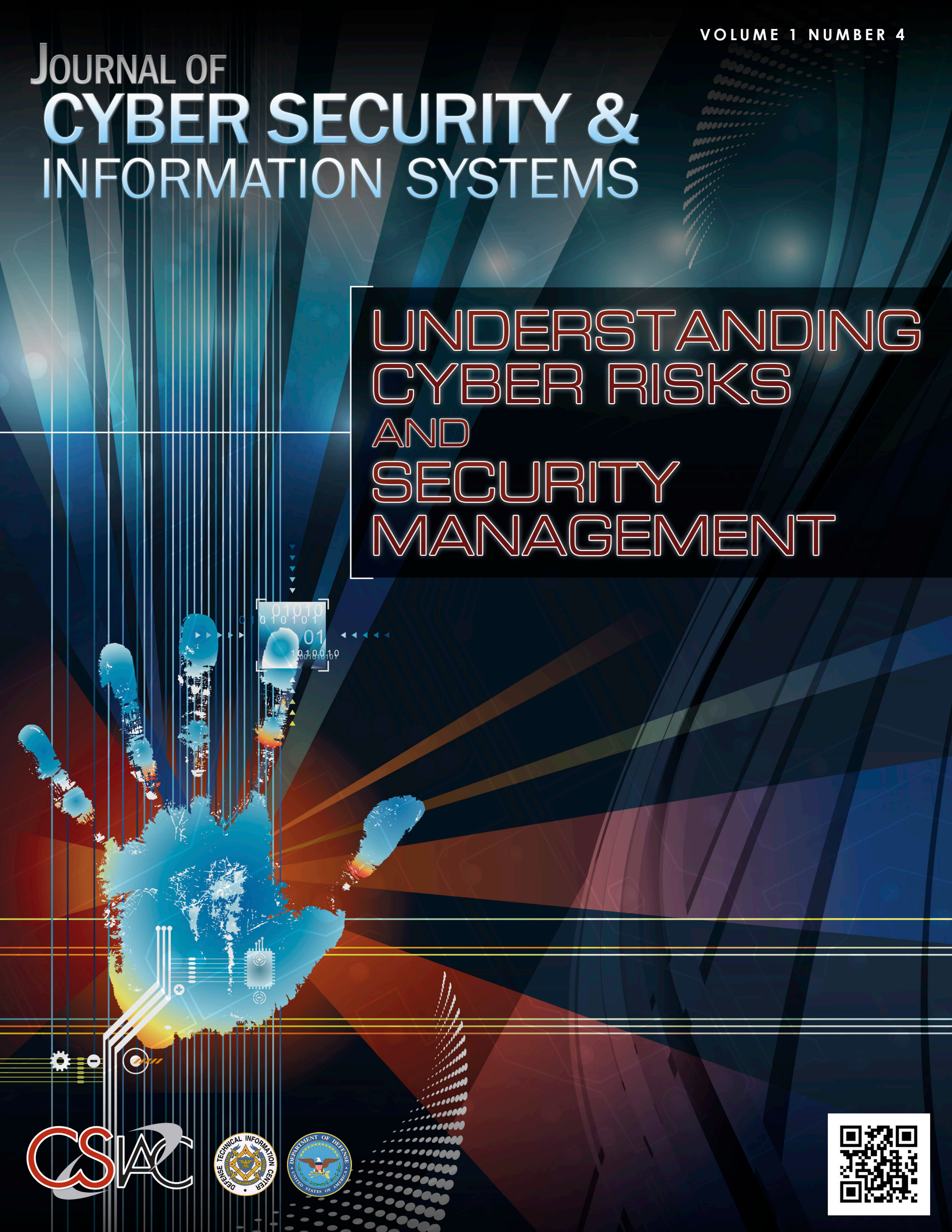
VOLUME 1 NUMBER 4

Journal of Cyber Security & Information Systems



Understanding Cyber Risks and Security Management

CSIAC

Cyber Risk to Transportation Industrial Control Systems

By R. Michael Robinson, Ph.D., Barry Ezell[1], Ph.D., Peter Foytik, M.S., Craig Jordan, P.E., and Joseph Weiss

This paper is a result of a cyber risk assessment undertaken with the goal of increasing the cyber awareness of operators of infrastructure, managers, and political leadership. The meaning of cyber has, in our opinion, been aggregated to a bumper sticker label so generic, it means very little of anything to anyone trying to understand cyber risk. Senior executives and political leaders have a very limited understanding of industrial control systems (ICS) and the crucial role ICS provide to public/private infrastructure, industry, and military systems. Therefore, to accomplish our purpose, we conducted a cyber-risk study focusing on a bridge tunnel ICS – a scenario of concern. In this paper we present the analytic approach, discuss our model, simulation, and analyze the results using a notational data and generic system description. As a result of this study we were able to discuss the importance of controls systems with senior leaders. We were able to demystify what we mean by "cyber" showing that it is possible through simulation to inject the effects of cyber scenarios of concern into simulations to assess impact. There was also an unintended benefit: During a system audit, ICS operators with decades of engineering experiences began to realize that the ICS is vulnerable to willful intrusion. More of these studies are needed to raise awareness.

Introduction

The rapid growth of information technology and increased interconnectivity has led to increased efficiency and functionality for transportation infrastructure. However, it has also significantly increased the risk to the cyber systems essential to the safe and continuous operation of the Commonwealth's transportation infrastructure. There is increasing concern among both government officials and industry experts regarding the potential for a cyber-attack on a national critical infrastructure via industrial control systems. Experts believe that ICS are more vulnerable today than in the past due to the increased standardization of technologies, the increased connectivity of ICS to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems (Wilshusen, 2012). Reported attacks and unintentional incidents involving control systems demonstrate that a serious attack could be devastating (Weiss, 2010).

ICSs are used to monitor, operate, and control major industrial systems including power production, power transmission and distribution, water and wastewater control, and transportation systems such as the bridge tunnel systems (Boyer, 1999). These systems are connected through a communications network that can include physical cable connection, radio signals, microwave, satellites, or connection through the Internet over LAN and WAN. As ICSs have evolved, they have increasingly embraced open forms of communication and are therefore vulnerable to many of the same threats as any typical corporate TCP/IP based communication system. In a typical ICS, there is very little authentication of the origin of the signals. A properly encoded transmission is usually accepted by the supervisor station and remote units without verification. If an attacker were able to access the ICS communications network for instance, they would be able to send deceptive signals to disrupt normal transportation operations by overriding failsafes in systems and cause severe infrastructure disruption and extensive downtime (Weiss, 2007).

Consequences of disruption of these critical infrastructures is not constrained to owners and operators, but can have a substantial impact on the rest of the community. Disruption of power, contamination of water supplies, and the breakdown of a transportation network can all have far reaching economic, social, and even human impacts to the entire region by disrupting businesses, creating widespread unrest, and creating illnesses and injuries. To date, there have been four control systems cyber incidents in the US that resulted in fatalities, three major cyber-related electric outages, and two nuclear plants shutdown from full power. Cyber incidents have impacted water, electric, manufacturing, transportation, and pipelines.

To address a situation described above we conducted a risk assessment. Risk assessment answers three questions: what can go wrong; what is the likelihood; what are the consequences (Kaplan and Garrick, 1981)? In this paper, we define risk as potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences (DHS Risk Lexicon, 2010). Conceptually, we model risk as the triplet of threat, vulnerability, and consequence. Mathematically, we calculate risk by multiplying the probability of an attack P(A), the probability of success, given an attack P(S|A), and the associate consequences, C. Equation (1), then, is a common expression of homeland security risk (Ezell et al., 2010).

$$Risk=P(A)\times P(S|A)\times C \qquad (1)$$

This probabilistic relationship has been used by DHS since 2005 and has been shown to be a useful first-order indicator of terrorism risk as the expected consequences (loss of lives, economic losses, psychological impacts, etc.) against which the benefit of existing or potential terrorism strategies, policies, and countermeasures can be evaluated and estimated (Ezell et al., 2010). However, Parnell et al. (2008) and others have been critical of the model in dealing with an intelligent adaptive adversary. In this probabilistic framework, the attack probabilities P(A) in Equation (1) are for the most part agreed to be the most challenging to estimate. Quantifying P(A) requires knowledge, data, or modeling about the motivations, intent, and capabilities of terrorists (largely the domain of the intelligence community), in addition to -- or instead of --knowledge about historical attacks and their relevance to current risk. Our analytic approach detailed in the next section addresses adversary behavior by including system audit and red team assessment to design an intelligent attack vector as one would expect a serious adversary to do.

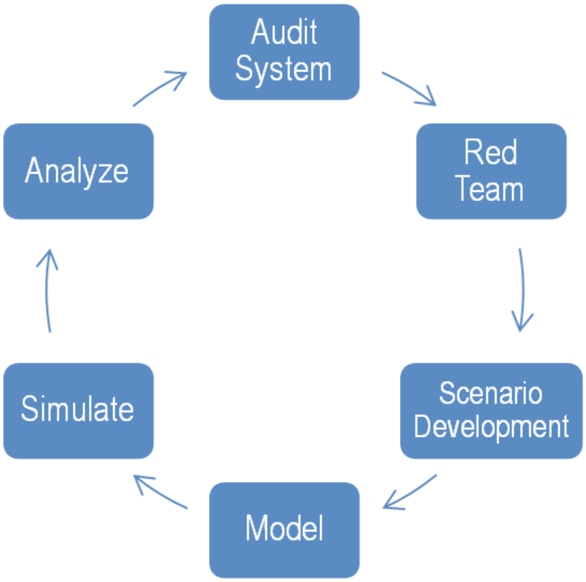


Figure 1. ICS Risk Analytic Methodology

Analytic Approach

Figure 1 depicts the six step analytic methodology we employed. The process began in step one Audit System, when we met with a transportation planning organization to assess the regional impact of cyber-attack on a tunnel system that resulted in a complete and extended (at least eight hours) closing. To accomplish this, we conducted site visits to the tunnel system to interview key stakeholders and learn about the ICS, workforce, and the physical tunnel system (step two). As a result of these visits, we concluded that for the tunnel system, a Stuxnet-styled attack through the ICS USB thumb drives was a scenario of common concern (step three). In step four we developed a model to estimate the likelihood of the scenario and the system consequences. Following this, we injected the effects of the cyber-attack into the transportation model to simulate the regional impact (step 5) and analyzed the results (step 6).

Stuxnet Cyber-Attack on a Tunnel's ICS

In this section we describe the scenario narrative. Second, we discuss the event tree model to estimate the likelihood of attack, followed by the transportation model to assess the regional impact. The final section concludes with a summary of the risk. For the tunnel scenario we chose to use a Stuxnet-style of attack that would be installed on the system unknowingly by one of the ICS operators through a USB file transfer. The motivation and intent behind the operator's actions are not part of the scenario. Obtaining the virus could occur in many places, i.e. conferences, tradeshows. It is however, an action that is similar to those of a disgruntled employee, trusted insider, or one bribed by an external threat. It is also important to note that because of the nature of the analysis, all of the data is notional and the details of the model are generic.

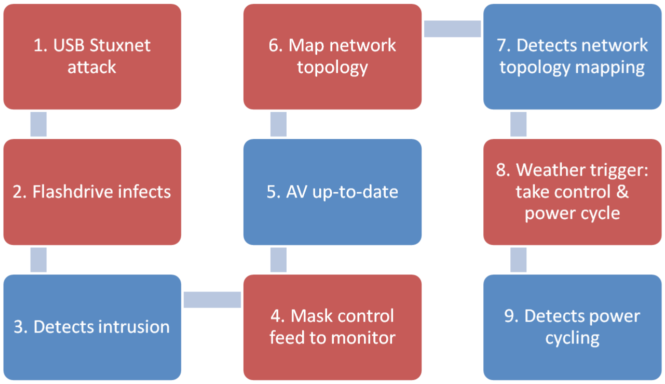


Figure 2 Incident Chain to Assess Scenario Likelihood

Notional ICS Description

The Tunnel ICS is an off-network system, meaning the ICS is not connected to the Internet or a part of the office LAN. All the program logic controllers (PLC) are hardwired to the system and at no point is the system connected to the Internet. Program changes and updates are pushed through using *USB transfer* from control system engineer to the SCADA system.

Red team attack vector and plausible scenario was described in the following way. A control system engineer doing scheduled maintenance on the control system placed all the upgrade files and program changes on his USB device that he uses for all of his daily work. A virus from his computer made its way to the USB device he was using. Because no malware checks were conducted on the USB drive prior to mounting it to the control system servers, the malware made its way to the ICS system without detection.

Once the virus was on the system it went live, going throughout the control system network, corrupting program files, changing file types and causing disruptions on the HMI user screen. After several weeks no major disruptions occurred and the virus was still undetected. The virus was designed to wait until sensors logged a heavy rain day and at that time, the virus would activate and cycle equipment off and on. Using a *Confiker*, the virus would mask the operator's monitor from the actual logged data. Based on recent similar attacks, forensics after the attack and damage would occur weeks later.

Estimating the Likelihood of Attack

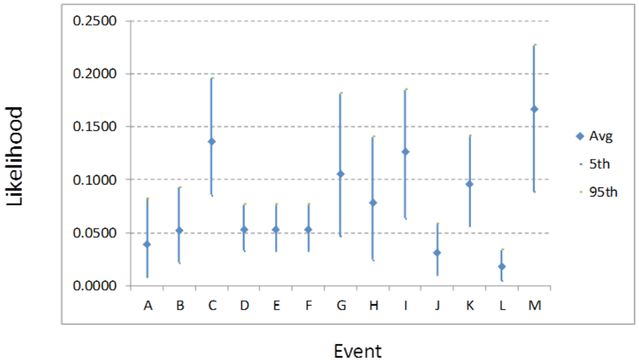


Figure 3. Events A-M: Tunnel Damage to Equipment vs. Likelihood Estimates

To model the attack, we developed an event tree using the incident chain shown in Figure 2. Each event (or node) is color coded red to indicate attack steps, or blue to indicate tunnel system actions. At each node in the tree, there was two-way branch split for yes/no or success/failure pairings. Event trees inductively model the sequences of events that lead to consequences. Event trees models work by assigning probabilities to branches to represent the likelihood for the correct value for each branch. Probabilities are assessed conditionally on the assumption that all the branches leading to that node represent the true state of the preceding parameters. Because they are conditional probabilities for an assumed mutually exclusive and collectively exhaustive set of values, the sum of the conditional probabilities at each node is one[1].

