NetS-X – Netzsicherheit lernen mit Spaß

Helmut Eirund, Richard Sethmann

Hochschule Bremen, ZIMT
Flughafenallee 10
D-28199 Bremen
Email: {eirund, sethmann}@informatik.hs-bremen.de

Zusammenfassung: Das Gebiet der Netzsicherheit ist ein schwer zu lehrendes und mühsam zu lernendes Fach in der Informatikausbildung. Dies hat verschiedene Gründe, z.B. erfordert es Fachkenntnis, die jenseits von bunten Bildern zu vermitteln ist und sich dabei mit geringer Halbwertszeit weiterentwickelt. Echte Bedrohungsszenarien müssen unter Laborbedingungen nachgestellt werden, und der Umgang mit den Sicherheitswerkzeugen ist sehr komplex. Auf der einen Seite muss das System konzeptionell verstanden werden und auf der anderen Seite sind viele Details in der Konfiguration von Firewalls, Netz-Komponenten und –Werkzeugen für klassische Prüfungssituationen in der Ausbildung anzuwenden. Mit NetS-X (Network Security Experience) stellen wir einen laufenden Prototyp einer e-learning Plattform vor, mit der ein weiter Bereich von Sicherheitsszenarien vermittelt werden kann. Dabei wird der Lernende in einem Spielsystem mit Situationen konfrontiert, die er in einer echten, auf Linux basierenden typischen IT-Infrastruktur eines Unternehmens beherrschen muss. Die sicherheitsrelevanten Aktivitäten des Lernenden, z.B. der Einsatz von Monitor-Werkzeugen oder die Konfiguration von Netz-Komponenten werden dabei nicht simuliert, sondern real durchgeführt und durch Prozesse des Spielsystems beobachtet und bewertet. Autorenwerkzeuge ermöglichen den Lehrenden und Spielern, selber neue Spielsituationen, Sicherheitsszenarien oder Wissenskomponenten in das System zu integrieren.

1 Einführung

1.1 Motivation

Die Sicherheit von Netzen gilt als eines der Hauptherausforderungen in der IT. Heute werden ungesicherte Netze innerhalb von Sekunden infiltriert und die Rechner angegriffen (Abb. 1).

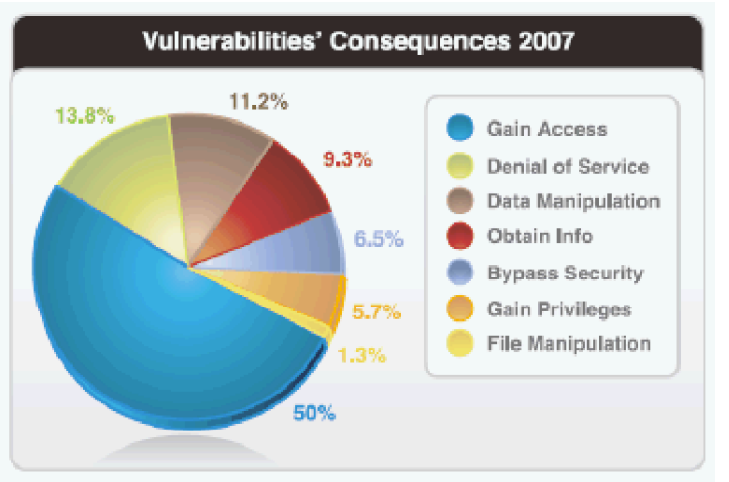

Abb. 1: Angriffsziele in Netzen [Quelle: IBM Internet Security Systems X-Force-2007 Trend]

Der Bedarf nach Sicherheitsexperten in der IT-Branche ist enorm hoch [Le Roux 2006] und kann bisher nicht durch die universitäre Ausbildung gedeckt werden.

