Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

AND YOU THOUGHT THE KILLER ROBOT WAS BAD

Richard Epstein, *West Chester University of Pennsylvania*, Member IEEE, ACM

Abstract – This paper describes a project that the author has begun and which he would like to share with the Information Assurance education community. The idea is to create a detailed fictitious scenario that is intended to educate students about the intersection between information assurance and software engineering. The scenario covers a variety of topics, including basic security concerns in software development, how security needs to be integrated into software processes, and work culture issues that can have a major impact upon the security of a product that an organization produces. Professional responsibilities and ethics are also important foci of the scenario.

Index terms – Software processes, building secure software, ethics, professional responsibilities, scenarios

1 – THE ORIGINAL KILLER ROBOT SCENARIO

In 1990 the author wrote a software engineering / computer ethics scenario called "The Case of the Killer Robot". This scenario was intended as a device to introduce ethical and professional issues into an undergraduate course in software engineering. After presenting his ideas to the SEI Software Engineering Education Conference in 1994 [1] and the ACM SIGCSE Symposium in 1995 [2], the author expanded the original scenario into a book [3]. In recent years, the author has been almost obsessed with the idea of creating a new software engineering scenario that involves a killer robot. The main question in his mind is "How have things changed since 1996 when the original killer robot book was completed?"

Obviously, things have changed dramatically during the last twelve years. The author has decided to scrap the original scenario and to write a completely new scenario that focuses considerable attention on the issue of security in software development. The fundamental goal of the new scenario is to explore how security must become a fundamental focus of the software development process. Let us conclude this first section with a brief description of the original Killer Robot scenario. Then, we will move on to how the new scenario radically alters the focus of the original scenario that was completed a dozen years ago.

The intention of the original Killer Robot (KR) scenario was to explore issues in software engineering, corporate cultures, and professional ethics. The scenario took the form of twenty-nine short stories. Most of these took the form of newspaper articles and media interviews. All of the newspaper stories were drawn from the fictitious newspaper: The Silicon Valley Sentinel-Observer. One of the first stories in the scenario presents a headline that informs the reader that a programmer has been charged with manslaughter due to the death of a robot operator. The programmer (Randy Samuels) had written the flawed code that was responsible for the robot's homicidal behavior. Each story had an accompanying technical discussion and list of references in an Appendix. The technical discussion for this particular story made it clear that the manslaughter charge was without legal precedent and was being used as a device to start a (hopefully, animated) discussion about professional practices and responsibilities in software development.

The author had a definite purpose in mind when he focused on the developer who wrote the flawed code right from the beginning of the scenario. The idea was to build wider and wider circles of corporate responsibility (and culpability) around that lone programmer. The ever-expanding circles of corporate responsibility showed that Randy Samuels did not work in isolation. He worked in a larger corporate environment. The ethical responsibility for the bad code was shared by his teammates, by his managers, and especially by high-level managers who were putting pressure on the project team to get the robot out to market by a certain date.

The scenario raised many important issues in software engineering, including issues relating to software process improvement, work culture, teamwork, programmer psychology and professional responsibilities and ethics. What factors contributed to the tragic death of the robot operator?

Only one chapter in the KR scenario is devoted to security per se. It is almost as if the author decided he needed to include security issues in the scenario (since this was a book about computer ethics as well as software engineering), but the security issues that were exposed in this one chapter had very little to do with the tragic death of the robot operator. The security-oriented chapter exposed the fact that there were poor security practices in

place at Silicon Techtronics, the company that created the CX30 Robot (the Killer Robot), but these poor practices had no direct relationship to the tragic death of the robot operator. Those poor security practices allowed Miasma, a black hat hacker, to get confidential documents from Silicon Techtronics, documents which revealed an in-house controversy relating to software process improvement at Silicon Techtronics. Miasma placed these documents on the Web in order to embarrass Silicon Techtronics. This hacking incident, revealed by Pam Pulitzer, the Silicon Valley Sentinel-Observer reporter who was covering the Killer Robot case, had no direct bearing on the behavior of the CX30 Robot that caused the death of the robot's operator.

