Homeland Security / Cyber Security
Autumn 2005

N.B. CONTINUALLY IN FLUX
Version 24: November 22

Course Requirements:

Red Team Exercise (~25%): You are a member of a 5-6 person team of engineers and policy professionals that has been hired by the Department of Homeland Security to 1) test cyber-security vulnerabilities in the US economy, and 2) recommend appropriate policy responses (if any). The team must conduct its investigation and write a 3-7 page report summarizing its findings and recommendations.

White Paper (~55%): Groups of 3-5 students will provide a comprehensive report describing a particular threat, assessing possible losses in the event of an attack, assessing current vulnerabilities, presenting possible responses, and evaluating the cost-effectiveness of each.

Wiki (~20%): Most class discussion in this course will be conducted on-line using a Wiki. Students will be graded on the quantity and, especially, quality of their participation.

Lectures:

BERKELEY ONLY: August 31 – September 21

August 31: The Logic of Terrorism

Modern terrorism has been with us since the 1870s. What can history teach us about the strategy, tactics, and limits of terrorism?

Steve Maurer, UC Berkeley: What Can History Teach Us?

Readings:

Walter Laqueur, *No End to War: Terrorism in the Twenty-First Century* (2004) (text; Amazon.com). Please read this text in three segments, concluding 9/21.

September 7: Terrorism as Warfare

Historically, nation states were the only entities that could credibly make war. Have new technologies and the vulnerabilities of modern life changed the rules?

Steve Maurer, UC Berkeley: Can Terrorism Challenge the Nation State?

Readings:

Walter Laqueur, *No End to War: Terrorism in the Twenty-First Century* (2004) (text; Amazon.com). Please read this text in three segments, concluding 9/21.

September 13 (Tuesday): The Al Qaida Threat

Can US foreign policy discourage rogue nations from putting WMD into the hands of terrorists?

Michael Nacht, UC Berkeley**:** Post 9/11 Diplomacy: The Bush Doctrine, Rogue Nations, and US Non-Proliferation Policy

Readings:

Online Bush Doctrine Memo. http://www.whitehouse.gov/nsc/nss.html

September 21: Technology Policy and the War on Terror

Can new technologies improve current trade-offs between civil liberties and security? How do homeland security experts use Threat, Vulnerability, and Consequence (TVC) models to identify and protect society's most critical assets?

Don Prosnitz, LLNL: Security and Civil Liberties: Can Technology Improve the Balance?
Steve Maurer, UC Berkeley: The Bioshield Dilemma: Developing New Technologies at an Affordable Price
Eric Norman, LLNL: Cargo screening technologies.

Readings:

Walter Laqueur, *No End to War: Terrorism in the Twenty-First Century* (2004) (text; Amazon.com). Please read this text in three segments, concluding 9/21.
Steve Maurer, "When Patents Fail: Finding New Drugs for the Developing World," May 2005. http://www.cs.washington.edu/education/courses/csep590/05au/readings/Maurer_When_Patents_Fail.pdf (pdf)

UW AND UCSD JOIN: September 28 – December 7

September 28: Profiling the Terrorist Adversary

What are the motives and capabilities of current terrorist groups? How likely are they to use WMD or attack the nation's cyber-infrastructure?

Gary Ackerman & Jeffrey Bale, Monterey Institute: Profiling the Terrorist Adversary

Readings:

Jeffrey M. Bale and Gary Ackerman. *Recommendations on the Development of Methodologies and Attributes for Assessing Terrorist Threats of WMD Terrorism.* Center for Nonproliferation Studies, Monterey Institute of International Studies. http://www.cs.washington.edu/education/courses/csep590/05au/readings/Bale_Ackerman_FinalReport.pdf (pdf).

October 5: Computer Security Primer

Comprehensive introduction to basic computer security principles, mechanisms, and approaches. Essentially, the highlights of an undergraduate computer security course, reduced to 3 hours.

