Standards Today

A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG
GesmerUpdegrove LLP

March–April 2010 Vol. IX, No. 2

THE ALEXANDRIA PROJECT :

Chapter 2: The Plot Thickens

Andrew Updegrove

*New to The Alexandria Project? Find a **plot synopsis and guide to the characters** here, find the earlier chapters here, and follow the Further Adventures of Frank on Twitter*

Frank wondered how long his phone had been buzzing. He was about to turn it off when he saw that it was his daughter Marla calling.

"Hi Kid," he said, "Listen..."

His daughter jumped in. "Hey, Dad, thanks for picking up. I considered worrying about you for a second, and then figured you'd never really jump out the window – you're only on the second floor, after all, and broken bones don't solve anything. I mean, you're just much too logical not to think of that.

"So how's your big morning-after-the-night-before coming along?"

Frank tried to escape again, "Listen, Marla, this just isn't a good time. I'm in the middle of something, and…"

"Right. Fat chance YOU got lucky last night. I'll be right over." She hung up.

Frank looked helplessly at the phone. He started to call her back, and then snapped the phone shut. She wouldn't answer anyway.

Frank turned back to his laptop and took stock. All he really knew so far was that a file directory in the most secure part of a government computer system had been compromised by someone with hard to guess motives. That, and the fact that whoever had broken in either had a snarky sense of humor, or wanted to lead him

down the wrong path – or both. No matter how you looked at it, there wasn't a lot to work with.

Frank's fingers drummed on the kitchen table for a full minute, and then opened the Alexandria Project screenshot again. This time, Frank opened it using a photo editing program. But cleaning the image up as much as possible uncovered no new clues. More finger drumming didn't help, so for want of anything more productive to do, he deleted the Greek text, typed in the English translation where the Greek characters had been, and stared at it some more.

Frank wondered how seriously to take what had just happened. After all, someone with truly malicious intent would never have left a message. Instead, whoever had launched the exploit would do everything he could to avoid detection. But if the intruder wanted his exploit to be known, what exactly was he trying to prove? Perhaps he was just showing off.

That would still be troubling enough, Frank thought, given how deeply inside the LOC's defenses the intruder had penetrated. And what if the files the mysterious cracker had decided should be "contributed" had been really important files? Or files that had just been created, and hadn't yet been backed up?

On a hunch, Frank started typing again. A few new passwords and a number from a different RSA SecurID token than he'd used before, and he was staring at the same directory at the offsite backup center for the Library of Congress. He hesitated, and then clicked on the enter key for his security proposal. Nothing. And then the following message appeared:

> *The material you have requested is being catalogued by the Alexandria Project Acquisitions Department*
>
> *Please try again later*

Frank was impressed; he also had to grudgingly admit he liked the guy's sense of humor. Whoever had hacked the LOC's system was good – really good. He had not only penetrated the LOC's primary security system, but managed to pass a virus through to the Library's backup site as well, thereby ensuring that whatever had been "contributed" was gone for good. That was truly disturbing. If the cracker could do that with one file, theoretically he could do it with every file on every server available from his point of entry. Frank would have to put some real effort into working this one out.

And then it struck him: why bother?

Frank smiled slowly and leaned back, all of the tension that had been building up inside him disappearing all in a rush as he laced his fingers behind his head and stretched his legs out under the table. This was actually rather cool, wasn't it? No, he corrected himself, this was really, *really* cool.

Up until that moment, Frank had been secretly dreading checking his email. Now he opened it with relish.

Yes, there was an email from George waiting for him. Frank grinned wickedly as he read the subject line – in all caps, even: "WHAT IS THE ALEXANDRIA PROJECT?"

"Great question!" Frank banged out happily. "Better get Rick on that right away!" He hit the "send" button with a flourish, and leaned back again, staring gleefully at the screen as the message disappeared.

Frank poured himself another cup of coffee and toggled back to the screen with the Alexandria Project logo in translation. Now he saw it with a new sense of appreciation. It actually was an awfully good looking image, wasn't it? Just right to replace his old screen saver. Amazing how quickly a day could take a turn for the better.

Just then he heard a knock, followed by Marla's key rattling in the door down the hall. Frank got up to usher her in.

"Hey, kid!" he greeted her, smiling broadly. "It's great to see you."

