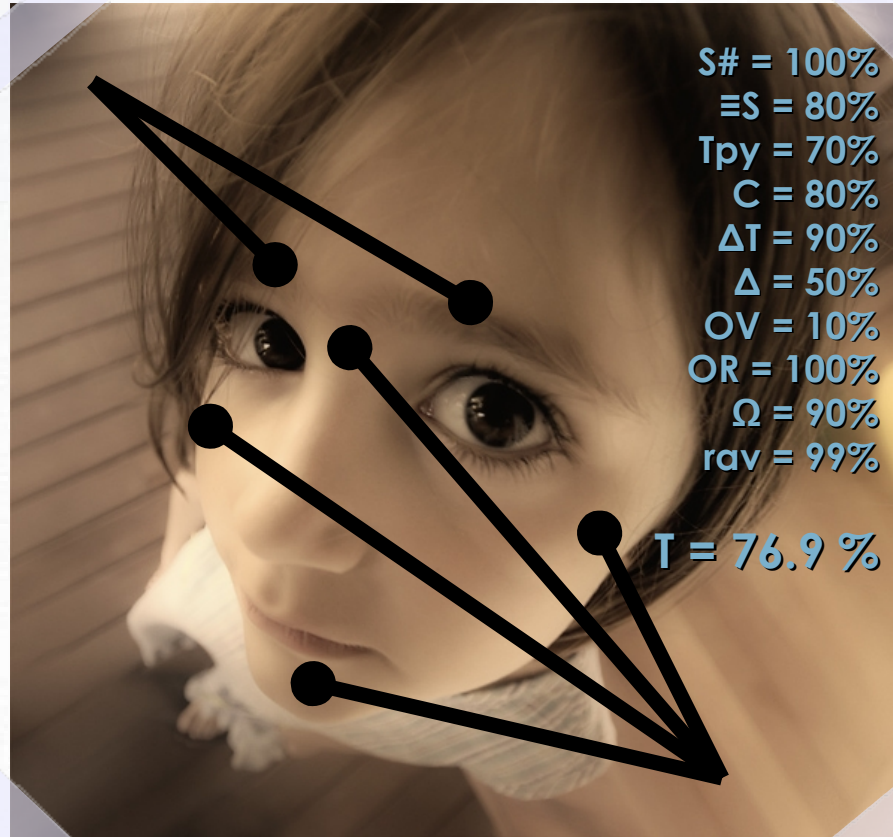


Smarter·Safer·Better



Mastering Trust

If you could take a pill which would **make you trust** everyone and everything much more, would you?



If you could take a pill which would **make you appear more trustworthy** to everyone and everything, would you?



Should We Trust More?

- Almost all people asked if they would take a pill to be more trusting clearly stated they would NOT want to take such a pill for fear of being used or abused.
 - One person said they would gladly take it if everyone else had to take it too.
- Almost all people asked if they would want to appear more trustworthy clearly stated YES they would take the pill as it would make life easier.
 - One person said it would make life easier mostly because it would be easier to lie to people as they would only expect the truth.

Mastering Trust Today

- You will learn how to analyze trust.
- You will learn how to make better trust decisions.
- You will practice this skill.
- You will master operational trust.
- Contact me later via www.isecom.org to take the Certified Trust Analyst course or certification exam.



What is Trust Analysis?

- The use of logic and reason to make a trust decision.
- It is a new practice originally developed to explore operational trust.
- Operational trust is new research from ISECOM for the OSSTMM 3 and is defined as "Each relationship that exists where the target accepts interaction freely from another target within the scope."
 - OSSTMM 3 describes all the ways one can try to thoroughly infiltrate or destroy any person, place, process, or communication type, hence the terminology "target" and "scope".
 - Further developed into the OSSTMM 3's "Möbius Defense" which significantly improves security by focusing defenses on changes in trusts rather than changes in threats.

Who Do You Trust?

