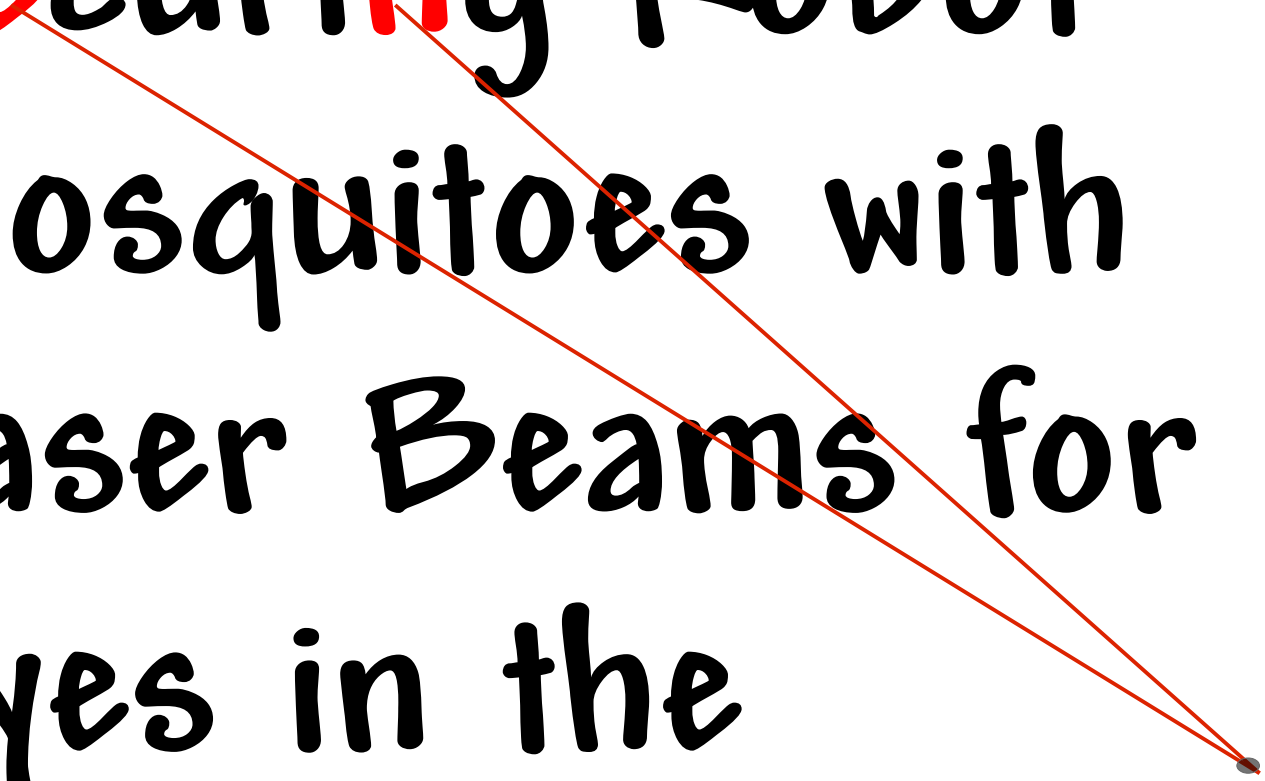
Securing Robot Mosquitoes with Laser Beams for Eyes in the Enterprise.



by Pete Herzog

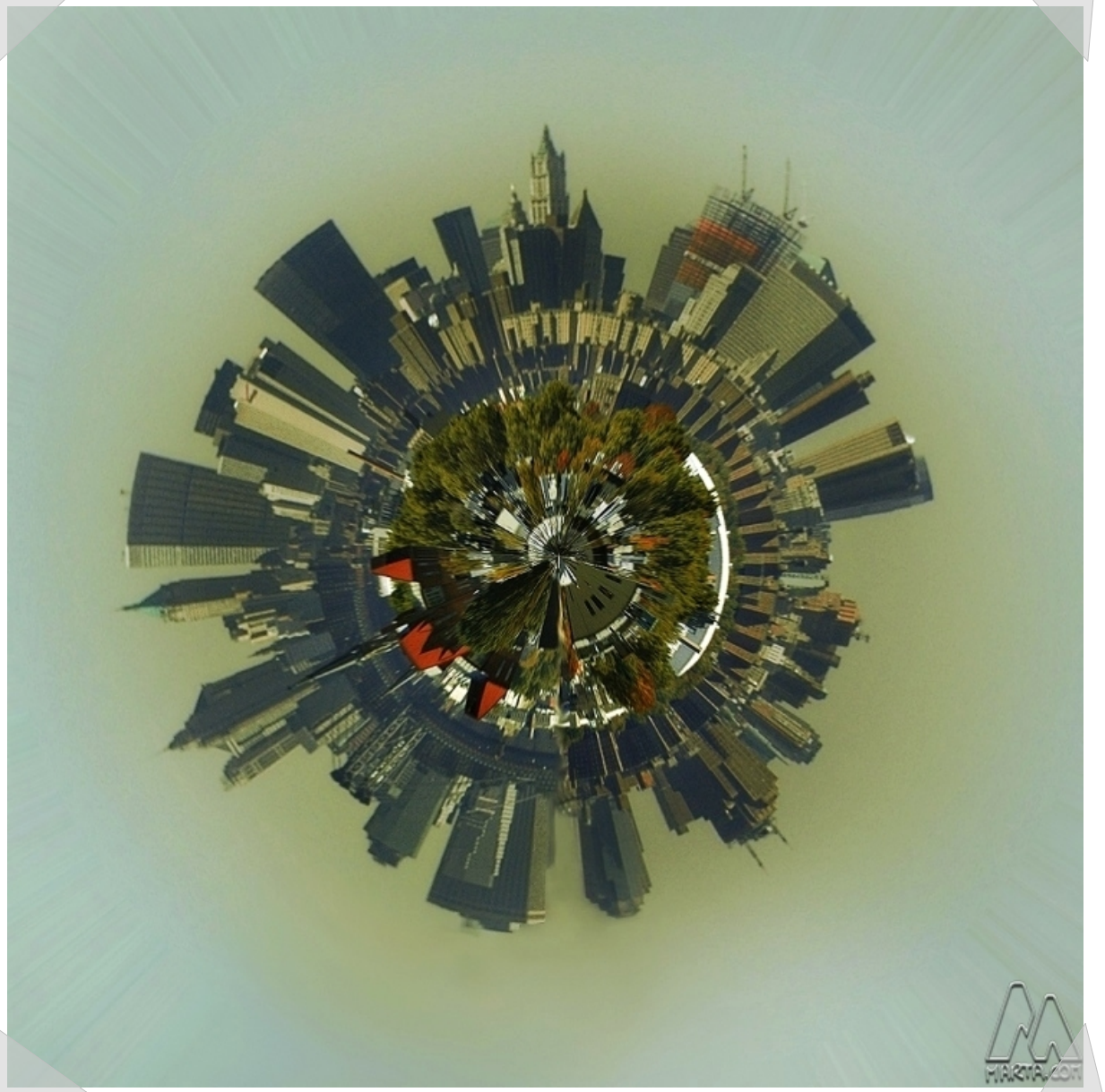
OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

