Virtual Worlds : “Next Generation” Security Awareness, Training and Education?

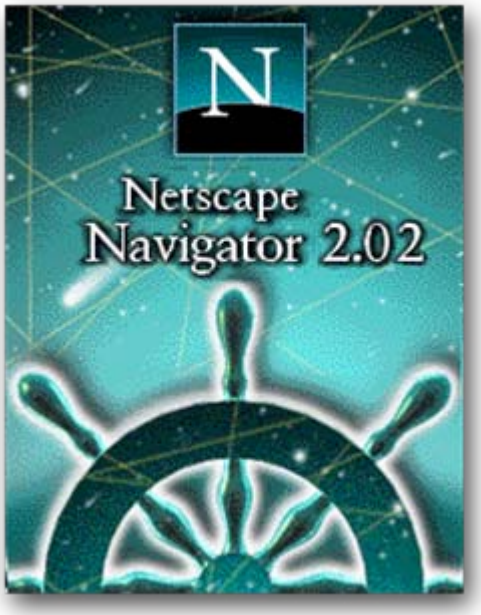
Fred A. Maymir-Ducharme, Ph.D.

IBM Federal, Executive Architect

FredMD@US.IBM.COM

Early days of the Internet…

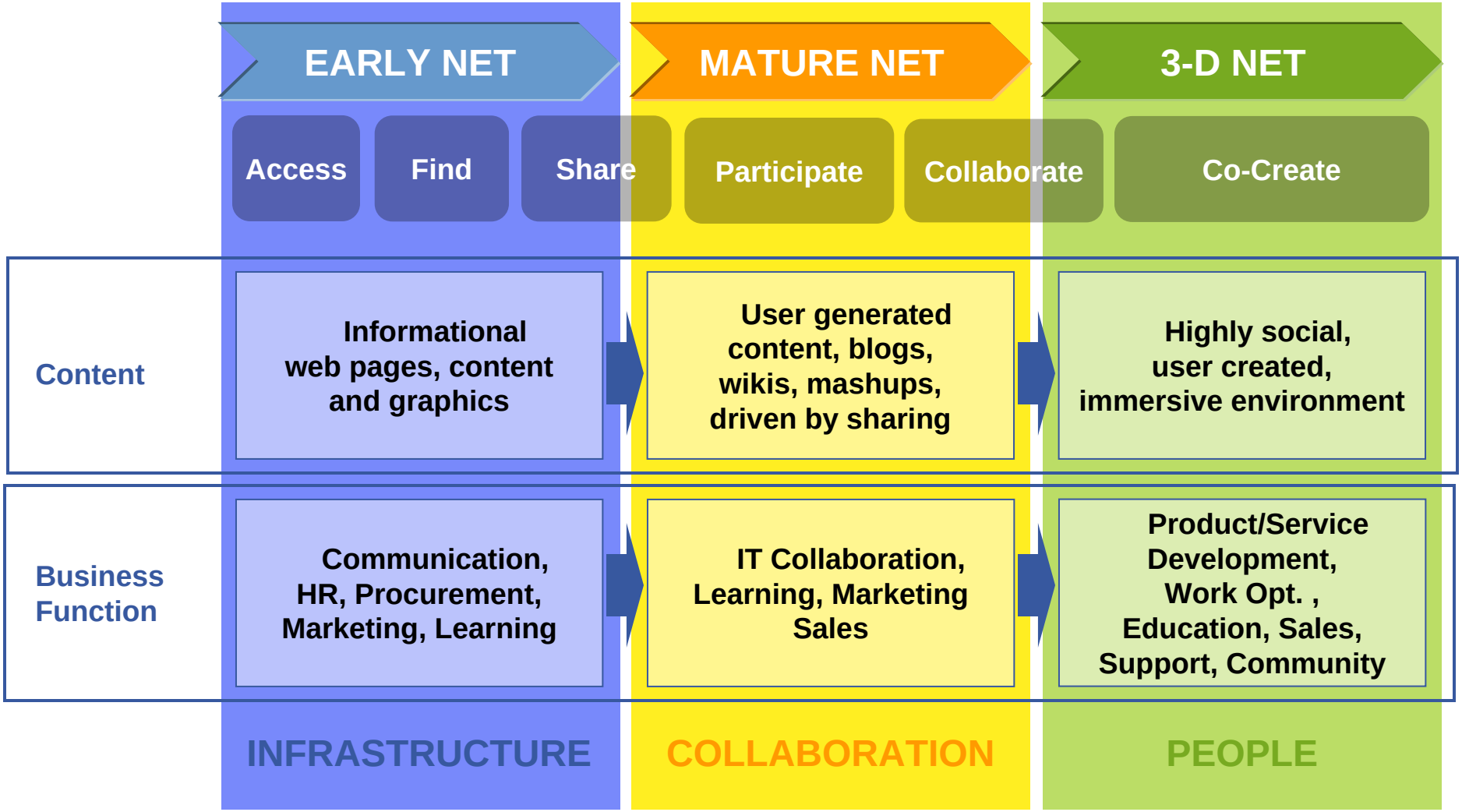
- **Few realized the Internet's business and social potential**
- **'80's (pre-web&windows) technology: rlogin, news, mail, talk/otalk, gopher, lycos**
- **Slow downloads, mainly informational web pages**
- **Killer apps, defacto standards, improving technology and lower costs drove business & social benefits**



YAHOO!

