Argonne NATIONAL LABORATORY

... for a brighter future

U.S. Department of Energy

UChicago ▶ Argonne LLC

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC

Invited Keynote Address
Secureworld Expo, Atlanta, April 29-30, 2008
and Chicago, May 21-22, 2008

Smirking & Vulnerability Assessments

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

Argonne Vulnerability Assessment Team

Physical Security

- consulting
- cargo security
- tamper detection
- training & curricula
- nuclear safeguards
- new tags, seals, & traps
- vulnerability assessments
- novel security approaches
- security psychological issues

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

The greatest of faults, I should say,
is to be conscious of none.
-- Thomas Carlyle (1795-1881)

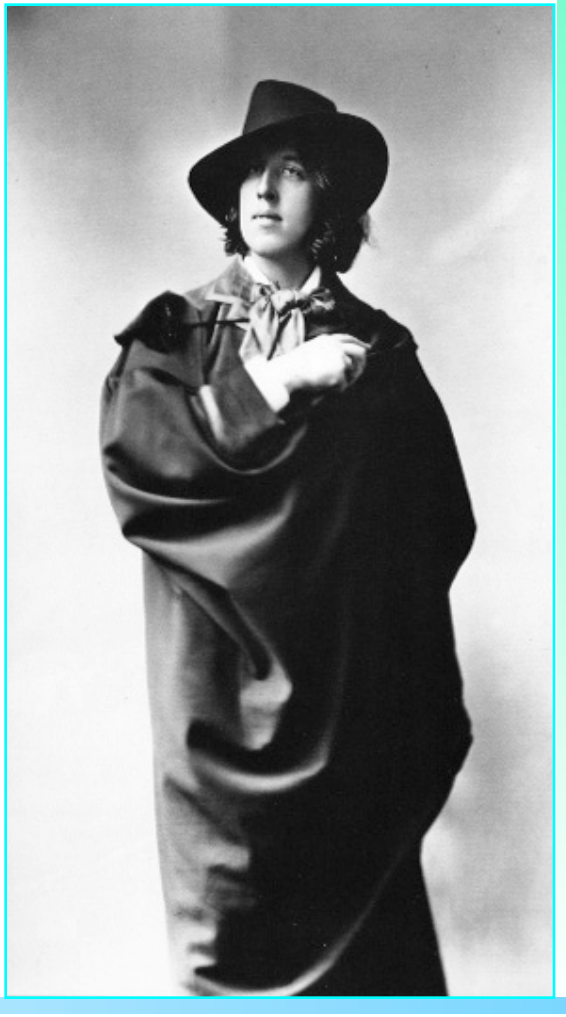
Wilde’s Smirking Statue in Dublin’s Merrion Square

Oscar Fingal O'Flahertie Wills Wilde

1854-1900 (died at age 46)

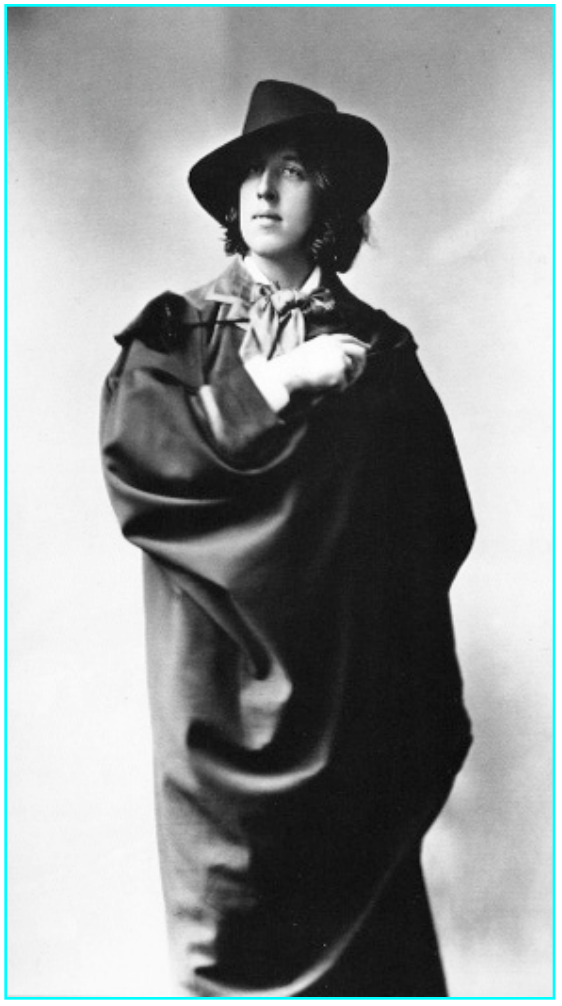
Wilde lectured in Chicago
February 10-15, 1882.

