

# **System Dynamics Modeling for Information Security: A Group Modeling Workshop**

## *Organized by*

*Dr. Jose J. Gonzalez, Agder University College, Norway  
Andrew P. Moore, CERT Coordination Center, Software Engineering Institute  
Dr. Jose Maria Sarriegui, University of Navarra, Spain*

## *With support from*

*The CyLab at Carnegie Mellon University  
Pittsburgh, PA 15213*

## **Dates**

- Introductory System Dynamics tutorial by Johannes Wiik of Agder University College, Norway: Monday, 2/16/04 (*optional*)
- Core group modeling activity: Tuesday, 2/17/04 through Thursday, 2/19/04
- Summary of workshop results to broader audience: Friday, 2/20/04 (*optional*)

## **Host and Location**

CERT/CC, Software Engineering Institute, 4500 Fifth Ave., Pittsburgh, PA 15213

## **System Dynamics Facilitators**

- Dr. David Andersen, University at Albany, Albany, NY
- Dr. Jose J. Gonzalez, Agder University College, Norway
- Dr. Mohammad Mojtahedzadeh, Attune Group/University at Albany, Albany, NY
- Dr. Jose Maria Sarriegui, TECNUN, University of Navarra, Spain
- Johannes Wiik, Agder University College, Norway
- Dr. Elise Weaver, Worcester Polytechnic Institute, Worcester, MA
- Aldo Zagonel, University at Albany, Albany, NY

## **General Objectives**

- to develop a preliminary System Dynamics model of some important aspect of the information security problem (see the appendices for the two proposed threads)
- to identify additional data on those aspects that are unknown or unavailable, but needed for future progress on this problem
- to investigate possible collaborations for longer-term work to propose to prospective sponsors

## **Contact Information**

- Dr. Jose J. Gonzalez, Faculty of Engineering and Science, Dept. of Information & Communication Technology, Agder University College, Groosvn. 36, NO-4876 GRIMSTAD, Norway ([jose.j.gonzalez@hia.no](mailto:jose.j.gonzalez@hia.no))
- Andrew Moore, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213 ([apm@cert.org](mailto:apm@cert.org))

- Dr. Jose Maria Sarriegui, TECNUN, University of Navarra, San Sebastian, Spain (jmsarriegui@tecnun.es)

## **Agenda**

- **Monday, 2/16/04 (Tutorial, open to anyone interested):**  
 1000 – 1200: Tutorial on System Dynamics: J. Wiik (Training Room D, SEI)  
 1200 – 1330: Lunch  
 1330 – 1600: Tutorial on System Dynamics: J. Wiik (Training Room D, SEI)
- **Tuesday, 2/17/04 (Group Modeling, open to group modeling participants):**  
 830 – 900: Continental breakfast (catered, Training room D, SEI)  
 900 – 1200: Plenary: Problem description (Training room D, SEI)  
 1200 – 1300: Lunch (catered, Training room D, SEI)  
 1300 – 1600: Break out:  
     Insider Threat (Training Room D, SEI)  
     Outsider Threat (Room 416C, SEI)
- **Wednesday, 2/18/04 (Group Modeling, open to group modeling participants):**  
 830 – 900: Continental breakfast (catered, Training room D, SEI)  
 900 – 1000: Plenary: Thread progress summary (Training room D, SEI)  
 1030 – 1200: Break out:  
     Insider Threat Thread (Training Room D, SEI)  
     Outsider Threat Thread (Room 416C, SEI)  
 1200 – 1300: Lunch (catered, Training room D, SEI)  
 1300 – 1600: Break out:  
     Insider Threat Thread (Training Room D, SEI)  
     Outsider Threat Thread (Room 416C, SEI)  
 1830: Workshop Dinner at Mount Washington
- **Thursday, 2/19/04 (Group Modeling, open to group modeling participants):**  
 830 – 900: Continental breakfast (catered, Training room D, SEI)  
 900 – 1000: Plenary: Thread progress summary (Training room D, SEI)  
 1000 – 1200: Break out:  
     Insider Threat Thread (Training Room D, SEI)  
     Outsider Threat Thread (Room 416C, SEI)  
 1200 – 1300: Lunch (catered, Training room D, SEI)  
 1300 – 1400: Break out:  
     Insider Threat Thread (Training Room D, SEI)  
     Outsider Threat Thread (Room 416C, SEI)  
 1400 – 1530: Plenary: Thread results presentation  
 1530 – 1700: Wrap up (plans for joint proposals and papers)
- **Friday, 2/20/04 (Results Presentation, afternoon open to anyone interested):**  
 900 – 1200: Construct workshop results presentation (Training Room D, SEI)  
 1200 – 1330: Lunch  
 1330 – 1500: Workshop results (Training Room D; open to anyone interested)

