TRACE Literature Review

(Traversal-driven Risk Assessment of Composite Effects)

Authors: Frank Lynam
Nick Huston

July 2020

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Department No: P633
Project No.: 51IRDC19-MA
Document No: MP200498

McLean, VA

MITRE

Overview

As part of development of the MITRE TRACE (Traversal-driven Risk Assessment of Composite Effects) analysis capability, the TRACE team performed a literature review of existing work in the area of graph-based cyber attack analytics. This paper discusses this literature review collection effort. The bulk of these materials were collected and reviewed over several years of research. An internal MITRE Innovation Project helped to fund the generation of this paper, with the goal of providing accessible context to relate these works together and to TRACE.

This literature review presents as a brief recent history of one common thread of methodology and approaches in the academic literature upon which TRACE has been built. An annotated bibliography has also been included as an appendix, providing short summaries from the perspective of the reviewers and key highlights from the references cited here. A few additional references not directly relevant to the chronology itself are also included in the annotated bibliography.

Literature Review

As an introduction to general background, it’s important to start thinking about how to model the cyber problem. An approach often considered is the use of Markov chains, which may actually be largely unsuitable to this space.[1] Markov chains provide many mathematical advantages and are a very approachable modeling technique, however Markov chains require both memory-less processes and non-forking process. That is to say, if a cyber effect were modeled somewhat naively as a Markov process, it would be making the assumption that the attacker is picking the next step in their attack agnostic of where they’ve been before (potentially retreading previously compromised terrain) and that they could only pick one “next step” at any given time. Both of these are requirements for Markov processes, but are trivially nonsensical when modeling a cyber attack, making pure Markov approaches infeasible for this application.

Another aspect to understand the cyber problem is relating the possibility space to actual mission risk. Understanding mission risk due to enemy action has been traditionally approached through understanding the series of conditional or otherwise related probabilities of the confluence of events necessary for a weak point in a system design to be exploited.[2] Consider that the probability that a mission survives might be able to be described as the probability that it either doesn’t encounter an enemy or doesn’t have an exploitable weakness. Additional elements can be added to better describe further gating functions in that process, such as the probability that the enemy doesn’t know about the weakness, or the probability that their attack on that weakness fails. These concepts can be readily applied to a non-Markovian process description of cyber attack paths to develop the sequence of conditional probabilities that an adversary is successfully able to find and employ some cyber attack path against a mission function.

[1] “Remarks on Non-Markov Processes”, Utrecht, 1998

[2] “Vulnerability Risk Assessment”, ARL, 2000

This concept has been effectively employed using attack graphs,[3] and iterating on those graphs to determine efficient solution sets.[4] Early work focused on discrete events, where probabilities are either 1 or 0 (the vulnerability is known to be present or not). However, the application of probabilistic models that account for likelihood of targeting[5] or likelihood of novel effect development as a central element of developing a Mean Time to Compromise measure[6] easily extend these discrete graph concepts into non-Markovian process graphs. Empirical analysis of vulnerability discovery rates supports treating the mean time to discovery of any particular novel vulnerability as a Poisson process.[7]

For targeting, data suggests that low-tier threats are likely to exploit the fact that a vulnerability[8] is well-known.[9] Extensive[10] data[11] is available in this space, for particular types of publicly-known exploits on particular types of systems. It is the considerations of our team that this is due to the fact that leveraging that vulnerability does not betray or disclose knowledge of unpublished vulnerabilities, and in a wartime scenario it is these unpublished vulnerabilities that pose the actual threat to critical mission capabilities. This data breaks the cyber problem into two spaces: mitigating peacetime effects (exploitation of public vulnerabilities) and mitigating wartime effects (exploitation of undisclosed vulnerabilities). As it is the intent of this research to protect wartime operations, the research effort has focused on the ability to mitigate the risk posed by undisclosed vulnerabilities.

Further research evolved the general understanding of the process models to better capture mission process disruption and scenario-driven cyber end effects[12], as well as non-tree attack graphs with both forking and re-converging path choices,[13] providing mechanisms for much more realistic capture of the possible space of mission disruption and attack path selection.