Die Hauptgründe dieses Problems stellen sich wie folgt dar:

a. Der Stoff ist mühsam zu erlernen.
b. Die Halbwertzeit des Wissens ist kurz, und es muss permanent weitergelernt werden. Neue Angriffstechniken machen eine Weiterentwicklung des Curriculums permanent notwendig.
c. Ein klassisches Unternehmensnetz lassen sich nicht an jedem beliebigen Ort aufsetzen (z.B. Zuhause), sondern müssen vor Ort im Labor betrieben und erlernt werden.
d. Laborsituationen spiegeln oft nicht die reale IT-Struktur von Unternehmen wieder.
e. Selbsttest ist selten möglich und erzwingt die Anwesenheit von Experten.
f. Eine an den Wissensstand des Lernenden angelehnte Struktur ist in der Laborsituation schwer zu realisieren.
g. Handelsübliche Sicherheits-Werkzeuge (Hard- und Software) und Labor-Umgebungen in der universitären Ausbildung sind teuer.

NetS-X (Network Security Experience) ist ein Lernspiel mit einer integrierten Entwicklungsplattform. Es bietet eine geschützte Umgebung für das Erlernen von Hacker-Methoden und Schutzmechanismen in realen Netzen für Studierende der Informatik an und kommt damit den Forderungen nach verstärkten Ausbildungsanstrengungen [Krempl 2006, Dornseif 2005] nach. In NetS-X kann eine Gruppe von Studierenden mit elementaren Vorkenntnissen der Netztechnik von der Anfänger- bis zur Fortgeschrittenenebene Sicherheitstechniken Schritt für Schritt erlernen.

1.2 Die NetS-X Lern-Innovation für Netzsicherheit

Bevor wir im Folgenden die Elemente des Lernspiels genauer beschreiben, zeigen wir zunächst kurz, wie der Ansatz von NetS-X auf die in 1.1 genannten Probleme eingeht.

a. Der Lernende lernt in einer Gruppe situativ in einer Spielsituation. Frühere Studien mit Lernspielen haben gezeigt, dass die Lernenden bessere Ergebnisse zeigen, wenn sie in konkurrierenden, unterhaltsamen Situationen lernen [Astleitner 2000, Hamey 2003, Näckros 2001]. Alle Lernmaterialien werden innerhalb einer Spiel-Story entwickelt und unter einem einheitlichen GUI zur Verfügung gestellt. Die Spiel-Story deckt dabei sowohl Angriffs- wie auch Verteidigungs-Szenarien ab (vgl. [Freiling 2006, Dornseif 2004, Conti 2005, Ledin 2005]).
b. Durch Autorenschnittstellen auf allen Spielebenen werden erfahrene Lernende und Lehrende ermuntert, neues Wissen und Szenarien in das System einzubringen und für alle zugänglich zu machen.
c. Das Spiel ist über eine Browseroberfläche aufrufbar und spielbar. Über eine sichere VPN-Verbindung zur Spielnetzinfrastruktur können Übungseinheiten außerhalb der Laborzeiten durchgeführt werden.
d. Das Spielnetz stellt eine Referenz-IT-Struktur eines mittleren Betriebes dar (siehe z.B. [Romney 2001, Yang 2004]), mit den üblichen Hardware-Komponenten und Diensten.
e. Nach allen Teilszenarien werden den Lernenden wiederholende Selbsttests angeboten, die die Konzepte des eben Erlernten vertiefen.
f. Das Spiel ist als ein wie aus Computerspielen bekanntes Adventure-Spiel angelegt, in dem der Lernende aufeinander aufbauende Teilaufgaben (Szenarien) in steigender Komplexität löst. Dabei hat er verschiedene, seinen Fähigkeiten und Bedürfnissen entsprechende, Handlungsstränge zur Auswahl.
g. Alle verwendeten Software-Werkzeuge sind frei zugänglich (Open Source) und werden in dem Spiel tatsächlich (unter Linux) eingesetzt (eine Übersicht findet sich in [Sethmann et al. 2007]) und nicht – wie in anderen „Häckerspielen“ (z.B. [Cone 2007]) – nur simuliert. Für die Lernenden in NetS-X gilt: „shooting with real guns“.