# **Appendix A**

## **Proposal for a Thread on the Insider Threat Problem**

### **Proposal Contributors**

- SEI/CERT, USA (PA): Chris Bateman, Dawn Cappelli, Casey Dunlevy, Andrew Moore, Dave Mundie, Stephanie Rogers, Tim Shimeall
- TECNUN, University of Navarra, Spain: Jose Maria Sarriegui
- Syracuse University, USA (NY): Jeff Stanton
- Agder University College, Norway: Jose J. Gonzalez

### ***Proposal history***

Proposed: January 23, 2004

Revised: January 29, 2004

### ***Objectives of the Insider Threat Problem Thread***

- to develop a preliminary System Dynamics model of some important aspect of the insider threat problem, based in part on an ongoing study of insider compromises across the US critical infrastructure sectors conducted by the U.S. Secret Service and the SEI/CERT
- to determine whether it is feasible to develop a generic system dynamics model for insider threat that will be useful to all organizations, or at least all organizations within a single critical infrastructure sector

### ***Objectives of this Proposal***

- to scope the aspect of the insider threat problem to be dealt with in the workshop
- to describe the problem in sufficient detail so as to provide a good starting point for the workshop and to ensure a good chance of success
- to provide a range of options in problem formulation that allows quick narrowing of problem scope at the beginning of the workshop according to the interests of the participants
- to provide the opportunity for other workshop participants to review and provide feedback for further refinement of this proposal prior to the actual workshop

### ***Insider Threat Thread Problem Outline***

1. *What is the real problem (not just a symptom of the difficulty)?*
  - a. Insider attacks cause organizations major damage to their reputation, employee morale, and bottom line.

2. *Why is it a problem?*
  - a. Explanation 1: Insider threat is a low base rate problem (similar to workplace violence, natural disasters)
    - i. Meaning that management does not see any way to predict or protect against insider attacks (insider compromises are often a direct or indirect result of abuses of legitimate authorization, which makes it very difficult to protect against or to detect once it occurs)
    - ii. And, because management views insider attacks as unpreventable, there is an associated loss of perceived control or self-efficacy on the part of management
    - iii. This loss of perceived control or self-efficacy leads to management inaction on the insider threat problem.
  - b. Explanation 2: Management misperceives the risk due to insider threat. They do not perceive the risk because they do not “measure” it, and they do not measure it because they do not think that it is a real threat or because they are unaware of tools and techniques that may be available for measuring it.
    - i. Organizations often concentrate on outsider attacks to the near exclusion of insider attacks
      1. Unfortunately, more *successful* attacks on organizations come from the inside than the outside (Schultz 2002)
      2. Insider attacks pose far greater *risk* to organizations than do outsider attacks (Schultz 2002)
      3. Situation analogous to looking for your lost watch where the light is, rather than where you lost it, because it would be easier to see
3. *How have organizational policies exacerbated the problem?*
  - a. Giving star players free reign because of fear of losing those employees.
  - b. Ignorance (either on purpose or due to naiveté) of indicators of insider threat
  - c. Disregard for information security best practices.
  - d. Poor human resource practices with respect to pre-hire screening of employees, ongoing monitoring of employees, and provision of facilities to help employees deal with problems (e.g., employee assistance programs, AKA EAPs)
  - e. Lack of training and education of employees on the reliance and trust that the company has in employee job performance
  - f. Lack of training and education of employees on the consequences of violations of employee trust, e.g., prosecution
  - g. The tendency of organizations not to report the problem and seek legal remedy for fear of damage to their reputation does not deter future insider threat attacks.