Also, there is no indication in the original KR scenario that the robot was connected to the Internet in any way. Thus, security did not play a major role in the original KR scenario.

2- A NEW SCENARIO

The author has been fascinated with the question of how things would change were the KR scenario to be rewritten today, in 2008, as opposed to way back in ancient times (1996). While 1996 was almost ten years after the Morris Worm wake-up call [4], it was still three years before the tremendous explosion in interest in computer security that arose due to historical events such as the release of the Melissa Virus [5] and of the Code Red Worm [6]. Things have changed so dramatically since 1996 that the author has decided that the original scenario had to be abandoned. An entirely new scenario had to be written that makes security in software development its major focus. This section will attempt to give an overview of the new scenario.

The new scenario focuses on the Nurse Ratchet robot, a robot that cares for elderly patients in nursing homes and assisted living facilities. As you might have guessed, the Nurse Ratchet robot gets attacked by malicious parties, causing the death of several patients. The chapters in the Nurse Ratchet robot scenario are organized into five sections that focus on the following issues:

1. Introducing the nature of the Nurse Ratchet robots and security concerns about these robots that were raised by security experts.
2. A discussion of attacks against the Nurse Ratchet robots. This section introduces many concepts from Information Assurance, including malicious software, authentication, social engineering, distributed denial of service attacks and so on. These attacks lead to the deaths of three patients.
3. A discussion of the software engineering practices at the company that created the Nurse Ratchet robot (ElderCare Robotics). This section explores different software processes as well as security goals and principles.
4. Work culture issues at ElderCare Robotics and their possible relevance to understanding the tragedies caused by the Nurse Ratchet robots.
5. A concluding section that brings out additional issues in software engineering (e.g., security testing) as well as new technical issues in Information Assurance (e.g., protection technologies such as intrusion prevention systems and additional information on exploits, social engineering, and the attacks that caused the deaths of the three patients).

As of this writing the author has over 120 pages written for this new scenario and he hopes to finish the scenario during the summer of 2008 (if not sooner). He is interested in sharing this scenario with the Information Assurance education community. Part of his intention in presenting this paper at the Colloquium is to get feedback from colleagues relating to how we might share this scenario with our students in the best possible way.

How did the author settle upon the idea of a robotic nurse as the focus of this new software engineering / information assurance scenario? Several years ago the author heard a report on the radio about how the Japanese were focusing on robot technology with the hope that in the near future robots would be able to care for Japan's aging population. Because Japan has a low birth rate, there will be a shortage of human nurses available to care for the elderly in Japan in the not too distant future. The (fictitious) Nurse Ratchet robots were produced by ElderCare Robotics in order to care for patients in nursing homes in the United States, Japan and other countries.

The scenario begins with news stories about the release of the Nurse Ratchet robots. The Nurse Ratchet robots are very much integrated into the world of the Internet, using wireless communications and other forms of communication that certainly raise security concerns.

As the Nurse Ratchet robots are being released to nursing homes and assisted-living facilities, a group of security experts are raising serious concerns about the security of the Nurse Ratchet robot system. This brings Nathaniel Chutney, a Silicon Valley Sentinel-Observer reporter, on to the case. Nathaniel Chutney is the author of most of the Nurse Ratchet news stories in this scenario. He is the information technology reporter at the Sentinel-Observer and he is very much interested in issues of security and hacker culture.

Step by step, the Nurse Ratchet scenario unfolds, with security issues becoming a central concern early on. An early incident involves a Nurse Ratchet Robot insulting a particular patient with harsh and rude language. Then, it

is revealed that this patient's ex-son-in-law was a software developer at ElderCare Robotics. This leads to a discussion of malware created by insiders and what might motivate an insider to create malicious software. A few days later the same patient's medical records are posted on a Web site in Russia. This raises issues of confidentiality and privacy (and HIPPA regulations, specifically), as well as hacker culture issues. These issues include the rise of the importance of hackers in eastern Europe and Russia.