2 Das Spielkonzept

Spielen bedeutet für die Spielenden Spaß, Befriedigung von Neugier, Ausprobieren neuer Mechanismen, aber auch immer soziale Interaktion, insbesondere durch den konkurrierenden Vergleich mit anderen Spielern und Zuschauern [Ghozland 2000, Malone 1980]. Das Spielkonzept von NetS-X macht sich diese Motivationen zu Nutze.

Die Lernziele von NetS-X lehnen sich an die in [Irvine 2003, Yang 2006] formulierten Forderungen an. Die Spiel-Story gliedert sich in eine Folge von Szenarien, in denen Lernende aktiv handeln müssen. Die Szenarien folgen den Empfehlungen für das Curriculum für Netzsicherheit aus [Bogolea 2004, Bratus 2007, ACM 2005].

2.1 Die Spiel-Story

Der Spieleinsteiger steuert einen Avatar, der einen neuen Angestellten (wahlweise eine Angestellte) in der IT-Abteilung einer fiktiven Firma darstellt, durch eine bunte 2D-Bürowelt (Abb. 2). Durch Frage-Antwort-Interaktionen mit autonom agierenden Non-Player-Characters (NPC) erfährt der Spieler Hintergründe über Bedrohungssituationen, Aufgaben und den Einsatz von Software-Werkzeugen. Weitere Informationen und Hin-

weise auf Lösungsmöglichkeiten findet der Spieler über einen virtuellen PDA (Personal digital Assistent) im NetS-X Wiki.

Abb. 2: 2D-Bürowelt Screenshot

Wenn der Spieler im Dialog mit den NPCs elementare Kenntnisse der für die Aufgabe notwendigen Werkzeuge und Methoden nachweisen kann (in Form von simplen Multiple-Choice-Tests), darf er in die „echte“ Linux-Welt einsteigen – für den Spieler harmonisch als Animation von einem virtuellen PC-Screen im Spiel auf den realen Linux-Desktop vollzogen – und dort die vorher genannten Werkzeuge und Methoden nutzen. Auch hier steht ihm das Wiki als Nachschlagewerk zur Verfügung. Nach dem erfolgreichen Absolvieren der Aufgabe gelangt der Spieler wieder automatisch in die 2D-Bürowelt.

Jede erfüllte Aufgabe erlaubt dem Spieler, mit diesen neuen Fähigkeiten (skills) neue, komplexere Aufgaben anzunehmen und zu lösen.

2.2 Spielelemente und Game Flow

Während des Spiels erhält der Spieler Zugriff auf die in Abb. 3 dargestellten Spielfunktionen – typischerweise auch in dieser Reihenfolge:

1. 2D-Adventure: Der Spieler bewegt sich im interaktiven Einzelspieler-Modus. Hier sammelt er Erfahrungen und Wissen über Sicherheitsmethoden und Techniken, die dann ein real-world-Szenario frei schalten.

2. Wiki: hier kann der Spieler tiefer gehende Informationen zum Szenario nachschlagen.
3. Real world scenario: in der Linux-Umgebung werden die Werkzeuge durch den Spieler angewandt.
4. Self assessment: in Multiple-Choice Tests wird das gelernte Wissen vertieft.
5. Authoring: Je nach Wissensstand ist der Spieler berechtigt, die vier Ebenen der Lernumgebung (2D-Story-Elemente, Wiki, Linux-Szenarios, Tests) zu erweitern.

Abb. 4: Gameflow in NetS-X

Mit dem in Adventure-Spielen zentralen "collect and advance" Game-Pattern wird das Belohnungssystem implementiert und der Gang durch die Story und damit durch den Lernstoff vorangetrieben. Einzelne Szenarien können sich dabei aus Teilaufgaben zusammensetzen, deren Erfolg einzeln bewertet wird. Beispiele werden in den folgenden Abschnitten aufgezeigt. Für den Abschluss von Szenarien und die das Gelernte zusammenfassenden Multiple-Choice Tests erhält der Spieler Siegpunkte. Alle registrierten Spieler sind mit ihren Profilen und aktuellen Siegpunkten sichtbar und dienen als Ansporn für Mitspieler.