Application of the Mean Time to Compromise concept to traditional security configuration considerations, such as “what are the odds the firewall settings are right”[14] begin to allow for a more engineering- and design-centric approach, less dependent on subjective quantifications of adversary capabilities. However, in application of empirical data to these factors, the observation is made that compromise rate is fairly invariant with items such as known vulnerability quantity, and that identifying “which indicators are truly important and how they affect [Mean Time to Compromise] will be an area for considerable future research.”[15]

[3] “Scalable, Graph Based Network Vulnerability Analysis”, GMU, 2002
[4] “Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs”, GMU, 2003
[5] “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems”, BCIT, PACG, 2004
[6] “Time-To-Compromise Model For Cyber Risk Reduction Estimation”, INL, 2005
[7] “Is Finding Security Holes a Good Idea?”, Rescorla, 2004
[8] “0-day Patch”, BlackHat, 2008
[9] “Does information security attack frequency increase with vulnerability disclosure, An empirical analysis”, CMU, 2006
[10] “Before We Knew It”, Symantec, 2012
[11] “Lessons Learned From a Rigorous Analysis of Two Years of Zero-Day Attacks”, Symantec, 2013
[12] “Threat Analysis Framework”, SNL, 2007
[13] “Measuring the Overall Security of Network Configurations Using Attack Graphs”, GMU, 2007
[14] "Estimating a System's Mean Time-to-Compromise", BCIT, BS, 2008
[15] “Comparing Electronic Battlefields”, BCIT, 2008

Additional progress on the modeling area was made in applying the concepts of common mode vulnerabilities in terms of commonly compromise-able "protection domains"[16], making the key observation that 60% of exploits observed in real data specifically allow for lateral movement vice focus on compromise of the specific component. In these cases, the risk posed by common mode systems is amplified, where a single exploit capable of providing for lateral movement results in the ability to rapidly pivot through a series of networks. These concepts are brought together to begin developing metrics for describing the resilience of systems based on attack graph models.[17] This work demonstrates the effective use of non-Markovian stochastic graphs to directly describe the relative merits across the security decision space, applying a well-founded engineering trade space analysis approach in a novel way to this problem space. This represents a set of core concepts around which the TRACE work has been built. However, additional work in this space begins to observe that the decision space for real attacks on a system of any meaningful size is impractically large to fully understand and analyze with traditional design of engineering approaches which examine the space of all variables.[18] This suggests that an employment of other analytical approaches or creative analysis algorithms may be needed for efficient and effective analysis.

Additional research has likewise evolved the general understanding of the cyber[19] and engineering[20] problems that are inherent in being able to describe both the attack graph itself and the end effects that can be employed to disrupt mission effects. Work to capture definitive principles about how to decompose cyber problems which soundly resonate with these other foundational works has been developed.[21] Approaches to apply a practical framework for quantification of this complete problem (both the likelihood of an initial effect and the likelihood of an impact) reminiscent of classical probabilistic vulnerability approaches have been developed.[22]

The observation is made that different types of systems (i.e. different operation systems or use cases) may have different types of vulnerabilities, and that difference must be captured in the attack graph.[23] Likewise, work progresses on capturing the undisclosed vulnerability space in terms of a simple discrete count of zero-days,[24] and attempts to estimate the probability of discovery and nature of those zero-days to establish a novel Mean Time to Compromise measure built entirely around the concept of highly-tailored predictive analytics of the rate of discovery of novel exploits.[25] At this point, a consistent description of the full problem space appears across the literature.[26]

A fairly complete decomposition of a standard model for a broadly-replicable component-level threat models becomes generally accepted in the form of a kill-chain, or the sequence

[16] "Advances in Topological Vulnerability Analysis", GMU, 2009

[17] "Measuring Security Risk of Networks Using Attack Graphs", GMU, 2010

[18] "Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs", GMU, 2012

[19] "Science of Cyber-Security", JASONS, 2010

[20] "Engineering a Safer World", MIT, 2011

[21] "The Science of Mission Assurance", JSS, 2011

[22] "A Method for Calculation of the Resilience of a Space System", Boeing, 2013

[23] "A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded components", UM, SPIIA, 2012

[24] "k-Zero Day Safety A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities", George Mason University, 2013

[25] "A Unified Framework for Measuring a Network's Mean Time-to-Compromise", GMU, 2013

