All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Misimpressions by decision-makers (with update at the end)

To some extent his whole series of articles is about the lack of understanding by decision-makers. But this particular write-up stems from attending the Panetta Institute for Public Policy lecture on March 14. The experts were indeed knowledgeable about their fields from the perspective of a non-expert, but then most folks are. The stark lack of basic understanding in cybersecurity by those who have been in extremely responsible positions in US policy decisions leads me to doubt them in other areas, where I know far less. Not good...

The policy experts

Mike Rogers was chairman of the house Intelligence committee, an FBI agent, an Army officer, and a congressman. Wendy Sherman, perhaps the most impressive one of the group, was an ambassador and lead negotiator in the Iran deal that slowed or prevented the proliferation of nuclear weapons, and also a key player in many other high consequence decisions and negotiations. Gen. Ray Odierno was commander of US forces in Iraq, chief of staff, commander of joint US forces, and on the joint chiefs of staff. Very impressive folks.

Their view of cyber-related issues

The panel expressed at least the following issues that I found particularly insightful:

- The US offensive cyber capability is truly extraordinary and incredibly strong.
  - The major problem is that when used, they may have difficulty limiting the effects.
- The US cannot gain access to an iPhone without Apple helping them.
  - If the negotiation were done less publicly, it might have been settled amicably.
- The US must gain access to encrypted content to succeed in counter-terrorism.
  - We need access to any and all content to achieve national security.
- Cyber attack on critical infrastructures could take out power for weeks or months.
  - We don't even know how long such an outage would last.
- Our experts are working on / will find ways to safely have unlimited authorized access.

Why did I find this insightful?

My insight comes from the inconsistencies in the views and the lack of understanding the participants seem to have in that they don't even recognize that they are self-contradictory.

As examples:

- The US has an incredibly strong and truly extraordinary offensive cyber attack capability, and yet we cannot access the content of an iPhone.
- Cyber attack on critical infrastructures could take out power for weeks or months, and yet we need to weaken defenses to gain unlimited access to increase national security.

- We will find technical ways to have unlimited authorized access, and yet we will be safer because nobody else will be able to gain or misuse such access.

The first two are quite ridicule-able and I will ridicule them presently. The third is more interesting because it merely flies in the face of the apparent nature of humankind and thousands of years of human history, including very recent US government history.

Like the clipper chip before, the hardware devices being developed to capture, store, and allow exploitation of all input and output, and whatever is coming next, the US government seems to think that people and industry worldwide will accept, properly implement, and use devices intended by the US government to grant unlimited access to systems and content. Here are some simple problems that might impede such an approach:

- The people don't trust the government and will subvert it.
- The other world governments will subvert the system.
- It will further weaken critical infrastructures.
- Many people (and mostly the bad folks) won't buy it as long as they have a choice.
- Add-ons will provide added security, at least for the bad guys.
- The US government will have to make “secure” versions if only for their own use.

If the US has such a strong cyber offensive capability, why can't we even access an iPhone commercial product not even made in the US, and how will we stop its use elsewhere? I have to conclude that either (1) the whole inaccessibility thing is a ruse or (2) the US offensive capability is not really that good at all. They both make sense of course, and this is what classification has brought us. Indeed they might both be true. But perhaps it's just that using the capability for such an unimportant matter would leak the secret of what the US can do, or perhaps the folks in government would rather weaken protections to gain access and this is their excuse. Or perhaps … the list is endless. The point is that national policy on encryption in specific and cyber-security in general has sewn two long-term effects now being reaped.

- Our defenses are far weaker than they need or ought to be, so we can break them.
- We are losing economically by forcing security technology R&D to be moved abroad.

It's a lose lose situation and the US is insane by definition because we keep doing what we know has the opposite of the desired effect. Or rather, perhaps, we choose offense and tactics above defense and strategy every time. We keep winning tactically but losing strategically. If we keep it up... like choosing security over freedom… we lose both in the end.

Then there's history. For ~5,000 years, people have built cryptographic schemes and every one of them has failed in relatively short time frames (except the “perfect cipher” with is provably secure if implemented properly, but this also leaves the key distribution problem).

Summary:

At some point society will either decide to stop the idiocy and agree on a sensible future for protection, or pay an eternal price in … I didn't even edit the first part of this sentence from my last article. I conclude that we, the actual experts, and not the government so-called experts, need to teach high-level government deciders (1) about cyber-security issues (2) to check consistency of their own statements. Something about group think comes to mind.

Update

Surprise surprise. I sent this piece to the folks at the Panetta institute for comment the day after their conference, as I generally offer the opportunity to respond to anyone I name in any of my write-ups. I asked them to communicate it to the attendees as well. Within a few weeks we all found out via the news media that the FBI can now open these iPhones! In fact, they are now opening them for other law enforcement agencies.

After this came out in the media, I got a thank you note from the Institute telling me they got my letter. No other comment was included. A classic non-response acknowledging receipt in a very appreciative way.

So was the FBI lying? Were they trying to cover up a classified capability that is now leaked? Were they trying to set a precedent? Was the new capability created in that time frame? Did the NSA have the capability and failed to share it? Was someone so embarrassed by the obvious potential future press that they decided to reveal it? Did Apple secretly solve the problem and not tell anyone? Was it under a classified court order? Did they in fact not get into the phone and are now lying about it so bad guys will not lock their phones this way anymore? I have no idea. But here's what I do have an idea of.

The process undertaken by the FBI regarding Apple has done more damage than could reasonably have been done by merely stating the truth and not bringing it to court.

- If the ability was classified, everyone now knows of it.
- If it was developed by the government in a few weeks, why didn't they just do it?
- If the capability existed and was kept from the FBI, it just shows government cannot be trusted even by itself.
- If the ability to break it was a lie, they they are digging an even deeper hole for themselves in the future.
- By making a legal stand of it, the government likely precluded ever being able to use that same legal argument again. Why would any judge every believe them?
- If it was done by a commercial company for the FBI, are they that incompetent that they didn't try to buy it from the market before making a Federal case of it?

And was anything actually on the phone and not available otherwise? We haven't been told anything other than that access was gained. I suspect that if there was a smoking gun, we would know about it by now, at least to the extent that they found something of value. I think they are hoping it will all go away like a bad dream. But from now on, we can rest assured that every bad guy out there with the wits to encrypt things at all will know to also use another encryption scheme on top of their lockout settings.

Sometimes it's better to remain silent and be thought a fool than to speak and remove all doubt. Hopefully, the FBI will learn this lesson. But I doubt it.

