Chapter 1

Dumpster Diving

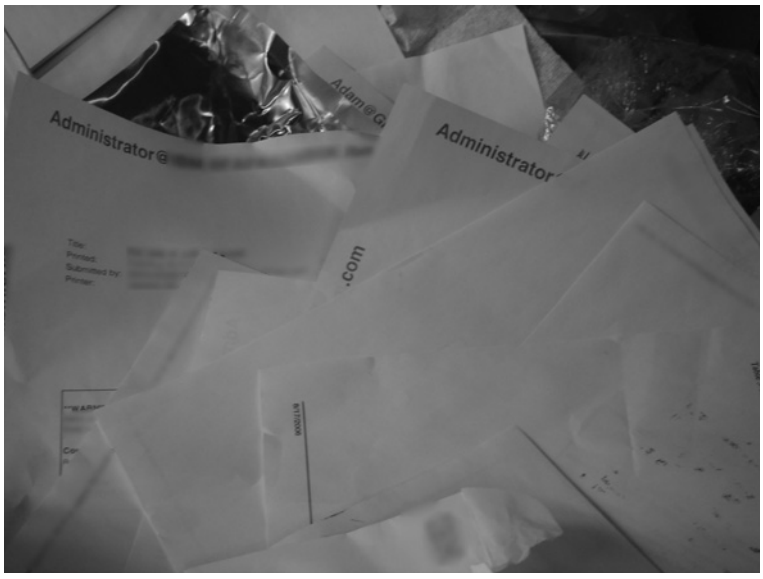
Hackers pilfer secret data in lots of different ways, but did you they can suck sensitive data right off a corporate network without even touching the network? You might think I'm talking about wireless technology, which doesn't require any "touching" at all, but I'm not. Be a good sport and don't read the two "D" words written in big bold letters at the top of this page, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). Or, don't play along, and pretend not to be surprised. In fact, maybe it's better you go on thinking your personal or corporate secrets aren't sitting exposed in a dumpster somewhere, waiting for a no-tech hacker to snatch them up. In that case you better just skip this chapter.

Introduction to Dumpster Diving

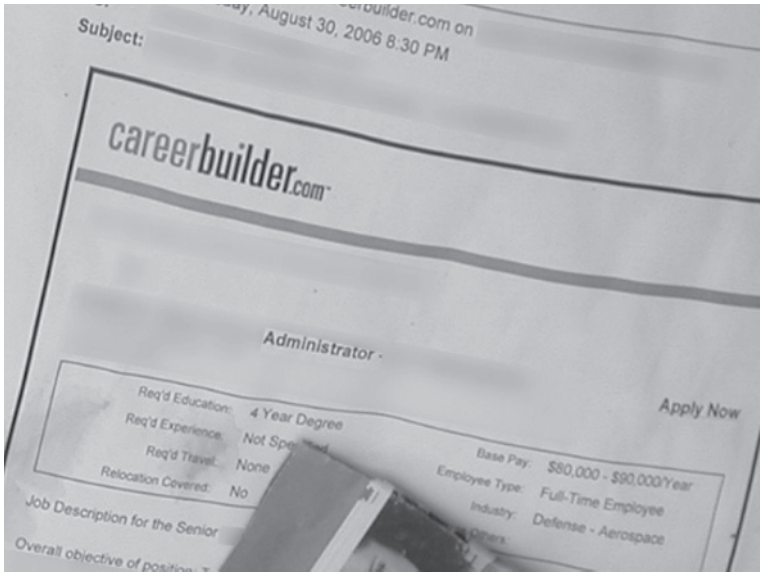
Dumpster diving involves… *diving* into *dumpsters* in search of valuable information. I know, it's bad form to use the phrase in the definition of the phrase, but that's what dumpster diving is, or what it *used* to be. These days, diving is optional. As this next photo shows, I find interesting stuff just hanging out in the open, waiting to be grabbed.

I find valuable trash in plain view all the time, like the insurance bill shown in the next photo, which is visible through the clear trash liner.

The next photo shows a pile of discarded documents belonging to a network administrator. I used my strong power of intuition to determine that these belonged to an administrator.

