Chapter 3

Product of Fate: The Evolution of a Hacker

by Russ Rogers as "Saul"

Looking back on the entire event, no one could really say how everything ended up the way it did. Saul has always done well in school. And though his parents might not have been the greatest people on the planet, it's not like they didn't love him. So, what could have enticed a bright, seemingly normal kid like Saul into committing such a heinous crime? No one knows. But, then again, no one knows what really happened, do they?…

Saul was the product of what started out as a normal middle-class family living outside Johannesburg, South Africa. His family lived in a simple house, nice but not too expensive. His father was a typical *Type A* personality who dreamed of working hard and becoming independently wealthy and his mother was a beautiful social butterfly in the community.

Saul's one big interest was technology. He had always been computer smart, ever since his father bought him one three years back, when he was still 15. It was a laptop and his father would often spend time with Saul teaching him to surf the Internet and set up web servers. It wasn't long before he was much more adept at using computers than his own father, which really served only as a precursor to their eventual isolation from each other. Instead of being proud of his son, Saul's father soon began to feel intimidated, creating a gap between them that only widened as Saul grew deeper into his teenage years. Eventually he lost the ability to communicate with Saul. The father-son relationship started to deteriorate.

As for his mother, she had never been much of a good influence either and had a tendency to spend far too much time boozing it up with her friends. Eventually, the normal middle-class family began to break apart; his parents divorced, and Saul found himself being forced to live with his mother in the city, picking up empty scotch bottles and feeding her canned soup when she could no longer feed herself. Despite all this, however, it was really just boredom that drove Saul into the project. He was just another bright kid at a local high school, bored with courses that continually failed to keep his interest, with a severe lack of friends due, in part, to his own introverted personality. Saul failed to find value in the everyday occurrences at school and certainly wasn't interested in competing in the inane day-to-day popularity contests. His father had told him many times before that the people you meet in school will generally not be around when you get older, so why bother getting attached?

Interest Piqued: The Fire Is Started

Saul soon graduated high school, with only mediocre grades and a limited interest in continuing on to college. But with the help of a school counselor who believed in Saul's ability, he was able to apply for the appropriate student grants and began his first semester at the local community college.

College wasn't too much different for Saul until he met a friend by the name of Beaker in a C++ programming course. The two were eventually paired up for a project by the instructor. They soon became close friends, and when Beaker eventually invited Saul to a local hacker meeting, it piqued his curiosity and he decided to see what it was all about. That first meeting was the spark that got Saul started on wireless security. It was called wardriving, and it fascinated him. The idea of these invisible packets flying over everyone's heads, constantly and at incredible speeds, was enough to give birth to his fascination with the medium. Saul began researching wireless networking and soon had his own network at home. Okay, so it wasn't that big of a deal at the time. Lots of people were getting into wireless networking. In the end, maybe it was the simple fact that Saul had indeed inherited his parent's addictive behavior.

About six months after this first meeting, Saul had become the resident expert on the topic, already writing several applications for wardriving, area mapping, and encryption key cracking programs. He had also created the largest database in the city of all known access points, and had a habit of taking advantage of the *free* wireless access throughout the various parts of town. His Web site served as Saul's journal, cataloging all of his activities, notes, and discoveries. Though he didn't know it at the time, it would also serve as the initial point of attraction for an unknown man who desperately needed someone with Saul's skills in wireless networking.

One day the e-mails started arriving. Someone, his name unknown to Saul, had been monitoring the hacking group and watching Saul's progress on the Web site. The e-mails came in with seemingly corrupt headers and commented on the skill with which Saul understood the wireless world. Each and every reply that Saul sent back would come back with a *User Unknown* error.

What?! You've Got To Be Kidding Me!

It was the first of March when the first identifiable e-mail arrived in Saul's box. He had almost deleted the e-mail because he didn't recognize the e-mail account, but the subject line was familiar and he opened it anyway.

```
Saul,
I have a job for you. I'll pay you well for your time. I have a need for
your knowledge. Meet me after the next meeting.
```

His hacker group met every two weeks, instead of the usual once a month, due to the interest level in the local area. The next meeting was in one more week, and at this upcoming one, Saul was due to give a presentation. Was it a coincidence? He had been preparing a comprehensive map of all the insecure wireless networks within a 10-mile radius of the college and was going to give the information to the other members at the meeting. The others in the group loved free Internet access and Saul was happy to oblige.

Saul was convinced the e-mail was a fake and never really expected anyone to show up. It was probably just one of his friends trying to be funny, so he promptly deleted and forgot the e-mail.

On the day of the meeting, Saul brought his materials with him to class. He hated having to run home, across town, before coming to the meeting so he had gotten himself into the habit of preparing the night before. So with everything already in his backpack, Saul grabbed his leather jacket as soon as the class finished and headed for the bus station. Public transportation around Johannesburg wasn't the greatest, but at least it was cheap.

The coffee shop was an old run-down place, but the manager was cool with the kids using the place as a hangout. Saul had even hooked up a wireless access point for the man so that he could be more like "those coffee shops in America." When he arrived, Beaker and some of the others in the group were already there waiting.

Jumping into the presentation, Saul never even paid attention to the man on the other side of the coffee shop apparently reading a newspaper and sipping at his coffee. It was actually Bender, Saul's friend, who noticed the man staring intently over his newspaper. As soon as Saul had finished his presentation, Bender walked over to tell him and said,

"Dude, you see that guy over there?"

"Yeah, so what? Wasn't my presentation awesome? Did you see their faces when I brought up the map of the city? Totally free Internet for everyone in the group!"

"Seriously," Bender went on, "that guy has been staring at you since you started speaking. He seems to know you. Have you ever seen him before?"

"Nope. I never saw him before. Besides what would a suit want with a poor college kid?"

"Maybe he's from the American FBI. I heard they're cracking down on hackers!" Bender sounded nervous as he made this comment.

"He's probably just some freak. Come on, let's get out of here," replied Saul.

Bender agreed and went to the toilet while Saul started packing up his gear and getting ready to leave. The man across the room folded the newspaper he had been reading and set it down on the table. His charcoal colored suit was Italian made with smooth, slick lines and straight cuts. He was a black man with a trim beard, wire-frame glasses, and the build of an athlete. The man walked directly toward Saul, passing by quickly. As he passed he dropped a letter envelope on the table in front of Saul. Never speaking a word to Saul, he continued walking out the front door. Saul grabbed the letter and saw his name on the front.

"Hey man, what's that?" said Bender, returning from his trip to the toilet.

"Ah, nothing," Saul replied quickly as he shoved the envelope into his jacket pocket. "Just some notes I forgot to open for the talk. No big deal. I didn't really need them anyway. Let's get out of here."

You Want Me To Do What?!

Saul was too intrigued to hang out with his friends after the meeting as he normally would. Instead, he said his goodbyes and hurried home. The envelope in his jacket pocket had been calling to him ever since he had stuffed it in there about 30 minutes ago. He wasn't quite sure what to think of it and started organizing his thoughts as he walked down the dark streets toward his home.

It took Saul only 20 minutes to walk home and he wasn't too surprised to find his mother away for the evening when he walked in the front door. After a quick stop at the fridge for a soda, he headed to his room. Opening the door, he tossed his backpack on the floor and hung his jacket on the chair in front of his desk.

