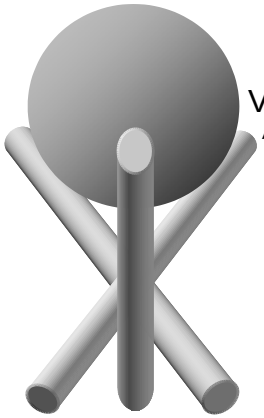


Vatic Technologies
Architecture Planning for Technology

Don's Diatribe XVI

Don Melton
Vatic Technologies Limited
meltond@acm.org

Disclaimers

- All opinions expressed in this presentation are those of the presenter and are not necessarily those of Vatic Technologies.
- All of the issues, discussions, and opinions in this presentation have been drawn from publicly available information.
- All trademarks are the respective property of the trademark owners.

Introduction

- This presentation tries to identify some of the most significant recent technology changes and elicit comments and discussion on them.
- As part of my job as a consultant I try to know a little bit about many things and a lot about a few things. This presentation represents an accumulation of the former.
- You may find some of these issues provocative, that's intentional. ☺

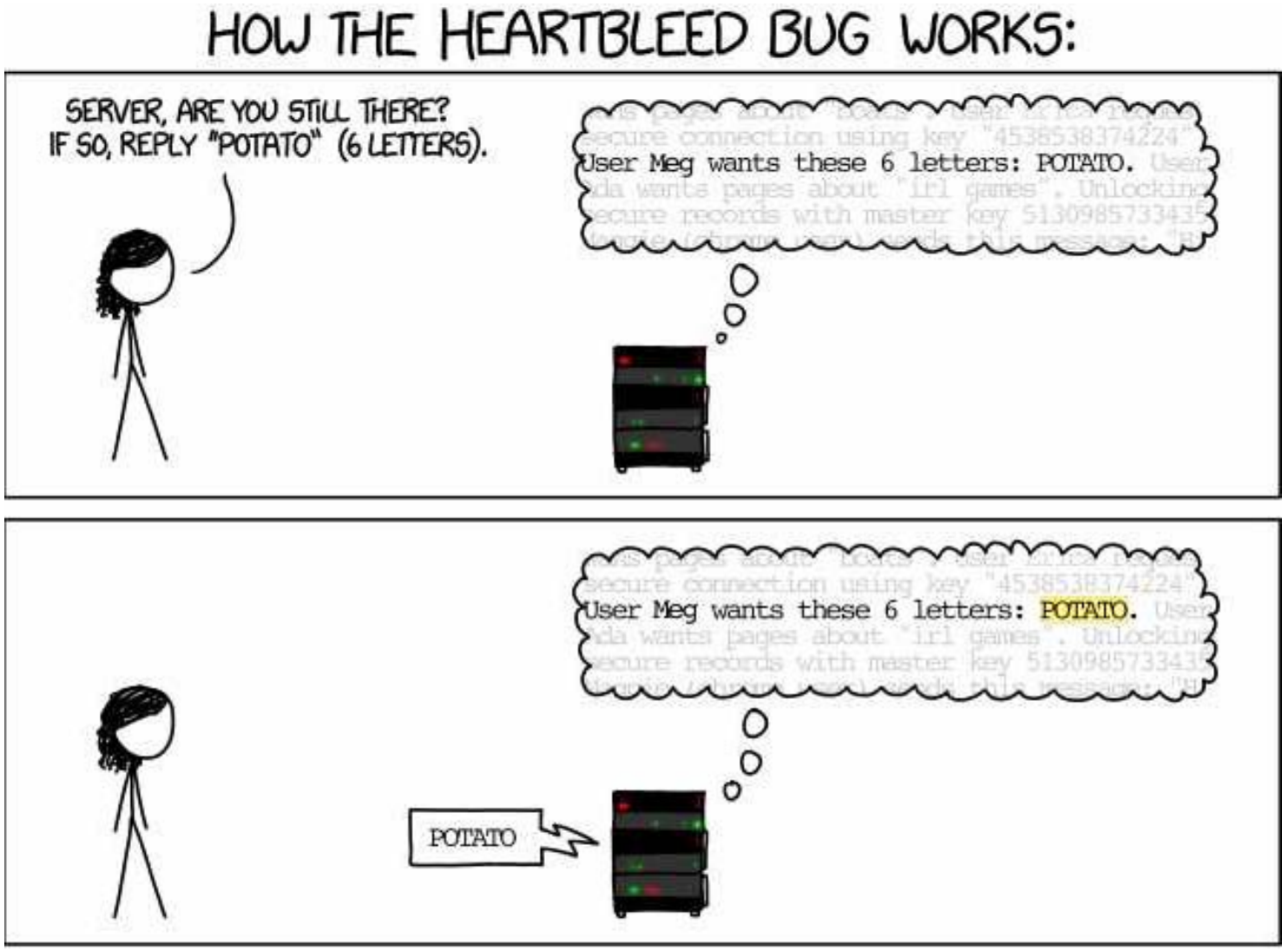
General Slide Format

- Category
  - Component
    - Issue
      - comments, and backup material
  - 😐 My “take” on the issue. (☺=omg! or ☹=wtf? or 😐=meh)
  - Your $0.02

Topics

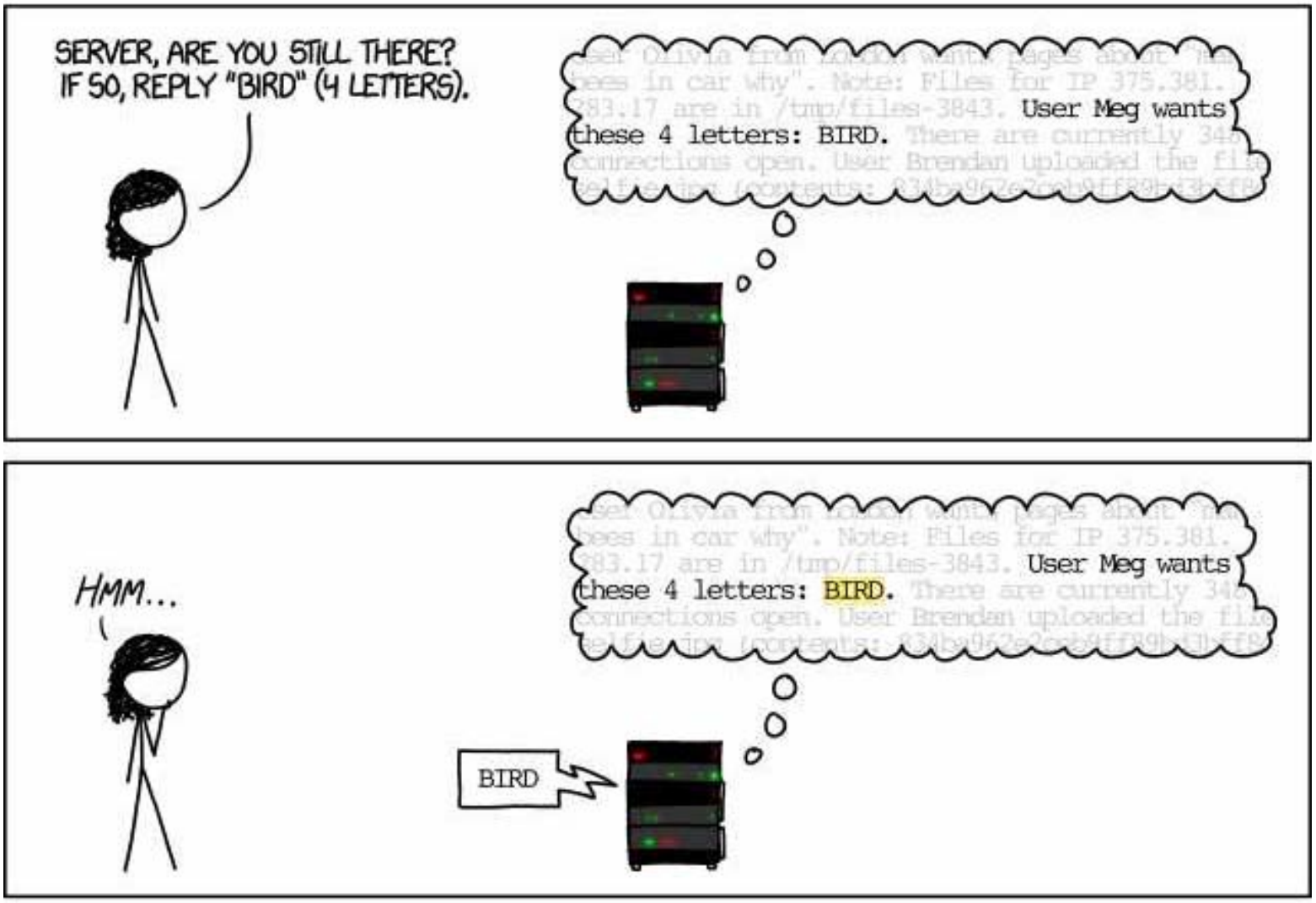
1) Security: “Heartbleed”
2) Security: Privacy
3) Security: Attack Vectors
4) Architecture: “Personal Datacentre”
5) Architecture: “Cloud Computing”
6) Architecture: “Open Source”
7) Architecture: “Big Data”
8) Architecture: HTML 5
9) Operating Systems: Windows (Windows XP)
10) Operating Systems: Windows (Windows 7/8)
11) Platforms: zSeries
12) Platforms: Internet (IPV6)
13) Platforms: Mobile vs. PC
14) Platforms: BYOD/CYOD
15) Further Discussion

