Common Reasoning Errors in Security

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity
htttp://rbsekurity.com

There are a number of classic fallacies in reasoning and in debating issues that can negatively impact security. Avoiding these logical errors can help with clarity of thought as well as increase our objectivity.

Some of these fallacies include:

Argument from Consequences Fallacy: This is where bad consequences of a certain course of action are assumed. The consequences may be likely or not, but in any case, they do not speak directly to the merits of the proposed action. Often used in politics.

Common examples in security: (1) It would be very bad if we had security vulnerabilities so therefore we do not. (2) Critics of election security reform use this kind of false argument, claiming that any discussion of election security vulnerabilities undermines faith in democracy. (3) Control often gets confused with Security.

Appeal to Fear Fallacy: This is warning of a bad consequence for which there is insufficient evidence.

Common example in security: Security sales pitches.

Slippery Slope Fallacy: Discrediting an idea by arguing that its acceptance will lead to a series of events that are undesirable. This fallacy typically assumes that the envisioned events are inevitable, even though no evidence is offered. It is related to the Appeal to Fear Fallacy.

Common example in security: Ironically, this fallacy is often used by people on both sides of the argument about the alleged need for greater national security versus the potential negative impact on privacy, civil liberties, and adherence to the Bill of Rights.

Straw Man Fallacy: This involves misrepresenting an idea as something more ludicrous than the actual idea. Often used in politics.

Common example in security: Frequently used to argue against a potential new countermeasure or change in security.

Appeal to Irrelevant Authority Fallacy: The views of those who are not credible experts on the subject are cited as strong evidence.

Common examples in security: (1) The sales guy says this security product is really good. (2) This security product or strategy is used a lot by _____ so therefore we need to use it, too. (3) This security product is high-tech so it must be good. (4) The engineers can't figure out how to defeat this security device so it must be good. (In fact, however, engineers typically have the wrong mindset and experience to perform effective vulnerability assessments.)

Equivocation Fallacy: This involves changing the meaning of a word. The new meaning is then used to reason or argue a wrong conclusion. This type of argument is used by lawyers all the time.

Common examples in security: (1) Vulnerabilities often get confused with threats, assets needing protection, and facility features. (2) Vulnerability assessments are often confused with threat assessments, security surveys, compliance auditing, performance testing, pen(etration) testing, and "Red Teaming". (3) Measurements of inventory are often confused with security measures, even when they make no significant effort to counter spoofing. (4) Calling a security product "high security" when that is the intended application, but not an attribute of the product.

False Dilemma (Black & White or False Dichotomy) Fallacy: Only 2 possibilities are presented with no others allowed, including shades of gray.

Common examples in security: (1) Security is often thought of as binary—we are secure or we are not. In reality, security is a continuum. The idea of "gap analysis" unfortunately plays to this binary mindset. (2) We hired a convicted criminal, gave him a crowbar, and he couldn't defeat the security device. Therefore, the device is undefeatable.

Not a Cause for a Cause Fallacy: Assuming a cause for an event when there is no evidence for such a thing. There are actually 2 kinds: correlation getting confused with causation, and *post hoc, ergo propter hoc,* which is an event preceding another event that is incorrectly thought to be the cause of that second event.

Common examples in security: (1) There were no serious security incidents recently so that must mean our security is working. (2) Scapegoating after security incidents.

Hasty Generalization Fallacy: Conclusions are drawn from too small or specialized a sample.

Common examples in security: (1) We can't immediately identify any obvious vulnerabilities. Therefore there are none and our security is excellent. (2) We did a Red Team exercise "testing" one specific attack so we therefore fully understand our security vulnerabilities.

Appeal to Ignorance Fallacy: A proposition is claimed to be true because there is no evidence it is false. Absence of evidence is incorrectly taken to be evidence of absence. A special version of this fallacy is Argument From Personal Incredulity—I can't see how this proposition can be true so this means it is false.

Common examples in security: (1) I've seen no evidence that this security device or program can be defeated; therefore it cannot be. (2) I (a non-expert) can't envision how to defeat this security (especially since I don't want to) so therefore nobody can.

Circular Reasoning Fallacy: A kind of begging the question where we assume the conclusion is one of the premises. Often the conclusion is reworded to disguise it. "You are wrong because you are not making any sense" is an example.

Common example in security: We've had no tampering because no tampered seals were discovered. (The flaw in the argument, however, is that—by definition—defeated seals are not detected.)

