stored on a hard drive in the machine, which can be accessed later by a technician) and even medical implants were constructed without considering the need for strong encryption or security. The reason - a combination of a naivety towards human nature, ignorance, a desire for convenience, ease of access and cheapness. We tend to ignore the danger because earlier forms of the same device were pretty harmless. However when these same devices are can be accessed remotely either via networks or radio they can be invisibly compromised.

One problem is that we have traded convenience for security. For example cell phones contain identifying information used to track calls as we move between locations - which can also be used to track us. New passports contain RFID chips that can be read remotely, and though cracking the code is difficult, it's not impossible. And RFID'd products that we by in combination could be used in combination as a digital signature. Information on driver's licenses isn't even encoded - Vamosi warns you that when you present your drivers license as ID to a business, just show it, don't let it be swiped.

Another problem is increased complexity. We tend to feature up when buying new tech, even though we wind up not using most of the "must have" features. To some extent neither the manufacture nor the consumer knows which feature will be useful - which is why bigger bundles sell well. (I know the problem intimately as I'm looking for a new washer - I'm going to be stuck with my choice for years and the different digitized options are to say the least intimidating. ;-( ) However the more features the harder it is to test how they might behave in combination. Buying a web enabled TV might result in exposing your credit information to hackers. Or your phone or transponder bill may have a few extra charges from a device that fakes your id - how many of us check all the charges every month?

To some extent the companies who market these devices depend on "security by obscurity", and in defending their interests are hostile to towards attempts to expose security flaws. Replacing or upgrading hardware after it has been distributed in the marketplace is an extremely expensive operation. Vamosi points out that the GSM cell phone A5/1 protocol which was broken in 1998 (A5/2 was broken in 1999) took years to replace. He also describes a design flaw in cellular communications in that while cell phones have to identify themselves to the communication towers, current protocols don't require the towers to identify themselves to your phone. For the cost of a laptop and an antenna the person sitting next to you at the coffee shop may be spoofing a relay station and intercepting your calls using what is known as a "man in the middle" attack. Even if you use a more sophisticated protocol such as EDGE, many phones drop down automatically to older protocols when a high speed channel is not available, a condition which can bee spoofed.

This kind of information is both current and in some sense urgent. According to the author by 2008 the US military was aware that the ROVER protocol (implemented in 2001) used in it's spy drones and surveillance devices could be compromised at relatively low cost, both in terms of tapping into the video feed and in overwhelming it's control module. However retrofitting existing drones to the ROVER 6 protocol was not done due to the cost. Apparently the Iranians were aware of this too - on Dec 4th, 2001 they shot down a US

drone that had been operating over the Afghan-Iranian border the great embarrassment of the US. While the actual details are not known one scenario is that the drone was jammed while looking for insurgents on the Afghani side of the border, at which point it continued along its flight path into Iran where it was shot down.

A fascinating book with a lot more examples and than I've been able to touch upon here. Vamosi writes well and is able to communicate his ideas without a lot of technical jargon. Recommended to consumer advocates, police and security personnel, and those in technical or retail management who need to become better acquainted with current issues in security.

Desiree says

I really enjoyed this book! Everyone should be reminded to turn off their blue tooth connections, as anyone can connect to it! The author also points out the dangers of RFID chips, which are popping up all over. With a simple antenna, these signals can be picked up from very long distances!

Definitely a techie book, but, if you have been to defcon, you will find this WAY too elementary.... For the rest (most) of us, I think it is within reach. Another reviewer said that it is somewhat disorganized and I do have to agree. However, that did not prevent me from turning page after page!

I already knew a lot of the info, but I do love reading about techie things. What I did learn was well worth it! If you are at all interested in technology and gadgets, I would recommend you check this one out!

William Blair says

Definitely for techies. Folks who have no clue about crypto or simple electronics should not bother. That is unfortunate, because this book is the clearest exposition regarding the misuse of crypto and the lack of actual security in deployed authentication schemes (e.g., smart cards, RFID chips, SIM cards, etc.). I checked this out from the library, but will buy a couple dozen to distribute to folks whom I have not been able to convince of the dangers of computer systems with inadequately analyzed and designed security.

Emily McCune says

Hey, I tried -I got a few chapters into it but it just wasn't what I'd expected it to be. I was hoping for a little more of the philosophical angle of when technology fails us, but what this book posed was more actual, technical instances of GPS units not working, and how virtually any car can be stolen (as well as any lock picked), etc. Oh, and apparently it's easier now more than ever for your identity to be stolen...surprise surprise. I dunno - I plan on living so off-grid someday that I won't even NEED to worry about faulty home alarm systems or the beauty of anti-theft devices in cars (as I don't plan on owning one ever again).

The writing style was great, though. I'd be interested in reading more from this author - just less 'technology-geeky' stuff.

Stefan says

The author knows his stuff, although a fair amount was not new news to me. The problem is the writing itself - it's one citation after another of research showing the limitations of technology presented in tabloid-scare fashion that starts to get a little stale after the second chapter. Invariably, he'll spend pages ripping apart something only to follow it with a one sentence, "well this probably won't affect you" line. Also - another sign of poor writing - most of the chapters end with a ridiculous sentence like, "if you thought that was bad wait until you see what happens next chapter" So frustrating.

He could have improved this by spending equal time on problems and potential ideas for solutions. As I said, he's no dummy - obviously well- versed in the tech world, he would probably be more readable as a columnist.

Jon says

Somewhat of a disorganized mess of a book. The author had some good points to make, mostly requiring the reader to infer those points from hints scattered about.

