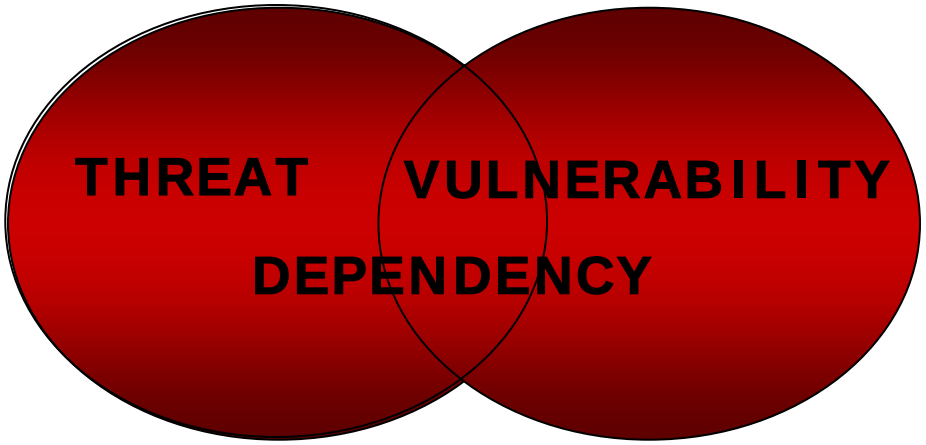
# Trust-Based Computing Overview


**Carlos Solari**
**Bell Labs, Security Solutions**

# Why: In a State of High Risk…




**High complexity in our networks**
**Security is unmanageable**
**Convergence to IP increasing complexity**
**Perimeter is expanding: wireless & remote**
**Patching: too much – too long – too late**
**Too easy to hack the system**
**Connectivity - inheriting each others risk**
**Data management & storage - a nightmare**
**Records Management - Privacy adds complexity**

## March 2004 GAO Report

**What GAO Found:** In addition to general cyber threats, which have been steadily increasing, several factors have contributed to the escalation of the risks of cyber attacks against control systems. These include the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems. … **Successful attacks on control systems could have devastating consequences, such as endangering public health and safety.**

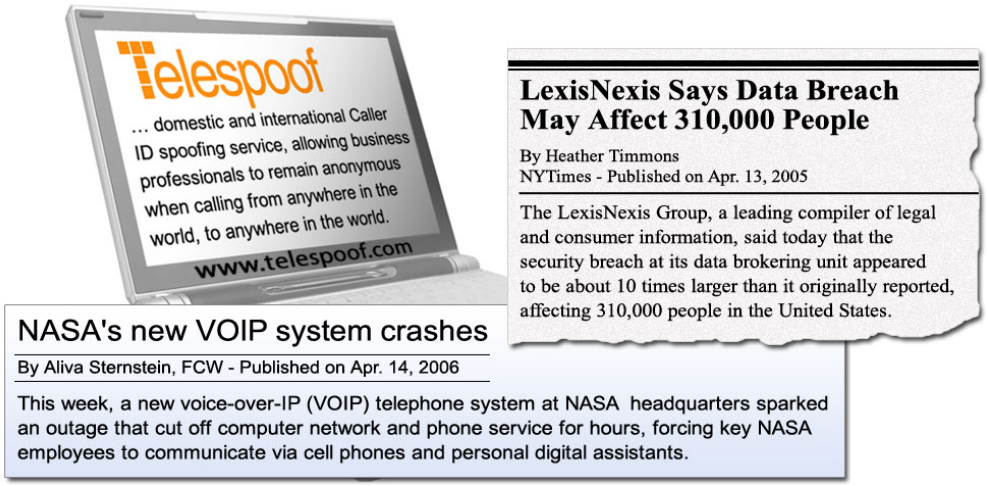
# Will the Current Model Work…with More Resources?

