The ISP Column
A monthly column on things Internet

October 2014

Geoff Huston

Privacy and Security - Five Objectives

It has been a very busy period in the domain of computer security. What with "shellshock", "heartbleed" and NTP monlink adding to the background of open DNS resolvers, port 445 viral nasties, SYN attacks and other forms of vulnerability exploits, it's getting very hard to see the forest for the trees. We are spending large amounts of resources in reacting to various vulnerabilities and attempting to mitigate individual network attacks, but are we making overall progress? What activities would constitute "progress" anyway?

What these attacks illustrate is that our online environment is built on various assumptions of trust, and that often our trust in the operation of the network and the integrity of its applications and services can be subverted and misdirected.

It's wishful thinking to believe that any of the next software release, the next technology standard, or the next code of practice, will address all of these issues and deliver us a robust and incorruptible environment that could shrug off various determined efforts to subvert it's integrity. That's just not going to happen. But at the same time we should not just give up. There are some broader objectives that we should not lose sight of that would reduce our overall exposure to malware and various form of hostile attack, and at the same time take some practical steps towards assuring ourselves that we all can confidently use a public network for private communication.

Here is my list of such objectives, and the reasons why I think that they are important for the Internet.

1. Open availability of robust, strong cryptography

> Yes, this is the case in much of the world, and yes there is widespread use of what are generally considered to be strong cryptographic algorithms. So why is this listed here? Because what exists and is accepted today may not be the case tomorrow. The pervasive use of good cryptography through open software libraries is a feature of today's network that promotes confidence in using this communications system for trusted service provision that relies on integrity and privacy. If we do not preserve this essential attribute of privacy and security, namely the widespread low cost readily available of high quality cryptographic systems, then we lose the trust of the network's users.

2. A Secure Name Infrastructure

> The symbolic labeling systems for the Internet is the domain name system. Every network transaction starts with a symbolic reference to the other party or parties to a transaction, be it an email address, a web address, or any other named network service. The network transaction commences by translating this symbolic name to a network IP address. If this mapping is corrupted then applications will be mislead and the integrity of network transactions is at risk. Applications need to have a mechanism that ken be used to validate that the mapping responses they receive from name queries contain authentic data. We have a defined security framework that can provide this assurance (DNSSEC), but attention is required to promulgate its use.

With a vulnerable and compromised name mapping system we cannot operate a trustable network.

3. A Secure Forwarding Infrastructure

At the heart of the architecture of the Internet is a destination-based hop-by-hop datagram transmission system. When an application passes a packet into the network, it is trusting that every router within the network has been loaded with information that allows it to make a consistent decision to switch the packet one hop closer to its addressed destination. The way in which this information is loaded into routers is via a routing protocol, and the way in which this function can be disrupted is by compromising the integrity of the routing protocol. There are long standing efforts to add cryptographic functions into routing protocols, with the intent of allowing a routing agent to validate the information that is provided by the protocol, and allow others to validate the routing information originated by this speaker. Research on this topic has been erratic, due largely to the ever-changing priorities of public and private research funding. We've made some progress, and constructed some prototypes, but its by no means the end of the story here, and it looks like there is more to understand. Meanwhile, the Internet still lacks a viable and robust technical platform that can provide this security function to routing and operate efficiently at a scale of ubiquitous adoption. We are vulnerable to various forms of disruption via corruption of the routing system, and need to elevate the importance of this area of operational research if we ever want to achieve a secure routing framework.

4. Encryption by Default

There is an increasing awareness on the part of Internet users that the Internet is not a black box. Transactions across the Internet are visible to third parties whose identity, role and intentions are unclear to the network's users. Assurances, various codes of practice, and even regulation are an inadequate response, particularly when state-based actors have been identified as having active programs of data collection from Internet networks. Users are looking for a far stronger assurance that the content of the transactions that are passed across the network are decipherable only by the intended recipient of the transaction. The most direct way of achieving this is to leverage the open availability of robust strong cryptography and encrypt all network transactions. This has altered the trust models for users. Reasonably, users can no longer trust that their transactions will not be inspected while being carried within the network, as that trust has now been irretrievably breached. There is an increasing use of end-to-end encryption of traffic to hide the content of transactions from the network, and this is entirely justified, and should be supported and encouraged. With encrypted traffic the users are no longer incidentally exposing their communications to the network and thereby risking exposure of their communications to unknown third parties.

5. A Useful Privacy and Security Public Policy Framework

The telecommunications sector has been a network-centric sector for the past century or more. The entire function of the public telecommunications network was contained within the network itself, and the interfaces to the network were constructed as simple human interface tools that exercised no control over the operation of the network. The Internet inverted that model. The entire functionality of the network in terms of service definition and support is now pushed to the devices on the periphery of the network, and the interior of the network is now a simple stateless datagram forwarding service with no transactional control elements. However, the regulatory focus for telecommunications has not embraced this change, and the focus for privacy and security policies and regulation persists in concentrating on the network and the network operators. An effective privacy and security framework needs to embrace the edge, and encompass the principles of a consumer's reasonable expectations of privacy and personal safety and security are obligations for the vendors of devices and applications used by consumers, and are obligations for the providers of online services. The Internet users, and the economic value of their use of the Internet is reliant on, trust in the integrity of the way in which their devices, applications and services handle their personal data. They may no longer have any justified reason to trust the ability of the network to protect their privacy, but they are forced to trust that their devices, applications, software libraries and the cryptography that they use operate with integrity. The policy and regulatory framework should match these expectations of trust with codified and enforceable obligations on the vendors of consumer product and services on the Internet to commit to a comparable level of attention to the integrity of the products that they produce.

Obviously everyone's list would be different, and I claim no special insight over and above those of all the other folk who contribute to privacy and security discussions. However, in thinking about this short list I've tried to pull away from the myriad of details, incidents and vulnerabilities in today's Internet and look at some larger common themes. I've tried to phrase these objectives in a way that invites the participation of public policy in a role that advocates industry-wide behaviors that hold the consumer's legitimate interests in privacy and security of their use of the Internet as a foremost consideration.

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.