His room was a geek's room. There were multiple computers all around the room, each one currently powered up and running a different operating system. Most of the computers were fairly old because the newer hardware was too expensive in that part of the world and most of his hardware came

from dumpsters anyway. Various books and magazines lie in haphazard stacks around the room. Saul sat on his unmade bed and glanced at his jacket hanging on the chair. "What's in there?" he wondered to himself. He reached over, slipped his hand inside the pocket, and retrieved the envelope.

The envelope appeared to be a stock bulk envelope and his name was hand written in black ink. Relatively impatient, Saul tore open the envelope and pulled out the letter. It was a normal letter-size piece of paper that apparently had been laser printed.

```
Saul,

Your skills with wireless networks are needed for a project I have.
Currently, I own several large medical organizations, including St. James
hospital in your city. I have concerns about the security of the wireless
network utilized at the hospital. Our physicians and administrative staff
use the wireless network for various routine and critical tasks. My biggest
concern is that perhaps my security team does not take their job seriously
where wireless networking is concerned.

Initially, all I want you to do is profile the network and provide me with an
idea of what sort of wireless footprint we're projecting into the
surrounding area. I'm also interested in knowing how difficult it would be to
break the encryption used on our network, if there is any.

I would appreciate it if you would spend a week examining the St. James
wireless network from some spot outside our facilities. Do not tell anyone
what you're doing and try not to draw attention to yourself. This assessment
of our wireless network must remain confidential as I'm testing the abilities
of my on-site security team. You can expect payment of $2,000 after your
next hacker meeting should you meet these requirements and have a report
ready for me.

Respectfully,
Your Friend
```

Saul read the letter several times to ensure he really understood what was being said. His instinct told him that this was probably a prank, but he had never really tested the security of the hospital's wireless network and it sounded like fun. He decided to try it out and see what he could come up with. Worst-case scenario, he got to do what he enjoyed doing. Best case, he got an extra $2000 for college and got to check out the wireless networks

around the hospital, which he hadn't had time to do up until now. It seemed like there was no way to lose.

It Was Only Harmless Fun…

That next Monday, Saul left school early and took a bus downtown to the area surrounding the hospital. He had packed his iPaq and a few other items in order to do some quick recon of the area to see what he could pick up. He wanted to be light on his feet and not really draw attention to himself so he left the laptop at home. The hospital was in the middle of a large plaza with shops surrounding the front of it. It was always a popular hangout for kids who liked to skateboard, so he could easily meander around the complex without looking overly suspicious.

As he sat on the bus, he reflected on the items he had decided to bring with him for this little adventure. When he *warwalked* like this, he preferred to use his iPaq because it was small and would easily fit into his backpack or jacket pocket. He also used the PC card expansion pack for the iPaq so he could use the more effective 802.11b WiFi card with the Hermes chipset. This also had the extra benefit of allowing an external antenna to be plugged into it. Attached to the antenna plug on the wireless card was a small 5dbi omni antenna with a shortened cable, thus extending the range of Saul's surveillance. The final piece was a GPS puck with the appropriate serial cable. The puck was much less conspicuous than a normal handheld GPS device with a liquid crystal display. Although he couldn't really monitor the output from the GPS device in real time, he knew that the cable connecting the antenna to the iPaq would transmit location data continuously and enable him to track the exact locations of each wireless signal.

Saul was using MiniStumbler for the iPaq. The output of the tool could be dumped into one of several scripts that he had written to draw maps of the area and display the propagation of the wireless signals. Saul knew that signals tend to bounce off various buildings in the area and wanted to know exactly where those signals could be intercepted. In fact, he had seen wireless signals bounce around in between buildings and be detectable several blocks away, so he was excited to see how the maps turned out for this work.

As he stepped off of the bus, Saul considered the personal risk he could be taking.

Technically, this was not illegal. He didn't intend to connect to any networks, he was just checking it out to see how far the signals extended from the hospital and to listen to the packets and see how tough the key would be to break. But the local authorities were technophobes and assumed that any activity like this was a crime. He has seen his friends in hot water with the local authorities for similar activities, which was part of the reason he was using the small kit today. But if things got rough he still had proof that he was asked to do this.

Saul walked from the bus stop to the plaza near the hospital. There were plenty of people out today, shopping or eating at the cafes. He stopped in front of a large fountain in the plaza and took the iPaq from the bag that was already connected to the required cables. He had turned on the GPS puck when he left the house. He didn't want to draw excessive attention to himself by taking it out of his backpack in front of the hospital. Grinning to himself, he switched on the iPaq, started MiniStumbler, and slipped it back into his pocket.

iPaq / GPS Puck / Orinoco WiFi Card

As he started walking across the complex, he began thinking about his set up. His iPaq was an older model, which he bought from a friend at school who had upgraded about a year ago. It certainly wasn't the best, but it was all he needed for wardriving. The PC card was an older chipset that was heavily supported in both the Windows and Linux software communities. His iPaq even had built-in drivers for the card, making it even easier to use.

Saul's iPaq Warwalking Kit

Some of his friends had argued with Saul that he didn't need a card with an external antenna plug, but he thought differently. To truly understand the range a network has, you have to be able to really capture the signal. Besides, the antenna that was now stuffed in a side pocket of his backpack was lightweight, small, and unobtrusive. If he could improve his tracking of wireless networks just by having the right card, it was worth it.

Saul walked around the complex for about half an hour and then headed to a nearby outdoor café to sit and relax while doing the next part of his mission. "I need to collect some packets off the network," Saul thought to himself. "If there are key packets being transmitted, I need to know how many per hour in order to estimate the amount of time it would take to crack their key." Saul was amazed that he was actually getting paid the kind of money he was to sit here and eat lunch, doing something he enjoyed so much. The waitress came by, took Saul's order, and then disappeared back into the restaurant.

Reaping the Rewards: A Little Bit Goes a Long Way

He continued this same routine for the next few days, as requested in the letter he was given. Although there was a big chance this was just a prank, Saul wanted the money. Besides, there was something to be said about being away from his home every day. "Gawd, I can't wait to move into the dorms. All I need is the money and I'm out of there." He thought of his mother again and sighed deeply.

On the last day, Saul headed home right after school to create the report. The report was fairly easy to generate. Saul copied the raw MiniStumbler files in their native .NS1 format and plugged them into NetStumbler on another computer. From here, Saul was able to convert the data into comma-delimited files and dump the numbers into a database. Some of the statistics collected were used to create the actual maps and images for his report. He still wasn't sure that this mysterious man would ever actually contact him again, but he hoped to eventually turn his work into a commercial service and make a living doing what he loved. So, technically, his time wasn't really wasted even if he didn't make a dime on this job.

The hospital was using a large wireless network that was bridged across multiple access points in the various wings. The coverage was much larger than required for the hospital, but Saul assumed that was so that the doctors could grab lunch out in the plaza by a fountain while still updating reports on the network.