No True Scotsman Fallacy: After a general claim about a group of things, a counter example is found. Then, that thing is declared not part of the group or not a "true" member. This fallacy is related to the Circular Reasoning Fallacy. (The name of the fallacy comes from the idea that no "true" Scotsman would ever say or do a certain thing, so that if a given gentleman does, he cannot therefore be a true Scotsman even if he is a Scotsman.)

Common example in security: That attack was demonstrated on Thursday but today is Tuesday. Therefore, the attack isn't viable today.

Genetic (Questioning Motives) Fallacy: An idea or proposition is devalued or defended solely based on its source or origins.

Common examples in security: (1) The motives and loyalty of vulnerability assessors or stakeholders who ask questions about security are questioned as a way of rejecting their concerns. (2) The higher ups made this security rule so it must be a good idea.

Guilt by Association Fallacy: Discrediting an idea solely because it is held by a demonized group. This is a kind of *non sequitur*. It falsely assumes that accepting the idea would make one automatically part of the demonized group.

Common example in security: They use these tactics in Russia, China, or Iran, so therefore we should not.

Affirming the Consequent (Converse) Fallacy: We know that "if A, then C" is true. We know that C is true. Therefore, A is true. This is false reasoning.

Common examples in security: (1) If we treat our employees well, they will be less likely to engage in insider attacks. We haven't detected any insider attacks. Therefore, we are treating our employees well. (2) If we have no adversaries, we won't be attacked. We haven't been attacked recently. Therefore, we have no adversaries.

Appeal to Hypocrisy (*Tu Quoque* = "You Too") Fallacy: Claiming that an advocate for a given idea or proposition has shown past inconsistency in thought, argument, or deed. This diverts attention from the truth or falsehood of the idea or proposition in question. Often used in politics.

Common example in security: This security manager was once a strong proponent of using contract guards but now uses proprietary guards, so her views on security awareness training are highly suspect.

Appeal to the Bandwagon (Appeal to the People) Fallacy: If a lot of people believe in something, it must be true.

Common examples in security: (1) Nobody else seems to be worried about these kinds of attacks, so we shouldn't be either. (2) The government and the police uses polygraphs a lot so they must be valid.

***Ad Hominem* ("To the Man") Argument Fallacy:** Attack the proponent of an idea (including his qualifications and assumed motivation), rather than the idea itself.

Common example in security: This argument is often used to discredit vulnerability assessors, security critics, and those proposing unconventional security strategies.

Composition Fallacy: Because part of a whole has an attribute, the whole must, too.

Common examples in security: (1) We encrypt or digitally authenticate the data so that rules out theft or tampering. (2) Because we use good locks, we must have good security overall. (3) The security device uses a lock, a seal, a mechanical tamper switch, or "tamper proof" screws, therefore it cannot be tampered with.

Division Fallacy: One part of a whole must have a certain attribute because the whole does.

Common examples in security: (1) Our security has held up well. Therefore, all parts are fully optimized. (2) We use layered security ("defense in depth"). Therefore, the effectiveness of any given layer isn't of concern.

Cognitive Dissonance Fallacy: Our reasoning is negatively impacted by the mental tension generated by ideas or facts we do not wish to be true or to contemplate. Cognitive dissonance is probably the main cause of bad security across a wide range of security applications. This can lead to Security Theater; wishful thinking; denial and wishful ignorance (deliberately avoiding facing the facts); stagnation/paralysis (not addressing problems); self justification (self-serving rationalization and excuse making); confirmation bias and motivated reasoning (incorrectly interpreting data in ways that make us feel good); and invoking any number of the above fallacies.

Common examples in security: (1) We have no serious vulnerabilities. (2) Our employees are too loyal to attack. (3) HR says we have an effective employee complaint/grievance process.

Fallacy of Precision: The belief that assigning a numeric value to something means we have a full understanding of it, or that semi-arbitrarily assigned numbers impart rigor.

Common examples in security: (1) Believing uncritically in risk probabilities that are often only semi-educated guesses, old news about the past, or just wishful thinking. (2) Hiring one candidate over another because he/she has a slightly higher GPA three digits right of the decimal even though the candidates attended different schools, studied different subjects, took courses with varying degrees of difficulty, and had completely different teachers/professors.

The more you can recognize and avoid these reasoning and argument errors, the better your security is likely to be!

About the Author

Roger G. Johnston, Ph.D., CPP is CEO and Chief Vulnerability Wrangler at Right Brain Sekurity, a company devoted to security consulting and vulnerability assessments. He previously was head of the Vulnerability Assessment Teams at Los Alamos and Argonne National Laboratories (1992-2007 and 2007-2015).