- Take a moment to write out the answers to these questions. You will be revisiting them throughout the class.
 1. Write down the name of a family member, colleague, teammate, spouse, or other adult person you trust.
 2. What reasons do you have for trusting that person?
 3. What don't you trust that person with (such as to save money, to keep a secret, to keep cool during a stressful situation, to be respectful, to tell the truth, to be there when you need them, and so on.)
 4. Write down any specific incidents where that person has EVER broken your trust, no matter how small.
 5. What changes could that person make to better gain more trust from you?

How Do You Trust?

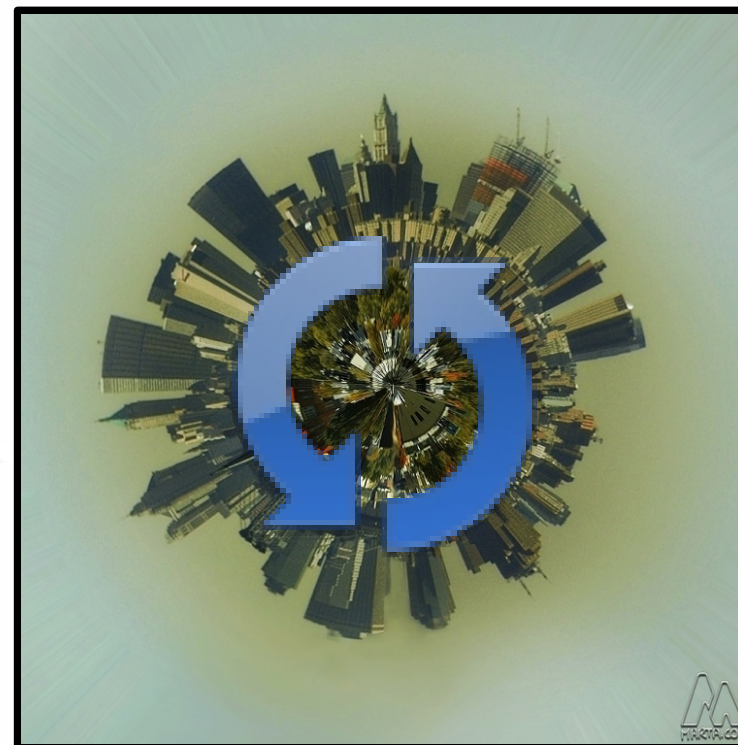
- Which one of the following fits your opinion of trust best?
 - A) I don't trust anyone or anything right away because trust is something earned over time.
 - B) I trust first but if that trust is broken, it's really hard for it to be repaired again, if ever.
 - C) I weigh the options I have and trust only if I need to, if it benefits me or the situation.
 - D) I trust based loosely on expected outcomes for a given scenario based on personal and public experience.
 - E) None of the above and I'll tell you why.

What Is Trust to You?

- Which one of the following fits your opinion of trust best?
 - A) Trust is a good thing that enhances relationships and makes people more connected.
 - B) Trust is a bad thing that can be used to con people and provide access to things like information through connected people who have no permission.
 - C) Trust is good for building relationships but bad for building security.
 - D) None of the above and I'll tell you why.

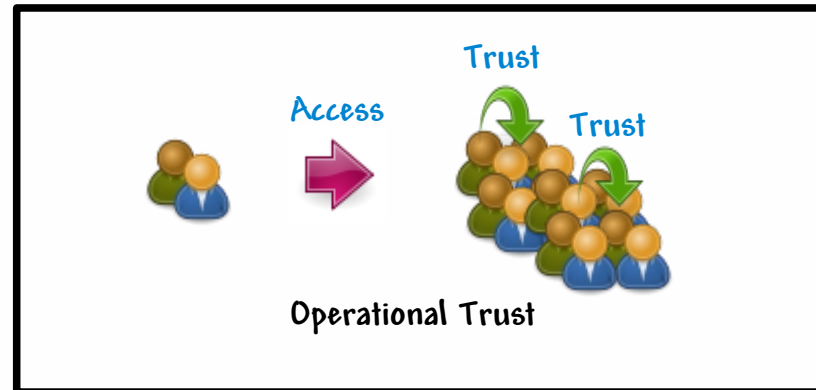
What is Trust? Is it really "reliance"?

