50 CyberSecurity Myths and What To Do About Them

2013-09-11

DARPA CyberSecurity Forum

Dr. Fred Cohen
CEO – Management Analytics (non-government)
CEO – Fred Cohen & Associates (government only)

The challenge of the day

- **"Despite 25 years of conflict in cyberspace, and investment of billions of dollars, our national leaders are calling cyberspace threats one of our Nation's greatest concerns."**
  - What are the facts?
  - What are myths?
  - What should we do about it?
- Myth 1: 25 years of cyber-conflict in cyberspace
  - Fact 1: It has been a lot longer
  - What to do: Use real facts to get real answers

The challenge of the day

- **"… and investment of billions of dollars, our national leaders are calling cyberspace threats one of our Nation's greatest concerns."**
- Myth 2: Billions of dollars seems like a lot
  - Fact 2: $4.5B/aircraft carrier | $929M/B-2 ...
  - What to do: Pay what it costs for what you claim to need.
- Myth 3: "leaders … greatest concerns..."
  - Fact 3: Our "leaders" don't know and neither do we - because Govt won't investigate it.
  - What to do: Do the work to get the real answers

More myths, facts, to do

- Myth 4: Computer science is a science
  - Fact 4: Information protection is not treated as one
  - What to do: Start to treat it as one
- Myth 5: Computers work at the speed of light!
  - Fact 5: Computers are not that fast
  - What to do: Stop exaggerating - get the facts right.
- Myth 6: [name your fear point] is growing exponentially
  - Fact 6: What we are seeing is mostly step functions
  - What to do: Stop exaggerating - get the facts right.
- Myth 7: Vulnerabilities are increasing
  - Fact 7: They are not - although threats are.
  - What to do: Use existing common language

More myths, facts, to do

- Myth 8: Attackers (hackers) are geniuses
  - Fact 8: Most attackers are script kiddies
  - What to do: Stop glorifying criminals and meanies
- Myth 9: Defenders are stupid
  - Fact 9: Mostly they are undereducated and undertrained
  - What to do: Make them into and treat as professionals
- Myth 10: The best defense is a good offense
  - Fact 10: Offense can be useful, but not the best today.
  - What to do: Increase defense budget to 10% of offense?
- Myth 11: COTS will save us
  - Fact 11: "We gots your COTS"
  - What to do: Build a real trusted GOTS industry in the US

More myths, facts, to do

- Myth 12: New attack methods keep emerging
  - Fact 12: Almost no attack innovation in 20 years
  - What to do: Study this for real instead of hyping it
- Myth 13: Locking people down further will fix it
  - Fact 13: The security squeeze is already to tight
  - What to do: Loosen the grip on people, tighten security
- Myth 14: The user is the problem
  - Fact 14: The user is the reason
  - What to do: Stop punishing victims, punish criminals
- Myth 15: XXX is a new defensive technique
  - Fact 15: There are almost no innovations in defense
  - What to do: Build a set of skunk works with real experts

More myths, facts, to do

- Myth 16: You can learn to defend in 1-3 months
  - Fact 16: It takes several years to get you competent
  - What to do: Treat protection as a profession
- Myth 17: We can defend a billion mobile devices
  - Fact 17: We can't. Not now or in the foreseeable future
  - What to do: Stop trying to boil the ocean
- Myth 18: Commercial industry will provide the solution
  - Fact 18: They will not and you won't buy it if they do
  - What to do: Stop imagining COTS will save you
- Myth 19: Economics will take care of it on its own
  - Fact 19: Sequential economic models favor less defense
  - What to do: Stop imagining economics will save you

More myths, facts, to do

- Myth 20: We can verify our way out of this
  - Fact 20: What is being verified isn't relevant
  - What to do: Do basic research on what to verify
- Myth 21: We can verify our way out of this - 2
  - Fact 21: We are nowhere near verifying large programs
  - What to do: Try generating verifiable programs
- Myth 22: We can verify our way out of this - 3
  - Fact 22: We haven't a clue how to verify in context
  - What to do: Work on composition of specific properties
- Myth 23: We can verify our way out of this - 4
  - Fact 23: Verification without source and specs is silly
  - What to do: Create GOTS sources for verification

More myths, facts, to do

- Myth 24: We can outrun the problem
  - Fact 24: Run faster can work, but only selectively
  - What to do: Select where to run quickly
- Myth 25: Risk management will save us
  - Fact 25: We don't even have common definitions of risk
  - What to do: Do real research in the nature of risk
- Myth 26: Risk management will save us - 2
  - Fact 26: We don't know how to assess risk well
  - What to do: Stop PRA and similar methods for “cyber”
- Myth 27: We know what “cyber” means
  - Fact 27: Cybernetics (Weiner 1948) is not computers
  - What to do: Stop hyperbolizing, start defining terms