2.3 Ein Game Play Beispiel

Im folgenden wird das Szenario *Web page defacement* beispielhaft vorgestellt.

Zwei Lernziele liegen diesem Szenario zugrunde:
1. Der Spieler lernt, ein wichtiges Sicherheitswerkzeug (hier: Ethereal/Wireshark) anzuwenden.
2. Das übergeordnete Lernziel ist, dem Spieler den Anwendungskontext dieses Werkzeugs zu vermitteln, und zwar sowohl als Verteidigung wie auch als Angriffsinstrument bei Hackerattacken.

Zunächst sammelt der Spieler mit Hilfe seines Avatars in der 2D-Bürowelt Informationen über das Sniffer tool Wireshark/Ethereal. Dies geschieht durch Andeutungen durch andere NPCs, in versteckten Hinweisen oder durch das Nachlesen von Detailinformationen im Wiki, das durch den virtuellen PDA zugänglich gemacht ist.

Erst wenn sich der Spieler mit dem Inhalt auseinander gesetzt hat und sicher fühlt, wird er durch einen für diese Szene bestimmten NPC (hier: der „Kollege“) mit einigen zufällig ausgewählten Fragen aus dem in der Datenbank hinterlegten Fragenpool zu Wireshark/Ethereal konfrontiert. Nach erfolgreicher Beantwortung der Fragen geht die Fähigkeit (skill) „Wireshark/Ethereal“ auf den Avatar über und das Szenario in dem realen Netz wird für den Spieler frei geschaltet.

Im Szenario hat der Spieler die Aufgabe, die Homepage eines illegalen Users zu verändern. Die Datei der Webseite ist im Web Server des realen Netzes gespeichert und nur mit den Schreibrechten dieses Users zugänglich. Die Aufgaben des Spielers bestehen nun darin, das Passwort des fiktionalen Users aus dem Netzverkehr herauszulesen, die Webseite im Dateiverzeichnis des realen Rechners zu finden und unter dem Account des fiktionalen Users die Seite zu verändern.

Nachdem der Spieler das Szenario über die Browser-Oberfläche gestartet hat, wird ihm ein Wireshark/Ethereal-dump über den relevanten Netz-Datenverkehr zugänglich gemacht (in diesem Einstiegs-Szenario wird dem Spieler der Start von Wireshark noch durch das Spielsystem abgenommen). Er interpretiert die Daten und sucht systematisch nach User Login und Passwort. Mit diesen Daten führt er einen Account-Wechsel durch und sucht die Datei der Webseite auf (um nachzulesen, wo z.B. die Dateien einer Web-Site auf dem Webserver abgelegt werden, steht dem Spieler auch hier über ein übliches Browser-Fenster das Wiki zur Verfügung). Nach der Veränderung der Datei mit einem einfachen Text-Editor meldet der Spieler sich vom Netz ab und startet damit den Evaluierungsprozess, der ihm ggf. seine Siegpunkte gutschreibt.

Jedes Szenario wird von jeweils einem Spieler gespielt, allerdings ist es möglich, dass mehrere Spieler gleichzeitig oder hintereinander das gleiche Szenario spielen und dabei die gleiche Netz-Infrastruktur nutzen, ohne sich (technisch) zu beeinflussen. Ohne an dieser Stelle in die Details der technischen Realisierung gehen zu wollen, sei hier festgehalten, dass für jeden Spieler beim Eintritt in die Linux-Welt und damit der Zugriffsmöglichkeiten auf das reale Netz ein Start-Prozess einen eigenen Account für diesen Spieler schafft, unter dem alle für das Szenario notwendigen Ressourcen angelegt werden (hier: Webserver, Wireshark dump file, Account des illegalen Users). Ein weiterer Prozess überwacht die Aktivitäten des Spielers mit den Lernzielen (hier: erfolgreicher Account-Wechsel, Dateiänderung) und führt nach Fertigstellung die Punktegutschrift durch. Ein dritter Prozess stellt nach dem Beenden des Szenarios den alten Zustand wieder her (hier: löschen der Accounts, Web-Server etc.).

