Part I

The Problem

If you only know half the rules of a game, do you *think* you can win?

We need to understand what is wrong before we can fix it. But the problem is not always simple. When we deal with the Internet, it almost *never* is. We need to understand the *technical* aspects of the problem. What is computed, what is stored, how can what we want to do go wrong? And the *social*—how people think, how do they make mistakes? These people—that includes *both* the potential victims and their attackers—why *do* they do what they do? Then we need to understand the *structural* aspects of the problem. Who knows what? Who can detect abuse? Who can stop it?

We will begin the book by describing the *problem*. We will explain some commonly exploited vulnerabilities—and some that are just emerging. We will talk about how taking advantage of these will enable attacker to reach his goals. That, of course, forces us to also have to understand exactly what motivates the adversary. And, of course, we have to try to understand the capabilities and limitations of the attacker. *Then* we can start thinking about how to address the problems we perceive.

This book is not about the particular vulnerabilities or solutions we will describe. It is about connecting the dots. The Internet is changing, and so are the threats that are posed to it. Once we recognize this, it becomes natural that we also need to be able to anticipate trends. Security trends are driven by both *markets* (such as an increase of vulnerable devices) and *opportunities* (such as the ability to easily monetize stolen information).We will look at existing problems through the lens of what caused them. This will give us practice to anticipate what comes next, and be proactive.

The Death of the Internet, First Edition. Edited by Markus Jakobsson.

Chapter 1

What Could Kill the Internet? And so What?

Anything that makes the Internet either *dangerous* or *meaningless* could kill it.

The dangers may be to your machine, to proprietary information, to your financial situation, or even to *you*.

Malware can corrupt your machine. It can destroy data and software. It can even destroy hardware—for example, by rewriting your computer's EEPROM or flash memories so many times that they burn out. That takes only a few seconds per block, and if strategically chosen blocks are damaged, the hardware is rendered useless. Malware can also affect external equipment or processes as the em Stuxnet worm gave an example in 2010. It can be used to turn on the microphone of your phone, turning you into a walking eavesdropping bot—and you would not even know it! Malware is believed to commonly be used to be used to steal corporate and national secrets.

Most of the time, though, malware will only attempt to steal your money. That is the same goal as phishers have. And it is the same goal as scam artists have, attempting to convince their victims to send them money or merchandise. Often referred to as Nigerian scammers, these are certainly not all in Nigeria, although a surprisingly high number is.

The Internet—as well as wireless networks—can also be used to spy on people, to determine their location, for example. This can have direct physical consequences, whether the attack is mounted by a crazed expartner, political enemies, or common criminals. While this type of tracking is not commonly heard about today, it does not mean that it does not happen. And it certainly does not mean that it *cannot* happen. In fact, and as we describe in Section 6.1, it can be done on a grand scale without any significant investment.

Those are just a few examples of dangers that did not exist just a few years ago, and which soon may take up first-page newspaper space. There are also plenty of ways in which the Internet may become *meaningless*.

When we speak of spam, almost everybody thinks of unwanted email. A similar type of spam affects mobile communications—SMS spam. Voice spam is closely related to telemarketing. Instant messaging and online game messaging are also vulnerable to spam. But not all spam is about selling counterfeit Viagra or Rolexes. The term is also used to refer to other junk material, whether it is intended to fool search engines to rank particular pages higher than they otherwise would have. It can be used to manipulate reputations of

The Death of the Internet, First Edition. Edited by Markus Jakobsson.

sites and services—typically to make them look more attractive than they are, but sometimes used the other way to stab competitors. Spam is used to mean polluted peer-to-peer material—material that claims to be things it is not.

Spam is not the only source of pollution of information, though. Criminals can deceive news organizations to broadcast untruthful information. Given the increased competition to be first in online media, it is sometimes hard for journalists to balance the need to validate information—and to be first. Malware and spoofing can be used to make information appear to have originated with trusted sources. Criminals may benefit from the pollution of information in many ways. Politically, by sowing doubts and causing fear and confusion. Financially, by manipulating the markets.

The Internet could also become meaningless by becoming so dangerous that typical users restrain their activities and only dare to engage in a minimal manner.