AOL.COM

The Internet evolution



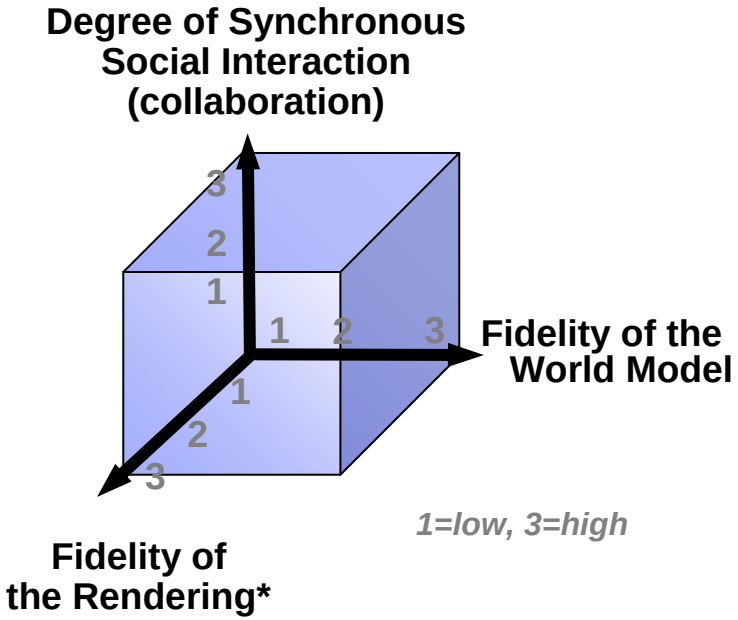
What is a virtual world?

- Interactive environment accessed by multiple people through an online interface
- Common features:
  - Shared Space: the world allows many users to participate at once
  - Graphical User Interface: the world depicts space visually, ranging in style from 2D "cartoon" imagery to more immersive 3D environments
  - Immediacy: interaction takes place in real time
  - Interactivity: the world allows users to alter, develop, build, or submit customized content
  - Persistence: the world's existence continues regardless of whether individual users are logged in
  - Socialization/Community: the world allows and encourages the formation of in-world social groups like teams, guilds, clubs, cliques, housemates, neighborhoods, etc.
  - Business: Opportunity for enterprises to conduct business tunneling through virtual worlds, in virtual worlds and as a result of virtual worlds

Source: virtualworldsreview.com

The quality of the user experience in a virtual world is a combination of the fidelity of the world rendering, the degree of real-time social interactivity and fidelity of the world model

- The immersiveness of the experience for the user is a factor of all three qualities
- Synchronous social interactivity in a *natural* and *compelling* environment is a major customer value of VWs that was missing from the previous waves of 3D web and which may have contributed to its failure
- The hardware and network is now capable of supporting a high level of experience for the user, and is expected by the consumer
- Fidelity of rendering and social interactivity are increasingly commoditized
  - future investment going forward will be in increasing the fidelity of the model, supported through simulation
  - ***This drives the need for lots of processing, storage and systems management.***



* rendering here means visual, aural and other senses such as haptic feedback

But enough traditional description… Show me!

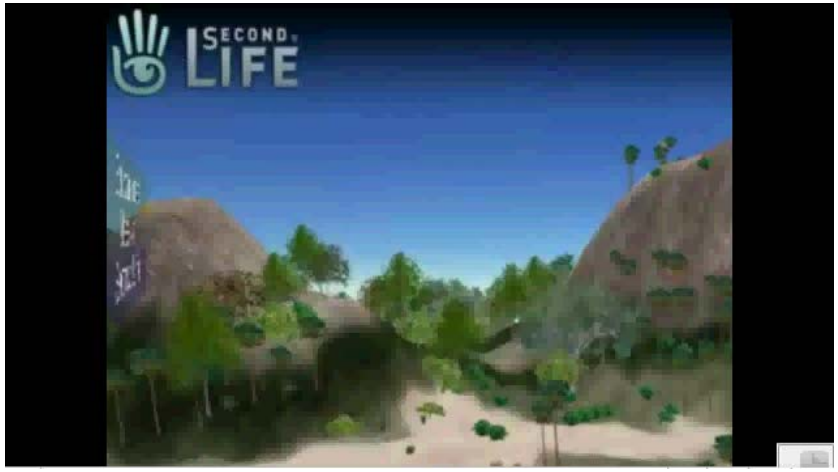
Learn more about Second Life

- Frequently Asked Questions
- System Requirements
- Membership Plans
- Land Ownership Information
- Online Safety Guide

Second Life for business or education

- Education in Second Life
- Business in Second Life
- Case Studies & Success Stories

[www.secondlife.com]



Video: Intro to 2nd Life
[www.youtube.com]

