Monitoring Smart Grid Operations and Maintaining Mission Assurance through Adaptive Computer Network Defenses

Daniel Bilar ∗
James J. Solderitsch †
Elvis K. Hovor ‡

∗ Director of Research, Siege Technologies, Manchester NH 03101

† Project Lead, Accenture PLC, Reston VA 20190

‡ Information Security Institute, Johns Hopkins University, Baltimore MD 21218

7th Cyber Security & Information Intelligence Research Workshop
Oak Ridge, Tennessee, USA
October 12th-14th, 2011

Who we are

Siege

Company Privately held R&D company with offices in Manchester (NH), Reston (VA) and Rome (NY)
Focus Computer Security, Information Operations, Information Warfare, CNO
What We Do Advanced System Testing / Red Teaming, Defense Engineering, Software Dev & Analysis, Code Analysis / RE , Special Application Support

Accenture

Company Global management & technology consulting & technology outsourcing company. Cyber Security Research Group based in Reston (VA)
Focus Cyber Security Group Enterprise, Infrastructure & App. Security, Data Protection and Privacy, Smart Grid Security
What We Do Security Research / Data Analytics / Controls / Enterprise Governance Risk and Compliance / High Performance Security Operations

Johns Hopkins Information Security Institute

Educational Institution NSA IA CAE & charter member of I3P in Baltimore (MD)
Focus Research and study of issues related to information security and assurance, including technology, privacy, strategic management and other emerging fields.
Research Preparedness and Catastrophic Event Response (PACER), Reliable, Auditable, and Transparent Elections (ACCURATE), RFID Security, NIDS, HIDS

Talk Roadmap

Status Quo

Blacklisting Deadend Detection of interactive malcode at least in complexity class $NP^{NP^{NP_{oracle}}_{oracle}}$ [JF08] & infeasibility of modeling malcode [YSS07]
Validation Lacunae Meta-survey of ninety security papers between 1981 and 2008 showed that quantified security was a weak hypothesis because of lack of validation and comparison against empirical data [Ver09]

Focus on Mission Assurance (MA)

Impact on Mission What matters is not attack agent identification per se
Analogy Doctor gives antibiotics for bacterial infection after measuring fever and noting headache. Primary effort is not identification of bacteria. Doctor continues to measure your fever and appetite (our MA metrics) to gauge effectiveness

MIssion Assurance Through Adaptive Network Defenses

Approach Continuously measure MA indicators (security properties) to gauge the network's mission state. When thresholds reached, optimization problem is solved to identify appropriate host and network defenses (security controls) given parameters (attacker efforts) and constraints (cost and mission assurance bounds)
Components Discrete Event Simulation System (ExtendSim); ExtendSim library (MESA); Excel Linear Programming Add-On (Solver)
Tie-in Communication between ExtendSim and Excel via macros

Related Work

Mission Essential Functionality [PRAS10]

Conceptual framework Goal is detection of MEF degradation with runtime support for mission assurance in terms of Quality Of Service and Information Assurance criteria.
Comparison Our work also defines metrics, measures them, and implement a quantitative, optimization-based mission assurance framework.

LANL FRNSE (Framework for Responding to Network Security Events) [DL08]

Automated responses Looks for evidence of threats to enterprise network and responds. One goal is substituting scripts for low level security analysts.
No cost consideration Detect and respond to all threats to enterprise
Comparison Our work engages defensive adaptations that maximize Mission Assurance within the available resource budget.

QRAN [Bil03]

Quantitative Risk analysis and Management risk induced by vulnerabilities present in non-malicious software.
Goal Snapshot of constitutive software on the network, assess fault/exploit risk, and manage that risk by rank ordering reduction measures subject to cost, functionality and risk tolerance constraints
Comparison Our work measures effects of realized attacks, not risk potentiality of vulnerabilities. We use a similar optimization formulation.

