

Multi-Level Security Thin Client (Networks and Information Integration in support of Force Transformation)

Lin Wells

November 12, 2008

Overview

- Trends in computing (Bill Coleman)
 - Into the cloud, commoditization of IT, and thin clients (p. 4)-- Full text attached
 - 30 year cycles, each with 3 ten-year phases
 - Thin clients are expected to be a significant part of “cloud computing” during phase 3 of cycle 4 (2010 to 2020)
- Thin client is sort of “Back to the future”—BASIC computer language text terminal in an earlier era, later became graphical terminals
 - No hard drive, cooling fan, and much of RAM. Read-only storage
 - OS in a flash drive, disk on module, or downloaded from the network
- CNCI (Comprehensive National Cybersecurity Initiative) reflects increased attention to security
 - Who doesn't know about CNCI?
 - Also addresses inter-agency
 - Focus has been on DoD and IC, but will reach to everyone
- Changing focus at DEFCON conference
 - Shift to identity theft means thin client won't solve everything
 - But see NASA approach discussed below
- Cyber attacks in Estonia and Georgia—Cyber will be a feature of future war
 - Mainly Distributed Denial of Service (DDOS) attacks in those campaigns, but will be more sophisticated going forward

Benefits

- Easier to secure
 - Easier hardware failure management
 - Enhanced data security
 - Reduced threat of network intrusion through desktop hardware
 - Configuration control
- Lower total cost of ownership
 - One administrator/50 machines now vs 1/2000 for thin client
 - Lower hardware costs
 - Less energy consumption
 - More efficient use of computing resources
- Less network bandwidth (maybe)

Types of Protection

- Operational (VSee and NASA): Possibility of laptops in space being attacked through browsers. Since VSee naturally supports ad-hoc node hopping, this approach can extend thin-client to these challenging network conditions.
- Data at rest (Personal Identifying Information--PII)—non-persistence
- H/W, S/W and maintenance/configuration control (patching)
- Multi-Level Security (MLS)—holy grail. View data simultaneously within multiple classification levels and/or networks using the same network environment.

- Need to have “No read up,” “no write down” protections

Definitions

- Thin: some processing done on client
 - For example, machines with video cards
- Ultra-thin (or zero-client in its ultimate extension): all processing on the server--client only gets pictures of the screen.
 - Brick plus keyboard. Very low power (under 10 watts and as low as 4.7 watts)
- Security Models:
 - Biba Model—access control rules to ensure data integrity.
 - Bell-LaPadula Model--data confidentiality
- MLS as:
 - Environment (or mode—system operating there when it has, or could have, data at a lower security level— independent of capabilities), and
 - Capability (products or systems to allow MLS data sharing must be able to implement a security policy robustly)
- Multiple Independent Levels of Security (MILS)—isolation of domains without addressing controlled interactions between domains
- Multiple Security Levels (MSL)—each security level isolated in a separate un-trusted domain

Broad Options

- Either thick or thin can be single level or multi-level security
 - Wired or wireless
- Two Main approaches in OS
 - Labeled
 - Applies security labels to all activities
 - OS keeps it straight
 - Clients can talk about labeled activities at appropriate security levels. VERY hard to keep straight, but Sun and TCS have made management easier
 - Thin and ultra-thin clients are labeled approaches.
 - Pretty good for sharing info, but must coordinate apps and maintenance
 - Examples
 - DTW (DODIIS Trusted Workstation) with DIA label is about same as CTW (Combined TW) and JTW
 - Multi-Level Thin Client (MLTC). Navy approach to Secret and Below Interoperability (SABI)
 - TCS: Trusted thin client
 - All are similar
 - Secure OS starting Virtual Machine (VM) that keeps everything separate
 - Better suited to thick clients
 - VM on client uses LOTS of resources, so not on thin client alone
 - But could virtualize a thin client inside a VM on a more capable machine.
 - Admin and maintenance are hard.
- Certification and Accreditation (C&A)
 - Certifying authority does testing
 - Accreditation is done by the present Designated Approval Authorities (DAAs), which are the big six agencies.
 - The Unified Cross Domain Management Office (UCDMO) monitors and coordinates cert efforts
- Another thin-client-like approach is being done by VSee for NASA:
 - Only mouse and keyboard events would be sent from space to the ground, and pixels of the browser would be sent up. Since this kind of viewer can be trivial, it becomes simple to verify program correctness. But this basic approach would also require a lot of bandwidth. As the approach adds different levels of compression, the viewer

complexity increases, and it becomes more difficult to verify viewer correctness from source code review. The standard approaches to thin client tend to use more compression to increase performance but this also makes it more difficult to verify program correctness