Mr. Joe Weiss, the project team's cyber consultant, provided probability estimates for each step[2]. For the probability estimate, we elicited a minimum, most likely, and max value to account for uncertainty. Using Oracle's Crystal Ball simulation software, we simulated the attack in the event tree. For the simulation, we assumed the Stuxnet style attack was

[1] For more information on event tree modeling, see Ezell et al. Probabilistic Risk Analysis and Terrorism Risk, Risk Analysis, Vol. 30, No. 4, 2010 (http://www.dhs.gov/xlibrary/assets/rma-risk-assessment-technical-publication.pdf)

[2] Joseph Weiss is an industry expert on control systems and electronic security of control systems, with more than 35 years of experience in the energy industry. He has conducted numerous SCADA system vulnerability assessments, taught numerous SCADA security short courses, given several university lectures, and authored the book- Protecting Industrial Control Systems from Electronic Threats.

initiated. The results of the simulation indicate that six paths through the event tree resulted in tunnel damage to pumps and fans as shown in Table 1. Figure 3 shows the uncertainty associated with likelihood estimates for each probability path (event) in the tree. For instance, Event C is the most likely event leading to tunnel damage.

Table 1. Event Probabilities for Paths in the Event Tree Model

Tunnel Damage to Pumps and Fans						
A	B	C	D	E	F	
No Damage to Pumps or Fans						
G	H	I	J	K	L	M

Consequences: Regional Impact of Tunnel Closure

The notional tunnel complex (Tunnel A) in this scenario is 5 miles long and enables vehicles using a highway system to traverse through the region. It serves as the major crossing between the northern and southern sectors of a major metropolitan area. A second tunnel complex (Tunnel B) serves a similar function located on the western side of the region between the north and south side.

The northern sector was simulated as having a population of approximately 400,000 and the southern sector a population of approximately 800,000. In addition to its higher population, the south side has a high proportion of the region's employment. The composition of the region's economy results in significant weekday peak period traffic flows from north to south in the morning and from south to north in the evening. Approximately 200,000 vehicles cross Tunnel A and Tunnel B daily in the region with Tunnel A serving a higher proportion. Daily traffic volumes across the Tunnel A exceed 90,000 vehicles. Peak period demand at Tunnel A exceeds 4,500 vehicles per hour, significantly greater than the typical maximum highway capacity simulated of 4,000 vehicles per hour.

Traffic was simulated for a nine-hour period, beginning one hour prior to the AM peak period and continuing until just prior to the expected start of the PM peak period. The one-hour of simulation prior to the AM peak period was used as a warm up period in order to fulfill the assumption that the road network would be populated when the simulation begins. Both the northbound and southbound tubes of the tunnel complex were simulated to be closed without warning due to flooding beginning at 7 AM as a result of the cyber-attack simulated. Identification and correction of the cause of flooding and restoration of traffic flow was simulated to require more time than available between morning and evening peak periods.

Simulation Testing

The tunnel scenario was simulated using Cube Avenue®, a mesoscopic traffic simulation. A mesoscopic simulation was selected for testing because it allowed assessing results in sufficient detail while allowing the high total number of vehicles over a regional network to be simulated in each run (over 1 million vehicle trips). Mesoscopic simulations model vehicles in packets with the number of vehicles included in each packet assigned by the user after considering the intended purpose. For these tests, 10 vehicles were included in each packet. The mesoscopic simulation allows dynamic loading of vehicles and better representation of peak period conditions. Figure 4 shows the rates of vehicle loading over the tested period.

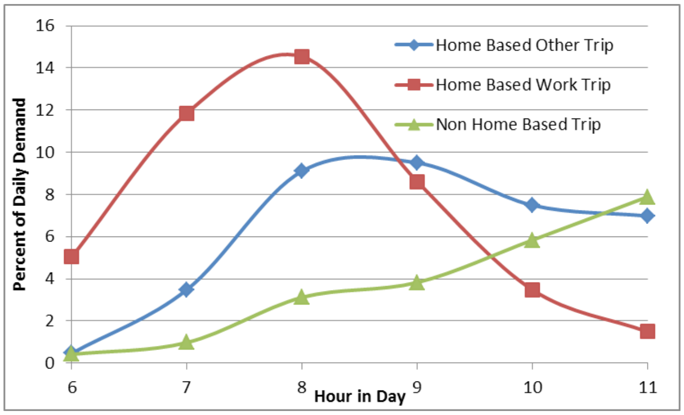


Figure 4. Demand Curves used for the Peak Period Mesoscopic Model

Simulations were initially run to establish and measure network conditions in a typical peak period. Each simulation run used to represent typical conditions were run for 10 iterations to approximate equilibrium conditions. Simulations were then run to simulate the hacked scenario with the network modified by closing the tunnel one hour into the simulation. This timing meant that some vehicles would have chosen their commute path prior to the closing and traveled far enough to prevent them from being able to adjust their route when congestion related to the closure became apparent. Simulations for the cyber-attack scenario were run for 7 iterations. Reducing the number of iterations allowed the simulation to appropriately model vehicles not having prior knowledge of the tunnel hacking. This resulted in the simulation allowing some vehicles to reroute because of the attack, but still model the confusion of vehicles attempting to travel across the tunnel without prior knowledge of the tunnel being shut down.

Intelligent Transportation Systems (ITS) could be used in a similar real world scenario to warn travelers or suggest alternate routes of the closure, but were not simulated in the scenario since most commuters would have begun travel or selected their routes prior to tunnel closure and ITS was unlikely to significantly reduce the severity of results. No accidents or incidents were simulated at any location. Metrics included in testing included:

- Total vehicle travel times for vehicles from the north to south
- Total vehicle travel times for all vehicles in region
- Total vehicle volumes across each major water crossing
- Queues remaining at the end of the simulation

Table 2 provides average results for the typical and hacked scenarios of vehicle packets with origins and destinations for trips that utilized Tunnel A during typical conditions. Table 3 provides total system averages of all packets in the system, not just packets that used the tunnel. Thirty simulation runs were made for each case, each with different random seed values. As can be seen in Table 2, the average travel time for the vehicle packets traveling over the tunnel increased from 54.5 minutes to 170.9 minutes because vehicles in the hacked case were forced to reroute resulting in congestion of the alternate crossings. This results in an increase of 214% in average travel time. Table 3 indicates that the average travel time of all vehicles traveling in the system increased from 19.4 minutes to 34.7 minutes (a 94% increase). In addition, the table 3 shows that the average speed of the vehicles traveling in the system decreased from 29.21 mph to 16.42 mph (a 44% decrease).

Table 2. Travel time results for just origin destination pairs that used the tunnel during the base scenario

Case	Total Packets Traveling between North & South sectors	Total Packet Travel Time (TT) Minutes	Average Packet TT Minutes
Base	27,437	1,386,208	54.5
Hacked	21,421	4,540,232	170.9

Table 3. System average speeds for base and hacked tunnel scenarios from 30 simulation runs with varying random seed values

		Travel Time Minutes		Speed Miles Per Hour	
Case	Vehicle Trips	Average	Standard Dev.	Average	Standard Dev.
Base	1,140,545	19.4	2.811	29.21	4.397
Hacked	1,140,545	34.7	4.448	16.42	2.512

Tunnel Consequence Analysis

As one might expect, most southbound traffic that would normally have used the Tunnel A diverted to Tunnel B when Tunnel A closed. Tunnel B is typically underutilized during all normal conditions, including the morning peak period. However, simulation tests showed that total vehicle volumes using the tunnel B remained under capacity during the AM peak period, even when traffic diverted from the tunnel with knowledge of the tunnel closing. This was due to vehicles that normally use the tunnel B having already cleared the crossing before the arrival of rerouted vehicles from the tunnel. The increase in vehicle volume significantly increased delays at already congested Southside bottlenecks.

The travel time for vehicles that would be expected to use other roadways in the region increased by 97%. Total delays at bottlenecks were so severe that they caused the average travel times for [all] regional commuters (not just those using affected routes) to nearly double from 19.4 to 34.7 minutes. Average travel times for commuters from the northern sector to the southern sector increased by 68%, from 54.5 to 170.9 minutes.

An additional analysis of traffic conditions at tunnel B and a river bridge in the region was conducted to assess what might happen during the PM peak period. In contrast to what was seen in the AM period, all commuters in the PM knew of the Tunnel A's closure prior to starting their trips. We expected that this would lead to more vehicles reaching the crossings at the same time, causing congestion that would not normally be present. As forecast, the additional traffic leaving the southside caused already severe congestion for westbound travelers. Traffic volumes were higher than with Tunnel B's availability, but remained below capacity with no queuing. This was due to the extensive congestion at other bottlenecks slowing the rate at which vehicles reached the Tunnel B.

Results

The simulation runs performed used traffic volumes consistent with a typical weekday. Congestion increases during the summer tourist season with more than 30 thousand vacationers traveling to Southside and thousands of others traveling through the region. Greater travel time delays might occur if a cyber attack happened during the peak summer tourist season. Accidents and incidents were not considered in the study. Commuters in any major urban area know how dramatically such events can increase travel. Because the simulation runs did not take this into account, the travel time delays may be conservative.

The impact of ITS variable message signs, radio traffic reports, and traffic information systems components were not simulated. Use of these systems to direct commuters to viable paths might have reduced some travel times. However, as seen in a test scenario with Tunnel A closed, increasing the number of commuters who arrive at network choke points such as all water crossings at the same time may actually exacerbate the congestion problem and have an effect in direct opposition to that desired.

The tunnel scenario caused an increase in total regional travel time of 276,116 hours. Considering only the hourly delay and assigning an average time value of $25 per hour provides an estimated cost of over $6.9 million. The risk of this scenario in terms of regional travel time and cost is assessed as the likelihood of the scenario resulting in tunnel damage times the increase in regional travel time exceeded 100,000 hours and $3 million, not including tunnel damage costs.

Risk Avoidance and Mitigation

There are many ways to mitigate this attack at very low cost. At the beginning of our paper we stated that an important goal was awareness. ICS engineers must know that simply not being connected to the Internet does not mean ones ICS is inoculated from cyber exploitations such as the one presented in this paper. One low cost mitigation solution would be to place a computer offline to test USB drives for viruses or malware before putting them on machines to run patches. Another mitigation strategy would be to adopt formal procedures for how updates are applied as well as policies on procurement of USB drives. For instance, free USB drives from conferences are a known source of malware and honeypots.

Conclusion

This paper describes a modeled scenario to understand the risk from willful intrusion into ICS regarding the tunnel. The cost impact is much less than kinetic attacks on the tunnel itself. However, the risk is still considerable at an expected value of 105,878 hours in regional travel time increase and $2,645,839. Also, we did not consider the societal risk perception impact as it was beyond our scope. The consequences of a tunnel cyber-attack scenario caused an increase in total regional travel time of 276,116 hours and an estimated cost of $6.9 million.

Despite known vulnerabilities to ICS, many critical infrastructure owners and operators have not taken the steps to adequately protect their ICSs. The scenario and simulated results show that physical separation of ICS and office communication networks is not sufficient cyber protection. The tunnel scenario shows how unintentional human interaction with ICS and lack of understanding of the types of control system attack vectors available to adversaries remain vulnerable to external penetration or internal threats. The reality is most networks are connected at numerous uncontrolled points through simple things like roaming notebooks and back-up data servers. Gaining access to a relatively unprotected network would be enough to allow an attacker to gain full control of the ICS in less than an hour, sometimes in minutes.

References

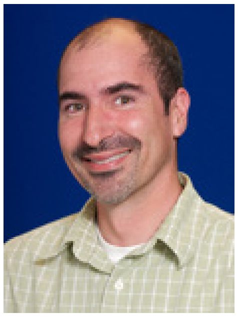
1. Wilshusen, G. (2012). Threats Impacting the Nation, Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, U.S. Government Accounting Office, Washington D.C.
2. Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats, Momentum Press, NY.
3. Boyer, S. (1999). SCADA Supervisory Control and Data Acquisition – 2nd Edition, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.
4. Weiss, J. (2007). Threats Impacting the Nation, Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, U.S. Government Accounting Office, Washington D.C.
5. Kaplan, S. and Garrick, B. (1981). On the Quantitative Definition of Risk, *Risk Analysis*, Vol. 1, No. 1, pp.11-27.
6. DHS Risk Lexicon (2010). Risk Steering Committee, p.27.
7. Ezell, B., Bennett, S., Von Winterfeldt, D., Sokolowki, J., and Collins, A. (2010). Probabilistic Risk Analysis and Terrorism Risk, *Risk Analysis*, Vol. 30, No. 4, pp. 575-589.

About the Authors

Dr. Mike Robinson is the Director of the Old Dominion University Center for Innovative Transportation Solutions and the lead transportation researcher at ODU's Virginia Modeling, Analysis, and Simulation Center. Mike came to ODU following a career as a nuclear submarine officer in the U.S. Navy. His research interests have focused on emergency transportation response, decision-making, and cyber security. He received an MS Degree in Physics from the Navy Post-Graduate School in Monterey, CA and holds a Ph.D. in Modeling and Simulation from ODU.