[26] "A Method for Risk-Informed Management of Enterprise Security (RIMES)", SNL, 2013

of steps an adversary is expected to take to successfully execute a cyber attack.[27] Sophisticated applications of explicit modeling techniques applying real system data have then been employed building on the body of commonly-accepted core concepts for base model construction.[28] However, traditional graph theoretic analytics present challenges to employ for meaningful quantitative conclusions relative to the domain-specific analytics that have been developed, which are unfortunately far more computationally intensive.[29] Work to develop application-adaptive threat models which tailor to the component technologies alongside mission-oriented graph measures which present information in terms of mean times to undesired effects, such as a security failure, show promise as a development area in lieu of more classical graph theoretic[30] abstractions.[31] Summary work in graph-driven security metrics begins to categorize and structure more mission-centric metric models, further articulating the value of departure from more classical pure graph-theoretic approaches.[32]

The application of these concepts into a process graph which treats the generation of novel vulnerabilities as a Poisson process enables the use of Monte Carlo simulations to solve for the probabilities of these undesired events as a function of time and network architecture, by evaluating across the attack graph itself.[33] This bespoke analysis approach truly realizes the promise of the Mean Time to Compromise measure as a security analytic.

In parallel, the concept of a threat model can be informed by a deeper understanding of vulnerabilities themselves. By examining the nature of vulnerabilities, conclusions can start being drawn about consistency between classes of vulnerabilities over time, where "meaningful vulnerabilities are inherent to interfaces".[34] The related expert observation noted therein, that “time turns the improbable into the inevitable,” is consistent with prior empirical analysis suggesting that vulnerability discovery rates are consistent with a Poisson process model.

In recent years, several[35] mature[36] implementations[37] have become available which provide various types of solvers across these types of graphs. However, these approaches suffer from incomplete reference threat models, highly subjective reference risk measures, and require expert use.

Notes on TRACE

Like other current mature solutions in this space, TRACE builds on the history and body of research in this subject area, using a highly similar approach to understanding the threat problem space and the risk posed by mission effects. The primary research efforts we believe to be unique to TRACE are (1) the consistent reference threat model based on

[27] “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Lockheed Martin, 2013

[28] “Keeping Intruders at Large”, GMU, 2014

[29] “Metrics Suite for Network Attack Graph Analytics”, GMU, 2014

[30] “Measuring Enterprise Cybersecurity Risk Through Attack Graphs”, GMU, 2017

[31] “A Method for Modeling and Evaluation of the Security of Cyber-Physical Systems”, IUST, 2014

[32] “A Survey on Systems Security Metrics”, UT San Antonio, 2016

[33] “Quantifying the mission impact of network-level cyber defensive mitigations”, JDMS, 2016

[34] “Hints for High Assurance Cyber Physical System Design”, Galois, 2016

[35] “A game theoretic approach to cyber security risk management”, JDMS, 2017

[36] “Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options”, GMU, 2017

[37] "BluGen: An Analytic Framework for Mission-Cyber Risk Assessment and Mitigation Recommendation", JHU, 2017

empirically observed vulnerability discovery rates, (2) the formal system and mission modeling structures designed to be straight forward and adaptable enough to be employed by systems engineers with expertise in system design vice cyber analysts with expertise in the history just described, and (3) the specific graph analytics employed by TRACE. Future work will focus on packaging the developed analysis capability into an accessible solution which can be employed by a broad audience of users with little need for cyber expert oversight.

Appendix – Annotated Bibliography

This annotated bibliography provides a cross-section of work relevant to this problem area, from a variety of sources, in chronological order. Not all of these documents are cited in the main body of this report, but all are relevant and recommended reading on this subject. I want to especially thank my MITRE colleagues Scott Musman, Steve Noel and Les Servi for pointing me toward a number of these references. The reader is encouraged to review these references for themselves, and to draw their own conclusions about the best approach to this problem space.

"Windex, A Predictive Model of Operator Workload", Honeywell, 1988

An intriguing paper about a numerical model for operator overload. Leverages fundamental concepts like morphological matrices, numerical methods, and forking process flow concepts. While the math itself is useful for specific technical applications (e.g., mitigation analysis), a big general takeaway from this for everyone is that it's not that hard to use real math, even for complex or human-centric problems.