4. *What is the purpose of the model?*
  - a. To show that the observance of key indicators and taking preventive action based on those indicators could substantially reduce the likelihood of insider attack in organizations that fit a certain profile
  - b. To study the effective balance between all the measures oriented to increment the security of information systems for those organizations
  
5. *What is the approach to modeling?*
  - a. To analyze the processes within a generic organization (people, incidents, or processes as the unit of analysis)
    - i. Identify multiple key exemplars of the generic organization to indicate the importance of the problem and to enable validation of reference modes of behavior
    - ii. Approach is not to analyze the dynamics of a grouping of organizations (organizations or groups of organizations as the unit of analysis)
  - b. Handle the low base rate problem by identifying a *proxy measure* that
    - i. is relatively easy, inexpensive, and/or convenient to obtain from the generic organization, e.g., measuring employees' *intentions to quit* as a proxy for *voluntary turnover* in a company
    - ii. occurs frequently or can be captured frequently or continuously (in contrast to the capture of low base rate events, which by definition happen only rarely)
    - iii. on conceptual or empirical grounds, can be shown to be substantially connected to actual insider malicious activity
  - c. Identify key behavior patterns that
    - i. indicate the likelihood or existence of insider threat compromises in the generic organization (as derived from its exemplars)
    - ii. represent suitable proxy measures for the insider threat problem
  
6. *What is the generic organization to be modeled?*
  - a. Primary candidate
    - i. Generic organization reference modes
      1. Very trusted environment for certain classes of employees (including the insider)
      2. Management recognition and/or response to security threats (indicators) posed by insider were minimal or non-existent
      3. Successive lessening of security controls to prevent detection and to magnify the damaging impacts of the attack

- ii. Exemplars (we continue to look for good public references to these)
  - 1. Timothy Lloyd case targeting Omega Engineering Corporation
    - a. Good public source: <http://www.nwfusion.com/research/2000/0626feat.html>
    - b. Prior system dynamics analysis: <http://www.systemdynamics.org/conf2003/proceed/PAPERS/294.pdf> (Melara 2003)
  - 2. John Rusnak case targeting AllFirst Bank
    - a. Good public sources: <http://www.usdoj.gov/dag/cftf/chargingdocs/allfirst.pdf>  
[http://www.erisk.com/LearningCenter/CaseStudies/ref\\_case\\_aib.asp](http://www.erisk.com/LearningCenter/CaseStudies/ref_case_aib.asp)
    - b. News article: [http://www.sunspot.net/business/balte.bz.allfirst06jun06\\_0\\_4228032.print.story?coll=bal-business-indepth](http://www.sunspot.net/business/balte.bz.allfirst06jun06_0_4228032.print.story?coll=bal-business-indepth)
  - 3. Thomas Varlotta case targeting the FAA
    - a. Primary public source: court records
    - b. Bit news article:
      - i. <http://archives.californiaaviation.org/airport/msg02974.html>
      - ii. <http://www.landfield.com/isn/mail-archive/2001/Jun/0068.html>
      - iii. <http://www.thetracon.com/news/trib092200.htm>
  - 4. Bahram Saghari case targeting TVI Interactive
    - a. Primary public source:
      - i. Lexis Nexis: 2002 Cal. App. Unpub. Lexis 4790 (SEI can supply upon request)
  - 5. Christopher Harn case targeting paramutual betting via Autotote Systems processing.
    - a. Good public sources
      - i. Burrough, "Winner Lose All," Vanity Fair, March 2003 (SEI can supply upon request)
      - ii. [http://www.baselinemag.com/print\\_article/0,3668,a=34708,00.asp](http://www.baselinemag.com/print_article/0,3668,a=34708,00.asp)

6. Roger Duronio case targeting Paine Webber
  - a. Primary public source:
    - i. [http://www.njusao.org/files/PDF%20files/Duronio\\_indictment.pdf](http://www.njusao.org/files/PDF%20files/Duronio_indictment.pdf)
  - b. Bit new clips (widely reported):
    - i. <http://www.usdoj.gov/criminal/cybercrime/duronioIndict.htm>
    - ii. <http://www.philly.com/mld/inquirer/news/local/4763384.htm>
- b. Other Candidate Generic Organizations
  - i. Generic organization that hires very young individuals at low salaries (often data entry clerks) to perform functions that require great trust in handling company assets (6 cases)
    1. Cases would seem to have been prevented through some training about the trust that the organization has in their performance, organizational development procedures that increase the levels of commitment on the part of employees, auditing procedures to detect abuses, and warnings about prosecution of violations of that trust
      - a. Although there seems to be a frequent thread of romance playing a motivational role in these cases: young insider romanced by an outsider to extract/falsify internal information; not clear how the above training would help there.
    2. Cases not very rich and therefore may not be a good target of system dynamics (some simple best practices seem to suffice)
    3. Could study the reasons why organizations do not have the insider threat problem on their radar screens; when simple security best practices are sufficient, why don't organizations implement and maintain them? This would seem to involve the organization's larger business missions and objectives.
  - ii. Generic organization that provides a rich environment for insiders to take company assets to create competitive product/service (3 cases)
    1. Feeling of entitlement to products/customers created by insider to the point of taking those products/customers along to next job