Security: “Heartbleed”



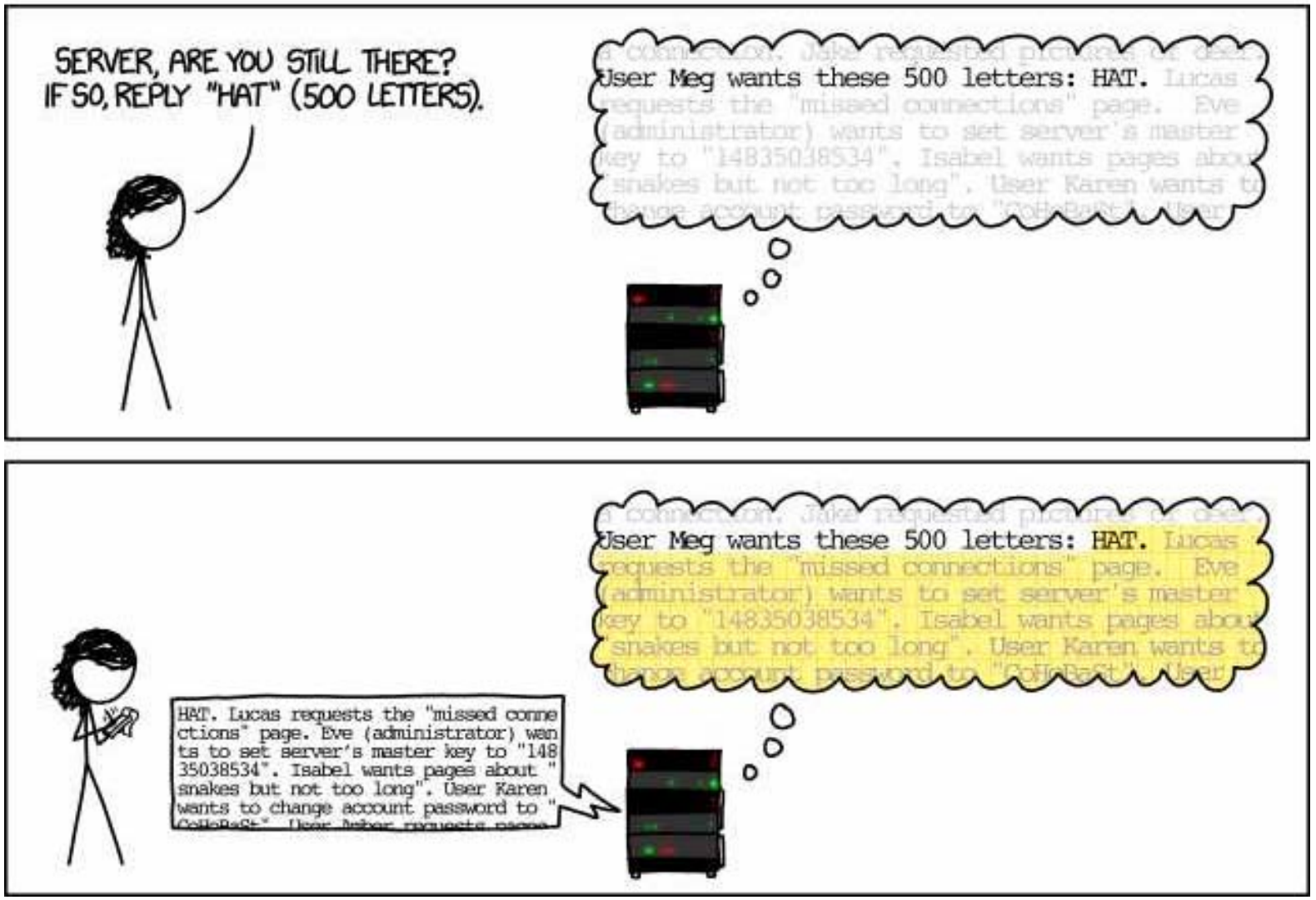
Source: http://xkcd.com/1354/

Security: “Heartbleed”



Source: http://xkcd.com/1354/

Security: “Heartbleed”



Security: “Heartbleed” 

- Heartbleed
  - What is it?
    - TLSv2 performance enhancement (keep-alive heartbeat)
    - OpenSSL v1.01 to 1.01f bug in length check (packet size ~= request size) returns buffer contents
    - No “footprints” (in negotiation phase)
  - Exposes inherent vulnerability in internet (not just OpenSSL)
    - Single point of failure (HTTPS)
    - HTTPS was a “band-aid” solution, it’s not “baked in” to internet protocols
  - More than just web sites
    - VPN, SIP, XMPP, SSH, SMTP, …
    - Embedded (router management interfaces), appliances (Cisco IP phones), client devices (e.g. VPN client)
  - More than just passwords
    - Private keys, PI data (e.g. SIN), etc.
  - Not just the “small guys”
    - Cisco, Juniper, VMWare, …
  - ☹ *Cloudflare’s challenge to extract private key from server was solved by 3 different people within 48 hours -- vulnerability has been around for 2 years.*
  - ☹ *Revenue Canada shut-down web sites (now reporting 900 SIN’s compromised)*
  - ☹ *Media telling everyone to change passwords (but **not** the right thing to do unless site is no longer vulnerable)*
  - ☹ *No way to tell if you’ve been compromised unless you have extensive logging (i.e. full packet capture during connection set-up)*
  - ☹ *All vulnerable sites need to patch and then replace CERT and revoke old CERT (some browsers don’t pay attention to CRL’s by default)*
  - ☹ *Checking long CRL’s will add latency to access*
  - ☹ *Need to assume that it’s been exploited by variou spy^H^H^H inteligence agencies for some time*
  - ☹ *Hosted sites may not be aware that they are vulnerable (ISP may not disclose versions of infrastructure software and site owners may not know how to find out)*

