SECURITY AND DISTRIBUTED SYSTEM PRODUCTS

- ***Increasingly distributed workforce *and* distributed resources are demanding and receiving more support from internetworking***
- ***Risk trade-offs need to consider a broader attack surface, including multiple OSI model layers (networking, transport, link-layers) and risks added by VPN and VM-based device management.***
- ***Planned network "behavioral monitoring" in addition to more traditional security measures and prepared in advance of primary service configurations and contracts, in order to establish expectations for security risk and potential losses, tailored to the kind of content traffic and scale of financial or other impact.***

PRIVATE NETWORKS USING WWW

The use of different models of Virtual Private Networks (VPNs) supports steadily increased numbers of distributed enterprise workforce who need more flexible access to resources. However, architectures and access design for effective network segment performance, need to weigh security risk trade-offs with respect to protecting valuable information, whether PII, business-financial, or national security related. Industry and public sector widely use VPNs, of both Layer-2 and Layer-3 types (OSI Models[i] ^). This paper considers some aspects of VPNs and balancing security considerations against satisfactory end-to-end performance for the network's users.

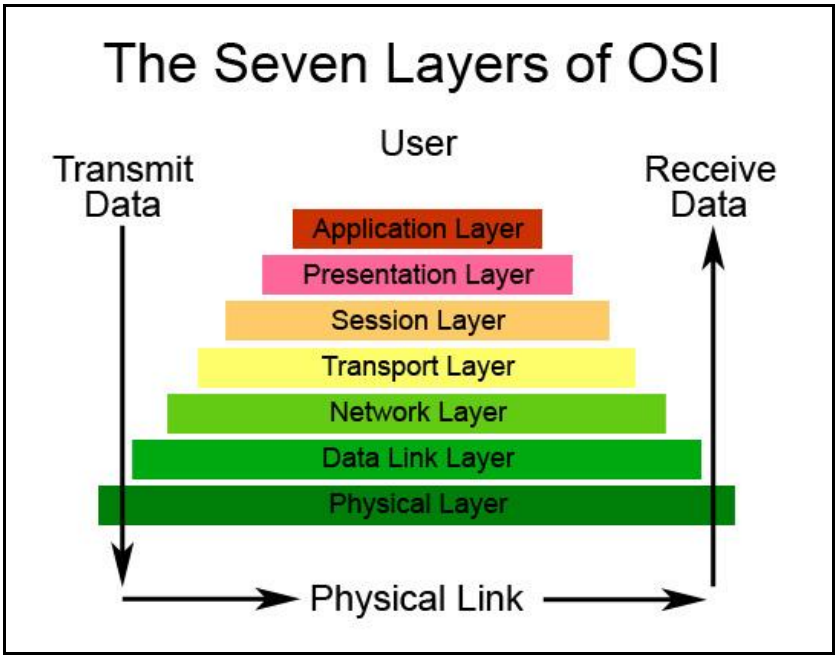

Figure 1, Washington University, Information Technology, URL at end.

These architectures also often incorporate virtual machines (VM) in key roles for administrative functions such as an authentication server. In addition to network node security (client and server computers), network design and protection should consider broader kinds of vulnerabilities and "the network edge" situations that valued content will meet, traveling over the network. Risk metrics can be used systematically to monitor and advise owners, users and administrators about the network's security, relative to potential attacks affecting: *Confidentiality* (sniffed or copied traffic); *Integrity* duplicated or altered message; *Authentication* and *Availability* (required service reliability).

Distributed Operating Systems and Networks Components

If connectivity is provided using segments of the WWW to private or public networked assets by a server or virtual server, message and data traffic are potentially exposed to *any* WWW user. This

liability could be increased when machine-administered border switches grow the network in an unintended way, with peering or neighboring process. In today's environment, however, explosive increase in networked communications has made machine-machine administration unavoidable and the maintenance of computer or terminal operating systems for individual computer nodes or routing-switches more technically specialized and challenging.

Connection of segments of networks changed in the last decade. Tier 2 Internet Service Providers (ISPs) use router peering for more effective traffic management and managing bandwidth availability to customers. Where earlier, a Tier 1 (national backbone) switch for traffic management typically received a high degree of protection against misuse, current ISPs at Tier 2 may not have been set-up for strong enough security, depending on the traffic character.

