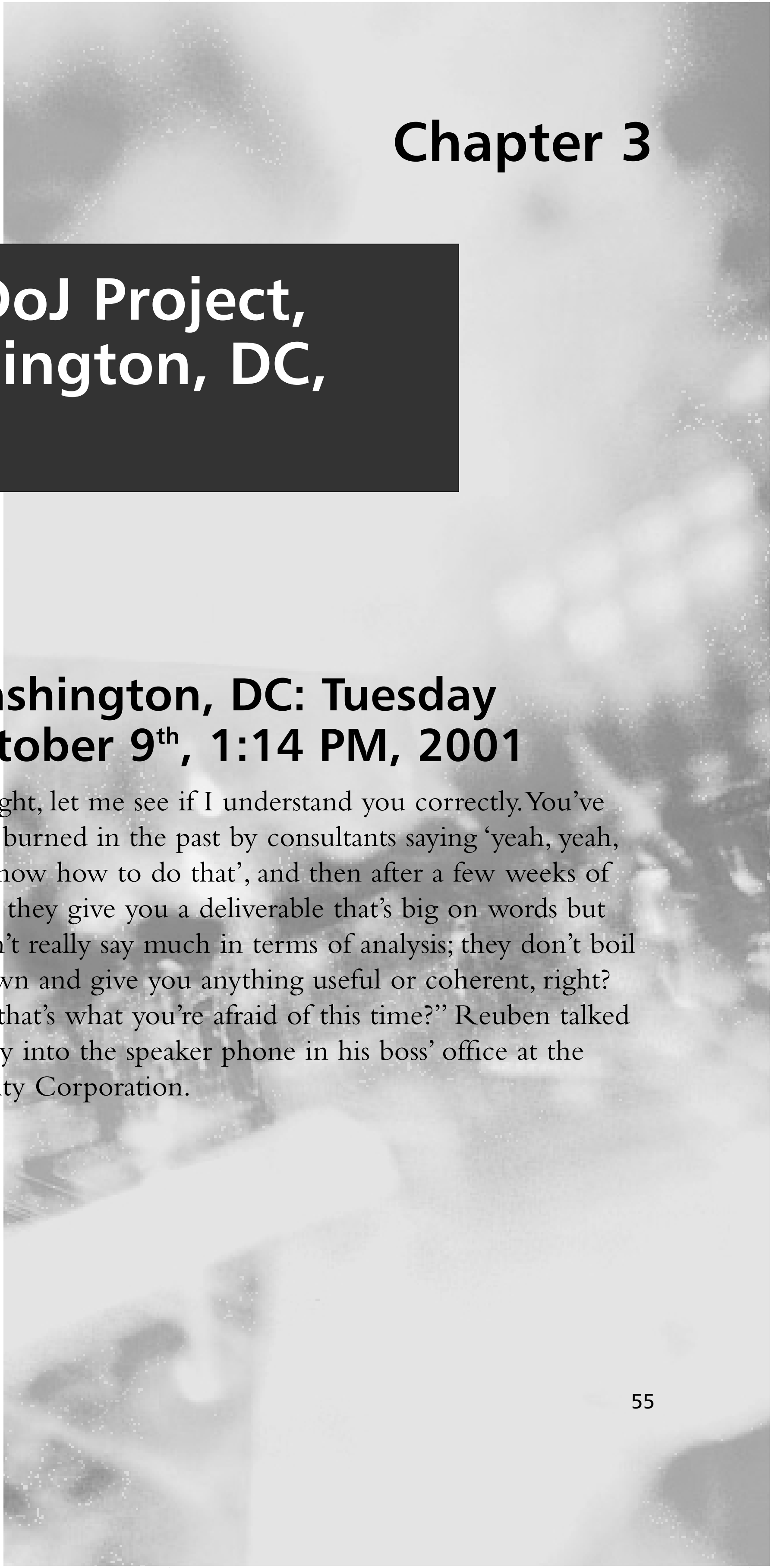

Chapter 3

The DoJ Project, Washington, DC, 2001

Washington, DC: Tuesday October 9th, 1:14 PM, 2001

"Alright, let me see if I understand you correctly.You've been burned in the past by consultants saying 'yeah, yeah, we know how to do that', and then after a few weeks of work they give you a deliverable that's big on words but doesn't really say much in terms of analysis; they don't boil it down and give you anything useful or coherent, right? And that's what you're afraid of this time?" Reuben talked calmly into the speaker phone in his boss' office at the Vigility Corporation.

The voice on the speakerphone piped back, "Exactly. We're on a tight schedule, so I can't afford to waste time on this." She called herself "Pam," and worked at the Department of Justice. A bigwig from Reuben's company had played golf with someone at DoJ over the previous weekend, and had learned that there was a need for some talent, in a hurry, for a project. Reuben's boss was instructed to make the call, and had Reuben with him for technical backup. The problem was, Pam hadn't been expecting the call, wasn't open to talking to vendors, and had someone in mind already. But she was also clearly not comfortable with what she had in the pipe; she was on a tight schedule and was afraid of spinning her wheels with someone who could claim to do the work better than they could deliver on it.

"Okay, good. That's what I thought, I've seen that myself." Reuben continued. "I'm not some sales guy, I'm just a geek. Bob has me in here because he wants someone watching over the technical things. I know how it is, how the salespeople offer things they don't really understand, but I'm not in that position, and I can't hide if I mislead you either. Bottom line, I'm the guy who'd be responsible for the geek work above anyone else, and I can tell you right now, we can give you what you want. If I'm wrong, it's my fault for lying to you outright, since I know what I can and can't do. Can I interest you in talking further?" He hoped this worked…

"Oh, definitely!" The woman at the other end seemed to do a total turnaround. Reuben's boss, Bobby "Bob" Marconi, had been about to acquiesce to her request to end the call when Reuben stopped him and interjected. Apparently it worked.

