G20 INSIGHTS

G20 GERMANY 2017
THINK 20 DIALOGUE

POLICY AREA:
Digital Economy

Addressing Market Failures to improve the health of the Digital Infrastructure

Paul Twomey (Centre for International Governance Innovation (CIGI))

March 22, 2017

Abstract

Market failures are resulting in network operators and device manufacturers not being incentivized to ensure improved cyber security practices in their operations. The result is a large global base of vulnerable computers, modems/routers and Internet of Things devices which can be manipulated by Cyber criminals. Practical recommendations are made as to how governments could address these market failures (with low-cost to government) and significantly improve the health of the cyber ecosystem.

Challenge

Connected technology holds both great promise and great peril for the G-20 countries and global stability. Increasing integration of technological and social systems unlocks new capabilities for prosperity, growth, health, safety, and resilience. The Internet of Things is bringing life-changing capabilities to more people, faster, and cheaper, than would be possible otherwise. Connected automotive safety features, medical therapies, logistics revolutions, utility services, and other advances improve public safety and human lives.

But these advances are also threatened by weaknesses in the digital infrastructure, many driven by present network economics ensuring that externalities of harmful behavior are not being captured in the business models of network operators and device manufacturers, but instead are being multiplied to users as whole. G-20 governments could adopt some relatively light-handed approaches to shift these economic incentives.

While the market and the multistakeholder coordination of the technical community has addressed many challenges in the growth of the Internet, governments could address some areas of market failure in particular as they relate to:

- Network operator practices which deliver increased vulnerability, for instance to Distributed Denial of Service Attacks
- The failure to build security into the connected devices of the burgeoning Internet of Things

Proposal

1. Network operator practices

DDoS attacks exhaust the available resources of computers by overwhelming them with data. This occurs because of two primary causes on the Internet, reflectors which amplify and reflect small amounts of data into large ones directed to others and spoofing of addresses. The DDOS vulnerability shows the implications of ISPs and network operators not taking care to ensure their modems, routers etc are deployed or maintained properly. The failure to maintain best practice management of 4 risk indicators alone (Open DNS, NTP, SNMP, SSDP) means that the an ISP can pollute the network as a whole – these risks are exploited by botnet and DDOS exploiters. But the pollution impact is greater to the users as a whole than to the operators who each do not have an economic incentive to clean up their own networks. Data from the non-profit CyberGreen Institute, shows that the potential attack capacity of the existing polluted network devices is five times larger than the biggest DDOS attacks to date. The failure to address this negative externality places the G-20 government agencies, enterprises, financial institutions and consumers at even greater risk than they face today.

Recommendation

G-20 communications regulators and/or CERTS:

- Utilize publicly available data on network risk indicators, such as provided by the non-profit CyberGreen Institute, to engage ISPs to encourage better device deployment processes and operational decisions.
- Encourage the adoption of the Internet Society's Mutually Agreed Norms for Routing Security, or MANRS (https://www.manrs.org) by network operators.

2. Internet of Things

Dependence on connected technology is increasing faster than our ability to build defensive capabilities and resilience against accidents and adversaries. Defects in a single common IT component may simultaneously impact cars, medical devices, power grid, smart homes, and aircraft. As we increase our society's dependence on the "Internet of Things, we must correspondingly increase the dependability of these connected technologies. Though IoT we are connecting life saving/preserving activities (hospitals, food supply, transport etc) to the network. If it fails or is manipulated, the results will not just be interruptions to Internet service – they may be death and injury.

As in the related area of DDOS remediation, we are facing the problems posed by a negative externality. As Bruce Schenier testified recently:

> The technical reasons that Internet-of-Things computers are insecure is complicated, but there is a fundamental market failure at work. Basically, the market has prioritized features and cost over security. Many of these devices are low cost, designed and built offshore, then re-branded and resold. The teams building these devices don't have the security expertise we've come to expect from the major computer and smartphone manufacturers, simply because the market won't stand for the additional costs that would require. Unlike your

> computer and smartphone, these devices don't get security updates, and many don't even have a way to be patched. And, unlike our computers and phones, they stay around. DVRs and cars last a decade. Refrigerators, twenty-five years. We expect to replace our home thermostats approximately never…
>
> They'll remain in use because of an additional market failure: neither the seller nor the buyer of those devices cares about fixing the vulnerability. The owners of those devices don't care. They wanted a webcam —or thermostat, or refrigerator —with nice features at a good price. Even after they were recruited into this botnet, they still work fine —you can't even tell they were used in the attack. The sellers of those devices don't care: They've already moved on to selling newer and better models. There is no market solution because the insecurity primarily affects other people. It's a form of invisible pollution.

If there is to be some regulatory response to this market failure, it must not repeat the mistakes of earlier regulation attempts. Government telling producers how to make their products and services has been singularly flawed in the technology space and has resulted in the growth of compliance "industries" without attendant increase in security. . Ex Ante minimum requirements (often stifling or brittle) should be avoided in favor of Ex Post accountability (more flexible in implementation). This is still an evolving technology. Any rules that are about technology, rather than principles, risk retarding innovation or having other bad effects. Accountability can be improved both by required transparency in the supply chain and by accountability for the outcome.

Recommendation

G-20 governments should:

- Promote transparency in the supply chain and labeling to reveal distinctions among market alternatives and permits evaluation of costs and risks. G-20 governments should coordinate on an internationally consistent IoT/Software Bill of Materials includes ingredients from any 3rd party and/or open source software parts (with versions) used in products (ideally machine readable). The list should not contain Known Vulnerabilities without a justification.

- Require that IoT devices be patchable. Because future vulnerabilities are inevitable, products must be patchable in a reasonable time frame

- Legally require vendors and/or ISPs to offer life-long security updates

- Conduct public awareness and cyber literacy programs to better informs buyers to increase benefits from the transparency and labeling initiatives

- Coordinate on evaluating where accountability should fit into the software/IoT value chain, and introduce such accountability in a careful and, measured way, after multi-stakeholder input.

References

1. http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-SchneierB-20161116.pdf