Operations and Data System Maintenance

Operating Systems (OS) as well as databases for servers might reside on multiple nodes, or be homed to several segments for networked enterprise assets. This practice supports rapid, redundant and more reliable service or communications, but raises questions for practical security maintenance:

- What patching-arrangement protects the operating system, whether Unix-related OS, Windows, or other, against new threat schemes which change at a current rate of many hundreds per year?
- Fair financial arrangements and licensing: OS are mostly proprietary, with patented elements, and require substantial development and test effort, recovered through licensing and service fees. Even OS that began as Open Source, now have licensing requirements as they are adapted to specific enterprises.

Applications Policy and Boundaries

Application level proxies enforce security elements like confidentiality and authentication on web-based systems; they now have responsibilities for everything from banking records to corporate product liabilities. An application firewall typically controls the session access for Web-enabled exchanges such as web-mail for approval processes, or online payment portals, in several ways:

1. Valid conditions for the user/operator have to be met under the session policy, such as matched password and matched ID validation to begin.
2. The application firewall examines the links and requests for context-appropriate activity.
3. Request is passed to the server will be blocked if they do not match policy.
4. Session policy is destroyed when the session ends (time limited)
5. Credentials will be retired or deleted within a specified time limit if not used (sunsetting). [ii]^

One of the challenges arising is the need to clearly delineate "address boundaries" (trusted segments) where greater security has to be maintained.

SECURITY SUPPORT WHILE INTERNETWORKING

Technical assistance and system administration for internetworking has grown more complex, specialized, and expensive, in terms of associated technical Human Resources, often divided among several organizations by formal Tiers of Service Level Agreements. Methods for managing security for web-based intra-networks have characteristic obstacles, including for example:

- Advanced content filtering for protected material
  - Expensive, labor intensive, tailoring for many categories
- Authenticated access filtering, for devices (servers and routers)
  - Administrative complexity, subject to spoofing if automated
- Role-based and view-based system administration, granting individuals' privileges
  - Administrative complexity, subject to spoofing if automated
  - High change management workload and labor intensive
- Restrictive transmit-receive nodes administration (autonomous system border routers)
  - Legal and administrative complexity (ownership of complex SW products or systems)
  - High change management workload and labor intensive
- Discretionary access control, human recognition based, for system operators-users
  - Weakness in authentication mechanisms (human and machine identifications)
  - High change management workload, and
  - Legal and administrative complexity (ownership of complex SW products or systems).

In distributed information structures use VPNs, the network protocol stack on a node is re-ordered and forced to communicate only with the designated organization (Provider's) router. ISPs maintain both gateway and network address-management strategies. Any architecture that establishes VPN access over WWW segments might also be used to provide (unintended) Internet connectivity to sub-sets of individual nodes using IP-address translation, with Network Address Translations.[iii] ^ NAT methodology has been recommended for retraction to "historic status" due to a variety of problems[iv] ^ for Internetworking managers:

- Vulnerability to re-direction
- Binding state decay
- Incompatible semantics
- Internet Group Management Protocol(s) – IGMP, exposure to misuse
- Non-global validity of records (…and more)

Configuration Challenges

To gain benefits of re-usable open-source software at lower cost, telecommunications and network implementations with non-standard or embedded architectures might use Linux-based or open-source operating systems. The same code that adds flexibility and cost advantages, however, may bring

characteristic network threats, related to older, more primitive network protocols. An example in IP-based systems' transport layer is the disruption of time-out settings of the ICMP message exchange, potentially making end-to-end connectivity unreliable.

Java or Javascript configurations may be used to define security constraints in web-deployed Company resources. These need clear use-case specifics to be effective. For example, a Web request may not be "blocked correctly" if the definition for advanced access works with a deployed software agent for link management. In troubleshooting examples: If Systems Admin uses a ping-request to find subnets, or flow-control devices (router), an attacker could duplicate captured packet information and potentially disrupt Time To Live settings or similar.

Layer-3 VPN uses for test, special-use addresses, like loop-back and default multi-cast routing provide methods for network initiation and testing. For systems administration, troubleshooting and internetwork performance validation well-known ports and addresses are used by the applications.