"All right. What do you want from us next, then? What should we do to move to the next step?" Bob asked.

"I'll get together a meeting…sometime in the next few days. I have to see when I can get everyone together, it'll be short notice. Can you be flexible?"

Bob and Reuben smiled at each other. Bob answered the question. "Sure, that's no problem. Just get back to us when you know, and we'll go forward from there. Look forward to hearing from you soon."

The call ended, and the two looked at each other. "I can't believe it…she was ready to hang up, and you turned her around!"

"Yeah, I don't know where that came from myself, but I'm glad I spoke up. I just knew what to say; I totally heard where she was coming from. I've seen so many companies promise this and that in security, and offer up shit, and get away with it because everyone expects it to be mumbo-jumbo anyways, so they don't know when they're getting bullshit."

Bob held his hands up. "All I know is, now we gotta get our act together so we can do this. Who do we have besides you to help out?"

Reuben smiled…this is what he did. "I can do this with Dan, and we need one more guy, from the outside. He's a specialist in cryptography; I met him at DefCon last year, and now we're good friends. He's in Seattle, and just plain brilliant." Frank was MadFast's real name, as Reuben had learned later on. In Reuben's mind, though, he'd always be MadFast.

Bob looked a little concerned. "We gotta do a background check on this guy. Are you sure he's okay? I mean, we can't have a risk on this…"

Reuben waved his hands. "Relax, Bob. You have to meet him to see what I mean, but he's fine. I trust him. Believe me, I have no illusions; I know it's my ass if I don't come through here. And we need this guy."

"Okay, I'm trusting you on this one. Do me a favor, ask him if he's got any criminal records. I don't care one way or the other, but we gotta do a background check, so let him know that."

"Don't worry, I'll ask. I'll be surprised if there's anything to worry about, though. You'll see." Reuben grinned as he hung half in, half out of the doorway on the way out, before going back to his cubicle to call MadFast.

Managers were always suspicious of security geeks, and with some reason. Many had less-than-innocent pasts with respect to their actions online, and some still crossed the line in their free time, despite making a good living working for the good guys. As pristine as he was, Reuben was still a bit distrusted early on, even though they recruited him. He wasn't worried though; MadFast was just as clean as he was, and at least as good-natured. Once they met the guy, they'd see that there was nothing to worry about.

Reuben had left DefCon with a renewed sense of purpose regarding his career. The conversations he had in the last 24 hours of the Con boosted his confidence in his own abilities, and brought him to leave LIS, taking a position with a large corporation that was building a red team for commercial work. Unfortunately, shortly after that an even larger corporation purchased his new employer, and the commercial unit to which Reuben belonged was being looked upon as an unwanted stepchild. One person at a time, the members of the team were being moved elsewhere or laid off; the team was already at a point where it lacked the critical mass to accomplish many things with its own staff. Everyone kept telling Reuben how valuable he was, and he believed it, but that wasn't the point. As long as the team was unsupported, they weren't getting any new business, and weren't *doing* anything. And Reuben hated that. When he was hired on there was the promise of being busy, busy, busy, doing all sorts of things. Red teams are primarily used to simulate an attacker, and thus working for one usually involves everything from hacking into systems to actually breaking and entering into facilities to gain access. Reuben loved the challenges and constant change in work that such a job entailed, but now he was stuck with something else entirely different.

The person at the other end of that phone call was in need of a company to take a look at a VPN product that her department was about to implement. Apparently, a new bit of regulation in the federal government stated that such things now needed independent evaluation by an outside company to verify that they were secure; as a result, the rollout was imperiled pending such an examination. The best part was, Reuben really did know that he could put together the team to do it, if he could get MadFast. Dan, one of the other few remaining members of the red team, was an infrastructure guy, and would be helpful in setting up the test network and running certain tests, but MadFast had the crypto experience that was needed to really test it properly. Nobody on the red team, including Reuben, had any idea as to how to perform tests like entropy analysis and other mathematically-based attacks. And Reuben had never coded an exploit; if there *was* a problem with the software, it would probably be necessary to prove it. He pulled out his PDA and looked up the phone number, dialing with one hand as he held the PDA in the other. He needed to work fast to see if he could put this together. People's attention seemed to be scattered lately, after the recent bombings, and it wasn't impossible that this could get lost in things if it didn't start to take on a life of its own in the next week or two.

Voicemail. "When you hear the beep, you know what to do."

"Hey, man! It's Reuben. Give me a call…I've got some work I want to pull you in for. It's sexy stuff, I think it'll be a blast. Talk to you soon!"

He hung up and took a deep breath. If MadFast couldn't come aboard for whatever reason, he had to go with "Plan B." The problem was that there wasn't one. *I am Plan A…there is no Plan B,* he thought. *Just remember that, and everything will be fine.* The hard part now was waiting…waiting for the client to come back with a meeting time, waiting for MadFast to call back…

The phone rang; Reuben rocketed around in his chair to suck the handset off the phone.

"Hello."

"Hey man! How've you been?" It was MadFast.

"Hey! Great to hear from you. I'm good! The weather's been really nice here, and I'm still driving around with the top down. How's life in Seattle?"

"Right on. Ah, same old, same old. So what's this work all about? I'm curious!"

"Oh, yes. okay, we don't have it for sure, but I think we'll get it. It's federal, but they're in a hurry. We need to look at a VPN and try and poke holes in it, see if it's really secure."

"Is it installed?"

"No, we're testing the product itself, as it's intended to be implemented. We'll stand up a lab here and work on it in a closed environment. Interested?"

