Installing Backdoors Assists CyberTerrorists

Carl Hewitt

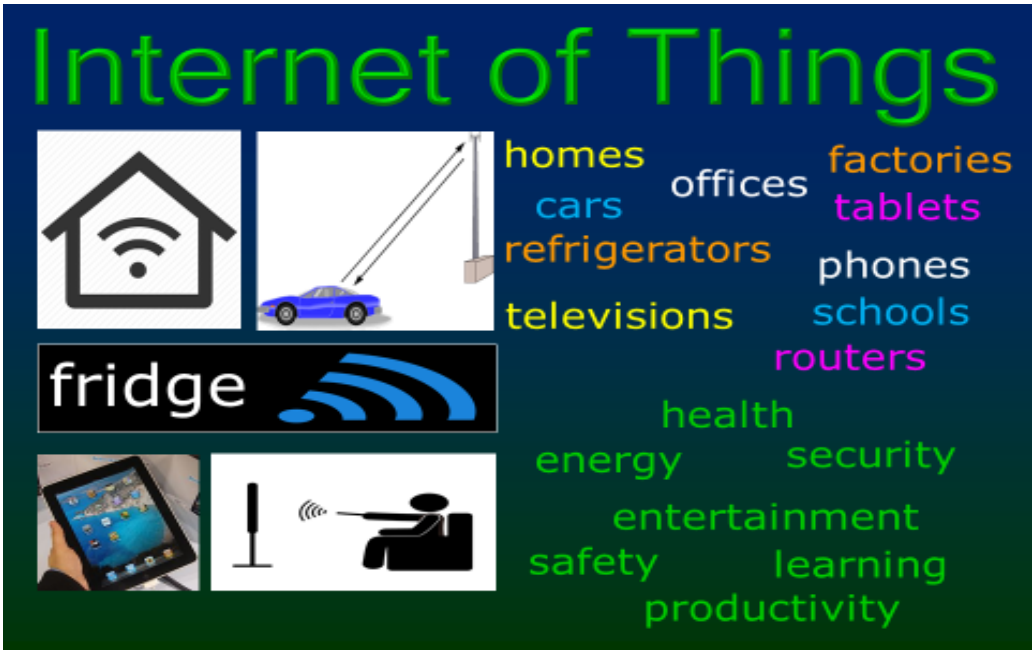
Installing Backdoors Assists CyberTerrorists

"Own your CyberThings" [i]

Carl Hewitt

To counter cybercriminals, security services have proposed mandatory backdoors on all Internet of Things (IoT) devices, but let's launch a government-sponsored crash IoT security campaign instead.

The Internet of Things (IoT) is becoming pervasive in all aspects of life including personal, corporate, government, and social.



A CyberThing is a physical or electronic artifact of Internet systems, e.g., light fixture, email, refrigerator, voice mail, cellphone, SMS, electronic door lock, *etc*. on the Internet.

[i] service mark of nonprofit foundation Standard IoT™

DataCenterism (*i.e.*, a system in which *all* electronic information is accessible in datacenters) is becoming the standard business model of the Internet. (Of course, encrypted information is not accessible unless the corresponding decryption key is accessible.)

In due course, it seems inevitable that governments in most countries will obtain (as each cyberattack increases pressure to react) bulk access to all information in datacenters with pipes to government surveillance datacenters in order to speed and coordinate government security efforts.

- ***DataCenterism*** is a system in which *all* electronic information is accessible[i] in datacenters.
- ***CyberTotalism*** is a system in which all electronic information is accessible in corporate and government datacenters with *total access* by the government.
- ***Sensitive information*** is nonpublic information whose revelation can potentially harm a citizen, *e.g.*, medical (including psychiatric), legal, financial, sexual, political, religious, *etc*.
- ***CyberLocalism*** is a system in which a citizen's Internet of Things information is stored locally in their own equipment–*the antithesis of both Datacenterism and CyberTotalism.*