Layer-2 tunnel VPNs validate access with IPSEC for legacy assets. (See RFC 3193 and RFC 3068 on Anycast IP process). Once requesting node is validated, PPP technology "unpacks and forwards the message or data to the intended host." IPSEC with Anycast conventions and encryption (can authenticate a remote access, transport layer) [v]^ Designers need awareness of limitations:

- Limitations due to default-addressing in Anycast, authentication process of communicators
- Host and gateway trust processes may require improvements for compatible operations
- Unix- Linux-based protocols for VPN, use SSL and SSH, with well-known ports and defaults.
- IPv6 to IPv4 relay mechanism uses well-known required default addresses.
- Extensible authentication protocol for variable authentication options is under current work, toward assuring PPP confidentiality
- IPv6 neighbor discovery process is impacted by variation in "maximum transmission unit" (MTU) that may be exceeded by changes to headers. [vi]^

Layer -2 VPN
In this case, the networking provider, perhaps a satellite services vendor, using Asynchronous Transfer Mode (ATM) with frame-relay based transport, depends on established trust relationships at the network edges. Each "virtual wire" is like a leased line, privately paid-for, with service level and quality of service agreements to subscribers. Packets on the "wire" are encapsulated and encrypted; or, if potentially selected for higher latency options *within commercial agreements,* when frames are tagged or labelled. instead of encapsulation and receive rapid switching across the segments, for example with Multi-Protocol Label Switching (MPLS).

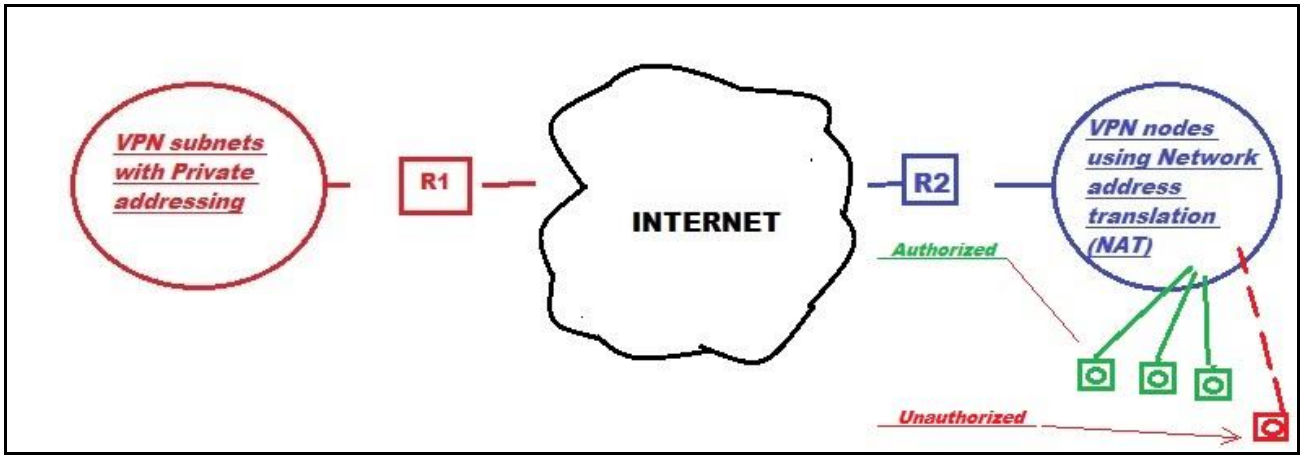

Figure 2, node address management strategies

Service Performance Quality: Conflict with Security Measures

For data-in-transport over public switch segments, some parts of the "wire" are not likely to get guaranteed quality of service (QoS), which is very attractive. Enterprises choose solutions as a best performance compromise, in order to take advantage of speedier, full-mesh networking paths, and should expect to harden authentication (know the users) mechanisms and keep encryption up to date.

When context or mission sensitivity is high, and categories of content have to be kept private, public segments' use has to be prevented (WWW). Rigorous identity authentication and role-privilege administration can be very challenging for distributed communications' environment. In general, IPSEC sits 'between' the Layer 3 (networking) and the Layer 4 (transport) layers; but for greatest security, controls are best implemented in the hardware.