7. *What are the key variables and concepts (proxy measures for insider threat)?*
  - a. Classes of variables indicating “precursor events” (Schultz 2002)
    - i. deliberate markers
    - ii. meaningful errors
    - iii. preparatory behavior (e.g., testing reaction to security threats, questions unrelated to job performance)
    - iv. correlated usage patterns
    - v. verbal behavior (e.g., aggressive, domineering, angry, frustrated)
    - vi. personality traits (e.g., aggressive, domineering, introverted, depressed, poor at handling stress and conflict, frustrated with work (Schultz 2002))
    - vii. changes in responsibility or position – demotions, reorganizations, ...
  - b. other variables/measures possibly of interest
    - i. IT total investments / Total budget of the firm
    - ii. Security investments / IT total investments
    - iii. "Hard" Security investments / Total security investments
    - iv. Software security investments / Total security investments
    - v. Losses due to Security incidents / Total budget of the firm
    - vi. Security people / Total people of the firm
    - vii. Reported insider incidents per year
    - viii. Total incomes of consulting firms working on security
    - ix. Number of firms which already have implemented structured security policies per year
8. *What is the time horizon for the analysis (cause and effect are often distant in time and space)?*
  - a. Insider threat problems seem to be roughly partitioned into cases that are motivated by personal gain (e.g., greed) and cases that are motivated by a grudge against the organization. Cases due to grudge are usually crimes of emotion for which the time horizon is relatively short (often less than a year). Cases due to personal gain are often much better thought out and can occur over a longer time span (up to 5 years in duration).
  - b. In some cases it could be interesting to establish an extended time horizon that permits simulating the growth of the Information Systems into the company and, perhaps, the “decline” of the insider
  - c. The sampling interval of measurement should be fine enough to accurately capture important changes to the dynamics of hiring, retention, and layoffs, insofar as these are important events that modify the composition of the workforce in substantial ways. Sampling daily is probably too fine; sampling quarterly may be too gross.

9. *What is the historical behavior of the key concepts and variables?*
  - a. Preliminary causal loop diagrams?
    - i. We are still considering this question. Our plan is to prepare chronologies for the exemplars of the generic organization. These chronologies would help in detailing the reference modes and causal loop diagrams.

## References

Melara, C., Sarriegui, J.M., Gonzalez, J. J., A. Sawicka, D.L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," in *Proc. of the 21<sup>st</sup> International Conference of the System Dynamics Society*, New York, NY, 20-24 July 2003 (also appears in *From Modeling to managing Security: A System Dynamics Approach*, J.J. Gonzalez (ed.), Norwegian Academic Press, Norway, 2003).

Schultz, E.E., "A Framework for Understanding and Predicting Insider Attacks," *Computers and Security*, Elsevier Science Ltd., 21 (6) October 2002, 526-31.

## Bibliography

- Shaw, E. D., Post, J. M., & Ruby, K. G. (2002). *Inside the Mind of the Insider*. Available at: <http://www.securitymanagement.com/library/000762.html>.
- Siponen, M. T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal*, 14 (4), 15-23.
- Brennan, R. O. (2001). Research on Mitigating the Insider Threat to Information Systems. Santa Monica, CA: Rand Corporation.
- Anderson, R. H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., & Van Wyk, K. (2000). Research on Mitigating the Insider Threat to Information Systems #2. Santa Monica, CA: Rand Corporation.
- Anderson, R. H., (1999). Research and development initiatives focused on preventing, detecting, and responding to insider misuse of critical defense information systems. Santa Monica, CA: Rand Corporation.

## **Appendix B**

### **Proposal for a Thread on the Outsider Threat Problem**

#### **Proposal contributors**

Agder University College, Norway: Jose J Gonzalez, Johannes Wiik  
SEI/CERT, USA (PA): Andrew Moore, Howard Lipson, Tim Shimeall

#### ***Proposal history***<sup>1</sup>

Proposed: November 17, 2003  
Revised: December 10, 2003, January 16 and 27-29, 2004

#### ***Objectives of the Outsider Threat Problem Thread***

- to develop a preliminary System Dynamics model of important dynamic aspects of the outsider threat problem,
- to determine whether it is feasible to develop a generic system dynamics model for outsider threat that will be useful to all organizations, or at least all organizations within a single critical infrastructure sector
- to identify additional data on the outsider threat problem that is unknown or unavailable, but needed for future progress on this problem
- to investigate possible collaborations for longer-term work to propose to prospective sponsors