Einige wenige Szenarien erfordern den ausschließlichen Zugriff des Spielers auf bestimmte Netz-Komponenten. Diese Szenarien sind in der Szenarien-DB als „one player at a time“ gekennzeichnet und werden beim Ausführen für alle anderen Spieler während dieser Zeit gesperrt.

Eine ausführliche Beschreibung der Spiel-Implementierung und Prozesskommunikation von NetS-X findet sich in [Boit et al. 2007] und [Boit et al. 2008].

2.4 Szenarioübersicht

Alle NetS-X Szenarien spiegeln verschiedene realistische Verteidigungs- aber auch Angriffssituationen wieder. Dabei steigert sich die Komplexität der Szenarien und Anforderungen von einfachen Linux- und Netz-Administrationsaufgaben bis zu spezifischen Themen und Werkzeugen. Das theoretisch angeeignete Wissen kann dabei unmittelbar in „hands-on"-Erfahrungen eingesetzt werden.

Alle Szenarien sind in die Game Story eingebunden und werden in entsprechenden Situationen spielbar. Einen kompakten Eindruck der Story des ersten Levels (von drei) gibt Abb. 4.

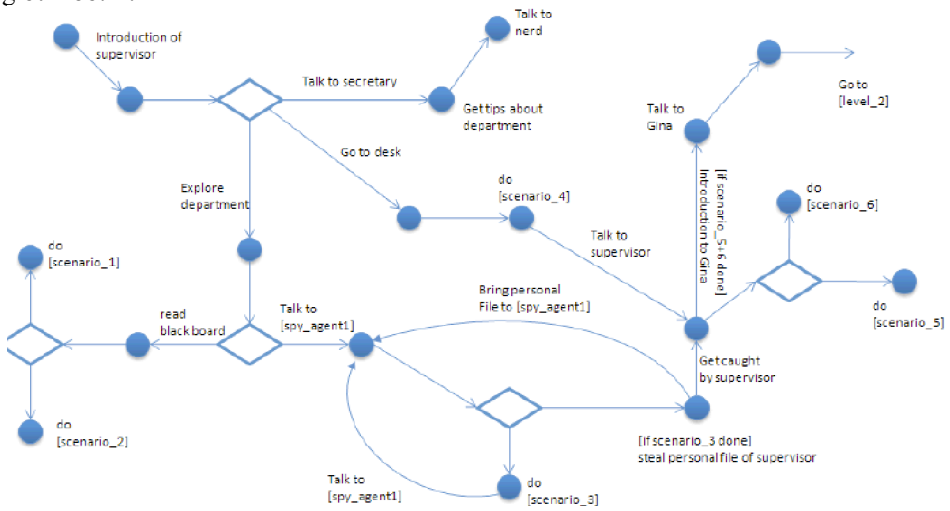

Abb. 4: Story Ablauf Level 1

Tabellen 1 bis 4 geben eine Übersicht über den aktuellen Stand sinnvoller Szenarien, die in die NetS-X Story eingebaut werden können, und zeigt damit den Umfang des Lerngebiets Netzsicherheit (auf eine detaillierte Beschreibung der zugrunde liegenden Techniken soll hier verzichtet werden).

Tab. 1: Angriffs-Szenarios

Password cracking techniques and tools (password crackers, Hydra, John The Ripper)
Network reconnaissance (port scanners, vulnerability scanners, etc.)
SSH attacks (man-in-the-middle, brute force)
Denial of service and service disruptions (DoS and DDoS)
Web server attacks and manipulation
DNS spoofing and manipulation
Web application security (SQL injection, session manipulation)

