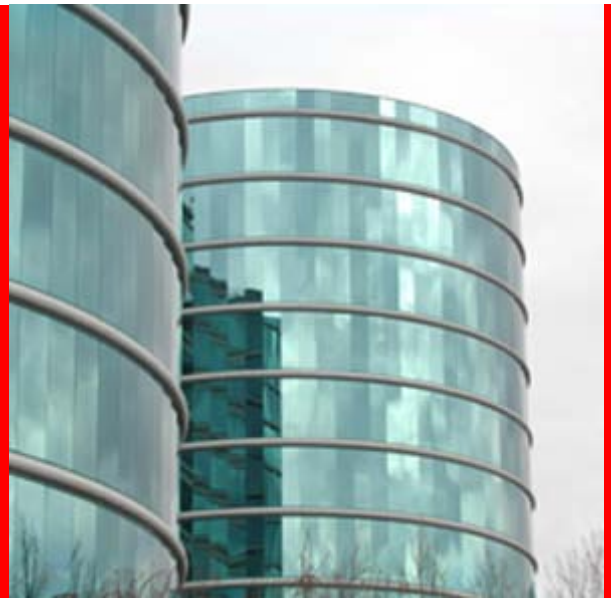

ORACLE

War Made New: Changing the IT Battlefield

Mary Ann Davidson
Chief Security Officer

syn·the·sis

1 : the combination of parts or elements so as to form a whole; *especially* : the production of a substance by union of chemically simpler substances
2 a : the combining of often very different ideas into an ordered whole b : the product so formed

(Merriam-Webster)

Why Court Synthesis?

- “There is nothing new under the sun” (Ecclesiastes)
- Synthesizing ideas, canons, patterns from other disciplines helps you look at old problems in a new way…and find old solutions to new problems
- Or start a revolution (e.g., OODA loop)

What Happens If We Don't?

- Stagnation, as academia and business is increasingly about specialization and not generalization…
- Loss of perspective and "commonality" from specialization
- "An expert is someone who knows more and more about less and less until (s)he knows everything about nothing"
- Narrowness of focus can lead to narrowness of vision

Eh, We Talk Story…

- Many aspects of art, music, history and other disciplines include synthesis and “borrowed” ideas
  - Music: Jazz, Hawaiian music
  - Language: words, alphabet, idea of writing itself…
  - Economics: relationship between risk/return, Black-Scholes model…
  - Art: Impressionism…
  - History: Western civilization…
  - Military history/strategy: force multiplier, energy maneuverability theory (OODA), defense in depth, Trojan horse
  - Nuclear strategy, biology: game theory

State of Information Security: A Tipping Point?

- The cost of poor security in the US alone is between $22.2B and $59.5 *billion* per year (US NIST)
- The security-worthiness of commercial software is a CEO level issue (Business Roundtable)
- Increasing (effective) regulation of IT – with all its unintended consequences
- **Increasing dependence of critical infrastructure on commercial off-the-shelf software that was in many cases not designed for the threat environment**
  - **Including US DoD…**
    - ***… including warfighter systems***

The Network is the Battlefield (1)

- *Network centric warfare* seeks to translate an information advantage, enabled in part by information technology into a competitive advantage through the robust networking of well-informed geographically dispersed forces
- Major tenets of network centric warfare:
  - A robustly networked force improves information sharing;
  - Information sharing enhances the quality of information and shared situational awareness
  - Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command; and
  - These, in turn, dramatically increase mission effectiveness

(Source: Wikipedia)

The Network is the Battlefield (2)

- 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 Isandhlwana, not Rorke's Drift?
- Desire for benefit means embracing asymmetric risk, because benefits seem clear … but risks aren't
- As warfighting increasingly 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 or other technology

…Which May Favor Adversaries

- Technology is a force multiplier, but can over reliance become an Achilles' backbone?
  - "Security happens"
  - …technology no longer a force multiplier if "enemies" can steal the technology
- Little to no situational awareness on the network
  - 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

Where Does Assurance Fit?

- Improving software assurance alone will not secure the GIG (or anything else)
- But
  - It will improve signal to noise in the network currently degraded from easy exploits
  - It will make attackers work harder
  - The resources and $$$ currently spent on constantly patching networks can be redeployed elsewhere
- Improved assurance (for defense) has knock-on benefits to many sectors of critical infrastructure

The poor security-worthiness of commercial software is a national security issue, and needs to be treated as such.