Things get worse. Eventually, three patients are killed when several Nurse Ratchet robots give patients incorrect medications. It is then found that the patient prescription database at a centralized location at ElderCare Robotics was hacked into, with patient prescription data maliciously altered by the attackers. Nathaniel Chutney must explore all of the security issues in this scenario in great depth, and there are many, many security issues that arise.

In the author's opinion, this is an opportunity to introduce students to many issues in information assurance and software engineering in a way that is entertaining and hopefully provocative. How these issues are brought forth in the scenario is discussed in the following sections.

3 – SETTING THINGS UP

The Nurse Ratchet scenario begins with a series of articles by Silicon Sentinel-Observer reporter Pamela Pulitzer. She introduces the readers to the Nurse Ratchet robots and to ElderCare Robotics, the company that produced the Nurse Ratchet robots.

Dozens of Nurse Ratchet robots are being deployed at nursing homes and assisted living facilities in the United States, Japan, and several other countries. Pamela Pulitzer's focus is on a nursing home and assisted living facility in Silicon Valley that is using Nurse Ratchet robots to care for patients. That facility is the Silicon Valley Life Assist Facility or SV-LAF for short.

The Nurse Ratchet robot is introduced to the public at a major media event sponsored by ElderCare Robotics and SV-LAF. George Critchton, the ElderCare Robotics CEO gets real testy when a reporter from CNN asks him whether the Nurse Ratchet robots might pose some danger to the patients in terms of security. George Critchton considers the reporter's question an outrage.

The security issue soon takes center stage in the media. Nathaniel Chutney, the IT reporter for the Sentinel-Observer, takes charge of the newspaper's reporting on the Nurse Ratchet robots. It turns out that one of Chutney's hacker friends, who is known on-line as "Vanilla Fudge" (a mixture of black hat and white hat), has decided to challenge George Critchton's claim that the Nurse Ratchet robots are secure.

Vanilla Fudge gives the author the opportunity to introduce students to some issues that relate to hacker culture. In some ways, the Vanilla Fudge character was inspired by the folks at lOpht (like Drudge and Silicosis) from the turn of the century. Indeed, even as this paper is being written, a big lOpht reunion event is being planned in Boston. Like the folks at lOpht several years back, Vanilla Fudge is trying to hold the software vendors' feet to the fire, trying to force them to take security more seriously.

Vanilla Fudge announces that he and his colleagues (who work out of a place they call "The Barn") have found vulnerabilities in the Nurse Ratchet software. They will not expose these vulnerabilities out of fear of placing patients in harm's way. Nonetheless, they have told the ElderCare Robotics folks about the vulnerabilities and the ElderCare Robotics folks seem totally uninterested in what the folks from The Barn have communicated to them.

Things have certainly changed since the days when lOpht was important in the world of computer security. Now organized crime and the profit motive are increasingly important in the world of finding and sharing software vulnerabilities and exploits. The Nurse Ratchet scenario makes all of this clear as the scenario unfolds.

A few weeks after Vanilla Fudge went public with his concerns about vulnerabilities in the Nurse Ratchet robot software, Michelle Matley, Chief Technology Officer at ElderCare Robotics, announces patches for the vulnerabilities that Vanilla Fudge and the folks at the Barn had discovered. Michelle Matley indicates that she does not think that these vulnerabilities posed significant risks for patients. She explains that the patches were mainly issued to calm the storm that Vanilla Fudge's comments in the media had raised.

This is the point in the scenario that a world-leading expert in software engineering from the Software Engineering Institute at Carnegie Mellon University speaks out regarding the Nurse Ratchet robot. The world-famous software engineer is Kyle Watts. He is enraged by the story emerging out of ElderCare Robotics and he shares his anger over lunch with Nathaniel Chutney (who, like the author of this paper, is heavily into Indian food). Kyle Watts criticizes the penetrate and patch approach to putting security into software. He tells Nathaniel Chutney (and Chutney's readers) that security must be included in the software engineering process right from the start.