- Multi-National Information Sharing (MNIS)→ Tunneling with lower classification info inside higher

Problems

- Most present approaches require good connectivity. How to handle disadvantaged or intermittently disconnected users?
 - Sun and TCS are working on virtualization to keep going if offline.
 - VSee approach with Space Station piggybacks on adhoc networking or Mobile AdHoc (MANET) networks
- Complexity: If either the label files or VM gets corrupted, it can be a problem.
 - Admin and maintenance are harder than usually acknowledged.
- C&A
 - DIACAP (DoD IA C&A Program) process is too long and too complicated
 - More time is spent in accrediting a solution than is spent to develop it
 - » Average is 1 – 2 years
 - SOUTHCOM only spent 6 months because we leveraged testing being conducted for similar product by the Coast Guard
 - Once a product is accredited, it should be readily available to any COCOM/ Service/ Agency (C/S/A)
 - » Ex., Another COCOM J6 should be able to submit SABI ticket to Joint Staff J6 with additional required documentation and within 3 months, they should receive authorization to conduct System Test and Evaluation (ST&E)
 - Unified Cross Domain Management Office (UCDMO) proposed refining process to make it easier/shorter, but it's taking a long time
 - Actual testing was only 2 – 3 months; more time was spent developing documentation and processing through respective panels/boards (ex. CDTAB, DSAWG)
 - There is very little consistency in the process for accreditation
 - It takes as much as 6 weeks for findings to be released to the vendor for fixes to be made
 - This tends to further delay/complicate the overall process of accreditation
 - Unless the DIACAP is changed, the warfighter will never be able to have best tools that industry can provide
- Labels don't lend themselves well to flexibility in "SECRET-REL" environments. If nation X drops out of the Iraq coalition and joins the Afghan one, it's hard to adjust.
- It's been hard to get systems accredited to PL-5 (TS to UNCLAS)

Next steps:

- Use clients just as Keyboard, Video, Mouse (KVM)—into the cloud
- New Apps are key
 - Build apps to take advantage of labels in OS
 - For example, within a single labeled OS, with the right app, you could open e-mails at a given security level and below and display in different windows.
- Provide more flexibility in REL-TO environments
- Support new approaches like iPhone or the screen controlled by hand movements as seen in "Minority Report" – e-commerce to me-commerce
- Revitalize C&A
 - A common set of methodologies would help, but not break the logjam.
- Ideas: National Cyber leap year—submit game-changing ideas by Dec 15. National IT R&D (NITRD) initiative

Very exciting times. Appreciate AFCEA's setting this up, and your interest

Dawn of the Information Age: 1960 – 2040

Into The Cloud!

by Bill Coleman
Cassatt Corporation

1. The Information Age: Cycles of Innovation

1.1. Cycles and their Phases:

History does not repeat itself but it sometimes rhymes - Mark Twain

1.1.1. **Cycles** are thirty years long and progress in three phases.

- Successive cycles build new value on the basis of previous cycle.
- New cycles begin at start of 2nd phase of the previous cycle; every ten years a new cycle begins resulting in three overlapping cycles.

1.1.2. **Phases** are about ten years long and proceed in three successive phases as follows:

1. **Invent Boom then Bust:** over investment in immature technology and unproven business models, usually ending in a recession.
2. **Build-Out & Consolidation:** the innovation becomes practical, consolidates the provider industry or industries and is widely deployed; new business models based on the innovation emerge.
3. **Commoditization:** the new business model(s) defuse and are the basis for creative destruction of what they are replacing.