REMOTE MANAGEMENT FOR SERVICES, A HOME POWER EXAMPLE

Power metering devices have been in used for close to two decades. Operating systems for the devices that collect and report usage of electricity are simplified versions of the major computer operating systems like Windows 7 or Linux. An example is Zigbee®. Zigbee radio terminal manages the HAN connectivity to cellular system. Like the Zigbee, leading OS use out-of-band control mechanisms for remote configuration. Head-end software (SW) connects via WAN, from head-end to the primary service provider, giving users/ user devices roaming usage information of multiple kinds. On communications power consumptions for multiple devices in a household such proprietary software administers Quad-band access to GPRS systems that operate in the 2.4 GHz band to automatically report on power usage of the system devices.

RFC 3193 describes IPv6 to IPv4 relay mechanisms with out of band management of servers for Ethernet connectivity to legacy equipment. The default IP-use has automated PPP "unpack and forward" that could potentially bypass system security.[vii] ^

When a Virtual Private Network crosses multiple Tier-1, Tier-2, and other segments, it can be protected with strong encryption and log-on processes, but identity management (authentication) and coordinating across internetwork proprietary technologies and file formats can present many challenges. While management of infrastructure mentions intrusion detection and firewalls as a matter of course, the discussion often does not include strengthening the authentication of identity mechanisms.

PPP Confidentiality

In view of the broad attack surface for using Internet (WWW) connectivity, Identity Management within systems is a key mitigation for security risk. High performance authentication strategies use "machine-machine," "user-machine" or "machine-user, and "user-user" recognition operations to secure messaging content. Filtering at the employment enterprise-end, might approach the problem with known-device methods and known-user-operator strategies.

Monitoring equipment on Home Area Networks (HANs) use many of the new Service Oriented Architectures that combine pay-per-service IT management solutions.

Home Area Network Monitoring, A Power System Example

A proprietary cell-based technology based on the Zigbee Operating System is described in Trilliant Communications data sheet for an integrated identify management solution, Home Area Network communications devices, the Mobile Identity Management Initiative – GSMA[viii] The radio device is a communications bridge connecting smart energy usage devices as well as Zigbee OS based tunneling for transparently supporting (usage monitoring). Many devices of different types within a home can be monitored for how much connectivity (bandwidth, based on the) they use and how much power (electrical consumption).

> "With their differentiated assets such as the SIM card, and strong registration, authentication, and fraud detection and mitigation processes, mobile operators have the ability to provide sufficient authentication to enable consumers, businesses and governments to interact in a private, trusted and secure environment and enable access to services."

VPN AND NETWORK ASSETS

Several kinds of VPN structures are common:

1. Trusted
2. Secure
3. Hybrid

:
In current types of VPN technology implementations common security assumptions include:

- "only provider (of the routes) can change the paths";
- "no (intermediate agent has a) possibility to change, delete or inject data";
- (and) addressing is pre-determined before VPN approach is initiated.

"Trusted" and "Hybrid" architectures that use the shared public infrastructure (WWW) to achieve performance advantages with trade-offs covered by policy and administrative measures:

- Example Layer 2: ATM, MPLS with BGP [ix]^
  Typically the "provider of connectivity" has a fee-structure with customers and protects networking resources to be available sufficiently to paying customer (BGP settings, for example, are oriented toward enforcing this).
- Dynamic addressing: Layer 3: DNS, Domain Naming Router, NAT, IP sub-/ super-netting
  - Here, the security measure could cause loss of the dynamic function of Web-based resources, needed for balancing large applications like a deployed Business Intelligence (BI) system, (see discussion under VPN architectures, of NAT issues).

Virtualization and OS-Model Hypervisor

Many current virtualization approaches use Unix-based architectures for distributed assets using VPN systems. Virtualization models can be of different types, possibly open-source, Public Use, or proprietarily licensed. The virtual machine uses a hypervisor to display abstracted functions, for example productivity applications on a "typical desktop."

The hypervisor makes use of the host's privileged systems through "porting," which executes required mapping of guest disk I/O functions to the physical disk I/O operations. These disk functions must use the same OS, for example a WIN OS would use Windows Terminal Services (RDP), while a LINUX OS would use Secure Socket Shell (SSH). The hypervisor executes on the host CPU by means of "time slices" and "slices" of memory and other key physical functions such as graphics processor.