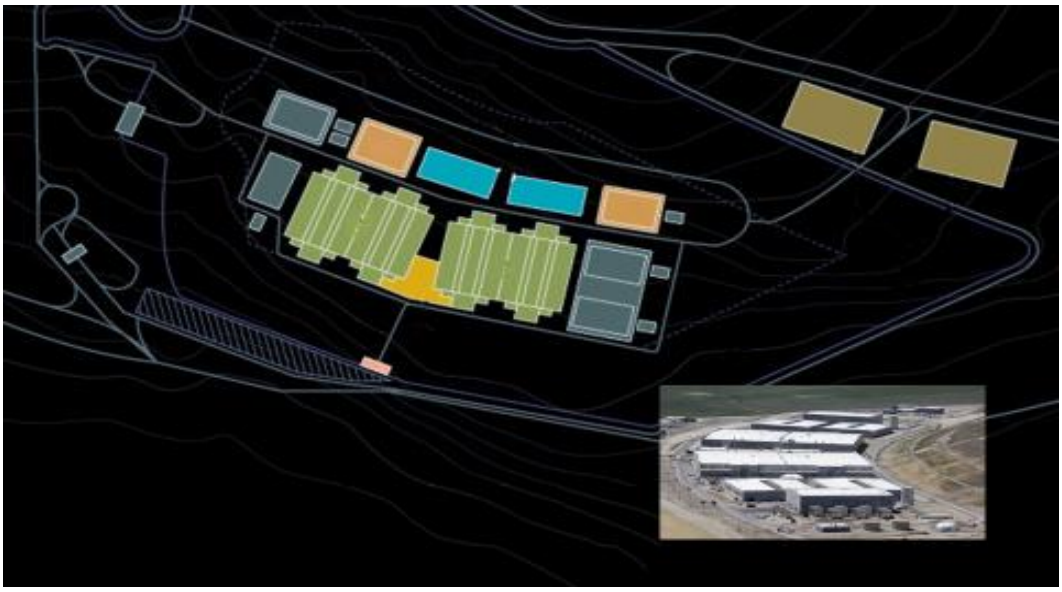
Consequently, DataCenterism inevitably leads to *CyberTotalism*, a system in which all electronic information is accessible in corporate and government datacenters with *total access* by the government to its citizens' information.

To facilitate faster and more comprehensive security operations, governments will want to use corporate information mining tools in corporate datacenters for security purposes (perhaps with some direct costs reimbursed by the government) thereby making their engineers and executives *increasingly complicit in mass surveillance*. Furthermore, businesses will be harmed by the following developments:

- their inability to change datacenter operations because it would disrupt government surveillance[1]
- the enforcement of uniformity of datacenter operations across companies (to the competitive disadvantage of the companies) because of government requirements for standardized surveillance operations.

Corporations need to come to better understand that sensitive citizen information is not always a corporate asset and instead can be a toxic corporate liability.

Corporate datacenters are best used for statistical operations that do not have sensitive personal information. Those with large amounts of sensitive citizen information (e.g. financial and medical) will be highly regulated..



.

Massive NSA Datacenter in Bluffdale Utah

Fortunately, there is an alternative to CyberTotalism as follows:

CyberLocalism is a system in which citizens' IoT information is stored locally in their own equipment– *the antithesis of both Datacenterism and CyberTotalism*. Of course, all of the convenience that is currently available must also be available using CyberLocalism:

- Local operations on citizens' equipment IoT will incorporate access to the Internet to provide scalable search, retrieval, and collaboration using commercial datacenters in cooperation with other citizens' equipment.
- Local information can be backed up elsewhere automatically encrypted using the citizen's public keys, e.g., in commercial datacenters and distributed on other citizens' equipment.
- A citizen can share selected information automatically encrypted with the public keys of other parties (so that it be read only by the intended recipient).

Sensitive information is nonpublic information whose revelation can potentially harm a citizen, *e.g*., medical (including psychiatric), legal, financial, sexual, political, religious, *etc*. For example:

- The FBI tapped into conversations between Robert Oppenheimer and his lawyer during the hearing designed to humiliate him by having his security clearance removed in order to punish him for some his political views. Also, the FBI COINTELPRO program persecuted thousands, *e.g*., gay people, almost all groups protesting the Vietnam War, and organizations and individuals associated with the women's rights movement.[2] For example, the FBI recorded conversations between Martin Luther King and his mistresses and then used the information to blackmail him suggesting that he commit suicide in order to avoid exposure.

- Suborning about 20% of the population, the Stasi secretly ruined the lives of tens of thousands.[3]

A citizen's information system (embedded in home modems, routers, car, gateways, large screen displays, audio-visual systems, computers, refrigerators, stoves, climate control systems, washer/dryers, *etc*.) can hold the most sensitive of a citizen's information where it can be integrated with other sensitive information as well as information from the following:

- other information from the citizen's IoT
- other citizens
- datacenters.

CyberLocalism has the following advantages over Datacenterism:

- *Lower communications cost* because it is not necessary to always communicate with datacenters
- *Faster response* because local communication can be faster than always interacting with datacenters, which might be slow to respond
- *Better coordination of IoT* because it can be difficult to get datacenters of competing companies to coordinate concerning the interoperation of a citizen's IoT devices
- *Greater reliability* because communication with datacenters might be interrupted
- Better protection of a citizen's sensitive information because it is not always available in datacenters.

