Expressing Trust
David Grawrock
Expressing Trust

If I have a trusted platform I will trust the platform to perform some operations.

Like buy a plane ticket online

But not a house
Level of Trust

My tipping point where I go from yes to no is my level of trust.

- It may be sufficient for a job.
- Or insufficient.

Online Ticket

House Purchase
It is also likely that my level of trust is not binary but has a grey area in the middle where I may or may not trust something.
Expressing Trust

He’s a hardware guy and knows what's going on?

She’s a domestic engineer and doesn’t trust technology

At some point we have to tell others what our level of trust is, but our trust may not match theirs
What is Their Level of Trust

They both are ok with buying an online plane ticket but Alice is not ok with purchasing stock while Bob is.

Do they use Bob’s trust or Alice’s trust?
What Happens in Grey Zone

Now are trust question is in the middle of Alice’s grey zone, she may or may not like the idea.

How does she make her split decision or how does Bob make it for her?
SO WHAT DO WE DO
Device Specific

Device trust is technology specific

How do we communicate that it’s ok to do a job on one device but not another?
Attestation is NOT the Answer

The TPM reports the current state

But how does current state indicate Bob’s trust level, and how does that state correlate with Alice’s trust level?
Anything Already Built?

Can we use an existing mechanism to perform the compare?

Validates that the product has certain trust capabilities. Does not provide any information relative to how an individual perceives the product.

FIPS 140

Validates the crypto properties but again no information relative to how an individual perceives the product.
Our language needs two main properties:

1. **Descriptive** enough that allows entities to express their level of trust along with the grey area.
2. **Mathematical** to enable a calculus for performing comparisons.
Trust Language Elements

Description

Nouns
- CPU
- OS
- Certification

Verbs
- Like
- Don’t like
- Use
- Don’t use
- Control

Adjectives
- Sometimes
- Always
- With condition
- Without condition

Example only I don’t really know what the language is
Trust Language Grammar

With elements we can then build a grammar. Rules are necessary as freeform makes parsing too difficult.

The grammar will allow us to describe exactly what our trust arrow looks like.
Our grammar undergoes at least two worldwide translations.

In addition to the normal cross country legal, you have the difference in evidence for continental versus common law.

Coco farmer in Latin America with bee keeper in Sweden.
We now need some math to calculate the differences in the arrows
Trust Calculus

Bob

Alice

Bob’s trust is TB
Alice’s trust is TA

Does TA = TB
Is TA > TB
Is TB > TA

And finally
If TA = TB and TB = TC
Does TA = TC

Just as algebra was able to solve big problems but the addition of calculus changed math, the addition of a trust calculus will change how we deal with trust.

\[
\int_{a}^{b} f(x) \, dx
\]
MOVING FORWARD
Using a Third Party

Maybe the trust brokerage can use a third party to referee the differences in policies.

History of third parties is not great;
- PKI except in Brazil
- TPM global attestation but that might change with 2.0

Liability for the third party is difficult
- What exactly is the ref saying about the parties?
- What happens if Alice really is a flake?
Identifying Users

Users should be strongly identified
How does the strength of identification affect trust

Platforms should also have strong identification
But many abstractions want anonymity

Users and resources want to quickly organize into
ad hoc groups with a shared trust setting

Must my trust depend on the trustworthiness of
your system manager?
Future

Solving these problems is as hard as the calculus of the past

I’m not doing that job, I helped create the algebra not it’s your turn to solve a hard problem
Backup