11 – The Public Roadways Component

Question 11 *Can the outdoor public transport system also benefit from QEI?*
Answer 11 The Public Roadways Component
The roadway system, the Internet, is far ahead of the real estate, the secure online places where people can safely gather. Its protocols, like those for the next generation of concrete interstate highways, are well established. But the facilities that control the In-ternet are entirely too vulnerable to criminals and vandals. Access controls based upon measurably reliable identities, as well as professional licensing, must be put in place for DNS and other essential roadway components.

Public Facilities Need Design Too
The Quiet Enjoyment Infrastructure enables bounded online spaces that are reached via the Internet but that are set apart from the Internet. Eleven of its 12 components describe and define an environment where people and information remain secure, inside bounded spaces connected securely by means of the very public information highway.

All sorts of exciting Internet developments are coming down the pike. There is IPv6, dramatically increasing the address space and fixing other problems. There is Caltech's remarkable Fast TCP, promising huge increases in effective bandwidth available over existing lines.

But the Internet is no longer the playground of a collegial worldwide old-boy network of developers from the world of academia. The root server system is expanding to encompass as many as 40 mirror sites in cities around the world. This adds both security and vulnerability, as the number of people with console, physical, and logical access to the additional servers will have to grow. The servers providing the 13 logical roots were subject to a major distributed denial of service attack in 2002. Wouldn't the perpetrators of that attack like to get past the parapets and into the inside of the castle? Surely they will try just that, if the proper identity mechanisms are not in place.

As the highway metaphor is useful in understanding the Internet, it helps us under-stand why policing the highway – inspecting vehicles for illegal substances and the like – is not the job of the highway department.

When it comes to regulating the construction and maintenance of the Internet highway system, rather than regulating the behavior of those who use it, the metaphor breaks down. In managing the physical highway system, unlike the Internet highway, there is no need to worry that rogue construction crews will build unauthorized on-ramps and intersections while no one is looking, or that bogus traffic cops will delib-

erately create congestion by putting extra millions of vehicles on the road, all headed for one building. Asphalt and cars have mass, they cannot be easily copied, or created and changed with keystrokes. By contrast the Internet highway system and the packet vehicles that traverse it are made of bits. Bits have no mass and can be created, altered, and destroyed instantly, with virtually no energy.

Recall what Mike McConnell, the former Director of the National Security Agency, had to say about Internet-borne vulnerability:

> If 30 terrorists with hacker skills and $10 million were to attack us today, they could bring this country to its knees. It would take one focused cyberattack to exploit our communications and our critical infrastructures such as the money supply, electricity, and transportation. The United States is the most vulnerable nation on earth when it comes to cyberterrorism. Our economy relies on IT networks and systems. Information is what we do.

That was from June 2002. In the intervening time the Internet dependence of the rest of the world has grown remarkably. If there were a way to measure the degree to which all of the world's infrastructures "such as the money supply, electricity, and transportation" systems of the entire globe – not just the U.S. – have become dependent upon the information highway, surely the curve would have an exponential look to it.

The Internet consists of lines, routers, servers called servers, and servers called personal computers, that is, broadband-connected home computers that have been turned into zombie servers for propagation of spam and worms. The process by which packets are put on the Internet must be regulated. If a piece of software sends those packets on their way, then the software must be signed by a licensed individual who takes responsibility for its actions.

The power to control how URLs are translated into IP addresses is regulated, but the identities of those who touch the controls are inadequately established. This situation must be fixed.

The identities of those who register and transfer URIs (URLs) are also inadequately established, generating excessive support costs and litigation for registrars and endless headaches for their customers. Identities based on Digital Birth Certificates would solve this problem in a snap.

All who actually control the routing of packets on the world's online highway system should be certified and licensed according to exacting standards.

In fact a highway department does exist, duly constituted, whose staff is for the most part trained and certified. To an extent it is held responsible for the smooth operation of the highway system. But the process by which its staff is selected and its policies made is dangerously unregulated. Perhaps the biggest example of the problem is in the oper-

ation of the Domain Name System (DNS). DNS is responsible for translating the names of resources into IP addresses, so for example if you type www.village.com a server near you in the DNS system can look up that name and send the packets in your request to the IP address known as 209.132.69.110.