The widespread adoption of CyberLocalism will depend on the development of new Internet business models. Please see the appendix of this paper for discussion.

The current default security strategy has not worked, namely, "beating up on personnel to improve security until the public outcry subsides."

CyberLocalism requires greater security of citizens' Internet of Things devices because state-sponsored intruders can hack into almost every citizen's personal cellphone, computer, tablet, etc. on the Internet.

To achieve adequate security, CyberLocalism needs the following:

- ***Strong personal authentication***, *e.g.*, using (3D) interactive biometrics instead of passwords
- ***Strong, ubiquitous public key authentication*** so that it can be verified to whom a public key corresponds. Often this authentication can be performed by local bank offices, *etc.* that publish online multi-national directories of public keys in a network of mistrust. Individual citizens can have their own directories of public keys that are used to automatically and invisibly securely communicate with others.
- ***Public keys for IoT ownership*** so that an IoT device has both:
    - a public key of its owner, which is installed when ownership is transferred
    - its own unique public/private key pair, which are installed when the device is manufactured.

  An owner can communicate securely with a device by encrypting information using the device's public key. (For efficiency reasons, most communication will actually be performed using symmetric keys derived from public keys.) A device takes instructions only from its owner and is allowed to communicate with the external world only through the information coordination system of its owner.[4] The nonprofit Standard IoT Foundation is working to develop standards based on the Actor Model of computation that provide for interoperation among existing and emerging consortium and proprietary corporate IoT standards.
- ***Hardware architecture security*** to help cope with the complexity software systems that can never be made highly secure without hardware assistance including the following:
    - *RAM-processor package encryption* (*i.e.* all traffic between a processor package and RAM is encrypted using a uniquely generated key when a package is powered up and which is invisible to all software) to protect an app (*i.e.* a user application, which is technically a process) from the following:
        - operating systems and hypervisors
        - other apps
        - other equipment, e.g., baseband processors, disk controllers, and USB controllers.
    - *Every-word-tagged architecture* to protect an Actor[5] in an app from other Actors by using a tag on each word of memory that controls how the memory can be used. Each Actor is protected from reading and/or writing by other Actors in its process. Actors can interact only by sending a message to the unforgeable address of another Actor.

Existing software (e.g., operating systems, browsers, mail systems) will need to be upgraded to use tags.

Because of impending security improvements, it will become extremely difficult even for state-sponsored intruders to easily hack into IoT endpoints.

The looming prospect of not being able to easily hack into IoT devices undetected (with court orders) has alarmed some security services prompting them to demand mandatory backdoors[6] be installed in all IoT equipment within their jurisdiction.

IoT Backdoors

On March 2, 2015, President Obama complained about a government attempt to require backdoors in companies' products saying:

> *"As you might imagine tech companies are not going to be willing to do that... I don't think there is any U.S. or European firm, any international firm, that could credibly get away with that wholesale turning over of data, personal data, over to a government."*[8]

If the US and EU adopt auditing against backdoors, then auditing will rapidly spread to the rest of the world, which is very much in their long-term security interests.

However, FBI Director James Comey [speech on October 17, 2014] and NSA Director Mike Rogers[10] have proposed[11] that CALEA[12] be expanded so that every cell phone, personal computer and any other network-enabled products and services that operate in the US must have a backdoor in order that the US government can hack in undetected with the approval of US courts.[13]

Rogers clamed: "Building it [secure backdoor command and control system] is technically feasible."[14] However, he admitted that if the FBI/NSA mandatory backdoor proposal is adopted, then it will be necessary to "work through" arrangements with other governments to have their own backdoors and any consequential restrictions on Internet interconnectivity and international trade of products involved in the IoT.

Highly secure backdoors can use the equivalent of a different public key on each device. Control of private keys for backdoors can use means similar to the ones currently used in nuclear command, control, and communication systems, which have had many problems.[15] However, at an expense comparable to nuclear command and control systems, it would be possible to create a system for protecting the keys of a backdoor system that is highly secure against outside attackers and even against a small number of inside conspirators. Such a system can use multiple command centers with divided keys. Even with such a system, it is possible that, later on, some backdoors of older IoT devices could be compromised by criminals and state-sponsored attackers.