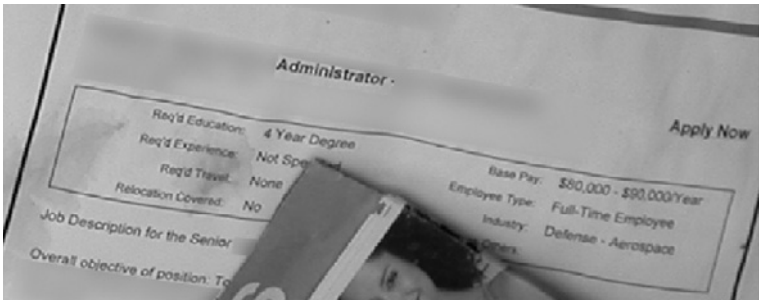


Judging from the next photo, "Fred" is obviously unhappy with his job—he's hard at work surfing careerbuilder.com in search of a new position. This printout reveals an awful lot about Fred. What else can you tell me about him based on this single document?



For starters, it's very probable that Fred's got a four-year degree of some kind, otherwise he wouldn't have printed out a job description that required that much schooling. It's a good bet that he makes a good deal less than $80,000 a year, judging from the position's salary, that he's looking for a full-time gig, and that he's probably working in the Defense Aerospace industry. Stuff like this makes me want to write Foreign Intelligence Service Recruiting for Dummies. Forget all the hard work of

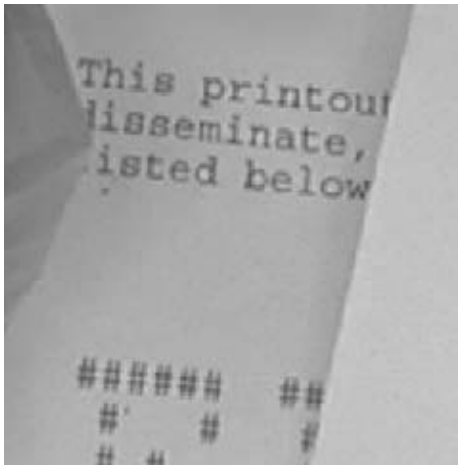
finding a mark's name, email address, employer, educational background, department of defense affiliation and career aspirations. All it takes is a brainless dumpster sweep to find juicy recruiting targets.



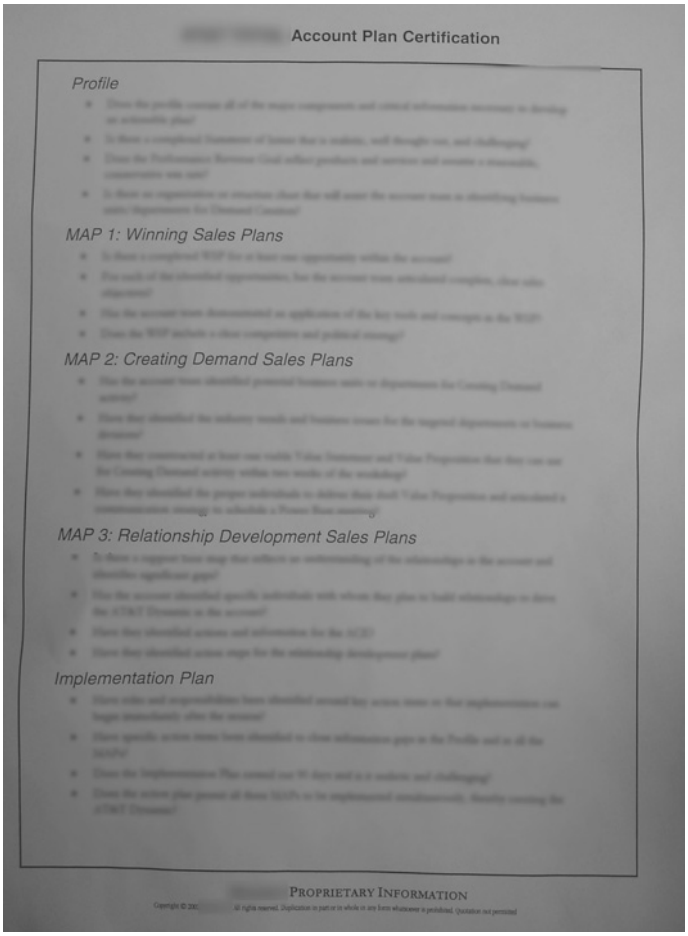
Personal info is one thing, but I find sensitive corporate information all the time as well. The next photo shows a purchase order, detailing a company's several thousand-dollar purchase.

