Paths to Creativity in Security Careers

Privacy, Security and Trust 2006

Dr. Gregory Newby
Arctic Region Supercomputing Center
University of Alaska Fairbanks

Arctic Region Supercomputing Center

The Message

- Security is, fundamentally, adversarial. Our goal is to protect against various risks.
- One element of an effective security posture is to insure the people protecting against risk are able to predict and understand their adversaries' actions.
- These people need to be as creative, skilled and innovative as their adversaries.

Arctic Region Supercomputing Center

Who is this Guy?

- Research faculty member @ UAF, serving as Chief Scientist of ARSC
- Research activity in information retrieval
- Varied information security credentials
- Active in creative technical communities
- Literary / information outreach focus

Arctic Region Supercomputing Center

Digital Literati

From the Abstract

- "Courageous, creative, educated, empowered and experienced individuals are a key component to building adaptable and healthy organizations." (gbn)
- Three themes:
  - The "hacker spirit"
  - Understanding complex systems
  - Creativity in the organization

The Hacker Spirit

- Bob Bickford, computer and video guru, defined the true essence of the hacker as "Any person who derives joy from discovering ways to circumvent limitations."
- A key question for is whether hackers are working *for* you, or *against* you

Arctic Region Supercomputing Center

Bruce Schneier in 2600

- Encouraging pursuing employees with the hacker spirit

Hacker Perspective

by Bruce Schneier

A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity.

I wrote that last sentence in the year 2000, in my book *Beyond Fear*. And I'm sticking to that definition.

This is what else I wrote in *Beyond Fear*:

"Hackers are as old as curiosity, although the term itself is modern. Galileo was a hacker. Newton was one, too. Aristotle wasn't. (Aristotle had some theories about proof that women had fewer teeth than men. A hacker would have simply counted his wife's teeth. A good hacker would have counted his wife's teeth without her knowing about it, while she was asleep. A good *bad* hacker might remove some of them, just to prove a point.)

"When I was in college, I knew a group similar to hackers: the key freaks. They wanted access, and their goal was to have a key to every lock on campus. They would study locksmithing and learn new techniques, trade maps of the steam tunnels and where they led, and exchange copies of keys with each other. A locked door was a challenge, a personal affront to their ability. These people weren't out to do damage - stealing stuff wasn't their objective - although they certainly could have. Their hobby was the power to go anywhere they wanted to.

"Remember the phone phreaks of yesteryear, the ones who could whistle into any phones and make free phone calls. Sure, they stole phone service. But it wasn't like they needed to make eight-hour calls to Kanjiza or Mombasa. And their real work was about knowledge. The phone network was a vast maze of information. They wanted to know the system better than the designers, and they wanted the ability to modify it to their will. Understanding how the phone system worked - that was the true prize. Other early hackers were ham-radio hobbyists and model-train enthusiasts.

"Richard Feynman was a hacker; read any of his books.

"Computer hackers follow these evolutionary lines. Or, they are the same urges operating on a new system. Computers, and networks in particular, are the new landscape to be explored. Networks provide the ultimate maze of steam tunnels, where a new hacking technique becomes a key that can open computer after computer. And inside is knowledge, understanding. Access. How things work. Why things work. It's all out there, waiting to be discovered."

Computers are the perfect playgrounds for hackers. Computers, and computer networks, are vast treasure troves of secret knowledge. The Internet is an immense landscape of undiscovered information. The more you know, the more you can do.

And it should be no surprise that many hackers have focused their skills on computer security. Not only is it often the obstacle between the hacker and knowledge, and therefore something to be defeated, but also the very mindset necessary to be good at security is exactly the same mindset that hackers have: thinking outside the box, breaking the rules, exploring the limitations of a system. The easiest way to break a security system is to figure out what the system's designers hadn't thought of: that's security hacking.

Hackers cheat. And breaking security regularly involves cheating. It's figuring out a smart card's RSA key by looking at the power fluctuations, because the designers of the card never realized anyone could do that. It's self-signing a piece of code, because the signature-verification system didn't think someone might try that. It's using a piece of a protocol to break a completely different protocol, because all previous security analysis only looked at protocols individually and not in pairs.

That's security hacking: breaking a system by thinking differently.

It all sounds criminal: recovering an encrypted text, faking signature algorithms, breaking protocols. But honestly, that's just the way we security people talk. Hacking is not criminal. All the examples two paragraphs above were performed by respected security professionals, and all were presented at security conferences.