Chicago Central Music Hall (1879-1901)
SE Corner, State & Randolph



Wilde lectured on “The Decorative Arts” in Atlanta, July 4, 1882.

DeGive’s Opera House
(burned down in 1978)
157 Peachtree Street

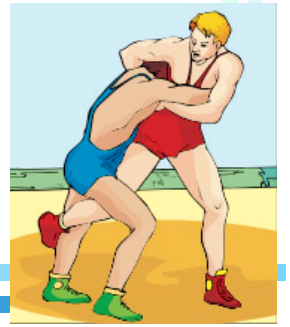


Vulnerability Assessment (VA)

Vulnerability Assessment: Discovering & demonstrating ways to defeat a security device, system, or program. Should include suggesting counter-measures and security improvements.

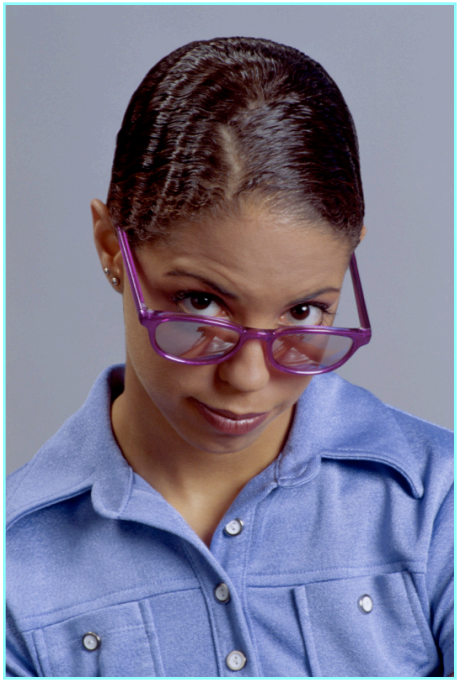
Adversarial Vulnerability Assessment: Really thinking like the bad guys, wanting to find security flaws, and not letting these things define the problem: the good guys, existing security, past security incidents, or a superficial understanding of the assets to be protected.

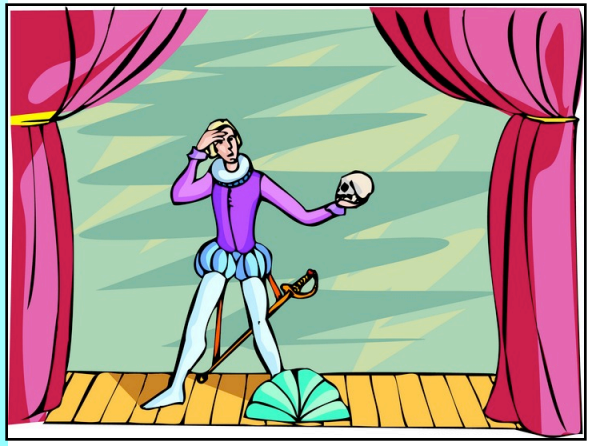
He that wrestles with us strengthens our skill. Our antagonist is our helper.
-- Edmund Burke (1729-1797)



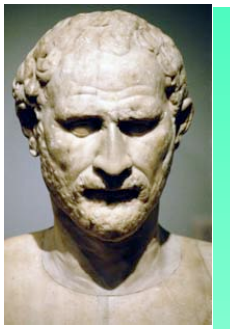
Good AVAs Require

1. skepticism (or cynicism)
2. creativity/imagination
3. confidence (or swagger)
4. role playing (or method acting)





Skepticism



There are all kinds of devices invented for the protection and preservation of countries: defensive barriers, forts, trenches, and the like... But prudent minds have as a natural gift one safeguard which is the common possession of all, and this applies especially to the dealings of democracies. What is this safeguard? Skepticism. This you must preserve. This you must retain. If you can keep this, you need fear no harm.

