MetriCon 3.0 Digest

Daniel Conway

1. Background

MetriCon 3.0 was held on July 29, 2008, as a single day, limited attendance workshop in conjunction with the USENIX Association's Security Symposium in San Jose, California. The name MetriCon 3.0 reflects that this was the third meeting with this name and topic, the first being in Vancouver in 2006 and the second being in Boston in 2007. The organizing committee was self-selected, and was chaired by Dan Geer (In-Q-Tel). Also on that committee were Fred Cohen, Dan Conway, Elizabeth Nichols, Bob Blakeley, Lloyd Ellam, Andrew Jaquith, Gunnar Peterson, Bryan Ware, and Christine Whalley. Dan Conway is the principal author of these notes.

Fifty people attended, predominantly representing industry. The meeting lasted from 0845 until 1800 with meals taken in-room.

Opening remarks were offered by Dan Geer, as well as housekeeping notes. Dan thanked Usenix for their logistical support. Formal presentations began at 0900.

2. Track 1: Models proposed and derived; Discussants: Ellam & Nichols

Using Model Checkers to Elicit Security Metrics	-	Heyman, Huygens
Games, Metrics, and Emergent Threats	-	O'Donnell
Bringing Clarity to Security Decision Making Using Qualitative Metrics in 2 Dimensions	-	Cohen

2.1 Using Model checkers to Elicit Security Metrics, Heyman

Heyman began by describing his contributions from MetriCon 1.0 and MetriCon 2.0 which lay the foundation for his secure model framework. In MetriCon 1.0, Heyman presented research on reusable metrics assigned to security patterns. In MetriCon 2.0, Heyman presented research related to combining low level to high level indicators. In this presentation, he distinguished between measuring application security and business level metrics, focusing only on the prior.

The goal of this contribution to the framework is to show how, using formal modeling techniques, it is possible to enumerate all model pattern preconditions or assumptions which are required

for the pattern to operate as expected. The pattern would then allow the production of post conditions or guarantees, which would imply security requirements and thus be a natural place for security measurements to be gathered. This process would be optimized with the use of model checkers.

Modeling as a process involves the activities of isolating assumptions, assessing risk, accepting, monitoring, and refining the model. The basic process begins with building a model and adding constraints as the model evolves.

Heyman then presents a case study for a secure logger. This pattern describes how log entries can be cryptographically pre-processed to ensure integrity & confidentiality. He begins with a logger and adds to the model. One of the guarantees is that the pattern should provide is the detection of entry deletions. The solution is to count the number of log requests and compare this to the log counter, forming a metric that can be monitored. He then suggests further model enhancements including adding key management and meta-metrics.

2.2 Games, Metrics, and Emergent Threats, O'Donnell

O'Donnell presented a game theoretic (single iteration prisoner's dilemma) model to answer the question "When will attackers move from target X to target Y", essentially a critical mass determination. Users can decide between the strategies of Defend A Targets or Defend B Targets. Attackers can choose between Attack A Targets or Attack B Targets. Parameters of the model include market size as a percentage (f), accuracy of security mechanism (p), and the value of a compromised host (v), which are all assumed to be fixed.

The game payoff matrix is given in the table below. The dominant solution occurs when [f / (1-f)] > [1 / (1-p)]. Any solution reversing the inequality represents a parameter space where target B becomes more desirable.

	Defend A	Defend B
Attack A	(1-p) fv	fv
Attack B	(1-f)v	(1-p)(1-f)v

With current assumptions, if the accuracy of the security measure p = 75%, then the critical point for moving from target A (Windows) to target B (Mac) for the market size would be 80% and 20%

respectively. If the accuracy of the security measure were roughly p=.9524, then the critical point from moving from attacking A to attacking B would be a market share of 4.775%. This also implies with the given assumptions that if the accuracy of the security mechanism (p) were only 50%, then the attack strategy would not shift to the Mac until the Windows market share dropped to 67%.

2.3 Bringing Clarity to Security Decision Making Using Qualitative Metrics in 2 Dimensions, Cohen

Cohen presented a continuation of his research into security decision making in a need-to-know context. The basic two-dimensional space can be described as ranging on the X-axis from Highly Opposed to Highly Favorable and on the Y-axis from Low Importance to High Importance. The tools he described and presented previously were Decider & JDM.