The software that sits on DNS servers around the world and makes all this work, called BIND, provides a reference implementation of the major components of the Domain Name System. More than 80% of DNS servers in operation today run BIND, including the 16 root DNS servers that serve as the ultimate source of IP addresses when name servers attempt to map a URL to an IP address. BIND binds a domain name to an IP address.

If you can get into BIND and alter that mapping, you can wreak havoc around the world by making Web addresses point to the wrong IP address. For example, you could redirect traffic intended for amazon.com to your own marysbooks.com. Of the tens of thousands of copies of BIND on servers around the world working to resolve Web addresses and send their traffic to the right server, a large number are obsolete versions of the software that carry severe vulnerabilities.

If there were ever a case for regulation of the use of software, the BIND problem articulates the case with an eloquence beyond words. In the physical world, everyone who uses the highway is vulnerable to the motor vehicle department with the worst, loosest standards for registering vehicles. But unlike the physical highway system where, say a vehicle registered in Lesotho is unlikely to be found operating in Quebec, it is not unlikely for a packet-vehicle from Lesotho to be wandering around the servers and lines in Quebec.

Who Regulates the Highway?

The ITU ought to regulate BIND installations, periodically reviewing them to ensure that they are up to date, with all known vulnerabilities fixed. Furthermore, all BIND installations should be licensed only after ensuring that the identity of the individual who takes personal responsibility for the operation of the software is associated with each installation of BIND.

However, the ITU is not involved with ICANN (International Corporation for Assigned Names and Numbers), the closest thing we have to a highway department. ICANN has something to do with the U.S. Department of Commerce and with an assortment of past Internet organizations. Its authority to carry out its important work is not well established.

ICANN ought to be made a unit of the ITU and be given clear authority over the governance of the world's roadways. That is the essence of our Public Roadways Component.

Most importantly, anyone who touches BIND or any of the other key parts of the highway infrastructure should be required to use an identity credential that is as strongly reliable as possible.

The identity and credentials of everyone who goes near those mirror servers must be strongly established according to a set of procedures that should be as exacting as those that governed access to the Minuteman missile silos of the SAC doomsday machine.

Even more sensitive are the "hidden primaries," the servers whose addresses are not published. The operation of those primaries is passing, according to the terms of the contract with the U.S. Department of Commerce – which originally operated the root server system – from VeriSign to ICANN. As part of this process, IANA, the Internet Assigned Numbers Authority, will apparently have the same level of access control as ICANN's Security and Stability Advisory Committee. The number of people with access to the consoles in the figurative and literal bunkers that control the Internet is expanding. Shouldn't we have a strong assurance about the identity of the people touching the buttons?

Outdoor Facilities Alongside the Highway

But as long as the subject is these outdoor things called web sites and their certificates, should we not look for the kind of accountability we have when the officer of a corporation takes responsibility for its actions? Is there any reason why the digital signature of an individual officer of QualityStuff, Inc., properly identified, should not accompany that site certificate?

Do you suppose that site's privacy statement might get a little more respect from management if management had personal skin in the game?

That wraps up the *places* part of the Quiet Enjoyment Infrastructure, the InDoors Infrastructure.

Unlike the Authenticity Infrastructure, we don't need clumsy mnemonics to help us remember how the InDoors Infrastructure works. All we need to do is recall how to use a building. That may require forgetting how to use traditional access controls, which shouldn't be hard, as their complexity makes them far beyond hope of rescue by mere mnemonic aids. If you don't spend twelve hours of every day immersed in rwx rwx r-x gobbledygook then there's no way you've retained that stuff anyway.

***

Now let's move on to the things part of QEI, the Common Vocabulary Infrastructure.

PART 2.3

THE COMMON VOCABULARY INFRASTRUCTURE

The *Things* part
of the
Quiet Enjoyment Infrastructure

Consisting of QEI's last component:
12. The Common Vocabulary Component