Adopting the NSA/FBI mandatory backdoor proposal can have the following effects:[16]

- Influence countries to require that IoT products legal to be used in a country will have to be audited against backdoors available to *other* countries. It is technically much easier to audit against *all* backdoors that to audit against other countries being able to exploit an *already installed* backdoor.
- Increase the danger of preemptive cyberwar[17] because of potential vulnerabilities in the many government backdoor implementations.[18]
- Decrease the competitiveness of US manufacturers in the market of the IoT, which will include almost *everything.* [19]
- Enormously increase the power of government security monitors.[20] State terrorists achieve political objectives by creating a general climate of fear. For example, J. Edgar Hoover (FBI), Joe McCarthy (US Senate Permanent Subcommittee on Investigations), Erich Mielke (Stasi), *etc*. terrorized citizens of their countries. *Cyberterrorists* can exploit the immense powers of the IoT to create mass terror on a scale that was heretofore unimaginable.[21]

Mandatory backdoors will mean that security services of each country will surveil citizens in their own country and perhaps swap surveillance information with other countries.

In fact, the NSA/FBI mandatory backdoor proposal has *already* increased mistrust by foreign governments and citizens alike, with the following likely consequence:[22]

Companies will be required to hire their own independent cyberauditors and/or submit to cyberaudits by foreign governments.[23]

Conclusion

The only thing necessary for the triumph of evil is for good men to do nothing. Edmund Burke

Future exports of U.S. companies will need to be certified by corporate officers and independently audited not to have backdoors available to the U.S. government.

An IoT Security Commission (ISC) needs to be established with the charter of:

1. *Jurisdiction*: ISC will have jurisdiction over all providers of IoT equipment in the US. Every IoT device will be required to be audited by mechanisms determined by ISC, *e.g.*, inconsistency-robust operational bi-simulation against a publicly available operational specification overview.
2. *Quarterly Corporate Security Report*: ISC will enforce that at end of each quarter, a corporate security report must be signed by the corporate officers of a covered company, which must specify either
    i. no evidence for the existence of a backdoor was found in any of the company's IoT products or that
    ii. evidence that was found for the existence of backdoors and the measures that were taken to remove backdoors from any products that were shipped and to prevent re-occurrence.
3. ***Oversight*:** ISC will provide independent oversight of public security accounting firms providing cyberaudit services ("*cyberauditors*") that will:
    - register cyberauditors
    - define specific processes and procedures for compliance cyberaudits
    - inspect and police cyberaudit conduct and quality control

- restrict cyberauditing companies from providing non-audit services (*e.g.*, consulting) for the same clients.
- enforce compliance with specific legal mandates, *e.g.*, the use of RAM-processor encryption and every-word-tagged architectures.

Using mechanisms outlined in this article, the US should immediately launch a crash program to secure IoT including corporate, citizen, utility, and government endpoints.

Acknowledgements

This article has greatly benefited from detailed critiques and organizational suggestions of Alan Karp, editorial suggestions of Dennis Allison, comments by Chip Morningstar, and a suggestion of Ron Rivest. John Dalton provided design and editorial consulting.

The following video covers material in this article:
Actors for CyberThings. https://youtu.be/DNbJY333vUs

Appendix

CyberLocalism will never come to fruition unless it is supported by a business model that is more efficient and effective than the currently popular system of datacenterism. Fortunately, recent advances in the development of inconsistency-robust information systems[24] technology can be used to facilitate new business implementations that are more *effective*, *pervasive*, and *profitable* by improving interactions among consumers and merchants because:[25]

- Consumers will no longer be continually hassled by *intrusive unwanted* advertisements. Instead, mediation systems running on a consumer's equipment can provide the ability to seek and help evaluate appropriate offers for their purchases. (Mediators can earn commissions and fees from merchants.)
- Merchants will no longer be burdened by having to pay for *grossly inefficient* advertising that annoys potential customers. Instead, businesses can provide their information to advertising brokers that will aggregate and package it for citizens' equipment to be used by their systems in evaluating offers. (Brokers can earn commissions and fees from merchants.)

References

[1] Lee Fang. *How Big Business Is Helping Expand NSA Surveillance, Snowden Be Damned.* The Intercept. April 1, 2015.