- The Social Science definition of trust is "reliance on another person or entity".
 - However, "reliance" by definition means you don't really have a choice. In the big picture, you rely on food, water, air, and safety and the rest is just "nice to have".



What is Trust?

- Operational trust is any free interaction that another person, object, or process makes with you within your current physical or social environment.
 - Outside that current environment, interaction is an “Access” not a “Trust” because it enters your physical or social space from an uncontrolled origin.



- Operational trust is where you decide that you have a reason to trust and do so not because you need to but because you want to.

Understanding Operational Trust

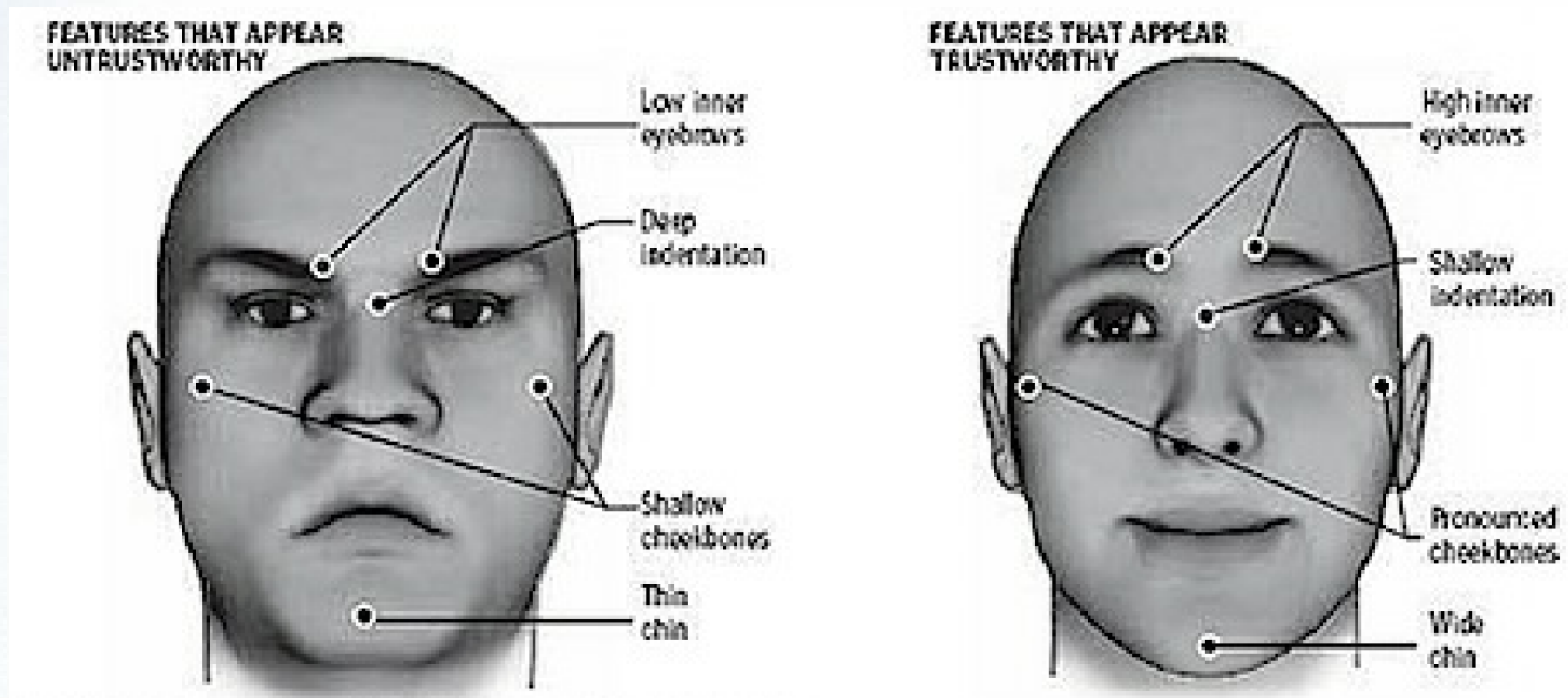
- Commonly, trust is considered a good thing to establish in operations because **it reduces the cost or resources** required to maintain security and controls.
- So when a trust is established then defenses are lowered as the interacting agent is **expected to be harmless**.
- What this means is that the trusted agent is considered secure **as long as it continues to behave as expected**.
- However, **the trusted agent can fall to an attack**, make mistakes, or unknowingly assist an attacker all without maliciousness and in no way behaving unexpected.
- This is why **trust is a hole** in operational security.

