All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Equities: FBI v. Apple

The “equities” issue may be simplistically described as the tradeoff between attack and defense. This has come to the fore of late because the FBI wants Apple to put a backdoor in the iPhone.

The history of the equities issue

The best defense is a good offense. A football saying perhaps, but the reason the intelligence community outspends the computer security community in government by orders of magnitude today as it long has. The ability to spy on others is apparently considered more important than the ability to prevent them from spying on us.

It's not just about spying anymore

Today, computers form cybernetic systems by integrating with physical world sensors and actuators, and for modern societies, have become critical infrastructure. While the debate rages about privacy, there are other implications of backdoors in systems. Implications like the ability to take over the systems and use them to alter the cybernetic systems they interact with. Like the power grid, water systems, banking and financial systems, chemical plants, household computers, locking mechanisms, traffic lights, where your car auto-drives to when you tell it to take you home (future soon coming), and so on.

Today, when you introduce a backdoor, it's not just leaking information that was otherwise harder to leak. It enables all sorts of other attacks in integrity, availability, use control, accountability, custody, and transparency.

It's about cost effectiveness and capabilities

50 years ago, when I started using computers, governments had a monopoly on spying and its technology with criminal groups close behind. The battle between the criminals and the government persisted as it does today, but the battle between government was also critical. In World War 2, arguably, breaking the Enigma may have won the war, and not breaking it may have lost the war. These were international efforts with coalitions struggling over world dominance. Today, the enigma can be broken very quickly using the computing power of a commercially available digital watch.

50 years ago, Internet-based attacks did not exist, and unique capabilities used for spying were created by nation-states and kept secret for a long time. Today, the US intelligence community cannot keep its list of covert operations secret, and because we have put so much weight on the security of computers by making our society so dependent on them, that it's worth the effort to attack. And the technology of attack is now practically free. Once I develop a machine to guess passwords quickly, I can make it available to everyone everywhere for almost no cost, and within a matter of seconds.

If you put a backdoor in your system, even if it is “secret”, it will be found by a 3rd party or leaked, typically within a few months or less, and made globally available at their whim. Which means that your “secret” backdoor will be globally available to anyone with malice soon.

Copyright(c) Management Analytics, 2016 - All Rights Reserved

But Apple can protect the details as trade secrets

One of the latest claims I have heard is that Apple should be able to protect the trade secret of how the backdoor is exploited to make it safe. This indicates a woefully ignorant viewpoint for many reasons. Here are a few:

- From the CEO down, folks at Apple don't want the backdoor weakening the security of their systems, so someone will leak enough information for someone else to find it.
- The backdoor is valuable enough that it's worth the time and effort to find it. Someone will.
- If the security agencies of the US government cannot protect their highly classified operations from a rogue individual, why do they think Apple, a commercial company with far less resource and focus on keeping secrets, can do better. Are they merely admitting their own incompetence?
- No doubt, the US government could develop its own capability to do this without engaging Apple at all. Which is to say...

The US government is trying to weaken commercial products writ large

Yes – that's the real issue. It's the equities issue. Commercial products are getting too secure for the US government to inexpensively bypass the protections. The defense is starting to win, and the offense cannot tolerate that. Spying is more important to the government than the safety of critical infrastructures. This has always been true and likely always will. That's because they believe ...

The best defense is a good offense (a fallacy)

The fundamental fallacy emerges. Those in government, and particularly in the military and intelligence communities, strongly believe in a fallacy and that erroneous belief is causing them to make a strategic blunder. This belief cannot easily be shaken, and for that reason, and because it is apparently hard to explain it well, the US is going down a path that is problematic at best and catastrophic at worst.

They fail to understand the implications and consequences of their actions in the greater context of, and erroneously prioritizing secrecy issues over, integrity, availability, use control, accountability, custody, and transparency. This may be because they are not normally playing in that wider arena. The arena they play in is the spy vs. spy and force on force arena, and in that context, their view may be well justified. But in the larger context of modern society which is highly interconnected and in which information technology acts as part of the larger cybernetic system, this falls apart. A major reason it falls apart is that keeping effective protection is extraordinarily hard value of defeating protection has extreme consequences. Backdoors defeat everyone, because information flow is transitive, and knowledge spreads.

Summary:

To be clear, it is my opinion, based on my knowledge, training, experience, skills, and education, that in the arena of cybersecurity and the context of national security, “the best defense is a good offense” is a fallacy. The equities should be readjusted to favor the defense, particularly as it relates to things that affect critical infrastructures and personal liberties, which today includes most commercial products and offerings.

Copyright(c) Management Analytics, 2016 - All Rights Reserved