-- Demosthenes (384-322 BC)

The Importance of Being Earnest

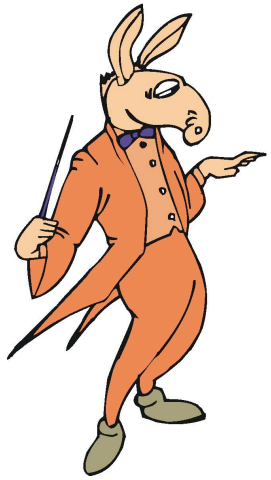
(A Trivial Comedy for Serious People), 1895

- “In matters of grave importance, style, not sincerity, is the vital thing.”
- “The truth is rarely pure, and never simple.”
- “To lose one parent, Mr. Worthing, may be regarded as a misfortune; to lose both looks like carelessness.”

Other Oscar Wilde Quotes

- “The play was a great success, but the audience was a disaster.”
- “I live in terror of not being misunderstood.”
- “A gentleman is one who never hurts anyone's feelings unintentionally.”
- “Seriousness is the only refuge of the shallow.”
- “What is a cynic? A man who knows the price of everything and the value of nothing.” *(Lady Windermere's Fan)*
- ”Whenever a man does a thoroughly stupid thing, it is always from the noblest motives.” *(The Picture of Dorian Gray)*

Common Attributes



Oscar Wilde, VAers & others good at finding security problems

- self-reliant
- cynical & skeptical
- need to feel special
- need to be seen as clever
- smart asses and/or arrogant
- little tolerance for BS
- hands-on & high-energy
- loop hole finders/exploiters
- unimpressed with authority, experts, bureaucrats, tradition, institutions, & regulations

Bad Guy Hackers & Inside Attackers

- self-reliant
- cynical & skeptical
- need to feel special
- need to be seen as clever
- smart asses and/or arrogant
- little tolerance for BS
- hands-on & high-energy
- loop hole finders/exploiters
- unimpressed with authority, experts, bureaucrats, tradition, institutions, & regulations

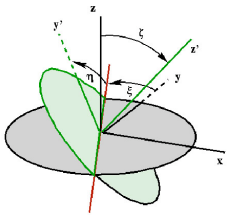
We don't see things as they are, we see things as we are.
-- Anais Nin (1903-1977)

Method Acting

- Originally developed in Russia (Konstantin Stanislavsky), but became big in the U.S. in the 40's and 50's.
- Emphasizes truth & authenticity, character's motivation, spontaneity, exposure to the character's physical environment, character continuity (the character does not spring into existence only once the play or movie starts), & staying in character.
- Well known method actors: Marlon Brando, Al Pacino, Gene Wilder, Robert De Niro, Ellen Burstyn, James Dean, Maureen Stapleton, Lee Grant, Dustin Hoffman, Marilyn Monroe, Paul Newman, Shelly Winters

We are what we do, not what we say.
-- Lee Strasberg (1899-1982)
teacher of method acting

Adversarial Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (This is much harder than you might think.)

> It is sometimes expedient to forget who we are. -- Publilius Syrus (~42 BC)

- Be much more creative than the adversaries. They need only stumble upon 1 vulnerability, the good guys have to worry about all of them.

> It's really kinda cool to just be really creative and create something really cool. -- Britney Spears

Adversarial Vulnerability Assessments

- Don't let the good guys & the existing security infrastructure and tactics define the problem.

> Evil will always triumph because good is dumb.
> -- Rick Moranis, as Dark Helmet in *Spaceballs* (1987)

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

> On a laser printer cartridge: "Warning. Do not eat toner."

We need to be more like fault finders. They find problems because they want to find problems, and because they are skeptical:

- bad guys
- therapists
- movie critics
- computer hackers
- scientific peer reviewers
- mothers-in-law

I told my psychiatrist that everyone hates me. He said I was being ridiculous--everyone hasn't met me yet.
-- Rodney Dangerfield (1921-1997)

"Two mothers-in-law."
-- Lord John Russell (1832-1900), on being asked what he would consider proper punishment for bigamy.

The Need for Creativity

Due to the rapid changes in the complexity of both technology and organizations over the past two decades, historical data has become less significant. Risk measurement and the identification of consequences require a combination of experience, skills, imagination, and creativity. This emphasis on subjective measurements is borne out in practice...