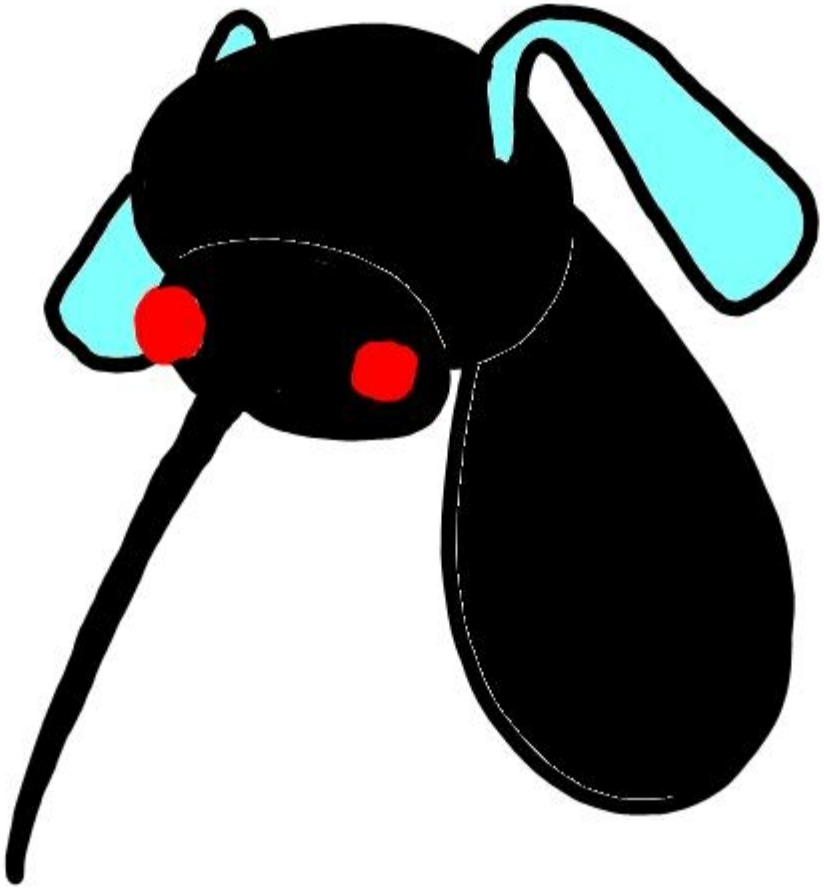
Presentation Creator:

- Pete Herzog
- Co-founder and Managing Director of ISECOM
- OSSTMM Creator and Project Lead
- Other stuff
- My policy - take me to dinner and I'll give you advice.

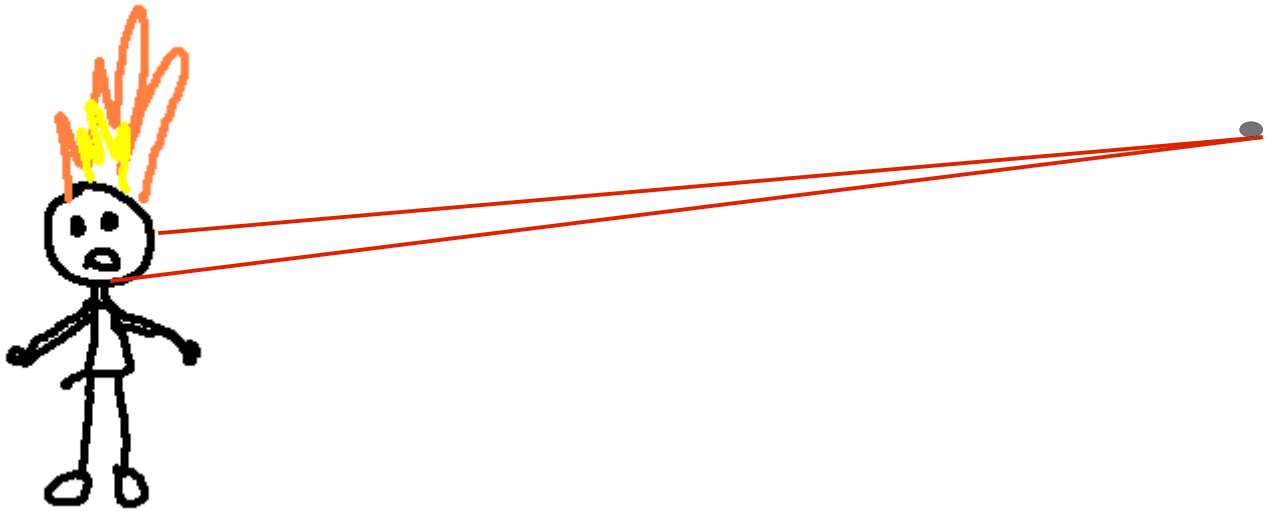
Another Reality



The Mosquito



Laserbeams for Eyes



Just a Gadget

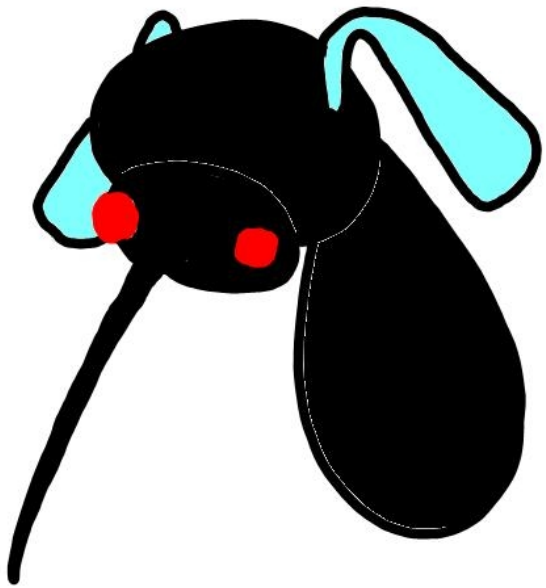
- Whispers via Bluefang and a earjack
- Flies to people in your contact list
  - Direct comms OOB audio
- Connects to wireless
  - Post to Talkbook
  - Update mumbles
  - Download updates, buy voxtones, fliht tricks
- It's new but it's already been jailbroken

How to Say Yes

- CEO and execs love them
- But they realize there could be security problems
- How do we do something about that?

What Reasons Do We Have To Trust It?

1. Size
2. Symmetry
3. Visibility
4. Subjugation
5. Consistency
6. Integrity
7. Offsets
8. Value
9. Components
10. Porosity