Mission (or Purpose) of Network

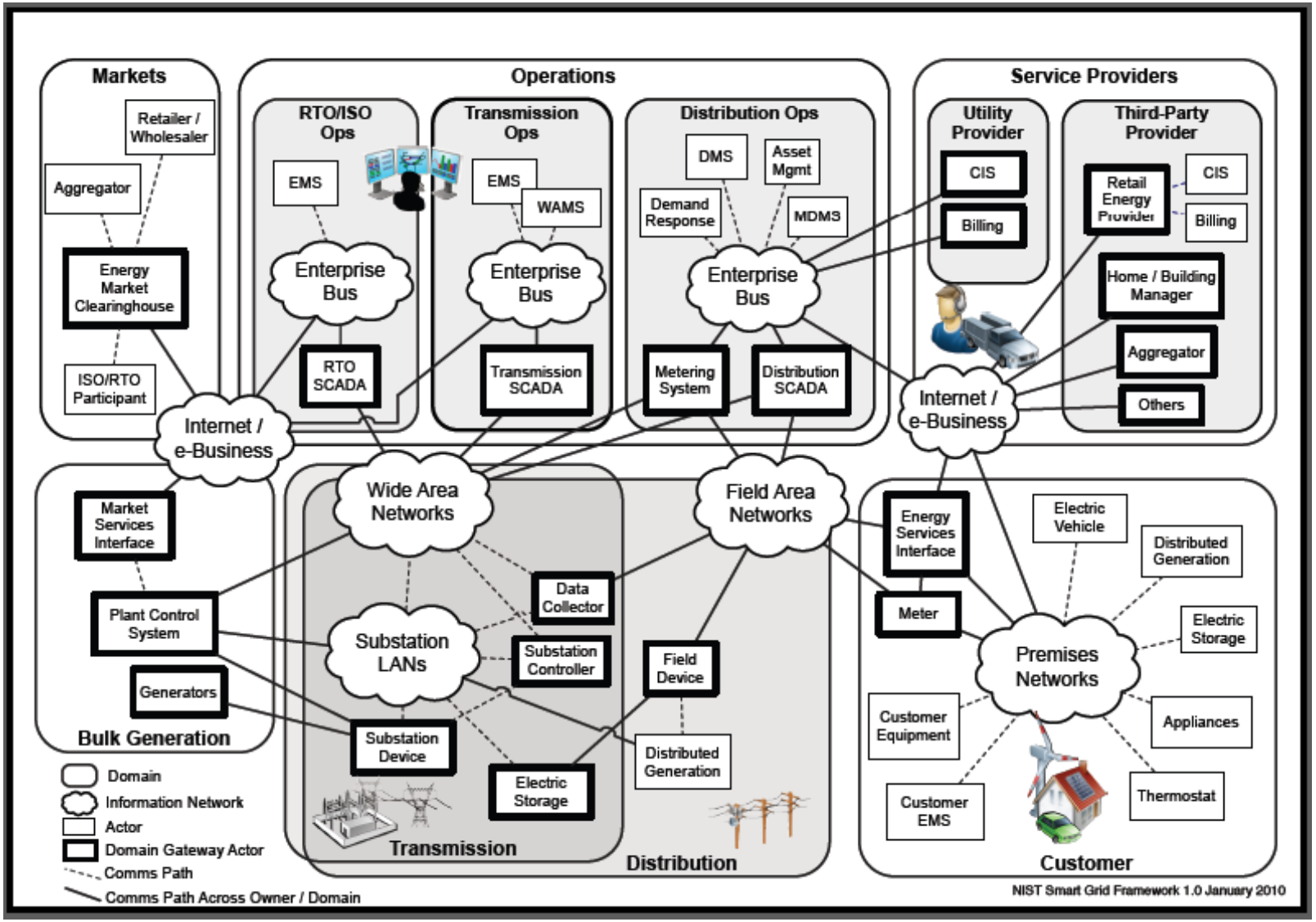


Figure: NIST Smart Grid - A domain is a grouping of actors that has similar objectives and rely on similar systems.Within these network domains, we measure mission assurance indicators (security properties) on actors as we optimize for defenses (security controls) given parameters (attacker classes) and constraints (cost and mission assurance bounds).

Mission Assurance: Attack Effort

Security Properties

Assuring Security properties In our framework akin to assuring mission.
CIA MA properties include **availability** (ability to use information/resources), **integrity** (prevention of unauthorized changes), **confidentiality** (concealment of information)
FRAUPUD More properties include authenticity (identification and assurance of origin), freshness (non-replay of stale data and commands) and non-repudiation (proof of responsibility).

Attacker Classes

Attacker Differentiation Opportunistic, Hobbyist, Organized Crime, Nation State, Malicious Insider.
'Efforts' General placeholder, includes (but needn't be limited to) person-hours invested, technical resources marshaled and drive