"Remarks on Non-Markov Processes", Utrecht, 1998

This paper could be described as arguing that Markov processes are overused due to the fact that they are easier to teach so more people understand them, but Markov is really only suitable for special cases. This suggests using caution whenever someone suggests using a Markov process, and validating that that kind of model is really appropriate.

"Vulnerability Risk Assessment", ARL, 2000

This is a foundational paper from Army Research Labs for how a lot of folks in the Department of Defense think about the concept of vulnerability from the perspective of mission risk. Required reading for working in this space.

"Scalable, Graph Based Network Vulnerability Analysis", GMU, 2002

Establishes multiple foundational concepts in graph-driven modeling of network security, in particular defining the monotonically-increasing intrusion depth assumption which, among other implications, makes Markov models non-viable.

"Birnbaum's measure of component importance for noncoherent systems", Loughborough, 2003

This is a good paper for describing Birnbaum's measure. It's an interesting graph metric, but it relies heavily on defining the structure and content of a graph in a very particular way (which isn't the way TRACE graphs are structured). I'm not certain how to make productive use of it for cyber, but potentially useful.

“Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs”, GMU, 2003

Uses attack graphs to efficiently search for effective mitigation sets in a straightforward manner. The number of references to GMU papers from Sushil Jajodia’s team in this annotated bibliography speaks for itself.

“Is Finding Security Holes a Good Idea?”, Rescorla, 2004

Examines vulnerability discovery rate from a purely empirical perspective, showing an exponential rate effect (consistent with a Poisson process) to a $p < 0.05$ level. Foundational model for the predictive analytics in TRACE.

"The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", BCIT, PACG, 2004

Provides useful background data. Talks about describing risk as “Likelihood * Consequence” and further breaks Likelihood down into the concepts of Threat, Vulnerability and Target Attractiveness. Data is based on self-reported incident data in Canada, where the threat source has shifted from mostly internal (pre-2000) to mostly external (post-2000) threats, and also breaks down percentages of different entry point types.

“Cyber Incidents Involving Control Systems”, INL, 2005

Great data on industry control system incidents from Idaho National Labs (INL). INL is widely recognized as a topical expert in this area.

“Time-To-Compromise Model for Cyber Risk Reduction Estimation”, INL, 2005

Fairly definitive work on empirical cyber risk prediction techniques. Provides citable numbers on mitigation effectiveness, ranging from 13%-30%. Has multiple examples of how people have tackled this issue before, with an extremely informative and useful history. Uses an equation for probability consistent with a Poisson process. Has metrics for the percentage of available exploits at differing skill levels based on actual analysis. Notably, their math converges on the inverse of some potentially subjective input factors, and appears to simply be amplifying input bias. However, this work cites the contemporary Rescorla work, observing that vulnerability generation rate can be treated as constant over time. Makes a case for an industrial control system-specific vulnerability enumeration repository, and identifies the threat posed by common-mode vulnerabilities.

“Does information security attack frequency increase with vulnerability disclosure, An empirical analysis”, CMU, 2006

Compares exploitation rate of patched and unpatched / published and unpublished vulnerabilities, which suggests that adverse actors tend to exploit publicly known vulnerabilities as much as possible. The authors make a good effort to ensure this work is not mis-interpreted to suggest that rapid patching of vulnerabilities as soon as they become public is more important than simply designing systems to have fewer vulnerabilities. Very good handling of data.

“Threat Analysis Framework”, SNL, 2007

This is a great SANDIA paper on threat analysis, which pairs well with the ARL 2000 paper to extends the same ideas into scenario-driven vulnerability assessments.

“Measuring the Overall Security of Network Configurations Using Attack Graphs”, GMU, 2007

This is a compelling GMU CSIS paper on attack graphs. Excellent discussion on the importance of using non-tree structures, and analysis issues that come from that.

"Integrating Security Modeling into Embedded System Design", ISIS, 2007

Introduces a Security Analysis Language and tool. Basically a model checker that performs two types of checks: 1) Ensure that the user-specified encryption algorithm and key size on every information flow is larger than what the user-specified adversary "knows how to break", and 2) Ensure that the user-specified sensitivity level of information that passes through each node is compatible with the user-specified access level of those nodes. Limited in scope to cryptography, but very interesting work on model expansion, where they set a useful pattern for transforming from any arbitrary design language to their analysis language and back.