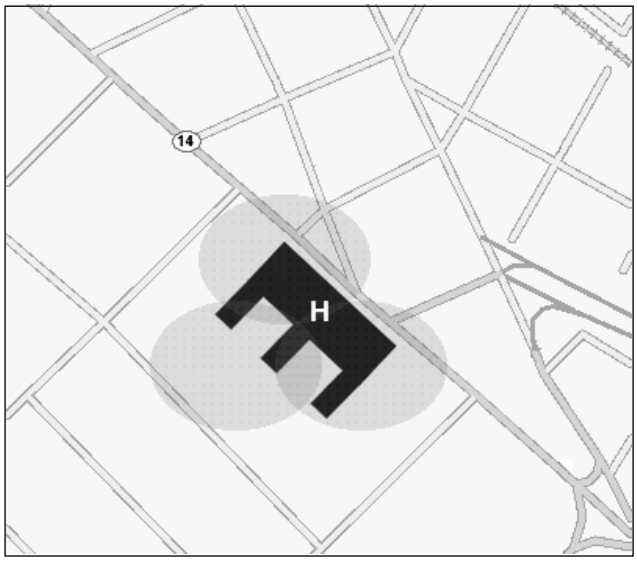
The fact that the hospital was even using a network was impressive, much less wireless networking. St. James was a state-of-the-art facility compared to the other medical facilities in the country. But the hospital was still using early 802.11b technology access points that are rather chatty about their locations and use a weak encryption scheme. Because the access points were all bridged, the identifier on each one was the same, stjames.

Saul had been able to collect an appropriate number of key packets to break the WEP encryption in only a few hours. To his surprise, the WEP key was set to st.james-hosp. With the number of key packets that were transmitted, Saul determined that the access points were most likely an older model of the Lucent AP-1000, but he would need a walk through the hos-

pital to be certain. "I'll do that another time. It's not really necessary for this report," he thought to himself.

The final map was clear and easy to read. Saul was able to see the area around the hospital where wireless signals were accessible.

Map of the Hospital's Wireless Signal



Saul added the new numbers to his own collection of local wireless information and settled in to his normal routine. The next meeting wasn't for another week and he had finals coming up at school. Grabbing his homework from his book bag, Saul lay on the bed and began to study.

Money—The Root of All Evil

The next week flew by for Saul, mostly due to his finals he had that week. In fact, most of the kids in the group had tests that week and very little actual planning had taken place for the next meeting. Apparently, they were just going to meet at the coffee shop to have a LAN party and order in pizza. Saul was looking forward to finding out if this whole wireless thing had been a hoax or not. He had tried to determine which of his friends it could have been, but had come up blank.

After his last class on the day of the meeting, Saul packed up his normal school gear and headed to the coffee shop. The spring air had been warming up and he realized he didn't need his coat, so he tucked it into his laptop bag. The walk to the coffee shop was short and Saul was the first one there. After a quick glance around the room to see if the mysterious stranger was there, Saul grabbed a seat in the back where the meeting normally was held.

It was about 30 minutes later before Bender and a few other friends showed up to start the party. Each person had their laptop bags stuffed with networking cables, hubs, and games. The game of choice was Unreal Tournament 2003. Bender normally ran the actual server off of an old Linux laptop he had picked up. He had installed a newer 120 gig hard drive and loaded it up with every available map he could find. Saul enjoyed these occasional jaunts into mayhem because it helped him relieve his built-up stress.

As Saul unpacked his laptop, he found the report he had created and looked around the room again. "I wonder if he'll really show or if I've been had by one of these guys." He laid the report next to his laptop, just in case, and pulled out his networking gear. One of the girls in the group was going to call for pizza, so Saul gave her his money and booted up for some well-deserved violence.

The pizza came and went. Multiple cups of java were consumed and just as many trips were made to the bathroom. It was four hours later when Saul noticed that some of the group members were packing up to head home. As he looked around the room, he saw a familiar figure sitting at the same table reading a newspaper.

The remaining group members were all engrossed in their game, so Saul grabbed the report and made his way over to the man in the suit. "Hello, I'm Saul. Did you want this wireless report?"

"Hello Saul," the man replied. "My name is Michael and I've been hired by our employer to act as a go between. He's a very busy man but wanted to ensure that you were paid for your work. May I see the report, please?"

Saul laid the report on the table next to the man. "I think it's pretty much what he asked for, but if it's missing something let me know."

"What's this?" the man asked politely.

"Oh, that's the map I created. It shows the range of the wireless signals being transmitted by the hospital. The cool thing about this particular network is that it's central to the area around it, so anyone around that plaza can easily pick up the network." Saul replied.

"Hmmm, that's interesting," the man said. "I've got your money with me. We've decided to pay you under the table to avoid any tax liabilities for your work. I hope that's okay."

"That works for me," commented Saul. "I can easily put that into my own account."

"Saul, there is another piece to this work that we'd like you to perform, if you're willing," he continued. "We're very concerned about the security team at the hospital. We have very strict guidelines about network security and patient privacy and we're not quite sure the team is taking these obligations seriously."

"Okay, what do you want me to do?" asked Saul.

"Here's another document that explains everything in detail. If you have questions, please send them to the e-mail at the bottom," replied the man. "All I ask is that you don't share this information, including the e-mail address, with anyone else."

"I can do that. Thanks for the money"

"And thank you for the work. Now you should probably get back to your game. It appears your friend has noticed your absence." He nodded toward the group of kids across the room.

With that, the man stood up, said goodbye, and left the coffee shop. Saul hurriedly stuffed the two envelopes into his pocket to review later. "So it wasn't a hoax!" He could hardly contain himself, but was careful to act natural as he walked back to the table to pack up his gear.

"Hey man, where'd ya go?" asked Bender when he returned.

"Eh, I wanted to see if they had something to snack on up at the counter, but nothing looked good. Then I thought I saw someone I knew, but it wasn't anyone," replied Saul. "Dude, I think I'm going to pack up for the night. I'm exhausted."

"Cool man. Be careful getting home," Bender smirked. "You know how these streets can be at night!"

Saul laughed and walked around the table to pack up his laptop. "I can't believe I have $2,000 in my pocket. And he wants more work done! That's awesome!" Stuffing the last of his gear into an already over-packed bag, Saul grabbed his coat and headed for home.

Innocence Lured

Saul decided to take the bus home that night. Considering the package he had in his possession, it seemed wise to travel with a group of people instead of alone. His head was still fuzzy from the adrenaline of having so much money for doing work that he considered more of a hobby. For a young man his age, $2,000 was the equivalent of being rich.

When he got home, Saul unlocked the front door and started toward his room. His mother was asleep so Saul moved silently in the dark until he was safely in his bedroom with the door shut. Turning on the light, he pulled out the envelope. He was still in shock at the wad of cash in the envelope but turned his attention to the folded letter tucked away neatly in between the bills.

```
Saul,

I want to thank you for your hard work and discretion in this matter. Enjoy
the money, it was well earned. Now I'd like to ask for your help on another
round of work.


As before, we must maintain the highest level of discretion. My security
team at the hospital has grown arrogant. In fact, I've been told by my team
that they would know immediately if anyone broke into our network, assuming
that anyone COULD actually break into the network. From a management
perspective, this kind of attitude is dangerous.


I need you to continue your work in several steps. I've listed the specific
steps below. Should you need money to finance any of these steps, please let
me know at the e-mail address below and I'll ensure you have what you need.


1) First, I need you to create a network of rogue wireless access points
around the hospital that are bridged directly into the hospital network.
There are a couple of ways I can see this taking place, but the end choice
is ultimately up to you. This network of fake access points should make it
more difficult for my team to detect your activities, thus proving my point.

a. There are plenty of public locations around the hospital (in the plaza)
where you could set up wireless repeaters to bridge into the hospital's
network. You can either buy commercially produced repeaters or build them
yourself. My ultimate goal is to create enough wireless traffic that no one
will detect your movements on our network, even if they happen to be paying
attention at the time.
```

b. An additional option is to utilize a number of USB 802.11b capable flash drives to bridge the network. The hospital uses a lot of insecure desktop computers that all have USB ports enabled. By walking through the hospital and attaching this device to the back of an unattended computer, you could create an initial point of access into the network. Since this unit is a flash drive as well, you could potentially create an autorun file on the drive that logs keystrokes or auto-configures the appropriate network information as well. I'll leave that to your discretion.