#### ***Objectives of this Proposal***

- to scope the aspect of the outsider threat problem to be dealt with in the workshop
- to describe the problem in sufficient detail so as to provide a good starting point for the workshop and to ensure a good chance of success
- to provide the opportunity for other workshop participants to review and provide feedback for further refinement of this proposal prior to the actual workshop
- to help the reader make a decision regarding which workshop thread to choose (for an alternative thread, see “Proposal for a Thread on the Insider Threat Problem”)

#### ***Outsider Threat Thread Problem Outline***

##### **Issue**

Attacks on information networks typically originate with the discovery of a ‘system vulnerability’ by advanced intruders (Schneier 2000, Ch. 13; see also Ellison and Moore 2002, p. 43ff). Crude exploit tools are developed and distributed, leading to the first attacks. Next, advanced automated scanning/exploit tools are used to roll out more numerous and more sophisticated attacks. On the ‘victims’ side, a process of developing

---

<sup>1</sup> In previous stages the problem proposal had the working title “The System Vulnerability Threat to Information Security.”

defenses ensues (detection of the source of the vulnerability, development of a software patch, distribution and installation of the patch). Ultimately, the attack wave subsides (Arbaugh, Fithen, and McHugh 2000; Lipson 2000). The whole process is referred to as a ‘vulnerability exploit cycle’ or ‘vulnerability life cycle’.<sup>2</sup>

Traditionally, most attacks on information networks have been performed by the hacker community. Although nasty enough, hacker attacks have mostly caused transient problems. However, the hacker threat might become an increasing nuisance as more advanced attack tools are developed and an exponentially growing number of poorly maintained units belonging to single individuals expand the number of vulnerable sites to unprecedented levels.

Schultz (2002) discusses the claim that insider attacks are more numerous than outsider ones. He concludes that it is wrong to claim that. But Schultz adds: «At the same time, however, to say both (sic!) that more *successful* attacks come from the inside (especially considering that so many organizations’ network security amounts to a “hard outer coating, but a soft-chewy middle”) is more likely to be true. Additionally, there is no debate that insider attacks pose a far greater level of risk than do outsider attacks.»

Careful reading of this statement reveals several issues:

1. There does not seem to exist data (at least not by 2002) to substantiate a hard claim about the relative prevalence of successful insider vs outsider attacks.<sup>3</sup>
2. No data is provided for the *dynamics* of point 1 (e.g. whether the relative prevalence of successful insider vs outsider attacks is changing over time and how).
3. The strong statement «... there is no debate that insider attacks pose a far greater level of risk than do outsider attacks» should be qualified, given that e.g. Code Red is claimed to have cost an estimated *total* of US\$ 2.6 billion (Ghosh 2002) and Love Letter of US\$ 8 billion (Ghosh 2000). Further, no data is provided for *dynamics* of the threat (e.g. whether the risk pattern is changing over time).

Indeed, a good question is whether increasing sophistication and automation of attacks might lead to more effectiveness of outsider attacks. (Although such automation also feeds into insider attacks, but up to this point subsets of the insiders have been too unsophisticated to be aware of such attack automation or already possess the access provided by such automation. This COULD change rapidly, however.)

There is a key difference between insider and outsider attacks: Insider attacks target normally single organizations – there are hardly instances of two or more insiders

---

<sup>2</sup> And, indeed, such vulnerability exploit cycle resembles a ‘product life cycle’ (see e.g. Ch. 9 in Sterman 2000).

<sup>3</sup> Tim Shimeall added the following comment: «All of the objectively citable data I’m aware of shows much fewer insider vs. outsider attacks – but there is a lot of reason to believe the data is incomplete. So your statement here is true.»

targeting several distinct organizations.<sup>4</sup> In strong contrast, outsider attacks can be automated to target virtually any number of organizations. This aspect of *number* – if paired with large severity of attack – can make outsider attacks an issue of national or even international importance.

On the other hand, several authors argue that the distinction between insider and outsider threat is becoming more and more fuzzy (Lipson and Fisher 1999; Schultz 2002). Lipson and Fisher write: «In the highly distributed applications and Internet-based systems of today there is little distinction between insiders and outsiders.» Schultz states: «With all the outsourcing that is occurring, it is becoming difficult and hard distinction between insiders and outsiders... Additionally, many so-called “insider jobs” have turned out to be the result of complicity between an insider and an outsider.» With this in mind, this workshop should look for possible synergies between its two threads (insider and outsider threat).