The final newspaper article in the introductory section of the scenario carries the headline "Web Site Sells Software

Vulnerabilities Discovered by Researchers". This article is intended to introduce students to the dramatic manner in which the hacker culture has evolved in recent years. The security researchers working out of the Barn who published their findings for free on the Web are being replaced by security researchers who are seeking money for their discoveries. They are selling the vulnerabilities they have found and the exploits they have created to the highest bidders. This article also highlights the role of organized crime in the world of hacking. It also suggests that cyberterrorism could be a major threat in the near future.

So, the basic goal of the newspaper stories in the first section of the Nurse Ratchet robot scenario is to introduce students to basic concepts and terms in information assurance (concepts like vulnerabilities, exploits and attacks; terms like confidentiality, integrity and accessibility). This section also presents indications that issues in software engineering will play a major role in the unfolding scenario.

4 – ATTACKS ON NURSE RATCHET AND THEIR TRAGIC CONSEQUENCES

The Nurse Ratchet scenario now moves on to a series of attacks against the Nurse Ratchet robot system. These attacks raise new issues relating to the importance of designing and implementing secure systems. In addition, they give the students more information about the "bad guys" who might be motivated to attack such systems.

The first attack occurs at the Silicon Valley's Life Assist Facility. Where else? Pamela Pulitzer is the author of a news story entitled "Nurse Ratchet Robot Insults Patient at Life Assist Facility". Pamela Pulitzer isn't into the technology (unlike her colleague, Nathaniel Chutney). She just reports on a strange incident at SV-LAF. Sarah Hanfield, a patient at SV-LAF is verbally abused in the most horrific manner by the Nurse Ratchet robot that entered her room.

George Critchton, the CEO of ElderCare Robotics cannot imagine that anything has gone wrong with his Nurse Ratchet robot. He tells reporters that he believes that Sarah Hanfield had a psychotic episode. She must be suffering from dementia. She must have been hallucinating. The Nurse Ratchet robot could not possibly behave in such a manner.

George Critchton was wrong, of course. A few days after Sarah Hanfield gets abused by the Nurse Ratchet robot, Sarah's confidential medical records are posted on a Russian Web site. The Web site explicitly thanks Nurse Ratchet for this interesting information. This brings Nathaniel Chutney back into covering the Nurse Ratchet robot story. The Nurse Ratchet robots become Chutney's full-time preoccupation. What is going on here? How did those hackers get access to Sarah Hanfield's medical records? What caused this particular Nurse Ratchet robot to behave in such a rude manner towards Sarah Hanfield?

It turns out that Nathaniel Chutney always invites his readers to contribute their view of things on his blog. A blogger, who says he works at ElderCare Robotics, claims that Sarah Hanfield's ex-son-in-law, who hated Sarah Hanfield and his ex-wife with a great passion, was a software developer for the Nurse Ratchet robot. The blogger says that his colleague blamed Sarah Hanfield for causing his ex-wife to leave him. This allows Nathaniel Chutney to explore the threats that insiders might pose to the security of software systems. Nathaniel Chutney would not have pursued the insider dimension of the unfolding scenario, except that the New York Times had just published a major story about the specific developer who was Hanfield ex-son-in-law, Steven Hatterman. The New York Times story reveals that malicious software was found to be responsible for the Sarah Hanfield scenario. Hatterman denies that he was responsible for inserting the malicious code into the software.

After the Sarah Hanfield incident, the attacks against the Nurse Ratchet robots intensify. The next headline in the scenario reads "Patient Dies After Robot Gives Him the Wrong Medication at Life Assist Facility". As this story comes to the attention of the public, the ElderCare Robotics folks deny that any security problem in their system was behind the death of this patient. This article in the scenario focuses much attention on the issue of authentication. The dead patient's prescription data had been modified by someone who was not authorized to have access to the patient prescription database. Security experts start to speculate that there is something seriously wrong with the authentication process for doctors who want to enter new data or modify data for the patient prescription database.