Cohen demonstrated the challenges to sound decision-making by engaging the audience in an interactive exercise to solicit opinion using Decider. The group was divided into (a) corporate and (b) government/education. A list of topics was presented and the groups did their best to agree as to where they would rank each topic in the two dimensional space presented earlier relative to making need-to-know decisions. The point of the exercise was to show that people and groups had different sensitivities to different decision factors and disagreed on the magnitude and ordering of factors in decision-making

. The results of the prior analysis and of the audience participation activity was to identify that weighting of decision-making factors related to need-to-know in a metric space produce substantially inconsistent results. Without mandatory guidelines for how to select and weigh factors in such decisions, the decisions are inconsistent and yield different results for the same situation depending on the decision-maker and type of organization.

For the need-to-know issue in the client organization referenced in the talk, a duty-to-protect analysis showed that decision-makers were not applying mandatory guidelines (a satisficing decision based on clearance, compartment, and utility for a sponsored activity) and that the duties could be fulfilled by a crisper decision process without the factors considered relevant by the decision-makers or the participants in the conference.

2.4 Discussion

Ellam & Nichols led the discussion on the modeling track. Discussion for the first three presenters was centered on the value of modeling, and assumptions of modeling were fair game. Cohen gave a short thesis on why we model, and O'Donnell provided additional support for Cohen's defense, suggesting that such models should be used more for decision support rather than for score cards or for input to dashboard applications.

Some of the model assumptions and possible extensions included topics related to the V in O'Donnell's model, the value of a host. Was this the value to the attacker or to the protector? (value to the attacker). Are all attackers the same? Do their objectives and motives play a role in what they attack and how? Can we even know the motivations of the attackers? Would bio-models be more appropriate to use as models rather than game theoretic models?

Many of these questions were generic to modeling in general, so the answer had to be "maybe". In O'Donnell's model, the granularity of the game theoretic model assumes not that all motives are the same, but that the probability of a successful attack is independent of motive. All agreed that models were not built or intended to be used with perfect predictive capabilities.

3. Track 2: Models Tools and their application; Discussants: Peterson & Jaquith

Metrics Driving Security Analytics	-	Beresnevichiene
Security Risk Metrics: The view from the Trenches	-	Mayer
How to Define and Implement Operationally Actionable Security Metrics	-	Williams

3.1 Metrics Driving Security Analytics; Beresnevichiene

Beresnevichiene presented a simulation based security analysis and metrics identification approach as opposed to one based on models driving continuous metrics gathering based on historical data. She began framing the topic with a discussion of the various processes used to drive security analytics, such as risk management lifecycle, historical data based metrics, and predictive simulations. In this framework, she distinguished between traditional assurance (cyclical reviews, historical based, intrusive, point in time) vs new requirements (ongoing assurance, real-time & predictive, non-intrusive & remote, and risk based).

Historical data based metrics are often reported to show whether controls are working effectively and are often a significant part of SLAs and Sarbanes-Oxley audits. They can be used to suggest emerging threats as well. Models of security processes, on the other hand, can be used to determine what metrics are of value as well as to determine how much effort should be concentrated on particular controls and at what rate. Discrete event simulation models allow for more appropriate responses to questions regarding time from vulnerability disclosure to risk reduction.

Beresnevichiene continued with an example of threat mitigation by patch management. In this case, the measure was that of the time taken from exploit code being published to the time when the organization considers the risk mitigated sufficiently. From a historical perspective, an organization could indicate the performance of a patching process. A more useful metric might be to determine how the organization would be impacted by exposure if the patch management process were implemented in a variety of ways, including time compression approaches.

The stochastic simulations described consisted of a model of the patching process where the stochastic elements consisted of inter-arrival rates of malware. The simulation outcomes are then used to derive probability distributions of metrics including the ratio of machines patched against the relevant vulnerability for the various assumed arrival rates of malware. The argument being that the model presents an opportunity for better understanding the trade-offs between effort and benefit. It was noted that the historical data is still valuable in model construction and validation.

3.2 Security Risk Metrics: The View from the Trenches; Mayer

Since Metricon 2.0, Redseal Systems has collected operational security metrics on 50+ IT environments, and this presentation was to share these findings. Mayer used “Threat Graphs” to display a security defect. Defects included (a) vulnerabilities on applications, OS, and embedded systems, (b) unapproved applications, (c) outdated software, and (d) Misconfiguration of network devices, firewalls, routers, load balancers. Defects were caused by (a) business risk, (b) policy violations, and (c) compliance failures.