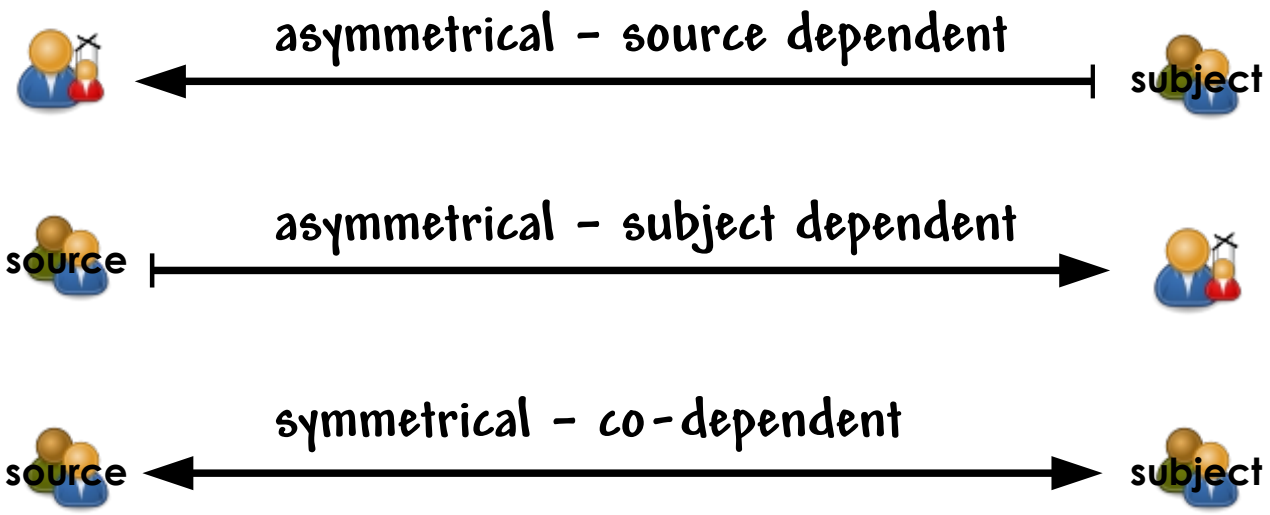


Size

- The number of subjects the trust extends to. Defines your scope on what you will test.
  - Must the trust extend to just one or to many?
  - Is the group to be a trusted one which is meant to make collective decision?
  - Does the trust rely on others such as a spouse, best friend, teammates, church members, political party members, etc. to make these kinds of decisions?
  - In effect, you may not be trusting just one person but also those who greatly influence that person.

Symmetry

- The vector (direction) of the trust.
  - Trust may be one way (asymmetrical) and defined as to which way the trust must travel or both ways (symmetrical).
  - A person who must also trust you has to consider the repercussions from breaking the trust.
  - Asymmetry allows for manipulation



Visibility

- The level of transparency of all operational parts and processes of the subject and its environment.
  - Visibility does not need to extend to you but can be openness in general, to anyone, whether anyone is watching or not. Sort of like something which is considered "public record".
  - Visibility may also be only to you, the source of the trust.
  - The subject does not need to be aware of the exposure like in Big Brother type watching through hidden surveillance cameras.
  - This equates to the amount of the real-time plans, movement, and actions of the subject you can know. Often this is limited to certain times of day like office hours or locations like at home.

Subjugation

- Subjugation, the amount of influence over the subject by the source.
  - The ability to predetermine the plans and actions of the subject provides an unparalleled amount of predictability.
  - The amount of control a source can exert over a subject is often restricted to certain time periods where roles are in effect like a boss and an employee or a guard over a prisoner.
  - However entitlement of control is NOT control. The amount of control during real operations is what must be evaluated and not just the possibility. The source may not be able to exert control or the subject may be especially resistant to control.

Consistency

- A historical evidence of compromise or corruption of the subject.
  - This is the typical background check. What the subject did in the past can be indicative of the future.
  - How often in the past has the subject broken a trust?
  - The subject's past, good or bad, should influence your reason to trust it or them.
  - Look at the number of problems and also the number of successes.
  - Consider not just the total but the time in between the frequency- are they recent or old? Are they sporadic or consistent, possibly marked by specific, justifiable events.

Integrity

- The amount and timely notice of change within the target.
  - Everyone and everything changes. How can you know when those changes happen?
  - Systems, people, processes, may all have key indicators that a change has taken place. Can you identify those indicators?
  - This may fall under "anomaly detection".
  - The indicators may be indirect. Take care not to rely on change indicators from a third party like, "I know when my brother is drinking again because his wife looks like she hasn't been sleeping."

Offsets

- Offsets of sufficient assurance are the compensation paid to the source or punishment for the subject when the trust is broken. It is a value placed on the trust with the target.
  - This could be Liability Insurance carried by professionals.
  - This could also be in terms of the legal system either under the criminal code for malicious attacks on the trust or it could be private, as in breach of contract.
  - Offsets relying on the law require evidence so key indicators of this would be some type of non-repudiation controls in addition to alarm or integrity controls to allow you to prove the breach in trust has indeed occurred.

Value

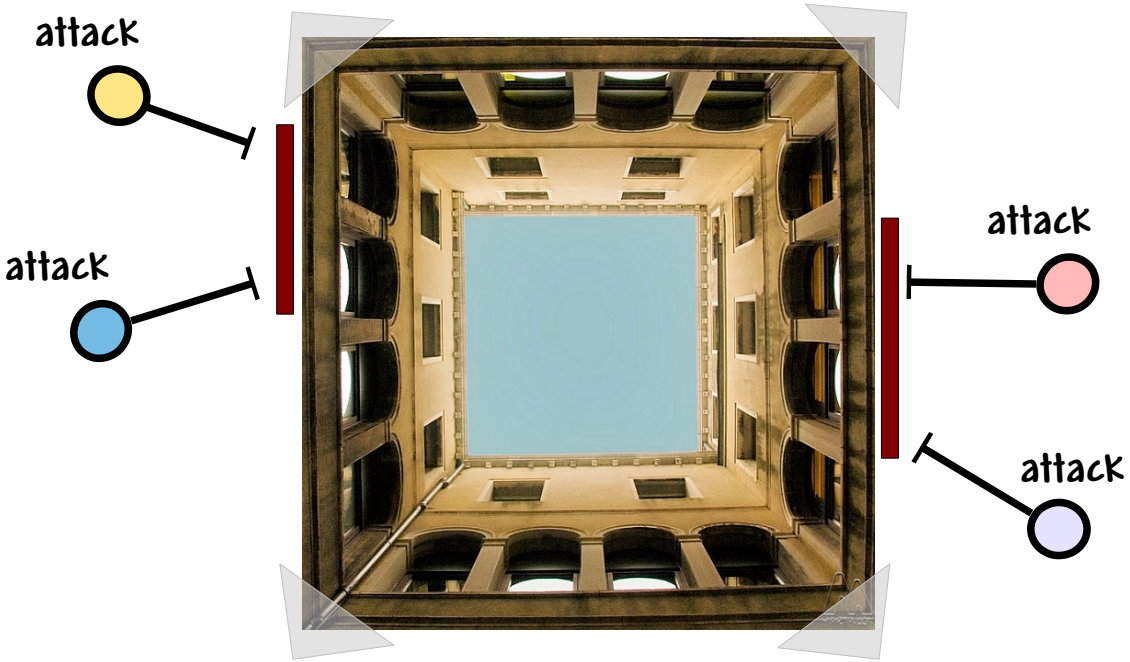
- The financial offset for risk is the amount of win or gain for the source where the potential gain for giving trust to the subject is sufficient to offset the risk of breach of trust.
  - In movies, where the bad guy offers his hand to the good guy to pull him off the ledge of the building, the hero must decide to trust the villain or to try to rescue himself. What he's doing is considering the Value of Reward. If the risk of being tricked by the villain is worth the reward of his life (or in bringing the villain with him to kill them both).
  - Stocks, mutual funds, and most any investment works on this principle and tries to prove to you that they have either low risk or potentially a huge win.

Components

- This is the number of elements which currently provide resources which the subject relies on either directly or indirectly.
  - Maybe the subject would have kept the trust had not for some interference, some need, force their hand.
  - Keep your scope small but not too narrow. It's easy to count food and water, for example, however it may not be appropriate for a reason to trust an employee. Then again the need to earn money to provide for one's family may be motivation for a new employee.
  - This is a serious issue in Trusted Computing because even though the computer may be trustworthy, the resources it receives, data, power, user-input, may not be.