That Trusting Feeling

- Trust impacts every decision we make.
- Trust affects our relationships.
- Trust is a key component of our security and well being.
- For all its importance, most everyone still approaches trust from "the gut". **We let our bio-chemistry call the shots.**
- Do we really feel trust **like love**? Or is it something rational that can be controlled, overcome, **like a bad habit**?
- We are **hard-wired to trust** and since **it's genetic**, we know some people will be wired differently, better, worse, different. So the ability to make good trust decisions is inherent. Why?

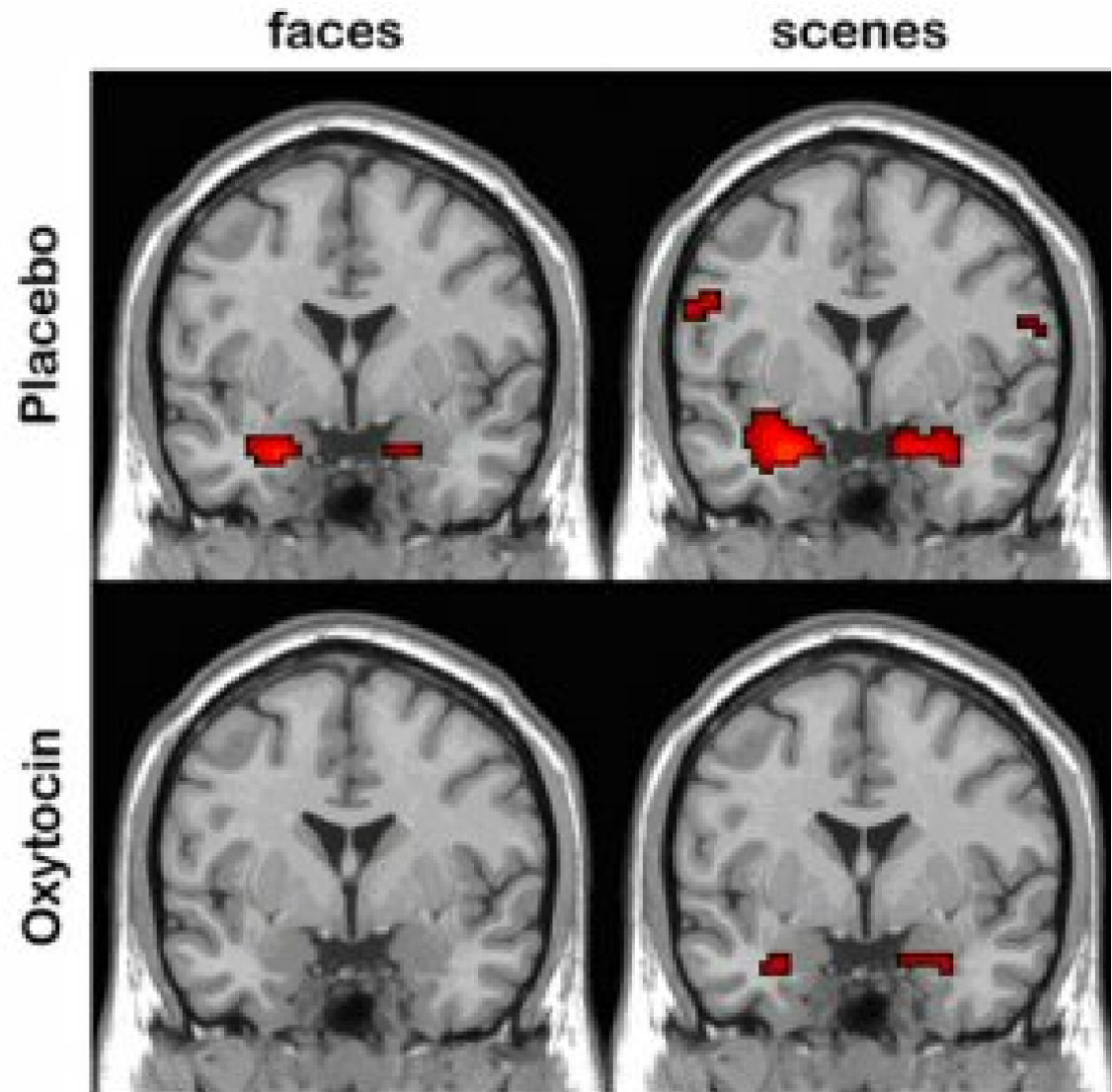
Faces of Trust

- We are hard-wired to feel trust for certain facial types and expressions.



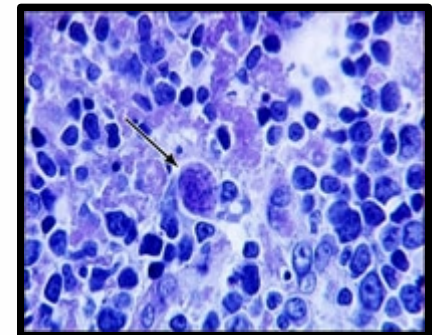
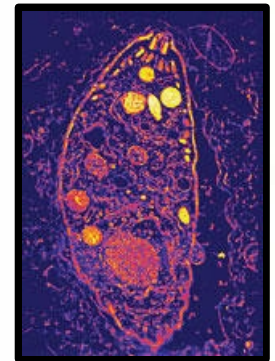
Trust Urges

- We are chemically encouraged by a hormone called Oxytocin to trust by our own bodies.
- **Brain scans show** it disrupts the fear-processing of our amygdala and brain stem making us more trusting.



Trust Sickness

- *Toxoplasma gondii*, a parasite, appears to manipulate human personality by the same adaptations that normally help it complete its life cycle between cats and rats.
- **Brain scans show** that the infected person's behavior alters so that it becomes more active and less cautious thereby affecting trust decisions.
- Infected **men are more jealous and suspicious.**
- Infected **women are more amorous and outgoing.**
- Worldwide, rates vary between 20 - 80 percent of the population, with under-developed nations being the worst affected (about 3 billion total worldwide).



Nurturing Trust



- Childhood affects how people trust.
- Environments where children are punished for showing sadness or pain attributes to a lack of trust in oneself and an increase in such emotional reliance on others (“clinginess”).
- Abuse, deep sadness from tragedy, constant fighting between parents, domestic violence, war, poverty, and parental unemployment also affect the child’s ability to trust later in life.

