Fusion CEO- CIO Symposium

Security – Getting Your Money's Worth

Peyton Engel, Technical Architect

March 5, 2009

Agenda

- The need to think creatively and clearly
- Security as a part of business strategy
- Get out of the rut we're in

- Our Mission
  - Facilitate better **decision-making** about risk
  - Make security the basis of our customers' success

Safety vs. Fuel, Performance

- Abraham Wald (statistician): studies the problem of adding adding armor to planes
- Observe bullet holes on planes returning to base
- Non-uniform distribution; seems obvious
- Taking data at face value can be risky

Must Patch Critical Vulnerabilities

- What percentage of announced/patched remote root exploits are actually used in attacks?
- Of those, how many are best defended by patching (as opposed to config, firewall, etc.)?
- The “Nirvana fallacy” we want perfection, but imperfection ≠ failure
- A cheaper patching strategy would be based on risk (probability & severity), not just severity.
- Safety is asymptotic: should we not be looking for the point of diminishing returns for patching?

What are the Ingredients?

- A problem of some sort must exist
- The problem must involve a change of security state
- It must be possible to trigger the problem

…it doesn't really get interesting until…

Someone finds out about the vulnerability
Someone figures out how to exploit the vulnerability
Someone has the ability to use the exploit on us

How to be Vulnerability-Free

- Plan 1: Find out about and fix all flaws in all products
  - Not likely; vendors keep releasing patches, indicating that they don't know them all…
  - "Apollo 8 has 5,600,000 parts and one half million systems, subsystems, and assemblies. Even if all functioned with 99.9% reliability, we could still expect 5,600 defects."
    - Jerry Lederer, NASA safety chief (quoted in Collins, Michael. *Carrying the Fire: An Astronaut's Journeys*, New York: Random House, 1974, p. 307)
- Plan 2: Prevent all flaws from being exploitable by anybody
  - Also problematic; generally this would involve denying all access…
  - "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."
    - Gene Spafford (quoted in Dewdney, A. K., "Computer Recreations: Of Worms, Viruses and Core War," *Scientific American*, March 1989, p. 110)

"Window of Vulnerability"

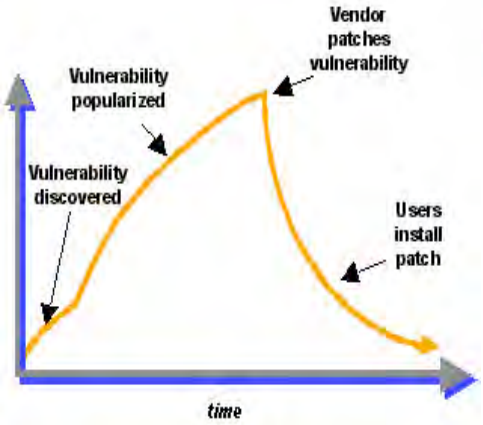
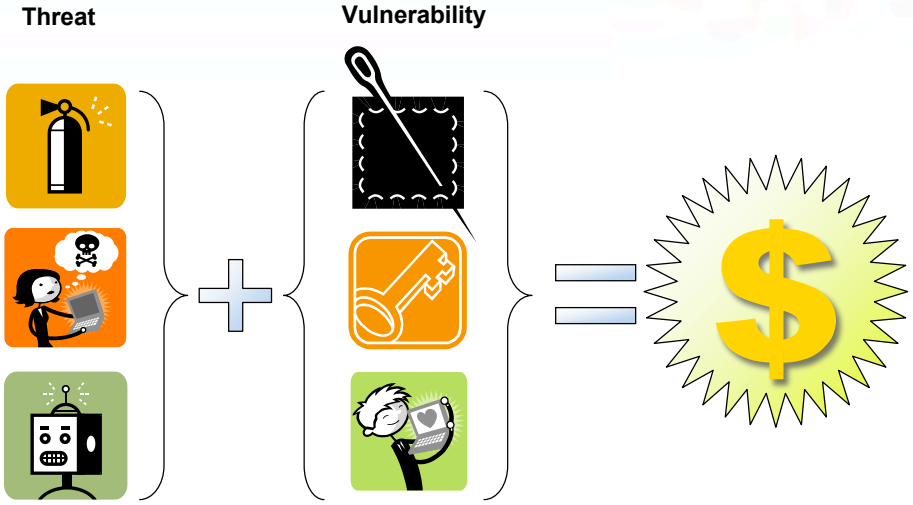


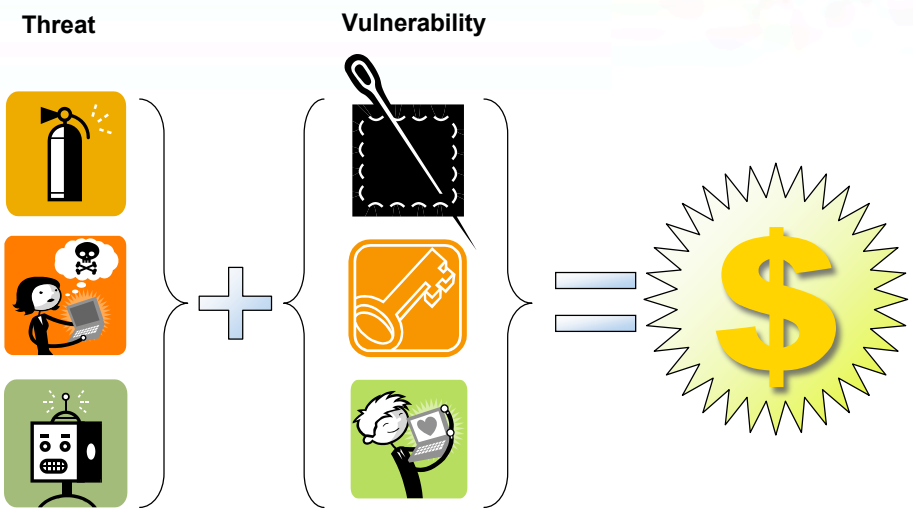
Figure 1
(graphic from counterpane.com)