What you just saw…

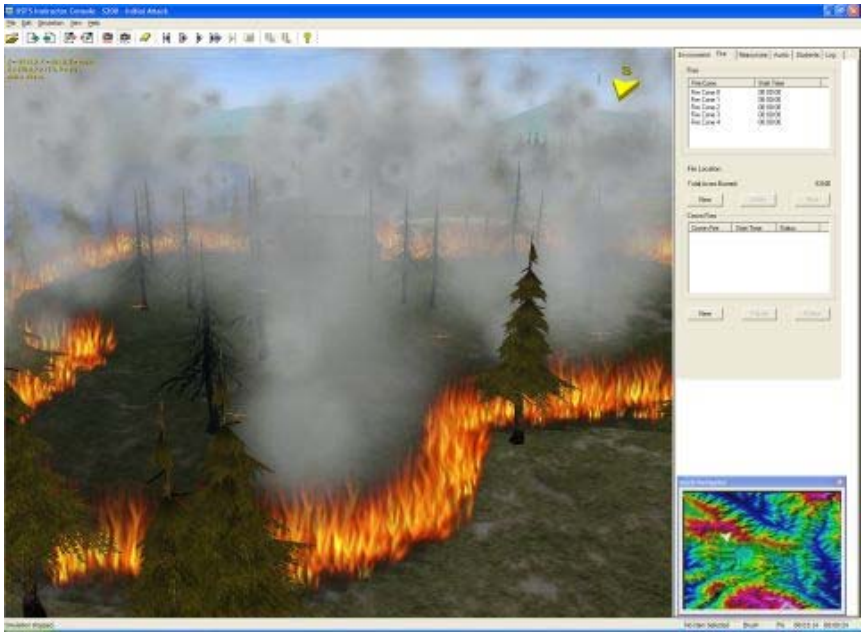
- Virtual World using 2nd Life : Avatars that walk, fly & transport, 3-D visualizations, socialization with multiple entities
- Interactive communications / actions / experiences with other people, different environments, and many “objects”
- Note use of objects as training aids
- Web 1.0 Objects (relatively static) : text, images, video, documents, slides/charts, menus, etc.
- Web 2.0 Objects (interactive) : mash-ups, news feeds, collaboration, machine translation
- Virtual World Objects (internalized) : 3-D visualizations, discovery (e.g., nondeterministic tacit knowledge), VW experience (you, inside the virtual world, with others!) Note: Every experience is unique…

Hundreds of VW videos in YouTube.com & SecondLife.com/video

VW Security Awareness, Training, and Education

Early Adopters - Education and Training

- **Spectators immersed in action**
- **Train in virtual world**
- **Rehearsal and Role Playing**



- **Simulations and response**
- **What-If analyses**
- **3-D models, immersive environments recreate real life and simplify the complex**

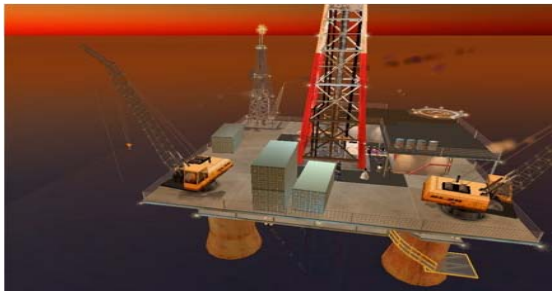
Sample business and societal applications

- **University of California Davis**

  Peter Yellowlees, a professor of psychiatry at the University of California is using Second Life to **simulate and experience** Schizophrenia

- **Center for Disease Control**

  Created virtual clinics in *Second Life* to **train emergency workers** who might be called upon to rapidly set up medical facilities in a national crisis



- **ANWR Oil Rig**

  SecondLife's ANWR oil rig demonstrates the ability for development of **education and workflow optimization** of process based industries.