Although the form is quite dated, it lists a great deal of information including the client's name, address and phone number, a description of the service (which is technical in nature and reveals information about the inner workings of the client), and authorized management signatures (which may be of use to a forger if the manager is still employed with the service company).

A purchase order isn't really a big deal, but I think the next document might be. It's marked "Do Not Disseminate."



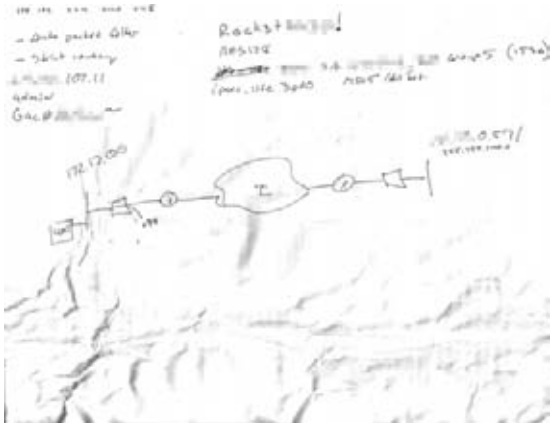
Disseminate is such a big word that I think people might not understand what it means. This causes obvious problems when it comes time to discard (or should I say *throw away*) the document. Confusing phrases abound though, like *proprietary information*. I found it written on the next document which was lying on the ground outside a dumpster.



A clearer phrase to use might be "For Internal Use Only." But even this phrase is obviously somewhat confusing, because I found it written on this now-famous dumpster dangling document.

I guess I miss the point of warning phrases like these. Inigo Montoya had it right in The Princess Bride when he said "You keep using that [phrase]. I do not think it means what you think it means." I vote for banning confusing phrases like Proprietary Information and Do not disseminate. I vote for splashing every document with a clearer tagline like "Put In Parking Lot For Everyone To Read." At least then there's no confusion about what people are supposed to do when it comes time to throw the thing away.

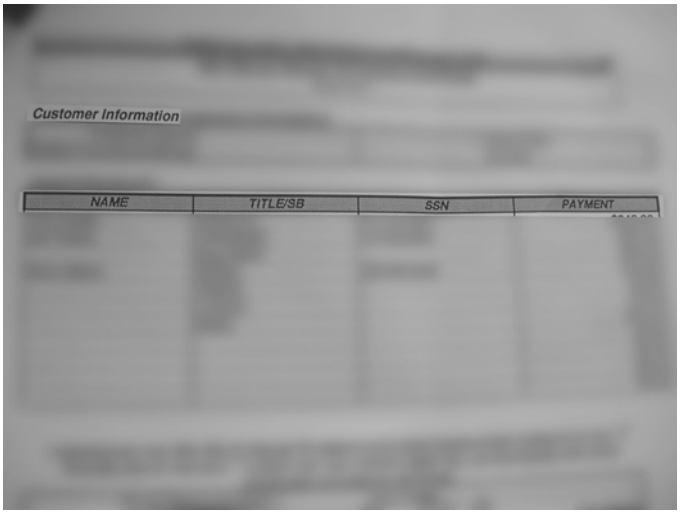
And just in case you think it's an awful lot of effort to walk past a dumpster and grab stuff that's hanging out of it, I've got good news. Sometimes if you're really lucky, all you have to do is stand in a parking lot on a windy day and wait for sensitive stuff to blow right into your face. That's exactly what happened to my buddy Mike at work one day. He grabbed the offending document and after discovering it didn't belong to his employer, he shared it with me. Now I'm sharing it with you.



This bunch of scribble might not look like much to the untrained eye, but any techie will tell you that this map outlines everything needed to take control of a computer network. The (blurred) IP addresses is a real live address, and the username (admin) and password (blurred, beginning with the letters "G" and "a") provide everything needed to log into the machine as an administrator. Another password (blurred, beginning with "R0ck3t") written at the top of the page provides access to another private IP address (blurred, ending with "0.57"), and perhaps to other machines on the private network. The routing and subnet map along with terms like packet filter and strict routing reveal that the scribbler is technically adept, while terms like AES128, MD5 and ipsec indicate that he or she is at least somewhat security-conscious, but the simple fact remains that this document was tossed aside (along with other documents Mike didn't bother to pluck out of the air) as if it were not important.

