Good Security Traits

What Makes Good Security Experts and Presentations

Travis H.

26 Aug 2009 AHA

Why This Talk?

- There are lots of people who want to become security experts
- Many of them would like to do presentations
- Motivated people want to improve themselves and do interesting work

My Qualifications

- Started studying security in 1985 with book "Out of the Inner Circle"
- Held computer security jobs in the military and financial sectors
- Helped designed and build an IDS in small startup company
- Have a bookcase full of security & crypto books
- Avid consumer of security info (presentations, conferences, blogs, papers)
- Writing an online book called "Security Concepts" - 170 pages so far

My Lack of Qualifications

- Not a "name" - not famous in security circles (yet?)
- Never been a pentester
- Never been published in a peer-reviewed journal

Disclaimers and Caveats

- No hard facts to back up my opinions
- But I think many consumers of security information feel this way
- My opinions are just that, feel free to have your own

Motivation

- Security can be a *very* complex subject
- Not just a single field of study, but intersects with many related disciplines
- Mastery of the various topics takes much time and effort
- Many open problems are very difficult to solve which is why they're still open
- Successful people are unusually motivated, and not just by money
- They love the work

Intelligence

- Most security experts are really smart people
- IQ measures how quickly you can come up with patterns, and test them against reality
- This maps rather well to many aspects of security
- Highly intelligent people don't necessarily have *consistently better* ideas
- They just have *more of them*, and discard the ones that suck

Domain Knowledge

- Security experts tend to have extensive knowledge about their field
- The action tends to be at the bleeding edges (but not always)
- ...where the security implications are not yet known
- Hard to break new ground if you aren't well steeped in the fundamentals
- Anecdote: Bobby Fischer

Lateral Thinking

- System designers build systems with certain uses in mind
- Exploitation involves coming up with uses that they didn't anticipate
- Good defense means trying to think of *all* the ways it could be (ab)used
- Anecdotes: Gordian Knot, Bruce Lee
- Examples: Lock Bumping, Side Channel Attacks

Intellectual Mavericks

- The best security experts are often non-conformists
- They think about things that other people don't
- They think about things in *ways* that other people don't
- They question conventional wisdom, assumptions, and are skeptical of claims
- If you don't have novel perspectives and ideas, you can't discover anything new
- Anecdote: Bruce Schneier on identifying airline passengers

Patterns and Analogies

- To some, genius is the ability to recognize similar patterns in two different contexts
- Solutions in the old context might have similar solutions in the new context
- Example: Slowloris vs SYN flooding vs zero-length TCP windows vs tarpitting

Daring

- It helps to be confident enough that you'll find a solution to the problem you're attacking
- The really great work in offense demolishes things that people thought secure
- The very act of publishing weaknesses in software is bold, and in the early days, controversial
- Lockpicking is still very controversial
- Other industries haven't grown up this way; for example, bringing up bumping with a locksmith isn't likely to lead to interesting conversation
- Ex: Einstein's theory of relativity offended many contemporary physicists

Curiousity

- To most people, computers are just a tool to do something
- They don't care how it works, only that it does
- Security experts tend to be unnaturally curious
- First about how things work
- (Next about how they can be made *not to work*)
- Ex: Feynman and the ants

Paranoia

- Call it what you will, paranoia, cautiousness, conservativeness, late adopter
- I actually think it's a good unless it stops you from doing *anything*
- How can you recommend a security measure that you yourself wouldn't take?
- Experience in actually implementing these measures is invaluable

Thoroughness

- Good security researchers are thorough
- They don't stop at the first neat thing they find
- They take the ideas and run with them
- Like finding new territory and then thoroughly mapping it out
- Ex: Yardley vs. Claude Shannon

Continual Self-Education

- Tons of security information out there
- Need to spend a lot of time "sharpening your saw"
- Oftentimes, your day job won't give you enough time
- Need to keep up with new techniques and technologies
- "If I have seen far, it is because I stood on the shoulders of giants"

Networking

- Your security-enthusiast friends can act as information filters
- Send you high-quality information you wouldn't have found otherwise
- New ideas are not just found in print but ofttimes in brains
- Every person has a unique perspective on problems
- "To many eyes, all bugs are shallow"
- Story: Leonardo and Michaelangelo in Florence in 1450

Novelty

- The reader or audience is reading to learn something new
- Shannon Entropy measures the amount of "surprise" in a data stream
- Some people call this a measure of information
- The more surprising a paper, the more "information" we have learned
- Minor tweaks to well-known things tend to make boring presentations
- Example: Euler's Formula: $e^{i*\Pi} = -1$

Other Domains

- A paper which applies knowledge from another domain to shed new light on security problems is often very interesting.
- The people who do this are modern "Rennaisance Men", being familiar with more than one field of study.
- Example: Axelson's The Base Rate Fallacy in IDS
- Example: Forrest's Biologically-Inspired Computer Immune Systems
- Example: Anderson's Game Theory applied to Covert Networks
- Example: Gutmann's application of psychology to User Interface Design

Simplicity

- In math, a shorter proof tends to be a better one
- In crypto, removing an assumption makes the proof stronger
- Software that is robust makes fewer assumptions about the environment
- In security engineering, complexity is the enemy of security
- Simpler programs mean fewer places to accidentally create vulnerabilities
- Simple solutions also tend to be more surprising

Consolidation

- Not all work has to be novel to be useful/interesting
- Survey papers summarize other people's works
- But by bringing all that information together, you save the reader time
- By bringing obscure information to people's attention, they may still learn quite a bit
- Sometimes comparing other works side-by-side yields new insights

Practicality

- A cryptographic attack which takes more resources than are available on Earth might be of theoretical interest but not nearly as interesting as one anybody can perform with their own resources
- A strictly theoretical paper on what *could* be done is less interesting than an actual, working program that does it
- An exploit against a very rare device or program is less interesting than an exploit against very common devices or software
- A solution that requires vast or rare resources is less interesting than one which requires very little

Timelessness

- Papers which introduce a new style of attack or analysis that might be applicable to other problems tend to be more interesting
- Papers on a specific technology that won't be around very long are less interesting
- Vulnerabilities that get patched the next day tend to be less interesting than intrinsic problems without easy solutions

Solves the Right Problem

- Results which speak to the current needs of a large group of people tend to be more interesting than those which don't
- Security solutions which solve the wrong problem are less useful than those that solve the right one
- Ex: Authenticode, SET

Humor

- Simply put, people like to be entertained as they're being enlightened
- Humor almost always involves some kind of surprise
- Successful simple attacks against hard problems are often funny
- Ex: Bic pen attack against Kryptonite locks
- Ex: Mark Tobias vs. the Cliq Electro-Mechanical Locks
- Being able to laugh about things, or yourself, shows confidence and strength

Hard Work

- People who do great work tend to work really hard at it
- Hard problems call for great efforts
- Solving hard problems is more interesting than solving simple ones
- Solutions to hard problems are often ingenious, and thus interesting

Requires Redesign

- Hardly any non-trivial software gets written in perfect form the first time
- Just like mathematical proofs
- Good solutions often evolve from earlier, weaker solutions
- Writing and making good presentations often means rewriting them

Can Borrow

- Nobody can invent everything from scratch
- Everyone builds on other people's work, using their ideas
- But you have to do enough novel work that it's not just a minor improvement
- "Good artists copy, but great artists steal"

Utility

- Good research is *useful*
- In academic circles, rough measure is number of citations
- In blogs, one can count linkbacks
- On web pages, you can count referrers or hits

For Further Reading I


P. Graham.
Taste for Makers.
http://www.paulgraham.com/taste.html