I remember one conversation I had at a Crypto conference, early in my career. It was outside amongst the jumbo shrimp, chocolate covered strawberries, and other delectables. A bunch of us were talking about some cryptographic system, including Brian Snow of the NSA. Someone described an unconventional attack, one that didn't follow the normal rules of cryptanalysis. I don't remember any of the details, but I remember my response after hearing the description of the attack.

"That's cheating," I said.

Because it was.

I also remember Brian turning to look at me. He didn't say anything, but his look conveyed everything. "There's no such thing as cheating in this business."

Because there isn't.

Hacking is cheating, and it's how we get better at security. It's only after someone invents a new attack that the rest of us can figure out how to defend against it.

For years I have refused to play the semantic "hacker" vs. "cracker" game. There are good hackers and bad hackers, just as there are good electricians and bad electricians. "Hacker" is a mindset and a skill set; what you do with it is a different issue.

And I believe the best computer security experts have the hacker mindset. When I look to hire people, I look for someone who can't walk into a store without figuring out how to shoplift. I look for someone who can't test a computer security program without trying to get around it. I look for someone who, when told that things work in a particular way, immediately asks how things stop working if you do something else.

We need these people in security, and we need them on our side. Criminals are always trying to figure out how to break security systems. Hold a new system - an ATM, an online banking system, a gambling machine - and criminals will try to make an illegal profit off it. They'll figure it out eventually, because some hackers are also criminals. But if we have hackers working for us, they'll figure it out first - and then we can defend ourselves.

It's our only hope for security in this fast-moving technological world of ours.

Bruce Schneier is an internationally renowned security technologist, referred to by "The Economist" as a "security guru." He is the author of approximately eight books - including the best sellers "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," "Secrets and Lies," and "Applied Cryptography" - and hundreds of academic articles and papers. His influential newsletter, "Crypto-Gram," is read by over 120,000 people. Schneier is regularly quoted in the press, and his essays have appeared in national and international publications. He is a frequent guest on television and radio, has testified before Congress, and is a frequent writer and lecturer on issues surrounding security and privacy.

WRITERS WANTED

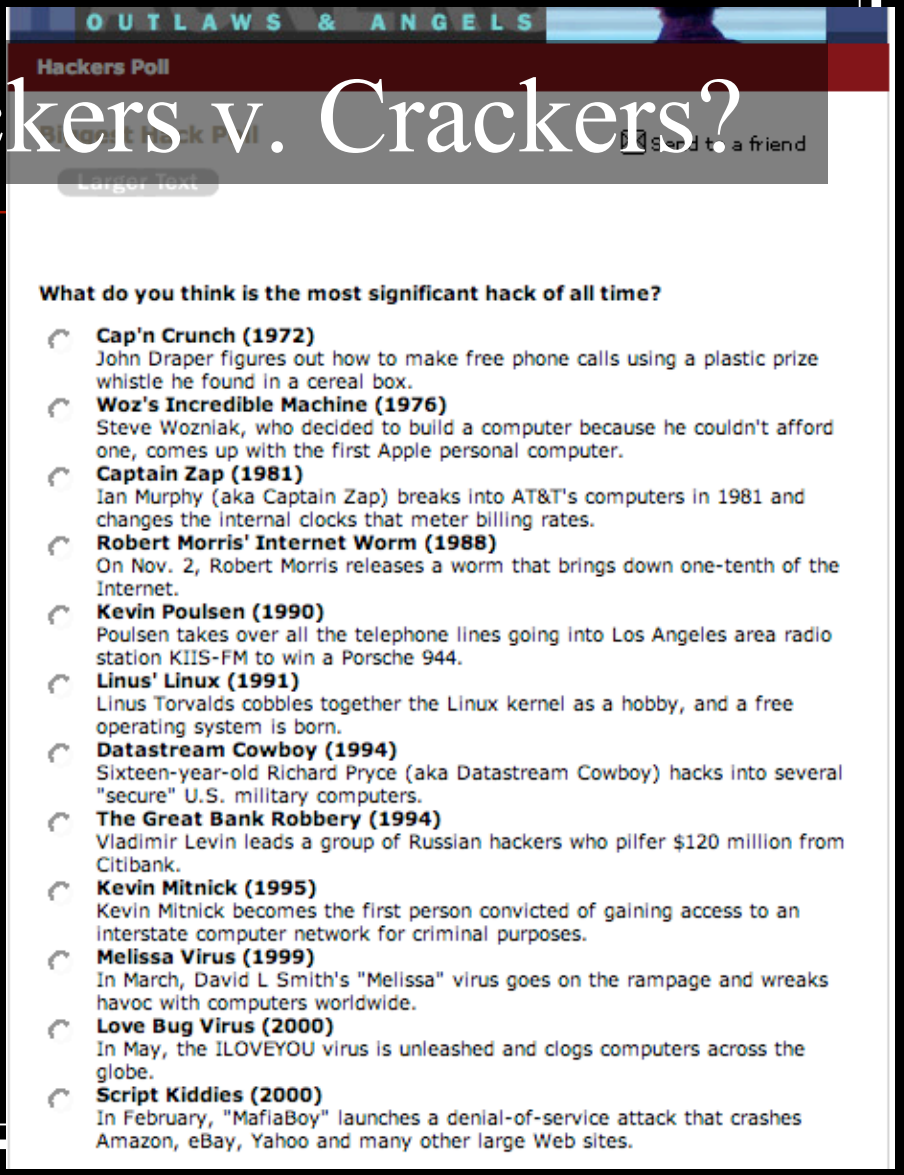
Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Arctic Region Supercomputing Center