The following article in the scenario reveals that an intruder definitely got unauthorized access to the patient prescription database. This leads to a detailed discussion of authentication, starting with a discussion of passwords (good and bad), as well as the use of two-factor authentication. Vanilla Fudge (VF) is once more interviewed by Nathaniel Chutney and VF launches into a description of alternative authentication technologies that use biometrics. Another expert that Nathaniel Chutney interviews for this article is Kevin Rudnick, a leading expert in the area of social engineering. He describes how social engineering might have been used by the attacker to gain unauthorized access to the patient prescription database. Rudnick explains how security policies, employee training, and system design could help to prevent this type of attack.

The attacks against the Nurse Ratchet robots continue. Two more patients die due to intrusions into the patient prescription database. ElderCare Robotics is still pretty much in a state of denial. The deaths of the two additional patients bring up the issue of the security of our computer infrastructure. Nathaniel Chutney writes an article about information warfare and cyberterrorism. He interviews a leading expert on cyberterrorism and information warfare, Richard Cottman. This article introduces the student readers to these important topics and the types of threats that are posed by nation states and terrorists.

It turns out that the threat to the computer infrastructure may not just come from nation states and terrorists, at least as we usually think of them. Nathaniel Chutney reveals the existence of blogs where people who are strongly opposed to robotic nurses had been speaking out strongly against the deployment of the Nurse Ratchet robots almost from day one. One of these bloggers goes by the angry name ScruU. He is quoted as saying, "Do we want robots to replace human beings in the nursing profession? Soon robots will be replacing humans in other professions, like writing computer code."

The next article in this second section of the scenario goes on to reveal that the Nurse Ratchet robots have become key targets for hackers around the world. The Nurse Ratchet robot system is constantly being probed and is constantly under attack. It is not clear whether the attackers are folks like ScruU, who want to destroy this emerging technology, or whether they are just going after the Nurse Ratchet robots for bragging rights or other malicious ends.

The next article has the headline "New Attack on the Web Paralyzes Nurse Ratchet Robots". This article discusses botnets and zombie computers and distributed denial of services attacks. The industry expert who gives Nathaniel Chutney the information he needs on this topic is Vince Verno. Verno also informs the readers how botnets can be used to spread spam and phishing attacks.

The final article in this part of the Nurse Ratchet scenario announces that ElderCare Robotics has decided to recall the Nurse Ratchet robots from the nursing homes and assisted living facilities. This article explores the issue of legal liability for creating insecure computer systems. This article discusses UCITA and other efforts that have been made to clarify liability issues as they relate to insecure software.

5 – SOFTWARE ENGINEERING AND SECURITY

The next section of the scenario focuses on software engineering and the issue of building secure systems. The first newspaper article in this section has the title "Software Developer Claims Security was not a Major Issue in Developing the Nurse Ratchet Robots". In this article a former ElderCare Robotics software developer, who wants to be known by the alias Harry Wilson, goes into great detail about how the management at ElderCare Robotics shot down every effort by the software developers to incorporate security concerns into the Nurse Ratchet project.

Harry Wilson describes a very unhealthy work environment at ElderCare Robotics, a work environment in which project managers did not seem to be familiar with software processes per se, and certainly had no background in producing secure software. The project plan the managers laid out for the software developers (in the form of a huge Gantt chart) was totally unrealistic. The developers were shocked at the project plan the managers put forth, but their efforts to get management to modify the project plan failed. Harry Wilson reveals other problems. For example, the project managers did not have good strategies for coordinating the many teams that were working in parallel on the Nurse Ratchet software.

Nathaniel Chutney's next article consists of an in-depth interview with the great software engineering celebrity Kyle Watts from SEI who was mentioned earlier. Watts lays out in detail how security must be integrated into the software development process. This and the following article were clearly inspired by the excellent book by Viega and McGraw [7]. How Viega and McGraw's suggestions (and the suggestions of other security experts) were applied to a specific software development project is described in an article by Apvrille and Purzandi [8]. Watts explains to Chutney (and Chutney's readers) how security can be integrated into the software development process from the very beginning. He introduces the readers to the basic goals of producing secure software: confidentiality, integrity, and accessibility. All three of these goals were severely violated in the Nurse Ratchet system. Watts introduces the readers to the security practices that are relevant during the requirements analysis, design, implementation and testing phases of the software life cycle. He stresses the importance of developing a security policy and doing risk assessment early in the project. He stresses that a well-trained security engineer must play an important role on such a project.