Porosity

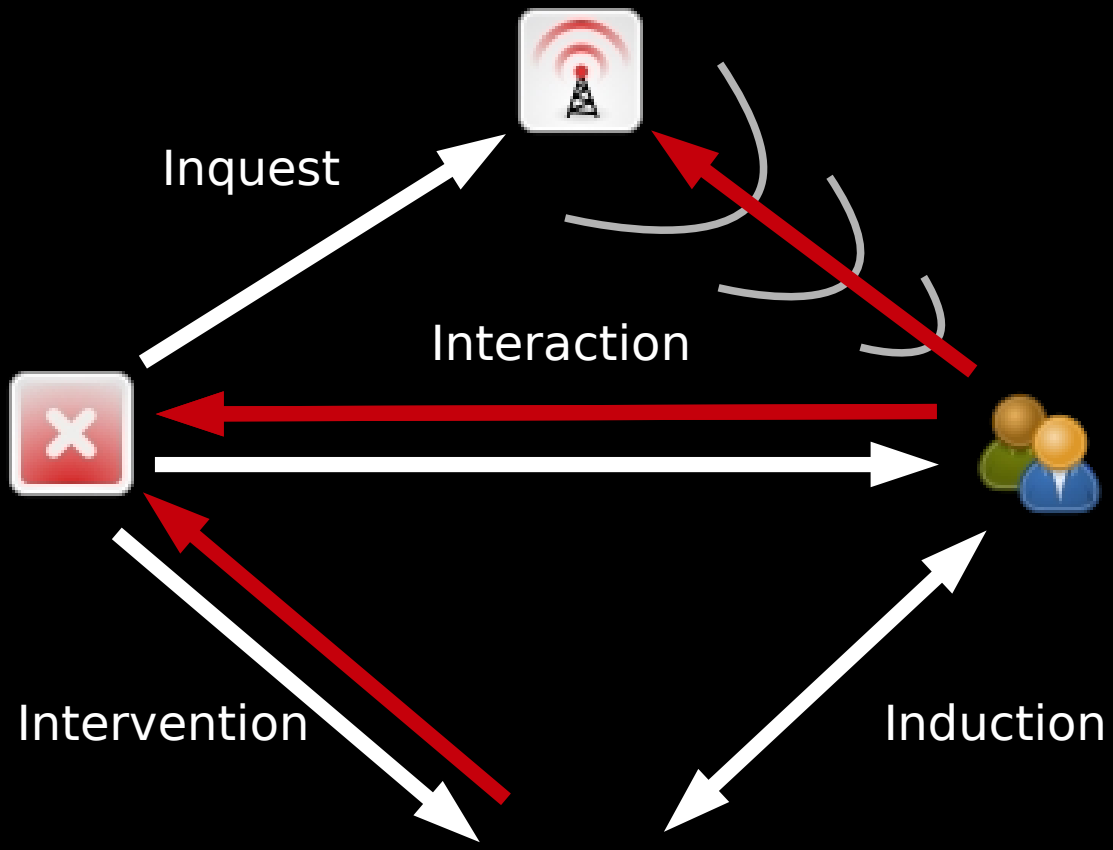
- This is the amount of separation between the subject and the external environment.



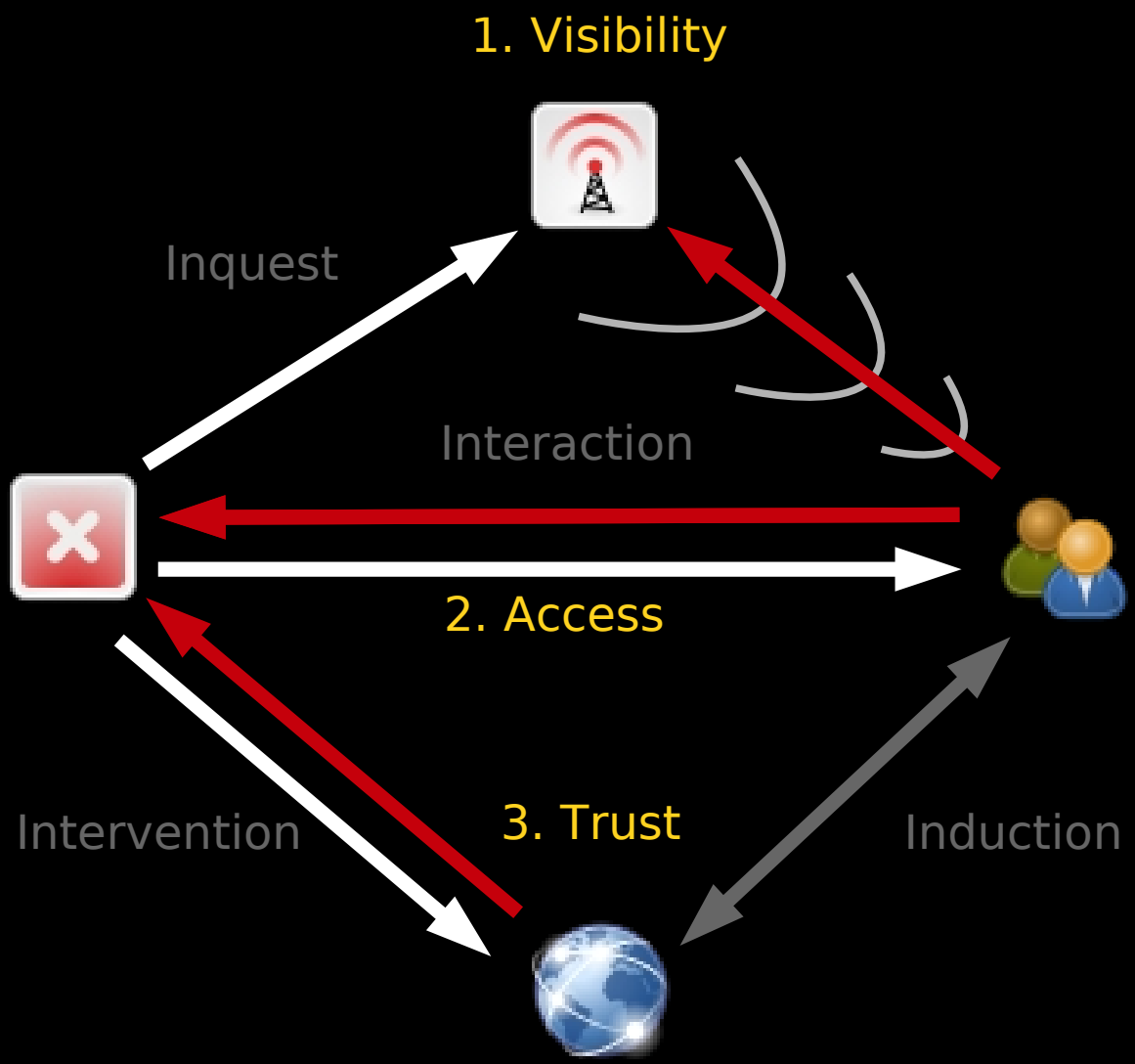
Hacking

- It's all about interactions.
- Operations.
- Figuring out how to change the operations in the way that you want.
- Knowing how it works better than the people who designed it.

It's About Interactions



Interactions Are Operational Holes



Operational Controls

- The 10 operational controls which make assets safer are divided into two categories:
  - Interactive
  - Process
- Furthermore, there are 2 non-operational controls which make up one of the Interactive Controls, Authentication:
  - Identification
  - Authorization
- These controls cannot be expressed operationally because they cannot be transferred.

Controlling the Threat

- It is the means to mitigate attacks which occur through operations.
- To make an asset safe, you need to identify and then control the threat as it appears.
- Often times controls have limitations which make them less effective.
- More controls also may increase your Attack Surface.