Tab. 2: Verteidigungs-Szenarios

Network monitoring tools (Cacti, NTOP, Nagios)
Intrusion detection systems (Snort, Prelude, creating and updating rule set)
Vulnerability management, patch-levels and updates, vulnerability scanners usage (Nessus)
Honeypots and Honeynets
Network authentication and authorisation mechanisms (Kerberos, Radius and LDAP)
Encryption and network security (IPSec, VPN technologies, Network layer security Wireless network security WPA/WPA2)
Securing web applications (SSL/TLS, input data sanitisation)

Tab. 3: Allgemeine Fähigkeiten

TCP/IP networks and services (DHCP, DNS)
Linux basic and advanced administration
Cisco routers configuration
Networking traffic analysis and sniffers usage
Cryptography
DNS server management

Tab. 4: Szenario Klassifikation

Scenario	Application/Description
Network monitoring tools	• Prevention • early problem detection • monitoring
Vulnerability management	• assess vulnerability • maintain patch levels in information systems
Encryption and network security	• assure the availability, confidentiality and integrity of in-transit information

3 Erweiterbarkeit und Autorenschnittstellen

Netzsicherheit ist ein außerordentlich dynamisches Lehrgebiet. Für ein Lernsystem mit Anspruch an Aktualität ist es daher unabdingbar, die Erweiterung des Systems zu ermöglichen – und um so einfacher dieser Prozess durchgeführt werden kann, um so größer ist die Chance, die Inhalte spannend und aktuell zu halten.

Die Möglichkeit der Partizipation der Spieler in der Um- und Neugestaltung (von Teilen) des Spiels bringt eine hohe Motivation mit sich und verteilt die Arbeitslast auf viele Teilnehmer. Zusätzlich werden bestimmte Beiträge durch Spielpunkte belohnt.

Jeder Nutzer von NetS-X ist mit einer Rolle registriert, die ihm bestimmte Änderungsoperationen im Spiel erlaubt. Möglich sind die folgenden Rollen (jeweils die vorgehende umfassend):
- Spieler
- Tutor
- Autor

Im Folgenden wird dargestellt, in welchen Bereichen die Nutzer auf welche Art das Spiel ändern können.

Spiel-Wiki:
Alle Spieler können die Wiki-Artikel zu Methoden, Werkzeugen und Szenarienbeschreibungen, die im Spiel mit dem virtuellen PDA zugänglich sind, ändern oder ergänzen. Ähnlich wie in öffentlichen Wikis muss dabei der Beitrag vor der Freigabe durch einen Tutor elektronisch bestätigt werden und unterliegen der GNU Lizenz [GNU project 2008].

Multiple-Choice Tests:
Die Sammlungen der Frage-Antwort-Tests (jeweils zu Themen zusammengefasst), auf die der Spieler in der 2D-Bürowelt trifft, können ebenfalls durch Spieler ergänzt werden und machen damit die Begegnungen mit NPCs im Spiel abwechslungsreicher. Nach Freigabe durch den Tutor erhält der Spieler hierfür Spielpunkte.

Szenario-Programmierung:
Neue LINUX-basierte Szenarien können über ein Web-Frontend editiert und neu hinzugefügt werden. Die Input-Masken leiten den Entwickler durch die Programmierung der drei notwendigen Prozesse, die ein Szenario beschreiben: Setup, Monitoring und Cleanup. Dabei kann der Entwickler auf ein Szenario Framework zurückgreifen, das ihm einige komplexe Shell-Programmierungen abnimmt und bestimmte Validierungen vornimmt.
Auf Grund der Komplexität der Aufgabe, dürfen nur Nutzer in der Autoren oder Tutoren Rolle Szenarien bearbeiten.

2D-Adventure Game Editor
Die 2D-Welt selber, zusammen mit den dort handelnden NPCs, kann von Autoren ebenfalls erweitert werden, um damit z.B. neue Bedrohungsszenarien in die Story einzubetten. Die 2D-Welt wird durch ein (in Flash erstelltes) Autorenwerkzeug manipuliert. Neue Objekte können importiert werden, NPCs platziert und Bewegungsabläufe festgelegt werden. Programmierkenntnisse sind hier nicht erforderlich. Das Verhalten der NPCs wird ebenfalls durch einen Editor festgelegt. In einer visuellen Umgebung wird jedem NPC ein endlicher Automat zugeordnet, in dem die Condition-Action Elemente, insbesondere die Frage-Antwort Aktionen definiert werden. Sowohl die 2D-Beschreibungen wie auch das Verhalten der NPCs wird in XML-Datenstrukturen in der NetS-X Datenbasis abgelegt und ist für alle Spieler zugänglich.