The "OS model" of virtualization, unlike the older hypervisor models, does not modify any of the host system physical processes. Instead, "...the host runs a single OS kernel as its core and exports operating system functionality to each of the guests." In this way, the OS-model hypervisor function is supported but makes sparing use of the host physical resources.

> "(Platform) common binaries and libraries on the same physical machine can be shared, allowing an OS-level virtual server to host thousands of guests at the same time." (Kizza, p. 451-2)

AUTONOMOUS SYSTEMS WEAKNESSES

Availability of services is sometimes be overlooked as a "security concern," but flow-control can be critical to an enterprise and has held strong popularity as a cyber-crime attack surface. Well-known ports, naming conventions or protocols and restricted physical framing parameters are enablers for this weakness.

AS make use of well-known ports and protocols for inter- and intra-network routing. These depend on automated resolution of "prefix specificity," and other validation mechanisms, to get correct routing to the users' or organizations' IP-based network segments within a segment where the traffic comes from a "guest." For example, security hazards could arise from flooding done with a query to find root-zone "ANY." Security administrators for the network or intranet would have to set up IP-tables rules to manually prevent or limit certain kinds of queries.[x]

Gateway Issues: **Protecting the Edge**
"Outside Domain" bind-process on an authoritative Name-server with a publicly available Name can be subject to flooding attacks, a characteristic vulnerability in distributed denial of service attack (DDoS). In this event, a recursive DNS query causes many faked- "ANY?" requests to be left open, too many "DNS BIND" resolvers (up to 1000 are allowed).

AS that are BGP speakers, an ever more popular solution to networks using multi-vendor equipment, have routing vulnerabilities due to "concentrators" or route-reflectors (RR). These are sometimes configured to add redundancy (availability protection) for a BGP-mesh network. The RR is a BGP-speaking central routing server that can "peer with" multiple ISP-BGP-speaking routers. It is able to share IBGP, *internal routes*, which that normally would not go outside an organization's own intranet. Any client of the RR should be configured to be unable to peer with internal BGP-speaking routers that are outside of its own association cluster, for better security. The RR could inadvertently create vulnerability due to preservation of NEXT-HOP properties, when mesh-routing redundancy has been set up without physical routing assets configured as back-up. Good practice should prevent this: "...route reflector redundancy (makes "no sense") if the physical redundancy itself does not exist." [xi]^.

VULNERABLE IN-TRANSIT STATE

Distributed use of systems is increasingly dominant in business and government, so the "State in which information is secure" must go beyond the computer itself. Some organizations charged with security of networks have not caught up with these implications. The trade-off in desired performance (particularly speed of applications and explosive growth in ubiquitous connectivity), attracts too much customer interest and drives commercial initiatives. Current research, in industry or public sector, aims to improve or help security professionals balance risk trade-offs early enough and clearly.

Data traveling over publicly switched segments runs the risk of easy capture, beyond malware threats. . Network security staffs regularly implement port scanning and filtering to protect against malware or back-door implementations using well known ports such as port 1080 for html files or port 1234 (Java client). However, recent technical attacks have begun using varied and unassigned port numbers, making protection against application layer attack more difficult. Even encrypted traffic faces more serious threat due to increase of states-sponsored advanced computing.

Channelized Physical Capacity

Information in motion typically travels in a communication channel and across different environments, media carriers like: air, wire cable, optic fiber, for example. With modern modulation and coding techniques, multiple voice-data channels are combined into a single digital line while in transport, often compressed. The physical limitations of channel transport can themselves pose a security risk, when maliciously misused, for example in spoofing of a node address (IP or MAC).

As information is in motion or transit, the protection from some kinds of threat or disruption has to consider the kind of circuit. LAN/WAN architecture may present issues such as:

1. Access related (violation of policy, whether careless/accidental or malicious, which may be machine-audited)
2. Inadequate cryptography (depending on the content's interest, captured messaging could have to withstand advanced computer decryption, "brute force" attempts)
3. Transport "pipe" operations or frame-sizing limits (flow control not maintained), distributed denial of service, ACK-flooding or spoofing related
4. Exchange protocols' inherent settings: relates to complexity or out-of-date configuration (old defaults on legacy equipment, like "stuck in connect" phenomenon, routers).