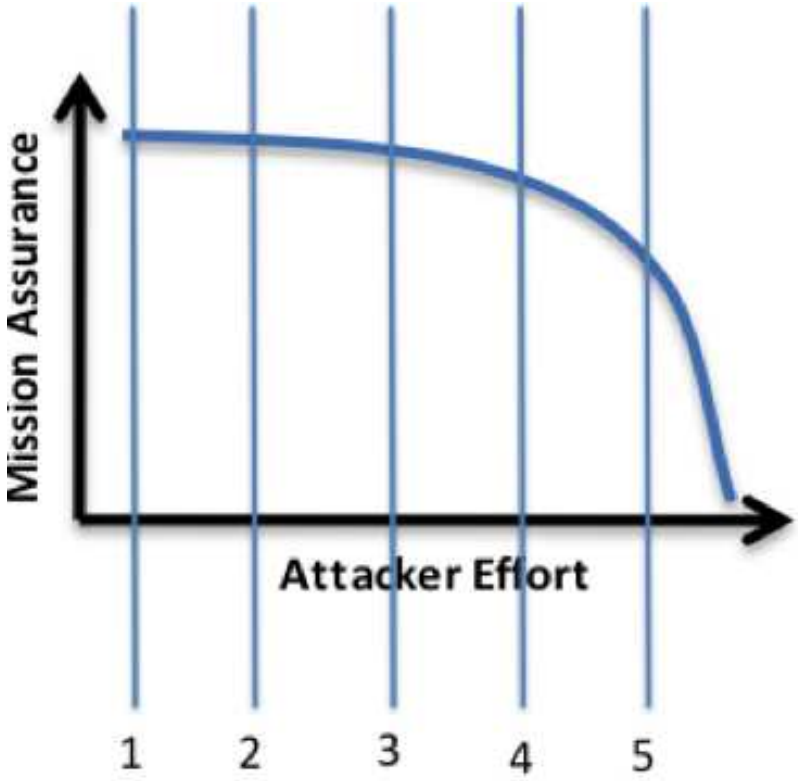


Figure: A notional Mission Assurance Curve. Mission assurance (MA) decreases as attacker efforts increases. Attacker effort serves to separate increasingly hardier attack classes (1)-(5). Purpose of defenses is to keep Mission Assurance high vis-à-vis all or subset of attacker classes/efforts.

Mission Assurance: Marginal Loss

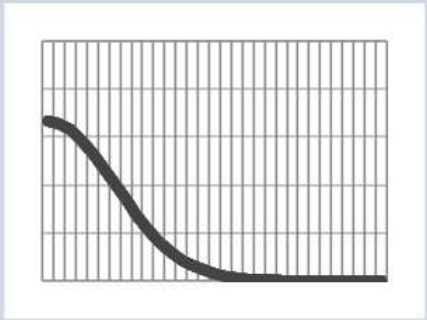
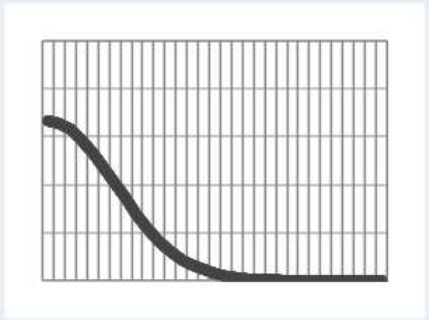
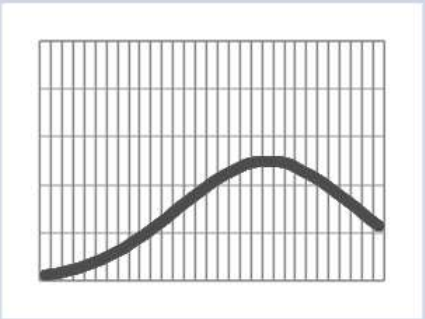
Impact on	Marginal value lost over time	Description
Confidentiality		Once a breach on confidentiality occurs, most of the value of the assets is lost. Confidentiality cannot be regained once compromised.
Integrity		Like confidentiality, attacks on asset integrity have the highest marginal loss of value at the onset of the attack.
Availability		Compared to confidentiality & integrity, attacks on availability result in a higher rate of loss over time. For example, a DoS on a web server, would have relatively little impact if it only prevents access for a few minutes or hours. An outage of days however would result in seriously losses (i.e. Sony Playstation Network).

Figure: Differentiating attack impact over time on Mission Assurance

Modeling and Optimization Framework

Commercial Discrete Event Simulation System: ExtendSim

Commercial ExtendSim
Use Create model network topology and model operation and reporting UI

ExtendSim library: MESA

Free MITRE library
Use Modeling higher level modeled network artifacts (nodes, services, links)

Excel-hosted Linear Programming Add-On: Solver

Commercial Frontline Solvers provides built-in LP in Excel
Tie-in Macro to invoke optimization from model