1.2. Cycles 1 - 3: Information Technology 1960 - 2010

1.2.1. Decomposition of the mainframe, building blocks of IT:

- Cycle 1: Semiconductors 1960 - 1990
- Cycle 2: Computers 1970 - 2000
- Cycle 3: Networks 1980 - 2010

1.2.2. Each cycle adds a new class of users by **extending the reach of computing to a new “end”**.
(**Ends:** a key concept)

1.2.3. Semiconductor Cycle as an Example of Phases:

- 1960 – 1970 Invention and Boom: Semiconductors invention and boom resulted in founding of about new forty semiconductor companies in Silicon Valley that busted in a recession.
- 1970 – 1980 Build out and Consolidation: Development of manufacturing processes and equipment, tools for usage (e.g. CAD, CAM, In-circuit emulators) and consolidation of most of semiconductor start-ups. Supporting the invention of Mini-Computers, PCs & Workstations; beginning of Computer Cycle.
- 1980 – 1990 Commoditization: Semiconductors become commodities used to assemble computers and all electronic equipment/appliances. All chips ride experience curves to \$10 and eventually \$1! Foundries emerge to further accelerate innovation.

1.3. Cycles 4 - 6: The Internet 1990 - 2040

1.3.1. **Emergence of the “Cloud” and “Web 4.0”** (two separate things)

- The network of identifiable things, presence and adapting services. Active, active, active; Always on; Always connected.
- Definitions:
 - **The Cloud:** Is the computing and communications utility including OSI Levels 1 – 6, an on-demand commodity which represents the end (Creative Destruction) of IT as we know it.
 - **Web 4.0:** Is the “applications” and “services” (OSI Level 7) which consume the resources of the Cloud On-Demand.

1.3.2. **Result:** The most important human invention since language, prosthesis for life.

- The Internet of “Presence”, “Identity” and “Things” in service to the “Ends”.
- Acceleration of the rate of change, globalization.
- Reinvention of commerce, from push to pull resulting in massive productivity gains.

1.3.3. **The Internet Triad: Leverage of the Internet (The Key Concept)**

1. **Free reach (Web 2.0 & The Cloud):** Reach to the “ends”, all ends, everything and everyone is connected.
2. **Straight-thru-processing (Web 3.0 & Identity):** Providing adaptive services connecting the ends that automatically adapt to the needs of the ends.
3. **Transparency (Web 4.0 & Presence):** The leverage of self-describing data with semantic context in association with goal-seeking “Identity” to adapt the network-of-things in response to the needs and desires of the “ends”.

1.3.4. **The Internet Cycles (4 – 6):** achieving the full power of the Internet!

- **From Mass to Micro Markets**
 - **Cycle 4, 1990 - 2020: Free reach** to connect the ends; enable Web 2.0 and commoditization of IT with the Cloud of utility computing. **The final END**, there are no more ends as the Cloud’s reach is complete; but there are new, dramatically better value propositions with each cycle from Web 2.0 in Cycle 4, to Web 3.0 in Cycle 5, to Web 4.0 in Cycle 6.
 - **Cycle 5, 2000 - 2030: Straight-thru-processing** with active Identity management to enable services in the Cloud to adapt to the demands of the Ends enabling Web 3.0.
 - **Cycle 6, 2010 - 2040: Transparency** with active data services adapting the environment to the needs and desires of the Ends, Web 4.0. The final leverage of the Internet and the full implementation of The Information Age!
- **From Push to Pull Economy:** The ends gain control as **the Pull economy** emerges.
 - Pull: the “killer application” of the Internet, service to the ends!
 - Leverages network effect and long tail simultaneously in an increasingly synergistic feedback loop!