IBM today –
a few examples in early education & collaboration

3D Jam at NMC

Almaden Research Meeting

VUC Round Table

GBS Innovation Conference

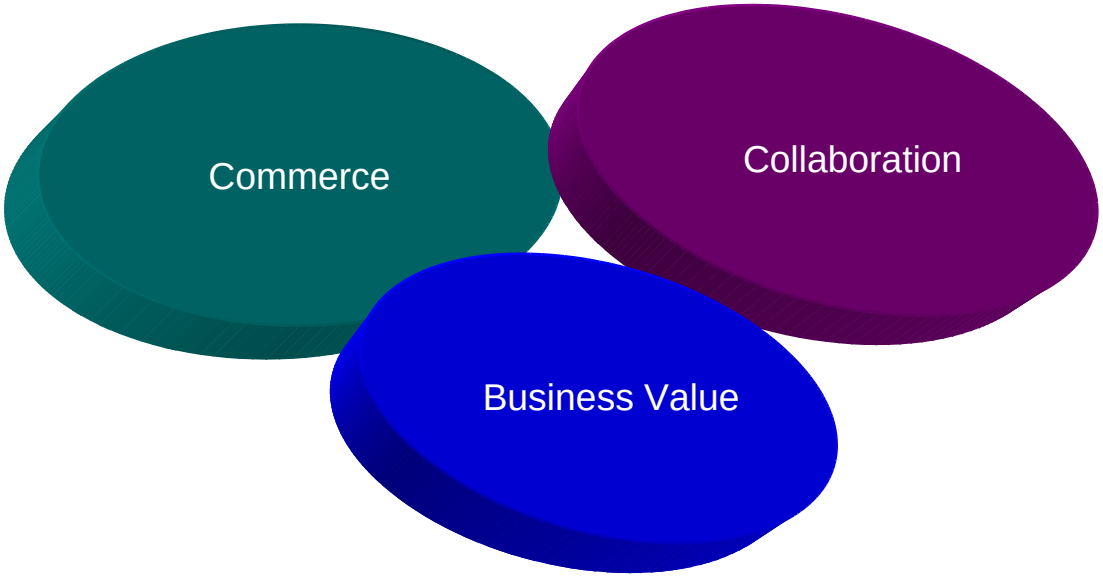
Greater IBM Alumni

Hursley Research

Help Desk

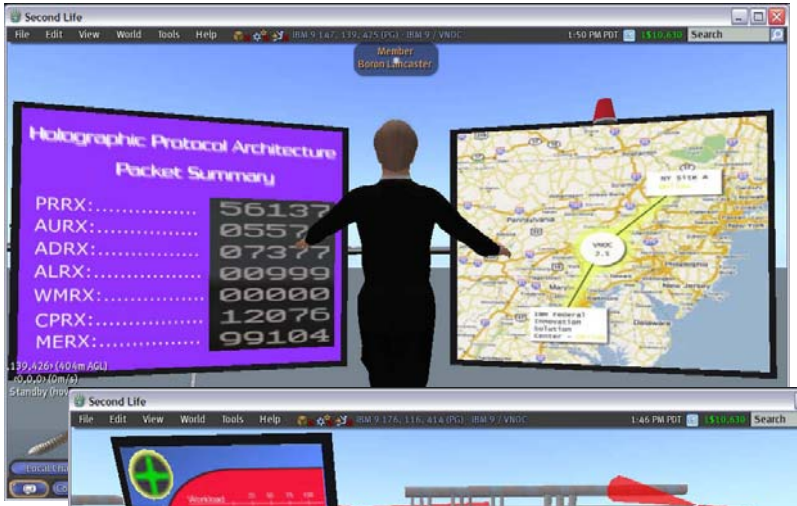
IBM in virtual worlds

- IBM is exploring these areas to ultimately help build out the 3-D Internet — one that is open, immersive and makes possible new classes of applications in all areas of business, commerce and government
- We are currently working on research inside IBM and with partners in the following areas:
  - Intraverse – a private virtual world that resides on an internal network not accessible by anyone outside of that network environment
  - Extraverse – privately owned virtual world that resides on a private network. These virtual worlds are accessible by one or more organizations but not by the general public
- As secure business tools become available, IBM will enable firms to build “3-D Intranets” and maintain radar on emerging business (e.g. IPTV) opportunities
- Established Policies: E.g., Virtual World Guidelines and Social Computing Guidelines for employees
- Extending Lotus suite of Collaboration and Web 2.0 tools to work in Virtual Worlds (Second Life)
- Emphasis and investment in Cloud Computing and Smarter Planet Initiative

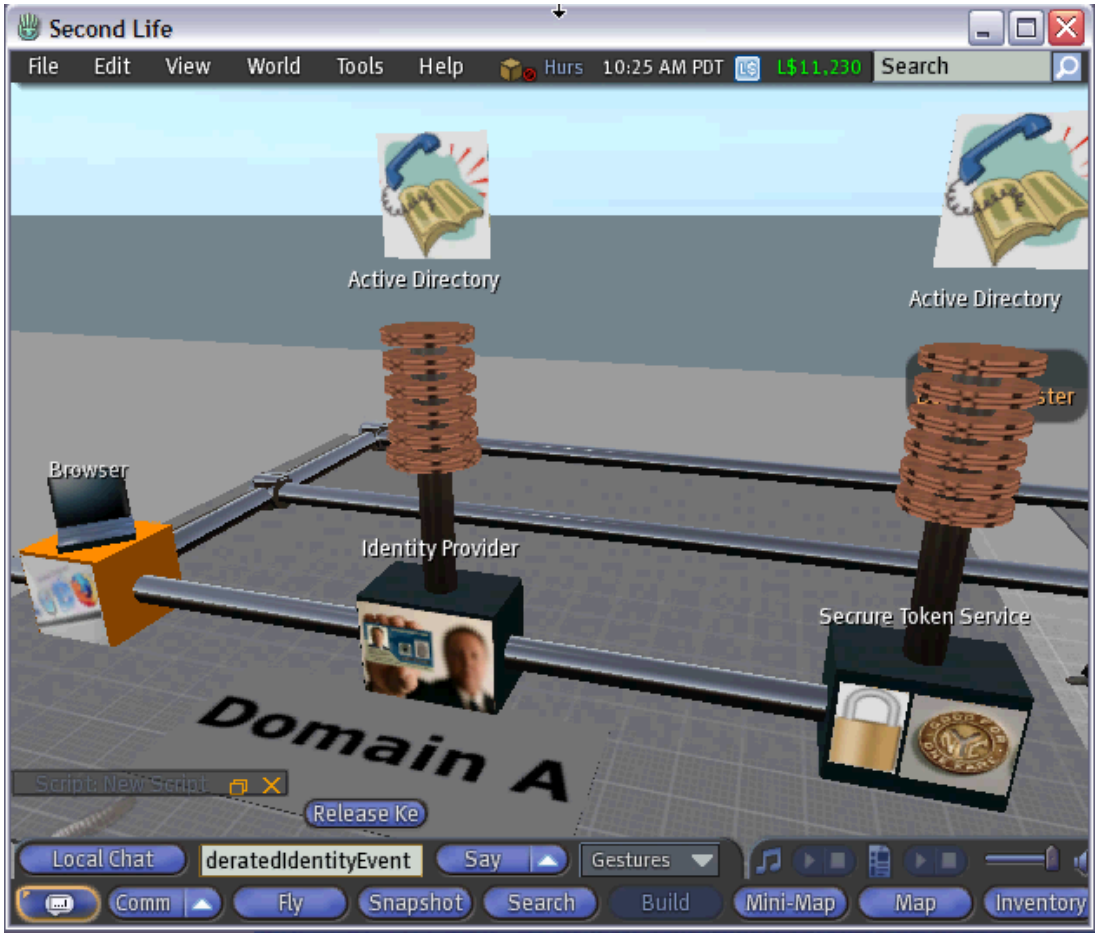


Virtual World System Monitoring

- IBM 3D Datacenter GTS offering using OpenSim.
- Engagements in Telecom, Healthcare, and Government
- Toolkit of reusable components.