Trusting Science

- A recent study at Yale shows neuroscience jargon made unlikely scientific claims more believable.
- By adding the claim that “Brain scans show” even field professionals were more likely to believe strange claims that defy their field of study.
 - For example, one report said brain scan studies show watching television increases activity in the temporal lobe improving math skills. It was not true and field professionals have known that but when presented like this, the field professionals believed and trusted the information.
- Despite the irony, the studies mentioned in the seminar are indeed real however.

Perception

- There is a great deal known about trust.
- Unfortunately it's ALL about how we **perceive** trust.
- Where it applies to the inanimate, like computers, the researchers manipulate the definitions of trust to fit a predetermined result, sort of like the statistics used by advertisers and political parties.
- Currently, trust is analyzed and compared like wine tasters rate wines. The measurement of trust is biased by the perception of another human being who has been chosen to represent your needs.
- Trust is currently measured by surrogate. This is most obvious in online stores like Amazon and eBay.

Addressing the Perception of the Problem

- Therapists who work with couples who have trust issues generally deal with the perceived trust issue by the individuals and try to get to the sources of the issue.
 - These issues may be unrelated to the current trust issue and may go back to childhood issues.
 - These issues may be hormonal or bio-chemical and require medication to address.
 - The end result is addressing the perception of the trust problem which often results in acceptance of problems which one cannot control.
- But fixing operational trust issues by dealing with how it makes you feel is like fixing a broken door in your home by examining how it makes you feel.