2) You will have 2 weeks to get this network in place. At some point before the morning of the 15th of April, I want you to look for a patient record by the name of Matthew Ryan. I need to prove that an information compromise is possible, so I want you to log in and change the blood type of this individual from Type B positive to Type A. This should provide sufficient proof to my staff that our security is not up to par. Remember, this is our test record, not a real patient record.

3) Report back to me when the work is completed and I'll pay you five thousand dollars. Also, please e-mail me about what resources you require and I'll have them shipped directly to you so you don't have to order them yourself.

Thank you again for your discretion in this matter. I'll certainly recommend your services to my colleagues. You could have a thriving business before you know it. As a bonus for your efforts on this project, you can keep the hardware you order once the job has been completed.

Respectfully,

Knuth

knuth@hushmail.com

Spreading the Net Wide

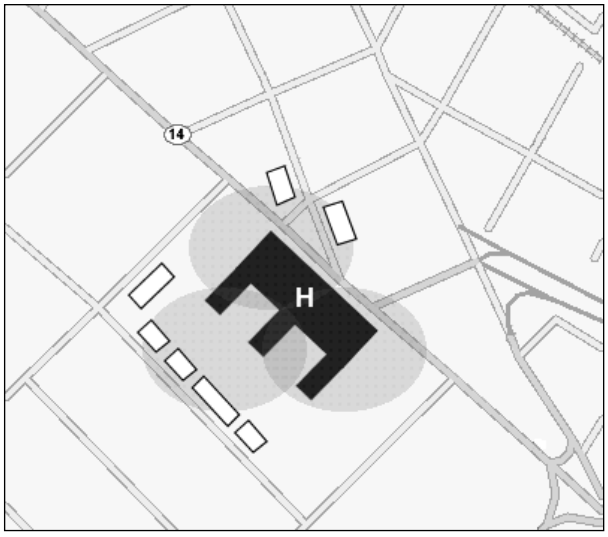
Saul folded the letter back up and stuffed it into the envelope with the cash. He quickly stashed the envelope between his mattresses to hide and sat back on the bed in shock. All the information in the letter was relatively easy to understand. He could see the logic behind the activities that Knuth was requesting and also the need for discretion. There had been many times in his very short career that so-called professionals had berated him for his ideas on wireless security. But when push comes to shove, the money wasn't bad. Saul was lured by the idea of

actually starting a professional career performing this type of work and Knuth could be the perfect contact he needed as a reference.

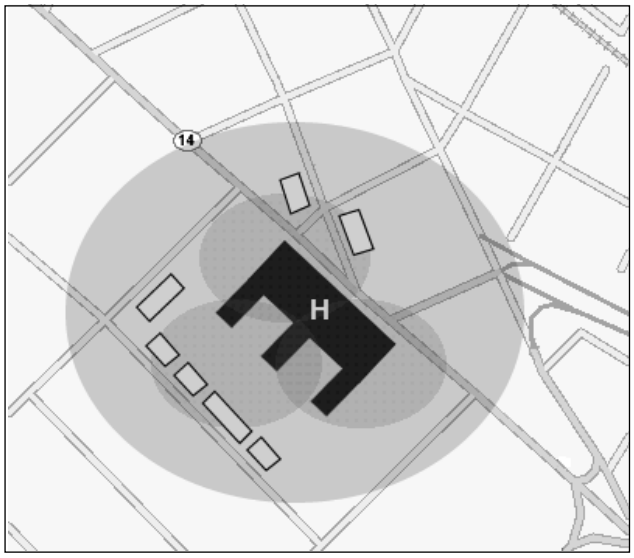
"The first thing I need to do is figure out what locations are best for placing some wireless bridges," Saul thought to himself. "Proper placement is key here if I want to inject as much miscellaneous traffic into their network as possible." Saul also knew that the signal from his wireless network would need to be stronger than that of the small cafés around the hospital. Saul thought to himself, "If I use the same type of access point as the hospital with a nice omnidirectional antenna, I should be able to extend the network cleanly and pretty much double the range of the signal."

Taking the map from his previous scans of the area, Saul began to draw in the cafés, shops, and other areas surrounding the hospital with a felt marker. The original map was created digitally on his computer, so Saul went back and updated the files on his computer with the new information. When he finished the map Saul noted to himself, quite happily, that with all the cafés and restaurants in the area that were now offering free wireless access to their customers, his activities would go quite unnoticed. It wasn't unusual to see people conducting business at an outdoor restaurant, or geeks hanging out at a local coffee shop after dinner checking their stock portfolios.

Map of Current Wireless Propagation



Planned Map of Wireless Propagation



Making Plans

The next morning he woke up energized. Saul knew he now had to look at this project in an entirely new light. What Knuth was asking would most likely be illegal in his country. His only saving grace was that Knuth actually owned the hospital and had asked Saul directly to do this. But to do this work, Saul would have to be more intrusive than he had been up to this point. There were areas that would require him to investigate the hardware and to actually connect to the hospital's wireless network and collect traffic. But it was apparent from the e-mail that Knuth intended for Saul to take this to the next level. Saul was excited to be doing this legally.

To bridge the wireless network, Saul had to know for sure that the access points being used by the hospital were actually Lucent AP-1000. This would require him to walk through the medical facility looking for an access point. He hoped they were hanging on the walls out in the open where they could be seen and recognized. Saul knew that his suspicions were probably correct about this but he had to be sure.

He also realized that there were potential issues with bridging the hospital's network to extend the range. The possibility that the access points participating in the network were identified and controlled by MAC address

filters had not occurred to Saul before now. The bridging within the hospital allowed a wireless user to roam from one area within the hospital grounds to another seamlessly, without losing their connection. He could always set up rogue access points outside the hospital, but this would only divert traffic from their network and Saul knew that he needed to actively participate on the hospital's wireless network. This required bridging.

The current configuration could cause serious issues for Saul because it would restrict his ability to bridge into the existing access points with his own hardware. "I'll need to figure out where the primary AP is and try to log in," Saul thought to himself. "If they have MAC restrictions turned on, I'll have to figure out a way to get into the AP management console and add the MAC addresses of the new access points.

Then there was the issue of housing the new APs in the local vicinity. The new hardware had to be within a reasonable distance of the existing wireless network in order for any bridging to work. He needed to figure out how to get wireless access points into the various locations around the hospital that he had chosen without appearing suspicious. Saul wondered to himself if any of the other kids in his hacking group had connections or jobs in this area and would be willing to help. "I could tell them that we're setting up free Internet access around the hospital as a test project," Saul thought to himself.

Plans Become Actions

The next morning, Saul jumped out of bed and decided to get started. He quickly threw on some clothes that were lying on the floor, grabbed his computer backpack, and went to the kitchen to grab breakfast. His mother was still passed out cold in the other room. "Must have been another rough night," he mumbled to himself as he grabbed some bread. "I can't wait to get out of here."