The security expert Vince Verno, who was also mentioned earlier, is the focus of Nathaniel Chutney's next article. Verno discusses basic security principles and goals (as listed in the report from a Department of Homeland Security task force on good processes for building secure software [9]). Verno shows how many of these principles and goals were violated by the Nurse

Ratchet robot system. Verno discusses the following principles and goals in this Sentinel-Observer article:

- Prevent vulnerabilities that can lead to exploits.
- Implement auditing and monitoring.
- Ensure confidentiality, integrity, and accessibility.
- Provide multi-level security.
- Provide trustworthy authentication processes.
- Follow the principle of least privilege.
- Fail securely.
- Be reluctant to trust.

He discusses each of these principles and goals in some detail, revealing how the Nurse Ratchet robot system violated nearly every one of these principles and goals (based upon what was publicly known about the Nurse Ratchet robot software when Verno was interviewed).

Nathaniel Chutney's next article bears the title "Security Objectives and Software Project Goals Often at Odds". In this article, Chutney is interviewing another insider who worked on the Nurse Ratchet robot software. Her name is Francine McElroy. She comes forward to contest what her colleague, known by the alias Harry Wilson, had told the press. Francine McElroy's position is that many of the security concerns were pushed aside because they were in conflict with important software project goals, such as user-friendliness, simplicity, efficiency, maintainability, and getting the project out the door in a timely fashion.

Francine McElroy goes through her list of software project goals and explains how many of them might be in conflict with the security goals discussed by Vince Verno and her colleague (Harry Wilson). However, as she works her way through the list, she has a change of heart. She begins to realize the enormity of the tragedy that some of the Nurse Ratchet robots have caused. The interview ends with Francine McElroy telling Nathaniel Chutney (and his readers): "I deeply regret any role that I might have played in producing software that might have caused harm to my brothers and sisters. On the other hand, we are just at the beginning of the development of this new technology. Perhaps this tragedy will lead to the creation of safer and more effective software systems in the future. Perhaps the Nurse Ratchet robot was the wake-up call that we all needed."

The next article has the title "Several Developers Pushed for a More Mature Software Process at ElderCare Robotics". In this article, a software developer who worked on the Nurse Ratchet robot (who goes by the alias Fred Materno) explains how he and other developers on the project were pushing ElderCare Robotics management to develop a more mature software development process. In particular, they were pushing for the use of the SEI's Capability Maturity Model Integrated (CMMI).

This article explores the nature of process maturity and of the CMMI in particular. It discusses the five levels of maturity in the CMMI and the process areas at each level of maturity. In addition, Fred Materno makes it clear that a highly mature organization is less likely to produce unreliable and insecure software. He stresses the importance of defect tracking and quality assurance in the CMMI.

The next article introduces agile processes and eXtreme Programming (XP). In this article Nathaniel Chutney interviews a group of developers at ElderCare Robotics who wish to be called "the Agile Crew". The individual members of this group go by the aliases Agile Crew I, Agile Crew II, and Agile Crew III. The author draws upon a variety of resources for this discussion of agile processes and XP, including a book by Ken Schwaber [10], and articles by Williams et al. [11], Grenning [12] and Schatz and Ibrahim Abdelshafi [13].

These developers introduce the readers to the basic practices of eXtreme Programming including project planning (release planning), the use of user stories, pair programming, daily stand-up meetings, iterations, continuous integration, unit testing, acceptance testing, and customer on site at all times. These developers used XP to develop several components for the Nurse Ratchet robot system. They explain how they got management to accept XP for the development of these components. There is not much focus on security per se. Instead, the Agile Crew is focused on the fact that no defects were found in their code. In other words, the code they produced was secure because XP involves good quality assurance measures, like comprehensive testing processes and pair programming.