Dr. Barry Ezell is the President of the Security Analysis and Risk Management Association and Chief Scientist at Old Dominion University's Virginia Modeling Analysis and Simulation Center. Barry is best known for his contributions in terrorism risk analysis, critical infrastructure and industrial control system risk analytics. Barry is a retired U.S. Army military officer and has 24 years of experience in military decision-making, operations research and risk analysis in the U.S. Department of Defense and U.S. Department of Homeland Security. Ongoing applied research and analytic work combines advanced concepts in adversary modeling, verification and validation, transportation infrastructure cyber risk assessment, and developing risk models to inform programmatic acquisition decisions at the federal, state, and local levels of government.

Peter Foytik has been a modeling and simulation professional for 8 years at the Virginia Modeling Analysis and Simulation Center (VMASC). Peter has a bachelor's degree in computer science and a master's of science in modeling and simulation. With a background in computer science, initial expertise has been in software development of support tools for simulations and models. For the last 5 years most of his work has been focused on transportation modeling and simulation with expertise in regional models used for planning. Projects include macroscopic as well as mesoscopic transportation model development. His latest research has included microscopic simulations enhanced with simulated vehicle to vehicle communication to support emergency response vehicles as well as utilizing artificial intelligence methods to improve performance of transportation models and simulations.



Craig Jordan is a Senior Project Scientist at the Virginia Modeling Analysis and Simulation Center (VMASC). Craig received his Bachelor's degree in Civil Engineering from the University of Connecticut and his Master's degree in Modeling and Simulation from Old Dominion University. Prior to joining VMASC, he was a design engineer for a civil engineering consulting firm. Craig's research interests include traffic microsimulation, connected vehicle applications, and emergency evacuations.

Joe Weiss provides thought leadership to industry and government in the area of control system cyber security and optimized control system performance. He has provided support to domestic and international utilities and other industrial companies. He prepared white papers on actual control system cyber incidents supporting NIST SP 800-53. He is supporting the NRC on the Regulatory Guide for nuclear plant cyber security. Mr. Weiss chairs the annual Control System Cyber Security Workshop and is an invited speaker to numerous cyber security and critical infrastructure events. He has co-authored a chapter on cyber security for Electric Power Substations Engineering as well as numerous articles. Mr. Weiss provided expert testimony to the October 17, 2007 House Homeland Security Subcommittee and provided control system cyber security recommendations to the Obama Administration. He has prepared a module for the IEEE Education Society. he is now a US Expert to IEC TC65 WG10.

CSIAC Cyber Security & Information Systems
Information Analysis Center

Journal of Cyber Security & Information Systems
Supervisory Control and Data Acquisition
Journal of Cyber Security & Information Systems
Understanding Cyber Risks and Security Management

Call for Papers for Publication

The Cyber Security and Information Systems Information Analysis Center (CSIAC) - https://thecsiac.com, is one of eight Department of Defense Information Analysis Centers (IACs) sponsored by the Defense Technical Information Center (DTIC) - http://www.dtic.mil/dtic/.

CSIAC has been formed as the consolidation of three legacy IAC's – the Information Assurance Technology Assurance Center (IATAC), the Data and Analysis Center for Software (DACS), and the Modeling and Simulation Information Analysis Center (MSIAC) – along with the addition of the new technical domain of Knowledge Management and Information Sharing. CSIAC is chartered to leverage best practices and expertise from government, industry, and academia on Cyber Security and Information Technology. CSIAC's mission is to provide DoD a central point of access for Information Assurance and Cyber Security to include emerging technologies in system vulnerabilities, R&D, models, and analysis to support the development and implementation of effective defense against information warfare attacks.

CSIAC publishes the quarterly *Journal of Cyber Security and Information Systems*, focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories. The latest issue may be viewed or downloaded at https://www.thecsiac.com/journal/welcome-csiac.

CSIAC will be accepting articles submitted by the professional community for consideration in the 2014 publications.

Articles in the areas of ***Information Assurance, Software Engineering, Knowledge Management, Information Sharing,*** and ***Modeling & Simulation*** may be submitted.

CSIAC will review articles and assist candidate authors in creating the final draft if the article is selected for publication. However, we cannot guarantee publication within a fixed time frame. Note that CSIAC does not pay for articles published.

To Submit an Article

Drafts may be emailed to Journal@thecsiac.com.

Preferred Formats:

- Articles must be submitted electronically
- MS-Word, or Open Office equivalent

Size Guidelines:

- Minimum of 1,500 – 2,000 words (3-4 typed pages using Times New Roman 12 pt font)
- Maximum of 12 pages, double column, including references
- Authors have latitude to adjust the size as necessary to communicate their message

Images:

- Graphics and Images are encouraged.
- Print quality, 200 or better DPI. JPG or PNG format preferred.

For the full Article Submission Policy, see page 30 of this journal.

An Overview of the Schedule Compliance Risk Assessment Methodology (SCRAM)

By Adrian Pitman, Elizabeth K. Clark, Bradford K. Clark, and Angela Tuffley

Schedule slippage is an unfortunate reality for many large development programs. The Australian Defence Materiel Organisation Schedule Compliance Risk Assessment Methodology (SCRAM) provides a framework for identifying and communicating the root causes of schedule slippage and recommendations for going forward to Program and Executive-level management. It is based on a repeatable process that uses a root cause analysis of schedule slippage model to locate factors that impact program schedule along with a "health check" of the documented schedule, assessing its preparation and probability distribution of completion dates. SCRAM can be used at the commencement of a program to validate a proposed schedule and identify potential risks, during program execution as a "health check", or as a diagnostic tool to identify root causes when schedule slippage occurs. To date, SCRAM has been applied to a number of major development acquisition programs in Australia and the United States.

According to one documented report, seventy-eight percent of US Department of Defense Programs have experienced some form of schedule slippage [1].

Schedule slippage is a symptom of any number of problems or causes occurring on a project. Examples include:

Optimistic, unrealistic estimates	Conflicting views among stakeholders
Evolving or unstable requirements	Poor subcontractor performance
Use of immature technology	Dependencies not realized and/or often not scheduled
Poor monitoring of changing workloads	Poor quality work leading to unanticipated or unplanned rework
Incurring Technical Debt with no plans to repay	Inadequate staffing
Lack of adequate planning and preparation for System Integration	Artificially imposed deadlines
Poorly constructed schedules	Lack of Technical Progression
Poor management communication	Lower than estimated productivity

Trying to identify root causes of schedule slippage is not always easy but is necessary if schedule slippage is to be remedied and managed.

This paper introduces the Schedule Compliance Risk Assessment Methodology (SCRAM) used by the Australian Defence Materiel Organisation (DMO) to identify and quantify risk to schedule compliance. SCRAM is an assessment approach and product suite developed by the authors and funded by the Australian DMO to facilitate remediation of troubled acquisition projects.

This paper describes the Root Cause Analysis of Schedule Slippage (RCASS) model used in SCRAM. Next the techniques used in SCRAM to estimate the most likely schedule completion date are discussed; these include Monte Carlo Schedule Risk Analysis and Parametric Software Modeling. Finally the methodology for collecting, organizing and communicating information is briefly described.

RCASS Model

Schedule slippage is a *symptom* of overly optimistic planning or other problems that negatively impact progress.

SCRAM is focused on identifying risks to compliance with a program schedule.

SCRAM utilizes the Root Cause Analysis of Schedule Slippage (RCASS) model that organizes these problems into ten information categories. These categories and relationships are adapted from McGarry [2] and Boehm [3]. They have been further refined based on experience with a number of SCRAM assessments.

The RCASS model is shown in Figure 1. The forward direction of an arrow indicates that there is an effect of issues in one category upon another. All arrows eventually lead to the bottom of the figure and to the categories that are of main concern: Program Schedule & Duration and Project Execution. By uncovering issues in each category, it is possible to identify risks and problems to schedule compliance and the causes of delays.

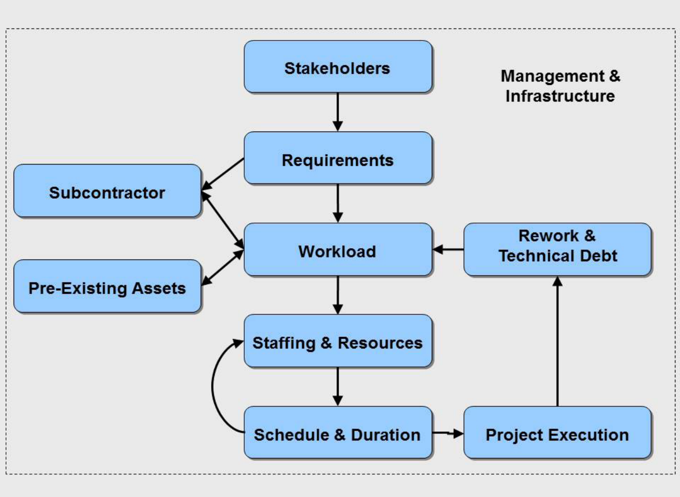


Figure 1. RCASS Model

The following sections briefly describe each RCASS category and present some sample questions addressed by a SCRAM team; during a SCRAM assessment, the answers to these questions help to identify root causes of schedule slippage. A real-world example of an issue or problem in the category is also provided.

Stakeholders

Description: Issues in this category represent project turbulence and entropy caused by difficulties in synchronizing the project's stakeholders.

Questions: Who are the stakeholders? How do they interact on requirements clarification, technical problems, and tradeoff analysis? Are one or more stakeholders imposing unrealistic constraints on implementation solutions or acceptance testing?

Example: One developer on a program described their stakeholders as being like a "100-headed hydra: nobody could say "yes" and anyone could say "no."' Stakeholder turbulence negatively impacts the ability to define a stable set of requirements.

Requirements

Description: Issues in this category represent the understanding and stability of the functional and non-functional requirements, performance requirements, system constraints, standards, etc. used to define and bound what is to be developed.

Questions: Are all of the requirements defined and understood? Have the requirements been agreed to? Are there (Regulatory and Technical) standards that have to be implemented? Is there a mapping of requirements to development builds and production components? Are there technical performance requirements that are being tracked? Are the interfaces to other systems well understood?

Example: One program misinterpreted a communication standard and discovered late in development an additional 3000 message format requirements implied by that one standard. Needless to say, the program schedule slipped.

In Figure 1, the arrow from requirements to subcontractors represents the handing off of program requirements to subcontractors so as to reduce the workload for the prime contractor. The arrow to Workload means that requirements are the basis of workload estimation and that workload increases with volatility or poorly defined requirements. Programs are often plagued with the IKIWISI (I'll Know It When I See It) approach to requirements definition and sign off which creates unplanned rework.

Subcontractor

Description: Issues in this category represent the subcontractor products or services that will be delivered as a part of the overall system. In Figure 1, the arrow from Subcontractor to Workload reflects additional work to correct poor quality products or handle late deliveries. Late products will cause other system components to be delayed having a ripple effect on workload and delivery schedules.

Questions: Are there subcontractors involved? When are their deliverables needed? How is subcontracted work coordinated, integrated and accepted? Are subordinate schedules aligned and integrated in an integrated Master Schedule? Are system interfaces well enough defined for the subcontractor to deliver a product that works within the system?

Examples: One program had a subcontractor that claimed highly mature development processes. A visit to the subcontractor site revealed that developers were sidestepping processes in order to make deadlines incurring Technical Debt (defects). Another program had a subcontractor that was eight time zones away severely restricting coordination and virtual meetings that impacted schedule performance.

Pre-Existing Assets

Description: Issues in this category represent products developed independently of the project that will be used in the final product, i.e. an asset that reduces the amount of new work that has to be done on a project. In Figure 1, the arrow from assets to workload shows that incorrect assumptions about functional assets may impact the amount of work to be done.

Questions: What COTS, MOTS, NDI, or GFE products are being used on the program? Are they providing the required functionality and are they meeting hardware constraints? Are there legacy products being used and were they developed locally? Is the current product architecture defined and stable enough to evaluate and accept other pre-existing products? Do existing interface definitions accurately describe the actual product interface? What level of assurance accompanies the product? How will unused function or features be managed?

Examples: A common program issue is the underperformance of pre-existing products, i.e. the legacy systems or COTS products do not work as advertised. Another common issue stems from underestimating the amount of code that must be written or modified in using a legacy product. One program reviewed planned to only modify 10% of a legacy system but by the end of the development phase, 50% of the system had been modified to satisfy requirements increasing the Workload dramatically.

Workload

Description: Issues in this category represent the quantity of work to be done and provide a basis for estimating effort/staffing and duration. Issues with requirements, subcontractor products, functional assets, and rework may negatively impact this category.

Questions: Is the scope of work well understood? Is the workload changing for any reason, e.g. changing requirements, unstable platform or unplanned rework? Is workload being transferred to a later build? Workload is different depending on the development life cycle phase. Has the amount of work to be done been quantified, e.g. number of requirements, hardware and software configuration items or test procedures to be developed?

Examples: Many programs underestimate the amount of software code to be written and the amount of documentation to be developed and reviewed.

Staffing and Resources

Description: Issues in this category represent the availability, capability and experience of the staff necessary to do the work as well as the availability and capacity of other resources, such as test and integration labs. The arrow in Figure 1 points from staffing and resource to schedule because issues in this category may negatively impact the amount of time needed (schedule) to do the 'actual' work.

Questions: Are the right people (with the right experience) working on the program and are there enough people to do the work? Is the work force stable or is there turnover? Are the key personnel qualified to lead their area of work? Programs often suffer staffing issues related to high turnover, especially among experienced staff; bringing more people onto the program late making things worse.

Example: An interesting example of a staffing issue on a program was that of the "star" software developer. This one person understood the most about how the software system worked. Even though he worked long hours, he was a bottleneck. He was so busy, he did not have time to respond to problems, train others or update design documentation.

Schedule and Duration

Description: This is a category of primary interest that is impacted by issues in the other categories. Issues in this category represent the task sequencing and calendar time needed to execute the workload by available staff and other resources (e.g. test labs).