Model in MESA

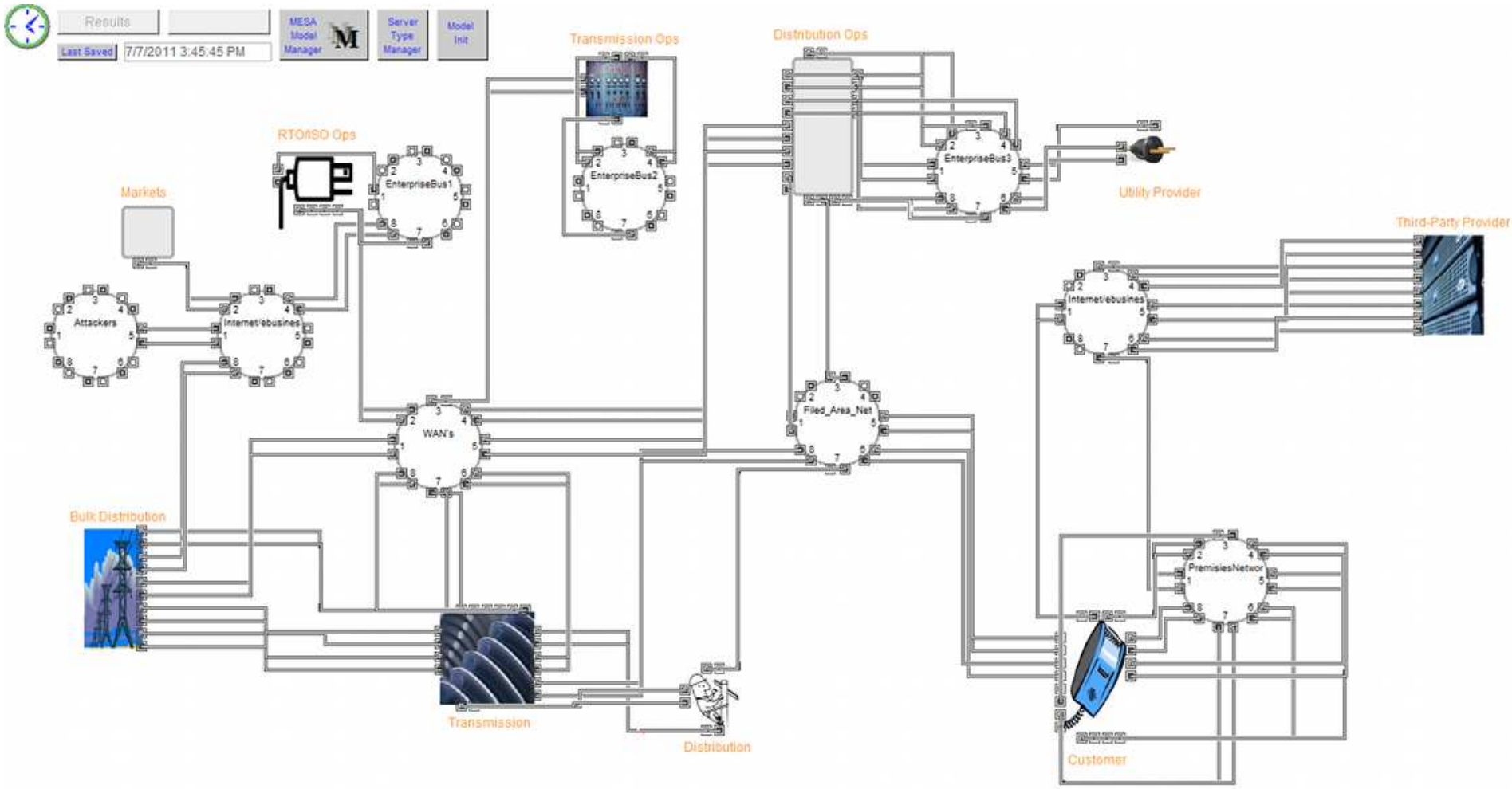


Figure: Simplified MESA-ExtendSim model of Smart Grid. Only some actors and domains are shown. Within network domains, we measure mission assurance indicators (security properties) on actors as we optimize for defenses (security controls) given parameters (attacker classes) and constraints (cost and misfxsion assurance bounds).

Optimization: Defenses, Attack Classes, Costs

Defense Options	Description
watermark	hashtag data
blackhole	change network routes
honeynet	add subnets
encrypt	add network encryption
SESRAA[LCSC08]	active denial
signature	enable whitelisting
randomize	change environment
timestamp	timestamp packets
data poison	mutate data
failover	add hosts

BIP formulation

$$\max_{x} \sum_{s} \sum_{i} \alpha_i A^{(s,i)} \vec{x}$$

$$\begin{aligned} A^{(s)}\vec{x} &\geq \overrightarrow{MA}_{rhs} \\ C\vec{x} &\leq \overrightarrow{Cost}_{rhs} \\ x &\in \{0,1\}^n \\ \sum_i \alpha_i &= 1 \end{aligned}$$