Mayer distinguished between operational and infrastructural metrics. Operational metrics attempt to measure the business impact of defects, with the result being priority ranking, effectiveness in deploying IT resources, etc. Infrastructural metrics attempt to measure an aspect of the IT infrastructure,

for example properties of the threat graph. The threat graph allows the accumulation of downstream risk from a host itself and to all the other hosts that follow the host in the threat map.

Graphs suggest different ways of measuring, and Mayer discussed some of these measures, including the max path (longest threat graph path), the coverage (threat graph coverage), and the surface (attack surface ratio). The accompanying document describes other measures of exposure, business value, risk, and downstream risk as well. Data collection was performed by evaluation and simply asking.

Results of the study suggest that the average device complexity – the average number of filtering elements per device – was about 12000. The surface vs. coverage ratio indicated that roughly 75% of hosts are protected. A consistent theme of the findings was that complexity is not your friend.

In conclusion, Mayer suggested that an organization can better understand risk by (a) analyzing data across every aspect of the organization's IT infrastructure, (b) discover & rand defects according to direct and indirect threat paths, (c) coordinate the efforts to patch, reconfigure, harden, and re-architect based on fixing defects that pose the highest risk first, and (d) instantly assess how changes will impact risk.

3.2 How to Define and Implement Operationally Actionable Security Metrics; Hawke

Hawke began the discussion by suggesting why people do not embrace metrics, indicating that they should be used to (a) measure, reward, & punish, (b) drive accountability, and (c) tie resources to strategic business initiatives. The problems faced by metrics programs include a lack of consensus as to what is important, a lack of visibility, and the division of responsibilities in that typically the security personnel do not own the management of the solution. Hawke then proceeds to suggest where to start with a metrics program in order to obtain operational excellence.

One key organizational capability cited is to develop methods and processes to measure efficiency in change management. Examples of this might include how quickly can an organization affect change once a decision has been made to change an environmental variable, such as modify PFW settings, configuration change to a device, etc. Measures might include what percentage of changes can be accomplished in a 24 hour period.

A second organizational capability cited is the ability to measure efficiency around auditing procedures, from time from incident detection to remediation. Other examples include (a) how often an organization monitors for non-compliance, and (b) what is the process for remediating non-compliant devices.

Hawke mentioned three projects which impact security, (a) power management for green purposes which lowers exposure, (b) software application management to minimize licensed applications, and (c) infrastructure consolidation. Finally, requirements for metrics were summarized with the five categories of measurable/demonstrable, relevant over time window, simple, actionable, and easily transferable between roles. In summary, Hawke suggested successful projects produce measurable results and that improvements should be measured over time.

3.4 Discussion

Much of the discussion of the "Tools and their application" track were directed toward questions regarding simulation tools. In particular, where did a modeler obtain their input distributions? Such input distributions must be estimated based on historical data. This is statistically complicated as historical data is biased toward the changes that have taken place over the horizon during which the data was collected. Data is known not to be clean, and environments for collection are known not to be mature. There are many challenges to the collection of good data, and those challenges map directly toward the determination of reasonable input distributions.

A second discussion theme dealt with funding decisions. The panel responded that money drove business decisions, but reputation, culture, and other known management concerns eventually impact financials. The panel also mentioned that the highest level they present to regarding metrics was the CIO, and that the typical reaction was that "I didn't know that I didn't know."

A final discussion topic was the impact of virtualization, and the consensus was that virtualization is scary. Virtualization allows for the instantiation of data resources from operating systems to databases to web services, and the fact that they can be instantiated, perform a service, and be de-allocated adds to the complexity of measurement. It was suggested that this be a topic for further discussion at a future meeting.

4. Comparing Metrics Designed for Risk-Management with Metrics Designed for Security; Bayuk

During the final thirty minutes of the in-room lunch, Bayuk offered a presentation to answer an organizational question: "Are you risk or security?" This is an important question as each group uses different tools and techniques and is subject to different regulatory and reporting policies. Often the groups are also parts of different organizational hierarchies as well.

Bayuk distinguishes between risk and security using several comparisons. Risk wants policy compliance whereas security wants zero tolerance. Unfortunately, zero tolerance is generally prohibitively expensive. Risk falls back on policy language which often allows exceptions, such as "unless authorized at a higher level…"

Contrasting risk and security, Bayuk refers to the basis for each: Process vs. Policy. Security policies often map to software implementation such as a firewall rule set. The language is often strict and does not correspond to risk terminology such as confidence intervals. Risk also refers to coverage whereas security refers to quality. In risk, organizations perform assessment whereas in security groups implement solutions. These are completely different skill sets.