Geoff Voelker, UCSD

Readings:

Ken Thompson, "Reflections on Trusting Trust," *Communications of the ACM 27*(8), August 1984. http://www.cse.ucsd.edu/users/voelker/cse291/fa05/thompson-trust-cacm84.pdf

Alma Whitten and J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," Proc. USENIX Security Symposium, August 1999. http://www.usenix.org/publications/library/proceedings/sec99/full_papers/whitten/whitten.pdf

Ross Anderson, "Why Cryptosystems Fail," *Communications of the ACM 37*(11), November 1994. http://www.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf

October 12: Cyber Security In-The-Large

Using information technology to attack – or to amplify attacks on – various elements of the nation's critical infrastructure

Ed Lazowska, UW: Assessing Cyber-Vulnerabilities: PITAC and Beyond
Phil Venables, CISO, Goldman Sachs: The Resilient Enterprise: Convergence of Security, Compliance, Redundancy and Risky
Kirk Bailey, ex-CISO, City of Seattle: Cyber-attacks and cyber-defense in the City of Seattle
Ernie Hayden, CISO, Port of Seattle: Cyber-attacks and cyber-defense at the Port of Seattle

Readings:

Information Technology for Counterterrorism. Computer Science & Telecommunications Board, National Research Council, 2003. http://www7.nationalacademies.org/cstb/pub_counterterrorism.html. Read the Executive Summary, Chapter 1, Chapter 2, and Chapter 4.

Cyber Security: A Crisis of Prioritization. President's Information Technology Advisory Committee, 2005.
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf (pdf).
Washington Post articles on cyber terrorism, August 2005.
http://www.cs.washington.edu/education/courses/csep590/05au/readings/WA.Post.terrorism/
New York Times article, "The Rise of the Digital Thugs," August 2005.
http://www.cs.washington.edu/education/courses/csep590/05au/readings/nyt.html
Time article, "The Invasion of the Chinese Cyberspies," September 2005.
http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm
CIO Magazine article, "The Sky Really Is Falling," October 2005.
http://www.cio.com/archive/100105/qa_lazowska.html

October 19: Nuclear, Radiological & Chemical Weapons

Richard A. Muller, UC Berkeley and LBNL: The Physics of WMD
J. Patrick Fitch, LLNL: Biological Weapons and Detection Technologies

Readings:

R. Muller, "Chain Reactions, Nuclear Reactors, and Atomic Bombs,"
http://muller.lbl.gov/teaching/Physics10/chapters_Jan_2005/Chapter05.pdf
R. Muller, "The Dirty Bomb Distraction,"
http://muller.lbl.gov/TRessays/29-Dirty_Bombs.htm
R. Muller, "Crop Duster Terrorism,"
http://muller.lbl.gov/TRessays/02_Cropduster_Terrorism.htm
R. Muller, "Al Qaeda's Anthrax,
http://muller.lbl.gov/TRessays/03_Al_Qaeda_Anthrax.htm

October 26: Biological Weapons; Remediation and Recovery Technologies

The biological weapons threat: today and tomorrow. Recovering from WMD attacks.

J. Keasling, UC Berkeley: Synthetic Biology and Tomorrow's Bioweapons
Tina Carlson, LLNL: Remediation
Christine Hartmann-Siantar, LLNL: Recovery Technologies
Christine Hartmann-Siantar, LLNL: Radiation and Human Health
Steve Maurer, UC Berkeley: Nuclear Fear

Readings:

November 2: Defenses – Cyber and WMD

Mark Pustilnik, Security Development Lead, Secure Windows Initiative Attack Team, Microsoft, Getting Vulnerabilities Out of Software.

Joshua Lackey, Security Software Developer, Microsoft, and ex-Senior Ethical Hacker, IBM Global Services, Ethical Hacking.
Brian Lopez, LLNL: Identifying and Prioritizing Terrorism Risk. How do homeland security experts use Threat, Vulnerability, & Consequence (TVC) models to identify and protect society's most critical assets?

Readings:

November 9: Large-Scale Internet Criminal Activity

Internet crime. Denial of service, extortion, phishing, botnet reselling, spam, spyware, etc.