Questions: What is the current schedule with respect to milestones, builds and phases? What are the dependencies, when are they due and are they linked into the schedule? What was the basis of estimates used to construct timelines, e.g. were analogous projects or parametric models used to estimate duration? Is there any contingency built into the schedule or is it success oriented? What is the "health" of the current schedule?

Example: A typical behavior seen in programs that slip schedule is early milestones or deadlines are missed, new requirements are added, productivity is lower than estimated but schedule milestones do not change. Activities later in the development cycle then get their durations squeezed. A common remedy is to add more people late in the program to increase production. This typically slows down progress due to lack of familiarization and training and increases communication overhead among development teams.

Project Execution

Description: Issues in this category stem from problems in communicating the schedule and monitoring and controlling the execution of the project in accordance with the project schedule. As shown in Figure 1, the capability to execute a project schedule is impacted by the feasibility and "health" of the schedule itself as well as by the effectiveness with which the scheduled tasks are executed. In relation to the latter issue of effectiveness, experience from multiple SCRAM assessments has highlighted the need to focus on Technical Progression and System Integration.

Many programs fail to validate actual versus planned productivities.

Questions: When was the schedule base-lined? Is it being used as a communication, monitoring and control tool? Is there an integrated master schedule? How is progress being tracked? Does actual productivity match the estimated or planned productivity? Does everyone on the project have access to the schedule (at an appropriate level of detail)? Are System Integration and Formal Test phases conducted as discrete activities with specific objective entry and exit criteria? Is the system under development Technical Progression based on objective evidence of a maturing system and is the level of maturity commensurate with the resources and scheduled consumed?

Example: Generally, programs report schedule problems as they enter the System Integration and Test phase. Progress stalls as tests become blocked whilst issues with the system integration and test are resolved. This typically reflects a lack of adequate planning, grooming and qualification testing prior to conducting formal testing.

Rework and Technical Debt

Description: Issues in this category represent additional work caused by the discovery of defects in the product and/or associated artefacts, as well as work that is deferred for short-term expediency (Technical Debt) and their resolution. Causes include rushing into development before requirements are fully understood, skipping inspections and verification testing due to lack of time, and deploying a product before the operating environment is ready. Technical Debt is often accrued with no plans to repay the debt until perhaps too late. The arrow in Figure 1 shows the disrupting impact that rework and technical debt has on workload.

Questions: Has the likely amount of rework been estimated and planned? Are the compounding consequences of incurring intentional Technical Debt identified and understood?

Examples: Technical Debt is often incurred through the suspension of process (e.g. stop peer reviews to meet deadlines) and other process short-cuts. Rework is often underestimated, not planned or prioritised for correction.

Management and Infrastructure

Description: This category impacts all of the above information categories. Issues in this category reflect the factors that impact the efficiency and effectiveness of getting work done, e.g. work environments and processes, use of management and technical software tools, management practices, etc. Efficiency is negatively impacted by a lack of tools, lack of facilities and burdensome security requirements. Effectiveness is negatively impacted by poor management practices such as in the areas of quality assurance, configuration management and process improvement.

Questions: Have the capacity requirements for the development system infrastructure (e.g. integration labs, network bandwidths etc.) been explicitly estimated based on an analysis of historical productivity and system under development operational performance needs? Is an active process improvement program in place that is driven by best practice assessment (e.g. CMMI)? Is the configuration management/change control system cycle time suitable to support development performance? Does the quality management system adequately support the program?

Example: It is common for programs to have inadequate system integration and test facilities in terms of capacity and/or fidelity, e.g. simulators, emulators, and live environments. On a major aircraft development program that involved very large size software development, it was found that the Configuration Change Management System could not keep pace with the software defect notification and resolution process slowing down software release to systems integration.

Schedule Risk Assessment and Parametric Modeling

Schedule Risk Assessment: During a SCRAM Review a schedule health check is performed to evaluate the quality of a schedule to determine its suitability for running a Monte Carlo simulation. The health check examines the construction and logic of the schedule under review and includes an analysis of the schedule work breakdown structure, logic, dependencies, constraints and schedule float.

A Monte Carlo analysis is then performed on the critical path and near critical path tasks and work packages in the schedule; an example of the output of this type of analysis is shown in Figure 2. Tasks are allocated three-point estimates based on the assessed level of risk. During a SCRAM assessment, risks and problems identified from each of the RCASS categories discussed above provide input into these probability estimates. The three-point estimate (pessimistic, optimistic, most likely) can be applied with either a generic risk multiplier (derived from past experience) across all like tasks or a risk factor based on a task-by-task risk assessment.

The result of the Monte Carlo analysis is a distribution showing the percentage probability of achievement for any planned delivery date. If the planned program delivery is on the left side of the program completion distribution curve, there is cause for concern, depending on the degree of risk the stakeholders are prepared to accept. Projects should use the results of the analysis to develop mitigation plans to ensure that the risks don't become reality.

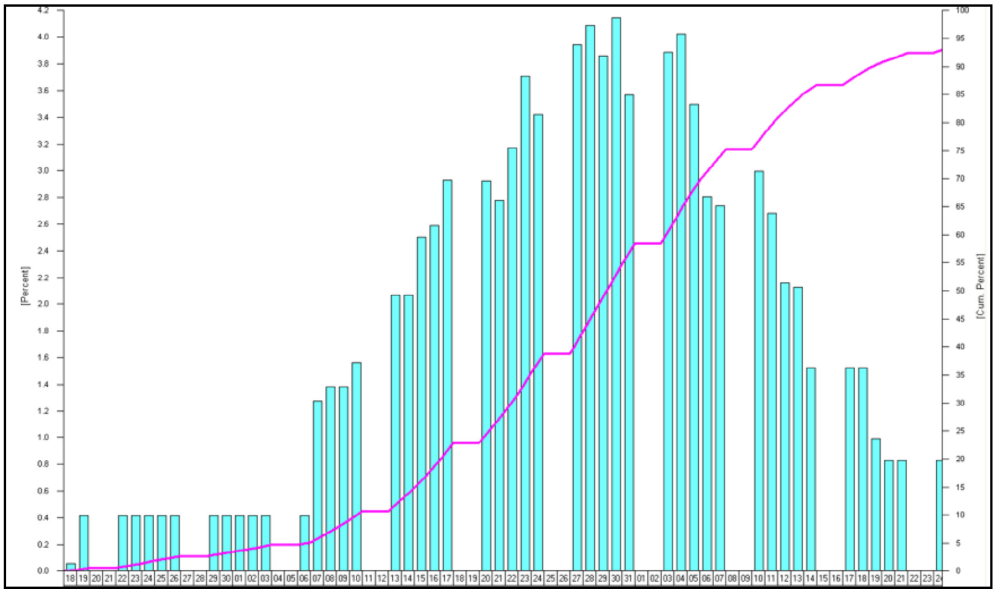


Figure 2. Monte Carlo Schedule Analysis

Another consideration of a SCRAM schedule health check is the allocation of schedule contingency. Some contingency is recommended for the inevitable rework. It is important to have some schedule contingency distributed throughout the schedule accompanying the higher risk tasks instead of a cumulative buffer at the end of the schedule before delivery or held as management reserve. This will allow some slippage to occur during development without disrupting subsequent successor task(s) scheduling.

Software Parametric Modeling: SCRAM can be applied at any point during the system engineering or project lifecycle. For the software development elements of a program, a schedule forecast tool is used to assess existing schedule estimates. SCRAM includes this forecasting activity because software is a common schedule driver for complex systems and software durations are almost always optimistic. While SCRAM is not dedicated to a specific forecasting tool, the preference is to use a tool that uses objective software metric data 'actuals' that reflect the development organization's current performance or productivity.

The inputs to the model are size (usually estimated source lines of code and actual code complete to date), major milestones planned and completed, staffing planned and actual, and defects discovered.

Figure 3 below shows a typical output from a modeling tool.

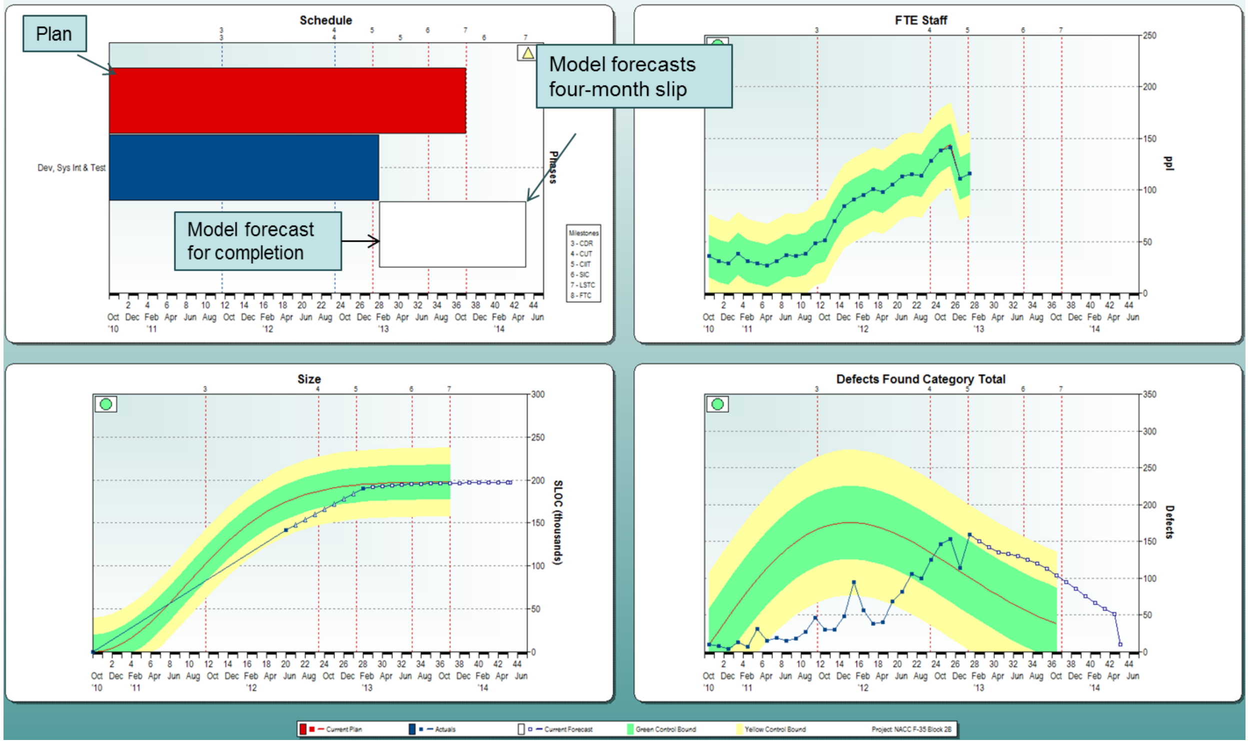


Figure 3. Parametric Modeling

SCRAM Methodology.

SCRAM has been used to find the root causes of schedule slippage and recommend improvements on programs that have experienced multiple or protracted schedule overruns. Moreover, SCRAM has proven extremely valuable in communicating schedule status and root causes of slippage to senior executives. Several recent SCRAM assessments found that schedule slippage was, in part, due to factors outside of the program's control. Once aware of these factors, executive management was able to bring about changes to facilitate resolution. Examples include late requirements levied by a senior external stakeholder and competition for operational assets that were required for system test on another program. Other examples were provided in each RCASS category discussed above.

In addition to using SCRAM once a program is experiencing problems, SCRAM provides a methodology for conducting an independent review of risk to program schedule.

SCRAM reviews produces three types of outputs:

1. Identification and quantification of Schedule Compliance Risks (this includes identification of significant schedule drivers, root causes of existing slippage, risks to schedule and the potential impact on Program objectives)
2. The "health" of the current program and schedule
3. Recommendations for going forward

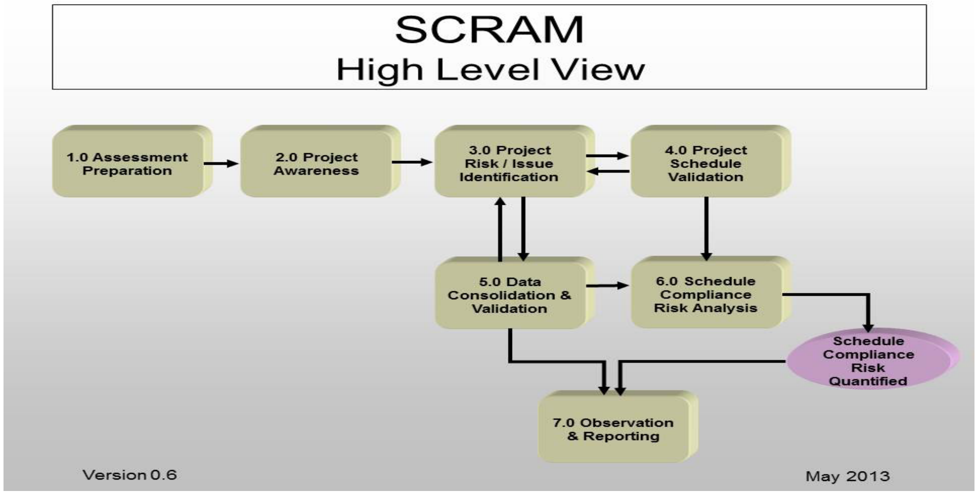

SCRAM
High Level View
1.0 Assessment Preparation
2.0 Project Awareness
3.0 Project Risk / Issue Identification
4.0 Project Schedule Validation
5.0 Data Consolidation & Validation
6.0 Schedule Compliance Risk Analysis
Schedule Compliance Risk Quantified
7.0 Observation & Reporting
Version 0.6
May 2013

Figure 4. SCRAM Assessment Process Overview

In the DMO a SCRAM assessment is conducted by a small team of highly experienced system and software engineering subject matter experts along with a schedule specialist, (someone who knows how to operate the project's scheduling tool and who is an expert in schedule preparation and construction).

There are seven key principles for this review methodology:

Minimal Disruption: Program information is collected one person at a time in an interview that usually lasts no more than one hour.