Bayuk concludes with a brief discussion of prevalent versus necessary metrics, leaving the group with a set of questions regarding security metrics: (a) what makes security an attribute, (b) how to find it, (c) what objectives are met using only risk metrics, and (d) should overlap be pursued or avoided?

5. Track 3: Scoring results and methods; Discussants: Cohen & Conway

Evidence-Based, Good Enough, & Open	-	Scarfone
Identity Protection Factor	-	Noor

5.1 Evidence-Based, Good Enough, & Open; Scarfone

The NIST is developing a new approach to answering the question "how secure are my organization's systems?" Scarfone begins with an overview of why host security is difficult to measure quantitatively. The focus of the overview is on both the complexity of network attack-focused models and multiple vulnerability classes to measure. The solution being pursued by the NIST is to develop a framework based on evidence-based, good enough answers, and reliance on open standards and specifications that facilitate automation.

Evidence-based implies that decision-making should not be based on conventional wisdom, but instead on "enhancing threat models so that they leverage the results of analyzing historical and current

operational and technical security measures and metrics related to vulnerabilities, attacks, and security controls." Good enough answers suggests that precision is unnecessary in order to support sound decisions, as most sound decisions are not granulated by precision themselves. For example, if a system has a mean time to failure of 6 weeks, that is more actionable information than a score of 74.58. Open standards are attractive for many reasons, including the interoperability standards for expressing, collecting and analyzing security measures and metrics.

Some of the applications of this new framework are (a) to compare a host's security to a baseline configuration or policy, (b) plan security policies and controls, (c) provide data for attack/threat modeling, and (d) assess and quantify risk.

The protocol currently being developed by NIST is "The Security Content Automation Protocol (SCAP)" and can be found at http://nvd.nist.gov/scap.cfm. The CxSS family of protocols includes (a) CVSS (Common Vulnerability Scoring System version 2), which uses base exploitability, base impact, temporal, and environmental scores, (b) CCSS (Common Configuration Scoring System) for analyzing configuration settings, and (c) CMSS (Common Misuse Scoring System) for documenting software feature/trust relationship misuse characteristics.

Currently, the five year project has seen completion of the initial framework planning and was presented in May 2008. The CVSS version 2 and the CCSS are currently available for public review.

5.2 Identity Protection Factor; Noor

Noor presented the Identity Protection Factor (IPF) scale, a classification scheme that permits the comparison of seemingly different identification and authentication technologies on the basis of their vulnerability to attacks. The scale is a one-dimensional scale ranging from 0 to 10. Level ten does not exist as it would imply perfect authentication. The term "factor" is borrowed from that used by producers of sun block. The eleven layers of the IPF Scare are given in the table below:

IPF	Description
0	No identification or authentication
1	**Shared-secret** based authentication on a local system, or a network **without** any network encryption
2	**Shared-secret** based authentication **with** network encryption
3	**Multiple shared-secret** based authentication **without** an external token, but with network

	encryption
4	**Asymmetric-key** based authentication with **Private Key in a file**
5	**Multiple shared-secret** based authentication with **external token** and network encryption
6	Asymmetric-key based authentication with **Private Key** generated and stored **on cryptographic hardware token** and using **keyboard** for authentication to token
7	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token and using an **external PIN-pad** for authentication to token
8	Asymmetric-key based authentication with Private Key generated and stored on cryptographic hardware token using an external PIN-pad and **being physically present at the machine** where the resource exists and where authentication is performed
9	Asymmetric-key based authentication with Private Key generated and stored on hardware cryptographic token, using an external PIN-pad, being physically present at the machine where authentication is performed and using **M of N control** for authentication to token
10	Non-existent/Unknown

Noor suggested many problems due to the current system of user id/password systems as a means of identifying and authenticating users, including (a) the average user has more than a dozen username password combinations to remember, (b) to achieve quick market penetration, businesses frequently initiate customer relationships with minimal authentication systems, (c) the market for identity theft products is pervasive, and (d) the number and types of attacks on end users have grown tremendously in recent years.