“Framework for System Resilience Discussions”, Sheard, 2008

This is a paper on resilience written for human-driven analysis. It makes a compelling case, but may struggle with generalization and formality in characterizing the problem space to make it readily adaptable to more use cases.

“What’s Wrong With Risk Matrices”, Cox, 2008

This paper makes a compelling case against use of an explicit risk function where Risk = Likelihood * Consequence. Some of the conclusions also hold if other generalized functions are used. A good primer on the subject.

“Limitation of R=TVC for Terror”, Cox, 2008

Makes a strong case around the complexity of the “many-to-many” problem of mitigations having diverse and non-linear impacts on risk. Also makes a compelling case about limitations of game theoretical approaches, where fixing the “top n problems” simply makes problem “n + 1” the new top problem. Some of the essential challenging concepts here are that the adversary only needs to win once, but we have to defend against every way they could try, particularly in defense applications where impact is a fairly fixed cost (mission failure). Further, the concept of constrained resource models may not be representative at the relevant scales for many defense mission sets.

"Estimating a System's Mean Time-to-Compromise", BCIT, BS, 2008

A very compelling methodology, however it presents a heavy focus on security configuration practices (e.g. patching frequency, frequency of reviewing firewall rules, etc.) vice topological considerations. Does not have clear mission relationship model. A number of the posited supporting equations are not clearly substantiated by the content of the paper.

“0-day Patch”, BlackHat, 2008

Good breakdown of the elements of a zero-day patch cycle. The heavy focus on risks imposed by publicly disclosed vulnerabilities may not apply as readily to undisclosed vulnerability stockpiles.

“Comparing Electronic Battlefields”, BCIT, 2008

Leverages a Mean Time to Compromise metric with exponential curves for attacker capability. Provides substantial references for comparable work. Makes a strong case that network reconnaissance threats are not meaningful to address in risk modeling. Provides a case that compromise rate is invariant of vulnerability quantity. Argues that additional research is needed to determine "which indicators are truly important and how they affect” Mean Time to Compromise. Discusses future work on honeynets. Makes strong case for the value of "relative" metrics in this space vice "absolute" measures.

“What’s Wrong With Hazard Ranking Systems”, Cox, 2009

This discussion of the inappropriateness of correlated risk approaches is directly applicable to my own concerns with rank ordering attack paths, as mitigations can have multiple simultaneous impacts. This extends previous arguments made in Cox 2008 related to the morphological analysis needing to integrate graph theory to properly handle combinatoric effects. Notably, the graph iterative model in TRACE was specifically and intentionally designed to better handle the mitigation correlation issue as identified in this work. Additional discussions have direct applicability to translation of platform- / element-centric risks to fleet or campaign level analysis, which suggests it could also apply to redundant channels. The approach needs additional work to manage common-mode threats.

“Game Theory and Risk Analysis”, Cox, 2009

Makes a valid case against using incorrect mathematics in combinatorial processes.

“Advances in Topological Vulnerability Analysis”, GMU, 2009

Makes an argument around the concept of “protection domains,” which is highly comparable to common mode vulnerability. Good employment of the concept in their modelling approach, and directly relevant to TRACE. Notably, this work states that 60% of exploits allow lateral movement. Mathematical approach is fairly similar to the TRACE approach.

“Defense Industrial Base Supply Chain Assessment”, Bureau of Industrial Security, 2010

Fascinating and informative breakdown of counterfeit risks in the defense industrial base.

“Science of Cyber-Security”, JASONS, 2010

Discusses some foundational scientific approaches to cyber concepts. Provides insightful and informative context across the problem space at a very high level.

“Measuring Security Risk of Networks Using Attack Graphs”, GMU, 2010

Provides a solid mathematical approach to solving graphs, with a robust sensitivity study on reference data fidelity. Includes an excellent history on other efforts to create resiliency metrics.

"Designing Secure SCADA Systems Using Security Patterns", FAU, 2010

Advocates for the use of patterns as an effective method for ensuring security principles are applied to system designs, even if the system engineers are not security experts. Names but does not describe several such patterns. Patterns are noted as published, but I was unable to find them after a cursory search.

“Cyber Resiliency Engineering Framework”, MITRE, 2011

Good overview of the MITRE cyber resiliency concepts.

