AmericanRhetoric.com

Dan Farmer

Opening Statement before Congress on the Threat of Computer Espionage

11 February 1997

[AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio]

I'm afraid I don't have a lot of good news to say you in my 10 minutes as well. Just to forewarn you. Briefly, I'm going to talk about security programs and sort of the state of the Net as I see it.

Security programs are nothing more than other programs you might encounter such as Lotus 1,2,3, Excel, Notes, whatever. They're just programs written to do things. And typically they fall into one of two categories: offensive and defensive programs.

Now, unfortunately for perhaps the good people in the "white hats," the defensive programs have been far outstripped by the offensive programs. It's much easier to build a gun than it is to build a wall that's going to stop this kind of weapon. And the offensive tools generally do very simple things. They can either, as Geoff [Mulligan] commented, they can disable a machine by a denial-of-service-attack, or some other form of attack. They allow you to spy on people, capture transmissions, or essentially they allow you to take control of the machine, whether it's individual files or the actual hardware itself.

And programs can do anything to a computer. Anything that can be done by a human being typing on a computer can be done by a program that takes over the computer. I just want to emphasize that. In 1988, probably one of the most influential and famous security programs ever was released -- the Internet Morris Worm, written by Robert T. Morris. And what it did is -- at the time the Internet was about 50,000 systems, broken into about 10 percent of the systems, about 5,000 systems -- and it was just as if someone was individually typing in and attacking all these systems by hand. But the age of automation makes this considerably more easy and very much more effective.

Almost 10 years later now, this last December, I decided to take a look at the network today and to examine, "Have we gone any further?" The Internet is pretty ubiquitous. Almost everyone is on it, including the Congress, the Senate, and the White House. And what is the difference, if any, between the physical and the virtual realms? Is there any difference in terms of security?

So I examined banks, government systems, newspapers, other very highly visible, highly laden with information content and sometimes financial content systems, and found that just using the most simple tasks -- not even trying to break in at all -- I could easily compromise about two-thirds of the systems. And I'm talking about, you know, things like the White House website and so forth. These are not, you know, "Joe's Garage and Website." And I estimate if further tests were done, you could probably break into about three-quarters of the systems.

So I estimate, on the Internet today, you have about a, you know, 75 percent vulnerability rate on all systems out there. For instance, with the government, we had the CIA and the DOJ recently broken into -- their websites -- and there should be no excuse for this. If the CIA cannot protect their own information, their own resources, how can you expect a business to do this that has, you know, one orders of magnitude less resources and such.

When I was doing the survey, I discovered that there was a problem with the White House security on their website. I sent them mail -- to the system manager -- and I never got a response. I explained that I was a security researcher. I'd found a significant problem. They never responded to me. If this was a physical problem, if I'd talked to the Secret Service about something that was a physical issue with the White House security, they would have [been] immediately on me, or perhaps taken me away with, you know, the men in black suits.

But the important thing is that there's a big disparity of how we view physical and how we view virtual security. We think of them as kind of being the same as a consumer, but when you actually get down to the actual physical operations and running these things, they're treated very differently.

Now there's banks, and Internet commerce being done -- 30 billion dollars, was it? And you would think that with this amount of money at stake they would know what was going on. Again, [I] run into the same sorts of issues. We're talking about real dollars that are at stake here.

Newspapers: There's an old *Bloom County* strip where Oliver, the little hacker boy, goes into *The New York Times*, breaks in, and changes a Reagan quote to say...women are "America's Little Dumplin's" or something.[1] And it was a joke at the time, but you can do this now. You can break into *The New York Times*. You can go into *Reuters*. You can go into the wire services and make headlines.

And it's not just pa[p]ers. We're talking about actual physical press. And in addition, we're getting more and more of our information from the electronic sources that are easily mutable. I was talking to CNN a few weeks ago and they said they were about six seconds from airing that George [W.] Bush had died in Japan because of the food poisoning incident.

What would be the impact if the President dies on the news, or that even something like there's an early freeze in the Florida orange groves? How is this going to affect prices of such things? And who's going to check on these things? And how can we tell what is actually going to happen with our electronic information? And how can we validate and verify this kind of thing?

In the military -- I was once a Marine...with hair significantly closer to yours than it is now[2] -- and I know how they use computers. They put all their stuff online, on their computers, and then a gunny or staff sergeant will sit on the computer and they'll dial up the Internet; or they'll dial up the local BBS, without any knowledge of how the information is stored on the computer and how it might get out.

I was at the Watergate last night, the Watergate Hotel, and it struck me perhaps what needs to happen now is that a Senator or Congressperson, perhaps the President, will get their information taken from their computer and somehow it will be used by someone else, or be publicized in a very public thing -- maybe, you know an "Electronicgate," an "E-Gate" of some sort in the future...It seems that we only react to disasters.

There is lots of stuff on all of our computers. Most people, certainly in businesses, and most people in government, use computers now for sending, you know, campaign funds. We had heard about the White House has this huge Rolodex of campaign funds. What if somebody went in and modified, or was able to publish, this kind of thing? This is really serious stuff we're talking about here.

And when I go to people and I say, "Well, I work in computers," their first response is: "Oh, I know nothing about computers. But my daughter..." or "my son is the real whiz." There's a real resistance to even listening to anything about computers. We're trained and such that somehow computers are difficult, or somehow they're beyond our comprehension; and so we'll just ignore them and hope they'll either go away or we'll die before they get too important.

So where are we now? The Internet now is -- I was talking to someone at AT&T and their internal network now is larger than the Internet was when the Internet worm hit. We're talking about orders of magnitude in size difference. If someone took the existing worm code that was used then, put in new tests[?] [and] all this kind of stuff, [it] wouldn't take much work. We could probably get about a five percent saturation hit rate on that. That means like something on the order of a million computers compromised in a couple of hours. That's a lot of machines. And a lot of those machines are machines that you people are depending on every day for your kind of transactions.

And just in closing, I would hope that the government does not try to throw billions and billions of dollars into some black hole, into buying the latest and greatest hardware or software. That is not the answer. These problems are not technical problems. These are real social problems we're facing here. I mean, it's not hard to defend a system. It's not hard to protect a system. It takes a lot of resources and it takes a lot of education. And I hope that any efforts on your part will fund these. Thank you.

[1] Full quotation "Reagan Calls Women 'America's Greatest Resource'" changed to "Reagan Calls Women 'America's Little Dumplin's'" [source: https://en.wikipedia.org/wiki/Toons_for_Our_Times]

[2] Just prior to Mr. Farmer's opening remarks, obviously balding USHOR subcommittee chair Vernon Ehlers quipped that "as an individual who is follically challenged I do have a bit of envy of you, Mr. Farmer."