Theoretic underpinnings of trust assessment

Eric Osterweil, Ph.D.
George Mason University
Verify, then trust

• From Internet ops to unattended IoT/CPS, we are vulnerable to unforeseen attacks
  • Hacked cameras, DDoS from refrigerators, power grids

• Trust assessment can get us ahead of surprises, but always been elusive
  • Reputation?

• IoT, mHealth, CPS, etc. all make this harder
  • Reputation might be a non-starter
  • who expects an online reputation for a refrigerator?

And not even the dog knows his collar has been compromised
We need an extensible trust-assessment framework

• Cybersecurity isn’t all about “cyber”
  • Devices in meat-space have non-cyber telemetry
  • This *must* contribute to trust

• We need to **fuse orthogonal signal** in a meaningful way
• Device admission control
  • Can we “introduce” IoT devices to each other in meat-space
• Role-based assessments?
  • Can we determine a device’s *de facto trustworthiness* from what its exposure is?
• etc.

But, we often don’t get to control *anything* about deployed IoT/CPS devices: we play catchup!
A path to trust: a candidate approach

• Consider that trust assessment might come from **verification** + **vulnerability** (a *conditional* probability of compromise)
  • $\text{Trust} = <\text{Verification}> + !<\text{Distrust}>
  • $\text{Distrust} = <\text{Transgressions}> + <\text{Exposure to attacks/Vulnerability}>

• If we model vulnerabilities as **Vulnerability** = $P(A|E)$ we can build verifiability and counter-balance it with measured [dis]trust

• Lends itself well to IoT/CPS deployments of many pseudo/un-attended nodes
[Dis]trust framework

• Attack surface [1] + **attack windows**
  • What is exposed + when is it vulnerable to attacks

• Trust on First Use (ToFU)
  • We trust because we hope our attack window is small and unknowable

• Enables privacy determination
  • By measuring P(A|E) vs. quantified privacy gains: make a *measured* decision

We **can** and **need** to quantify these elements and can be implementation agnostic

http://techreports.verisignlabs.com/docs/tr-1120004-5.pdf
Thank you!