Rapid turn-around: For major programs a SCRAM team typically spends one week on-site gathering information and data. A second week is spent consolidating, corroborating, analyzing and modeling the data culminating with an executive presentation on the results. The RCASS model is used to structure the presentation to show the interrelationships (causes and effects). Finally, a written report is provided by the end of the fourth week.

Every activity has a stakeholder, a need, work to be done, people to do the work, and a timeframe.

Independence: Review team members are organizationally independent of the program under review.

Non-Advocate: All significant issues and concerns are considered and reported regardless of source or origin. The review does not favor the stakeholder, customer, end-user, acquisition office, or developer.

Non-Attribution: None of the information obtained on an assessment is attributed to any individual. The focus is on identifying and mitigating risks to schedule.

Corroboration of Evidence: The findings and observations of the review that are reported are based on at least two independent sources of corroboration.

Openness and Transparency: For the Monte Carlo analysis or software parametric analysis component of a SCRAM review, the developer is invited to assist in resolving data anomalies, witness the analysis process and challenge model results. This transparency (no surprises) builds cooperation, trust and confidence in the schedule forecast. However the SCRAM Team is the final arbiter.

Interviews are conducted with key personnel, both acquisition office and developer, and the review questions are structured around RCASS categories. Interview comments are captured then tagged to the relevant RCASS category. The review includes the examination of program development plans, management and product artifacts, risk databases and the schedule health check discussed earlier.

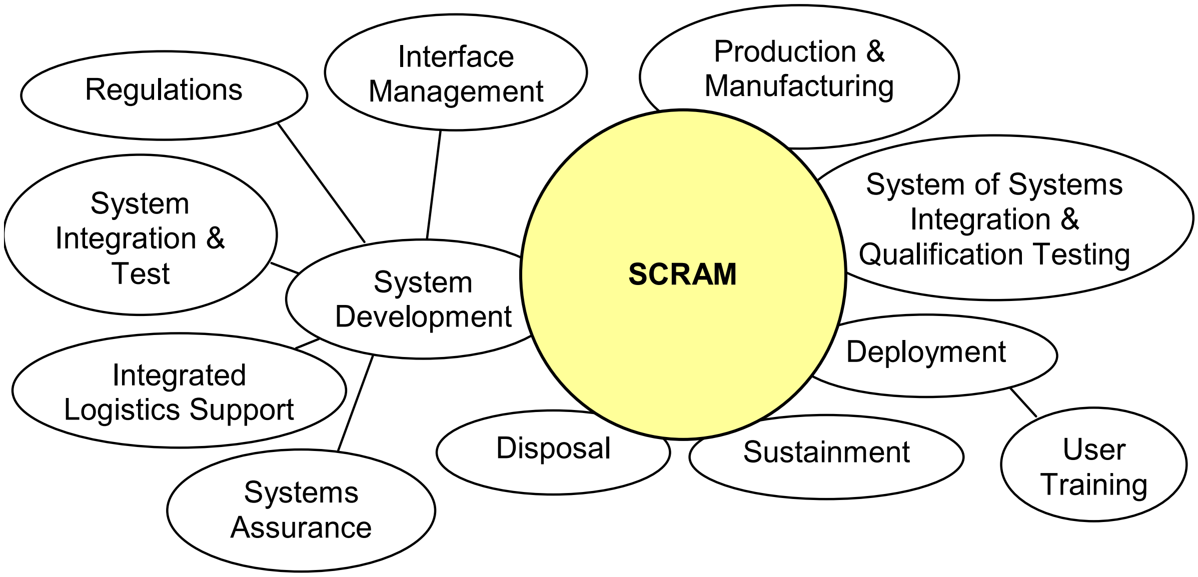

Regulations
Interface Management
Production & Manufacturing
System Integration & Test
System of Systems Integration & Qualification Testing
SCRAM
System Development
Deployment
Integrated Logistics Support
Disposal
Sustainment
User Training
Systems Assurance

Figure 5. System Life Cycle Activities

As previously stated SCRAM can be applied to any major system engineering activity on a program (Figure 5). All of these activities have stakeholders, tools and facilities, requirements to be accomplished, possible help from subcontractors, a defined amount of work to be done, quality standards, staff to do the work, a timeframe to accomplish the work, and processes and infrastructure to support the work.

Elements of the SCRAM Product Suite

Apart from the RCASS Model described in this paper, additional elements of the SCRAM Product Suite include:

- An ISO 15504 [4] compliant Process Reference / Assessment Model (PR/AM) for SCRAM (Relates processes and best practices to the relevant RCASS category)
- SCRAM PR/AM Model and Assessor Training Courses
- SCRAM Assessor Guidebook

The PR/AM is available for download from www.scramsite.org. Additional details about SCRAM can also be found at this website

SCRAM Application

There are three potential areas of SCRAM application:

Pro-Active SCRAM or P-SCRAM: Conducted at or immediately prior to or shortly after Contract (e.g. at Integrated Baseline Review) to ensure the systemic issues covered by SCRAM are avoided.

Monitor SCRAM or M-SCRAM: Conducted at regular intervals to monitor all categories for status and new risks, i.e. provide program health checks to support appropriate gate or progress reviews.

Diagnostic SCRAM or D-SCRAM: Conducted on challenged programs or programs of concern. The methodology is used to assess the likelihood of schedule compliance and identify root causes of schedule slippage. Recommendations are made to remediate or mitigate the issues and risks respectively.

References

1. Edmound Conrow, "An Analysis of Acquisition Cost, performance, and Schedule Characteristics for DOD Programs," Acquisition Community Connection, Defense Acquisition University, 2003.

2. John McGarry, David Card, Cheryl Jones, Beth Layman, Elizabeth Clark, Joseph Dean, and Fred Hall, "Practical Software Measurement: Objective Information for Decision Makers," Addison-Wesley, 2001.

3. Barry Boehm, "Section 2: Risk Management Practices: The Six Basic Steps," from Software Risk Management, IEEE Computer Society Press, 1989.

4. Ricardo Valerdi, "The Constructive Systems Engineering Cost Model (COSYSMO): Quantifying the Costs of Systems Engineering Effort in Complex Systems," VDM Verlag, 2008.

5. International Organization for Standardization; ISO/IEC 15504.2:2003 – Information Technology Process Assessment – Part 2: Performing an assessment

About the Authors

Mr. Adrian Pitman is the Director Acquisition Engineering Improvement in the Standardisation Office of the Australian Defence Materiel Organisation (DMO). He has over 45 years military systems experience, including 20 years as a member of the Royal Australian Air Force and 25 years in capital equipment acquisition in various engineering, project management and quality assurance management roles. Throughout his career Adrian has focused his work on implementing organizational improvement including his role as a foundation member of the DMO Software Acquisition Reform Program and as Director Quality Systems in the Australian Department of Defence. Adrian obtained his engineering qualifications at the Royal Melbourne Institute of Technology and is a SCRAM Lead Assessor, a former DMO CMMI Lead Assessor, ISO 9001 Lead Auditor and a Certified International Software Configuration Manager.

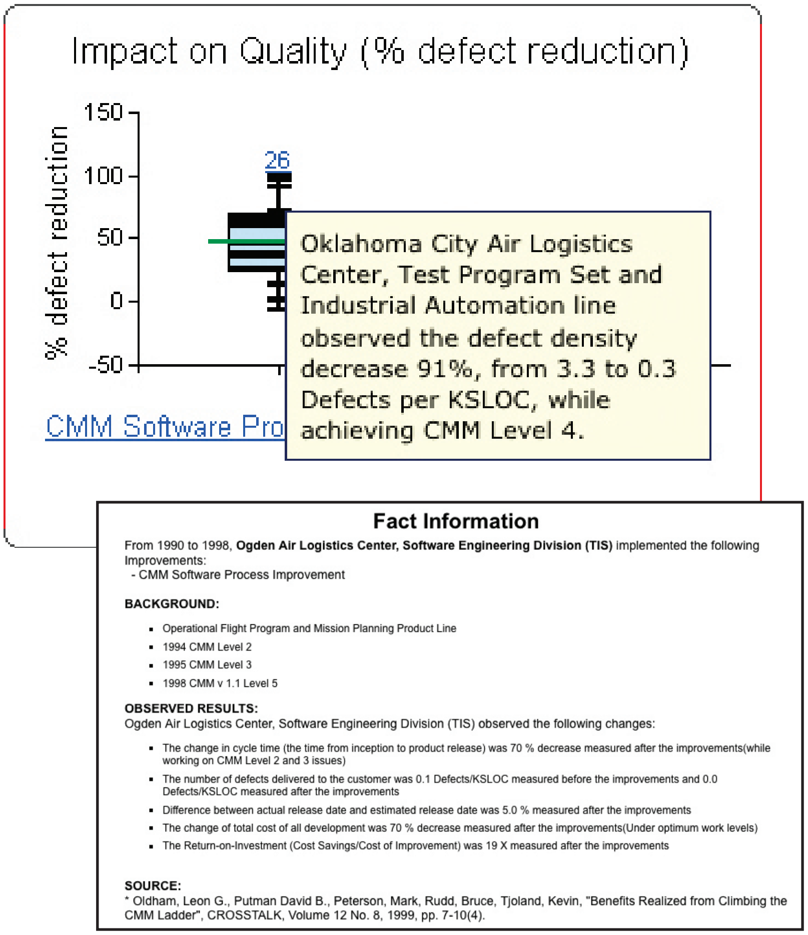
Dr. Elizabeth (Betsy) Clark is President of Software Metrics, Inc., a Virginia-based consulting company she co-founded in 1983. Dr. Clark is a primary contributor to Practical Software Measurement (PSM). Dr. Clark was also a principle contributor to the Software Engineering Institute's (SEI) core measures. Dr. Clark is a Research Associate at the Center for Systems and Software Engineering at USC. She collaborated with Dr. Barry Boehm and Dr. Chris Abts to develop and calibrate the COCOTS model. She is a consultant to the Institute for Defense Analyses and the Software Engineering Institute. She is also a primary contributor to SCRAM. Dr. Clark received her B.A. from Stanford University and her Ph.D. in Cognitive Psychology from UC, Berkeley.

Dr. Brad Clark is Vice-President of Software Metrics Inc. – a Virginia based consulting company. He works with clients to identify and resolve key issues that prevent organizations from becoming more efficient and more effective. He has helped organizations identify the root causes of schedule slippage, performed feasibility analysis of a program's staffing levels and duration, and helped organizations create and use leading indicators that forecast changes in progress, productivity or quality. Dr. Clark received his Ph.D. in Computer Science in 1997 from the University of Southern California. Brad is a former Navy A-6 Intruder pilot.

Ms Angela Tuffley is the Director of the RedBay Consulting, an Adjunct Senior Lecturer with Griffith University and Software Engineering institute (SEI) Visiting Scientist. She has over 30 years of industry experience, both in Australia and overseas, providing expert professional services in training, assessment and advice for the acquisition, engineering and support of software intensive systems. She is a co-developer of the Schedule Compliance Risk Assessment Methodology (SCRAM) and provides consultation on SCRAM, the adoption of the Capability Maturity Model Integration (CMMI) and ISO/IEC 15504 Information Technology Process Assessment (SPICE). She is a CMMI Institute Certified CMMI Instructor and has a Bachelor of Science and a Graduate Diploma in Software Quality from Griffith University.

ARE YOU GETTING THE MAX FROM YOUR SOFTWARE INVESTMENT?

The CSIAC ROI Dashboard



Oklahoma City Air Logistics Center, Test Program Set and Industrial Automation line observed the defect density decrease 91%, from 3.3 to 0.3 Defects per KSLOC, while achieving CMM Level 4.

Fact Information

From 1990 to 1998, **Ogden Air Logistics Center, Software Engineering Division (TIS)** implemented the following Improvements:
- CMM Software Process Improvement

BACKGROUND:

- Operational Flight Program and Mission Planning Product Line
- 1994 CMM Level 2
- 1995 CMM Level 3
- 1998 CMM v 1.1 Level 5

OBSERVED RESULTS:
Ogden Air Logistics Center, Software Engineering Division (TIS) observed the following changes:

- The change in cycle time (the time from inception to product release) was 70 % decrease measured after the improvements(while working on CMM Level 2 and 3 issues)
- The number of defects delivered to the customer was 0.1 Defects/KSLOC measured before the improvements and 0.0 Defects/KSLOC measured after the improvements
- Difference between actual release date and estimated release date was 5.0 % measured after the improvements
- The change of total cost of all development was 70 % decrease measured after the improvements(Under optimum work levels)
- The Return-on-Investment (Cost Savings/Cost of Improvement) was 19 X measured after the improvements

SOURCE:
* Oldham, Leon G., Putman David B., Peterson, Mark, Rudd, Bruce, Tjoland, Kevin, "Benefits Realized from Climbing the CMM Ladder", CROSSTALK, Volume 12 No. 8, 1999, pp. 7-10(4).

Technologies Covered:

- SEI/CMM/CMMI
- SEI Team Software Process (TSP)
- SEI Personal Software Process (PSP)
- Inspections
- Reuse
- Cleanroom

And Many More!

Graphs Showing Impact of Software Technologies on:

- ROI
- Productivity
- Quality

Summarizes Facts from Open Literature

Access the CSIAC ROI Dashboard
https://sw.thecsiac.com/databases/roi/

CSIAC
100 Seymour Road
Suite C-102
Utica, NY 13502
https://www.thecsiac.com/

4G LTE Security for Mobile Network Operators

By Daksha Bhasker

Mobile network operators (MNOs) must grapple with complex security management in fourth generation Long Term Evolution (4G LTE) deployments. The security architecture of 4G LTE may lull MNOs into a sense of complacence that the technology intrinsically addresses security in LTE operations. 4G LTE has known security vulnerabilities. Besides inherent LTE vulnerabilities, 4G LTE includes long standing internet protocol (IP) based security weaknesses. The third generation partnership project (3GPP) has included security in their system architecture evolution (SAE) from inception, yet there are numerous security considerations deferred to the MNO. In terms of service delivery and operations MNOs are left to manage both LTE and IP based security vulnerabilities. This leads to complex security management requirements for MNOs. This paper covers a broad sweep of security issues that MNOs should consider when operating 4G LTE networks, and proposes directional preventative measures with the objective of highlighting the critical role MNOs have to play in securing 4G LTE operations.