The first thing Saul had to do was figure out what he was dealing with regarding the hospital's wireless hardware. The quickest way to do this was to walk through the hospital. But in order to not look obvious, he would need to visit a part of the hospital that always had a lot of visitors. St. James was a large facility and there were lots of people going in and out almost constantly during the day. "I think I'll walk through the Patient Care wing. I can't imagine that it's that unusual seeing kids my age walking through there to

visit grandparents or such." Saul finished up his breakfast, put an apple in his bag, and went to catch the next bus to the hospital.

The sun was already blazing when Saul walked out the door toward the bus stop. It was late morning at this point and there were a lot of people already moving about. The bus stop was relatively close to his house so the walk was short and Saul soon found himself on his way back to the hospital.

Arriving at the bus stop, Saul found himself standing in the same plaza he had visited multiple times over the last couple of weeks. Staring at the massive structure, he decided he would just walk in the front doors and head toward the Patient Care wing of the hospital. "I'll just act like I know where I'm going and that I belong here." With that in mind, Saul headed toward the front doors, only slightly nervous about what he was doing.

As the doors to the hospital opened for Saul, the smell was immediate and distinct. This was a hospital. It smelled clean but gave off an aura of cold and distant inhumanity. The floors were standard linoleum tile and the walls were a distinct medical mint green color. He was still sweating from the heat outside and the cool air in the hospital felt good on his dark skin. Saul shivered to himself as he took a quick look around. "People die here," he found himself thinking. Pushing these thoughts from his head, he tried to focus on the task at hand and began walking down the corridor to the Patient Care wing.

The corridor was brightly lit and although the temperature in the hospital was comfortable, it still seemed cold to Saul. The nurses seemed to match the paint on the walls, all wearing mint green scrubs. As he approached the nurse's station for the Patient Care wing, he began looking along the walls for any sign of an access point.

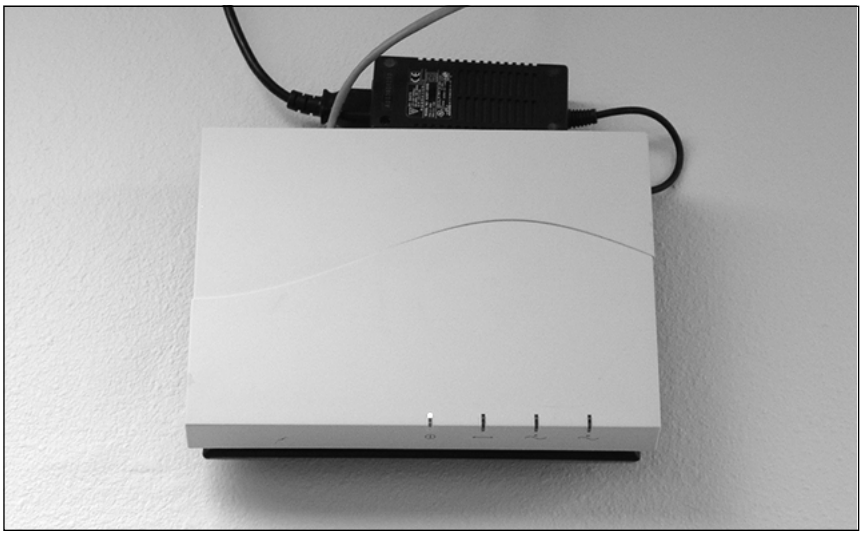
"Can I help you?" a young nurse with a nice smile asked Saul.

Saul jumped slightly in his skin. He cursed himself for being so easily caught off guard. "No, ma'am. I'm just looking for a toilet," he replied.

"Oh, then you need to make a right at the next corridor," the nurse said back. "The men's room is on the left."

The nurse didn't seem to see anything odd about Saul being in this area. As he was preparing to say his farewells and leave, Saul noticed what he had been looking for. Hanging on the wall, directly behind the nurse's station was a Lucent AP-1000 access point. He could easily see the two ORiNOCO gold wireless cards sticking out from under the white plastic cover of the AP.

ORiNOCO AP-1000



"Thank you very much," Saul replied happily. "I've been looking for the men's room for the last five minutes."

With that, he headed off in the direction of the men's room.

Breaking the Code

Saul left the hospital by the front entrance and walked over to sit down at a fountain. With the new information Saul had about the wireless network at the hospital, he knew he could at least start working on getting access to the management console of the access points. He knew he could locate the APs quickly by associating with the wireless network and running a port scan on the network. Nmap was free and worked well in situations like these, even though it tended to misidentify AP-1000 access points as an Apple Airport Base Station. He already knew they were Lucent; all he needed to know now was the actual wired IP address of the APs.

The real problem would come when he tried to log in to the management console of the access points once he did have the IP addresses. He knew the default username and password for the Lucent AP-1000 series was normally *admin* and *public*, respectively. But what were the chances that the hospital had not changed the passwords? Of course he would try those, but he could not believe that they would be left at their defaults.

He knew that his only other option would be to sniff the traffic on the network long enough and hope that he could pick up the appropriate username and password. "I need to ensure that the administrators try to log in to one of the access points so I can get the password quicker," Saul thought to himself. "If I can get someone to call in a problem to one of the access points, maybe the administrators will have to log in and find out what the problem is."

Saul thought about his options for a few minutes and then grabbed the apple from his backpack to snack. The day was definitely getting warmer as he sat on the edge of the fountain. Suddenly it occurred to Saul that the best way to cause a problem without actually breaking something or compromising his work was to use software to disassociate any clients from the access point in the area.

He knew that it was easy enough to spoof the MAC address of other clients and that by doing so he could disassociate the legitimate clients from the wireless network. His laptop was already loaded with software that could continuously scan wireless networks for association and data packets from wireless clients. A database is created that contains all of the client MAC addresses and continuously disassociates those clients from their connection on the access point. This would create a temporary denial of wireless service in the area. If Saul did this a few times for just a couple of minutes each, the administrators would have to check out the problem. He hoped this would work.

Saul pulled out his laptop and booted into Linux. First, he needed to run Nmap against the wireless network. This would require him to connect fully to the network by associating with a wireless access point. Since he already had the WEP key from his earlier scans, he configured his PCMCIA wireless card for the hospital's network and set himself up to receive DHCP information.

The connection took only seconds and Saul found himself with a working IP address on the wireless network. Saul ran the command **nmap -v -sS -O 192.168.1.0/24** on his laptop and waited for the results. Hopefully the stealth mode option would help him stay undetected.

Nmap Scan of the AP-1000

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (192.168.1.85) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.1.85)
The SYN Stealth Scan took 0 seconds to scan 1601 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at lea
st 1 open and 1 closed TCP port
All 1601 scanned ports on  (192.168.1.85) are: closed
Remote operating system guess: Apple Airport Wireless Hub Station v3.x
No OS matches for host (test conditions non-ideal).