Security Training & Education in Virtual Worlds



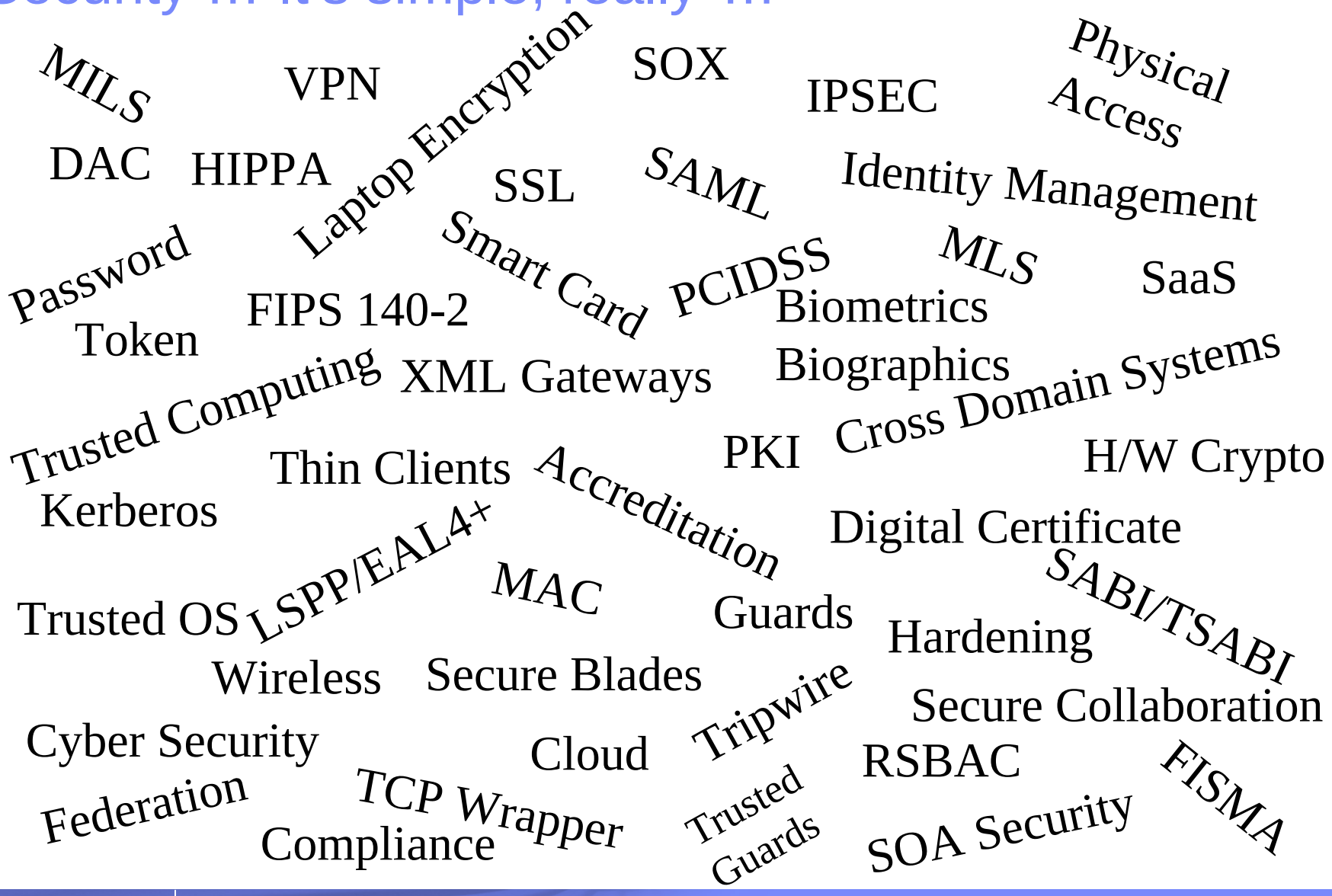
Video: IBM Federated Identity Management in Second Life

Virtual World(s) Observations

- **Immersive, social attributes reflect real life experience, and perpetually expand virtual world**
- **Beyond Second Life, moving toward a 3-D Internet, integrated with current 2-D Net**
- **Significant potential for all industries : Retail, Education, Crime**
- **Move towards open standards will reduce interoperability challenges**
- **Faster computers, improved graphics, more bandwidth continuing to improve user experience**
- **Security of Virtual Worlds is a key challenge**

