First Working Session - Models

Tuesday, August 17, 2010

5:44 PM

* What should the world of models look like in order to be able to feed this nirvana of understanding the cyber threat?
* Collect ideas onto the 'idea gallery'
* What are some of the challenging research directions?
* Danko Nebesh
	+ Capture someone in military - want to figure out who this person is; what is the relationship and should we investigate further?
	+ Generate a models based on activities that this person has been involved in (resume)
		- Use personal interests/backgrounds
	+ Trying to build information in real time in a automated fashion
	+ 'meet up with the person in cyber space'
* Two aspects - how to gather the data and how to ask the questions
	+ How to make sense of the information
* Pat looking for something beyond semantic index
	+ Will not provide a lot of depth quickly and in real time
* Have some fragment on info that may not totally identify the individual; reducing uncertainty by proposing actions
* How to define an adversary?
	+ Have to know what to look for
	+ Computational power
* Question is: can we actually generate concrete instantiations of adversary behavior?
* Victor Harrison
	+ Two ends of the spectrum: well known problem and how to deal with the data
	+ More interesting problem is where you have massive collection of events and data and trying to discern if there is something significant in that and if there is something to be presented to an analyst
	+ Proof by counter positive
	+ Maybe invert the problem; think of it inductively
* Rita Barrios
	+ We also need to understand what's non-adversarial so we can 'weed out the noise'
	+ Think about models that are normal as well as abnormal
* What happens if there is an outlier that is not adversarial?
* Marco
	+ Different classes of adversaries
	+ What a feedback system
	+ Think of something that allows analysts to have this interface
	+ Human can play a very important role
* Sean
	+ Model integration is one of the bigger problem
		- Having all of the models 'talk' to each other
	+ Pushing more towards human on the loop
	+ Human interaction is minimized
	+ Get context into the conversation (meta information)
		- Information about the information
	+ Which pieces of that meta data do we really care about?
	+ Focus on essential information
* Pam
	+ Think about: how do we see *that* happening in the future
* Meta-data - things that describe data
* Meta-information - things that the human cares about to describe the data
* Deborah
	+ Combine sensitive data about employees and put that together with behavior
	+ Power grid: teach operators anticipatory behavior
	+ Human is used to responding as opposed to predicting
* Victor
	+ Meta object facility - extend to include dynamic capabilities
		- Used right now for complex event modeling
* What kind of questions about these models would we like to address?
	+ Rather than what language should the model be written in
* Victor
	+ Interchange between different model types
* Know how to operate what is important to us and how to use the network
* Filter - grab models that intersect your model
* David
	+ Identity is a lot murkier
* How can you tell that you are dealing with the same entity
	+ Fingerprinting machines and people
* Somesh
	+ Hard to trust a lot of data
	+ Build fingerprinting on top of that
* ***Fingerprinting***
	+ ***Resolving the behaviors to entity(s)***
		- ***Either a person or malware***
		- ***Even could be an individual host on the network***
	+ ***When you run across something weird you can see who they are***
* Somesh
	+ Calling models are different scales
		- Lowest level are network sensors
		- Hierarchy of models
		- Each level gets more clarity and more abstract view as you go up
	+ These are all built models
	+ Not worried about construction
	+ Understanding things at multiple level of scale
* ***Models at different levels of abstraction***
	+ Is this model already covered by this model?
* ***Adapt area of hierarchical state machines***
* John
	+ Extent to which attacks are exploiting bugs
	+ Multihoming
		- Cannot multi with ip in an effective way
	+ All of the economic an market forces are aligned at preserving the bugs; preserving ip
	+ Need to have people that care enough to make the change to the architecture (smoking example)
	+ Patching things that you cannot fix
	+ From a security perspective give a coherent critique of the architecture
	+ What could this community do that is complementary to what is already being done?
	+ What would we fix to stop these attacks
		- Getting people to stop smoking, not how to treat cancer
	+ Cannot be part of an application without having an authenticate identity
* Current attacks are more at application level, not ip level
* What is a model for a network that could keep an attacker out?
* What is the model that enables us to use our computing environment?
* ***Designing the model so that you know where it is going to be compromised***
* How can you become pre-aware that it is going to be compromised
* ***Design the environment to better deal with the compromise***
	+ ***Make the environment more resilient***
	+ ***Use a model to design that***
* Marco
	+ We need to develop models that allow humans to participate
	+ Instead of having the loop eventually fail and having the human detect it, have the human be a part of it in preventing the fail
		- Decide what is/is not a attack
		- How to make the human involved and be efficient
* ***Mixed initiative response systems***
	+ ***Delegate to machines***
	+ ***The system presents info to the human so that the human can decide***
	+ ***Architecture that feeds both ways***
	+ ***Simulation is a key component to incorporate probalistic modeling***
* John
	+ No natural way of limiting scope
	+ Application layer have limited scope
	+ Need to be able to create different local scope
* ***Local scope is the norm***
	+ ***Assuming we have this accountability, what is possible?***
* Once we get past authentication, we're still going to have adversarial issues
* Who is going to administer that scope
* John
	+ Trade-off with security and freedom
	+ Trying to think about adversaries in a more fundamental way and less about the attacks
* Always fight the last war because we know it but now we have to be able to anticipate
* What happens when you are your own adversary?
* Why is model combination and integration hard?
	+ Maybe inconsistencies?
	+ Ultimately going to have many different researchers with many different approaches coming up with the models
		- Cant agree with one modeling approach
	+ Abstraction issue
	+ Different assumptions that you make
	+ What would the solution look like and what research would have to be done to get to that solution?
		- Automate as much as possible
	+ Somehow need to repair these inconsistencies using a meta-model
		- How to fix?
	+ ***Automatic way to repair/identify conflicts with a meta-model***
* Where are all these models coming from?
* What are we going to represent?
* ***What matters and how do you know?***
* ***How do we decide what matters?***
	+ Be able to specify adversary behaviors
* Can we model behaviors of a compromised system?
* More about hierarchy of models
* What constitutes an attack?
	+ Violation of any of those properties
* ***Need to model the mission "the stakeholder environment"***
* Indy
	+ Understand what the different subgroups want
* What to do if 'my laptop is compromised'?
	+ Want feasibility
* Victor
	+ In order to model compromise you have to have a basis for comparing it
* Want to build systems to ambiguously tell what world we are operating in
* Need to be able to model the analyst as well as the enemy
* Tell them what they need to know when they are making a wrong decision
* Deborah
	+ Need to model children, drunks, etc….basically who knows
	+ ***Authorization that a user has on a system depends on the user's 'state'***
* Victor
	+ If you just have a reasonable model of non-bad behavior, you wouldn’t do/allow these kinds of things
	+ Coding practices that will enable attacks to occur
	+ Had a reasonable model that would augment what the software people are dealing with it would be a very reasonable thing to do
* How to choose whether a certificate is trusted or not?
	+ User cannot possibly make this decision with the information that the system gives the user
	+ For most users security is not on the mind (I want free music)
	+ Would be nice if there was a clear engineering trade-off
	+ ***Maybe if there was some way to see what would happen to your machine if you install this bad software***
		- A good way to let people make mistakes to learn
		- Have models to help train the user
	+ Incentives are not aligned
* ***Use of dynamic context is a first class object for data and model interpretation and application***