"My, you sound perky," she said, looking at him with curiosity. "I thought after last night's little passion play I'd find you huddled in the corner in a fetal position, moaning softly."

For all our wealth and strength, any third world country – or even a terrorist organization – can theoretically crash an entire agency – or, for that matter, Wall Street – if they put some smart guys to work on it

Marla put the bagels and fruit she'd brought with her on the kitchen table, and then went into the hall to hang up her coat. Returning, she found her father standing behind his laptop with arms crossed, and a goofy grin spread across his face.

"So what gives, Charles Atlas? Somebody else holding all the world's cares on their shoulders for you this morning? I haven't seen you look this happy since Rush Limbaugh got busted for popping illicit pain pills."

Frank just continued to grin and pointed at the laptop. Marla's face looked a question, but she didn't want to ask for an explanation if her father hadn't chosen to offer one. She sat down and stared at the screen, searching for clues.

"Okay," She said. "So you've found a new charity you like, and that makes you all giggly?" Frank just raised his eyebrows, so she looked at the screen again, vexed that her father had posed a riddle she couldn't solve.

Finally, she had to give up. "Alright, whoever you are, what have you done with my cranky old man? I'm not saying this isn't a huge improvement, but unless you agree to keep him, you might as well let him go now."

Frank traded the goofy grin for a simple smile and sat down. "Sorry to be so mysterious," he said, pouring her a cup of coffee. "It's just that it's not every day I get to savor something this delicious. And this really is good."

"Fine," she said. "Now share."

"So here's what's up: you've certainly figured out by now that I expected to get the project that Rick was given last night. And you've also assumed, I'm sure, that it was a security project, or my nose wouldn't have been so far out of joint." Marla shrugged. Of course that much had been obvious, but she didn't want to embarrass her father further by admitting it.

"If so, you're right on target. Now here are two things you don't know: first, the project is an important one: the boys up on the Hill suddenly have their knickers all in a twist about cybersecurity. And it's a damn good thing they do, too, because there are bad guys out the wazoo out there with plenty of reasons to want to tuck it to us – North Koreans, Revolutionary Guards from Iran, the big boys in Al Qaeda, wherever they're hiding out, criminals in Eastern Europe and Russia, and who knows who else. And the easiest way to wreak havoc on the only remaining super power in the world is via an Internet connection.

"Isn't that a bit of an overstatement, Dad? I mean, with all the money we spend on defense, how could some rogue nation, much less a criminal outfit, manage that?"

"How? Because we haven't done enough to prevent it. In fact, it wasn't until last June that the Department of Defense formally acknowledged that cybersecurity protection needed to be part of national defense. That's when Secretary of Defense issued an order establishing a Cybersecurity Command - but it won't be fully operational until this October. That's just the first step needed.

"And that's pretty scary, because if you think about it, our $600 billion annual defense budget makes us more vulnerable, not less so. Why? Because everything we do now is controlled by computers – all the bombers, all the rockets, all the ground troops – everything. Worse, it's all controlled through the Internet.

"Sure, the government uses passwords and firewalls and all that, but data still has to get in and out or it isn't useful. The CIA bigwigs at Langley have to suck information in from their resources all over the world, and they also have to get instructions back out to their agents in the field. Same with the Department of Defense. The generals and civilian managers back at the Pentagon need to bring information in and send orders back out. All that data is spewing in and out like a giant fire hose – video from predator drones flying over Afghanistan, satellite data

from all over the world, battlefield intelligence from spotters in forward positions, and much, much more – gigabytes of it every hour.

Marla looked unconvinced. "Okay, so why is this any different from the old days, when all they had were secure telephones and secret codes for anything that went out by radio? It may be more information now, but aren't the challenges just the same?"

"Yes and no," he admitted, "and the 'yes' bit is by far the smallest part. The first thing to realize is that in the old days, besides sending paper documents by courier, all you had to worry about were voices and Morse code signals. Both of those data streams relied on "analog" technology – telephones and radios generated electric, and electromagnetic, pulses. Even if a bad guy managed to intercept the call or transmission, all he could do was record it and play it back later. These days, of course, we can send all kinds of information electronically in addition to voice - everything from text to spreadsheets to video to radar images to you name it. And all that information is transmitted as "digital" data – as you know, that's just ones and zeroes. But those ones and zeroes can be analyzed, stored, searched, repurposed and altered in ways that a voice recording never could.