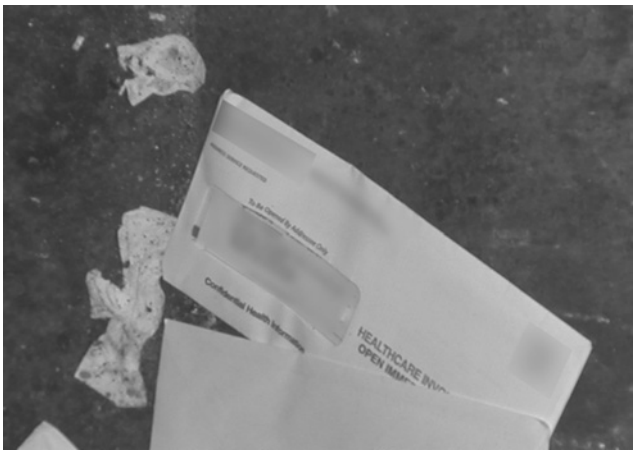
A high-tech attacker could spend hours, days, or weeks poking at the external box in an attempt to bypass AES-128 encryption and IPSEC to gain access to the private network behind it. Even then, he or she would struggle to bypass the security of the internal machines, to gain access to the "rocket" box. On the other hand, a no-tech hacker can bypass the security of the entire network in moments, just by peeling a document off his face and hanging on to it.

Fortunately, this kind of parking lot fodder is pretty rare. Admittedly, I've only seen a handful of cases that were this blatant. Most of the time I have to really push the limits and actually stick my head into the dumpster and peer inside. I discovered the next document in a dumpster on top of an open box of similar papers. The doc lists client names, account information, and a handy list of sales reps, the commissions they made and their Social Security numbers. A rival company might be interested in these documents, but an identity thief would have a field day with them.



When I found the dumpster shown in the next photo, I was disappointed because it had obviously just been emptied. The scattering of white envelopes left behind seemed innocuous enough, until I read the words *healthcare information* in bold red lettering. The rough, ripped edge of the envelope shown in the next photo seemed to suggest that some dummy had gotten the invoice in the mail, opened it, stuffed it back in the envelope and threw it out for a creepy (talented) no-tech hacker like me. If this were my invoice, I would have shredded it, then used the scraps to line my cat's litter box—which seems to deter even the most dedicated of dumpster divers.

But the white envelope was not alone in this dumpster. I spotted a few more envelopes, each bearing the same scarlet lettering, and realized that each of the other envelopes (like the one shown in the next photo) was *unopened*, and each one had a different mailing address.



Curious, I walked around to the front of the building to check the tenant listing. Sure enough, the building directory listed the name of the healthcare provider I had seen stamped on the discarded envelopes. At that moment I knew that this was not a careless patient, but rather a careless healthcare provider.

I vaguely remembered something about legislation that threatened stiff penalties for healthcare providers that leaked patient information. A later Google search (yes, Google, and not Yahoo, thanks) revealed that the amendment to the Internal Revenue Service code of 1986, known by the acronym HIPAA (the Health Insurance Portability & Accountability Act) dealt with patient privacy. Specifically, it accounts for the "Protection of confidentiality and security of health data through setting and enforcing standards" and threatens fines of up to $250,000 for blatant abuses of its suggested standards. Although I knew this was not a quarter-million-dollar offense, I knew someone somewhere would probably be ticked off to know what this company was up to.

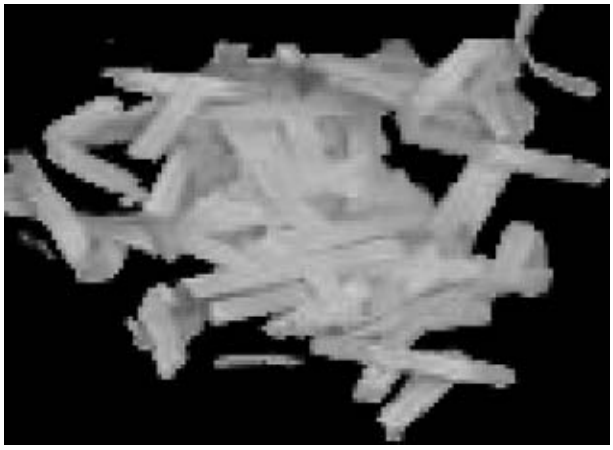
So did you tell them?