- Introduced to describe worm/patch cycle
- Note that it is never really 0 (i.e., there are always some vulnerabilities we don't even know about)
- This is the 0-day problem, and we are not likely to solve it any time soon
- We'd better accept that we have some exposure, then…

Ingredients in an Incident



Interdiction/Defense Options



Hey, wait a second…

- It's really *incidents* that cause us losses, not just *vulnerabilities.*
- Vulnerabilities are addressable, but it's unrealistic to think we can discover *all* vulnerabilities, let alone cure them.

…so we are left with a question…

- *HOW SERIOUS IS ANY GIVEN VULNERABILITY, REALLY?*

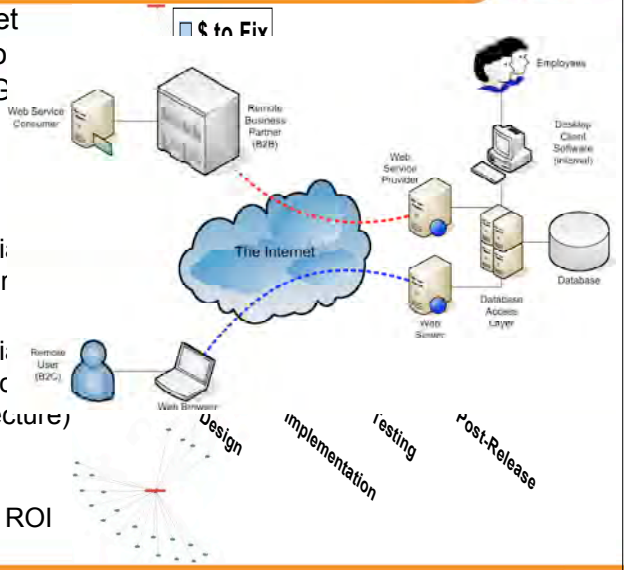
In

Blank Administrative Password
Administrator Account w/ Weak Password
Missing Critical Patch
Blank SQL “sa” Password
Weak Domain Admin Password
Additional Implied Trust Relationships:
•UNIX Environment
•Wireless
•Infrastructure

Bad practices or poor choices in one part of the organization can put other pieces at risk.

Security and the Budget Cycle

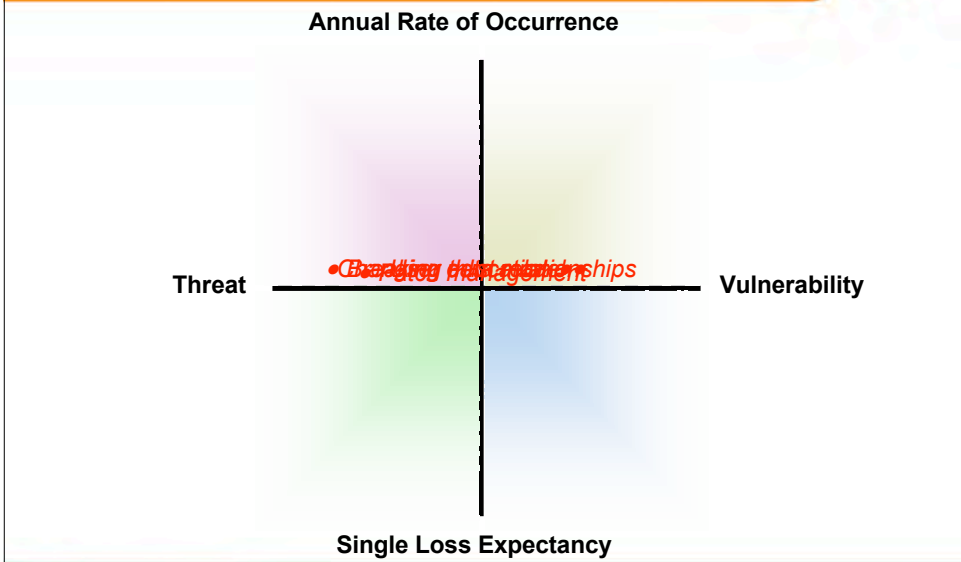
- Challenge: shift budget towards the creation o new capabilities (CMG
- Risk has some cost
- Three strategies for reducing it:
  - Reduce costs associ with tactics (i.e., impr implementation)
  - Reduce costs associ with redundant servic (i.e., improve architecture)
  - Structure security spending to be cost-neutral or producing ROI



How Would Rational Security Guidance Look?

- Explain what type of incident it counters
- Explain what source of risk it addresses:
  - Threat
  - Vulnerability
- Explain what amplifier of risk it reduces:
  - Frequency
  - Severity
- Explain to the right people:
  - What will get better? How much will it improve?
  - How much will it cost? What are the side-effects?
- Make the reasoning transparent

What Does A Security Measure Do?



Our Goal

- A better decision-making process
  - Transparency
  - Rationality
  - Context-sensitivity
- Effective investment
  - Avoiding irrational spending
  - Getting business value for the money
  - Using security to drive the business forward

Thanks!