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
root@mercury:/tmp#
```

Saul was able to find five access points using Nmap. He wrote the IP addresses down on a scrap piece of paper he had in his backpack and brought up a tool based on a wireless toolkit, called Radiate, that would disrupt the wireless network. "Just a few minutes at a time," Saul thought to himself. "That's all I need. Once the administrators get a few complaints, they'll be forced to check out the problem."

Before he disrupted the network, though, he knew he should try some basic brute force activities just to see if security was really that lax at the hospital. Trying the defaults wasn't working for Saul on any of the access points he had discovered so he began trying common sense words instead. Brute forcing isn't glamorous and Saul knew he could be at this all day with no success, so after just a few attempts, he decided to go with his plan and disrupt the wireless network.

Running the program was easy. It was run from a normal root user shell prompt under a Linux kernel. The only real stipulation was that the laptop be within a reasonable distance of the access point. He watched the output to the screen intently as multiple IP addresses on the wireless network were being displayed as spoofed and disassociated. The information on the screen was more for gauging the progress of the program. Since the program dumped this same information to a text file, Saul knew he could review it later.

Saul let the program run for only a few minutes and then shut it down. After giving the users about five minutes of time to use the network, he ran the program again and watched the screen as those users were once again denied access to their network. He ran this same routine a couple of more times before closing out his prompt and opening up a network analyzer window.

Ethereal is a cross-platform network analyzer. The network analyzer would sniff packets off the network and store them in a file for review. Saul could also watch the packets as they were collected in real time. He knew he needed that username and password in order to get into the access points at a later time.

With the sniffer running, Saul didn't have to wait long until he saw an attempt to log in to one of the access points. The username and password pair wasn't the default for an AP-1000, but it wasn't too hard. Someone logged in to the access point at 192.168.1.85 using the username *sysadmin* and the password *st.james*. The connection didn't last long, but knowing that he shouldn't try to access the management console today, Saul decided to pack up and go home for the day.

Along with the wireless information he had collected about the network, Saul had discovered several different IP addresses on the network that appeared to have database ports running. Any of these could have been the patient database, but they also could have been an inventory database for the cafeteria inside the hospital. He knew he would have to check out each individual database to see what information they contained. But that could wait until later, when he was looking for usernames and passwords.

Choosing the Equipment

The bus ride home was uneventful for Saul. He was tired and hungry. Saul walked straight to his room to go back over all the information he had gathered over the last couple of weeks. Sitting on the bed, he pulled out his laptop and papers and inspected what he had.

There was the map of the area around the hospital and the propagation of its wireless network. He had the username and password of a hospital access point. The Nmap scans of the wireless network that identified the access points was on his laptop along with the traffic he had managed to capture from his sniffing activities. All in all, it was a successful day, but the hard work was just getting started.

The fact that the hospital was using AP-1000 hardware for their network meant that Saul needed to use the same hardware for his rogue access points. It wasn't required, but using the same hardware made the work a lot simpler. With time being a huge issue there was wisdom in keeping things simple. Saul decided he would ask for more AP-1000s to maintain consistency.

The choice of antennas was fairly easy as well. The space around the hospital was wide open due to the plaza and Saul knew that meant that he could use a higher gain antenna. This would effectively expand the range of the wireless signal. He opted to use standard 8dbi gain omnidirectional antennas. Omnidirectional antennas would allow the wireless signal to travel in a 360 degree circle around the antenna.

So Knuth needed to know what Saul needed. He decided it wasn't prudent to tell Knuth all the details he had over e-mail, just in case the administrators at the hospital were nosey. Instead, he decided to keep it simple.

```
Knuth,
The project is going well. Thank you. I need the
following supplies to complete it.

5 Lucent AP-1000 access points
10 ORiNOCO Gold wireless PCMCIA cards
5 8dbi omni antennas that operate in the 2.400 – 2.440 Ghz range with N type
female connections
5 pigtail connectors with an ORiNOCO connection on one end and an N type
male connector on the other.

Saul
```

He finished typing his e-mail to Knuth and hit Send. It had been a long day and Saul was ready for dinner. Contacting his friends for help placing the new access points could wait until tomorrow. For now, he was going to get some food and relax.

Working with Friends

The next morning, Saul woke up early and got online. The plan was laid out and the equipment was ordered. Saul was satisfied with the way things were going up to this point. The next step was to e-mail the group and see if any one of the other kids in the group lived near the hospital or had connections there.

Saul decided to sell the idea to the group as a test of wireless network bridging. The fact that the hospital was in such an open area made it attractive for a project like this. Explaining the fact that the access points would be in

place for only a few weeks, Saul asked his friends if they could help. He hoped that with such a large group to work with, at least some of the kids would have access to the area.

His e-mail went out to the entire group and Saul spent the day in his house waiting for responses. He was surprised to find that he got four responses from his group members. Two individuals lived in the area because their parents worked at the hospital. Two other members worked at shops or cafés in the area and could easily arrange to help Saul out.

The equipment showed up on his doorstep two days later and included everything that Saul had requested. Carefully he started unpacking boxes and laid the items in small piles around his room. After double-checking that he had the right number of each item, Saul pulled the laptop from backpack and grabbed a network cable. He knew that he needed to list the MAC addresses of each access point and set them up for bridging mode.

Over the next two days, Saul worked with his friends to get the access points in place and ensure they were working. According to his rudimentary calculations, the range of the hospital's wireless network would be nearly doubled, which was his original goal. Next, he needed to start generating traffic on the network.

Saul sent an e-mail to everyone on the list giving them the information required to connect to the network. He told them that the SSID was stjames and the WEP key was st.james-hosp. "Set up your network for DHCP because the hospital hands out IP addresses automatically," Saul told them in his e-mail. "Please test the network as much as possible over the next couple of weeks."

Stepping Way over the Line

A couple of days after the network was finally in place, Saul was ready to go back to the area around the hospital. He needed to get some usernames and passwords from personnel at the hospital so he could access the patient database. In fact, he still wasn't even sure where the patient information was being held.

This was the part he had been waiting for. Knuth had given him complete freedom to hack directly into the hospital's network and change a patient record. This was going to be the fun part of the job. Pulling on a shirt and

pants, Saul started getting ready to leave the house. It was going to be a boring day in the plaza.

Saul packed some food and a couple cans of soda into his backpack along with his laptop. He bent down, lifted the top mattress of his bed, and took some money from the envelope. Having money was a great feeling and he may want to eat in a café while he was hanging out in the plaza. Grabbing the backpack, Saul walked out the front door and headed down the street.

The plaza was still relatively empty this early in the morning, so Saul sought out a nice shady spot to take up residence for the day. There was a large tree near the fountain that would provide cover for him while he hung out. Picking a spot under the tree, he unpacked his laptop and his school books.

Saul cursed as he sat down in the still damp grass. The morning sun had not reached the point of evaporating the dew under the tree yet. But he made himself as comfortable as possible and plugged in the wireless card. He knew he may need to sit here for the entire day in order to get the information he needed.

The laptop booted up into Linux and Saul logged in as the root user. The laptop was still configured to attach to the hospital's network so when he pushed in the wireless card, the laptop beeped twice and got an address from the local DHCP server. He was online.

Saul preferred to use Ethereal as his sniffer software under Linux. It was easy to use and the results could be stored and manipulated. Watching network traffic when no one was aware made him feel powerful. All those people at the hospital had no clue that their information was flying over the heads of thousands of people everyday. How easy it really was to get into the network. He brought up the application and started the long process of collecting usernames and passwords. Hopefully, one of the usernames and passwords he got today would help him log in to the patient database.

He pulled out one of his programming books and a notepad. Pretending to do school work was the best way he could think of to not look overly suspicious hanging out under the tree. Lots of people hung out here to get fresh air under the clear blue skies. The real reason for having the notepad out was to log usernames, passwords, and IP addresses that popped up on the wireless network.

The problem with sniffing on a wireless network is that you see only traffic being transmitted across the access points. Any wired connections just

won't show up. Saul spent the first half of the day logging information but was able to log in only to the database at the front desk for admissions and patient tracking. About lunch time, he decided it was time to eat so he pulled a sandwich out of his bag. "It's going to be a long day, again," he thought to himself. He was beginning to think this might take more than one day. "Don't any of the doctors or nurses use the wireless network?!?"

It was getting hot outside the hospital and Saul was sweating, even in the shade of the tree. More and more people had descended upon the hospital as the day lingered on. Medical personnel from the hospital were moving and out of the hospital, some of them eating lunch on the edge of the fountain and others checking e-mail. But still there were no account names that gave any clue to the patient database.

Saul sighed to himself and adjusted the way he was sitting. Just then, Saul overheard a conversation between two apparent doctors sitting nearby. Maybe there was hope after all.

"Hey Jorge, what are you doing after lunch?" asked one of the doctors.

"I've got a routine appendectomy. I forget what time it starts though," was the reply. "Why do you ask?"

"I've got an abnormal x-ray that I wanted to get your opinion on. It won't take long, if you have a few minutes," the doctor responded.

"Alright, let me check my schedule."

Right before Saul's eyes, the packets showing the doctor's login showed up on the screen. The doctor directly logged into one of the IP addresses that Saul had identified as a potential patient database. He was ecstatic. He finally had the information he needed. Saul breathed a sigh of relief.

But he could not leave until he had tested the information he had for himself. Saul was using a FreeTDS-based PERL script to connect to the database. It was rudimentary and didn't provide a constant connection, but it would have to work. Microsoft refused to release a Linux client to access their SQL Server database, so there were very few options. Besides, he didn't need constant access to the database, just long enough for a few transactions.

Logging into the database using the doctor's credentials, Saul performed a basic query to search for the name Matthew Ryan. Only one hit came back for the name Matthew Ryan. The name Matthew wasn't exactly a popular name in South Africa and Saul had assumed it would be fairly easy to bring up.

Looking around nervously, Saul decided to try and change the record. He felt silly being so paranoid when he had obvious authorization to be doing

what he was about to do. There was no one watching him. Saul reminded himself of the $5,000 he was going to get in a few days once this had been done.

April 15th was still two more days away. He had plenty of time. But Saul knew that he was here now and logged in to the patient database. Now is the time. "Make the damn change," he told himself angrily. "This is totally legit. You have been asked to do this by the owner of the hospital."

With that in mind, Saul made the query that would change the listed blood type from Type B positive to Type A. He wasn't a doctor but he knew that these two blood types were completely incompatible. "I suppose that was the point that Knuth wanted to make to his security team," Saul thought to himself.

The record had been changed and Saul needed to verify it one last time. Running the original query again from his PERL script, he got the record back for Matthew Ryan. The blood type had indeed been changed and Saul's work here was done. He packed up all of his books and gear and headed back home to notify Knuth.

The e-mail that Saul sent to Knuth that evening was simple.