ORACLE

Assertions

- Lack of software assurance is a fundamental cultural problem manifested as a technical weakness
  - You can't win a war if you don't think you are in one
  - You don't win wars with technology *alone*
  - You don't cure patients with band aids, but with vaccines and (sometimes) major surgery…and not all patients will survive
- Governments are a much stronger catalyst for change than they think they are
  - Collective wave energy of the North Shore of O'ahu can light a city
  - Collective buying power of governments changes the market dynamic

What Needs to Change

- Education
- Accountability
- How Government Buys Software
- Innate Defensibility of Software
- Self-awareness of the Network
- Innate Defensibility of Data

Governments can and *must* be a catalyst for change

Education (1)

- Cultural shift must start in universities
- The Epaminondasic Oath: “First, assume an enemy…”
  - Could improve both code quality and malware issues
  - Goal: every developer thinks like a hacker
- Software vendors spend $$$ training CS grads in *basic* secure coding
  - And millions more remediating avoidable, preventable defects resulting in large part from lack of basic security education

Education (2)

- The CS – and other related - curricula need to change to have security embedded within each class
  - *Every* course builds on a secure coding foundation
  - Red team/blue teaming part of *each* class
- Accreditation programs need to force this change
- Governments should withhold research monies from universities that refuse to modify their curricula

Accountability

- What if software developers had to be licensed, like licensed professional engineers (PEs)?
  - Changing lightbulbs, adding a dimmer switch and designing the power grid need *different* levels of electrical engineering expertise
  - Increased, *meaningful* accountability for IT professionals is the ultimate process improvement

How Government Buys Software (1)

- Require transparency in development practices, improving ability to do risk-based acquisition
- Require proof of assurance (e.g., Common Criteria evals, automated security testing done during development)
- Require vendors to do more in an automated way, lowering lifecycle cost-to-secure
  - Secure configuration by default
  - Minimal installations (don't install what I didn't license and don't use)
  - Patch automation, etc.
  - General uplifting works; multiple flavor variants won't

How Government Buys Software (2)

- Use RFPs to suss out what vendors did and did not do to build assurance into product development
  - "Market signaling"
- "Procurement effect" can be magnified if large government customer base acts as one
- Benefits of Big Buyer approach will accrue to multiple customers, raising the bar across many sectors

Changing the Battlefield:
Innate Defensibility of Software

- The US Marine Corps is a lethal fighting force
  - But does not assume “no casualties and an unbreachable perimeter”
  - And Marines understand what is strategic to defend (e.g., Henderson Field)
- “Every Marine a rifleman…”
  - 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
  - Mentality shift in development to disallowing every other possible future use instead of allowing all possible future uses

Changing the Battlefield:
Self-Awareness of the Network (1)

- Lack of situational awareness is caused by lack of basic information
  - 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?
- Causes
  - No standards for what data is collected
  - No standards for format (though some contenders)
  - SIEM vendors can't correlate non-existing data
  - Value add is the BI component, not "translation services"

Changing the Battlefield:

Self-Awareness of the Network (2)

- Government could enforce such standards as a public good
  - Example: Transcontinental Railroad
  - Or find other ways (procurement, “certifications”) to force the market to provide situational awareness (e.g., SCAP)
- Could enable “dynamic redoubts”
  - Reconfiguring networks and products that go to “DEFCON-n” when under attack

Changing the Battlefield:
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)

Changing the Battlefield:
E-M Theory Applied to Networks

- Fighter pilots “win” based on agility (Boyd’s energy-maneuverability (E-M) theory)
- OODA (observe, orient, detect, act)
  - OODA was an air warfare concept that changed the face of war (notably in Gulf War I)
  - And has been applied to other disciplines
  - Is there applicability to cyber-offense and defense?
    - If targets are not static but evolving, it might

Summary

- Sid Sibi Pacem Para Bellum
- Those who design and build critical information systems need a warrior mindset reinforced by warrior training – and “war games”
- Systems need to be designed to be defensible – instead of assuming a peaceful world
- The art of war has much to teach us about defending the network battlefield

Remember

- At Dawn We Slept…

"A nation, as a society, forms a moral person, and every member of it is personally responsible for his society.“

-Thomas Jefferson
(in letter to George Hammond, 1792)

Resources

- *War Made New* by Max Boot
- *Carnage and Culture* by Victor Davis Hanson
- *Boyd: The Fighter Pilot Who Changed the Art of War* by Robert Coram
- *Strong Men Armed* and *Helmet for My Pillow* by Robert Leckie
- *Last Stand of the Tin Can Sailors* by James Hornfischer
- *The Soul of Battle* by Victor Davis Hanson
- *Intelligence in War* by John Keegan

ORACLE IS THE INFORMATION COMPANY