4 Zusammenfassung und Ausblick

Das NetS-X Spielsystem ist ein neuartiger Ansatz zur Vermittlung von Netzsicherheit. Durch die Kombination von theoretischem mit situativem Lernen in einer realen Netz-Infrastruktur, geleitet durch eine durchgehende Spiel-Story, wird Spielspaß und Nachhaltigkeit des Lernens gesichert.

Zurzeit sind Story-Elemente für 3 Levels mit jeweils ca. 6 Anknüpfungspunkten für Szenarien entwickelt und insgesamt 8 Szenarien implementiert. Durch Autorenschnittstellen wird die permanente Erweiterung des Spiels in allen Lernelementen ermöglicht. Die Verwendung von Open Source Software erlaubt eine freie Weitergabe und Entwicklung des Spiels, wodurch wir eine quantitative und qualitative Komplettierung des Spiels erwarten.

Spielbarkeit und Spannung werden in weiteren Versionen permanent verbessert, nicht nur an der Hochschule Bremen sondern in allen interessierten Einrichtungen. In nachfolgenden Projektgruppen werden die Effekte des Lernspiels auf die Ausbildung ebenfalls untersucht (Start WS 08/09). In einem fortgeschrittenen Stadium kann NetS-X eine

wertvolle Ergänzung und ggf. auch eine kostengünstige Alternative zur professionellen IT-Sicherheitsausbildung darstellen.

Das NetS-X Spiel ist aus einem einjährigen Master-Projekt im Studiengang Digitale Medien an der Hochschule Bremen (HSB) hervorgegangen. Im Oktober 2007 erweiterte eine Bachelor-Projektgruppe das Spiel um neue grafische und Story-Elemente. Aktuell wird das System getestet und dokumentiert. Die in Abschnitt 2 und 3 genannten Spielmechanismen sind als Tutorial-Videos unter [NetS-X Tutorial Videos (2008)] abrufbar.

Im Projekt EdiNet des EU-ERASMUS Programms (134608-LLP-1-2007-1-FI-ERASMUS-EVC) wird das System vier anderen europäischen Universitäten als Lernmodul für die Sicherheitsausbildung zur Verfügung gestellt und weiter ergänzt. In einem durch den DAAD geförderten Curricular-Austausch wird das System ebenfalls an einer Partner-Universität in Kalifornien eingesetzt.

Literatur

Astleitner, H. and Leutner, D. (2000), "Designing instructional technology from an emotional perspective", Journal of Research on Computing in Education, Vol. 32, pp 297-510.

Boit A. et al (2007) "NetS-X Report", Technischer Report Master-Projekt Digitale Medien, Hochschule Bremen.

Boit A. et al (2008) "NetS-X – Network Security Experience", Proc. European Conference on Information Warefare, Plymouth UK

Bogolea, B. and Wijekumar, K., (2004) "Information security curriculum development", Proceedings of the 1st annual conference on Information security curriculum development, Kennesaw, Georgia, ISBN:1-59593-048-5, pp 59-65.

Bratus, S. (2007) "Hacker Curriculum: How Hackers Learn Networking", IEEE DS Online Exclusive Content Education, Vol. 8, No. 10, Art. No. 0710-ox002

Conti, G. (2005) "Why Computer Scientists Should Attend Hacker Conferences", Communications of the ACM, Viewpoint, Vol. 48, No. 3, pp23-24.

ACM (2005) "ACM Computing Curricula 2005 - The Overview Report", ISBN: 1-59593-359-X, ACM Order Number: 999066, IEEE Computer Society Order Number: R0236

Cone, B. D., Irvine, C. E., Thompson, M. F., Nguyen, T. D. (2007) "A Video Game for Cyber Security Training and Awareness", Computers & Security 26, pp. 63-72.