I have a feeling I'll be putting this sidebar in just about every chapter, but it bears repeating. I see this kind of near-criminal negligence all the time, but I hardly ever report it. I know from a moral standpoint that I should, but I have rotten luck reporting my finds. I've been scolded, threatened with legal action and harassed one too many times for trying to do the right thing. So for now, I'm out of the reporting game. Instead, I use the edited versions of these photos in my books and talks to raise awareness about the seriousness of the problem. At least in this way, these photos can serve some sort of positive end.

So what's the solution? First, raise awareness about the importance of trash. Signs like the one in the next photo are a nice reminder.

A lock to secure the dumpster gate is also a nice touch.

Even if this gate were locked, a motivated dumpster diver would just hop the fence. A gate lock combined with a dumpster lock isn't a half-bad idea, but when it comes to clamping down on dangerous dumpster docs, the golden rule is to shred everything. But shredding is a subjective word. There are lots of varieties of shredders, each of which provides a different level of security. A general-purpose strip-cut shredder will shred documents into vertical strips which can be easily reassembled. A cross cut shredder will cut the vertical strips horizontally. The smaller the resultant shred, the harder it is to reassemble the document. For example, a basic strip-cut shredder cuts documents into 1/8" by 1 1/8" pieces, like the ones shown in this photo.



A top of the line, ultra-aggressive scanner will obliterate documents into 1mm × 5mm dust particles (shown in the next photo) that would frustrate even the world's best spy agencies.

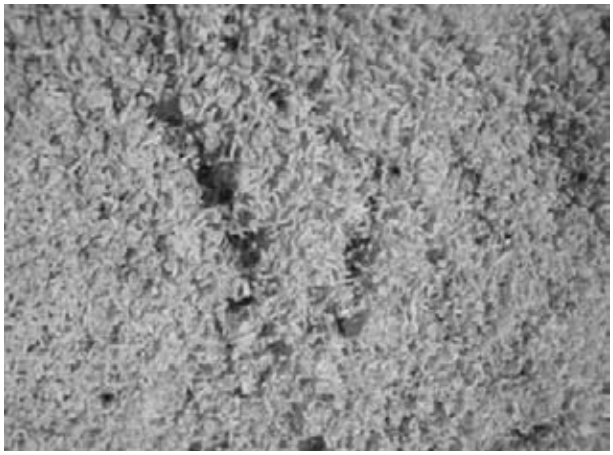


Table 1.1 lists shredder specifications from least secure to most secure.

Table 1.1 Shredder Specifications

Type	Shred size	Purpose
Strip cut	3/8"	General documents
Cross cut	3/8" × 1 1/2" – 3 3/8"	General Documents
Strip cut	1/4" – 1/8"	Sensitive documents
Strip cut	1/16"	Confidential documents
Cross cut	1/8" × 1–1/8"	Confidential documents
Cross cut	1/16" × 5/8"	Secret Documents
Cross cut	1/32" × 1/2"	US DoD and Canadian RCMP rated Top Secret documents
Cross-cut	1/26" × 1/5" (1 mm × 5 mm)	Highest security level backed by U.S. government

A decent "micro-cut" shredder from an office supply store will cost around $200, and can cut paper, CDs and even credit cards into 3/32 × 5/16 pieces, for better than average security. Generally speaking, you'll get what you pay for. Whatever you chose, anything's better than putting documents in the trash in one piece, or laying them in the parking lot.

It's also smart to know what's in your trash before the bad guys do. If you're in charge of security for your company, consider at least a weekly visit to your dumpster. Get a feel for what's being tossed and what condition it's in when it lands in the big green box. If you're a consumer looking to protect your privacy, get a personal shredder and have a discussion with your family members about what should be shredded before being thrown away. If your family refuses to comply, you might consider relocating them. If they are not particularly noisy, you might find another great use for a dumpster with a lock on the lid.

(just kidding!)