"So?" Marla asked. "That should just make things a whole lot easier to deal with, shouldn't it? I mean, computers can just encrypt all that information automatically, right? In the old days, someone had to use code tables and other tricks to encrypt messages at one end, word by word, and then someone else had to do the same thing in reverse at the other end before they could be read. And if someone broke the code and you didn't know it, you were cooked. Remember how the Brits cracked the Nazi's Enigma machine code and the Germans never figured it out.

"All that's true," Frank said, "but there are some important differences. Back when most information existed only in paper form, it was easy to control how many copies of a top secret document there were, and who had access to them. And you could put them behind walls, locks and guards. Now they're all on servers, and those servers are all linked together, and…"

"Ok, Ok," Marla interrupted. "You've ranted at me about this often enough before."

"Hardly ranting," he said primly. "Simply fulfilling a father's duty to pass along important information to the next generation." Marla made a face at him. "But to continue: every day, every big enterprise is adding new computers for new employees; swapping out old routers as part of normal maintenance; updating obsolete software and adding new programs. All of that has to be done according to strict protocols, or it introduces points of vulnerability. And as you know, when you allow email to be received, bad stuff can come in that way, too.

"These are all very real vulnerabilities. Every moment, the bad guys are probing our systems for gaps in our defenses. It only takes one vulnerability to allow a bad guy to get something through the firewall, and it may be very difficult for us to find

it thereafter. Once it's inside, it can start prowling around, and when it finds what it's looking for, it will try and open up a port so it can send that data back out again to whoever planted it in the first place. Or maybe it will corrupt or delete the information so it's no longer available, or perhaps subtly alter it in such a way that while it may seem fine, it's actually no longer trustworthy.

"Or maybe the virus just sits there, like a living member of a sleeper cell, just waiting for the right time. You don't know it's there, but it is. One day its clock runs out, or it gets a signal from outside, or maybe even gets triggered by something inside it's been waiting for. Then it does something truly destructive, like take down a key system just when it's needed the most.

Marla broke in. "OK, I'm appropriately impressed. But if this is so dangerous, why don't we hear more about this kind of risk?"

"But you have, my dear," he replied. "Do any of these names ring a bell? Heartland? T.J.X? Hannaford Brothers?"

"I remember hearing the name Heartland before. Wasn't that the big credit card security breach that was in the news awhile back? So I'm guessing the other two were also security breaches, right?"

"Bingo." Frank nodded. "In the biggest breaches, like those, the credit and debit card information of millions of people gets compromised, and often even by the same guy, a cracker named Albert Gonzalez." Frank had been pulling Gonzalez's mug shot up on his computer while he was speaking. "Here - that's the guy."

"Hmm. Not a bad looking hacker," Marla observed appreciatively, watching her father out of the corner of her eye.

"Cracker!" Frank corrected her. "Crackers wear black hats. Hackers aren't criminals. Your father is a hacker."

"Whatever," Marla responded emphatically. "Are we getting any closer to the point here?"

"Yes," Frank replied tartly. "And I doubt Gonzalez will look like that by the time he gets out of Federal prison. Anyway, in the data breach you remember, Gonzalez got a virus called a "sniffer" inside the firewall of an information processing company that sits between the merchants downstream that take in credit card information, and the financial institutions upstream that complete the card transactions.

"What a sniffer program does is look for information, and when it finds what it wants, it sends it back to the cracker that planted it to begin with. All it took was one employee adding a wireless router to the system and forgetting to set the security settings up properly. Probably in no time flat, the automated software Gonzalez was using found this vulnerability, and in went the sniffer. It was two years – and 40 million pirated customer records - before Heartland realized it was broadcasting sensitive personal financial data to criminals.

"Okay, so a company goofed up," Marla objected. "I would certainly expect our government to be much more careful."

Her father raised his eyebrows, and Marla paused. "Or maybe not," she admitted.

Frank smiled smugly and continued. "Unfortunately, the federal government is a lot like the credit and debit card system – it's got thousands of locations with computers, countless types of hardware and software products in use (and changing) at any time, and millions of people who might be a little bit lazy or not well enough trained. So every government agency has thousands of points of potential vulnerability. All it takes is one careless moment by one individual, and this time it could be the Department of Defense, or the CIA, or the White House that gets the sniffer.