Confused about Hackers v. Crackers?

- It's no wonder. This TLC show mixes criminals, viruses and others.
- Consider the social & technical changes over time that makes yesterday's pranks today's crimes



OUTLAWS & ANGELS

Hackers Poll

Send to a friend

Larger Text

What do you think is the most significant hack of all time?

- **Cap'n Crunch (1972)**
  John Draper figures out how to make free phone calls using a plastic prize whistle he found in a cereal box.
- **Woz's Incredible Machine (1976)**
  Steve Wozniak, who decided to build a computer because he couldn't afford one, comes up with the first Apple personal computer.
- **Captain Zap (1981)**
  Ian Murphy (aka Captain Zap) breaks into AT&T's computers in 1981 and changes the internal clocks that meter billing rates.
- **Robert Morris' Internet Worm (1988)**
  On Nov. 2, Robert Morris releases a worm that brings down one-tenth of the Internet.
- **Kevin Poulsen (1990)**
  Poulsen takes over all the telephone lines going into Los Angeles area radio station KIIS-FM to win a Porsche 944.
- **Linus' Linux (1991)**
  Linus Torvalds cobbles together the Linux kernel as a hobby, and a free operating system is born.
- **Datastream Cowboy (1994)**
  Sixteen-year-old Richard Pryce (aka Datastream Cowboy) hacks into several "secure" U.S. military computers.
- **The Great Bank Robbery (1994)**
  Vladimir Levin leads a group of Russian hackers who pilfer $120 million from Citibank.
- **Kevin Mitnick (1995)**
  Kevin Mitnick becomes the first person convicted of gaining access to an interstate computer network for criminal purposes.
- **Melissa Virus (1999)**
  In March, David L Smith's "Melissa" virus goes on the rampage and wreaks havoc with computers worldwide.
- **Love Bug Virus (2000)**
  In May, the ILOVEYOU virus is unleashed and clogs computers across the globe.
- **Script Kiddies (2000)**
  In February, "MafiaBoy" launches a denial-of-service attack that crashes Amazon, eBay, Yahoo and many other large Web sites.

HPC Modernization Program

UAF

Arctic Region Supercomputing Center

What color is your Hat?

- Does it matter? Or does only your activity, and intentions behind your activity, matter?
- Orgs
  - HAL 2001, WTH, H2K, H2K2
  - SC|06, PST2006
- Certs
  - CISSP, SANS
  - Being "3l334" on the nets

Arctic Region Supercomputing Center

Understanding Complex Systems

- For systems of significant size (such as the Internet, or an operating system), nobody can fully understand complex systems
- So, we use models, we experiment, we think
- Apply diversity in skill sets, knowledge, and methodologies