Spoofing and Routing on IPv4 and IPv6-mixed VPNs

Following provision in the Internet Standards RFC [xii]^ for IPv6 systems to IPv4 systems introduces a weakness in machine-to-machine authentication: "(4.2) ...6to4 relay routers...shall advertise the 6to4 any-cast prefix, using the IGP of their IPv4 autonomous system, as if it where (sic) a connection to an external network RFC 3068 added any-cast mechanisms…" Since the IPv4 autonomous system will advertise this relay router (as if) it were a reachable network:
"Packets sent to that unicast address will follow the same processing path as packets sent to the anycast address, i.e., be relayed."

This set-up represents a vulnerability to address spoofing for the protected relay domain: "(4.3) …an IPv4 autonomous domain that includes 6to4 relay... advertise(s) reachability of the 6to4 anycast prefix..." In addition, since default routing for the any-cast domain generally will use hardware based routing when available, for the sake of speed, the vulnerability may represent a destruction threat to key resources in the domain.

An IPv4 autonomous domain that includes 6to4 relay, under current conventions, has to "... advertise reachability of the 6to4 anycast prefix... (and) "also include an indication of the actual router providing the service…" [xiii]^

VM-agent V&V process for establishing "peers" that control traffic routing and maintaining availability of subnets, called "prefixes." Current IETF process suggests performing this function by documenting the router's equivalent IPv4 address in the BGP aggregator attribute.

Routing Aggregation Problems (CIDR and VLSM)

Aggregation-disaggregation attacks take advantage of how CIDR is implemented to provide dynamic controlled use of (limited) connection resources:

> VSLM is used to implement subnets of various sizes, whereas CIDR is used to implement Supernetting. CIDR and VLSM are concepts. Routers need to be able to support these concepts if you are to use them. If a router supports one then it supports both. CIDR refers to assigning any size mask to a network regardless of its class. VLSM refers to increasing (subnetting) or decreasing (supernetting) the mask bits in relation to the IP class.
> (https://learningnetwork.cisco.com/thread/13749)

Identity and Any-Cast

Inter-system routing solutions could depend on any-cast routing and IP allocation validation when there is a mix of IPv6 and IPv4 protocols in the stacks. Finding the effective route in such an architecture has challenges and is not always resolve the same way between organizations. With IP Any-Cast routing, configuration can be designed to simply, set the configuration of IPv6 to IPv4 relay routers ("6to4"), with a prefix (network) advertisement that supports a "pseudo-interface." These routers for 6to4 use a default inter-domain route with a standard "null prefix" host identifier for each end, the IPv4 and IPv6.

Encryption (updated treatment of wireless segments, between cabled secure segments) has to be agreed in advance for authenticated access to: Modems, Cable-heads, Wireless device (MAC or address) to include "agent administered" systems tools, for remote networking and communications maintenance.

Switches, routers, load balancers, and network translation devices have potential, as programmable entities, to improve the effectiveness of a network or to harm it. The distributed protocols used in this context may also optimize link utilization and define special "reachability domains." Dynamic bandwidth allocation has become practical in many situations, so the "device" itself can calculate, request, and inform contracted service (of the amount) of connectivity required.

Network equipment vendors currently do not usually allow or permit applications on their equipment although they certainly could process them. Routers, considered "too critical," typically do route calculations all independently of particular topographical information on the router. Routing solutions often are dependent on "rumor" in the architecture

BGP scales badly (too much overhead) and intranets are subject to "De-aggregation" attack, where the specification of "global limit" for (routing resolution search) is not good enough; global routing is disrupted because of the rule that "more specific" address resolution should be preferred. How often does "prefix specificity" create errors? Can it be done intentionally, as a kind of attack (this would be a form of DoS attack)

Economic aspects have to be carefully considered in advance of Service agreements:

> "It is estimated that the global number of identity theft victims since 2005 is more than 500 million, with an associated cost to businesses worldwide of more than US$200 billion.

Added to the picture created by theft and fraud attacks are integrity and authentication attacks against signal traffic in travel, protected availability or end-to-end flow. Network performance can be "held hostage" in a variety of ways, both physical – for example frame-size restrictions managerial.