Attack Effort	Description
Opportunistic	Quasi-random attack
Hobbyist	Low skills (no strong incentives)
Mafia	Med. skills (fincl inctvs)
Nation-State	High skills (natsec inctvs)
Malicious-Insider	Abuse of insider trust (financial, ideological or personal motives)

Cost Item	Description
configuration	deploying defenses
acquisition	delivering defenses
maintenance	updating defenses
opportunity	'road-not-taken'
utilization	negative impact
transition	'swap' costs

Optimization: Formulation

D	(m-by-n-by-e) **MA effectiveness of defenses against attacker classes**.
$A^{(s)}$	(m-by-n subspace of D) **MA effectiveness of defenses against subset of attackers** selected by $f : D \rightarrow A^{(s)}$
$A^{(s,i)}$	subspace of $A^{(s)}$ denoting **attacker domain of interest selected by** f
C	(c-by-n) denoting **cost associated with defense responses**
MA_{rhs}	minimum total mission assurance to maintain
$Cost_{rhs}$	maximum total costs allowable
α_i	**relative weight of the mission assurance metrics**
x	(n-by-1) indicator vector solution $\vec{x}$ for set of defense responses to be actuated

BIP formulation

$$\max_x \sum_s \sum_i \alpha_i A^{(s,i)} \vec{x}$$

$$\begin{aligned} A^{(s)}\vec{x} &\geq \overrightarrow{MA}_{rhs} \\ C\vec{x} &\leq \overrightarrow{Cost}_{rhs} \\ x &\in \{0,1\}^n \\ \sum_i \alpha_i &= 1 \end{aligned}$$

n	# defense responses to optimize over
e	# attack classes of interest
m	# mission assurance metrics of interest
c	# cost factors to be considered

Solving: MS Excel & Solver plugin

Complexity BIP class generally NP-hard. However, since MA_{rhs} and $Cost_{rhs}$ plausibly integer valued, efficiently solvable by transforming C and $A^{(s)}$ into TUMs [MTA81]

Sample Run: Excel

MA_count	macount	3		9	data poison
Threat_count	threatcount	5		10	failover
MA_minlevel	maminlevel	4			
Cost_maxleve	costmaxlevel	8000			
		bounds			
Obj Func: max	5.85		x		DefenseResponse
MA constraint:	4	4	1		watermark
Cost constrain	7849.8	8000	1		blackhole
			1		honeynet
			1		encrypt
			1		SESRAA
			1		signature
			1		randomize
			0		timestamp
			1		data poison
			1		failover
MAmetrics	(All)				

Sum of DefEff	Threat Clas				
Row Labels	Opportunistic	Hobbyist	Organized Cri	Nation/State	Insider
watermark	25	22	19	17	13
timestamp	26	22	19	17	14
signature	25	22	19	17	13
SESRAA	25	23	20	16	15

Figure: A BIP solution in MS Excel with notional data. Given MA lower bounds of 4, cost upper bound of 8000, and all attacker efforts, every defense except timestamp selected.