"Hell ya! Sounds like fun! There's one problem; I'm kind of tied up here with a company right now."

"Can you get some unpaid leave? A sabbatical? Anything? We only need a couple of weeks, I think. And we'll pay for it, obviously, including travel."

"Yeaaaaah, I think I can get them to go for it. Let me talk to them and call you back. I definitely want to get in on this. They'll probably think I'm crazy, wanting to go to DC right now, but that's their problem."

"Thank God, because I have no *idea* who else I'd call! You're the only guy I know who'd be able to do what I need. Oh, another thing…I don't think it'll be an issue, but they have to run a background check. Anything to worry about?"

"Don't think so. Some parking tickets."

"Nah, that doesn't matter. I didn't think it'd be a problem. Cool. Go talk to them, and give me a call back, man. It's going to be great working together!"

"No doubt! Talk at ya later!"

Alright, that was one thing taken care of. At least he wanted in, that was the good thing. Without that, nothing would work out. He decided to assume that MadFast would succeed in getting the time free, and went down the hall to go tell Bob the good news.

Bobby Marconi, was definitely the most interesting person and best manager, he'd worked for. For one thing, he was a paradox of the tech world; a manager with no technical background who knew exactly how to manage geeks. He was the antithesis of the pointy-haired boss; he did not micromanage, he had fantastic common sense, and wonderful people skills. He had served in a major law enforcement agency for nearly his entire career, doing undercover work and decades of field work before deciding to become management, at which point he rocketed up in the ranks until retirement. After retirement, he had been recruited to work here.

Bob didn't need to understand the technology; he could clearly smell bullshit a mile away, and trusted certain geeks to give him simplified answers to the basic questions, based on their own technical analysis. Bob had no problem with being unable to geek with everyone; he knew what his skills were, and was entirely comfortable with his own proficiency. Reuben respected him deeply, and enjoyed being a part of decisions. Reuben had long since decided that geeks made bad managers, and Bob was the ultimate proof. It seemed that usually ex-geek managers didn't know that managing people was a skill, not just something added to a job. Even worse, they had trouble facing the twilight of their technical hands-on skills, which deteriorated while they spent time managing. It was hard for a geek to let go like that, and most seemed to resent it on some level. It helped not at all that they were expected to know how to manage automatically, without actually being taught any of the fundamentals of management.

It didn't matter that Bob didn't know the finer details of what Reuben did; hell, Reuben had to help Bob with his e-mail from time to time. He trusted Reuben to accomplish the larger goals, and stay within the lines of what was acceptable. What mattered was that Bob had no fear of admitting when he didn't know something; he knew more about how to do his job than anyone else Reuben had ever known, and didn't feel like he had to know how to do anyone else's on top of it. It was a wonderful and refreshing change that made Reuben wonder why there weren't more people who "got it" when it came to management. It seemed so clear when you saw it like this. You found good people, you asked their advice, and you trusted their counsel. They maintained their particular areas of knowledge, and the manager saw to it that they had the resources they needed to do their job.

He arrived at Bob's office, leaning in the doorway. "Alright, I just got off the phone with Madfa...I mean Frank. He's interested, and he's working out taking leave from the company he's working for at the moment. And yes, I asked, he's clean, no problem with a background check."

"Good. Now, what else are you gonna need? Computers to install this on?"

"Yeah, I'm thinking about that now. I need to know what they're going to run it on first, as far as operating systems. We can get that at the meeting. I need to think about how many we'll need, but we've got time for that. Oh, we also need a room that we can lock, to use as a lab."

"Are you sure we can do this?" Bob was nervous, but in a rather amicable way.

"Trust me, Bob. We can do this. Watch…this is going to be amazing. ALL software has problems, and we're going to find some." He smiled broadly. "I can't wait until you meet Frank!"

"How much money is he going to need?"

"We can figure that out. From what I can tell, he's not making much right now, but I don't want to take advantage of him either. We really need him, and he's a nice guy."

"Okay, but remember, he'll cost more because of the travel issue."

"Yeah, I've been thinking about that. A hotel in the area is really expensive, but there's this bed and breakfast down the street, half a block from me, where he could stay; it'd be really cheap, and quite comfortable. Besides, he and I could spend more time together working and whatnot that way too. We need to know as soon as possible when he'll be here, so we can get the tickets cheaper, but that's alright because we need to know that anyways so he can get the time off."

Reuben knew all too well that he and MadFast would be working much the same way, interspersing work with rest and fun. It just made more sense for them to be close by each other during the engagement. The trick was going to be the timing; everything had to be planned out in advance, and the clock would be ticking once MadFast arrived.

"Good. Set it up."

Reuben was pumped. This was some meaty fun work, and he was driving the project. He felt dangerous and excited. But there were still at least half a dozen ways this could die before he even got to do his thing. *No sense worrying about what's out of my hands…just think positive. Better to be prepared for something that doesn't happen then to be unprepared when it actually happens*. Walking back to his cubicle, his mind swirled with of all the ways he could attack the VPN.

One problem that always bothered Reuben was how fast he thought at times like this; he'd have idea after idea flash through his mind, and all he could do to keep them organized was to type them out as quickly as possible so that he'd have a list to go back to. *It would be really great if only the thoughts weren't so fleeting.* He launched Notepad for simplicity and started capturing all of the ideas in his internal brainstorming session. The keys clacked away like a Geiger counter as he smiled widely, loving the flow of thought coming out of his mind. He broke the attacks up into groups, depending on how the client was going to implement the VPN system. If they were going to use VPN gateways to link entire networks, that limited the scope of the attacks to VPN gateways only, but if they planned to use it for remote access from laptops and the like, that also meant that the VPN client could be attacked and that it would have to prove secure even if the laptop were in the wrong hands.