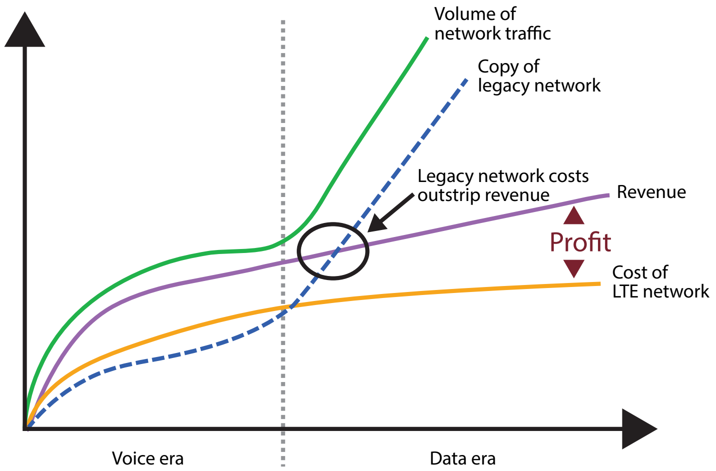
LTE is designed with strong cryptographic techniques, mutual authentication between LTE network elements with security mechanisms built into its architecture. However, trusted industry organisations have identified security vulnerabilities that should be assessed by virtue of network deployment. With the emergence of the open, all IP based, distributed architecture of LTE, attackers can target mobile devices and networks with spam, eavesdropping, malware, IP-spoofing, data and service theft, DDoS attacks and numerous other variants of cyber-attacks and crimes. MNOs are focused on increasing business profitability by 4G deployments, and are the first point of contact, for subscribers in the event of security or privacy breaches. To protect profit dollars from being spent on recovery and remediation from security breaches, MNOs should keep abreast of prevalent security risks in both LTE and IP, the evolving security threatscape and actively invest in preventative security measures.

This paper provides an overview of security threats/risks and preventative measures recommended for MNOs by network segment in the 4G LTE architecture. The paper does not present a comprehensive review of all possible security threats and does not address detection or recovery measures. The paper assumes that the reader has basic knowledge of LTE architecture, operations and common security threats and attacks.

Background

Technically 4G LTE is a boon for MNOs. Broadband capable, LTE is designed to support up to 300 Mbps peak downlink and peak uplink of 75Mbps. LTE specifications include an all IP network including support for IPv6, flat architecture with fewer network elements, spectral efficiency, low latency as well as backward compatibility with existing wireless technologies.

Financially, the impact of LTE deployment restores profitability to the MNO, by re-establishing costs below revenues. The current growth trend in data traffic is getting progressively unprofitable for MNOs on the legacy 2G/3G networks [1] . LTE operators benefit from improved cost efficiencies, both capex and opex, while dramatically increasing service performance for the subscriber.



Source: Analysis Mason

Figure 1: Impact of LTE deployment

It is evident, that profitability and competitive pressures will force the transition to LTE definitively for operators. Figure 1 [1]

4G LTE architecture was developed by 3GPP taking into consideration security principles right from its inception and design based on five security feature groups [2].

(i) Network access security, to provide a secure access to the service by the user.
(ii) Network domain security, to protect the network elements and secure the signalling and user data exchange.
(iii) User domain security, to control the secure access to mobile stations
(iv) Application domain security, to establish secure communications over the application layer
(v) Visibility and configuration of security, bring the opportunity for the user to check if the security features are in operation.

However, in reviewing the 4G LTE architecture, the 3GPP, next generation mobile network (NGMN) alliance and international telecommunications union (ITU) have identified security vulnerabilities and recommended mitigation strategies. Consideration and implementation of these security enhancing measures are discretionary to the many LTE stakeholders including MNOs. As a result, the security of LTE networks and services will vary widely between MNOs, subject to the MNOs knowledge of security risks and impacts, the MNOs risk appetite and wallet size among other factors. Speed to market, tight budgets, profit targets, concerns with network performance, business models, network interoperability, regional regulations and business priorities lead to further inconsistencies in security implementation amongst MNOs.

At the fundamental level, the LTE ecosystem (Figure 2) comprises of MNOs, LTE subscribers, LTE device manufacturers and service providers (SP) offering content, applications and other IP based services [3] [4] [5].

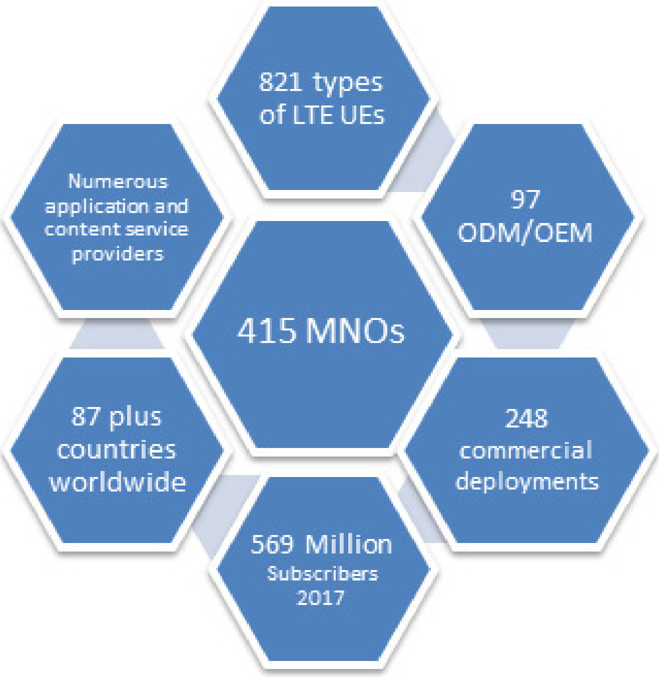

821 types of LTE UEs
Numerous application and content service providers
97 ODM/OEM
415 MNOs
87 plus countries worldwide
248 commercial deployments
569 Million Subscribers 2017

Figure 2: LTE ecosystem 2013 [3] [4] [5]

As a result, MNOs need to contend with security vulnerabilities, brought about not only by interconnections with other MNOs but also the varying security standards of 821 ODM/ OEM LTE devices, unsecured behaviours of 68.33 million subscribers and the security weakness of numerous third party applications and services [3]. With such a large inter meshed growing milieu, and considering that cyber-attackers are poised to target mobile networks, security management in 4G LTE operations is a critical and complex challenge for MNOs.

The fragmented, disparate deployment of security in LTE networks will bring the overall security level down from the perspective of subscriber experience to the lowest common denominator, exposing subscribers, MNOs and service providers to security and privacy vulnerabilities. This heightened exposure to security threats in LTE networks through open architectures with multiple interconnections, has the potential to cause the MNO, business and financial losses, as well as a tarnished reputation.

With the objective of highlighting the significant role MNOs have to play in the securing LTE networks, operations and service, the following sections review some of the key known security threats and offers preventative measures.

Overarching Security risks in 4G LTE

For purposes of this paper, the 4G LTE architecture model has been divided into the following network segments: user equipment (UE), Access, Evolved Packet Core (EPC)/ Transport and Service network (Figure 3).

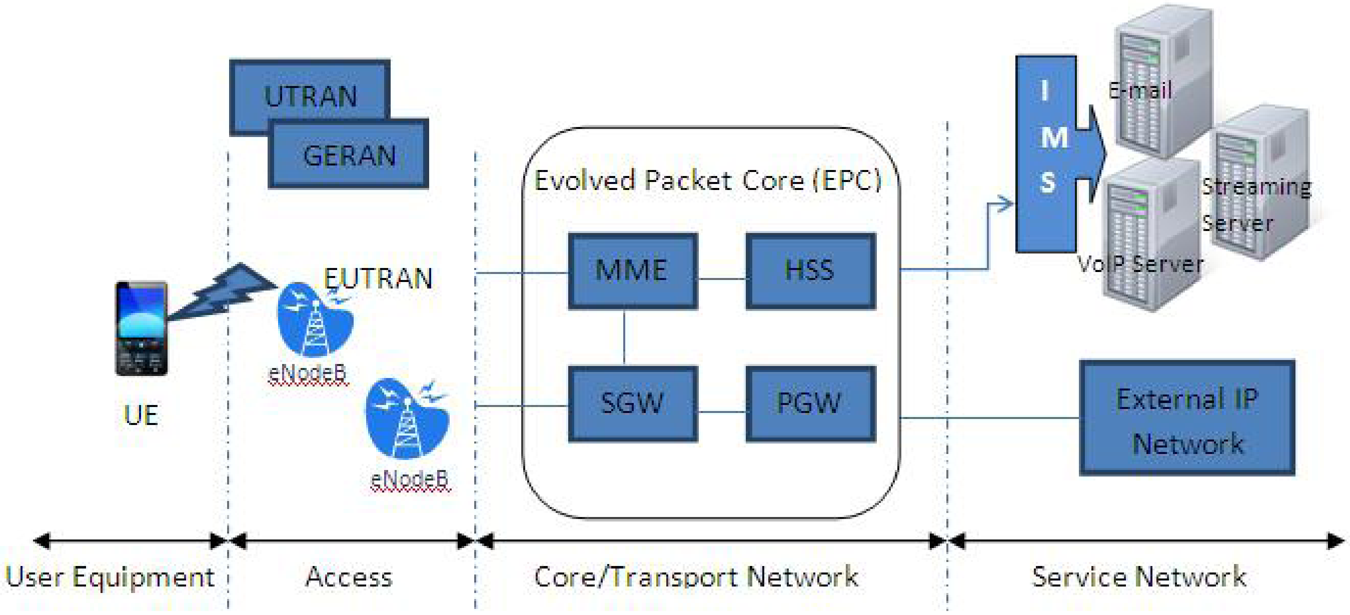


Figure 3: Basic LTE/SAE architecture

Key security threats/risks:

- Distributed network and open architecture
- Complex business models (IS/Service sharing)
- Decentralised accountability for security
- Minimising security spend

Distributed network & open Architecture: 4G LTE architecture brings with it an end to physically segregated networks owned and operated by a single MNO and the security that came with it. With legacy technologies, operators could enforce security policies on their own infrastructure, secure their perimeter and be reasonably confident that a subscriber while on their platform was protected. 4G LTE is an all IP based end to end deployment where seamless roaming with service continuity is offered to the end user. As a result, the MNO entrants to the LTE market, share security risks and threats as their respective infrastructures and services are now interconnected into one aggregated service providing network. Distributed network and open architectures enables weak security configurations on one device or interface provide the entry point to attackers looking to compromise the LTE network.

Complex business models with infrastructure (IS) and service sharing: LTE offers network sharing capabilities that present new business models for MNOs. Service could be offered to end customers by a virtual network operator, where one MNO owns the E-UTRAN while a different one owns the MMEs. Cost benefits will lead MNOs into various models of active infrastructure sharing arrangements with new revenue sharing business models. An example of such network sharing is the joint venture of rival Swedish operators Telenor and Tele2 called Net4Mobility where the radio network and certain part of the access network are shared. Ovum forecasts that by 2015, 30% of all LTE networks will involve some form of active network sharing [6] indicating that complex business models with LTE deployment are here to stay. These types of LTE arrangements bring with it challenges with ensuring consistent security configurations and security management across such virtual network operators. Multiple MNOs with varying security controls and standards interconnecting with shared pools of network elements pose a threat to security levels.

Decentralised accountability: MNOs wishing to present universal end to end security levels to subscribers will find it problematic that a single MNO does not have unilateral decision control over security parameters of the LTE networks and operations. For instance, security standards will vary with global roaming or choice of application, based on the security settings of the application service provider. This decentralised accountability and lack of overall control on security of the LTE service experience will be exacerbated as hosted and cloud services penetrate the marketplace creating new and complex operating models.

Minimising security spend: LTE operators are quickly deterred by the millions of dollars required for a full IPSec rollout alongside other security infrastructure deployments and look to cut corners and launch to market with the minimum requirements to provide service. There is significant disparity between network designs of large operators and smaller operators with limited resources. With LTE the interconnectedness of the network brings the security level of the overall architecture to the level of the least common denominator, lowering security thresholds.

Preventative measures:

- Interoperability standards
- Strong partner agreement
- Security audits with remediation commitments
- Security Budget

Interoperability standards: As legacy network architectures have been closed, interoperability with MNO peers were founded on implicit underlying trust, that each MNO would secure their own networks. With subscribers roaming on the LTE ecosystem, and the interconnectedness of legacy platforms, trusted and untrusted networks, it is imperative that MNOs set out interoperability standards and configurations to ensure the MNOs service, network and service promise to the subscriber is not compromised. For example encryption, latency or quality of service (QoS) specifications should be set out between peer operators in order to enable contiguous security and service levels.

Strong partner agreements: MNOs should set out security standards, policies including configuration requirements within their partner and peering arrangements. These agreements should particularly set out implementation of security infrastructure and configuration such as security gateways, security protocols, subscriber security parameters in vertical hand offs, QoS, key management, authentication, encryption, confidentiality and privacy policies. In addition, MNO's should ensure that the set security measures are cascaded down to relevant 3rd party agreements, partner MNO's may enter into.

Audits: Regular third party audits of partners should be set out in agreements to verify and enforce required security standards, policies and practices allowing for remediation and hardening as identified, in advance of potential security attacks.