“Engineering a Safer World”, MIT, 2011

Foundational piece for Systems Theoretic Process Analysis, which is an increasingly important failure analysis method in industry and the military. I personally think the theory here is exactly right, definitional of how we should be thinking about defining the totality of the problem space for end effects. However, the notional implementation is very human-centric and presents some execution challenges for complex systems.

“The Science of Mission Assurance”, JSS, 2011

This is an excellent paper from Dr. Jabbour. I certainly cite it in numerous places, and it has a lot of higher order logic constraints that I think are consistently valid. I don’t know that I fully agree on his ontology of terms. Directly related to TRACE.

"A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded components", UM, SPIIA, 2012

Provides a “domain specific metamodel” for enumerating the types of attacks that a component might be vulnerable to according to attacker access type and ability level in order to facilitate requirements analysis. Does not calculate risk. Reliant on security expert's ability to predict a priori all relevant attack modes.

"SP 800-30 Guide for Conducting Risk Assessments", NIST, 2012

Provides a taxonomy and a high-level framework for conducting risk assessments of information systems. Defines risk in terms of likelihood and impact. Describes risk assessment at different tiers (i.e. levels of abstraction). Spells out "standard practices" for the general shape and composition of risk assessments without constraining the discussion to any particular methodology, implementation or domain.

“Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs”, GMU, 2012

An impressive cost model for hardening concepts. The selection of the graph model approach presents some technical problems for consistent representation of exploits and security conditions. Nevertheless, this analysis cleverly looks at removing functionality, vice implementing resiliency techniques and additional software, which is arguably both novel and extremely effective. It argues that the number of paths to assess makes assessing paths not necessarily actionable, which is an important idea. It references the 2002 GMU paper for down selecting subsets of attack graphs based on the monotonically increasing assumption.

“Before We Knew It”, Symantec, 2012

“Lessons Learned From a Rigorous Analysis of Two Years of Zero-Day Attacks”, Symantec, 2013

This is a somewhat large-scale, data-driven analysis with a focus on measuring the time to exploit published vulnerabilities. While the data only applies for Symantec-protected systems, it is still a good swath and makes a compelling case for an observable effect (and therefore exploitation rates are predictable).

"SysML-Sec SysML Environment for Design and Development of Secure Embedded Systems", EURECOM, 2013

This paper introduces the SysML-Sec profile which is meant to provide a taxonomy and methodology for combining the efforts of systems engineers and security engineers. However, the paper itself does not go into great depths on what is in the profile and the approach appears manual, qualitative, and primarily focused on requirements analysis.

“Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Lockheed Martin, 2013

This paper contains some foundational ideas in cyber-attack lifecycles, which bears a striking resemblance to earlier work from Air Force Research Labs as well as later work at MITRE on the MITRE Cyber Attack Lifecycle and the MITRE ATT&CK matrix. These concepts are definitely useful, and bear some significant relation to the ECHO traversal model. This piece of the problem is essential for tying the graph theory work to a useful cyber operations / cyber domain perspective.

“k-Zero Day Safety A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities”, GMU, 2013

This graph analysis is highly similar to the core elements of TRACE, but without the ECHO data analysis work for distribution function estimation. Excellent work. Most significantly, it’s about counting the number of unknown vulnerabilities you’d need before you’re at risk based on attack graphs, vice the number of known vulnerabilities.

“A Measurable Definition of Resiliency Using ‘Mission Risk’ as a Metric”, MITRE, 2013

This is a MITRE paper about measuring impact on a continuous scale (vice discrete as used in TRACE). This concept could arguably be more realistically characterized in terms of design margin to failure.

“A Unified Framework for Measuring a Network’s Mean Time-to-Compromise”, GMU, 2013

Combines the K-zero day concept with known vulnerabilities, but goes on to say doing so is nonsensical because of the predictable risk of unknown vulnerabilities. Their Mean Time to Compromise definition is highly consistent with TRACE. The paper provides an informative history of comparable metrics. While this method does handle the combinations of probabilistic process comparable to how TRACE does, it relies on CVSS scores as an input to determine the initial probabilities. Unfortunately, CVSS scores appear to have little bearing on the effect of the vulnerability itself on the attack graph. This method leverages a mathematical construct highly similar to a Poisson process.