As the time between each generated idea increased, it became time to find more information based on what others had done. Googling for data turned up nothing, however. Most of what came up were posts informing people that a VPN was going to be tested for functionality. Nobody seemed to be trying to poke holes in them. *That's so odd,* Reuben thought. *It seems like there are so many avenues of attack.* In his mind, he walked through the potential impact if a VPN went down, as connections tried to recover. If the VPN stayed down, the impact could be severe; it wouldn't be trivial to reconfigure networks to speak to each other in the clear, if you even wanted to take that risk. Some VPNs did things like bridge broadcast traffic, and that functionality would be lost as well - a huge issue for many Windows-based networks.

Alright, so it looks like we're going into fairly uncharted territory here. That's okay, Reuben pondered. He decided to Google some information on the Diffie-Hellman key exchange algorithm, so that he'd have a better idea of how things could be done wrong. He knew that many products on the market utilized algorithms that were secure, but implemented them incorrectly, making them insecure.

The problem now was Reuben's lack of background in the form of mathematics that he was currently looking at. In college, he'd attended business school rather than focusing on computer science; the math curriculum was composed of simpler things, alloyed with such idiotic notions as an equation to tell you how much of each product to produce to maximize your profit as a corporation. Making matters worse, the maddening uselessness of such exercises drove Reuben to essentially do the minimum amount of work necessary to pass those classes, and now he had even less to work with than he did back then, mathematically speaking. *Oh well, time to learn now, I guess,* he thought. *I've taught myself harder and less well-defined things. At least with math, you can check your own work before anyone else has to rely on it.* He clicked back and forth through some of the pages that he was looking for, picking a few to print out and take home to look over after dinner before shutting down. He was cooking tonight, and wanted to do something nice for Briana, his girlfriend.

He walked over to the printer, grabbed the printed pages and put them into order before walking back to his cubicle and dropping them into his laptop case. Packing up his laptop and mouse, he looked around to see if there was anything else he needed. He still had time to get to Whole Foods and pick up something special for dinner, and to find nearby parking once he got home.

Tuesday, October 9th, 9:21 PM, 2001

The beef was truly excellent, and now Reuben was sipping wine while talking shop with Briana. "Yeah, so they need this work done, and fast. I think they're really nervous, I couldn't find anyone who'd ever done any research or work like this either. They were probably about to deploy the thing, but now they have this huge requirement for outside examination, and it might muck the whole
thing up."

"And you get to save the day. You must be loving this!" Briana smiled. She enjoyed it when Reuben talked shop. She herself was an IT worker, but not in the same field as Reuben; she'd started out with web design, moving on to build the intranet of the law firm where she worked. When that was done, she became more database-centric and now was in charge of a colossal document management system migration, all for the same large D.C. law firm. She loved listening to Reuben gush about what he was working on, which was part of what got her interested in him to begin with. "He talked nerdy to me," as she described the first interaction between the two. She was intrigued by his day's events.

"Well, let's see if we get the business, but I don't know who else they'll go to, frankly. And I think I got Pam's trust; there's nobody else they could possibly talk to who will be able to say what I did with regards to geeky personal responsibility for the work. At least, not without lying their ass off!"

"Now tell me, what exactly is a VPN? I think I know, but I want to hear your version."

"Well, it's fairly simple to describe, but hard to do. Let's say you're a big bank, and you have major offices in a lot of different places. Between all these offices you have to be able to communicate securely…you really don't want anyone to listen to your internal communications, right?

Okay…the normal way of doing this for a long time was to have private leased lines between the offices, but that's really expensive. At first, it wasn't so bad, because Internet connections were expensive too, and so it was simpler to do it that way."

"But the Internet got cheaper."

"Exactly. So now the best way to do it is to make use of the Internet connections, but you still have the privacy/security thing to worry about. So you use encryption on all the packets that travel between offices that way. It ends up being cheaper than leased lines, although you have to use bigger Internet links because of the added traffic."

"Okay, but what about remote users? Isn't there something about them?"

"Yeah, that's another thing you can do with a VPN. What I just described is when you have two gateways talking to each other; if you do it right, the two different office networks are joined transparently, as if they were one larger network. But you can also have a gateway that clients log into, and they can act like they're on the local network when they might really be in a hotel room quite some distance away."

"Like dialup?"

"Yes, but here's the thing. Dialing into an office has some problems. There have been security risks with such access in the past, the modems have always been a bit finicky as well as expensive, and you either have to pay horrendous long-distance charges or equally heinous 800-number costs. But if you can just dial into the local access number for some large ISP like Mindspring…"

"Oh! No long distance, and a connection to the Internet…use the VPN client to connect to the home office, and it's secure."

"Exactly, you got it! And that's the main thing they'll be using this for, as I understand it. At least that's the application we're examining. It actually raises a lot of risks for security if done wrong, though."

"Why's that?"

"Well, okay. In a perfect world, the guy whose laptop has the client only gets used by him. But what if it gets stolen? How do you make sure that it can't be used by anyone else?"

"Didn't think of that."

"Even worse, what if the computer at someone's home office has been hacked, and has a Trojan? Or if the software on the laptop or home computer stores credentials in some insecure fashion, so that they can be copied onto another system. That's one of the worst things that can happen, because then nobody knows that an attacker has gained access. At least if someone steals the laptop, the guy will know about it and the attacker can only have access until the laptop's owner calls in to report the theft."

"So what are you going to be doing to check the software?"