Interactive Controls

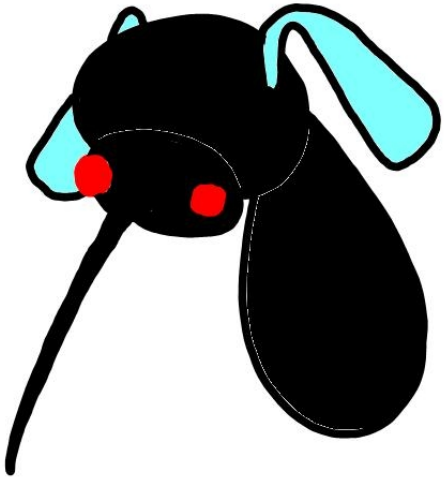
- These are controls which can directly affect interaction with Visibility, Access, or Trust.
- These include:
  - Authentication (includes Identification and Authorization)
  - Indemnification
  - Subjugation
  - Continuity
  - Resilience

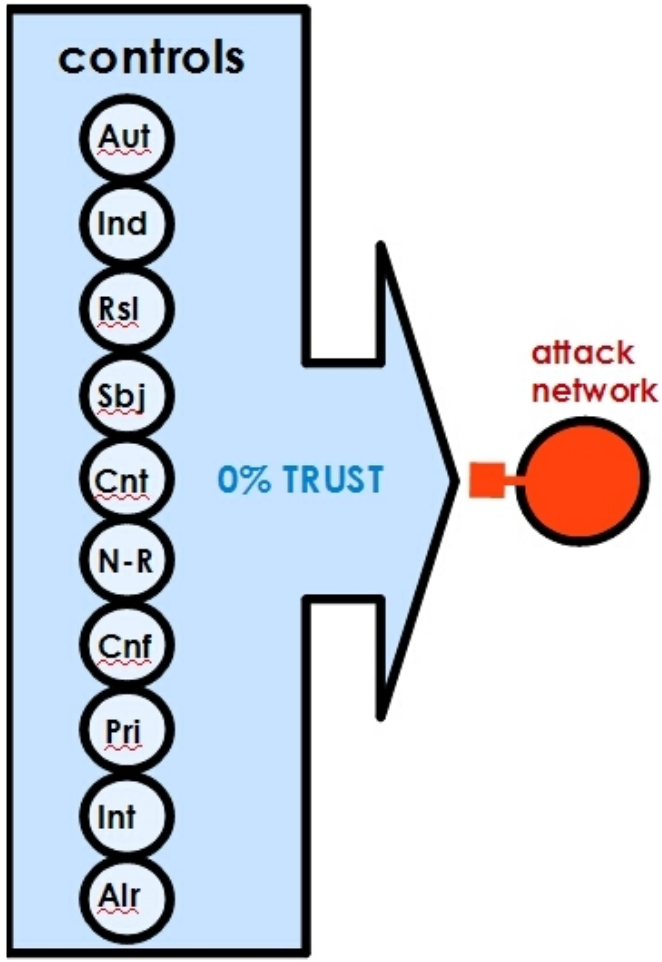
Process Controls

- These are controls which are used to protect assets once the threat is already present.
- These include:
  - Non-repudiation
  - Confidentiality
  - Privacy
  - Integrity
  - Alarm