Agent-based Gateway and Time Referencing
Eco-systems of growing IP-based services and Service-Oriented-Architectures bring increasingly complex management scenarios and sometimes unforeseen security risks. Host and gateway trust processes make effective VPN use possible. Current improvements introduce more accountability for SW process problems: Studies used geometry-of-contact events to see computer driven effectiveness, integration, processing and (led to assignment of) rescheduling "penalties" during builds of audio-visual "stepping functions." [xiv]^ (See *ACM magazine* on smart-grid, Quality of Service considerations).

Time Referencing
Timing and clocking for signal processors has made great strides in the last 5 years. A cesium beam clock, similar to one manufactured by Symmetricom® costs about $50,000 and keeps time true to about 1 microsecond a month (10^{-6}) seconds-lost in that period. More stable and portable clock designs enable utilities and networking fault tracing with inexpensive microchip-size atomic clocks. [xv]^

IP and higher layers (e.g., TCP, UDP) MUST continue to accept and process datagrams destined to a deprecated address as normal since a deprecated address is still a valid address for the interface. ..

MAINTAINABILITY AND BALANCING RISK

- Threat correlation and team planning for turn-around time in maintainability

- Sensor false-positive, false-negative verification process or VM-agent V&V; techniques for filtering
- Effective data-mining for keeping a better track record on complex system
- Game day strategies for improving survivability of a key system and flushing out surprise weaknesses
- Better network security risk management requires management involvement and not just IT and security staff.
- Good data mining support and automated tools to help system administrators scope the people-strategies, distributed auditing, and protective SW or HW that is needed.

Economics and Overhead for Security
Customers normally care most about performance and responsiveness of system and internetworking security strategy may be overlooked or rejected as having too much network overhead. The potential for financial damage or organizational damage potential needs to be quantified during enterprise initiative planning in order to gain leadership support for the "somewhat invisible" mitigation needed for mixed system security.

Non-technical or Low-technical Risk: Social Engineering
A great many examples are known about human "system members" vulnerability to criminal tricks and schemes. The local phone base station switch can be spoofed (temporarily reprogrammed) to show "any number." This trick has been used by social engineers to fool a call receiver into thinking they got a call from "corporate headquarters" or "police" and to relay whatever information was requested. Anonymous FTP accounts can be installed for bad purposes on innocent organizations' equipment, such as a library. Attackers in Mitnick's example impersonated members of an R&D team and asked to have files transferred to "Research Center" computer by FTP. They provided the fixed-IP-address of the machine that was really a general computer of the University. Then, proprietary source code can be taken from the (general school computer), using a USB drive, and FTP server uninstalled from that machine. Unauthorized people have used such a method to take a private SW Product – which could have been sold to competitor or even foreign government. [xvi]^ Motivation is most often financial, for example: an inside attacker is aiming to get cash flow and P&L information on a company prior to the information's release, in order to take advantage of stock trading before the SEC makes the information public

Speed of Change and Operations Monitoring
Network operations, and particularly weak areas like known system defaults, should be examined routinely from a "behavioral" viewpoint. Speed of change puts pressure on responsible network centers to understand the financial impact of weaknesses, to be active with models for distributed intrusion detection, and to have a good grasp of how serious or non-serious the resulting damage could be.

To get balanced business value for expensive tools and security services on networks, organizations in the near-term have recently been "unbundling" a variety of configuration management services, according to Armed Forces Communications and Electronics Association article of Sept. 2013 [1]^:

> "Right now, many companies offer cybersecurity as part of a larger package deal ...larger contract" (but) "cybersecurity will be unbundled" and "value chain (will take opportunity to) sell cybersecurity services, hardware and certain software….
>
> We didn't go from Kitty Hawk straight to fighters with turbojets, but that's what has happened with the Internet... The easiest place to catch someone (encounter threat) is on the superhighways, on the big backbones of the Internet." (Seffers, G.

1 "Critical Infrastructure Ripe for Attack," Cyber Trends, AFCEA International Journal, June 2013, SIGNAL® publication of the AFCEA, Fairfax, VA.

I., "Cybersecurity-Everybody's Doing It," *Armed Forces Communications and Electronics*, June 2013, p. 33)

For large autonomous systems' enterprise configurations, constant technical watch has to capture audit data by means of filtered and automated templates tailored to security interests and examined against a logic-driven model to analyze for suspicious system-behavioral patterns. The tool would catch and count things like "failed attempts at access," "(hidden) system files access," or anomalous changes in access control. (See discussion of University of California, Davis, model, *Stallings*, p. 579).