"And it's worse than that," Frank continued. Check out this article in the New York Times, which describes a recent top brass meeting on how the U.S. could respond to a cyber attack:

> The results were dispiriting. The enemy had all the advantages: stealth, anonymity and unpredictability. No one could pinpoint the country from which the attack came, so there was no effective way to deter further damage by threatening retaliation. What's more, the military commanders noted that they even lacked the legal authority to respond — especially because it was never clear if the attack was an act of vandalism, an attempt at commercial theft or a state-sponsored effort to cripple the United States, perhaps as a prelude to a conventional war.

"And what state are our defenses in? Check this quote out:"

> William J. Lynn III, the deputy defense secretary, who oversaw the simulation, said in an interview after the exercise that America's concepts for protecting computer networks reminded him of one of defensive warfare's great failures, the Maginot Line of pre-World War II France.

"So I'm getting the "not good" part here loud and clear." Marla acknowledged. "But what does that have to do with you and Rick and the LOC? And what does it especially have to do with the gnomic message on your laptop, by the way? Remember your laptop? I believe it's what I see on your laptop we were actually talking about."

"I'll get to that." Frank responded, but Marla groaned and put her head on the table; she was all too familiar with simple questions posed to her father that were still unanswered fifteen minutes later.

Frank made a face this time. "Alright. I'll move on. But just keep this part in focus: for all our wealth and strength, any third world country – or even a terrorist

organization – can theoretically crash an entire agency – or, for that matter, Wall Street – if they put some smart guys to work on it.

"Fine. I'm appropriately terrified. Now Daddy, make your little girl feel warm and secure again. You are going to make it all better now, aren't you? Please?

Frank smiled ruefully. "That's a tall order. But I will tell you what we're trying to do about it, or at least the non-classified details that make their way down to someone at my level.

"The new administration is much more aware of cybersecurity than the old one, thank goodness, and more creative, too. They've decided to take a competitive approach to the problem and have told every single agency and semi-independent department, like the LOC, that it has to design its own security plan – and fast. We've only got until February 28 to submit our security proposal to the White House.

"And that's a really good idea. The thought is that if we get fifty different teams competing, we'll come up with a lot more clever ideas than we would if we had just one design team. And if we cherry pick the best ideas that come back, we'll get better system-wide solutions than if we hired just one outfit to design a plan. Even better, we should be able to come up with and implement several different system plans, rather than just one. That way the whole government won't be vulnerable to a single attack across the board, or as likely to permit a successful exploit in one agency to infect another once it's inside the first one.

"And George thinks that Rick is going to be able to pull that off better than you?" Marla looked both dubious as well as offended on her father's behalf.

Frank suddenly looked less cheerful. "Yes, and George may be right. This is one of those projects that requires getting a whole lot of people on the same page. It will take lots of meetings; lots of compromises; lots of cajoling. That's not exactly where I shine. Last night I could have punched George in the nose, but this morning I have to admit that everybody else would probably want to punch me within a week if I was in charge.

"Still having trouble with that 'smartest guy in the room' problem, huh? And it sounds like it would involve actually having to talk to people. I know how that makes your day.

"It's not only that," her father replied wearily. "Yes, I'd be frustrated when some people couldn't keep up with me. But at the same time, I probably wouldn't focus well on the big picture, either. Plus, whoever is in charge is going to have to spend a lot of time grinding away on administrative details, and I get too impatient.

"Finally, anybody that tackles something like this has to balance what's perfect with what's practical, so that overly strict security requirements don't bring everything to a standstill, or require people to do more than you can actually get them to do. And that rubs up against the purist in me. In order to come up with a really good solution, we need to take into account how people really act. Otherwise, people will be tempted to take short cuts that leave security gaps.

"In short, doing something like this takes lots of things I just don't have the patience for, or for that matter, much talent.

Marla interrupted him and gently changed the subject: "So what about this Alexandria Project thing?"

"Ah yes!" Frank responded, brightening considerably. "It seems that my good friends George and Rick may be facing a deadline that's much earlier than they expected, and a challenge that I bet is a lot more than either of them bargained for.

Read the ***next chapter***

Read the ***last chapter***

Email this chapter to a friend

Follow Frank's Further Adventures here and on twitter