Finding the Real Problem

- You need to know what the problem is before you can find a reason to trust or not to trust.
- Unfortunately, most of what we understand about trust is based on the perception of trust, how we feel about it. So we might not be able to identify the problem specifically.
- We hold onto illogical reasons to make trust decisions:
 - People who don't trust others are themselves untrustworthy.
 - People with eyes too close together can't be trusted.
 - You can't trust people who live like "THAT".
 - Seat belts don't matter because I knew people who were killed in accidents who had their seat belts on.
 - Hundreds of positive votes and comments for the book Twilight and only a few negative- it MUST be good!

Discovering the Trust Properties

- To find how to make logical trust decisions, we first needed to know all the valid, logical reasons one has to trust in any given situation.
- This work started back in 2006 for the OpenTC Project, an EU sponsored project to find trust in trusted computing.
- ISECOM approached this pragmatically and collected ALL the ways that anyone can name as a reason to trust from academic papers, scientific articles, and in social networking sites.
- They attacked each with logic tests and quickly eliminated one after another and were left with just **10 reasons, the trust properties**.
- When these properties are applied to any trust decision you have a very good idea of what not only the reason for trust is but also how trust is deficient.

The 10 Trust Properties

1. Size
2. Symmetry of trust
3. Transparency
4. Control
5. Consistency
6. Integrity
7. Offsets
8. Value of reward
9. Components
10. Porosity



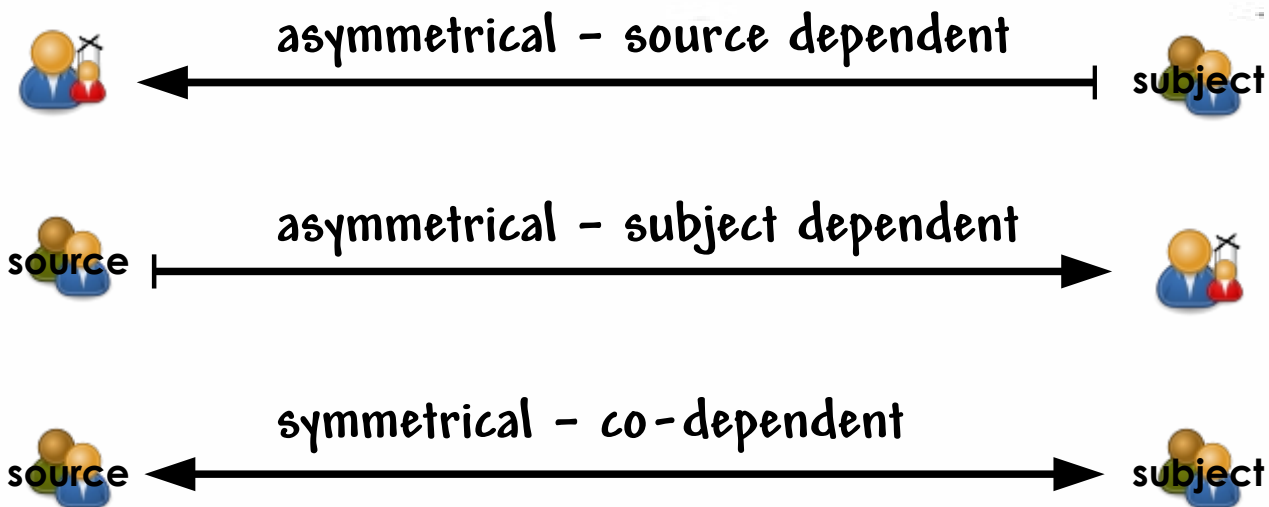


Size

- The number of subjects the trust extends to.
 - 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 of Trust

- 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





Transparency

- The level of visibility 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.



Control

- 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 of Reward

- 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.
 - The reasons to trust the subject may only be as long as the subject is within the controlled scope or environment.
 - The military creates this by bringing all new recruits into a controlled environment (boot camp training) where they get no leave for 8 weeks and are only around other military personnel.
 - The more the subject is within the known environment the more reason to trust you will have because the subject will then not be influenced by anything new or different than what is already known.
 - You have no reason to trust the unknown. Perhaps that's why it's so thrilling to do so. Perhaps that's also why it tears apart so many relationships.