"Anything and everything. When MadFast gets here we'll work out a plan of attack, I don't know how to do some of the things he'll be trying. We'll set a small network up, install the software, and set up a VPN. Then we'll just try all kinds of things to break it. I haven't been able to find much about doing this kind of work, so I think we'll be figuring it out as we go along, a bit. It's okay though, I know we can do this. The important thing will be remembering not to believe anything that we're told. If you listened to the companies that made software, you'd think everything was secure…in truth very little is as secure as it could or should be."

"This sounds like great work! I'm so proud of you…"

Reuben waved his hand, smiling, "Hang on, we don't have it locked up yet. Well, I think we'll get it, but we can't be sure. A hundred things could still go wrong. They might not give the okay for me to bring MadFast over, or DoJ might take so long to drop the hammer on this project that Bob and Dan and myself will all be at other companies by then…"

"But I thought they were under the gun?"

"Yeah, but I've seen it before; in federal work, it's hurry up and wait, and sometimes the waiting happens for stupid reasons. Budgets, politics or God–knows-what other things can fuck it all up without warning. I really hope nothing like that goes down this time though. I really want to do this work. How do you like the shiraz?"

Briana looked at her glass and examined it a bit. "It's okay, but I'm not much of a red wine person."

"Yeah, I know. I just figured I'd at least get you to try a lot of different kinds anyway, in case you were just missing something you liked." Reuben smiled. He loved food, and loved introducing others to it only slightly less. "It's a lot different from the other reds you've had, I was betting."

"That's true. It's kind of like berries, not as strong-tasting either."

"Right."

"I've got another question. How bad is it if someone can break into a VPN?"

"Well, it's really bad. VPNs carry stuff that's sensitive, obviously. But something that's sensitive enough to secure like that is also important in another way. It's not enough to keep the information secret, the connections need to stay up so that the information can be transmitted from end to end. It's not cheap or simple to set up a VPN correctly yet, so if someone's using one, you can be damned sure that whatever communication takes place over it is as important as the secrecy surrounding it. Make sense?"

"Yeah, I didn't think of that. Makes a lot of sense."

"So, someone doesn't need to be able to actually read the traffic to cause a lot of harm. If they can just do a DoS attack, they've inflicted significant harm. And since the functions of a VPN are more complex than those of just normal networking, theoretically it should be easier to knock them over than it would be to just DoS normal unencrypted links."

"Okay, I had you until about halfway through. Then you lost me."

"Alright, let me put it another way. Good encryption in something like this involves certain things. One of them is the notion of a session. Sessions exist in a lot of things; all TCP-based connections have them, which means that a session exists when you browse a website, send mail, and so on. But in a VPN, the 'session' I'm talking about happens on *top* of that TCP session, so it's an added level of things that can go wrong."

"Ah, okay. Got it."

"Now, an attacker might not be able to decrypt the VPN session, but he might just want to bust things up. All he needs to do is break either kind of session and he's succeeded in that task. The good news is that TCP sessions have gotten steadily more robust over the years, as hackers have developed different ways to attack them. The bad news is that VPN sessions are, I think, an uncharted territory, and probably a lot less hard to screw with. They haven't undergone much of an evolutionary process yet to kill off the weaker ways of doing things."

"Wow. Why do you think that?"

"Well, for one thing, they're fairly new technology. They've been around a little while, but are not too widely used. And for another thing, I haven't been able to find much at all about how to attack them. So either everyone got it right the first time when they started making VPNs, or nobody's done too much research yet into how to break them. Take a guess which one is more likely?" Reuben laughed lightheartedly.

"Uh, yeah. I see your point. I love talking about this with you! This sounds like fun!" Briana was beaming at him, clearly proud of him for one reason or another. "And it makes a difference. Nobody seems to know what to do right now, so it's amazing to see you having a chance to make things more secure." Neither of them talked much about 9/11, having been so close to it. Reuben had stayed in the Marriott at the World Trade Center on several occasions on business, and while he'd been at home doing some research on his home network that day, he heard the impact at the Pentagon.

"That's what I think too." Reuben was a very lucky guy to have a girl like Briana. She didn't feel like she competed for his energy and attention when it came to his career and geeky interest, and supported him for what he was. *If only I could find women like this for my friends,* he thought. Speaking of which, "I can't wait for you to meet MadFast, too. He's got to be the smartest guy I've ever met. And coming from my family, you know that's saying something."

"Wow. I've never heard you say that about anyone before. He must be something else. How does he act?"

"That's the really incredible thing. He's a really nice, socially-adjusted guy. He's fun to talk to, and has lots of interests. Mind you, he's a true dyed-in-the-wool geek like me, so tech is always hanging around in conversation, but that's okay too. When he talks tech, if you don't understand something, he'll gladly explain it to you, and doesn't talk down in the slightest. Good thing too; I'd not have understood much at all of what he spoke about at DefCon otherwise."

"So, when will he be coming?"

"I don't know; that depends on the work, and when it happens. Just a heads up, we'll be playing host to him when he does come. I want to get him a room at the Adams Inn so that he'll be close by. That way he won't need a rental car, and we can all hang out together."

"Great! If he's anything like what you're saying, he sounds like fun to spend time with."

"Just to warn you, I think we'll be spending an inordinate amount of time working. But it'll be a short sprint, really, just a couple of weeks I think. But just the same, I really need all the time I can make use of during that period. Not that you've ever been jealous of my work, but I just wanted to warn you in advance."

"Alright. And thanks for letting me know. Is there anything you want me to do? Try to stay out of the apartment in the evening or something? I can spend some time with Michele a couple of nights; she's after me for a girls' night out…"

"Ah, I don't know yet. Can we play it by ear at first? I don't know when exactly this will happen, for how long it will be, or what it's like to work with him."

"Sure, I understand. Oh, I'm so proud of you!" She leaned in and wrapped her arms around him, hugging him awkwardly but enthusiastically on the sofa.

