Models Brief Out

Wednesday, August 18, 2010

1:01 PM

1. Modeling the non-compromised system
	* Any system will have stakeholders and those stakeholders will define the non-compromised stake
	* Can model and understand the behavior of non-compromised state
	* Then you have the basis for measuring what a compromised state would look like
	* Systems and people should be modeled and those models work together
2. Mixed initiative response system
	* Do you keep the human in the loop and gain human capabilities?
	* Or keep the human out of the loop just observing?
	* Better to have a mixed approach to balance the strategies
	* If there is a time scale not at human level, the system must take initiative
	* There is a risk
	* http://portal.acm.org/citation.cfm?id=303030
	* http://ieeexplore.ieee.org/xpl/freeabs\_all.jsp?arnumber=932233
	* http://www.cs.utep.edu/novick/papers/mi.aaai.html
	* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.149.714
	* http://academic.research.microsoft.com/Paper/2414215.aspx
3. Hierarchy of models at different scales
	* You have sensors giving raw data but you need to make some high level sense of this data
	* How do you arrange these models so that you can analyze them
	* Layered approach to models where the lower models feed into the higher models
	* Lowest level could be what events are coming through the sensor and the highest level could be this group is trying to take over this machine
	* Analyze what the models cover
	* More towards model representation
4. Behavior modeling
	* Should be models of different kinds of users and their use
	* Prepare against what you think may be an adversarial model
	* Fingerprint people based on their behavioral model
	* Many different ways to represent behaviors
	* Multi-media models
		+ Language
	* Need to model attackers
		+ Goals they might have
		+ Methods they might use
	* Difficulties of physical modeling in terms of behavior
	* Intention-based modeling
		+ Normal behavior and goal based modeling
	* Commercial industry is doing a lot of work in this area
	* How to model behavior based on *who* is using the box
	* Combination of devices
	* Not the norm to be only using one device
	* ***Multi-devices use by individual and multi-users on a single device***
	* Groups come up when we describe what we want to use the results of the analysis for
	* Broader sense - don’t have to take particular behavioral method and user
	* Nation state offense can be derived by studying the nation state defense.
	* Maybe to look at offense
		+ Model a bad guys offense and look at his defense
	* Their defense is incredibly strong on things we had never considered
	* “In game theory you can’t tell the difference between the incredibly crafty player an the incompetent one”
	* Non specifically to model know bad actors
		+ More to model unknown bad actors
	* Good guys vs bad guys
		+ In reality good guys might accidentally do bad things
		+ Bad guys do normal things too
		+ Focus on benign activity
		+ Distinction is that the bad activity is a small part on the activity we think of as bad guys
		+ If we build models that are based on the actor being bad or good most accurate models say no one is ever bad
		+ Good guy vs bad is dangerous
		+ *Need to be able to disguising the small amount of activity that is “bad”.*
	* Normal vs abnormal behavior
		+ Could trick yourself
		+ most of the adversary exploitation is based upon “Normal Behavior”
			- it is a trick to use the normal behavior to disguise hostile behavior
			- a bad guy who does normal things and bad things but a bad guy will deliberately hide behind or fake normal activity
	* Help old people who live independently
		+ Could have modeling implications
		+ Look for the pre-cursors
		+ Worth exploring
	* Trying to make a distinction between establishing a baseline to identify intent-based malicious behavior different from risky behavior that would put the system at risk
	* Modeling the mission
		+ Used to guide the interpretation of the behavior models
	* Model the impact of the attack on something that we care about
		+ All the targets are not equal
	* http://ieeexplore.ieee.org/xpl/freeabs\_all.jsp?arnumber=588541
	* Lot of different kinds of behaviors and needs. Everything from traditional to second life and multimedia models. Including voice and changing. The need to model attacks, attackers. The goals of attackers and being able to resolve that to an attack. Combining physical to human and with a goal of fingerprinting with timing being a critical issue.
5. Combination and integration of model
	* Want to be consistent
	* Be able to maintain multiple models to be able to go to the right model when needed
	* What if the inconsistency is the information?
	* Redundant and different perspectives
	* Need to be able to maintain two different perspectives
	* Should include methods of randomizing models so the attacker cannot know what a model might be
	* Generalize more to a notion of an ensemble of models
6. Modeling context
	* How do you actually represent context and manipulate context
	* Clustering of files
		+ Discovering potential anomalies
	* *Use of dynamic context as a first class object for data and modeling interpretation*.
	* Structurally it was potentially an anomaly but contextually it makes sense.