Harnessing Trust

- Most people are used to having trust be an uncontrolled emotion, like love, which rides them.
- Suggesting they ride the trust was like telling them not to believe in the magic of love. It actually offended them.
- What ISECOM was really showing was that if you want to understand trust, you need to see it for the bio-chemical reaction to specific input that it is to us
- We are victims of this reaction unless we take control of it.
- We just needed a way to apply the newly discovered properties to each situation.
- This is done in the form of the Trust Rules.

Trust Rules

- This is where you take the trust properties and use them to make baseline rules to complete specific, trust tasks:
 - employee hiring, security boundaries, assigning permissions, etc.
- Most people use fallacious trust properties for trust decisions.
 - Composability (wisdom in crowds?)
 - Transitivity (chain of trust?)
- Many products and policies are built on fallacious trust properties.
 - This is why so many fail.
- Solid trust rules allows for consistency in quality rather than relying on the “gut instinct” of the gate keepers who need to make the trust decisions.

Fallacious Trust: Composability

- In composability, a person makes a trust choice based on what a large number of people have to say about the thing or person in question even if those people aren't individually trusted.
- Basically, a person accepts the group's trusts as their own.
- This is similar to the pressure created by social or political groups and mass media.
- It's also used by Amazon, Ebay, and other website retailers.
- It is illogical because the individual experiences of others, especially strangers, are all relative.
 - "Smoking is good. 300 million smokers cant be wrong."
 - Another point is that bad experiences are most strongly noted while other experiences are not recorded to the site.

Fallacious Trust: Transitivity

- Transitivity is when a person accepts the trust decision of a trusted person for themselves.
- It is also known as the chain of trust:
 - you trust Alice and Alice trusts Jack therefore you trust Jack too.
- It is illogical because you may trust Alice for some things but perhaps not the same things for which she trusts Jack.
- There is also the possibility that Alice has approached the trust for some emotional benefit not available to you.

Creating Trust Rules

- All rules must include quantifiable properties, be objective, and be understandable by the common person not necessarily involved in the security field.
- It must be represented as a percentage to express a degree of trust.
- The rules need to allow for the creation of specific, objective, verifications which can quantify and count operational trust into that percentage.
- Trust decisions are not linear, no order, order value system.
- May feel wrong but it really is completely rational.

- Assure the rules determine a finite quantity.
 - An infinite quantity may be too relative to the source and does not provide the constraints necessary for expressing the result in a percentage.
- You may have more than one question for each trust property.
 - More will be more precise and help you understand the type of trust better.
 - But the final calculation is the sum total of all tests which will provide a single percentage for that rule.
- The end metric however is one which is the mean of all ten percentages.

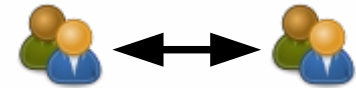
Example Trust Rules for New Employee Hiring

- This is a sample of generic Trust Rules anyone can use to make better hiring decisions beyond that of just the technical qualification of the applicant.
- It follows the 10 trust properties as everything else.
- The goal was to make quantifiable questions to be answered for each of the properties and applicable by any source on any potential new hire.
- After this example, you will have the chance to make trust rules for something of your choice.
 - We ask that any Trust Rules you make you share back with ISECOM as part of this open information initiative.



New Hire Trust Rules: Size

- Calculate the applicant divided by the total group of applicants.
(applicant / all applicants)
- Calculate the number of people the applicant appears to know in the group divided by total applicants from the total group.
(known in group / total group)
- Calculate the number of current employees the applicant knows (and is "friends" with) in this location and divide it by the total number of employees in this location.
(friends / total employees here)
- Record the average of these results.



New Hire Trust Rules: Symmetry

- The number of people the applicant must rely on to do their job in this position (including the applicant) divided by the number of professionals who must rely on the applicant in this position.

(people applicant relies on / people relying on applicant)



New Hire Trust Rules: Transparency

- The number of hours per day the applicant will be working alone, unassisted, unmonitored divided by the number of working hours.