Security Budgets: MNOs should allocate funds for security infrastructure and operations in their LTE deployment to ensure they meet their business objectives while minimising risks to levels acceptable to the MNO. The MNO must keep in mind legal and regulatory requirements for security and privacy while building out LTE networks and plan fund allocation accordingly. Since inadequate security measures have the potential to damage the MNOs business, it is prudent for the MNO to give security investment due consideration and priority.

User Equipment (UE)

UEs are the subscriber entry points into the LTE network and are perhaps the weakest element on the LTE architecture as the MNO has least control over its security parameters. In context, UEs can be the gateway for various security vulnerabilities into the LTE service.

Key Security threats/risks:

- Physical attacks
- Risk of data loss, privacy
- Lack of security standards & controls on UEs
- Application layer: virus, malware, phishing

Physical attacks: Smart devices are small and portable and are inherently prone to loss and theft. A smart device or UE can be physically tampered with and used to access and attack the operator's networks. Subscribers jailbreaking smart devices (hardware or software) compromises the manufacturer's security settings on the device. The increased intelligence and processing capability of the LTE UE proportionately elevates the sophistication of the possible cyber-attacks from the UE. For example, smartphone zombies could be set up to continuously dial numbers and hang up, using up valuable radio resources in the cell that will eventually adversely affect network performance. [7]

Risk of data loss, privacy: Due to broadband data capabilities, LTE UEs will store more data on the UE than ever before making them attractive targets for attackers. Deloitte reports that 90% of user passwords on LTE devices are vulnerable to hacking in a matter of seconds [8]. Once an attacker can access user data, the subscriber can then become a victim of an array of crimes from identity theft, loss of financial or sensitive personal information, to violation of privacy.

Lack of security standards & controls: A plethora of smart phones, tablets and other 4G LTE devices from numerous manufacturers, with disparate, open and proprietary operating systems (OS) and software, will roam the LTE network. Further, most UEs lack security management tools. MNOs opting to allow unsecured devices to connect to their network provide an entry point for attackers. MNOs in the legacy architecture, limited the selection of ODM/OEM devices connecting to their networks, setting basic security parameters on the chosen UEs. However with the ubiquitous nature of LTE, profit seeking MNOs will move towards inclusion of most UEs from a global subscriber base adopting a permissive, inclusive approach. This brings a weakened security configuration at the LTE edge.

Application vulnerabilities: Since UEs on LTE are essentially IP devices, they are now susceptible to IP based vulnerabilities and attacks. Subscribers who indiscriminately download applications and content expose the UE to viruses, malware, spam, phishing and similar threats that compromise the integrity of the device, bandwidth usage on the MNO network, security of the LTE edge and the subscriber. According to McAfee there was a 4000% increase in mobile malware year over year in 2012 over 2011to just under 37,000 variants [9]. In alignment, attacks on applications on LTE devices are expected to rise. With bandwidth rich applications such as mobile banking, mCommerce and trading, attackers will find vulnerabilities in mobile financial applications attractive targets.

Preventative measures:

- Subscriber education
- Antivirus
- Industry security standards & controls on UE
- Strong authentication, authorisation, OS encryption

Subscriber Education: Subscriber education is the most effective approach to protecting the UE. Informing the user about the risks of damage from unsecure devices will motivate users to keep the UEs physically safe. Informed users can turn off the geo-location features on their devices to protect the privacy of their physical location. MNOs can further emphasize this by transferring accountability for mischief initiated from the UE, and responsibility to protect the UE, to the subscriber via user agreements and associated penalties.

Anti-Virus: UEs like personal computers (PC) are susceptible to viruses, malware and social engineering attacks. Anti-virus programs protect devices from a vast set of virus, malware, spyware and other cyber threats and are constantly updated by vendors. Anti-virus, anti-malware software should be installed on UEs and kept up to date as a basic protection mechanism for the device.

Strong authentication, authorisation, encryption: UEs should have strong authentication mechanisms to verify users accessing the UE. Subscribers should set up strong passphrases on UEs. As a result attackers will no longer have immediate access to the data on the device, even if the device is physically in their possession. Authorisation grants or denies access to resources. The UE can be set up with different access privileges for a user and an administrator. This will offer the UE another layer of access protection. Further, LTE users should be advised to choose devices with OS encryption, remote wipe capabilities, as well opt for encryption of data stored on the device.

Industry security standards and controls: With over 97 manufacturers and 821 UEs accessing the MNO networks [3], MNOs should continue to work through global operators' consortiums with manufacturers to establish firm security standards and controls on smart devices, align on default security settings on UEs, security management tools and share the burden of educating subscribers on the use of security features on the UE to protect both themselves and the MNO.

Access

Figure 3, depicts the access as the EUTRAN, and the interconnection between the UE and the EUTRAN.

Key Security threats/risks:

- Physical attacks
- Rogue eNodeBs
- Eavesdropping, Redirection, MitM attacks, DoS
- Privacy

Physical Attacks: Increased demands for LTE bandwidth and footprint in densely populated areas have given rise to smaller cell sites, installation of eNodeB's in public locations (such as shopping malls, utility poles), introduction of femtocells and installation of less expensive HeNBs on the LTE edge. eNodeB's in public location are vulnerable to physical tampering allowing for unauthorised access to the network as MNOs do not tend to invest in securing these smaller access points.

Rogue eNodeBs: Unlike legacy base stations, smaller LTE eNodeB's are not cost prohibitive. Being accessible, attackers attempt to introduce rogue eNodeB's into the LTE network. Rogue eNodeB's can impersonate the operator's node, and intercept voice and data transmission from the UE. The attacker can then passively eavesdrop or redirect user traffic to a different network.

Eavesdropping, Man in the middle attack (MitM): Attackers can take advantage of a known weakness in LTE wherein the user identity transference occurs unencrypted, in clear text between the UE and the eNodeB, during the initial attach procedure [10] [11]. This allows an eavesdropper to track the user cell-location or launch a man in the middle attack by user international mobile subscriber identifier (IMSI) impersonation and relay of user messages. [10] [11]

Privacy: Privacy threats have been exposed by Arapinis et al. where attackers can utilise paging procedures to locate phones by injecting paging requests multiple times and correlating the gathered temporary identity (TMSI) of the phone with the paged permanent identity IMSI [12]. Attackers can further replay the intercepted authentication request and determine the presence of a specific phone in a certain location. When the UE receives a replay of an intercepted authentication request it will send a synchronisation failure request. This attack has the potential to enable location tracking thus compromising privacy and security.

Preventative measures:

- Physical security
- Authentication, authorization, encryption
- Network monitoring, IPS systems
- Security Architecture

Physical security: MNOs can begin by being aware of security exposure as a result of leaving HeNB's physically accessible and vulnerable in public locations and doing their best to secure such sites. In areas where attackers could tamper with the device implementing access control lists or alternate access and identification measures on the HeNB would deter attackers.

Authentication, Authorisation, Encryption: 3GPP specifies access security in TS 33.203 which includes authentication related mechanisms and traffic protection between the UE and core networks. Strong encryption in the attach phase and UE authentication to the eNodeB will deter both rogue elements and man in the middle attacks. Adopting public key infrastructure (PKI) with the public key of the MNO being stored in the USIM allowing the UE to encrypt privacy related information such as the IMSI transmitted to the eNodeB will enable confidentiality [12]. Encryption should be implemented between the UE and eNodeB to thwart attackers leveraging IMSI paging and location identification vulnerabilities thus protecting subscriber privacy [12] and security.

Network monitoring: Wireless Intrusion prevention and wireless intrusion detection systems may be used towards rogue eNodeB detection and network security. It is recommended that MNO's monitor their access networks real time for rogue access points and wireless attack tools, to identify attacks quickly, minimising impacts [13].

Security Architecture: With volumes of data on LTE rising exponentially, MNOs are further faced with the challenge of managing bandwidth overhead allocated to security measures such as authentication and encryption without adversely affecting latency and QoS of user data traffic transmission.

MNOs are best to consider security upfront in the network design phase and architect scalable networks enabling security operations in LTE networks.

Evolved Packet Core (EPC)/Transport

The EPC (Figure 3) is the core of the LTE network that manages user authentication, access authorisation and accounting (AAA), IP address allocation, mobility related signalling, charging, QoS and security.

Key Security threats/risks:

- Unauthorised access
- DoS and DDoS attacks
- Overbilling attacks (IP address hijacking, IP spoofing)

Unauthorised access: MNOs must interconnect their authentication systems to allow subscribers to access the internet even when roaming. Untrusted roaming devices need to connect to the MNOs' LTE network to enable service continuity while roaming. The network operator remains responsible for the security of the data that has traversed the access securely entering the network core. Unless specifically designed by the MNO and security protocols enabled, (IPSec, IKE, EAP/TLS), neither the control traffic nor the data traffic is encrypted nor integrity protected between the EUTRAN and the EPC [14]. This leaves the traffic vulnerable to listening or modification should this segment of the network be hacked into or an attacker gain unauthorised access.

DoS and DDoS attacks: In January 2012, NTT DoCoMo experienced a signalling flood caused by a VoIP application running on Android phones that disrupted network access leaving 2.5 million subscribers out of service for over four hours. [15] According to Nokia, the signalling requirements between the EUTRAN and the EPC in the 4G architecture is about 40% higher per LTE subscriber than 3G networks. Since the LTE architecture is flat, all the signalling traffic generated at the EUTRAN flows to the MME. If the signalling load either benign or malicious exceeds the provisioned capacity of the MME, then service may be compromised. This in essence, is a vulnerability that can be targeted for DoS attacks

Overbilling attacks (IP address hijacking, IP spoofing): The all IP network bring with it IP related security threats such as IP address hijacking, spoofing, packet injection and the like into the LTE networks. An attacker can hijack the IP address of a legal subscriber when the IP address in being returned to the IP pool and take control of it. The attacker then utilises the LTE data services at the expense of the subscriber [16]. Alternately when an IP address is reassigned to another subscriber overbilling attack can occur. [16]

Preventative measures:

- Security Architecture: VPNs, VLANs
- Encryption, IKE/ IPSec
- Network monitoring, management and load balancing

Security Architecture: In order to address IP based vulnerabilities 3GPP recommends the use of IPSec [17]. The final deployment decision to apply IPSec to either control traffic, user traffic or both resides with the MNO. The next generation mobile network alliance (NGMN) recommends the use of VPNs to secure transmission in the core [14]. As well, the use of VLANs for network and traffic segregation as a security measure is suggested. This would isolate signalling traffic to specific network zones or paths as defined by the VLAN [14] [18]. These measures would limit damage done by attackers by unauthorised access, eavesdropping, spoofing and other attacks.

Encryption IKE/IPSec: 3GPP recommend the inclusion of IKE/IPSec for authorization, authentication, integrity and confidentiality protection. [17]. Both the aforementioned measures will offer a certain degrees of protection against IP based attacks and can deter overbilling attacks.

Network monitoring, management: MNOs are advised to monitor networks for suspicious activity. The novelty with LTE is that operators need not only be concerned about protecting their own networks but also reach agreements with neighbouring cell operators and partners at interconnection points on configuration management, performance management, fault management and security management at the edge and in the core.

Load balancing: Operators must protect their networks from signal surges directed at any of the elements of the EPC. Policies, shaping, and prioritisation of traffic volumes should be used to prevent overload. These would help reduce effects of attempted DoS/DDoS attacks. The operator may consider conducting a hop by hop analysis between network elements to ensure security between elements. Deployment of security gateways, firewalls, IDS and IPS are recommended by many infrastructure vendors.

Service Network

(Figure 3) According to 3GPP, IP multimedia subsystem (IMS) is a way of delivering multimedia (voice, video, data etc.) regardless of the access type, service provider or the user device used in LTE architecture [19]. Security management in IMS is particularly important as it has implications to QoS, charging, billing and enabling of applications.

Key Security threats/risks:

- Unauthorised access
- Service abuse attacks, Theft of service
- Network snoop, session hijacking

Unauthorised access: The open and distributed architecture of IMS creates a multitude of distribution points that must be secured. IP peering between service providers with diverse service offering and varying security standards are often in semi-trusted zones that can make the IMS core vulnerable. Large volumes of multimedia traffic need reliable protection mechanisms from attacks from the internet across multiple technological ecosystems.

Service abuse attacks, theft of service: Service abuse and theft of service represent compromised subscriber service and loss of revenues to the MNO. Service abuse is achieved by the subscriber gaining more privilege to services than those allocated to the user. An attacker can access the IMS with a compromised UE. One of the ways theft of service is achieved is by the UE not releasing the established media stream between a UE and IMS core after a Bye request has been sent to a call session control function (CSCF). This leads the CSCF to stop accounting for the session while the user or attacker continues to stay connected to the media stream [20].

Network snoop breaches confidentiality where the attacker intercepts information flow between two users in a SIP session. Without network protection, attackers can use tools like Wireshark to capture SIP signalling [20]. Session hijacking involves the attacker inserting malicious packets, substituting traffic and breaching integrity, impacting QoS and service.

Preventative measures:

- Border Security
- Strong authentication
- Enable security protocols
- Implement Security Gateways

Border security: The IMS needs to have network to network border security to protect from unauthorised access via other networks. Roaming subscribers will access the IMS via the internet and this untrusted entry point, needs to be particularly protected. MNOs must secure and control their network borders and invest in security infrastructure such as firewalls, packet filtering, address translation, VPN and encryption capabilities between peering networks.

Strong authentication: MNOs should implementation strong authentication between the UE and IMS networks, as well use security gateways (SEG) to ensure confidentiality of data between client and IMS network. The networks must be configured such that the UE is routed to the correct SEG before connecting to the IMS network and ensure IPSec is enabled from the UE for transmission through the internet to the IMS. [21] IPSec provides confidentiality, integrity, data origin authentication and protection against replay.

Enable security protocols: Security protocols offer protection at various layers such as secure socket layer (SSL)/Transport layer security (TLS) and datagram TLS (DTLS) [20]. Network snoop can be prevented by encryption of SIP signalling. The MNO must design networks to allow stable operations with security protocols enabled. These protocols allow for secure connections and transmission of data between the UE and the IMS service.

