Introduction

When talk began a half-century ago about linking computers into a revolutionary new network, few imagined the possibility of a dark side. Designers foresaw the need to protect the network against potential intruders or military threats, but they didn't expect the Internet's own users would someday use the network to attack each other. Nor did they expect how popular and essential the Internet would become.

What began as an online community for a few dozen researchers to move information quickly and reliably now is accessible to an estimated 3 billion people who collectively use it to pursue a full range of human motives: good, bad and everything in between. The network itself, meanwhile, has not aged well. The Internet can appear as elegantly designed as a race car, but it's closer to an assemblage of "hacks" or "kludges," short-term fixes that were supposed to be replaced yet never were. They endure because they work, or at least work well enough.

The consequences play out across cyberspace every second of every day, as hackers exploit old, poorly protected systems to scam, steal and spy on a scale never before possible. The Internet's original design — fast, open and frictionless — is what allows their malicious code to wreak havoc so widely. The flaws they exploit often are well-known and ancient in technological terms, surviving only because of an industry-wide penchant for patching over problems rather than replacing the rot.

A rising waves of viruses, worms and hackers prompted a chorus of warnings in the 1990s as the Internet was exploding in popularity with the

arrival of the world wide web. But the federal government had neither the skill nor the will to do anything about it.

And now the vulnerabilities may never be fixed. After hundreds of billions of dollars has been spent on computer security, the threats posed by the Internet seem to grow worse each year. Where hackers once attacked only computers, the penchant for destruction has now lept beyond the virtual realm to threaten banks, retailers, government agencies, a Hollywood studio and, experts worry, critical mechanical systems in dams, power plants and aircraft.

As the number of connected devices explodes — from roughly 2 billion in 2010 to an estimated 25 billion by 2020 — security researchers have repeatedly shown that most online devices can be hacked. Some have begun calling the "Internet of Things," known by the abbreviation IOT, the "Internet of Targets."

Widespread hacks on cars and other connected devices are destined to come, experts say, as they already have to nearly everything else online. It's just a question of when the right hacking skills end up in the hands of people with sufficient motives.

The future looks no safer as a single operating system, Linux, comes to dominate the online world despite serious security issues that could be fixed but haven't been. Yet again, other priorities — speed, flexibility, ease of use — often win out. Warnings get ignored.

The Post's Craig Timberg spent a year delving deeply into the story of how the Internet became at once so crucial and so insecure, by speaking to dozens of scientists, industry leaders and skeptics to tease out the unforeseen consequences of decisions made over decades. His reporting, collected together for the first time in this e-book, tells an essential tale about the

creation of our new digital world that's at once thrilling and unexpectedly dangerous — with the most serious perils still waiting to be revealed.