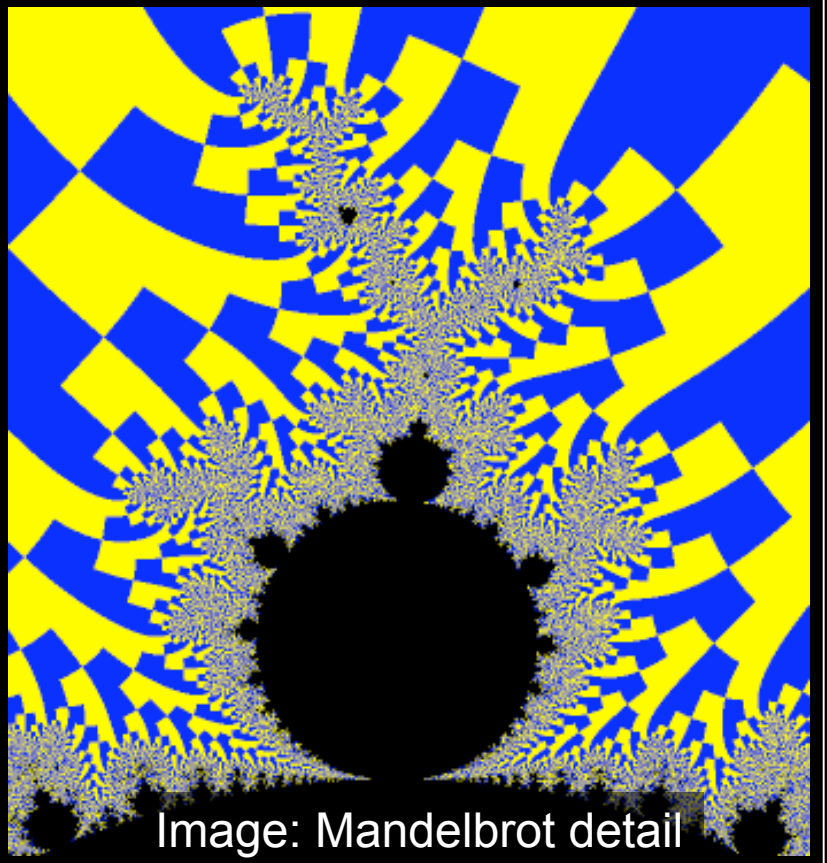


Image: Mandelbrot detail

Puzzles

- Piecing together all aspects of security scenarios: tough
- Different areas of expertise required
- Build a multi-disciplinary team