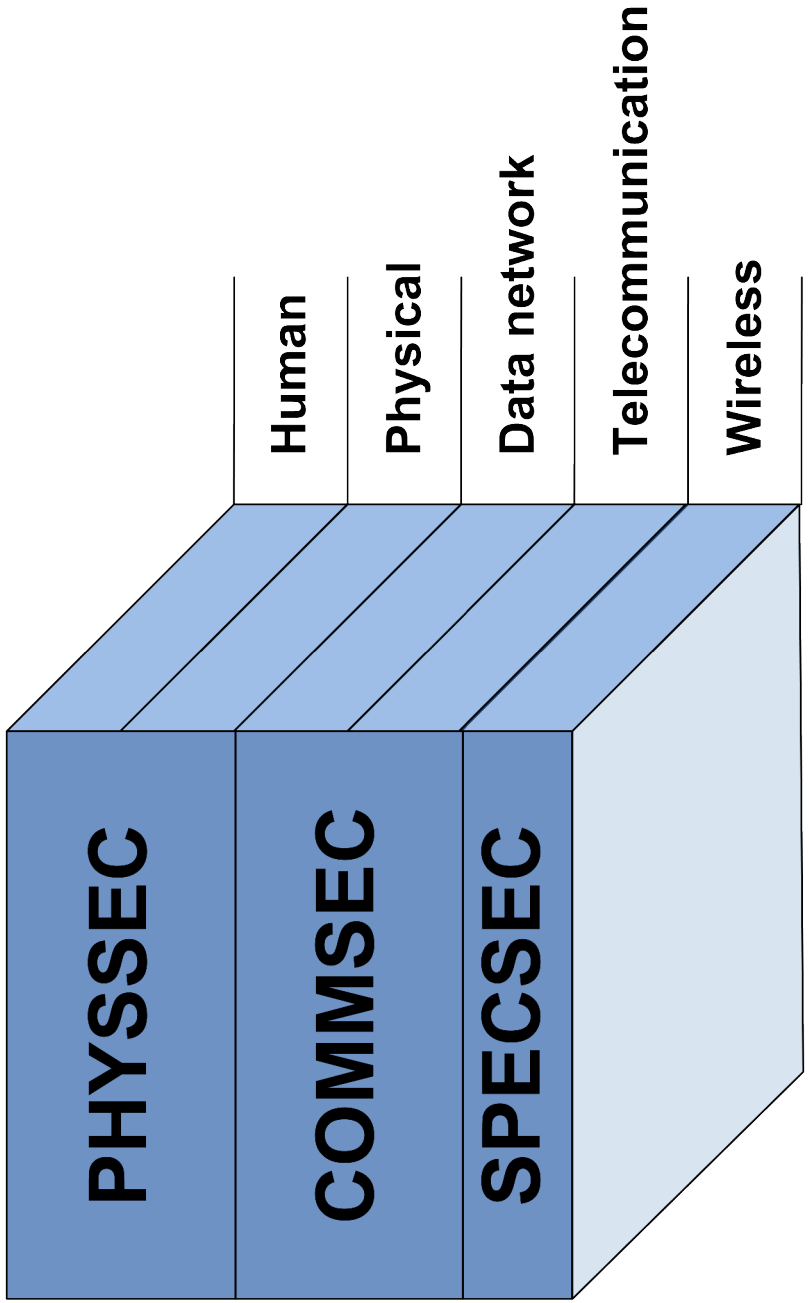
Look for Controls

- The 10 Operational Controls



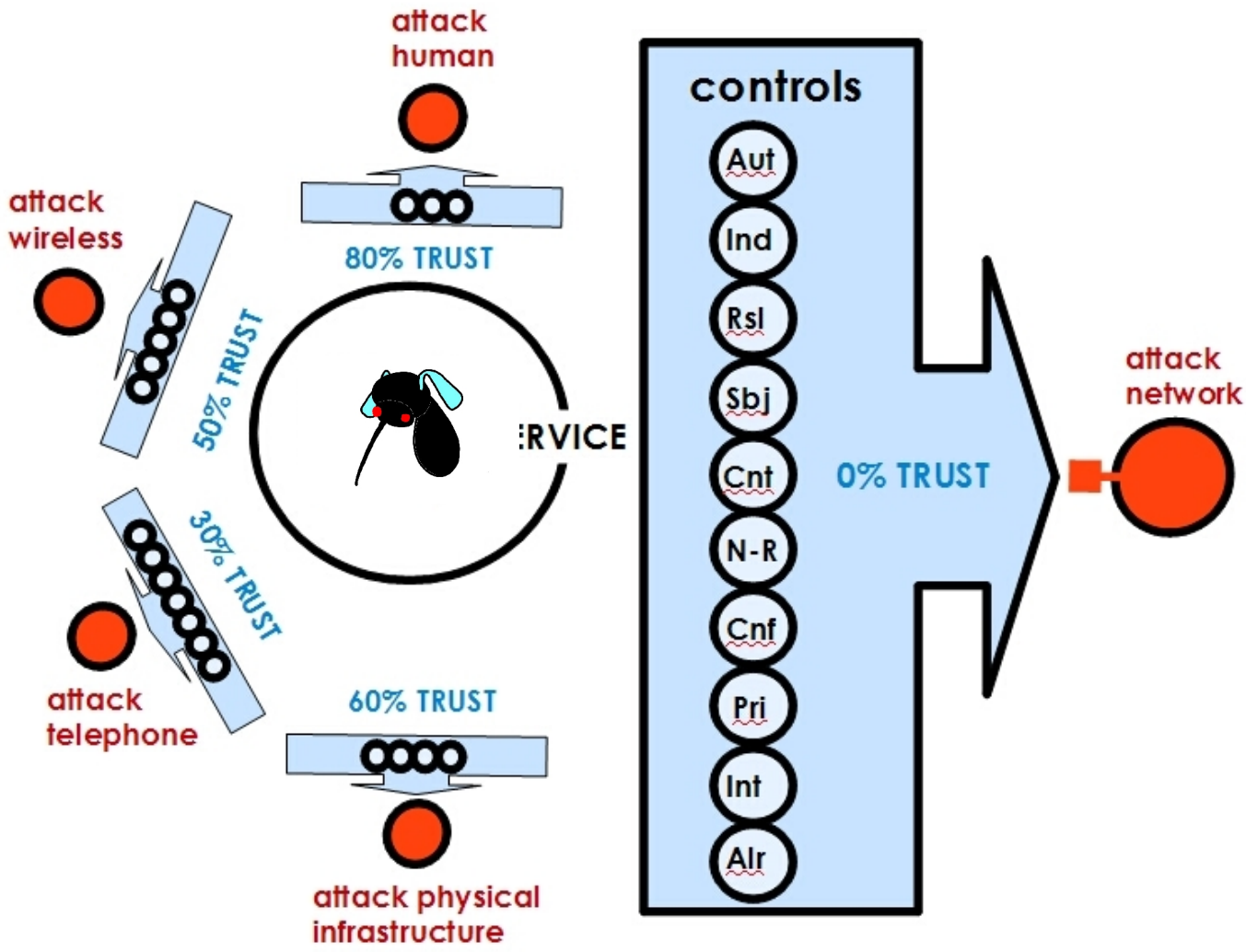


Channels

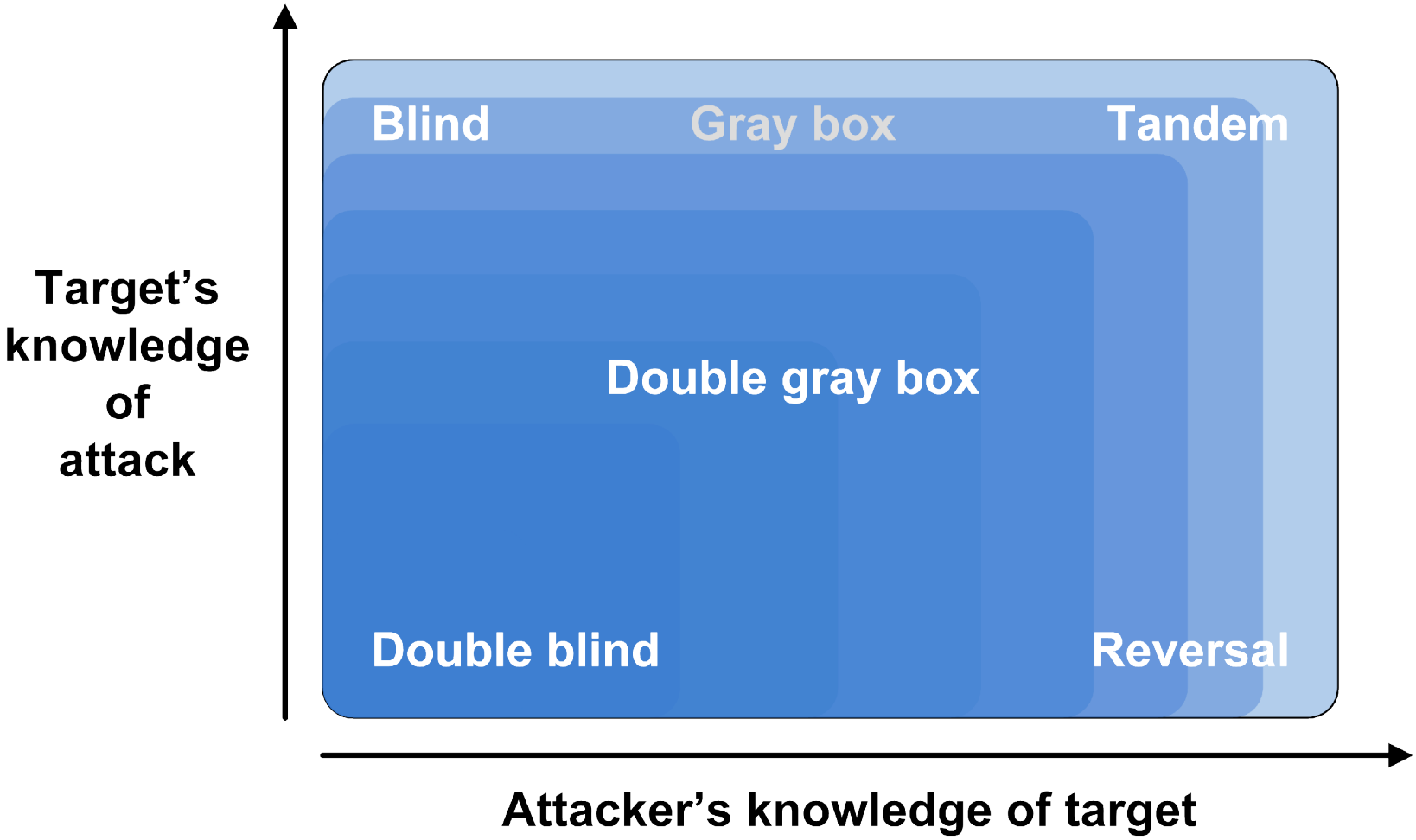


Operational Security / OPSEC

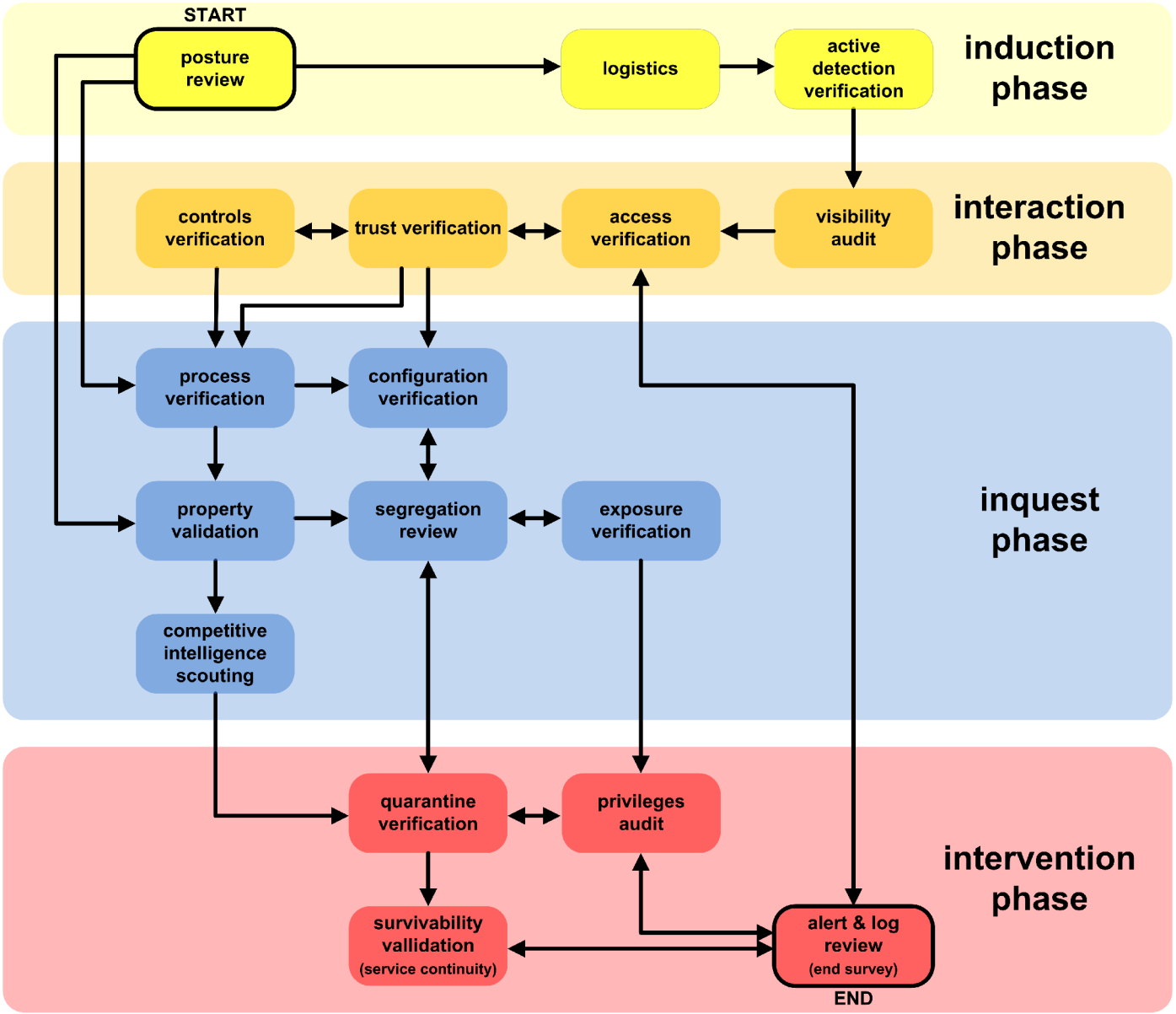
Channels


attack human
attack wireless
80% TRUST
50% TRUST
:RVICE
30% TRUST
attack telephone
60% TRUST
attack physical infrastructure
controls
Aut
Ind
Rsl
Sbj
Cnt
N-R
Cnf
Pri
Int
Air
0% TRUST
attack network

Test Types


Blind
Gray box
Tandem
Double gray box
Double blind
Reversal
Target's knowledge of attack
Attacker's knowledge of target

Testing


START
posture review
logistics
active detection verification
induction phase
controls verification
trust verification