## Current Industry Approach to IT Security…

| | | | | | |
|---|---|---|---|---|---|
| **Blacklists** AV/AS, url blocking | Reacting to infinite possible sources Ex: polymorphism | **Point Products for Point Roles** | Un-manageable and no single sit-awareness | **Weak Links Prevalent** | No inherent security applied to network components |
| **Increasing network Complexity** | Increases the vulnerability | **Threat-Expl Window Smaller** | Threat can occur faster than we can detect and respond | **Lack of Universal Standard** | That addresses security in a comprehensive way |

## Current Approach Insufficient to the Challenge

- **Increasing financial losses**
- **Brand confidence at risk**
- **Infrastructures at risk**



# The “Trust Paradigm”

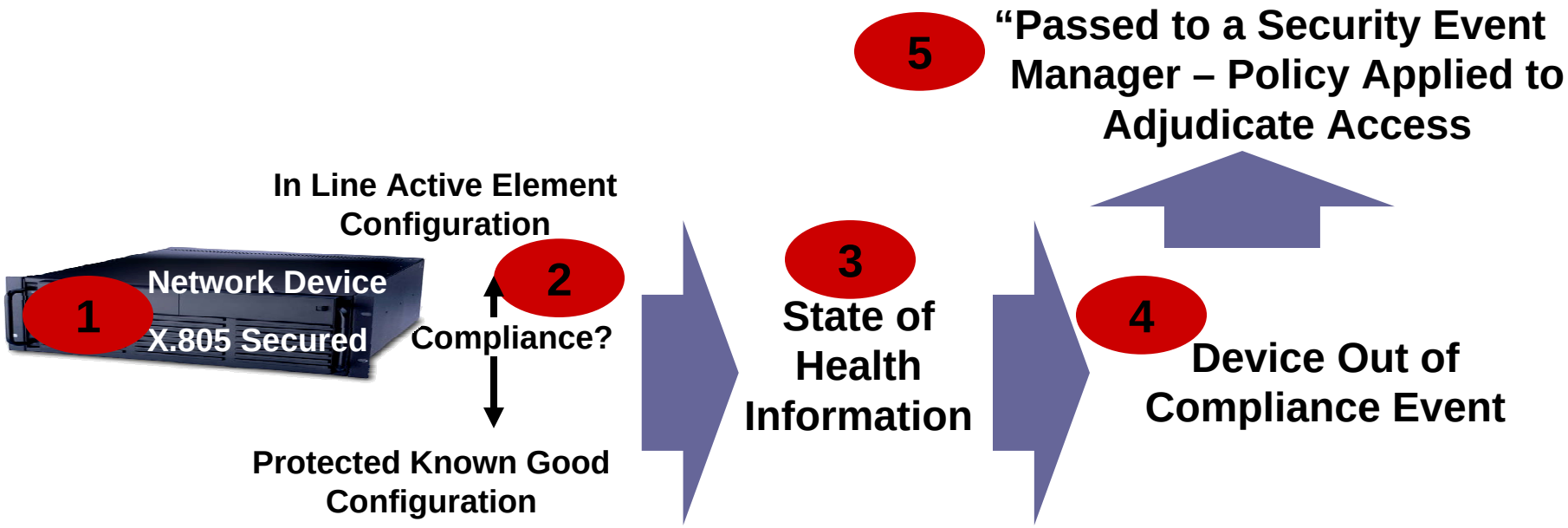
## A different way of thinking about security

- Trust not assumed – must be measured and validated
- Trust must be built up from the ground up….cannot be applied after-the-fact
- Used to adjust levels of access
- Not a new concept – modeled after existing systems and real world modalities

## What is “Trust-Based Computing”?

- Device attestation (state-of-health)
- NAC and NAP
- Access based on an exchange of “trust” credentials
- Security engineered into every device – designed - architected into the system

# Using Trust to Adjudicate Acess



# Can We Build Trust-Based Systems?

- Actually – solutions at work – albeit independently
- Have to change the dynamic of demand and supply
- Government can lead the transformation
- Supply won't change until the demand is there
- Not a big bang – can be – must be incremental
- So – time to begin