But "meaningless" is in the eye of the beholder. Typical users would have one view of what could make the Internet meaningless. Service providers have a very different view. To online merchants, the Internet would be meaningless if nobody buys their products using it, or if it cannot be used to advertise products that are sold off-line. If this were to happen, advertising would plummet. Since many free services depend of advertisements, that type of development would affect them, and they would scale back or vanish. A lot of services we have come to take for granted fall into this category, starting with search engines, but also including online news services, many content distribution sites, email service providers (do you remember—we used to pay for email . . .) and other services, such as translation services, recommendation services, navigation services, consumer advice services . . . you name it, it is probably on the list.

So what happens if people do not dare to watch advertisements? Or if click-fraud runs rampant? It is the same end result. No advertisements . . . no services.

Severe attacks on the Internet will send shockwaves through society.

If your livelihood depends on the Internet—like mine does—then you are surely aware of what the impact would be to you of any severe problems with it. You know that you would not be happy if the Internet were crippled by fraud. But if that does not describe you, you might shrug, thinking that this is not such a big deal. After all, you may think, you can live just fine without reading the news online, and you can drive to the store instead of shopping online. Right? Wrong.

- "My phone will still work." Well, maybe not. *You* may not use VoIP services, but most phone calls are still routed over the Internet. If the Internet goes down, your phone goes dead. And so will the phone of your local 911 dispatcher.
- "My lights and heat will still work." Maybe. Maybe not. Our electricity infrastructure is almost as complex as the Internet. Power is routed to where it is needed. The production is ramped up and down to meet the demand. The failure of one part of the system can cause failures in other parts of the system. And since the coordination of this complex system is done using the Internet, even electricity delivery may suffer from severe attacks on the Internet.
- "I can still walk down to the grocery store and get what I need." Yes, you can. But what if their ordering system or delivery system depends on the Internet, or on companies who depend on the Internet? Will the shelves still be full? Maybe not.

- "I still have money in the bank." You may not lose your password to phishing or malware, but what if your bank clerk loses it—or accidentally leaks your mothers maiden name? It may take a while for you to get your money back. And what if the financial system is hampered by a lack of trust; by invalid trades; by general abuse?

Even if the Internet is not taken down by attacks, we may all be affected by rising levels of fraud.

You and I may have bulletproof antivirus software on our computers —and phones—and still be affected. For example, if people passing you on town have infected phones, these phones may render your phone useless simply by making phone calls or web accesses in dramatic quantities. It would be hard for you to get a connection when you want one.

If you use a Bluetooth enabled headset and let your phone be discoverable, then your phone can be tracked by infected phones in your neighborhood. In fact, it may not matter whether your phone is discoverable or not if nearby devices can eavesdrop on signals: your phone will send its Bluetooth device identifier in the clear.

But it is not all about phones. Do you use social networking? Many services will detect if you are online or not. You online/offline patterns may say a lot about you. Who you are, what you do.

Internet terrorism is easy, and we are weak.

So far, I have argued that online attacks may result in problems in society. In lack of trust, degradation of our infrastructure, increases of costs to do business. *But the consequences of online attacks could also be what invites abuse.* If a hostile country or organization wants to hurt us, they may find that the easiest way of doing it is by attacking the Internet. Our dependence on the Internet will *invite* attacks. We have already seen instances of massive cyber attacks, such as those on Estonia in 2007. We are not safe from such attacks. If anything, we may be more vulnerable to them, as our dependence on the Internet is greater—and increasing by the day.

Since 2001, we are all aware of terrorism. What makes it terrifying is not only its arbitrariness, but its asymmetric nature. A small number of dedicated aggressors can inflict massive damage and suffering to large numbers of victims. The terrorists, of course, do not attack us because it is *fun*—they do it to further their political agendas. From their point of view, what they do is justified by the needs.

Of course, every society does what they think is justified by their needs—if they think they can get away with it, at least. Now, imagine that you belonged to an organization that needed to send a strong signal to a society or organization you disagree with. You may not have a powerful army to engage to pressure your enemy with. But you have other, and simpler, ways. You can degrade their infrastructure—with the click of a mouse. You can cause severe interruptions, degrade their economy, spread fear and confusion. Would you be tempted to click? *Of course you would.* And if you would not, then somebody else in your organization surely would.

That is also what we are up against. It is not *only* about fraudsters trying to make a profit.