Web 2.0 – Securing the Brave New World

May 23, 2007

Agenda

- Web 2.0 – What Is It?
- Security Implications, and an Example
- Some Emerging Use of Technology
- What’s Needed
- Web 2.0 – Non-Technical Issues
- A Modest Proposal

Web 2.0 – What Is It?

- No precise definition, but not market-ecture, either
- Web 1.0 - Largely Static
    - Fixed content (web pages)
    - Non-mutable applications
    - Constrained communications (by protocol by device)
    - Generally detached, layered defenses
- Web 2.0 – Dynamic, “Web Improv”
    - Collaborative (blogs, wikis)
    - “Mashups,” including applications (SOA)
    - Constraint-less comms - “All my data, all the time, on all devices”
    - Defenses, TBD

Security Implications

- Deperimeterization to the nth degree
  - No “data fortresses”; more like “flexible data camps/tentlets”
  - More to defend (devices, entry/exit points)
- “Need to share” trumps “need to know”
- Assumption that physical security “does not apply” – even though that is sometimes the best defense
- Embrace of asymmetric risk
  - Because risk is not understood – benefit is
  - Competitive, cost factors
- *Effective democratization of security without commensurate increase in skills, training or tools for defense*
- Overall complexity means no clear picture of “security posture”
  - Whether that is network, apps, “data risk”…

Example: “The Network is the Battlefield”

- US DoD’s Global Information Grid (GIG) vision: combine physically separate networks to increase timeliness of information to the war fighter
  - …thus eliminating several natural defensive boundaries
  - …and forcing defense of the entire network
  - …leading to Ishandlwana, not Rorke’s Drift?
- Flexible, dynamic associations for “controlled collaboration”
- Desire for benefit means embracing asymmetric risk, because benefits seem clear … but risks aren’t
- As warfighting relies upon an IT backbone, the network itself becomes the battlefield
  - Superior force-of-conventional-arms – hard to get
  - Superiority of cyber-arms – potentially easier
  - Attacker’s Goal: disrupt defender’s ability to wage war and prevent the use of information technology

…Which May Favor Adversaries

- Technology is a force multiplier, but over reliance upon it can be an Achilles' backbone
  - "Security happens"
- Little to no situational awareness on the network – and getting worse
  - Who is on the network?
  - Friend or foe?
  - What is on the network?
  - What is my "mission readiness"?
  - What's over the hill?

"He who defends everything defends nothing." – Frederick II

Some Emerging Use of Technology *Rights Management*

- More adoption of IRM in targeted instances
  - Highly proprietary material of high value
- A compelling case for larger IRM use within the enterprise
  - Data subject to privacy/security/compliance directives
  - Includes email, IM, doc, presentations…
  - Control data beyond the firewall
  - Rights to change, read, forward, print are all different
  - Logging of usage
  - Identify and potentially “scrub” hidden data (hidden slides, tracked changes, author history, user or network identity data)

Some Emerging Use of Technology *Intelligent Search*

- “Web search” != enterprise search
- Security needs are different
  - Preventative/compliance/need to know vs. strictly ‘what’s out there’
- Less gaming the system (no keyword purchase)
- Flexibility in security model enables “appropriate search”
  - “Compliant-search”
  - Potential use for enterprise data redaction

Some Emerging Use of Technology *Network Access Control*

- *Flexible* “friend or foe” challenge before connecting to the network
- “Network inoculation” effect
- Can include inbound and outbound policy enforcement
- And proactive defense

What’s Needed: Innate Defensibility of Software (1)

- “Every Marine fights…”
  - *Products must self defend, every one of them*
  - “Armed guards” will not work any better than bastion defenses, particularly as apps become collaborative
  - N devices should not require n defenders
  - Requires mentality shift in development to disallow *every* possible future use
- “Dynamic redoubts”
- Secure ecosystem
  - “Public good” functionality, and standards

What’s Needed: Innate Defensibility of Software (2)

- Network situational awareness – real time
  - Who’s on my network?
  - What is on my network?
  - What is my “mission readiness” (performance, bandwidth, security posture)
  - What is happening that I should be worried about?
- Software assurance as the *norm*
  - Best practice around process, training, tool usage as expected behavior, for *all size companies*
  - Mindshift to safe/secure/reliable not just “cool technology”
  - Overhaul the CS educational system to include security in every class: a discipline, not a “trade”
  - Third party validation in various flavors

What’s Needed: Innate Defensibility of Data

- Search (and-destroy) engines?
  - What data is where on my networks?
  - Options include report/retrieve/erase/destroy?
  - The corollary to information lifecycle management/data retention is what you should *not* have/use/keep
  - Can help with security/privacy housekeeping as well as data retention policy
- More flexible access models?
  - Self sealing/time-to-live data
  - Narrow risk/attack vector through more contextual access (time of day/pattern of use/who do I think you are/what device are you using)

Web 2.0 - Non-Technical Issues

- *"Pre-parsed Knowledge" or "Pre-packaged Ignorance"?*
  - Does "community" continue to have meaning when people self-select into communities of one?
  - Do we need MSM's "common, vetted reading material" for community discussion?
    - Or have communities thrived because of new information outlets?
  - MSM has *some* standards of conduct and means for error correction – should bloggers?
    - Or have "blews outlets" forced more accuracy on MSM?
  - In Web 2.0, will information and applications be "self-correcting" if proven to be wrong?
  - Can non-experts realistically be their own data redactors?
    - Where to draw the line (can elementary school kids "mashup" curricula?)
    - Do self-reinforcing prejudices magnify in web-ified world due to "crowding out effect"?

Web 2.0 - Non-Technical Issues

- *“Wisdom of the Crowds” or “Mob Mentality”?*
  - In theory, many eyes review material – but are they always *critical* eyes?
    - Or have many redactors/reviewers enabled expertise nobody could afford before?
  - Does the collaborative advantage go to propagandists and attackers rather than truth-seekers/truth-tellers?
    - Urban legends spread proactively, but corrections do not (there’s no ULD-ML)
    - “On the Internet, nobody knows you are a (lowdown, dirty) dog”
    - Remember The Big Lie; imagine Big Lie enabled by Web 2.0

Web 2.0 - Non-Technical Issues

- *“Mistakes Writ Large” or “Your Moment in the Sun”?*
  - Everyone can have 15 minutes of fame – or 15 minutes of opprobrium
  - Public as paparazzi: no more private sins
    - You-all on YouTube
    - No more “file and forget”
  - Reputational smear is already a problem
    - For 15 minutes of fame or 15,000 links, “nice” does not sell – anger and vitriol does
    - Where are cybergrandmas when you need them?
  - Have we become a community of showoffs?
    - Or does “exposure” also give confidence to new talent?

A Modest Proposal

The cyberworld is a digital community, a community enabling links and relationships that might not develop at all, or not develop as richly, or that would otherwise wither through inactivity.
In the physical world, they nonetheless represent real people.
While Web 2.0 does enable each of us to be a market of one, it takes more than 1 to become a community.

We can start by each becoming a citizen of 1, by adopting at the very least, a cyberversion of the Golden Rule: Do unto others, as you would have them do unto you. *It has served us well for over two millenia, and technology has not improved upon it.*

Q&A

ORACLE IS THE INFORMATION COMPANY