Reuben stretched his back a bit, hugging her back. "Thank you…I'm really happy about it." He smiled, just enjoying the moment.

"And you know how I love it when you talk nerdy to me, but you knew that," she added. She looked into his eyes, smiling demurely at him…

Wednesday, October 10th, 9:25 AM, 2001

"Good news," said Bob on the cell phone. Reuben was zipping along the George Washington Parkway, headed to the office in Tyson's Corner. "Pam just called, and it looks like the meeting will be later this week."

"Great! Do you need anything from me right now?"

"No, not yet. Right now it's just…it's only about money, and the bullshit of how to make the contract work out. They don't have time to bid it out, and there are some things you have to do in the government when you just give someone business like that, without putting it out for bidding. So we, I mean Pam and myself and Brenda from contracts and whoever else, will get with them to sort it out and see how to make it work."

"Alright. I'm about ten minutes out now. I'll do what I can to figure out what I'll need exactly in terms of the lab. At least then you'll know one aspect of the cost, if we need to buy anything."

"Good, do that. I'll see you when you get in."

Reuben closed the phone and put it back on his belt, downshifting to get onto Route 123. *This can work,* he thought. *I can feel it, it's really going to happen.* His mind methodically played out variables as he moved with the traffic past the entrance to the Central Intelligence Agency, noticing just how many cars turned off to enter the secured facility. He hated to wait to get information before trying to solve a problem; it was more interesting to play it like chess, and treat the information that came later as moved by an opponent, narrowing the options as they took him down one set of branches on the tree in his mind. *Three possibilities. Server to server, client to server only, and a combination of both.* He didn't know what the software was yet, so he didn't know what it ran on. That would come after everyone started signing Non-Disclosure Agreements, or NDAs as they were known.

As traffic started backing up, he slipped onto the Dulles Toll Road, rocketing along at 60 for about a mile, slowing as he approached the tollbooth. He flipped a quarter into the basket and sped off. Five minutes later he was pulling his laptop out of his car and walking into the building.

He was out of the elevator before the doors were half open, spinning abruptly to barely avoid crashing into some older fellow who probably had something to do with some large boring federal contract. He waved his ID at the plate next to the door and went in, stepping briskly to his cubicle and yanking out the laptop before he even put anything down.

Plugging in, he booted up, and started pulling his shoulder bag and laptop case off of his shoulders, stripping off the jacket and hanging it up. He took a moment to log in, and let everything start up as he got organized. He was hungry for some more work; it felt like being a dog on a short chain, just barking and pulling and yanking back and forth. Now that something was happening, he felt himself barking louder inside, all the more eager for seeing something almost within reach.

He started up Outlook and let it start pulling down mail as he walked down the hallway to Bob's office. Leaning his head into the doorway, he saw Bob was on the phone, waved to him and let him be. Turning around, he went to go get some coffee and sit back down at his desk. Nothing too significant in his mail, just some continuations of discussions on various mailing lists, and a little bit of administrative stuff. He started going through his morning reading, opening up Slashdot first.

While many people read a newspaper, Reuben was like many geeks in that he read websites instead. He had his routine set of sites: Slashdot, the Internet Storm Center, Washingtonpost.com, and occasionally SatireWire or The Onion for some comic relief.

Bob came by. "Hey, I just got off the phone with Brenda. The money might be a problem; apparently the contract vehicle they use pays next to nothing. She's seeing if we can get onto another vehicle. The company that's rolling out the product might be able to sub something to us, and we can get on that way; they're seeing about it now."

Reuben was deeply glad not to be a contracts administrator. "Whatever you say. Makes you wonder why they can't just pay what's fair, doesn't it? You'd think the government could merely use its bargaining power to keep from getting screwed. It seems stupid that they can't even pay the right amount easily if they want to."

Bob laughed. "Oh, my friend, you have no idea." He loved how Reuben was so utterly un-federal, even to the point of naïveté about how things worked. Bob had been in the DEA his entire professional life up to a short while ago, so he knew it well and thought of such things as they were. Reuben, on the other hand, was idealistic and thought of things as they should have been. "You should see what it's like to get office supplies at some places, someday."

Reuben laughed. "No thanks! I'll stay here in the private sector, nice and comfy and well-supported. Which reminds me, I think I know how many systems we'll need for the lab. It depends a little bit on what configurations we'll have to test, but the number only really differs by one either way, from that. The thing that really matters is what operating systems will be involved; can you ask them which ones they're planning on using? I figure they can tell us that without us having to sign an NDA. And do we have any servers lying around we can use for this?"

Bob thought for a second. "I'll ask…can't hurt to see. And I don't know what we've got lying around, but we may have to come up with something to set up the lab. I don't get the impression there's a lot we can call upon these days. And there's no way we can charge the client for buying machines."

Reuben nodded. "I've got an idea then. I think we can rent some systems, and it shouldn't cost us too much. We won't need them for long, and maybe we can even include that in the pricing."

"Good thinking. Call and get some idea of the cost. Figure on two weeks."

"Will do. I'll make sure the systems are clean before we give them back too. Odds are the company re-images them each time, so they won't mind if I do a little formatting."

"Ah, that's a good point. We need to be careful about who has access to what we find. Let me see about finding a room you can use for the lab. We've probably got something on the sixth floor. Do you need anything special?"

"No, just a phone, a working network drop, and power outlets. Oh, yeah, and one more thing. We need guns…lots of them."

Bob laughed in shock, "What??"

"Oh, sorry. Matrix quote." He smiled widely.

Bob chuckled, getting the joke…or at least getting that it was a joke…at that point. "Gotcha."