More myths, facts, to do

- Myth 28: More surveillance will save us
  - Fact 28: Watching everything creates a weaker society
  - What to do: Stop using technology against the public
- Myth 29: Forensics will save us
  - Fact 29: After-the-fact for court doesn't stop attacks
  - What to do: Recognize fundamental limits of approach
- Myth 30: Intrusion/Anomaly Detection will save us
  - Fact 30: This technology has deep and real problems
  - What to do: Recognize the real limits and use wisely
- Myth 31: [ANY ONE THING] will save us
  - Fact 31: Big complicated issues – no itty bitty solution
  - What to do: Recognize the scope of the issues

More myths, facts, to do

- Myth 32: We are at a loss for good ideas
  - Fact 32: We haven't explored enough ideas to tell good
  - What to do: Create sets of skunk works with experts
- Myth 33: There are no bad ideas
  - Fact 33: There are plenty of them out there
  - What to do: Stop funding so many of them?
- Myth 34: Ideas are free, we only pay for “research”
  - Fact 34: You don't pay for the hard part & don't get it
  - What to do: Start buying the things that will help most
- Myth 35: We can't fund smart people based on records
  - Fact 35: Yes you can, but you won't.
  - What to do: Find a way and make is stick

More myths, facts, to do

- Myth 36: Cyber attacks are as bad as nuclear attacks
  - Fact 36: Nuclear → many millions dead, cities destroyed
  - What to do: Stop exaggerating, put it in proportion
- Myth 37: Cyber attacks are as bad as biological attacks
  - Fact 37: Influenza killed ~40M people in 1918-19s
  - What to do: Stop exaggerating, put it in proportion
- Myth 38: Cyber is a WMD
  - Fact 38: It's not and will not be – unless we make it so
  - What to do: Stop building more/higher consequences
- Myth 39: Our society protects the innocent victims
  - Fact 39: Grandma gets ripped off, police ignore it
  - What to do: Stop crime where it starts: small / human

More myths, facts, to do

- Myth 40: There are hoards of untraceable threats
  - Fact 40: There are a small, growing number
  - What to do: Hunt them down before they grow
- Myth 41: There are hoards of untraceable threats -2
  - Fact 41: They are traceable, but we don't trace them all
  - What to do: Find better ways to do attribution
- Myth 42: There are hoards of untraceable threats - 3
  - Fact 42: The US declared global cyber war by its actions
  - What to do: Don't declare a war you don't want to fight
- Myth 43: We can't reduce threats
  - Fact 43: Attrition works
  - What to do: Start attritting targets

More myths, facts, to do

- Myth 44: Cyberspace isn't physical
  - Fact 44: Yes – it is physical
  - What to do: You can use physical capabilities against it
- Myth 45: Digital information has the same physics
  - Fact 45: It doesn't – it has additional features
  - What to do: Do research in the nature of digital physics
- Myth 46: Prevention is a failed approach
  - Fact 46: Prevention works great – for what it prevents
  - What to do: Use / fund prevention where appropriate
- Myth 47: Perfect is the enemy of good enough
  - Fact 47: They are allies
  - What to do: Get to good enough by seeking perfection

More myths, facts, to do

- Myth 48: Be afraid! Be very afraid!
  - Fact 48: There's nothing to fear but fear itself
  - What to do: Don't live in fear - face fear and get facts
- Myth 49: It's as bad as “they” say it is – maybe worse
  - Fact 49: Whoever “they” are, they are likely wrong.
  - What to do: Get facts and draw conclusions from them
- Myth 50: It's all perception
  - Fact 50: It's not. There are realities.
  - What to do: Get facts and draw conclusions from them
- Fact: Nothing I have put here is new (see http://all.net/)
  - I write a free monthly article and have for ~15 years
  - If anything here surprised, it's your willful ignorance

A final thought or two

- I hope you already knew everything in here
  - I exaggerated slightly to fit things in one line
  - I apologize if I painted too broadly
  - If you were offended – good.
  - The idea is to get you out of your group think
- If you knew, why didn't you do the things suggested?
  - These suggestions are only some of many possibilities
  - Many folks tell me they wish they could but they can't
    - If you want to know why you fail, that is why
    - You can do more, but you have to take risks to do it
    - You can't do your job if you are afraid of losing it
- Yes we can – so let's!

Thank You

http://fredcohen.net/ http://all.net/
fc at fredcohen.net - - fc at all.net