In conclusion, the digital highway in the last decade is clearly moving to ubiquitous availability of working resources. System security staff do well to invest in

- Means for behavioral monitoring of inter-networks, according to information sensitivity and value
- Regular automated checks of a broader attack surface for key enterprise systems, including link-layer and transport technologies, and
- Quantification of the "risk assessment" calculation to be able to quickly support decisions facing necessary large upgrades or migrations of valuable assets.

Primary References:

1. Comer, D.E., *Internetworking with TCP/IP*, 5th Ed., Cisco Systems and Purdue University, copyright 2006, West Lafayette, IN
2. Kizza, J.M., *Guide to Computer Network Security*, 2nd Ed., Springer Publishing, copyright 2013, Chattanooga TN.
3. Halabi, S., with McPherson, D., *Internet Routing Architectures*, 2d Ed., Cisco Press, copyright 2000, Indianapolis IN
4. IBM International Support Organization, "Multiprotocol Switching Services (MSS) Release 2.1" SG24 – 5231 – 00, http://www.redbooks.ibm.com/redbooks/pdfs/sg245231.pdf , Nov. 1998, accessed repeatedly Nov. 2013.
5. Stallings, W., *Cryptography and Network Security*, 3rd Ed., Prentice-Hall Publishing, copyright 2003, Upper Saddle River, NJ.
6. Stewart III, J.W., *BGP4 Inter-Domain Routing in the Internet*, Addison-Wesley, copyright 1999, Saddle River NJ
7. University of Colorado, "Java ™ Web Services Tutorial: Web Services Security," Colorado Springs, CO, http://www.cs.uccs.edu/~cs526/jwsdp/docs/tutorial/doc/WebAppSecurity4.html accessed Oct. 10, 2013.
8. Weltman, R., Dahbura, T., "LDAP Programming with Java," *ACM Digital Library*, Addison-Wesley copyright 2000, Boston, MA.

[i] University of Washington, "Learning and Scholarly Technologies", UW Information Technology, http://www.washington.edu/lst/help/computing_fundamentals/networking/osi accessed Dec.1, 2013.

[ii] Kizza (above), Chapter 7, Security Requirements specifications.

[iii] Comer, *Internetworking*, (above), p. 352-370.

[iv] RFC 4966 "Reasons to Move the Network Address Translator-Protocol Translator to Historic Status" (IPv4 with IPv6 problems), http://tools.ietf.org/html/rfc4966#page-13

[v] RFC 3068 and 3193, anycast routing and authentication, Layer 2 tunnel, https://tools.ietf.org/html/rfc3068 accessed Nov 30 and repeated.

[vi] RFC 4861, "Stateless Address Autoconfiguration" "Neighbor Discovery in IPv6", https://tools.ietf.org/html/rfc4861#page-52 accessed 1 Dec 2013.

[vii] RFC 3193, "Securing L2 Tunnel Protocol" http://tools.ietf.org/html/rfc3193 accessed Nov 30-Dec. 2, 2013.

[viii] *Trilliant Communications Hub: Data Sheet*, a Zigbee (OS) based Home-LAN device, "GSMA," http://www.gsma.com/mobileidentity/, accessed October 5, 2013.

[ix] Stewart, *BGP4 Inter-Domain Routing, (*above), p. 66-71.

[x] "Tier 2 Security Measures, Protecting Against Attacks," *OpenNIC Wiki*, http://wiki.opennicproject.org/Tier2Security accessed October 10, 2013.

[xi] Halabi, above, (p. 264-267).

[xii] RFC 3068, IETF rules for IPv6 to IPv4 routing, https://tools.ietf.org/html/rfc3068 accessed repeatedly, Nov. 2013.

[xiii] RFC 3068, see above.

[xiv] Harmon, D., et al., Asynchronous Contact Mechanisms, *Proceedings of ACM SIGGRAPH*, July 09, "Comm. of the ACM" 04/12.

[xv] Gibbs, W.W. "Portable Precision: Atomic Micro Clocks" *Scientific American*, March 2012, p. 64.

[xvi] Mitnick, K. and Simon, W., *The Art of Deception: controlling the Human Element of Security*, Wiley Publishing Inc., copyright 2002, Indianapolis IN.