"One more thing. I've started looking ahead to plan how we'll approach this. Should I be logging my time spent on that? Can we retro-bill that kind of thing?"

"I'll ask. My feeling is no, so don't do all the work in advance. But keep track, just in case, and don't be afraid to be prepared. Besides, if you've got nothing else going on at that moment, it's not costing us anything."

"Good point. Okay. I'll call about rentals now."

Bob stepped away, and Reuben started looking on the web for computer rental options in the area.

Wednesday, October 10th, 8:21 PM, 2001

Reuben sat in Tryst, a coffee lounge in his neighborhood, alternating between attention to his coffee and his laptop. Larger than many restaurants in the Adams Morgan section of Washington, Tryst was an expansive space of chairs, lounges, and sofas, with a full bar, a small kitchen and the best coffee in the city, hands down. It was also extremely laptop-friendly, providing numerous power outlets and even analog phone jacks for local dialup connections.

It was where Reuben often did some of his best work when it came to the more mundane, writing-oriented parts of his job. It was at Tryst that he wrote scopes of work, deliverables for untold numbers of clients, and an entire marketing plan, not to mention the occasional small article to be published in one place or another.

In the dim light of the place, his face glowed white with the light of the document on the screen. Reuben was documenting the attack plan, as he could guess at it. He figured that it might change a bit, but then it could be changed; better to have something to start with anyway, since MadFast wouldn't be there long. Too much time spent doing things like this could cause a problem, since the whole thing would be a failure if they didn't cover enough ground in what time they had to work.

First they'd be looking over the documentation, approaching the whole thing blind. Learning the architecture of the system was probably the most important thing they'd need to know, and in the subtleties of suggested configurations one could find things that go wrong when a different setup was tried.

Next, obviously, would be installing the software. Looking for ways to screw up and leave things insecure was key; they'd go about it as blindly and in as much of a hurry as they could, then they'd go back and see if they missed anything. If there was any significant difference between the correct and actual configuration, they'd need to test things with the weaker config before hardening it and having another go, in addition to documenting the mistakes that were easily made.

Then, they'd start using the software, doing network captures and trying to learn how to read the packets. Buffer overflows were definitely something that they'd try, and while Reuben was building packets to test data fields, MadFast could try entropy analysis on the encrypted data.

After that, they'd start assaulting the remote client, assuming that would be part of the intended configuration. They'd run RegMon and FileMon while starting up and using the client, and sift through the deluge of resulting data to see which registry keys and files were involved in it. File permissions on the client would be important; they'd also look for things like private keys and authentication information on the system, and settings that might be security-related. One possible goal would be to dumb-down the encryption; many applications that used encryption supported multiple versions, and could be forced to use weaker forms by an attacker. And they'd see if they could buffer-overflow the client as well, in case it opened up any weaknesses on the client machine.

Beyond that, it got rather fuzzy. Half of what they did would probably be determined by what they learned at some earlier step of the process; a whole set of tests could come to light based on the configuration, and other tests could be eliminated by the design of the software or how it would be used. But it helped a lot to think and plan ahead; at least now Reuben felt like there was a solid game plan, and that he'd save some time when the test happened.

Reuben realized he was about finished, and put down the coffee. He flagged down Kellee, one of his favorite people at Tryst, and ordered a beer. He had a feeling he'd be here a lot more over the next two or three days.

Friday, October 12th, 11:52 AM, 2001

"We've got a problem," Bob said.

Reuben looked up and over from his desk, turning around to face him. "Uh oh. What is it? The cost?"

"No…they're letting Dan go."

Reuben carefully considered this for a moment. "Well, hmm. I think we can still do this without him. I was truthfully bringing him in so that we could try and throw a bit more manpower at it, and set up more of a network, but the parts that really matter are at the ends. And as far as any infrastructure things go, I can handle that myself too. Remember, I was a networking guy before I went into security full-bore."

"Are you sure? We can do this with two people?"

"Yeah, we can. I know, you're worried that I'm overextending us because I want to do the work so bad. And yes, I really want it, I want it so bad I can taste it. But I'm not stupid, and I'm not going to get us into a nightmare situation. We really can do this. Wait until you meet Frank; you'll see what I mean. Remember how you once said you wished you had three or four of me?"

"You're saying he's like you."

"Yeah, except he's actually more like more than one of me. Just trust me on this."

"Okay. But just so you know, it's all in your hands now."

"That's how I've been looking at it all along. I won't let you down. How's everything else looking? Any news?"

"Yeah, we can get on with the other company, so that's all fixed. We'll get our rates covered, and can make some money on the work. I got a room for you guys, and there aren't any computers we can use…that's the bad news. The good news is that we can bill the client for the rental costs."

"Oh, good! So we've got our money for work and a lab. How about bringing Frank down?"

"Yeah, we got that approved to, but there's a catch."

"Uh oh. What's that?"

"He's got to clear a background check."

"Oh, that's no surprise. That's fine. Don't tell me you're still worried about that?"

"Yeah, I am. I'm just concerned. I mean, it's down to you and him, and without him we can't do it. So what if there's some unforeseen thing? I'm not saying he's lying to you, but how does he know what might be significant? If he's been charged with something, but then the charges were dropped," Bob added, clearly worried that MadFast might have dabbled on the wrong side of the law, "then that's enough to make them cut him from the picture."

"Trust me, he doesn't have to know what is and isn't significant. There's nothing, there really is nothing out there. And nothing can't be significant. I mean, really, nothing. I'm sure of it."

"Are you sure? Remember where you met this guy."