access verification
visibility audit
interaction phase
process verification
configuration verification
property validation
segregation review
exposure verification
competitive intelligence scouting
inquest phase
quarantine verification
privileges audit
survivability vallidation
(service continuity)
alert & log review
(end survey)
END
intervention phase

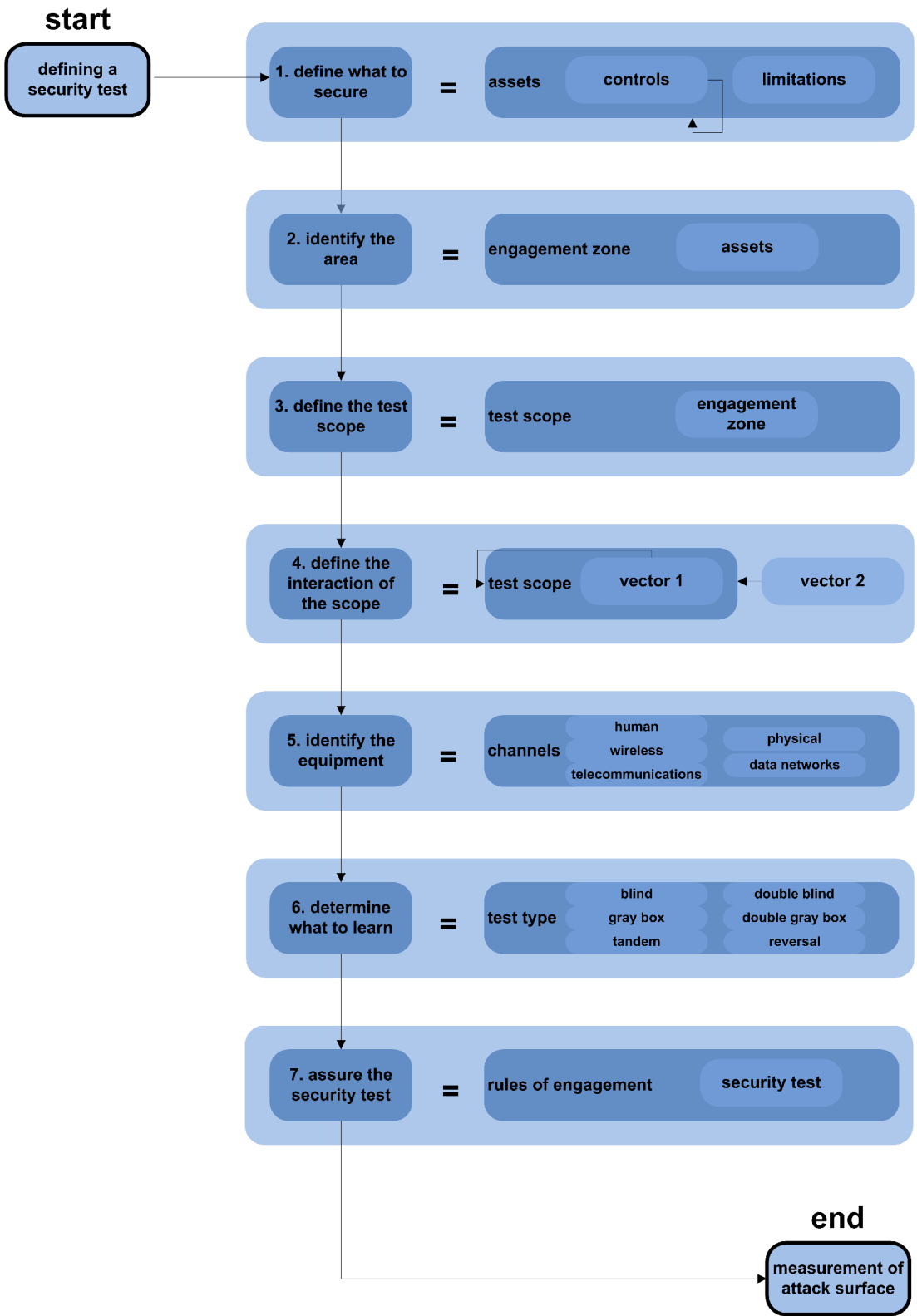
Follow the Methodology

Configuration Verification

Test to gather all information, technical and non-technical, on how assets are intended to work, and to examine the ability to circumvent or disrupt functional security in assets, exploiting improper configuration or programming of access controls, loss controls, and applications.