Noor defended his one-dimensional linear scale by contending that the over-riding factor that truly matters is the ability of I&A systems to resist attacks, and conceded that it would be possible to create more complex scales. He also compared other frameworks such as the Liberty Alliance Framework, Microsoft's CardSpace, Higgins Open Source Identity Framework, and Oracle's Identity Governance Framework. He indicated that his scale was under consideration as an Oasis standard, and that there was some overlap with NIST Special Publication 800-63. Noor concluded with an invitation to participate in the refinement of the scale, noting that there is no methodology based on the risk of compromise to credentials available otherwise.

5.3 Discussion

The primary topic of discussion was the implications of the IPF model in using a numeric number to represent categorical variables. There was also concern regarding definitions of what an identity

actually was – could it be partially compromised, does a name and address in one context imply an identity but is not sufficient in another context, and so on. There were other concerns about definitions, all complicating the notion that a linear scale was appropriate. However, there were no suggestions as to what might be a better formula or index.

6. Track 4: Enterprise Plans and Lessons Learned; Discussants: Whalley & Geer

eBay's Metrics Program	-	Wong
CIS Security Metrics & Benchmarking Program	-	Kreitner, Nichols
Great-West's Metrics Program	-	Peuhkurinen

6.1 eBay's Metrics Program; Wong

Wong described eBay's two-fold vision of security metrics and described the automated tool they use for data collection and dashboard reporting. First, metrics drive the "roadmap, resourcing, budget & indicate success of the overall business plan". Second, metrics inform business units to drive organizational change. This is done through benchmarking and operational and tactical decision making.

Wong continued to describe a predictive model with a feedback loop. The elements of the loop included culture, technology, risk, and strategy. Assumptions of the security metrics model included (a) security is a means to an end, (b) metrics are also a means to an end, (c) metrics serve security professionals, not the other way around, and (d) least effort – don't over analyze.

The approach taken at eBay is top down (what you want to know) and bottom up (data you already have). Data can be business data or technical data. An important consideration is to identify key risk indicators to avoid collecting data simply because it is easy to do so. Finally, the ability to automate data collection is integral to the design of the collection process. Wong's experience in managing this program has led to two conclusions: (1) there is danger in believing the numbers too much; and (2) aggregation of data sources is difficult. She also indicated difficulty in trying to combine top-down and bottom up approaches to the risk methodology.

6.2 CIS Security Metrics & Benchmarking Program; Kreitner, Nichols

Kreitner discussed the Center for Internet Security's (CIS) Consensus Security Metrics and Benchmarking initiative. The CIS was formed in October of 2000 with a mission to help organizations

reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. Team members consist of corporations, academics, and other organizations.

Kreitner's description of current reality consists of four observations: (1) A focus on compliance with practices/processes with no attention to outcomes; (2) security investment decisions being made on an intuitive basis; (3) methods for risk assessment which lack a feedback loop; and (4) lawmakers and executives asking questions that pose a threat to security funding. The initiative seeks practical approaches to security management, is outcome-based, and ultimately has the internet infrastructure used in the same way as the current highway infrastructure is used.

The operational goal of the initiative is to first reach a consensus on an initial small set of unambiguous security metrics. Next, to launch an operational benchmarking service that enables (a) communication of internal security status over time, (b) inter-enterprise benchmarking of status, and (c) development of a database from which security practice / outcome correlations can be derived to better inform future security investment decisions. The current status is outcome metrics over time (still at a conceptual level) and process metrics such as %systems configured to approved standards, %systems patched, % business applications that had a pen test.

Nichols continued on with a description of cross enterprise benchmark metrics. Two enabling features of such an endeavor include (1) Anonymization, or de-identification and (2) you get what you give (YGWYG), where data owners determine how much information they wish to reveal and are provided with that level of granularity in the reports they receive. Currently, the report consists of current descriptive stats (min, max, mean, stdev, histograms, percentiles, youarehere display), and trend (rates of change of groups and individuals, current rates, youarehere trend displays.

6.3 Great-West's Metrics Program; Peuhkurinen

Peuhkurinen describes his role and experiences in implementing an information security metrics program at Great-West, a holding company that operates in Canada, Europe, the USA, and the Far East. His approach is a "top-down approach to metrics, beginning with stakeholder buy-in of objectives, designing KPIs that support the objectives, and finally creating metrics that feed into the KIPs." The program is in the pilot phase and replacing an ad-hoc practice.