2. **Cycle 4: The Age of Reach 1990 - 2020**

- **First Phase: Invention, boom and bust 1990 - 2000**
 - **Invention:** We invented the WWW, while cycle 3 networks were built out (deployed, distributed data, distributed applications).
 - **Boom:** Technology boomed (1998 – 2001): WWW, J2EE/.NET, Web Services, Application Integration and the vision of SOA.
 - **Bust:** We busted with an over investment in technology and premature new Internet business models (e.g. ASP, WebVan, SFA).
- **Second Phase: Build out and consolidation ~ 2001 – 2010**
 - **Internet Buildout 2001 ~ 2005:** Broadband to the home, Wireless G2.0 – G3.0, IM, Search, Application & Infrastructure “Good-Enough”, Application software consolidation, SaaS.
 - **Cloud’s Infrastructure Buildout 2005 ~ 2010:** The final piece needed to complete the cloud falls into place; utility computing technology and business model are defined and validated.
 - **Consolidation:** IT Infrastructure industries (hardware and software).
 - **WEB 2.0 Emerges:** The first generation application model of the Internet. Based on the leverage of reach to the ends; it enables peer-to-peer, social-networking.
- **Third Phase: Commoditization, ~ 2010 – 2020 (The Cloud!)**
 - **IT Commoditization, IT’s an IP World:** All things really will be digital! (See “*Creative Destruction of the IT Industry*” below).
 - Triple convergence: Voice, Data, Video converge to IP. Everything generated on “servers”, distributed over IP networks

- The Network of “Things”, everything is connected.
- Drivers of change: (1) Economics of Globalism, (2) IT systems and operations complexity restricts competitiveness, (3) the new value proposition of Web 3.0 emerges (Cycle 5).
- **The Cloud: Commoditization of IT** into Scott McNealy’s dial tone!
 - Abstraction of “Application Services” (OSI Level 7) from the data center (OSI Levels 1 – 6).
 - Utility Computing: Capacity-On-Demand for application service flow. Supply/producer independent of demand/consumer. Metered utilization and billed by consumption of quantity and quality of service.
 - Commodity Pricing: Zero cost of generating incremental capacity and no borders mean commodity pricing and market consolidation on steroids! Suppliers are “transparent” inside the cloud.
 - Massive market consolidation of the service provider industries (Telco, Cable, ISP and Portal), only a handful of suppliers.
 - Autonomic: Self-configuring, self-optimizing and self-healing.
- **The IT Consumer: Surfing the Cloud On-demand.**
 - **Thin client: No “application” or “computers” for consumer!**
 - Relationship with the cloud is a metered billing relationship based on the quantity and quality of services consumed.
 - Application service (ISO Level 7) abstraction is independent of cloud (data center), owned/leased and controlled by consumer. Consumer controls usage and policy; owns their IP and can freely changes suppliers within the cloud for service and/or pricing value.
- **Creative Destruction of the IT Industry**: The Cloud commoditization of products, services, business models and pricing of IT as we know it during Phases 4 and 5.
 - **System Infrastructure** (Servers, Storage, and Network): Massive market consolidation resulting in a market which resembles the telecommunications equipment industry where there are only a handful of major players the global market by about 2020. Almost everything they sell will be generic, commoditized product.
 - **Service Providers**: Sell commodity utility IP-based service on-demand. The ultimate convergence of Telecommunications Companies, Cable Companies, ISP’s, and Portals on a global basis. Wildcard: Electrical utilities. A small number of suppliers (4-8) will constitute ~80% of global market by about 2020. Competitive keys: (1) Cost of generating incremental capability will approach zero; (2) A global market without borders; (3) Network effect. Keys for winners: Scale of economics and ability to take consolidation risk.
 - **IT Outsourcers**: Displaced by Utility Service Providers
 - **Application Software (Cycle 5)**: gone as we know it, applications will have disintegrated into loosely coupled services that will be part of the generic infrastructure. Some collaboration on open source, “service” development and specialty service component suppliers.
 - **System Integrators & “Software” Developers (Cycle 5)**: Evolve into Solution assemblers and Component vendors: Provide value through combination of: (1) time-to-value; (2) content and (3) domain knowledge.