Simulation traces before and after defense actuation

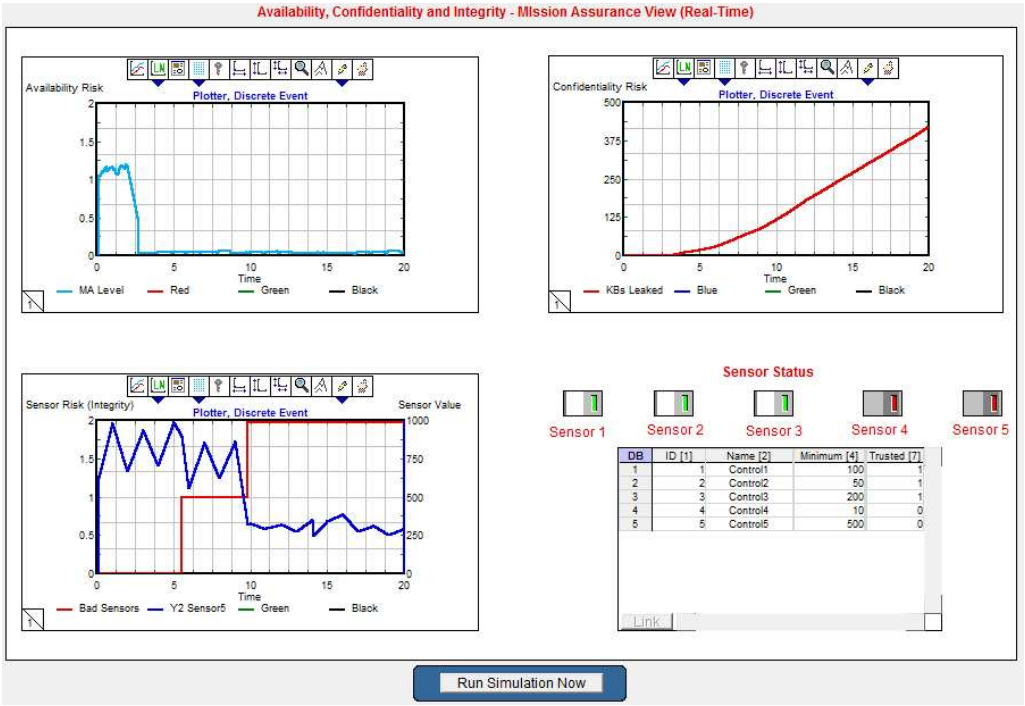


Figure: MA measured before defense actuation
Availability plot (upper left) shows measured service processing time (decrease at t = 3). Confidentiality plot (upper right) shows suspected data leakage overtime (in KBs). Integrity plot (lower left) shows sensor readings for a named sensor (blue line) and a count of the number of sensors with abnormal readings (red line).

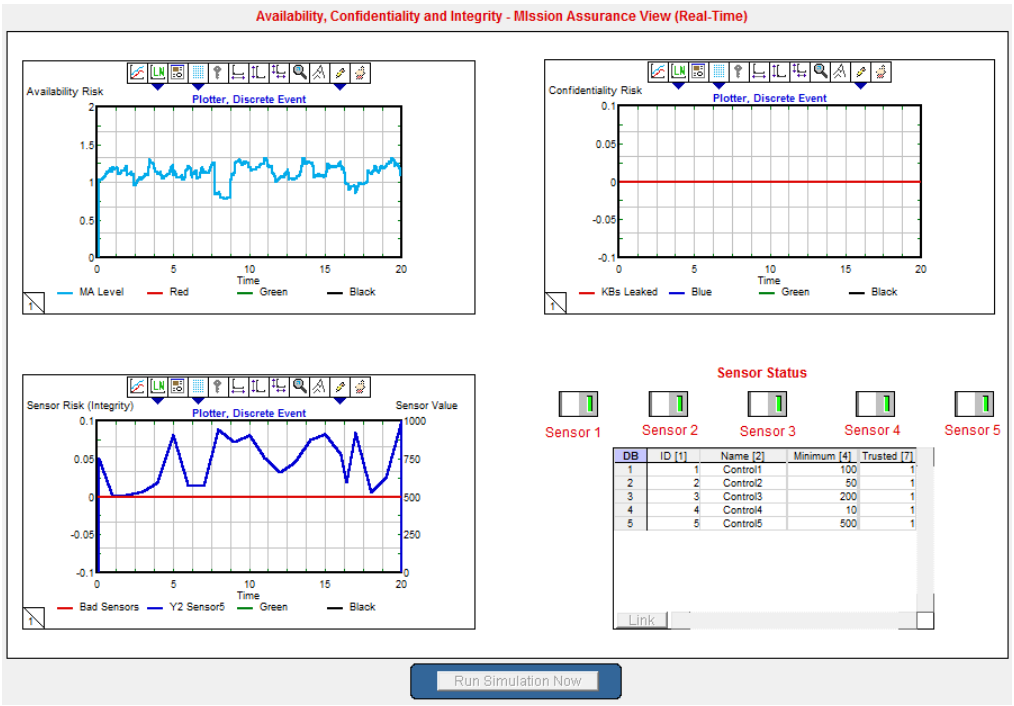


Figure: MA measured after defense actuation
Three simultaneous defenses (signature, blackholing and watermarking) activated. Increased assurance level measurements across the confidentiality, integrity and availability security properties