Security: Privacy

- Privacy
  - Social Networking Sites
    - Security settings are obscure and non-intuitive
    - Need to remember that these sites are trying to make a profit
    - Worm distribution via social networking
    - API's allow access to user profile
    - Increased aggregation of data (i.e. Facebook Mail, Facebook "Home")

☹ *Social Networking services use private information to generate revenue. "TANSTAAFL".*

☹ *Do you really want John Doe from high school demanding to be your "friend"?*

☹ *Traditional "news" channels are becoming eyeball-focused and many simply re-publishing social media feeds.*

Security: Attack Vectors

- Attack Vectors
  - What's Out:
    - E-mail Viruses
  - What's In:
    - Social Site Hacking
      - Twitter, Facebook "Applications"
    - Drive-by
      - No clicking required, Code "injection"
    - Social Engineering
      - Telephone calls to "fix" your infected computer
    - Pervasive monitoring
      - Vulnerabilities that allow unfettered access to data (e.g. Heartbleed)
    - Point Of Sale exploits
      - Poorly implemented POS systems (ineffective PCI certification)
  - ☹ *The bad guys will continue to win until the end-points [e.g. home computers] are secured [or "un-hackable"].*
  - ☹ *"Safe" computing tends to be less "exciting" [i.e., no scripts, no Flash, no HTML e-mail, …]*
  - ☹ *Proliferation of end-points: "Wetware", SmartPhone, SCADA, …*

Architecture: “Personal Datacentre”

- Personal Datacentre-in-a-box
  - Starts out as a NAS, becomes full-blown home server
    - File server (even iSCSI), Media server, LDAP, SMTP, FTP, DropBox, Torrent, Syslog, Diaspora, …
    - Multiple LAN segments (segregate Home/Guest access)
  - E.g. (Synology, QNAP, …)
  - Configuration is still a bit of a chore (Linux under the covers)