There are reasons for considering the possibility that outsider attacks – rather than originating in dispersed hacker communities and without other major purpose than beating the defenses – could be coordinated and launched by organized groups (e.g. mafia or terrorists).

What would happen if a billionaire fundamentalist were to fund an organized activity involving hundreds of brilliant computer scientists for the purpose of identifying dormant system vulnerabilities, develop advanced exploit tools and – without advanced notice – roll out a series of devastating attacks towards some neuralgic point of the global information network? Could such roll out be too fast for the defenses to cope with, i.e. could the attacks outnumber the defenses? Could the financial game of chess be in a state of check for days and weeks – could it even be set mate? Could a well-timed attack cause the energy supply to break down at the worst thinkable moment, e.g. in the middle of an unprecedented ‘cold wave’ striking North America? (The issues here are very complex; it is hoped that the best answer is “probably not”, but the parameters on this “probably” are a very complex mix of defensive measures, business processes, redundancies and emergency planning as opposed to malicious access, malicious processing, attack resource requirements and other attack planning complexities. A nice challenge to system dynamics and other tools that have been developed to manage complexity to tack!)

A preliminary study of available literature has documented that such concerns about concerted and planned attacks are shared by colleagues (see e.g. Johnson, Guttman, and Woodward 1997; Schneier 2000; Shrobe 2002). We take such concern as indicative that it is worth looking closer at the issue, without necessarily assuming worst case scenarios.

---

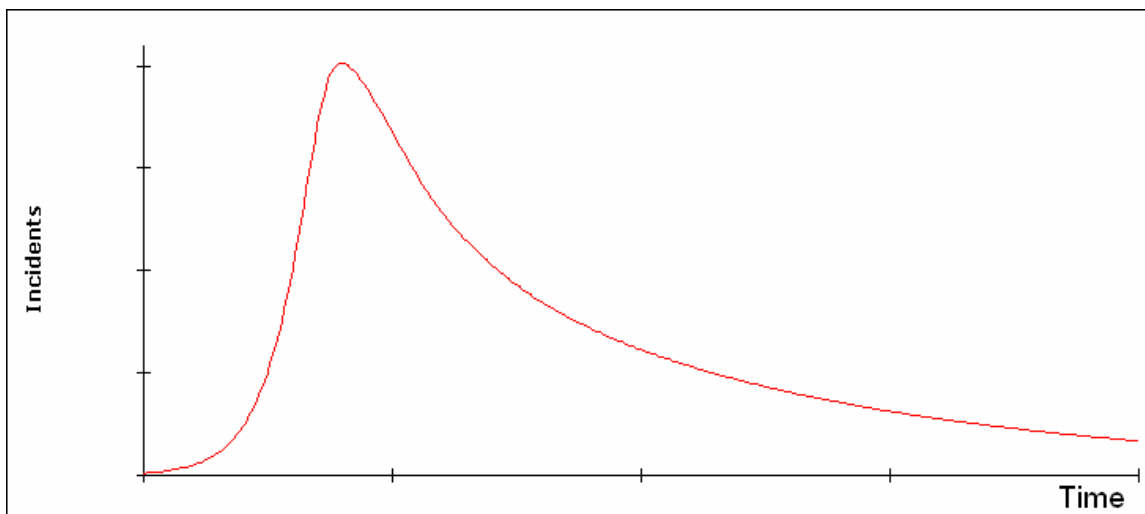
<sup>4</sup> A lot of the truth of this statement depends on the word “organization” – in the Harn case, [http://www.baselinemag.com/print\\_article/0,3668,a=34708,00.asp](http://www.baselinemag.com/print_article/0,3668,a=34708,00.asp), more than three different organizations were targeted (more than three different racetracks/pools of betters). They were all attacked via the same methodologies and access at a single location, but the loss was felt by several different organizations.

## ***Problem milestones***

The problem sketched in the previous section is vast. For convenience we suggest approaching the problem in several stages, each of intrinsic interest, all of them connected by logical threads.