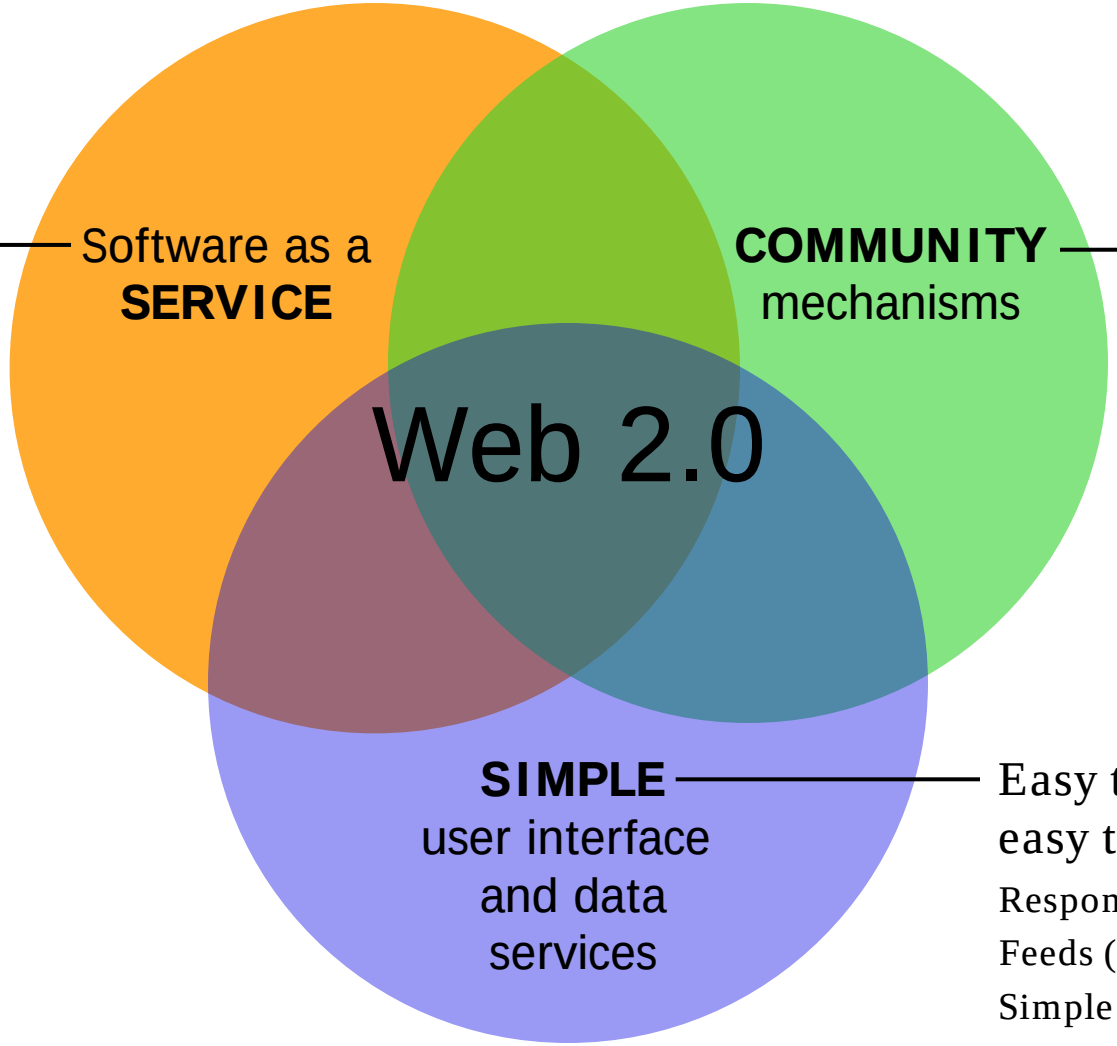
Securing Virtual Worlds

Security … It's simple, really*…



*** Not an exhaustive list**

The three patterns driving Web 2.0



Service, not software

- User-driven adoption
- Value on demand
- Low cost of entry
- Public infrastructure

Users add value

- Recommendations
- Social networking features
- Tagging
- User comments
- Community rights management

Easy to use, easy to remix

- Responsive UIs (AJAX)
- Feeds (Atom, RSS)
- Simple extensions
- Mashups (REST APIs)