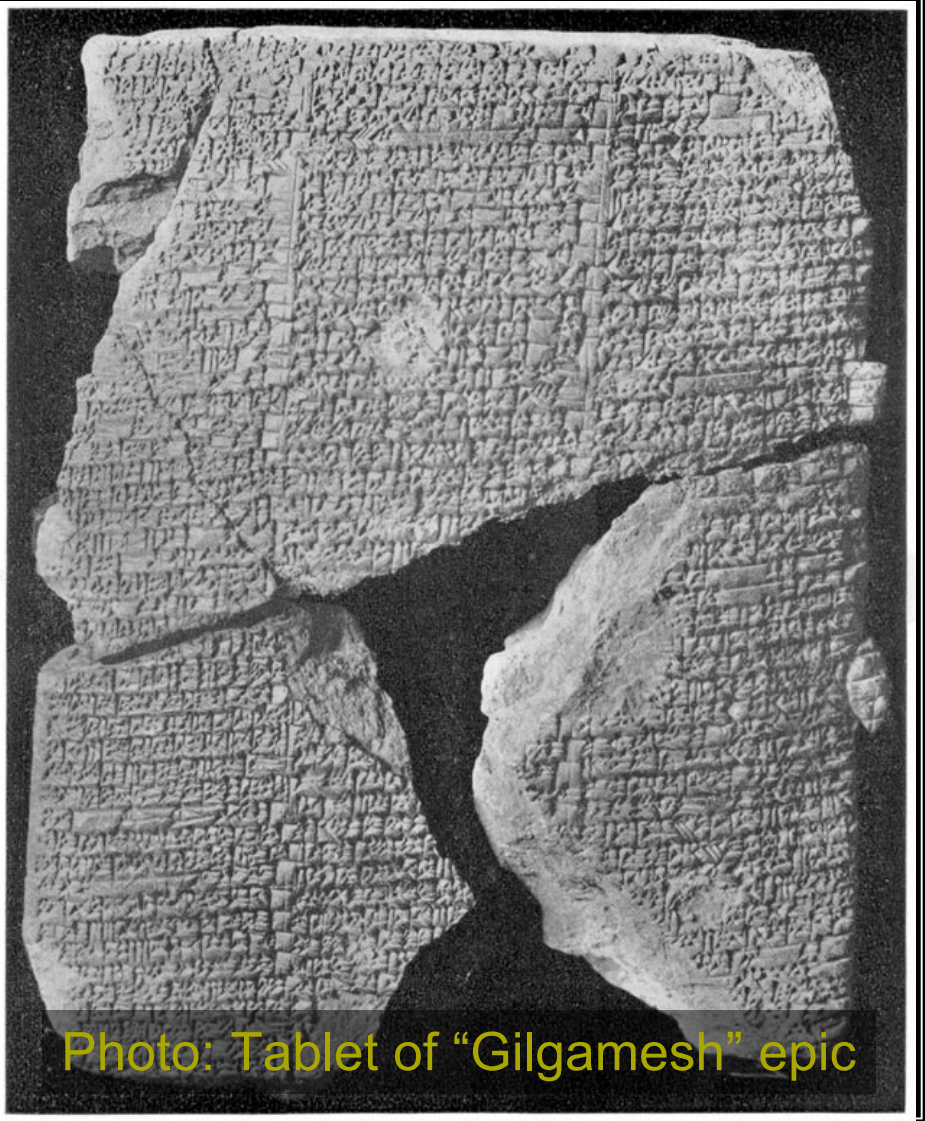
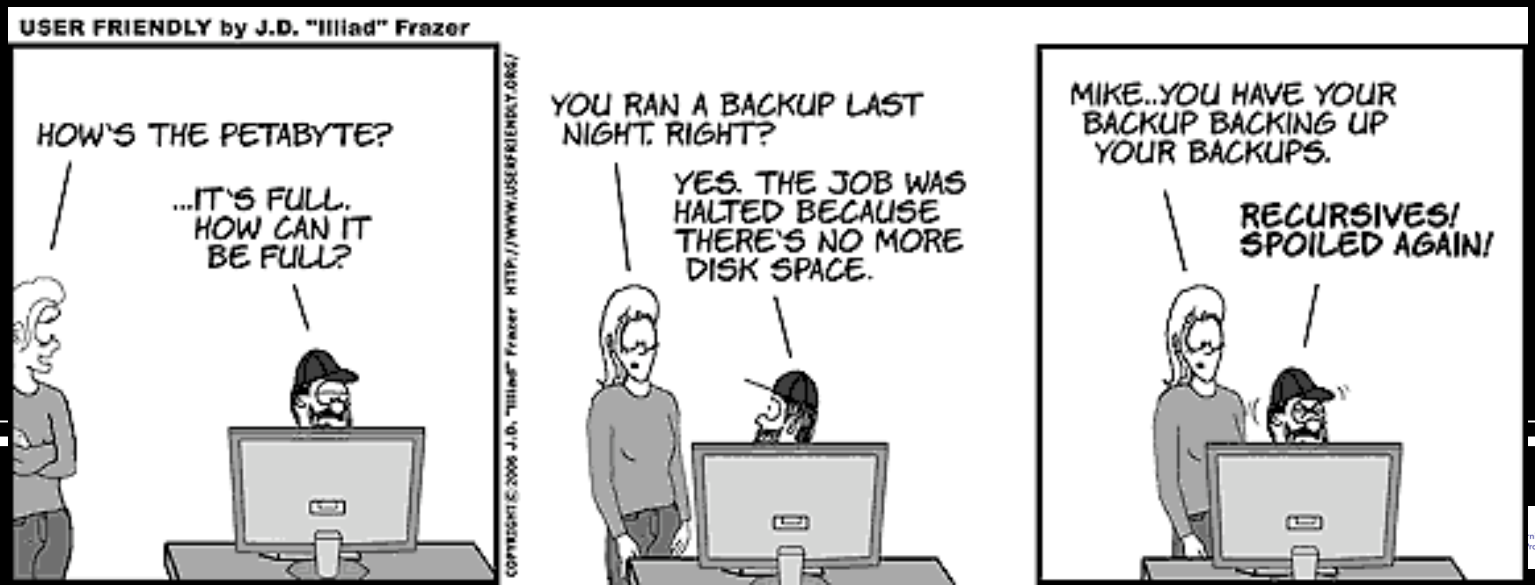


Photo: Tablet of “Gilgamesh” epic

Arctic Region Supercomputing Center

Addressing Complex Systems

- Can you insure adequate and diversified staffing and attention to information security environment?
- How can the technologists benefit from the domain experts, and vice-versa?
- What are some "best practices" that can help (such as encryption, backups, privilege separation, and logging)?