“A Method for Risk-Informed Management of Enterprise Security (RIMES)”, SNL, 2013

Excellent definition of the cyber problem space. I’d argue it makes a strong case that traditional game theoretical analysis methods will fail in this area due to the high combinatorial complexity of the attack graphs, requiring an alternative definition of the game context to be effective.

“Resiliency Techniques for Systems-of-Systems”, MITRE, 2013

Expounds on the earlier Cyber Resiliency Engineering Framework work.

“A Method for Calculation of the Resilience of a Space System”, Boeing, 2013

Broadly referenced model for describing system resilience using a fairly straight-forward mathematical construct.

“On Mission Assurance”, AFRL, 2013

Focuses on the big picture across cyber in the DoD acquisition process and that relationship to all the dimensions of the cyber problem space.

"Designing Sequence Diagram Models for Robustness to Attacks", ECP, MAS Laboratory, 2014

Presents a methodology for modelling nominal behavior of a component-based system and known attacks on sequence diagrams and then using a computational engine to formally verify whether the behavior is robust to the attack based on whether or not it always reaches a state where a user-specified "security watchdog" (one of the components participating in the behavior) is prompted to emit a "warn" signal. It's not clear how well this translates to real systems or complex attacks which may not be easily modelled following their particular paradigm or whether this can derive any novel conclusions outside the information you already need in order to build the model in the first place.

"A Method for Modeling and Evaluation of the Security of Cyber-Physical Systems", IUST, 2014

Aims to provide quantitative measures of security for cyber physical systems, including "mean time to security failure", "steady-sate security", and "steady-state physical availability". Similar to other approaches, this method represents security failure in terms of loss of confidentiality, integrity or availability of individual components, without developing any mission relationship to those effects (a very reasonable simplification here). Unclear if there is a substantial objective basis for the fundamental equations and probability distributions that the core math depends on, or if the modelling paradigm is sufficiently detailed to represent (and therefore measure) how actual attacks happen.

“Metrics Suite for Network Attack Graph Analytics”, GMU, 2014

This outlines several different metrics available using the Cauldron tool, which are broadly generalized graph theoretic metrics with limited domain-specific utility.

“Keeping Intruders at Large”, GMU, 2014

Uses attack graphs to talk about how effective honeypots might be. This work really only applies to intrusions where the adversary has “hands on keyboard,” which may not be the limiting case.

“Formal Methods Case Studies for DO-333”, NASA, 2014

Studies on applied formal methods, with a broad conclusion that it’s easy, cheap and extremely effective.

"Design Techniques and Applications of Cyberphysical Systems: A Survey", IEEE, 2015

Talks about cyber physical systems very broadly. While this paper doesn't contain directly applicable details itself, it provides a long list of useful references on the topic of cyber physical systems and cyber security.

“Dramatically Reducing Software Vulnerabilities”, NIST, 2016

Further studies on applied formal methods, with a broad conclusion that it’s easy, cheap and extremely effective.

“A Survey on Systems Security Metrics”, UT San Antonio, 2016

An excellent survey paper which grapples with rigorously defining the space of possible “answers” or metrics from a number of insightful angles with some pretty compelling context. Notably makes the strong statement that "quantitative metrics are weak due to unavailability of data to support or refute them". The meta-analysis or metrics is severely limited to a traditional IT scope (i.e. continuously evolving systems, up-to-date patching, internet facing). Identifies that antimalware tools can detect 45% of malware, which is a substantially higher claim than anywhere else I've seen that estimated. Excellent discussion on zero days and targeted attacks.

"Quantifying the mission impact of network-level cyber defensive mitigations", JDMS, 2016

Excellent, mature application of Poisson processes in a Monte Carlo model for evaluating the effect of patching cycles. While the threat space is exceptionally narrow, the approach itself has a heavy similarity to TRACE.

"Hints for High Assurance Cyber Physical System Design", Galois, 2016

Simply spectacular paper on formal methods from the folks who brought us HACMS. States that buffer overflow is a solved problem. Identifies that "meaningful vulnerabilities are inherent to interfaces", where in their analysis "virtually all vulnerabilities emerged at the interface boundaries between code written by distinct organizations". Makes the claim that the threat concept distribution holds across classes of vulnerabilities, like cyber physical systems to information technology, which I can't imagine how to prove but we do currently assume in TRACE. TRACE uses that assumption as a basis to argue that addressing classes of vulnerabilities vice specific holes improves security more efficiently. Notes that "in the fault-tolerance community we say that 'time turns the improbable into the inevitable'"

"Analyzing Mission Impacts of Cyber Actions (AMICA)", NATO, 2016

Brief overview of the AMICA tool with little technical detail. Highly similar to TRACE, but I was unfortunately never able to connect with their team to elicit any details about its design or operation.