### **The Single Vulnerability Problem**

Briefly stated, the problem is to understand the determinants of the life cycle of a single vulnerability (Arbaugh, Fithen, and McHugh 2000). For the purpose of illustrating the issue, the problem can be simplified to understand a generic life cycle such as given in Fig. 1 of Arbaugh, Fithen, and McHugh's paper. (A qualitative rendering is presented in the figure below, using arbitrary units for both axes).<sup>5</sup>



A successful model would throw light on aspects of the hacker community that are difficult to assess directly (i.e. the ability of the model to render actual reference behavior from several well-studied vulnerabilities – such as Figs. 3-5 of Arbaugh, Fithen, and McHugh's paper – would increase our faith in the model's assumption about how knowledge spreads in the hacker community, etc.)

Further, the model could be used to:

- Experiment with policies to prevent or at least reduce the impact of attacks.
- Help identify trends and explain the determinants of trends
- Assess the extent to what current data can be used for numerical simulation analysis; suggest further empirical studies; suggest further modeling studies; all these would be steps in developing an application for funding.
- Build a basis for the next two problem stages

---

<sup>5</sup> At this stage the figure should not be taken as too literally. This is one of many curve shapes (basically, one can vary the amplitude, skew, kurtosis, and variance of the above curve pretty arbitrarily and find examples in the real world; there are numerous examples where the tail is much steeper than the head). Rather, the purpose of the figure is to serve as generic reference behavior mode for a simple model prototype.

We do have a simple System Dynamic model for the Single Vulnerability Problem that is able to render the idealized reference behavior shown in the figure above. Arguably, this model can be used as a basic for further discussions at the workshop. (A detailed description of the model will be distributed one week ahead of the workshop.)

## **The Multiple Vulnerability Problem**

Hackers roll out attacks on vulnerabilities so that exploitation of several vulnerabilities might overlap and interact. At the outset one would expect that the ideal shape of the vulnerability life cycle depicted above will not hold when several vulnerabilities compete for the hacker community's attention. In fact, Figs. 3-5 in Arbaugh, Fithen, and McHugh's paper do suggest the existence of two or more humps. Indeed, there are lots of reasons for multiple humps other than competition – such as bundling of attack tools, “attractiveness” of the target, new exploit discovery, etc.

We have not investigated in depth the issue of reference behavior for the Multiple Vulnerability Problem. It would appear that there is at least partial information in terms of the aggregated number of incidents reported (the CERT/CC Statistics 1988-2003, [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)). There are some curves showing incident reports against services and vulnerabilities that may be relevant – see <http://www.cert.org/archive/ppt/IntelDataExamp.ppt>, although there is more data than is shown there.

Again, a successful model would throw light on aspects of the hacker community that are difficult to assess directly (i.e. recruitment to the hacker community, how the hackers pick various vulnerability types, the R&D pipeline in the hacker community, etc)

Further, the model could be used to:

- Experiment with policies to prevent or at least reduce the impact of attacks. An intriguing issue would be to model traceability (Lipson 2002).
- Devise better ways to monitor and measure hacker activity including spread of information
- Impact of growth of IT systems including larger system integration
- Help test controversial issues (e.g., whether full disclosure of vulnerabilities is beneficial or detrimental).
- Assess the impact of the R&D competition between defenders and attackers. Again, traceability – if feasible – could provide ways to explore this issue.
- Help identify trends and explain the determinants of trends
- Help explore the robustness of internet sectors (i.e. the energy or the health care sector) in various scenarios of increasing frequency of attack or even of greater attack sophistication and automation.
- Help estimate damages of potential attacks and assess cost-benefit ratios of defensive policies.

- Assess the extent to what current data can be used for numerical simulation analysis; suggest further empirical studies; suggest further modeling studies; all these would be steps in developing an application for funding.
- Build a basis for the next problem stage

### **The Concerted Attack Problem**

Here the issue would be the ability of internet sectors (i.e. the energy or the health care sector or even the .mil domain) to perform critical functions in case of a concerted attack.

At first sight, modeling such challenge would involve the identification of a target sector within the information network for the study (such as the financial system, the energy sector, possible the .mil domain). One would need to estimate the amount of dormant system vulnerabilities (e.g. buffer overflow bugs in Internet Explorer, etc),<sup>6</sup> the rate of discovery of vulnerabilities depending on the attacker's resources, the rate of development of defenses once vulnerabilities are exploited by attackers, etc.

Some, may be most of the data needed might be known, or at least easily ascertained, other data might be uncertain, but critical (thus demanding further studies).