3. Cycle 5: Straight-Thru-Processing 2000 – 2030

- Making services adaptable; the internet of position aware, self-identifying things. The pace of change accelerates!
- **Phase 1: Inventions, boom and bust! ~ 2000 – 2010**
 - **Inventions**:
 - **Application Service-flow**: Loose-coupled, composite applications and mash-ups which provide service-flow which adapts to the needs of the ends.
 - **Identity**: The fulcrum of the Internet level
 - Personal profile, roll-based, context sensitive identity system.
 - Separate of Identity, Authorization and Authentication.
 - The end of search: self-discovery

- Catalyst: Probably health records
- **Boom:** Web 3.0 is invented as Web 2.0's reach is connected through the leverage of straight-thru-processing enabled by application service-flows.
- **Bust:** This will result in bust due to over-investment in premature Web 3.0 technologies and business models.
- **Phase 2: Buildout and consolidation ~ 2010 – 2020**
 - **Service-flow Buildout:** Loosely-coupled applications service flows and Identity buildout and adoption.
 - **Web 3.0 Buildout:**
 - Ends become empowered by leveraging Straight-thru-processing to adapt, change and evolve.
 - Self-forming, self-adapting communities, value chains and economies out to the tail through the leverage of free reach.
 - Pull business models evolve.
 - **Consolidation: The end of software**
 - Disintegration of Applications
 - Applications disintegrate into infrastructure (services) due to: Loose Coupling, Open Source and Good-Enough convergence with Web 3.0 value.
 - Louse-coupling as basis of “integration” of “services”
 - Implementation is evolution not revolution.
 - Consumer (Ends) control of services delivered (policy).
 - Enabling technology evolution required: Address critical network scalability, security and latency issues.
- **Phase 3: Commoditization ~ 2020 – 2030**
 - **Commoditization:** Enables the reinvention of commerce as we know it through the power of Pull! Creative destruction of the push economy as the synergies between the network effects and the long tail dominate. The search industry is commoditized by identity.
 - Keys: Network Effects (commoditization, productivity) and the long tail (innovation and segmentation) drive everything.

4. **Cycle 6: Transparency ~ 2010 – 2040**

- The ability to turn “noise into signal” leveraging transparency.
- Automatically adapting to meet goals & policies for the ends.
- Making technology “invisible”.
- **Phase 1: Invention, boom and bust ~2010 – 2020**
 - **Inventions:**
 - **Data Services:** self-describing, self-identifying, semantic-based data management and goal management facilities which leverage and extend personal profile identity systems. Associative memory based data services will begin to emerge during this time.
 - **Web 4.0:** “Applications” which leverage transparency and automated goal-seeking technology to self-adapt and evolve
 - **Boom & Bust:** This will result in a boom and bust from over-investment in pre-mature Web 4.0 technologies and business models.
- **Phase 2: Buildout and consolidation ~ 2020 – 2030**
 - Buildout: Goal-seeking adaptive services.
 - Consolidation: The last vestiges of the mass-market economy.

- **Phase 3: Commoditization ~ 2030 – 2040**

- Pull economics enables my world under my control.
 - The dawn of the **Age of De-materialization**: three to six cycles of innovation where Nanotechnology meets Biotechnology in and on the Web. 4.0 Cloud!
-

Inter-Governmental Multi-Level Security Thin Client Event

**"Open discussion of Interoperability, Engineering and Policy Challenges"
Wednesday 12 NOV 2008**

This represented the first open inter-governmental discussion of multi-level security thin client requirements that have not been met. This event will bring into focus the state of technology today, including its advances and limitations, as well as address the engineering and policy challenges. No one can solve all of these challenges on their own; ***this event offered the opportunity to participate in building the framework that will produce solutions.***

Keynote Address:

[Dr. Linton Wells II](#), Distinguished Research Professor and serves as the Transformation Chair at National Defense University, former Principal Deputy Assistant Secretary of Defense



1. Multi-Level Security Thin Client (Networks and Information Integration in support of Force Transformation)
2. Q&A

Panel Session:

"What are the major engineering and/or policy issues that you face today in implementing multi-level security thin client?"

Moderator: [Dr. Ryan Durante](#) - DTW - Program Manager, DR-III (GG14)

Panelist: [Mr. James Seitz](#) - DISA/GO - Joint Staff Task Force

Panelist: [Mr. Hamid Ford](#) - CIO - U.S. Army Center for Army Analysis

Panelist: [MAJ Robert Castillo](#) - USSOUTHCOM - Deputy Program Chief [*not able to attend, but his points on problems with DIACAP are included in the text above*]