Peuhkurinen begins by describing a maturity model for an information security balanced scorecard program with five levels: (1) Initial, (2) Repeatable, (3) Defined, (4) Managed, and (5)

Optimized. The objectives for the plans are to (a) show value for investment, (b) provide input into the strategic planning process for the information security program and track progress toward goals, (c) provide visibility into risk, and (d) support the continuous improvement requirements. The balanced scorecard consists of corporate contribution, customer orientation, internal processes, and future orientation. Each is assigned a mission, objectives, and potential measures.

Peuhkurinen closes by describing some of his issues of concern, including how to measure value to the six different organizations, as well as how to measure IS operations when they are not standardized across the various companies. He conceded that each have their own business leadership teams who naturally are most interested in their own risk profiles, and cites this as his greatest metrics challenge.

6.4 Discussion

Discussion began with a question: how do you incent people to share data, especially when counsel says no to any request outright. This is a difficult problem, and while anonymizing information is also difficult, it can sometimes be a compromise. eBay measures compromised accounts as a critical metric for security improvement. The discussion continued onto anonymizing – that when there is a small sample size, then it is easier to determine who is who. Wong notes that they have had success starting small and having success, both in receiving upper level support and in getting people to share more information. Ashed suggests we need to impose regulation – to force companies to share. The room came to life at this suggestion. Finally, there was some discussion about moral hazard – how does one know that the information others are sharing is even accurate or intended to skew the descriptive statistics.

7. Track 5: Perimeters are the simplest possible thing to measure, right?; Discussant: Blakley

Metric-Based Firewall Management	-	Bhatt, Rao, and Okita
Firewall configuration Errors Revisited	-	Wool

7.1 Metric-Based Firewall Management; Bhatt, Rao, and Okita

Bhatt presented research concerning the problem of managing firewall rule sets and the trade-off between complexity and management cost. The hypothesis was that the more complex the rule set (possibly thousands of records), the more difficult to manage and likely the more insecure. Security problems are introduced into firewall rule sets from practices of implement once / remove never, changes with unpredictable effects, cargo cult mentality, and a disconnect between business need and business risk. The suggested solution is to keep it simple (stupid). This is accomplished by reducing confusion/complexity, improved understanding, reducing decisions, and better implementation understanding.

The authors propose a new metric – effectiveness – to evaluate the complexity of a rule set. In essence, this metric captures the degree to which different rules are independent of one another with the assumption that the greater the intersection, the more complex, the more expensive to manage. The tool breaks up the rule set into non-overlapping blocks and the metric attempts to capture the remaining complexity.

The authors' findings presented included the following.

- No clear relationship between the number of rules and the number of locations was found.
- Higher numbers of objects do seem to suggest more interference.
- Rules that get into a rulebase don't tend to be removed.
- There is interference in most configurations, but the amount of interference varies dramatically.
- There is a direct relationship between the number of interfering rules and the number of interfering rules with conflicting activities.
- Over time, objects which interfere will continue to interfere.
- Effictiveness varies dramatically and over time
- Manual rule cleanup is effective.

7.2 Firewall configuration Errors Revisited; Wool

Wool revisits a 2004 research finding that indicated that corporate firewall configurations were often enforcing poorly written rule sets containing many mistakes, and that the higher the complexity of the rule set, the more detected risk items were allowed. Wool tests whether its findings are still valid with the more recent firewall products Checkpoint and PIX. The original study showed that over 50% of firewalls had problems. Newer versions had slightly fewer errors on average as they had stronger default settings. It concluded that small is beautiful.

The conclusion is that small is still beautiful. The Cisco PIX firewall was found to generally be "less badly configured", though it was difficult for Wool to cite a cause for this. It was also found that a rule-set's complexity, as measured by their firewall complexity metric, is still positively correlated with the number of detected risk items. This was true independent of the vendor product. Unlike 2004, Wool's research found that later software versions were not any more likely to have fewer errors, as recent versions do not appear to have any changes to the default settings.

7.3 Discussion

Each talk was very lively and the attendees were generally captivated during the presentations. The topic of discussion converged onto "how important are firewalls?" and "are poorly configured firewalls less secure than well configured firewalls?" While the researchers agreed that firewalls minimally were useful for traffic management, it was difficult to map complexity to security directly.

8.0 Conclusion; Dan Geer

Geer thanked the attendees and presenters, declared the workshop a success, and the festivities began.