-- David McNamee, *Business Risk Management*, (1998), p. 43

The future ain't what it used to be. -- Yogi Berra

It's a poor sort of memory that only works backwards.
-- Lewis Carroll (1832-1898), *Alice in Wonderland*

Delaying Judgment

Nothing can inhibit and stifle the creative process more--and on this there is unanimous agreement among all creative individuals and investigators of creativity--than critical judgment applied to the emerging idea at the beginning stages of the creative process. ... More ideas have been prematurely rejected by a stringent evaluative attitude than would be warranted by any inherent weakness or absurdity in them. The longer one can linger with the idea with judgment held in abeyance, the better the chances all its details and ramifications [can emerge].

-- Eugene Raudsepp, *Managing Creative Scientists and Engineers* (1963).

Keep the possibility phase completely separate from the practicality phase!

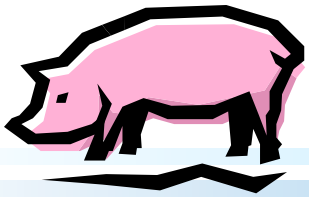
We all know your idea is crazy. The question is, is it crazy enough? -- Niels Bohr (1885-1962)

Realities of Creativity

Individuals are creative, not groups…

but the right group dynamics can energize, egg-on, & fertilize individuals…

and a group is usually necessary to fully explore attacks & countermeasures.



Could Hamlet have been written by committee, or the Mona Lisa painted by a club? Could the New Testament have been composed as a conference report? Creative ideas don't spring from groups. They spring from individuals.

-- Alfred Whitney Griswold (1885-1959)

Realities of Brainstorming (BSing)

- Individuals must be given ownership of their original idea & should be personally recognized for their creativity.

- The group environment needs to be:
  - diverse
  - high-energy
  - urgent but not stressful
  - humorous, joyful, & fun
  - cohesive but not too cohesive
  - competitive in a friendly & respectful way
  - enthusiastic about individual differences & eccentricities

> Sanity is a one trick pony--all you have is rational thought. But when you're good and loony, the sky's the limit!
>
> -- The Tick

- Every idea, no matter how wacky or stupid, gets written down & treated as a gem, at least initially.

Security Maxims

The following maxims, based on our experience with physical security, nuclear safeguards, & vulnerability assessments are not absolute laws or theorems, but they will be essentially correct 80-90% of the time…

Learn the principle, abide by the principle, dissolve the principle. -- Bruce Lee (1940-1973)

Argonne NATIONAL LABORATORY

Security Maxims

Infinity Maxim: There are an unlimited number of security vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or bad guys).

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

When men are the most sure and arrogant, they are commonly the most mistaken. -- David Hume (1711-1776)

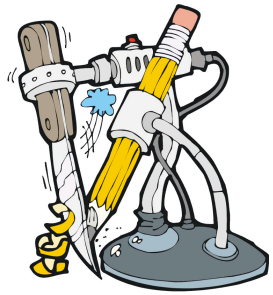
Security Maxims

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it.

Be Afraid, Be Very Afraid Maxim: If you're not running scared, you have bad security or a bad security product.

Self knowledge is always bad news. -- John Barth

Security Maxims



High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology it uses.

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems).

Schneier's Maxim #1: The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

Security Maxims

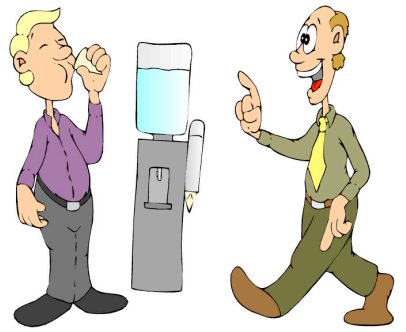
Yipee Maxim: There are effective, simple, & low-cost countermeasures (at least partial countermeasures) to most security vulnerabilities.

Arg Maxim: But users, manufacturers, managers, and bureaucrats will be reluctant to implement them, often for reasons of inertia, bureaucracy, pride, fear, wishful thinking, or cognitive dissonance.

I cannot imagine any condition which would cause this ship to founder, nor conceive of any vital disaster happening to this vessel.

-- E.J. Smith, Captain of the *Titanic*

Security Maxims



Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

All methodologies are based on fear. -- Kent Beck

Security Maxims

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

"You mean they've scheduled Yom Kippur opposite *Charlie's Angels?*"
-- Fred Silverman, TV Programmer, when told Yom Kippur would fall on a Wednesday

Security Maxims

Somebody Must've Thought It Through Maxim: The more important the security application, the less careful and critical thought has gone into it.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware and strategies being employed.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e., security based on keeping long-term secrets, is not a good idea.