The Silicon Valley University decides to hold a panel discussion on what has been called "the war," the conflict between the traditional waterfall life cycle folks and the agile process folks. This panel discussion is the topic of the next article in the scenario. This article quotes extensively from the panel discussion. An important issue is whether eXtreme Programming can produce secure software (an important issue for the panelists in light of the Nurse Ratchet tragedies).

The panelists sit at two separate tables on a stage at the University. At one table you have the waterfall process folks (big fans of CMMI for the most part). At the other table you have the agile process folks. The panel discussion goes into great depth into the conflicting views on the two sides, but one of the panelists on the waterfall side of the table, praises agile processes and announces the idea that perhaps a maturity model for agile processes should be produced.

The last article in this series on software processes bears the title "Former ElderCare Robotics Developer Worked on Making eXtreme Programming More Secure". This article draws upon ideas in the author's Colloquium presentation last year about this very issue [14]. Nathaniel Chutney interviews Aaron Maxwell who goes on to reveal how he has developed a modified version of eXtreme Programming that attempts to focus on producing secure software. Maxwell presents the specific ideas from his version of XP, called XP-Secure. These ideas include having a security engineer on the development team, making sure that security testing is part of the XP testing processes, developing security stories that eventually lead to a security policy. This article concludes this section of the Nurse Ratchet scenario.

6 – WORK CULTURE ISSUES AND SECURITY

The next section of the Nurse Ratchet scenario focuses on work culture issues and their impact upon security. This section draws heavily upon McLendon and Weinberg's concept of a congruent work culture [15] and the author's work on demons in the IT workplace [16].

The first article in this section has Nathaniel Chutney interviewing a psychologist whose specialties are (1) the software development work culture and (2) programmer psychology. The psychologist's name is Sigmund Freudberg. Freudberg arranged (after the Nurse Ratchet robot disaster) to hold a workshop and discussion session with a group of Nurse Ratchet robot software developers. He shares what he learned from the developers with Chutney and his readers. The picture that emerges is not pretty. Dr. Freudberg makes it clear that the work culture at ElderCare Robotics was what McLendon and Weinberg call a blaming culture. In the above cited article, McLendon and Weinberg say: "Blaming is the dark secret underlying the failure of many [software] projects." [15, p. 36]

Chutney's interactions with Dr. Freudberg (who likes people to call him "Siggy") continue in a second article entitled "Demons Were Rampant in ElderCare Robotics Workplace". In this article Freudberg reveals how his interaction with ElderCare Robotics software developers revealed clearly that demons infected the ElderCare Robotics work culture and that this had very negative impacts upon the quality of the software that was produced. These demons included arrogance, sexism, inability to listen to others, disrespect for the other, and so forth. Freudberg makes it clear that the incongruent (and blaming) work culture and the workplace demons had a big impact upon the quality of the system that was produced, with the result that the Nurse Ratchet robots had very poor security properties.

An important message in this section of the Nurse Ratchet scenario is "why software fails," a topic that is explored in a paper by Robert Charette [17]. Another factor that is explored is Steven McConnell's concept of a "problem programmer," a programmer who is unwilling to accept feedback from his or her colleagues, a programmer who prefers to work alone [18]. This kind of personality can have serious implications in terms of the quality of the software that is produced by a software development team.

This section of the Nurse Ratchet scenario ends with a discussion of the Software Engineering Code of Ethics [19]. Although security is not a central focus of this code, software reliability and quality are.

7 – HOW THE SCENARIO WILL END

The author has yet to write the closing section of the scenario, although many of the headlines are tentatively in place. The closing section of the scenario will return to issues in software engineering and security. Issues to be covered in this section include:

- Security testing
- More about security vulnerabilities (like backdoors and Trojan horses)
- More about authentication and man-in-the-middle attacks
- More about social engineering
- An introduction to intrusion detection and intrusion prevention systems, including a discussion of computer immunology
- More about cyberterrorism
- The prosecution of one or more individuals in the attacks against the Nurse Ratchet robots, including the prescription database modification attack and the distributed denial of service attacks.