☹ *Unlikely to integrate with “Walled Garden” services (Twitter, Facebook, etc.) because it undermines their business model.*

☹ *Needs a support model for typical consumer (maybe ISP?)*

☺ *Could be the beginning of personal “Hybrid Cloud”*

☺ *Could provide balance for privacy (My Data – My Server)*

Architecture: “Cloud Computing”

- “Cloud Computing” just *Keeps On Truckin’*
  - SaaS/PaaS/IaaS/AaaS by another name
  - Ultimate outsourcing
  - Concerns regarding security, integrity, availability
    - I’ve seen an Amazon “Elastic Computing” Cloud server “probing” my web server for vulnerabilities
  - Can provide consumer mobility
    - Consistent applications across devices
  - Interoperability is an issue

☹ *All the issues with outsourcing with a much smaller “stick” on the consumer side.*

☹ *Single point of “access” for all data raises security/privacy concerns.*

☺ *In-sourced “cloud” may be the driver of infrastructure architecture.*

Architecture: “Open Source”

- Open Source is in the news due to Heartbleed
  - OpenSSL
    - Calls for mandatory checks on Open Source code but …
    - Not all instantiations of OpenSSL have the same risk
    - E.g. internal management-zone security not equivalent to shopping cart check-out
  - Open Source provides *Control*
    - Not necessarily more secure, can be secured through code review by end-user
    - Not necessarily free, but cost of management can be associated with business risk
  - Source is source
    - Need to treat Open Source projects the same as in-house coded applications
    - Assess risks to business and apply appropriate QA, change management, risk management to the programs

😐 *Can’t expect the authors of open source code to be perfect. They’re generally volunteers and have day jobs as well.*

☹ *Disappointing that “big” vendors (i.e., Cisco, Juniper) apparently eschewed internal controls that might have found the bug before embedding in their systems.*

☹ *Worriesome calls for getting rid of Open Source projects that are related to “risky” systems.*

Architecture: “Big Data”

- Big Data is the “New Black”
  - Should be familiar to Capacity Planning people
    - Massive amounts of information (logs, SMF, performance monitors)
    - Search for correlations and then determine Cause & Effect
  - Data Analytics tools
    - Tools being provided to business may be re-purposed to do capacity planning?
  - Planning for “Big Data”
    - Experience with managing CP data stores can be leveraged against business data

☹ *Capacity planners always seem to be “The Shoemakers’ Children”*

Architecture: HTML 5

- HTML 5
  - Latest version from W3C
    - http://www.w3.org/html/wg/drafts/html/CR/
    - Includes DRM support
    - Still in draft status
  - Not all browsers support it yet

☹ *Some web-sites are HTML5-only (problem if your browser doesn't support it)*

☹ *DRM support will make it possible to "hide" source from the browser user. A compliant browser won't show you everything that is going to be run on your computer in View-Source.*

Operating Systems: Windows (Windows XP)

- Windows
  - Windows XP is now end of support
    - Some users still migrating to Windows 7
      - Large government sites
      - Specialized driver requirements (e.g. CNC machines)
    - Workarounds
      - Run XP in VM disconnected from internet

☹ *Expensive migration if not synched with H/W lifecycle*

☹ *Vatic Technologies' upgrade still in work (critical XP-only applications)*

☹ *Lack of backward compatibility (I'm spoiled by IBM S/360 ☺)*

Operating Systems: Windows (Windows 7/8)

- Windows
  - Windows 7
    - Virtual XP mode
    - Cannot join a non-AD domain
    - XP now out of support
  - 😐 *My clients are gradually moving to Windows 7*
  - 😐 *Don't know if it'll work with a Samba "domain controller"*
  - ☹ *Vatic Technologies' upgrade still in work (critical XP-only applications)*

  - Windows 8
    - Not for business?
    - Windows 8.1 is out
    - Un-enthusiastic response from many users
  - ☹ *No personal experience yet*
  - ☹ *Do not bypass windows 7 unless you are focused on consuming information.*
  - ☹ *May security patches not available unless on 8.1 but Win8.1 has install issues.*