Gossip Maxim: People and organizations can't keep secrets.

Three may keep a secret,
if two of them are dead.
-- Benjamin Franklin, *Poor Richards Almanack*, 1735

Security Maxims

Plug into the Formula Maxim: Engineers don't understand security. They think nature is the adversary, not people. They tend to work in solution space, not problem space. They think systems fail stochastically, not through deliberate, intelligent, malicious intent.

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

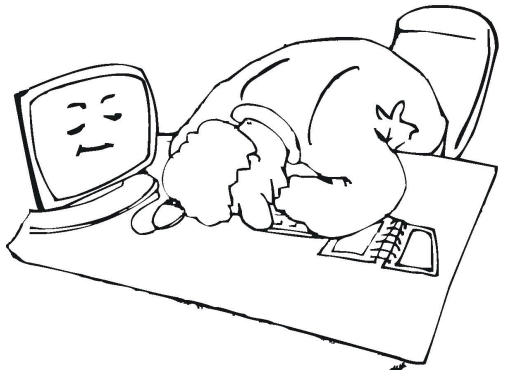
Rohrbach Was An Optimist Maxim: Few security devices, systems, or programs will ever be used properly.

Cleveland Indians catcher Harry Chiti was once traded for himself: He was traded for a player to be named later, and (2 months later) he turned out to be that player.

Security Maxims

Insider Risk Maxim: Most organizations will ignored or seriously underestimate the threat from insiders.

We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees & contractors exceeds the threat from malicious insiders (though the latter is not negligible.)



If people don't want to come to the ballpark, how are you going to stop them? -- Yogi Berra

Security Maxims

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

Everything I did in my life that was worthwhile I caught hell for. -- Earl Warren (1891-1974)

Security Maxims

Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.

Backwards Maxim: Most people will assume everything is secure until provided strong evidence to the contrary--exactly backwards from a reasonable approach.

It only had one fault. It was kind of lousy.
-- James Thurber (1894-1961)

Security Maxims

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, manufacturers, vendors, and end users will always be amazed at how easily their security products or programs can be defeated.

You Could've Knocked Me Over with a Feather Maxim 2: Having been amazed once, security managers, manufacturers, vendors, and end users will be equally amazed the next time around.

Invader Zim: "You're lying! Nothing breaches my defenses, nothing! You hear me!....Nothing!... [To self: Maybe there is some kind of flaw, but what?]" -- Invader Zim cartoon, episode 109b, "Rise of the Zitboy"

Security Maxims

<u>Better to be Lucky than Good Maxim:</u> Most of the time when security appears to be working, it's because no adversary is currently prepared to attack.

<u>That's Why They Pay Us the Big Bucks Maxim</u>: Security is nigh near impossible. It's extremely difficult to stop a determined adversary. Often the best you can do is discourage him, and maybe minimize the consequences when he does attack.

There is no such thing as security. Never has been.
-- Germaine Greer

Security Maxims

That's Entertainment Maxim: Ceremonial Security (a.k.a. "Security Theater") will usually be confused with Real Security; even when it is not, it will be favored over Real Security.

Schneier's Maxim #2: Control will usually get confused with Security.

> Those who would give up an essential liberty for temporary security deserve neither.
>
> -- Benjamin Franklin (1706-1790)

Security Maxims

A Priest, a Minister, and a Rabbi Maxim:
People lacking imagination and a sense of humor should not work in the security field.

Over-seriousness is a warning sign for mediocrity and bureaucratic thinking. People who are seriously committed to mastery and high performance are secure enough to lighten up. -- Michael J. Gelb

Security Maxims

When we have strong emotions, we are liable to fool ourselves.
-- Carl Sagan (1934-1996)

Mr. Spock Maxim: The effectiveness of a security device, system, or program is inversely proportional to how angry or upset people get about the idea that there might be vulnerabilities.

Irresponsibility Maxim: It'll often be considered "irresponsible" to point out security vulnerabilities (including the theoretical possibility that they might exist), but never irresponsible to ignore or cover them up.

Security Maxims

Mission Creep Maxim: Any given device, system, or program designed for inventory will very quickly come to be viewed--quite incorrectly--as a security device, system, or program.