Creativity in the Organization

- Everywhere? Maybe not…
- Good judgment is still a key requirement
- Checks and balances are needed
  - Remember that most computer crime is committed by insiders

Photo: Jeffrey Skilling (Enron) heading back to jail

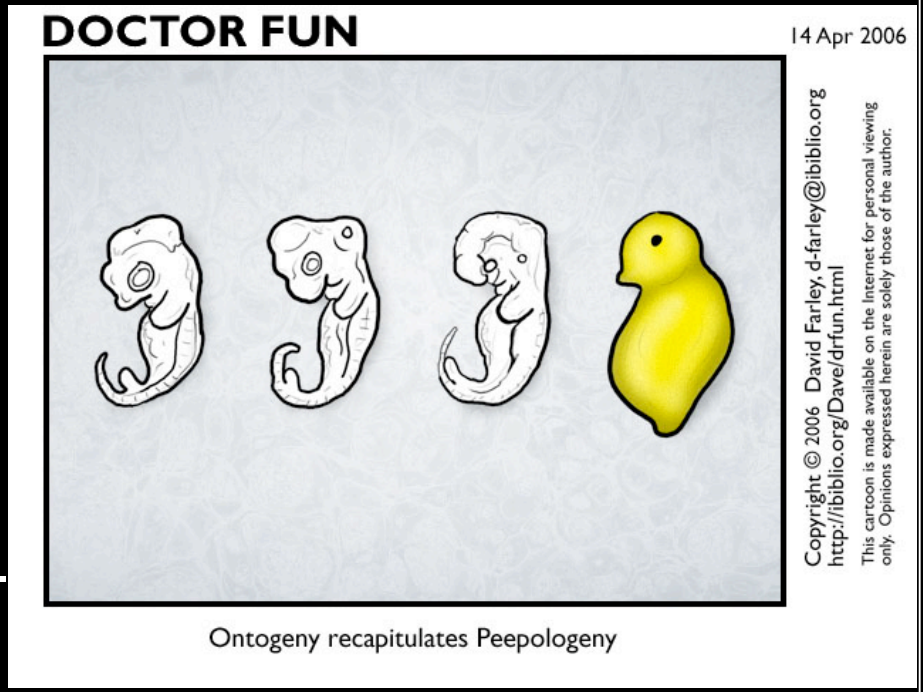
Tips for Students

- Be broad; Be deep; Be technical
- Develop good communication skills
- Develop good habits for time management, so you have ability to monitor information security events and study them

© Scott Adams, Inc./Dist. by UFS, Inc.