Security Gateways: Since the premise of IMS is to create a single platform across multiple providers, security management goes beyond just traditional firewalls and routers, as multiple sessions are active, requiring various levels of QoS, policy enforcement, authentication and encryption. It is recommended that MNOs invest in scalable security infrastructure and security gateways to manage the complexity.

Conclusion

Despite the fact that 4G LTE architecture has a strong security framework developed by the 3GPP, MNOs have an essential role in security management of LTE networks through design, deployment and operations. MNOs cannot be complacent about LTE security and need to actively protect the multiple entry points into the LTE network (Figure 4). 4G LTE brings with it increased complexity in security management for the MNO, however, with proper diligence MNOs can minimise the impacts of various security threats. It is well known that security is a moving target that needs continuous attention and investment to keep abreast of the changing threatscape. Security is an integral part of the business lifecycle of MNOs and will continue to remains as such with the adoption of 4G LTE services and technologies.

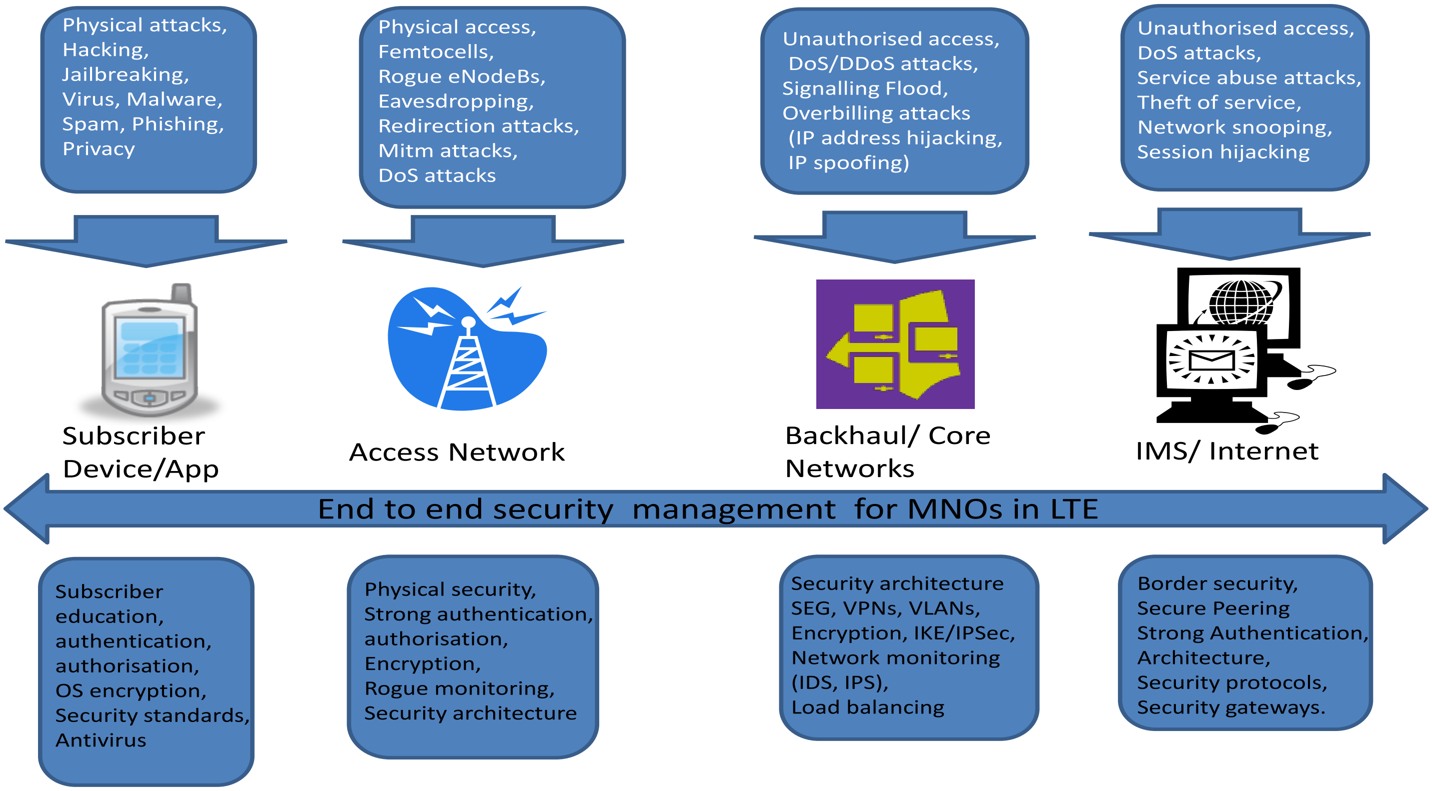


Figure 4: Entry points in LTE, security threats, security management for MNOs

References

1. P. Mottishaw, "Policy control and charging for LTE networks," Analysis Mason, 2009.
2. 3rd Generation Partnership Project, "TS 33.401: System Architecture Evolution (SAE); Security architecture. Network, ver.11.2.0, release 11.," 3GPP, 2011.
3. Global mobile suppliers association, "Status of the LTE Ecosystem," March 2013.
4. S. Téral, "LTE market nearly doubling in 2013," Infonetics Research, Campbell, California, March 2013.
5. Global Suppliers Association, "GSA Evolution to LTE report: 163 commercial networks launched; 415 operators investing in LTE," 7 April 2013. [Online]. Available: http://www.gsacom.com/news/gsa_375.php. [Accessed 14 September 2013].
6. Ovum, "Mobile network sharing: a post-recession reality," September 2010. [Online]. Available:http://www.researchandmarkets.com/reports/1396699/mobile_network_sharing_a_postrecession_reality. [Accessed 16 June 2013].
7. H. J. W. Z. Chuanxiong Guo, "Smart-Phone Attacks and Defenses," Microsoft Research.
8. Deloitte, "Deloitte Technology, Media and Telecommunication Predictions 2013," 13 Jan 2013. [Online]. Available: http://www.deloitte.com/view/en_GX/global/press/global-press-releases-en/e608748edba3c310VgnVCM3000003456f70aRCRD.htm. [Accessed 16 June 2013].
9. McAfee, "McAfee Threat Report: Fourth Quarter 2012," McAfee Labs, Santa Clara, CA, 2012.
10. G. Escudero-Andreu, R. C-W. Phan and D. J. Parish, "Analysis and Design of Security for Next Generation 4G Cellular Networks," PGNet, Loughborough, U.K., 2012.
11. C.-E. Vintila and V.-V. Patriciu, "Security Analysis of LTE Access Netwwork," in *The tenth International Conference on Networks*, Bucharest, Romania, 2011.
12. M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon and R. Borgaonkar, "New Privacy Issue in Mobile Telephony: Fix and Verification Computer and Communications Security," *ACM,* vol. unknown, no. unknown, pp. 205-216, 2012.
13. D. Lee and D. Won, "A study on Security Management Service System for Wireless Network Environment," *Applied Mathematics & Information Sciences,* vol. 6, no. unknown, pp. pp209s-220s, 2012.

14. Next Generation Mobile Network Alliance, "Security in LTE backhauling, ver 1.0,," 29-02-2012.

15. M. Donegan, "Light Reading: Docomo Counts Cost of Signaling Storm," 22 February 2012. [Online]. Available: http://www.lightreading.com/core-network/docomo-counts-cost-of-signaling-storm/240140700. [Accessed 11 June 2013].

16. M. A. Mobarhan, M. A. Mobsrhsn and A. Shahbahrami, "Evaluation of Security Attacks on Different Mobile Communication Systems," *Canadian Journal on Network and Information Security,* vol. 3, no. 1, Aug 2012.

17. 3rd Generation Partnership Project, "http://www.3gpp.org/," 29 May 2011. [Online]. Available:http://www.3gpp.org/ftp/information/presentations/presentations_2011/2011_05_Bangalore/DZBangalore290511.pdf. [Accessed 3 June 2013].

18. C. Kowtarapu, C. Anand, K. G. Guruprasad and S. Sharma, "Network Separation and IPsec CA Certificates-Based Security Management for 4G Networks," *Bell Labs Technical Journal,* vol. 13, no. 4, pp. 245-256, 2009.

19. 3rd generation partnership project, "TS 22.228: Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1," 3GPP, 2010.

20. E. Belmekki, N. Bouaouda, B. Raouyane and M. Bellafkih, "IP Multimedia Subsystem: Security Evaluation," *Journal of Theoretical and Applied Information Technology,* vol. 51, no. 1, 2013.

21. D. Slezak and Y. Gelogo., " Securing IP Multimedia Subsystem with the appropriate Security gateway and IPSec Tunnelling," *Journal of security engineering,* 2011.

About the Author

Daksha Bhasker, CISM, is an Associate Director for Governance at Bell Canada managing controls on complex custom Information and Communications Technology (ICT) solutions. Her role has encompassed security controls for Sarbanes Oxley compliance and security risk management in complex deals with large enterprise customers. She received a M.S in computer systems engineering from Irkutsk State Technical University, Russia and a MBA in electronic commerce from University of New Brunswick, Canada. In over a decade of experience in the telecommunications industry, she has held various management position in business intelligence, product management, business operations controls and strategy planning. Her interests in security includes research, analysis and authorship.

Author's Note: Opinions expressed in this paper are the author's and not those of Bell Canada.

Acknowledgement: The author would like to thank Tyson Macaulay, VP Global Telecommunications Strategy, McAfee (Intel), for inspiration, guidance and insights shared.

Article Submission Policy

The CSIAC Journal is a quarterly journal focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories. CSIAC accepts articles submitted by the professional community for consideration. CSIAC will review articles and assist candidate authors in creating the final draft if the article is selected for publication. However, we cannot guarantee publication within a fixed time frame.

Note that CSIAC does not pay for articles published.

AUTHOR BIOS AND CONTACT INFORMATION

When you submit your article to CSIAC, you also need to submit a brief bio, which is printed at the end of your article. Additionally, CSIAC requests that you provide contact information (email and/or phone and/or web address), which is also published with your article so that readers may follow up with you. You also need to send CSIAC your preferred mailing address for receipt of the Journal in printed format. All authors receive 5 complementary copies of the Journal issue in which their article appears and are automatically registered to receive future issues of Journal. Up to 20 additional copies may be requested by the author at no cost.

COPYRIGHT:

Submittal of an original and previously unpublished article constitutes a transfer of ownership for First Publication Rights for a period of ninety days following publication. After this ninety day period full copyright ownership returns to the author. CSIAC always grants permission to reprint or distribute the article once published, as long as attribution is provided for CSIAC as the publisher and the Journal issue in which the article appeared is cited. The primary reason for CSIAC holding the copyright is to insure that the same article is not published simultaneously in other trade journals. The Journal enjoys a reputation of outstanding quality and value. We distribute the Journal to more than 30,000 registered CSIAC patrons free of charge and we publish it on our website where thousands of viewers read the articles each week.

FOR INVITED AUTHORS:

CSIAC typically allocates the author one month to prepare an initial draft. Then, upon receipt of an initial draft, CSIAC reviews the article and works with the author to create a final draft; we allow 2 to 3 weeks for this process. CSIAC expects to have a final draft of the article ready for publication no later than 2 months after the author accepts our initial invitation.

For some issues CSIAC has a Guest Editor (because of their expertise) who conducts most of the communication with other authors. If you have been invited by a Guest Editor, you should

PREFERRED FORMATS:

- Articles must be submitted electronically.
- MS-Word, or Open Office equivalent (something that can be edited by CSIAC)

SIZE GUIDELINES:

- Minimum of 1,500 – 2,000 words (3-4 typed pages using Times New Roman 12 pt font) Maximum of 12 pages
- Authors have latitude to adjust the size as necessary to communicate their message

IMAGES:

- Graphics and Images are encouraged.
- Print quality, 200 or better DPI. JPG or PNG format preferred

Note: Please embed the graphic images into your article to clarify where they should go but send the graphics as separate files when you submit the final draft of the article. This makes it easier should the graphics need to be changed or resized.

CONTACT INFORMATION:

CSIAC
100 Seymour Road Suite C102
Utica, NY 13502
Phone: (800) 214-7921
Fax: 315-351-4209

John Dingman, Managing Editor
Phone: (315) 351-4222
Email: jdingman@quanterion.com

Michael Weir, CSIAC Director
Phone: (315) 351-4211
Email: mweir@quanterion.com

CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC), technically managed by the Air Force Research Laboratory (AFRL) in Rome, NY and operated by Quanterion Solutions Incorporated, Utica, NY.

ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

Distribution Statement
Unclassified and Unlimited

CSIAC
100 Seymour Road
Utica, NY 13502-1348
Phone: 800-214-7921 • **Fax:** 315-732-3261
E-mail: info@thecsiac.com
URL: http://www.thecsiac.com/

ABOUT THIS PUBLICATION

The Journal of Cyber Security and Information Systems is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC). The CSIAC is technically managed by Air Force Research Laboratory in Rome, NY and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the CSIAC, and shall not be used for advertising or product endorsement purposes.

COVER DESIGN

Shelley Howard
Graphic Designer
Quanterion Solutions, CSIAC

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the Journal of Cyber Security and Information Systems Vol.1, No 4 October 2013."

In addition to this print message, we ask that you notify CSIAC regarding any document that references any article appearing in the *CSIAC Journal.*

Requests for copies of the referenced journal may be submitted to the following address:

Cyber Security and Information Systems
100 Seymour Road
Utica, NY 13502-1348

Phone: 800-214-7921
Fax: 315-732-3261
E-mail: info@thecsiac.com

An archive of past newsletters is available at **https://journal.thecsiac.com.**

Cyber Security and Information Systems
Information Analysis Center
100 Seymour Road
Suite C-102
Utica, NY 13502

Journal of Cyber Security and Information Systems – October 2013
Understanding Cyber Risks and Security Management

— IN THIS ISSUE —