Platforms: zSeries

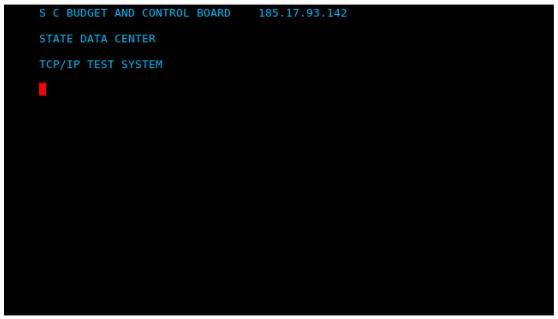
- "z" systems on the Internet
  - Growing interest in finding/analyzing on-line systems
    - Soldier of Fortran http://mainframed767.tumblr.com/
    - A lot of universities, but also government, business

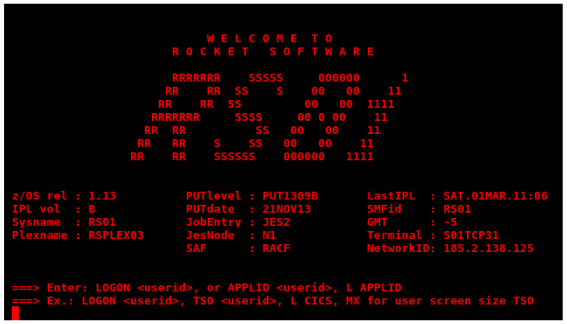
☺ *Good to see someone recognizes "mainframe" as a current platform*

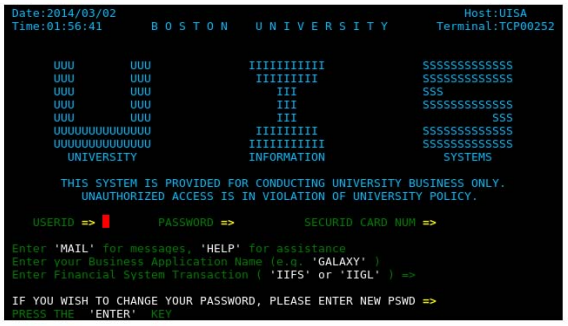
☹ *It's not clear that the system owners have considered security*

☹ *Shouldn't these things (at least some of them) be behind a VPN*

☹ *Don't know what Audit or a "Pen test" would find.*







Platforms: Internet (IPV6)

- Internet
  - IPV6
    - IANA IPV4 addresses have all been assigned, ARIN will run out in April 2015. (see: http://www.potaroo.net/tools/ipv4/index.html)
    - *Is* being rolled out within carriers
    - Every device gets a “static” IP?
    - Every device is routable at the internet level?
    - No NAT standard (a few IEEE drafts)

☹ *No simple, low-cost, sub-netting*

☺ *Static IP which makes running local services easier? (home web server)*

☹ *Static IP makes privacy harder? (everyone knows who you are)*

☺ *Static IP make authentication possible? (similar to caller-ID)*

☹ *Changing ISP may require re-numbering your network (no NAT)*

☹ *Consumer-grade Gateway/Routers not widely available*

Platforms: Mobile vs. PC

- Mobile (Phone/Tablet)
  - Apple, RIM, Google, all have products
    - Internet “consumption” device
    - Priced FTW ($0.00 with a plan)
    - Walled Garden (end of “generative internet” – Communications of the ACM)
    - Security (no Firewall, un-encrypted local storage, …)
  - ☺ *Synergy of VOIP, embedded 802.11, and WiFi hotspots may ease bandwidth issues.*
  - ☺ *“Locked down” nature of mobile may help overall security (but bad code still seems to make it in)*

- PC (Mac/Windows/Linux)
  - PC sales declining
    - Expected? since majority of users are consumers
    - Windows 8 doesn’t help but it’s not the root cause
  - ☹ *PC prices will rise due to loss of scale*

Platforms: BYOD/CYOD

- Bring/Choose Your Own Device
  - Employees use consumer-grade devices for the business
    - Improved employee contentment/productivity
    - Justify 7x24 employee availability
  - Challenges
    - How to split business/personal usage charges?
    - Separation of personal/business applications & data
    - Proliferation of device types to be managed
    - Proliferation of vendor purchasing agreements

☺ *BYOD eliminates cost of providing employee device*

☹ *BYOD employees may become disenchanted with 7x24 availability expectations when they are paying the bill.*

☹ *Conflicts around personal/business use are likely to drive separation of devices again.*

☹ *IT and purchasing will have to "staff-up" to support additional devices and this may offset cost savings.*

Wrap-up

Notes