Dornseif, M., Holz, T. and Mink, M. (2004) "An Offensive Approach to Teaching Information Security: The RWTH Summmer school on Applied IT Security 2004", Laboratory for Dependable Distributed Systems, RWTH Aachen University, pp1-13.

Dornseif, M., Gärtner, F., Mink, M., and Pimenidis, L. (2005) "Teaching Data Security at University Degree Level", Fourth World Conference on Information Security Education, Moscow (2005-05-19), RWTH Aachen, pp1-13.

Ghozland, D. (2007) "Designing for Motivation", Gamasutra website, Section 5 - Score System, Key system, and Multi-Choice, [online], http://www.gamasutra.com/view/feature/1419/designing_for_motivation.php

Hamey, L. (2003) "Teaching secure communication protocols using a game representation", Conferences in Research and Practice in Information Technology Series, Vol. 140, Proceedings of the fifth Australasian conference on Computing education, Vol. 20, ISSN:1445-1336 , ISBN 0-909925-98-4., pp187-196.

Irvine, C. E. and Thompson, M. (2003), "Where parallels intersect", Teaching Objectives of a Simulation Game for Computer Security, Center for the Information Systems Stu-

dies and Research, Navel Postgraduate School, Monterey, USA. Informing Science, InSITE, pp779-791.
Irvine, C. E. (2003), "Teaching constructive security", Security & Privacy Magazine, Vol. 1, No. 6, ISSN: 1540-7993 , pp59-61.
GNU project (2008) License information, [online], http://www.gnu.org/licenses/fdl.html
Jones, A., Kovacich, G. L., Luzwick, and Perry G. (2002). Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages, CRC Press. ISBN 0849311144. p171.
Krempl, S. (2006) "Universities need lessons in IT security", Coverstory, Infosecurity Today, DOI 10.1016/S1742-6847(06)70455-4, Vol. 3, No. 5, pp24-26.
Ledin, G. Jr. (2005) "Not Teaching Viruses and Worms Is Harmful", Communications of the ACM, ISSN 0001-0782, Vol. 48, No. 1, p144.
Näckros, K. (2001) "Game-based Instruction within IT Security Education", PhD Thesis at the Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, Sweden, [online], http://people.dsv.su.se/~kjellna/pages/publications-kjellna-en.html
NetS-X Tutorial Videos (2008), (z.Z. noch auf:) http://www.frankbruenjes.de/nets-x_videos/
Malone, T. W. (1980) "What makes things fun to learn? Heuristics for designing instructional computer games, Proceedings of the 3rd ACM SIGSMALL symposium and the first SIGPC symposium on Small systems", DOI 10.1145/800088.802839, Palo Alto, California, United States, pp162-169.
Romney, G. W. and Brady, R. S. (2004) "An isolated, multi-platform network sandbox for teaching IT security system engineers", [online], CITC5 '04: Proceedings of the 5th Conference on Information Technology Education, pp19-23.
Le Roux, Y. (2006) "How Cisco is helping to plug the Skills Gap in Advanced Networking Technologies", Cisco Academy Website, Cisco Networking Academy, [online], http://www.cisco.com/web/IT/training_education/networking_academy/stampa/ictskillgap.pdf
Sethmann, R., Eirund, H., and Gitz, S. (2007) "Netzsicherheit: Spielerisch Hacken auf Basis von OS Software", Proceedings GI Jahrestagung 2007, Bremen, Springer Verlag.
Yang,T. A. et alli. (2004) "Design of a distributed computer security lab", University of Houston-Clear Lake, [online], http://portal.acm.org/citation.cfm?id=1040231.1040274
Yang, T. A., and Tuan Anh Nguyen (2006) “Network Security Development Process - A Framework for Teaching Network Security Courses”, Journal of Computing Sciences in Colleges, Consortium for Computing Sciences in Colleges, Vol. 21, No. 4.