```
Knuth,

It's done. Thank you for he opportunity. I hope to work with you in the
future.


Saul
```

Aftermath… Report of an Audit

I was called into St. James's (a relatively wealthy hospital in the South African city of Johannesburg) to perform an audit of the hospital's wireless network after a systems administrator employed by the hospital discovered that a rogue MAC (or Media Access Control) address had been added to the list of trusted MAC addresses on the hospital's primary wireless appliance. Although my initial thoughts were that a mistake may have been made by hospital staff, suggesting to the hospital that the purported "rogue" address perhaps had been added legitimately, through cross-referencing a list of all authorized hospital wireless appliances against the list of MAC addresses held on the master appliance, there was no doubt in my mind that a discrepancy was present. Further, a month-old backup of the wireless appliances configuration was checked against the current configuration. In theory, the configurations should have been identical, because no authorized configuration modifications had been made in over six months. But again, the very same MAC address appeared in the current configuration, but was not present in the backup configuration.

The information security organization I worked for is paid to perform wired and wireless network security audits in order to assess the vulnerabilities to which an organization is exposed. Our tests normally consist of running an out-of-the-box security scanner and formatting the report, outputted by the automated scanner in our company colors, complete with logos and other marketing fluff. To this end, dealing with a real incident was entirely new territory and somewhat out of my remit. But now I was interested, and since the hospital was a regular client, my line manager was keen for me to remain on site and help the client "in any way you can." Because of my lack of knowledge in this area, I spent the next few days reading through a handful of books recommended to me by a friend.

Over those two days, I attempted to cram my brain with information ranging from methodologies used for characterizing cyber adversaries, wireless "war drives," to performing forensic testing on compromised computer systems. The hacker underground sure did seem to be a far more complex and larger beast than I had ever previously imagined. Many of the tools that I discovered on the Internet were far more complex than anything I previously had used—the hacker training into the use of automated, graphical user interface security auditing tools that I had received from my employer was of no

use to me now. The tools and information I found were simply in another league than what I was used to.

After questioning several hospital systems administrators, it was apparent that no obvious system compromise had occurred as a result of any compromise of the hospital's wireless network, which may or may not have happened. With little information more than the rogue MAC address left in the wireless appliances configuration to go on, I decided that the best course of action was to use the techniques I learned over the past two days to perform a wireless audit of the hospital and surrounding plaza. To my surprise, the hospital wireless network appeared to be available for some three blocks away from the hospital itself. Among the wireless traffic being emitted from the hospital, I also discovered three or four wireless networks that appeared to be those belonging to several local cafés and local businesses. From my reading, I knew that wireless networks could travel at least two hundred feet, but had never come across a wireless network as widespread as the hospital network appeared to be—I knew something was amiss. Upon discovering this, I returned to the hospital to have lunch with Dan Smith, one of the systems administrators, in the hospital's restaurant facility.

Dan Smith was also the individual assigned to leading the incident investigation for the hospital, so he was my primary point of contact for any findings I made during the course of my testing. After disclosing the results of my morning's work, Dan asserted that the wireless equipment was thoroughly tested after its installation and was found to be available at (approximately) a one-block radius around the hospital's perimeter—a distance, which at the time, the hospital had determined to be an acceptable amount. After insisting that the signal I received must have originated from another wireless network and that my data was inaccurate, I was compelled to present Dan with the technical data I had collected that morning. The results displayed precise GPS (global positioning satellite) coordinates for each of the networks that had been detected by my laptop. In addition to the wireless network coordinates, my laptop collected sufficient wireless traffic to perform what I had read was an attack against the RC4 crypto algorithm, used to encrypt the hospital's wireless network traffic. Upon reading the hospital's WEP (Wired Equivalent Privacy) key displayed in clear text on my laptop screen, Dan's jaw dropped. After gazing at my screen for what seemed like three or four minutes, Dan made a telephone call to his superiors and scheduled an urgent meeting for

one hour's time, to which I was invited to present my findings. Although this was now well outside of my regular remit, the hospital was a good client, and I had been instructed to do all I could to aid the hospital in their investigation, so without hesitation I agreed to attend.

As I was collecting my equipment from the restaurant table, a middle-aged lady placed her hand on my shoulder and in a timid voice said "Excuse me, sir?"

"Yes, can I help you?" I replied. The lady was dressed in what appeared to be a white doctor's uniform; her name tag read "Dr. Sarah F. Berry." The lady claimed to be the mother of Daniel Berry, a teenager in his sophomore year who was purportedly somewhat of a wireless expert. Intrigued, I inquired as to why she thought he was such an expert on the topic.

"Well you see, he goes to these clubs where all they do is talk about wireless and security, and he was here just a few weeks ago with his friends helping to set up a new wireless network at the hospital," she replied.

Pretending not to find this information at all useful or interesting, I proceeded to make my excuses and leave the hospital restaurant in order to prepare for the presentation that I was now due to give in a little under 45 minutes. Hurriedly, I made my way to the office of Dan Smith to inquire into the legitimacy of Dr. Berry's offspring's activities over the past weeks. It became apparent that this was something of which Smith had no knowledge, and he pressed me for everything I had been told by Dr. Berry. Although Smith was impatient to confront Dr. Berry regarding the activities of her son, I explained that through what I had read regarding characterizing cyber adversaries and more precisely, potential "insider" cases, a direct confrontation often is the worst thing that can be done.