Refinements: Thresholds

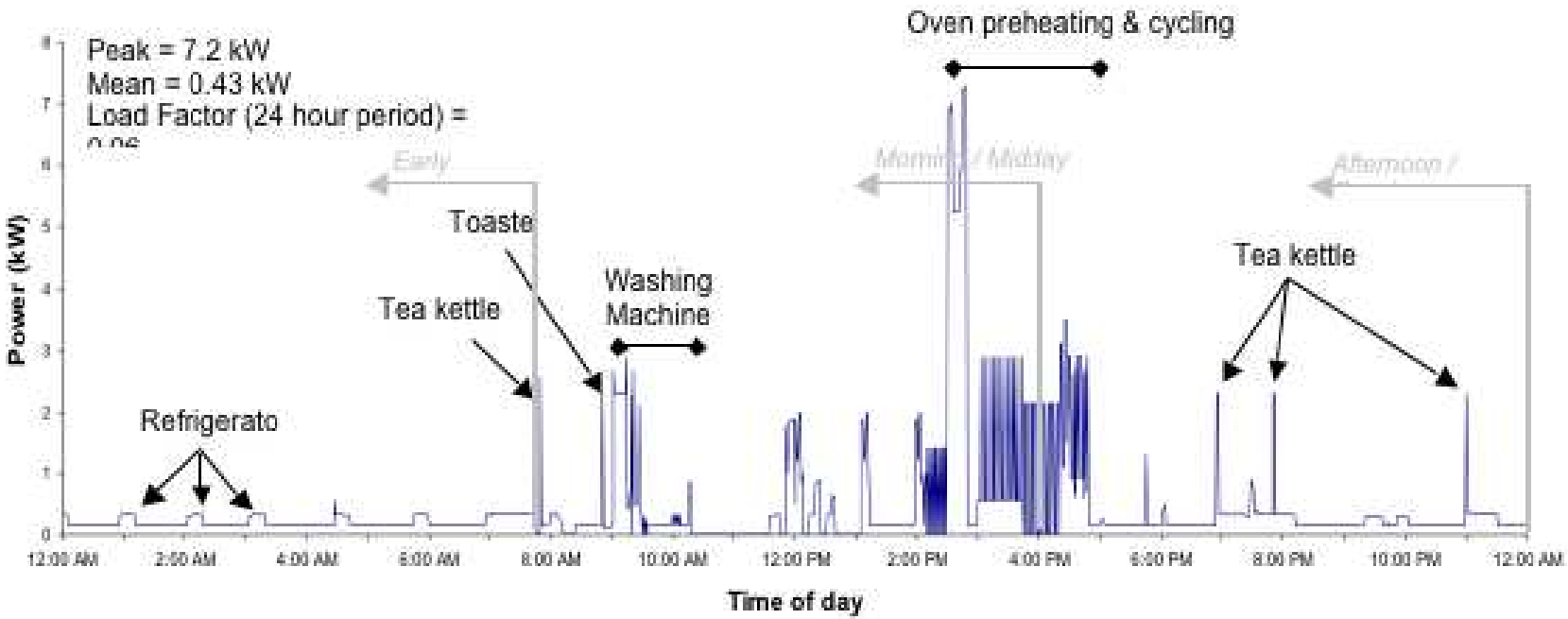


Figure: Household power consumption. Load factor (maximum power compared to mean value)is 0.06. Data from [NA99].

Effect-based Anomaly Detection

Defense Actuation triggered by deviation from baseline Mission Assurance levels
Thresholds based on residential electricity time use series [WLV+09]
Fluctuation patterns consumption patterns fluctuate greatly within daily activity periods [FSL01, TPCC10].