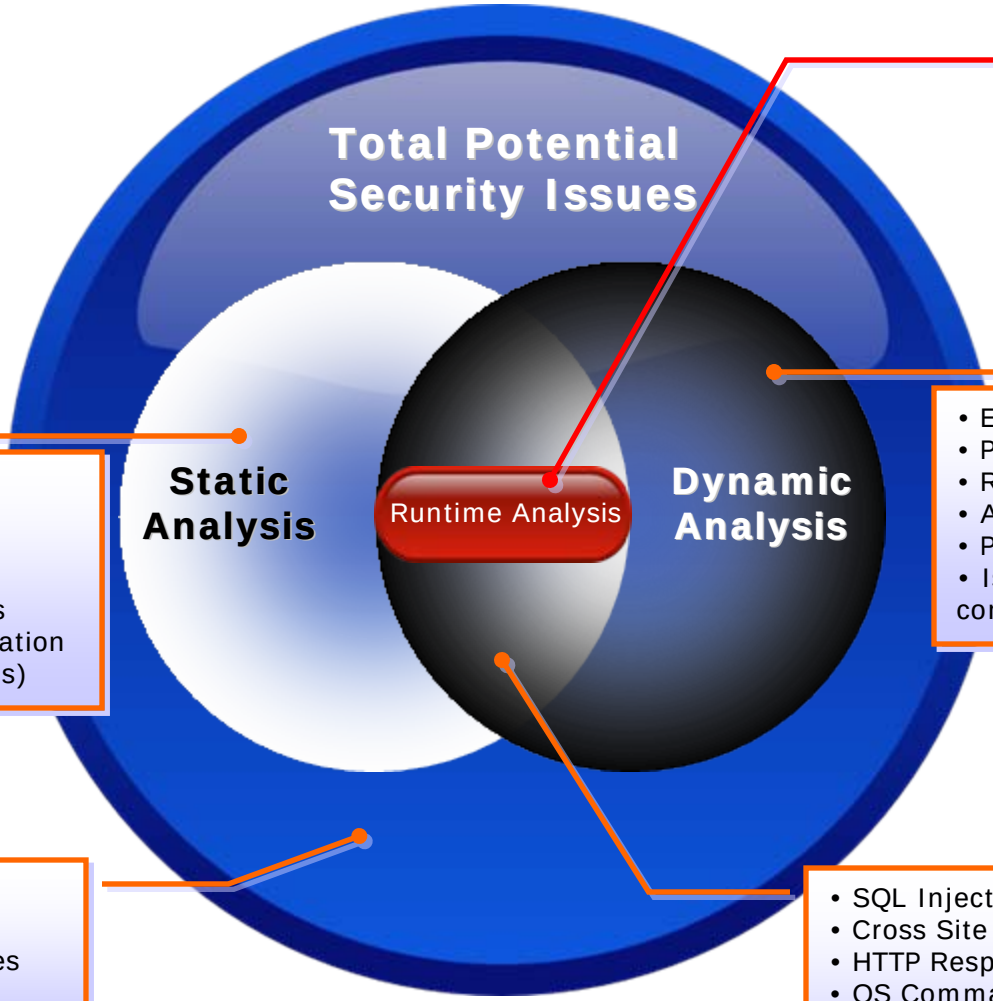
(Web 2.0 security) → (Web 1.0 Security)++

- Web 1.0 problems get amplified:
  - Everybody contributes → Input validation gets more critical

    E.g. Cross Site Scripting (e.g., Malware, Viruses)
- Mashup / AJAX related issues
  - Unrestricted DOM access within one mashup document → what about the ”Same Origin Policy“ for security?

    E.g., Cross Site Request Forging
- Client side scripts / libraries are the backbone for everything
  - Disabling JavaScript in the browser becomes unattractive
- Authenticating in a fractured / distributed web world
- Access to services in n-tier applications (e.g., SSO on steroids)
- Dynamic access controls on information shared during collaboration (e.g., IM, blog, wiki)
- Assurance of Service and Integrity in dynamic Web 2.0 topology

Security Issues Coverage



Runtime Analysis serves as the “glue” between Static & Dynamic Analysis. It helps correlate results and improve overall accuracy & actionability

- Null Pointer Dereference
- Threading Issues
- Code Quality Issues
- Issues in Dead Code
- Insecure Crypto Functions
- Issues in Back-End Application Code (Multi-Tier Applications)

- Environment Configuration Issues
- Patch Level Issues
- Runtime Privileges Issues
- Authentication Issues
- Protocol Parser/Serializer Issues
- Issues in external 3rd party components

- Application Logic Issues

- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- …

The Virtual World workload, client and server, is very different from the 2D web, and can play to our strengths

Aspect	2D Web	Web of Virtual Worlds
Model Computation	Little or no model computation required. Mostly data retrieval.	Runs a complex physics simulation: gravity, deformable objects, fluid flow, etc. Requires HPC computing. Requires "AI" for NPC actions. Computational load increases with model fidelity, a keystone differentiator.
Model Autonomy	Seldom changes; updates sent to users infrequently, and only in special cases (chat, stock tickers).	The world continuously changes, and can affect a user with no action on his part. (Who just walked into view? Pushed me?) Implies the server often autonomously updates the client.
	Little change after the user exits the system.	Model continues evolving after user leaves: true 24x7 operation.
Rendering	Text layout with static images or video streams.	Dynamically calculated shading, textures, shadows, reflection, hidden surface removal, etc. Some must also be done on server: who sees who?
User action locality	Most within the client: scrolling, data entry, AJAX.	Most actions sent to server so other inhabitants see them: looking around, moving, etc. (compare 2D "scrolling").
Parallel Scaling Paradigm	Embarrassingly parallel; little interaction between user transactions.	Continuous implicit interaction between inhabitants, since actions are observable by others and affect what they can see and do.
	Scales on loosely-coupled clusters.	Cluster scaling only by restricting areas' populations to what one server can handle.
	Large SMPs increasingly irrelevant.	Large SMPs and Sysplex-like techniques may be strongly applicable.

The size, scale and complexity of Web 2.0 environments grow exponentially in Virtual Worlds. Similarly, the vulnerabilities [V = f (T,A)] explode as new entities, objects and environments are dynamically introduced in the the Virtual World.