We'll Worry About it Later Maxim: Effective security is difficult enough when you design it in from first principles. It almost never works to retrofit it in, or to slap security on at the last minute (especially on an inventory system).

Show Me Maxim: No major security vulnerability, including blatantly obvious ones, will be dealt with until there is over-whelming evidence and widespread recognition that adversaries have already catastrophically exploited it.

We are never ready for what we expect.
-- James Michener (1907-1997)

Security Maxims

Ass Sets Maxim: Most security programs focus on protecting the wrong assets.

Vulnerabilities Trump Threats Maxim: If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited and by whom). Plus you might even be ok if you get the threats all wrong. But if you focus mostly on the threats, you're probably in trouble.

There's no sense in being precise when you don't even know what you're talking about.
-- John von Neumann (1903-1957)

Another famous smirker from history:

Niccolo di Bernardo dei Machiavelli (1469-1527)

Good Reads

2 great books not about security that are really about security:

Carol Travis & Elliot Aronson, **Mistakes Were Made (But Not by Me)** (2007).

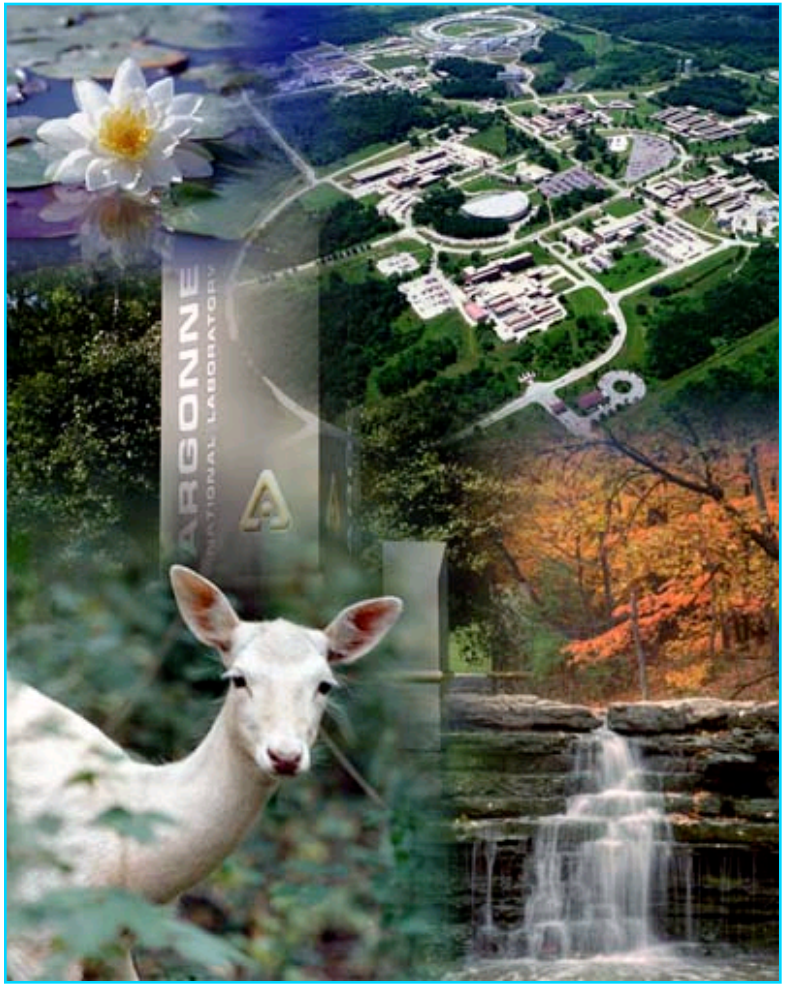
Thomas L. Friedman, **The World is Flat** (2006).

Good security books:

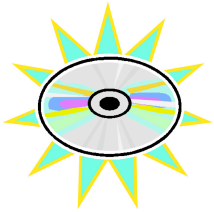
William L. Simon, **The Art of Intrusion** (2005).

Frank W. Abagnale, **The Art of the Steal** (2002).

Vulnerability Assessment Team



Related papers, reports, and presentations are available from rogerj@anl.gov



http://www.ne.anl.gov/capabilities/vat

If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort…only soft soap and wishful thinking to begin, and in the end, despair. -- C.S. Lewis (1898-1963)