"Cyber Risk Assessment in Distributed Information Systems", CDR, 2016

Largely about the execution value from pairing design analysis with red teaming (called red books vs blue books). The blue book process involved a functional / physical model interaction concept seen across the literature.

"Deriving Global Criticality Conditions from Local Dependencies", MITRE, 2016

Major paper on using Functional Dependency Network Analysis to develop a Degradation Index metric. Struggles to provide meaningful justification for the structure of the graph, the formulation of the underlying mathematics, or the conceptual basis for the Degradation Index metric itself.

“Table-top Mission Cyber Risk Assessment Standard”, SPAWAR, 2016

“Attack Path Analysis Model”, AFRL, 2016

“Cyber War Gaming”, AFRL, 2016

“Cyber Table Top Guidebook”, NAVAIR, 2016

“Cyber Risk Assessment Standard Work Package Implementation Guide”, NAVAIR, 2016

“Adversary-Driven Cyber Resilience”, MITRE, 2017

A variety of human-driven cyber risk assessment approaches. Largely, these processes can be consistently described as subject matter expert generation of somewhat subjective pseudo-quantitative measures employed in an ad-hoc computational fashion.

"BluGen: An Analytic Framework for Mission-Cyber Risk Assessment and Mitigation Recommendation", JHU, 2017

Touches on a lot of the same points as TRACE with regards to automating the analysis process, tying risk to likelihood and mission impact, and a persistent and growing catalog of asset types, threat types, mitigations, and mappings between them. It may be beneficial in the future to standardize the TRACE catalog around the BluGen Entity Type Taxonomy in their Reference Catalog; they use an inheritance structure with their entities similar to what we have considered with our asset types in the past (e.g. Cisco Router -> Router -> Network device, etc., with threats and mitigations associated with each). At a glance, BluGen may be challenged due to a lack of consideration of the network topology – assets are considered in isolation. Also, the method for determining likelihood and impact seems to lack a robust empirical basis (largely a simple ratio of the number of threats that are unmitigated to the total number of threats that apply along with some subjective scoring of criticality).

“Measuring Enterprise Cybersecurity Risk Through Attack Graphs”, GMU, 2017

This is a great paper on lots of different technology agnostic approaches to graph theory-based network analysis. Reading between the lines, it makes a solid case that they all only have any potential meaning if you have an extremely homogeneous network, which makes them a challenge to apply to most defense systems.

"Comparative Review of DoD Mission-Based Cyber Risk Assessment Methodologies", Institute for Defense Analyses, 2017

A review created by the Institute for Defense Analyses of twenty different cyber risk assessment methodologies that are in use by the Department of Defense. There is also a section that describes some considerations for choosing which methodology may be a best fit for a given acquisition program.

“Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options”, GMU, 2017

Using attack graphs to harden networks against unknown vulnerabilities. Effective treatment of cost and other programmatics. Excellent highlight of the need for solving a well-defined problem, emphasizing the struggle on how to collect likewise rigorous data to substantiate a real model, and how to define a set of factors that are meaningfully bounding of the problem space.

“A game theoretic approach to cyber security risk management”, JDMS, 2017

Foundational paper for the MITRE Cyber Security Game tool. Largely, the big muscle movements keep pace with the literature. Appears to leverage somewhat informal and subjective models to drive conclusions, which may be resolved in implementation details not stated in the paper.

“Design and Acquisition of Software for Defense Systems”, Defense Science Board, 2018

This paper is on software development security in particular.

“Systems Confrontation and System Destruction Warfare”, RAND, 2018

Excellent RAND paper on Chinese systems model theory used to characterize warfare analysis. Compelling in the way it contextualizes the entire trade space for confrontation between complex socio-technical systems. Highly comparable graph theoretical concept problem which may directly relate to the larger discussion of attack graphs and systems analysis.