This is a common architectural pattern across all virtual world applications - consisting of real-time event driven, parallel simulation engines

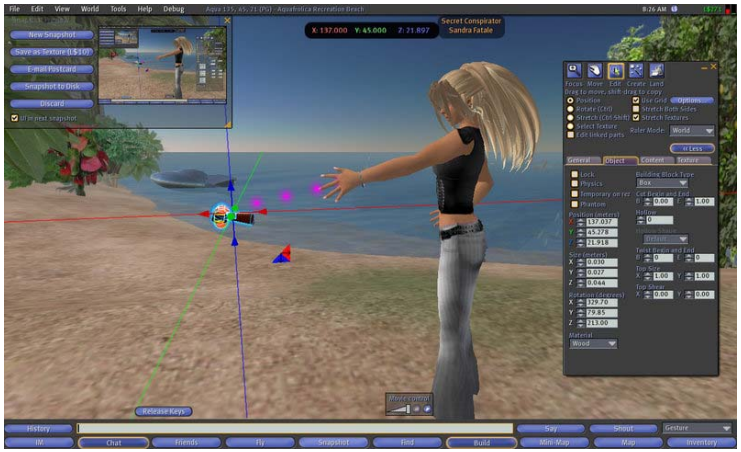
User's experience is with/through their **client simulation engine**, which models what the user is aware of...

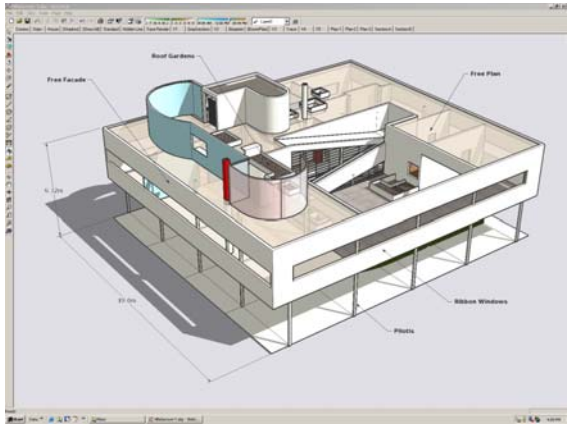
...simulation state in the client is updated by user input, simulation execution and server's authoritative rationalization of multiple changes...

...multiple **sim engines** used to manage state of **regions** of the overall virtual world as a whole. Each node manages world state of a single region.

Virtual World Security Concerns

- ID Management – same individual can be represented by multiple (and varying) avatars. Virtual biometrics are invalid. Need stronger, dynamic authentication, Biometrics? Biographics?
- Integrity of objects: environment objects, personal objects, shared objects.
- Multi-facetted phishing, viruses, worms and trojan horses made possible – and far more difficult / complex to dynamically monitor & recognize
- False sense of security (ignorance) – e.g., person, sensor, or device/object may be above/below surface, on or outside of perceived perimeter,etc. Also consider external or covert systems





- Virtual Worlds have become more and more of a hybrid, combining virtual and “real” objects (e.g., data center monitoring feeds into VW, sensors w/in private world that notify owners of visitors in realtime). Covert channels? Hacking into feeder systems & networks?
- Assurance of Service is a major challenge
- Denial of Service attacks have potentially unlimited resources
- Auditing & Logging?!?
- Non-repudiation, provenance, geneology challenged by intentional anonymity of Virtual World participation

Key Market Trends & Drivers

Threats Are Increasing in Volume & Sophistication

- Bipartisan support for more action and investment
- But lack of agreement on how it should be led

Consolidation/Centralization

- e.g., AF Cyber Command, National Cyber Security Initiative
- Questions of ownership and Admin transition slowing action

Rapidly Changing Technology

- Niche markets
- Automation of compliance
- Continued movement to “real time” situational awareness

Recommendations

Establish a converged open platform for the Web of Virtual Worlds

Strategy consists of two concurrent themes

- Theme 1: Distributed SecondLife – surround and conquer
  - Phase 1: Work with Linden to host their simulation engines in our data centers but enabling access from mainland SL to IBM hosted islands – identity federation required. IBM hosts enterprise islands.
  - Phase 2: Start open source effort. Extend SL server engine with our value add capabilities, including security/privacy/reliability/scalability but also more advanced simulation capability. IBM hosted sims are more functional and higher fidelity. Mainland SL feels more like a lowest common denominator “sand pit”.
  - Phase 3: Accelerate commoditization of their platform through open source. Start to implement standards into platform for interchange (X3D), interop (behaviour/interaction – X3D) and distributed simulation (HLA/DIS). Open client based on these standards.
- Theme 2: **Best of Breed VW platform – IBM offering**
  - Phase 1: Partner/acquire best of breed engine middleware and integrate with extended WebSphere platform to provide complete end-to-end VW solution. Aimed at “private” virtual world solutions for intranets/extranets. Very high fidelity capability and high flexibility of solution.
  - Phase 2: Implement key standards for interchange/interop (X3D) and distributed simulation (HLA/DIS)
  - Phase 3: Open source client to access this platform based on the IBM offering.
- Convergence: Integration of VWs hosted on IBM platform into SecondLife
  - Phase 1: Open client users can access SL and IBM platform VWs through one client, and traverse between them. Enable external referencing of non-SL VWs from SL.
- End Goal: Converged open platform for the Web of Virtual Worlds
  - Standards-based (interop and API standards)
  - Distributed content, distributed ownership, distributed simulation
  - Federated avatar identity and presence

Recommendations

Recognize you play two roles in Virtual Worlds: Producer and Consumer

- Theme 1: Leverage Virtual Worlds for Security Awareness, Training and Education, pragmatically use VW where effective & efficient
- Theme 2: Virtual Worlds Security Levels of Defense : **Defend against what you can, dynamically detect and recover from what you weren't able to defend against, log & audit where possible – to identify what got through and what you may be able to improve in the front end.**
- Add……