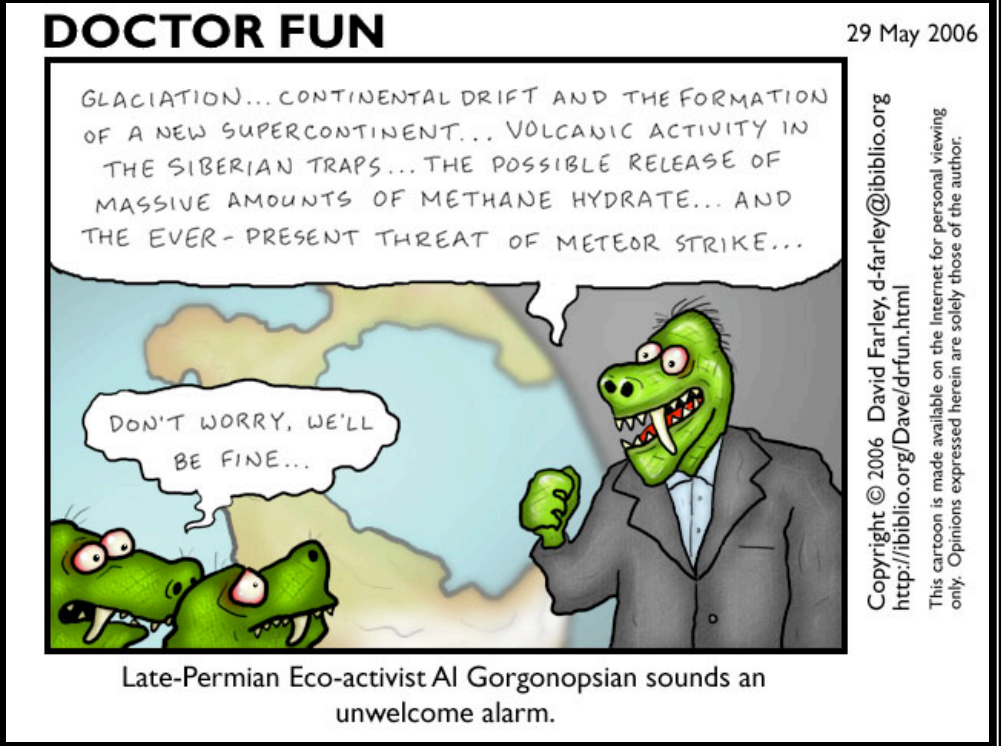
Tips for Employers

- Give attention to security
- Encourage everyone to play an active role in information security
- Provide on going training for all aspects of technology, including security
- Don't marginalize security -- make it a core activity
- Work to evolve a sound, secure organization



Tips for Information Professionals

- Take time to reflect on security issues for any application / product / activity
- Learn to work with others to assess security risks. Don't be a lone wolf, or closed-minded
- Be user-friendly
- You're the front line, the last bastion, and the only hope



Late-Permian Eco-activist Al Gorgonopsian sounds an unwelcome alarm.

Arctic Region Supercomputing Center

Challenges with Creativity

- Schools tend to teach conformance, and reward compliance
- Thinking “outside the box” might be frowned upon
- Performance & outcomes-driven organizations have little patience for deep thinkers
- We’re often too busy to be as creative as we wish
  - How can you encourage creative thinking?
  - Is it obvious why this is key for information security?

Photo: Anyone you know?

Creativity in Information Security

- Put yourself in your adversary's shoes
  - G.H. Mead: Humans are the animal with the ability to perceive the other's self-model
- If monkeys can do it, so can security professionals!
  - Scenario planning
  - Penetration tests
  - Systems/code auditing
    - (If you don't do these things, maybe your adversary will)

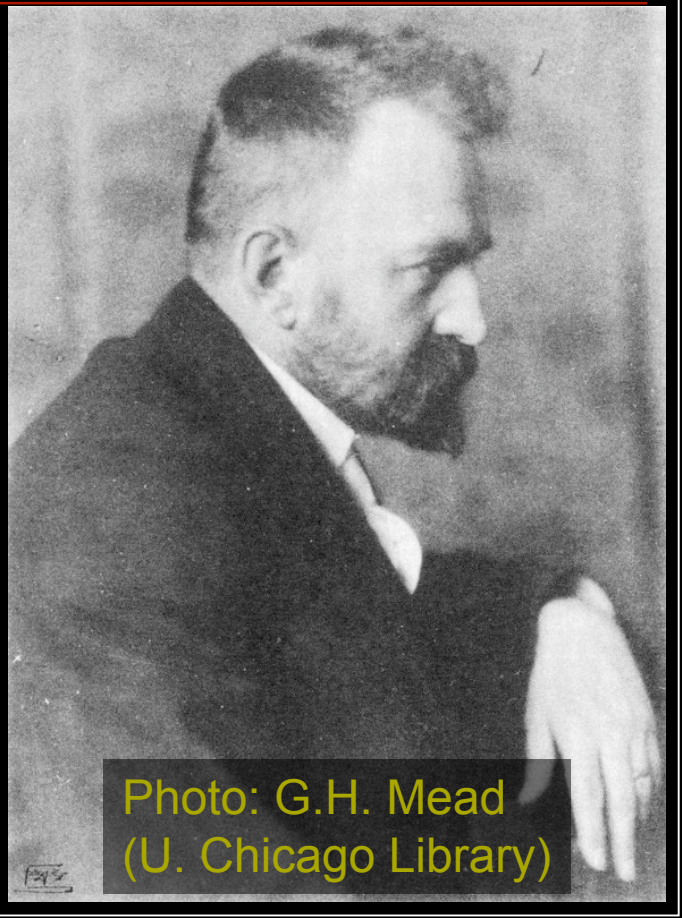


Photo: G.H. Mead (U. Chicago Library)

Arctic Region Supercomputing Center

Take-Away points

- Security is hard, and requires multiple approaches (duh…)
- Waiting for other people to develop strategies for responding to attacks is risky
- Your security posture needs to envision potential attacks and attackers
- If your attackers are more creative than you, you might be in trouble.
  - *Therefore, seek out and foster creativity in your information security organization*

Arctic Region Supercomputing Center

See ya on the trails…

Photo: gbn in TRDMA dog race (see stinkypup.net)