- Input Validation and Parameter Manipulation
  - Fuzz all application entry points that have been mapped during the Visibility Audit, including including URLs, query strings, GET parameters, POST data, HTTP cookies, HTTP headers, web services, and user-controllable out of band channels such as SMTP and possibly FTP.
  - Test for Reflected and Stored Cross-Site Scripting (XSS).
  - Test for HTML injection.
  - Test for HTTP header injection.
  - Test for SQL injection.
  - Test for OS command injection.
  - Test for LDAP injection.
  - Test for XPath injection.
  - Test for SOAP injection.
  - Test for SMTP injection.
  - Test for DOM-based attacks.
  - Test for Open Redirect vulnerabilities.
  - Test for path traversal vulnerabilities.
  - Test for local and remote file inclusion vulnerabilities.
  - Test for common software flaws (buffer overflows, integer bugs, format strings, etc.).
- Configuration Management
  - Perform a full port scan on web servers and application servers to identify any administrative interfaces running on a different port than the target applications, and verify the presence of default or otherwise predictable authentication credentials

Once-Over-Again



OSSTMM 3

The Open Source Security Testing Methodology Manual

Contemporary Security Testing and Analysis

Created by Pete Herzog

Developed by ISECOM

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Attack Surface Security Metrics

RAV version 3.0 – OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 for more information.

OPSEC	
Visibility	1
Access	2
Trust	54
Total (Porosity)	0

CONTROLS		
Class A		Missing
Authentication	12	0
Indemnification	15	0
Resilience	4	0
Subjugation	1	0
Continuity	2	0
Total Class A	54	0

Class B		Missing
Non-Repudiation	3	0
Confidentiality	23	0
Privacy	6	0
Integrity	4	0
Alarm	1	0
Total Class B	76	0

		Missing
Total	0	0
Whole Coverage	0.00%	0.00%

LIMITATIONS		Value	Total Value
Vulnerabilities	4	0.000000	0
Weaknesses	1	0.000000	0
Concerns	2	0.000000	0
Exposures	5	0.000000	0
Anomalies	10	0.000000	0
Total # Limitations	110		0.0000

Δ OPSEC	0.000000
Δ True Controls	0.000000
Δ Full Controls	0.000000
True Coverage A	0.00%
True Coverage B	0.00%
Total True Coverage	0.00%
Δ Limitations	0.000000
Attack Surface	0.00
Protected Surface	100.00

Actual Security: 100.00

STAR

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Report ID		Date	
Lead Auditor		Test Date Duration	
Scope and Index		Vectors	
Channels		Test Type	

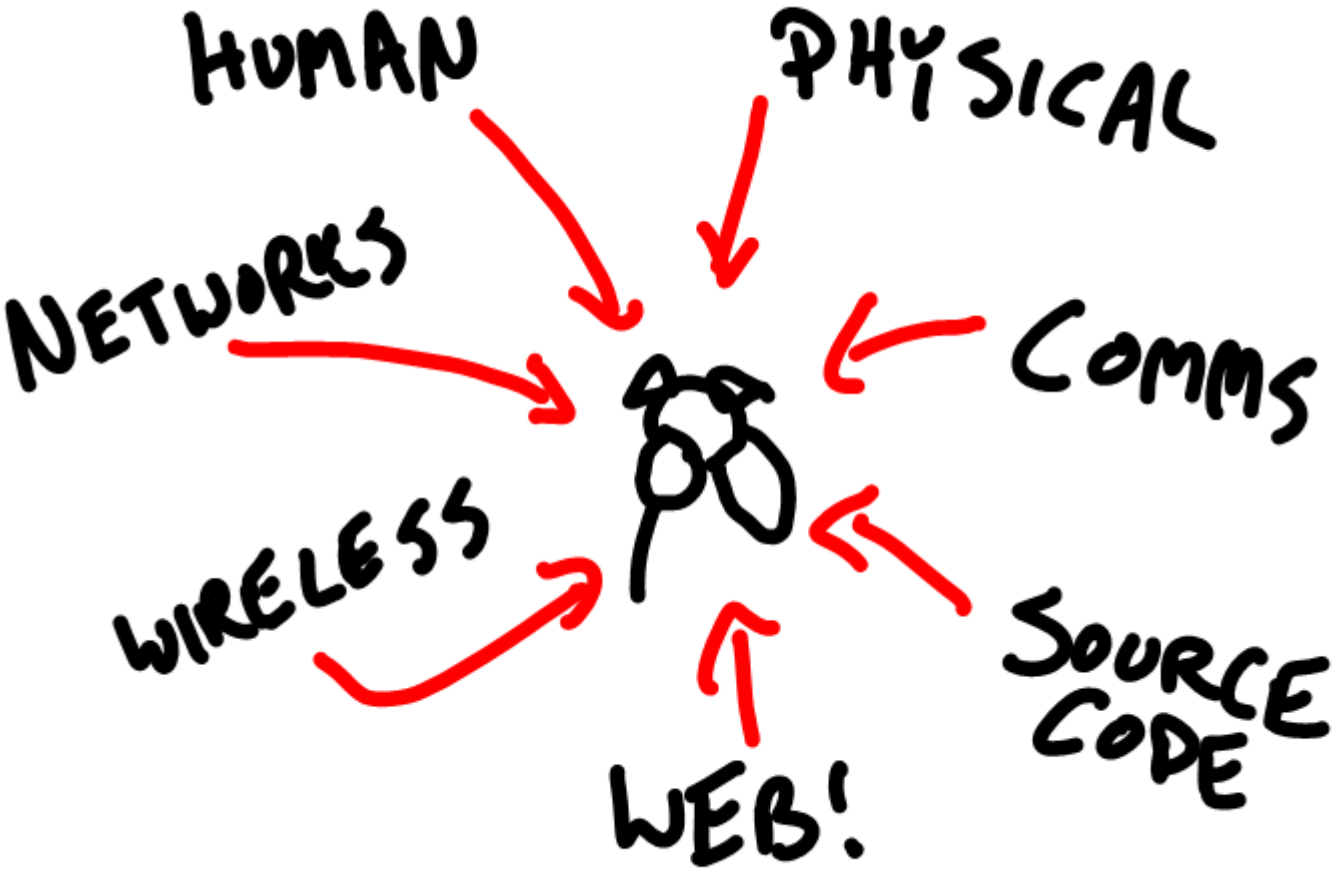
I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE	COMPANY STAMP/SEAL

ISECOM Certification #		ISECOM Certification #	

OPERATIONAL SECURITY VALUES		CONTROLS VALUES	
Visibility		Authentication	
Access		Indemnification	
Trust		Resilience	
		Subjugation	
LIMITATIONS VALUES		Continuity	
Vulnerability		Non-Repudiation	
Weakness		Confidentiality	
Concern		Privacy	
Exposure		Integrity	
Anomaly		Alarm	
OpSec		True Controls	
Limitations		Security Δ	
True Protection		**Actual Security**	

Customized Methodology



Questions?!