Refinement: Realistic Activity Patterns

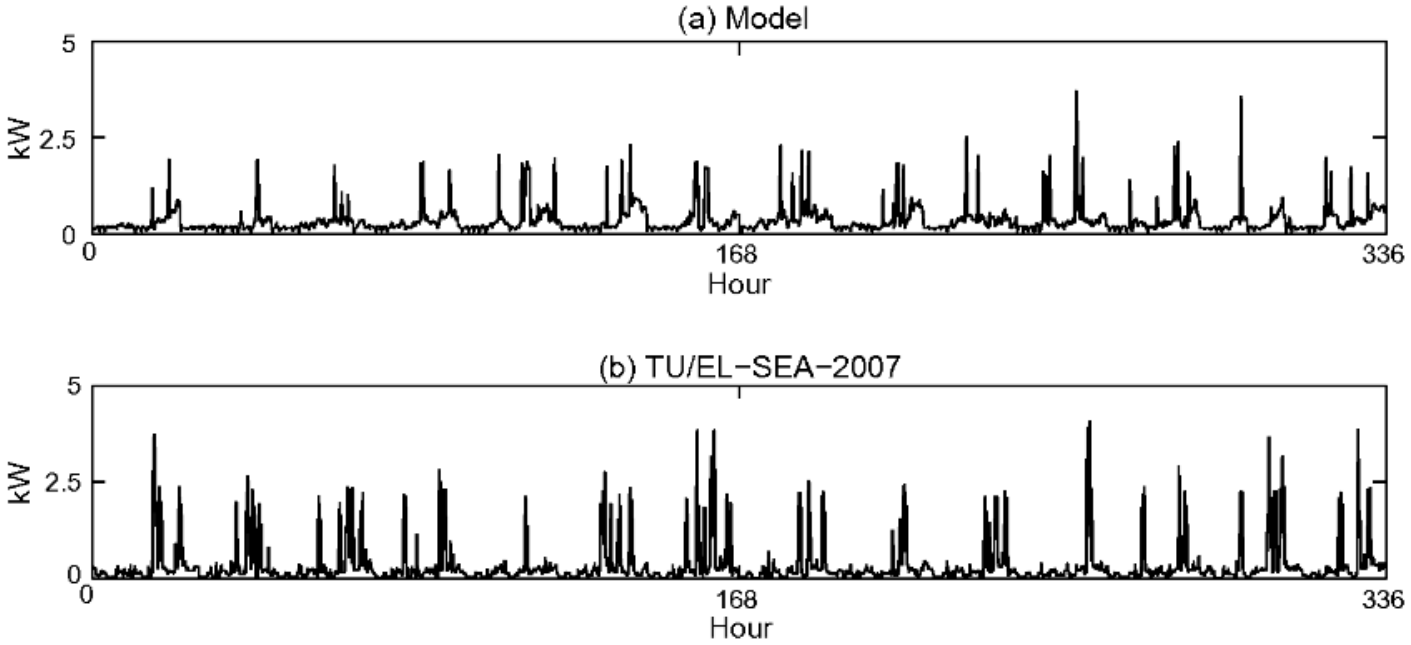


Figure: Measured time series data (2 weeks, 1 minutes sampling, resolution 10 minutes) and Markov model of one household [WW10]

Multi-state non-homogeneous Markov chain activity models [WW10]

Idea Identify anomalies through n-tuple (rather than just one) thresholds and by accurately modeling household consumption through multi-state non-homogeneous Markov chain activity models

Lessons

Mission Focus Primacy MA determinations based on combination of security-based data (IDS, SIEM, etc.) and core enterprise data
Domain Both head-end and consumer-end

Future Work and Improvements

Integration Improve tie-in between model & Excel optimization
Automate Improve automation of reaction to detected threats
Realism Improve MA effects across defense types, threat classes and threat severity
Expand Include commercially available security tools and explore other application domains, both commercial and government
Deployment Instrumentation on real enterprise networks
Write Full research paper
Collaboration Find R&D partners and opportunities

Thank you

Thank you for your time and the consideration of our work.
We appreciate being back at the CSIIRW in beautiful Tennessee ☺

References I


Daniel Bilar, *Quantitative risk analysis of computer networks*, Ph.D. thesis, Thayer School of Engineering (Dartmouth College), June 2003.


Justin Doak and Aaron Lovato, *Framework for responding to network security events (FRNSE)*, Tech. report, Los Alamos National Laboratory, 2008.


B. Fuller, J. Sikora, and J. Lyons, *Review of residential electrical energy use data*, Tech. report, NAHB Research Center, July 2001.


Gregoire Jacob and Eric Filiol, *Malware As Interaction Machines*, J. Comp. Vir. **4** (2008), no. 2.


Q. Liao, D.A. Cieslak, A.D. Striegel, and N.V. Chawla, *Using selective, short-term memory to improve resilience against ddos exhaustion attacks*, Security and Communication Networks **1** (2008), no. 4, 287–299.


J. F. Maurras, K. Truemper, and M. Akgül, *Polynomial algorithms for a class of linear programs*, Mathematical Programming **21** (1981), 121–136.


M. Newborough and P. Augood, *Demand-side management opportunities for the UK domestic sector*, Generation, Transmission and Distribution, IEE Proceedings, vol. 146, IET, 1999, pp. 283–293.


P. Partha, K. Rohloff, M. Atighetchi, and R. Schantz, *Managed mission assurance - concept, methodology and runtime support*, Proceedings of SOCIALCOM, IEEE, 2010, pp. 1159–1164.


S. Taherian, M. Pias, G. Coulouris, and J. Crowcroft, *Profiling energy use in households and office spaces*, Proceedings EECN, ACM, 2010, pp. 21–30.

References II


V. Verendel, *Quantified security is a weak hypothesis: a critical survey of results and assumptions*, Proceedings of NSPW, ACM, 2009, pp. 37–50.


J. Widen, M. Lundh, I. Vassileva, E. Dahlquist, K. Ellegård, and E. Wackelgard, *Constructing load profiles for household electricity and hot water from time-use data-modelling approach and validation*, Energy and Buildings **41** (2009), no. 7, 753–768.


J. Widen and E. Wackelgard, *A high-resolution stochastic model of domestic activity patterns and electricity demand*, Applied Energy **87** (2010), no. 6, 1880–1892.


Michael E. Locasto Yingbo Song and Salvatore J. Stolfo, *On the infeasibility of modelling polymorphic shellcode*, ACM CCS, 2007, pp. 541–551.