[2] US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Final Report on Intelligence Activities and the Rights of Americans.* 1976. The report documented that Constitutionally illegal surveillance spanned all presidents from FDR to Nixon, including the following [summarized in Wikipedia]:

- President Roosevelt asked the FBI to put in its files the names of citizens sending telegrams to the White House opposing his "national defense" policy and supporting Col. Charles Lindbergh.
- President Truman received inside information on a former Roosevelt aide's efforts to influence his appointments, labor union negotiating plans, and the publishing plans of journalists.
- President Eisenhower received reports on purely political and social contacts with foreign officials by Bernard Baruch, Eleanor Roosevelt, and Supreme Court Justice William O. Douglas.
- The Kennedy administration had the FBI wiretap a congressional staff member, three executive officials, a lobbyist, and a Washington law firm. US Attorney General Robert F. Kennedy received the fruits of an FBI wiretap on Martin Luther King, Jr. and an electronic listening device targeting a congressman, both of which yielded information of a political nature.
- President Johnson asked the FBI to conduct "name checks" of his critics and members of the staff of his 1964 opponent, Senator Barry Goldwater. He also requested purely political intelligence on his critics in the Senate, and received extensive intelligence reports on political activity at the 1964 Democratic Convention from FBI electronic surveillance.
- President Nixon authorized a program of wiretaps which produced for the White House purely political or personal information unrelated to national security, including information about a Supreme Court Justice.

[3] Florian Henckel von Donnersmarck. *The Lives of Others.* Wiedemann & Berg, *et. al*. 2006.

[4] Mike Burnside, D. Clarke, T. Mills, A. Maywah, S. Davadas, and R. Rivest. *Proxy-Based Security Protocols in Networked Mobile Devices.* SAC'2002.

[5] Carl Hewitt. *Actor Model of Computation*. in "Inconsistency Robustness" College Publications. London, U.K., 2015.

[6] A ***backdoor*** is means by which a cyber device can provide information and control about the users of a device

- to parties that were not specifically enumerated
- concerning kinds of information and control that were not specifically described
- that was not specifically authorized by users of the device.

[8] Jeff Mason. *Obama sharply criticizes China's plans for new technology rules.* Reuters. March 2, 2015.

[10] Mike Rogers. *A Conversation with Admiral Mike Rogers* Cybersecurity for a New America: New America Foundation. February 23, 2015.

[11] Concerning pitfalls with such proposals see [Steven Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter Neumann, and Jennifer Rexford. *Risking Communications Security: Potential Hazards of the Protect America Act*. IEEE Security & Privacy. Vol. 6. No. 1. Jan.-Feb. 2008] and [Jonathan Zittrain. *An Open Letter to Prime Minister Cameron*. Medium. February 11, 2015.]

[12] According to [*EFF Response to FBI Director Comey's Speech on Encryption.* October 17, 2014]:

Here's the relevant part of CALEA that Comey wants to effectively undo:

"USC 1002(b)(3): A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."

Also from the CALEA legislative history:

"Finally, telecommunications carriers have no responsibility to decrypt encrypted communications that are the subject of court-ordered wiretaps, unless the carrier provided the encryption and can decrypt it. ... Nothing in this paragraph would prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access ... Nothing in the bill is intended to limit or otherwise prevent the use of any type of encryption within the United States. Nor does the Committee intend this bill to be in any way a precursor to any kind of ban or limitation on encryption technology. To the contrary, section 2602 protects the right to use encryption."

[13] Jeremy Scahill and Josh Begley. *The CIA Campaign to Steal Apple's Secrets*. The Intercept. March 10, 2015.

[14] Mike Rogers. *National Security Agency Director Mike Rogers on Cybersecurity.* CSPAN. February 23, 2015.

[15] Eric Schlosser *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety* Penguin Books. 2014.

[16] Carl Hewitt. *What to do about our broken cyberspace.* CACM. February 2015.

[17] Bill Marczak, et. al.. *China's Great Cannon.* University of Toronto. April 10, 2015.

[18] Shane Harris *@War: The Rise of the Military-Internet Complex.* Eamon Dolan/Houghton Mifflin Harcourt. Boston, MA, 2014.

[19] James Staten. *The Cost of PRISM Will Be Larger Than ITIF Projects* James Staten's Blog at Forrester Research. August 14, 2013.

[20] Anna Funder. *Stasiland: Stories from Behind the Berlin Wall.* Harper. 2011

[21] Michael Glennnon. *National Security and Double Govenment* Harvard National Security Journal. Vol. 5. 2014.

[22] Peter Swire and Kenesa Ahmad. *Encryption and Globalization* Columbia Science and Technology Law Review, Vol. 23, 2012.

[23] Li Dandan. *Apple expresses willingness to accept the Chinese domestic network security review.* Beijing News. January 21, 2015.

[24] Carl Hewitt and John Woods assisted by Jane Spurr, Editors. *Inconsistency Robustness.* College Publications. London, U.K., 2015.

[25] Carl Hewitt. *Actors for CyberThings*. YouTube. https://youtu.be/DNbJY333vUs