The model could be used to:

- Explore the robustness of various internet sectors to concerted attacks
- Help test controversial issues (e.g., degree of causation by software developers vs system managers).
- Devise better ways to monitor hacker activity
- Help identify trends and explain the determinants of trends
- Help explore the robustness of internet sectors (i.e. the energy or the health care sector) in various scenarios of increasing frequency of attack or even of greater attack sophistication and automation.
- Help estimate damages of potential attacks and assess cost-benefit ratios of defensive policies.
- Assess the extent to what current data can be used for numerical simulation analysis; suggest further empirical studies; suggest further modeling studies; all these would be steps in developing an application for funding.

We have implemented a generic model developed by Rudolph and Repenning (Rudolph and Repenning 2002b, 2002a) using Powersim Studio. The purpose of the exercise was to keep the model in store for adaptation to information security.

We discovered several minor errors in the model ("minor" in the sense that they do not affect the overall behavior of the model, i.e, the conclusions of the study stand).

---

<sup>6</sup> Undiscovered software bugs can often provide points of attack for malicious agents. It is estimated that released professional software has between 5 and 15 undiscovered bugs per 1000 lines of code. Windows 2000 has 43 million lines of code, Windows XP even more. Interesting question: How many of the estimated half million bugs in Windows XP (and other software) can be exploited by attackers?

The Rudolph and Repenning study might be useful for the workshop in two ways:

- It can help making concepts of System Dynamics available to a general audience
- It might be used as a starting point for the concerted attack problem, including suggesting reference behavior modes (the “system” copes with concerted attacks up to some threshold. Above that threshold it becomes “choked”.)

## **Perspective**

Several perspectives can be appropriate (to be further discussed at the workshop):

- Software vendor
- System manager
- Homeland security (government, military, etc)
- Scientific (NSF, etc)

## **References**

- Arbaugh, William A, William L Fithen, and John McHugh. 2000. Windows of Vulnerability: A Case Study Analysis. *Computer* 33 (12):52-59.
- Ellison, Robert J., and Andrew P. Moore. 2003. *Trustworthy Refinement Through Intrusion-Aware Design (TRIAD)*. CMU/SEI 2002 [cited 17.11. 2003]. Available from <http://www.cert.org/archive/pdf/03tr002.pdf>.
- Ghosh, Anup K. 2000. *Code-Driven Attacks: The Evolving Internet Threat*. Dulles, VA: CIGITAL.
- . 2002. *Challenges for Anomaly Detection of Program Exploits*. Baltimore, MA: Johns Hopkins University.
- Johnson, Dale M. , Joshua D. Guttman, and John P. L. Woodward. *Self-Analysis for Survival, in 1997 Information Survivability Workshop - ISW'97*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890 1997 [cited January 16, 2004. Available from [http://www.cert.org/research/isw/isw97/all\\_the\\_papers/no14.html](http://www.cert.org/research/isw/isw97/all_the_papers/no14.html).
- Lipson, Howard F. *Survivability – A new security paradigm for protecting highly distributed mission-critical system* 2000 [cited 17.11.2003. Available from <http://www.cert.org/archive/pdf/surviv-paradigm.pdf>.
- . *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. CMU/SEI 2002 [cited 29 January 2004. Available from <http://www.cert.org/archive/pdf/02sr009.pdf>.
- Lipson, Howard F., and David A. Fisher. 1999. *Survivability — A New Technical and Business Perspective on Security*. Paper read at New Security Paradigm Workshop, September 22-24, 1999, at Caledon Hills, Ont. Canada.
- Rudolph, Jenny W., and Nelson P. Repenning. 2004. *Disaster Dynamics Model Documentation* 2002a [cited January 14 2004]. Available from Home page: [16](http://mitsloan.mit.edu/omg/people/index.php--> People-->Faculty Nelson Repenning-->[3] Rudolph, J. and N. Repenning (2002). Disaster Dynamics: Understanding the Role of Stress and Interruptions in Organizational Collapse, Administrative Science Quarterly, 47: 1-30. -->Link to model.</a></p></div><div data-bbox=)

- . 2002b. Disaster Dynamics: Understanding the Role of Quantity in Organizational Collapse. *Administrative Science Quarterly* 47:1-30.
- Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc.
- Schultz, E. Eugene. 2002. A Framework for Understanding and Predicting Insider Attacks. *Computers and Security* 21 (6):526-31.
- Shrobe, Howard. 2002. Computational Vulnerability Analysis for Information Survivability. *AI Magazine* 23 (4):81-91.
- Sterman, John D. 2000. *Business Dynamics : Systems Thinking and Modeling for a Complex World*. Boston: Irwin/McGraw-Hill.