If Dr. Berry's son was indeed involved in the wireless incident at the hospital, he may well have retained access to computer systems and may be in a position to wreak havoc if he were to be confronted. Time was running out, and we agreed to take the discussion of what to do with Dr. Berry into the meeting with Dan Smith's superiors. As planned, I presented my findings to a naïve hospital IT management team. As with Smith, they, too, were keen to confront Dr. Berry and her son, a move I explained could cause more problems for the hospital. As an alternative, I offered to take responsibility for having a chat with Dr. Berry's son upon his return from the next meeting of his group in three days' time. I would pose as a reporter who had heard of the

hospital wireless project and wanted to write an article in a local paper regarding how local residents can get access to the wireless network.

The hospital records' office provided us with the home address of Dr. Berry and as planned, two nights later from my position outside of the address I observed a boy in his mid-teens leave the house at approximately 18:00 hours. Sure enough, some three hours later, the boy returned. I made my move and stepped out of the car. "Mr. Berry," I yelled.

The boy swung round and in a timid voice replied "Yes, but are you looking for my pa?"

"No," I replied. "Are you Daniel? My name is Simon, I work with your mother. She said that you were somewhat of a computer and wireless network genius, that you had something to do with the new wireless network at St. James hospital." As the boy approached me, he inquired as to my identity. "I am a reporter for the St. James hospital newsletter," I replied. "I would like to write an article in the hospital newsletter regarding the new network and how it makes the hospital one of the most technologically advanced in Johannesburg."

The boy laughed. "It's not *that* advanced!" he exclaimed.

"Well, perhaps you can tell me more about it?" I inquired.

He responded, "You'd be better off talking to my friend Saul. I just helped him set up some wireless appliances, Saul is the *real* wireless genius."

"How can I get in touch with Saul?" I asked. The boy reached into his backpack and pulled out a pad and pen. He scribbled down an e-mail address through which I could purportedly contact this Saul character. I thanked him for his help, and assured him that he would be credited for his help in the hospital newsletter.

As I turned away to return to my car the boy yelled out "Hey!" I turned around. "Please don't mention my name in your newsletter. My friends just call me Bender."

Chuckling under my own breath, I agreed and thanked the boy again. With that, he turned and ran off up the street to his home.

As far as I was concerned, this was all I needed; this was getting way too serious for a simple security consultant to be dealing with. It was time to inform the hospital of my full findings and recommend that law enforcement be informed of the incident.

I rushed home to draft my report for the hospital, and if the hospital chose to, for the consumption of law enforcement officers.

Dear Sirs,

I have been called upon by my firm (on behalf of St. James hospital) to investigate the possible wireless compromise that purportedly occurred over the past three or four weeks.

Although it was my initial inclination to believe that the purported event was perhaps a false alarm, an audit of the hospitals wireless appliance configuration indicated that certain unauthorized activities had indeed taken place.

Wireless appliances often contain a list of "authorized" appliances to which they can "talk." These addresses are often referred to "MAC" addresses or a HW (Hardware) address.

All rogue addresses that had been added to the device shared the same hexadecimal prefix to the devices used in the hospital, indicating that rogue devices used to ultimately expand the hospital network were manufactured by the same firm (Lucent) as the wireless appliances used legitimately by the hospital.

From my reading of various publications pertaining to the characterization and attribution of cyber adversaries, it is my opinion that whomever carried out these attacks against the hospital wireless network was both fairly skilled and well funded or resourced. After carrying out a number of what are known as "war walks" around the hospital perimeter, I found that at least four, perhaps five wireless access points were used to extend the hospital's wireless coverage. This is not the sort of equipment that most people have laying around in their basement, let alone the purported perpetrators, a group of teenage boys.

Several days into the investigation, Dan Smith and I sat in the hotel restaurant to discuss my day's findings. As I was about to leave, a Dr. Berry, who I presume overheard our conversation, approached me to inform me that her son was an expert in wireless networking and security and would be an invaluable resource in whatever it was we were discussing (Dr. Berry was clearly not technical in this area). Further to this, she informed me that her son was at the hospital only two weeks ago "doing something" to the "new" wireless network at the facility. On discussing this point with Dan

Smith, these activities were carried out without the knowledge of Dan or any of his team.

With the above facts in mind, I engaged the son of Dr. Berry, posing as a reporter for the hospital newsletter, claiming to be writing a story on the "new" wireless network. Of course, while I didn't indicate otherwise to him, her son genuinely believed that his activities were legitimate, directing me to a friend of his named "Saul" who was apparently the individual responsible for arranging the activity. Accordingly, I have passed his e-mail address, provided by Dr. Berry's son, to Dan Smith.

The following questions remain. The hospital wireless network does not offer any kind of Internet access; it simply acts as a gateway to the hospital network, allowing doctors to modify patient records and other data from their wireless PDA device.

To this end, who would want to extend such a network, and for what purpose? Given the highly sensitive nature of the resources that are potentially accessible via the hospital wireless network, it is very possible that whomever orchestrated this project was interested only in the theft and potential modification of patient data. Given that we already have determined that those behind it were well resourced, both financially and technically, apparently making use of individuals who believe what they are doing is legitimate, I am inclined to suggest that whomever is behind this is highly determined, and whatever it is that they want, they clearly want it badly enough to invest considerable resource in getting it.

I have therefore recommended to a slightly dubious Dan Smith that his administration team consider disabling the hospital wireless network until law enforcement have concluded their investigation into who it was and why it was that the hospital network was extended to an almost three-block radius outside of the hospital's perimeter fence.

Regards,

Simon Edwards

Mickey Mouse Security LLC

"Running automated scanners since 1998"

So there it was; as far as I was concerned this was now in the hands of law enforcement and the hospital administration. I didn't tell Dan or my employer directly, but whoever was behind this probably has already gotten what they wanted from the hospital network. And from what I have read about hackers—well, put it this way—this wasn't just a lame Web site defacement or a denial of service. Whoever was behind this was well resourced, highly capable, and highly motivated about what they were doing. In a place like a hospital that makes for a pretty dangerous person.