"Yeah, but I was there too, and you know I'm not a bad guy. I just know some such people so that I'll know what's going on. Frank's fine, no problems, I'm sure of it. And he doesn't even look like a bad guy." Reuben smiled. "Just relax, he's not something we need to worry about. He's fine, he's going to be great. Do you want to talk to him on the phone? That way you can get a feel for what he's like, and I guarantee you'll feel a hundred percent better after."

"That's a good idea. Yeah, let's all talk about the project and make sure we're on the same page."

"That works. I need to call him anyway and see where he is at his end, on getting time off from work to do this. I'll set it up so we can call him from your office, and I'll introduce you. When's good for you?"

"He's in Seattle, you said? That's three hours back. How about three-thirty."

"Okay, I'll contact him and set it up."

They nodded to each other, and Bob went back to his office.

Reuben turned back around to his computer and reconsidered everything. He was sure that he could handle this, even with a third of the team eliminated. Well, he'd included Dan mostly to help Dan out, he realized; they were cutting people away here and there, and being allocated to something was helpful for survival. Too bad it didn't pay off in his case, but Reuben was sure that Dan would be able to find other work fast enough. He was plenty skilled and experienced, and he knew lots of people who could help him look for a new job. He picked up the phone and called MadFast, figuring he was probably in the office about now anyway. He got MadFast's voicemail.

"Hey, it's Reuben. I want to set up a phone conversation between you, Bob and myself. I was thinking three-thirty our time, so half past noon yours. E-mail or call me back and let me know. Talk to you soon." He hung up.

He pushed away from the desk and closed his eyes a moment, thinking. He went down the list of all the aspects of the project, and everything that needed to be done, checking to make sure he had everything covered to the best of his ability. *So far, so good, despite all the surprises. I guess surprises are inevitable, and it's good luck that none of them have torpedoed this yet.*

Friday, October 12th, 3:33 PM, 2001

"Alright, now I'm finally going to be able to get the two of you to talk to each other. Bob, meet Frank. Frank, Bob." Reuben spoke into the speakerphone, happy that this was finally happening. Things were probably going to start happening fast now, so for Bob and Frank to be able to talk directly would be a plus, and it would keep Reuben out of the middle when it came to things like compensation and organizational matters.

Frank responded first. "It's good to meet you. Alright, where are we now?"

"I'll let Bob give you the update on what's going on at this point. I think we're pretty far along, but I'm not the real authority on that."

Bob piped in. "Alright, here's where we stand. We've got the authorization to do the project, and to bring you in. We'll be setting up a lab, using rental computers, in a room downstairs. One thing, though. I need to put in for a background check on you, just to make sure there's no big problems or anything like that."

"That's fine, Reuben told me about that already. What do you need, my social security number and full name?"

"Yes. And your current address."

"Not a problem. You want them now, or in an e-mail?"

"Why don't you give them to me now, so that I can get it taken care of. Just in case there are any problems, it's better to know sooner so we can do something about it."

As MadFast gave his information over the phone, Reuben relaxed. He was a little worried that there'd be some offense taken at Bob's concern, but it seemed to be going alright. Reuben had always understood when people were cautious, so maybe MadFast was the same way too. Whatever the reason, all seemed to be going fine.

Bob spoke up. "Okay, with that out of the way, why don't the two of you let me know how you're planning to go about doing this. I mean, I might get asked, and I don't want to be caught looking like I don't have an answer."

Reuben nodded. "I've been working up an attack plan. I need to e-mail that to you, Frank. It's not entirely done, but it's about as good as I can get it. I need you to tell me if I missed anything in it. I'm betting there are things you can do that I can't, too."

"Right on."

"Here's the gist of it. We set up the lab first, and then we go over all the documentation. I think there are things in there that we can find, clues as to what to look at. Then we set it up as haphazardly as we can. No point in setting this up like a kick-ass security guru, since that's not who's going to be installing that all the time. If it's easy to screw it up and make it unsafe, I want to find out."

"Right, right. Good idea."

"Then, we play around with it a bit, see if we can get an encrypted connection, that sort of thing, and we sniff the packets."

Bob looked confused. "Sniff?"

"Yeah. It's like eavesdropping on the network traffic, and we'll record what the systems say to each other, and look at the raw data."

"You can read that?"

"Depends, but usually yes. Some of it, at least. And that's the next thing I want to do. I want to see if I can figure out how the packets are built, what packets do what and how they are structured. If there's a buffer overflow in there somewhere, I want to find it, and that means we need to know the anatomy of the traffic."

Bob was impressed. "Wow. You guys scare me." He smiled.

Reuben continued. "After that, if they'll be using a remote client, I want to go after that. There's lots of fun I can think of there. Frank, how are you at reverse-engineering software?"

"I'm not bad. What are you thinking?"

"I'm thinking that this software might store credentials or whatnot in not-so-safe places on the local machine of the client. And I'd like to get at them, and do what we can with the information."

"Right on! I think we can do that." MadFast was audibly smiling at the other end.

"And aside from that, there's a lot of little things, but that's basically it."

"Sounds good to me," MadFast piped in.

"Alright, I think I have what I need," Bob answered. "Anything else you guys need?"

"I need to know when and for how long," MadFast answered.

"Yeah, me too. We need dates."

"Okay, I think we'll have those soon enough. Reuben will give me your e-mail address, Frank, so I can contact you when I have that."

"Right on."

"And I'll e-mail you the outline I made of the attack plan. There's more detail of attacks in there, things crypto-related."

"Okay," MadFast concurred.

Reuben finished up the call as he pretty much started it. "I guess that does it. One of us will be calling you soon, Frank. Be well."

"Talk to you guys later." And he was off the phone.

Reuben smiled at Bob. "What did you think?"

"He sounds fine, you're right. I got a good feeling about him."

"Exactly what I thought would happen. Wait until you meet him."

"Okay. I trust you now."