All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

May Day - attack mechanisms revisited - were you surprised by the NSA's activities?

The published literature on methods of attacking information technology is longstanding and extensive. The summary of 94 classes of attack methods published in the late 1990s[1] is only one of several variations on the theme from that time, and it cites publications starting in the 1970s. This also included a review of threats, identifying among others, government agencies and information warriors/ The CID database (available at all.net at the bottom of the left hand menu under “Database” - click “GO!” to use it) has been operating since the 1990s as well, and it provides associations of threats with the attack methods they use. Let's look and see the link between what they do and the methods they are known to have used 15 yours ago.

As of 1998...

Covering all 94 attack methods identified would take too long, so I selected a few to review:

- **audio/video viewing:** Recording at the end-point was apparently used, no surprise there, but of course governments readily do this in bulk at the infrastructure level.
- **breaking key management systems:** False certificates are increasingly apparent, and subversion of the random number generation process is a classic from way back.
- **data aggregation:** We call this “big data” today.
- **dependency analysis and exploitation:** The subversion of companies like Google are classics of getting into the dependency chain.
- **device access exploitation:** The claim is a program to systematically introduce false hardware into devices by intercepting shipments.
- **error-induced mis-operation:** As an example, forcing fallback to a cryptographic system you can break.
- **false updates:** This is the software version of device access exploitation.
- **implied trust exploitation:** The whole NSA / CIA / FBI / DOJ / Senate / who know who else scandal stems from implied trust.
- **Man-in-the-middle:** This has been widely published and discussed and apparently used to beat network-level encryption schemes.
- **repair-replace-remove information:** Software version of device access exploitation.
- **Trojan horses:** Apparently these are strewn throughout essentially all of the hardware, software, and network-based systems and methods in widespread use today.

And this is just the tip of the iceberg in terms of what can be done and perhaps has been.

---

1 Fred Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart, “A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model, and The Application of that Model for CyberWarfare in CID”, IFIP-TC11 Computers and Security, V17#3, 1998 pp. 211-221 (11). A version is available online at: http://all.net/journal/ntb/cause-and-effect.html

Power corrupts[2]

It should be no surprise that when the people cede the power to access and alter information on large scale to the agencies of government, those agencies gain and use the power to keep their power. The FBI apparently did it under Hoover, so it has happened here (the US) before, but it has also happened everywhere such power has been granted and ceded to an agency of government. The “black swan” claim may come up next, but this is just another excuse.

Trust in government is not justified and never has been. Power corrupts. That's the basis on which the US and most democracies were founded. And that is why we must not continue to cede power to government. And don't imagine that they can take it away if we are unwilling. It is the public's lack of diligence that drives these issues. When we the people look away, they the rich and powerful take more wealth and power.

Sunlight is the best disinfectant[3]

The sunshine laws in some states are intended to address these issues, but clearly, we could use a national sunshine law, and a global one. Somehow, the most fundamental requirement of sound governance is that the governed be aware of what the government does and is. This applies to corporations for shareholders and to a lesser extent to workers as well. But all the sunshine in the world won't help people who shut their eyes to the reality of their situation.

Open your eyes

In the mid-1980s while teaching one of the first courses I ever taught to graduate students, they were assigned to go out every week and collect stories on computer security incidents. And every week they came back with stories from newspapers, magazines, and so forth. This was before the Internet (then ARPAnet) had a way to search for news or anything like it, and when news and media was largely print, radio, and broadcast television. Finding stories was a manual effort reflecting only the magazines and papers of the day, in Lehigh, PA, which is and was a small town. Nevertheless, the students came back every week with at least a few stories each. They were amazed by the fact that, even though they hadn't noticed it before they started looking, there was actually a lot of computer-related attack information out there.

For almost 20 years, all.net has had a free online collection of computer-related attack methods open to the public. It is based on books and articles that have been around a lot longer. There are thousands of stories every week on these issues. There are books, classes, CDs, videos, etc. Ignorance is not bliss. In the information age, it approaches suicide.

Summary

If you were surprised by the recent revelations about purported attacks on computer systems by the NSA, you haven't been doing your homework. It's time to start doing it, because there's certainly more out there, both today and coming soon. And the US government isn't the only or necessarily even the most prolific threat using these attacks. If it can be done it will be tried, and there's a lot more that can be done. Our freedom depends on it. You are warned!

---

2 John Dalberg-Acton, 1st Baron Acton, "Power tends to corrupt, and absolute power corrupts absolutely. Great men are almost always bad men.", Letter to Bishop Mandell Creighton, April 5, 1887 published – see for details http://oll.libertyfund.org/search/results?q=power+corrupts

3 “Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." 1913 Harper's Weekly article, entitled "What Publicity Can Do." http://www.law.louisville.edu/library/collections/brandeis/node/196 – Louis D. Brandeis