(work hours per day alone / total daily work hours)



New Hire Trust Rules: Control

- The number of decisions the employee will be making daily, independently, without input, divided by the total number of decisions the position normally requires in a day.

(independent decisions / total decisions)

- The applicant divided by the number of team members the applicant will be working with daily.

(applicant / team members)

- Record the average of these results.



New Hire Trust Rules: Consistency

- The total number of months which the applicant has not been employed divided by the total number of months the applicant has been on the workforce and eligible for employment.

(unemployed months / total possible working months)

- The total number of criminal offenses known divided by the current age less eighteen years (or the legal age of an adult in your region) of the applicant.

(total criminal offenses / age - 18 years)

- The number of neutral or negative references from past employers divided by the total number of past employers.

(neutral or negative references / total past employers)

- Record the average of these results.



New Hire Trust Rules: Integrity

- The number of deliverables the applicant must produce or show for on a weekly basis divided by the work week.

(weekly deliverables / total hours in a work week)



New Hire Trust Rules: Offsets

- Amount of assets by value the applicant will have access to divided by a standardized cost of prosecution and cost of recovery.

(assets accessible / cost of recovery or prosecution)



New Hire Trust Rules: Value of Reward

- The monthly income created or saved by the applicant in the position divided by the monthly cost of the applicant.
 - We don't measure the amount paid by the position compared to the national average because no clear correlation exists between pay grade and job satisfaction preventing an employee from leaving, stealing, or sabotaging the workplace.

(monthly income created or saved / monthly cost of applicant)



New Hire Trust Rules: Components

- The number of processes which require the applicant divided by the total number of processes for the position.

(processes including applicant / total processes)

- The number of resources the applicant will use monthly divided by the total number of resources available for all employees in that position.

(monthly resources used by applicant / all resources)

- Record the average of these results.



New Hire Trust Rules: Porosity

- The amount of time weekly the applicant would spend interacting directly with competitors, partners, or clients divided by the total number of weekly work hours.

(hours of offsite interactions / weekly work hours)

- The number of employees living in the same community as the applicant divided by the total number people in the community.

(total employees in community / total members of community)

- Record the average of these results.

Trust Mastery

- You have now completed the Mastering Trust instruction seminar.
- If you are interested in completing this course and learning:
 - Improving the safety of trusts.
 - Analyzing trust in a security context.
 - Applying trust tests as a Trust Analyst.
- Then we urge you to take the Trust Analyst certification course and exam!



Trustworthy Origins

- **Mastering Trust** is based on research for the Open Source Security Testing Methodology Manual v. 3.
- OSSTMM established Jan. 2001.
- The OSSTMM provides a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way.
- OSSTMM was created by Pete Herzog and Developed by ISECOM, an open, non-profit, security research organization.
- OSSTMM is part of many security standards and is currently in process of becoming an ISO standard.

Professional Certifications

- OPST
 - Skills-based Professional Security Tester Exam
- OPSA
 - Skills-based Professional Security Analyst Exam
- OWSE
 - Applied-knowledge-based Wireless Security Expert Exam
 - Full electro-magnetic spectrum analysis
- OPSE
 - Knowledge-based OSSTMM Professional Security Expert Exam
 - Full understanding of the OSSTMM
- CTA
 - Applied-knowledge-based Trust Analyst Exam
 - Full understanding of applying trust metrics

ISECOM

- Making sense of security.
- Institute for Security and Open Methodologies (Est. 2002)
- A registered Non-Profit Organization
- Offices in Barcelona, Spain and New York, U.S.A.
- Open Source Community using Open and Peer Review to assure Quality and develop a chain of trust to create an Authority.
- A certification authority grounded in trust and backed by Academic Institutions (La Salle college and university network).



Trust Master presentation creator:

- Pete Herzog
- Co-founder and Managing Director of ISECOM
- OSSTMM Creator and Project Lead



Photographic images provided by:

- Marta Barceló
- Co-founder and Director of Operations of ISECOM
- Photographer, Marta.com



tango!

Special thanks
to the Tango
Desktop project
for high quality
icons!



www.isecom.org
www.trustanalyst.org