There is some good, although in my estimation common sense, advice presented. Read the documentation about the gadgets you purchase. Don't depend solely on electronic security (lock your doors!) . But these are things that should be applied to our non-electronic possessions as well. I can't say that I couldn't take this author's work, replace all references to 'gadgets' with, say, chemical oven cleaners or circular saws, and provide much the same advice.

The discussion of implanted medical devices was the one area that truly seems worthy of the title of the book. A compromised cardiac pacemaker would indeed betray the owner. Sadly, thar section of the book was all too brief and didn't present any solution.

This book was *not* the anti-technology screed I was expecting. Neither was it all that useful.

Read the documentation for your gadget.

That will be $6.95 please. Don't bother to send a check... I already know your credit card number. (Kidding)

Warren Gossett says

This book gives useful surveys of security problems on the internet and mobile phones. There is no one size fits all solution to keeping our digital data and our electronically managed devices or possessions safe. The author explains how layering or multiple overlapping approaches are necessary to enhance security although we should not imagine that it will ever be perfect.

Nathan says

Vamosi is a PC World journalist and he has tackled the thorny subject of security and privacy problems with modern computing devices: phones, laptops, RFIDs, and so on. The book is a collection of horror stories (researchers silenced, locks picked, cars hacked), but I felt it lacked a synthesis: what are we supposed to do with this information, what changes should be made? We can't really live our lives in a different way, and the book had no call to arms for greater pre-release security checks or audits. As such, the book ended up being a necklace of woe with no clasp to make it hang together.

David says

This book is a compendium of the ways that modern gadgets can work against us. While the computer software world has matured in terms of improving security, the hardware world is a decade behind the times. Most of this is about security lapses--just about any gadget can be hacked, for nefarious purposes. And many people are simply not aware that some of these gadgets even exist! For example, personal information can be stolen digitally from a driver's license, if you give your license to a clerk to be swiped. Your passport and cell phone can be hacked without even physically giving them to somebody--they simply need to be in proximity to an RF gadget. Cars can be hacked, TV remote controls can be hacked, even pacemakers.

I thought it was interesting, that many manufacturers deny the existence of problems, and keep their (weak) security algorithms secret. If they were to publish their algorithms, then hackers with good intentions could try to break their security systems, and inform the companies about their weak points. The result would be much more secure systems.

The style of the book is quite technical and detail-oriented. The book serves as a warning, but the common person cannot do very much with all of this information. It really serves as a warning to a program director who is in charge of developing a gadget, that there should be multiple layers of security. So, it does not help the common reader (like me) very well.

Scottsdale Public Library says

When Gadgets Betray Us is a well-researched book on how the technologies people are using today, although making life more convenient, allows thieves easier access to our information and belongings. Vamosi covers everything from automotive anti-theft devices to biometrics in a book that brings to the forefront the dark side of technology.

-Michael S-

Yuto says

"When Gadgets Betray Us" describes the various types of technologies that on one hand can be convenient and on the other hand can be harmful. Additionally, this books mentions the different types of technologies

(all) that are susceptible to hackers. The only problem with this book is that there is just a chunk of information thrown at the reader. There isn't a real narrative nor analysis in this book. This book is a book of multiple sources used.

Anthony says

Even if this wasn't the best written book it was probably the most important. We go about our lives not realizing all the ways we are now offering our identity and tempting others to steal it from us. THis book really opened my eyes, not that I was naive but this covered things that I didn't even give a passing concern for. I may not make life altering changes from this but will be much more aware when using the technology daily.

Stan says

why do we think things have a desire or reason to betray us , they are designed by humans , employed by companies , to make money for their product. Humans aint perfect , why think that gizmos made by dudes are ?
Although we get into a lot of geek tech about how smart they are , and can beat the flaws , duh !
why dont you ask the age old question ,
how come antivirus programmers are so good at their day job?
as they have the night before to do virus programming

Yeeeeoooow

Mario says

I had the opportunity to finish this book last week while at work on a quiet,lonely night but even having more time at my disposal,I have to say that this book was not an easy read. As with most non-fiction with a technical insight this book was not a quick page turner but instead a detailed description using historical references and third-party anecdotes to demonstrate the vulnerability we citizens have when using our new technological gizmo. I initially found interest in reading this book because while I appreciate the usefulness technology can offer, I am dismayed by the dependency that this new technology age has fostered in the masses at large. This book highlighted many of the fears I have seen in laziness and ignorance that most consumers exercise when purchasing their new gadgets without the full knowledge of how it works. It offered many examples of information exposure and insecurity within most of our cellular and GPS networks. I recommend it to anyone wanting to know more about the risks involved when purchasing a new device.

D.M. Dutcher says

Decent book about how many gadgets, including ones you wouldn't think of, have serious technical and privacy vulnerabilities. The author's main point is that too many technologies that exist rely on security

through obscurity-by not being found out in the first place, and that it is relatively easy to hack them for nefarious means. He also towards the end looks at positive uses of these interconnected technologies, like reality mining and the shift to a central, mobile phone-based standard and various levels of privacy.

It's at its best describing how things as mundane as parking meters or pay-per-view hotel televisions can be hacked, but a big problem is that too many of the examples are only done so by very skilled hackers, either academic or private, or even proof-of-concept groups. This undercuts his argument about the dark side, because it's really only when that technology becomes wide spread or in government hands that the danger appears.

He also only briefly touches on the dangers of these technologies for privacy, and not well in my opinion. It's an all right book, but needs to be more philosophical and less nuts and bolts.