An important issue that the author would like to discuss with his colleagues at the Colloquium is how this scenario could best be shared with students in Information Assurance. The author is wondering whether creating a Nurse Ratchet web site would be a better way to distribute this scenario than having it published as a book. Furthermore, the author would like to discuss the kinds of learning experiences, including homework assignments that would help students to take advantage of this scenario.

8 – CONCLUSIONS

The author finds it fascinating that so much has changed since the original Killer Robot scenario was completed twelve years ago (in 1996). So much has changed in the world of software engineering, especially when we consider the security issues involved. The author hopes that the new scenario, centering upon the Nurse Ratchet

robot system and its problems, will provide a stimulating and entertaining introduction to important issues in Information Assurance for many students. A central focus of the Nurse Ratchet scenario is software engineering and how software processes and work culture issues can have a big impact upon the security of a software product. The author is looking forward to feedback from his Colleagues at the Colloquium relating to how this scenario can best be shared with students in Information Assurance.

9 – REFERENCES CITED

1. Epstein, Richard G., "The Use of Computer Ethics Scenarios in Software Engineering Education", SEI Software Engineering Education Conference, San Antonio, January 1994.

2. Epstein, Richard G., "The Case of the Killer Robot – Progress Report", ACM SIGCSE Symposium, Nashville, March 1995.

3. Epstein, Richard G., The Case of the Killer Robot, John Wiley and Sons, New York, 1997, 242pp.

4. Eugene H. Spafford, "Crisis and Aftermath," Communications of the ACM, June 1989, pp. 678-687.

5. Garber, Lee, "Melissa Virus Creates a New Type of Threat", IEEE Computer, June 1999, pp. 16-7.

6. Berghel, Hal, "The Code Red Worm", Communications of the ACM, December 2001, pp. 15-19.

7. Viega, John and McGraw, Gary, Building Secure Software, Addison-Wesley, Boston, 2002, 493. pp.

8. Davis, Noopur, Humphrey, Watts, Redwine, Samuel T., Zibulski, Gerlinde, and McGraw, Gary, "Processes for Producing Secure Software", IEEE Security and Privacy, May/June 2004, pp. 18-25.

9. Apvrille, Axelle and Pourzandi, Makan, "Secure Software Development by Example," IEEE Security and Privacy, May/June 2004, pp. 18-25.

10. Schwaber, Ken, Agile Project Management with Scrum, Microsoft Press, Redmond, WA, 2004, 192 pp.

11. Williams, Laurie, Kessler, Robert R., Cunningham, Ward, and Jeffries, Ron, "Strengthening the Case for Pair Programming," IEEE Software, July/August 2000, pp. 19-25.

12. Grenning, James, "Launching Extreme Programming at a Process Intensive Company," IEEE Software, November / December 2001, pp. 27-33.

13. Schatz, Bob and Abdelshafi, Ibrahim, "Primavera Gets Agile: A Successful Transition to Agile Development", IEEE Software, May/June 2005, pp. 36-41.

14. Epstein, Richard G., "Can Software Engineers Be Agile and Secure?", CISSE, Boston, June 2007.

15. McLendon, Jean and Weinberg, Gerald M., "Beyond Blaming: Congruence in Large Systems Development", IEEE Software, July 1996, pp. 33-42.

16. Epstein, Richard G., "Demons in the IT Workplace", IEEE ISTAS, Worcester, MA, June 2004.

17. Charette, Robert N., "Why Software Fails", IEEE Spectrum, September 2005, pp. 42-49.

18. McConnell, Steve, "Problem Programmers", IEEE Software, March/April 1998, pp. 128-7.

19. Gotterbarn, Don, Miller, Keith, and Rogerson, Simon, "Software Engineering Code of Ethics", Communications of the ACM, November 1997, pp. 110-116.