Dave Aucsmith, Senior Director, Institute for Advanced Technology in Governments, Microsoft Corp.
Steve Gribble, UW: Spyware
Butler Lampson, Microsoft: Computer Security in the Real World

Readings:

David Moore, Geoffrey Voelker, and Stefan Savage, "Inferring Internet Denial of Service Activity." *Proc. 2001 USENIX Security Symposium*, August 2001. http://www.cse.ucsd.edu/users/savage/papers/UsenixSec01.pdf
Stefan Saroiu, Steven D. Gribble, and Henry M. Levy, "Measurement and Analysis of Spyware in a University Environment," *Proc. NSDI 2004*, March 2004. http://www.cs.washington.edu/homes/gribble/papers/spyware.pdf
The Honeynet Project & Research Alliance, "Know your Enemy: Tracking Botnets," March 2005. http://www.honeynet.org/papers/bots
Computer Security in the Real World, http://www.research.microsoft.com/lampson/64-SecurityInRealWorld/Abstract.html

November 16: Incentives to Exploit and Protect

What do we know about the Internet's vulnerabilities? History of past exploits, worms, viruses. What could a determined, well-funded adversary accomplish?

Hal Varian, Berkeley, incentive-based strategies for enhancing cyber security
Stefan Savage, UCSD, Internet outbreaks: Epidemiology and Defenses
Vern Paxson, ICIR and LBNL, Network intrusion detection systems

Readings:

Carey Nachenberg, "Computer Virus-Antivirus Coevolution," *Communications of the ACM 40*(1), January 1997. http://crypto.stanford.edu/cs155/virus_antivirus_coevolution.pdf

Sumeet Singh, Cristian Estan, George Varghese and Stefan Savage, "Automated Worm Fingerprinting," *Proc. OSDI 2004*, December 2004. http://www.cse.ucsd.edu/users/savage/papers/OSDI04.pdf

David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy 1*(4):33-39, July 2003. http://www.cse.ucsd.edu/users/savage/papers/IEEESP03.pdf

Vern Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks 31*(23-24), December 1999. ftp://ftp.ee.lbl.gov/papers/bro-CN99.ps.gz

November 23: Publicity of cyber vulnerabilities; Responses to radiological attack

Steve Maurer, Berkeley, Nuclear Fear, Nuclear Evidence: What do we really know about the health effects of radioactivity? How will society react to the possibility (or fact) of a dirty bomb?

Eric Rescorla, consultant, Looking at the big picture on vulnerabilities.

Readings:

Will Grover, "All the Easy Experiments: A Berkeley Professor, Dirty Bombs, and the Birth of Informed Consent," *Berkeley Science Review* 5:2 (Fall 2005) available at http://socrates.berkeley.edu:7066/articles/issue9/plutonium.pdf

Eric Rescorla, "Is finding security holes a good idea?", Workshop on Economics and Information Security 2004, May 2004. http://www.rtfm.com/bugrate.pdf

Eric Rescorla, "Security holes... Who cares?" Proceedings of the 12th USENIX Security Conference, August 2003. http://www.rtfm.com/upgrade.pdf

Andy Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting." http://www.cl.cam.ac.uk/users/jo262/papers/weis05-ozment-vulnrediscovery.pdf

November 30: US Interrogation Policy and the War on Terror

What limits should the US military observe in prosecuting the War on Terror? What is current policy and how was it developed?

Christina Filarowski-Sheaks, Alan Liotta, and Bryan Del Monte, U.S. Department of Defense

Readings:

Geneva Convention Relative to the Protection of Civilian Persons in the Time of War. http://www.unhchr.ch/html/menu3/b/92.htm

Geneva Convention Relative to the Treatment of Prisoners of War. http://www.unhchr.ch/html/menu3/b/91.htm

The Convention Against Torture and Other Cruel, Inhumane or Degrading Treatement or Punishment. http://www.unhchr.ch/html/menu3/b/h_cat39.htm

US Torture Statute. http://www4.law.Cornell.edu/uscode/18/pIch113C.html

US Code of Military Justice. http://usmilitary.about.com/library/milinfo/mcm/blmcm.htm

Church Report.
http://www.cs.washington.edu/education/courses/csep590/CurrentQtr/church_report.pdf

Army Field Manual 34-52. http://www.globalsecurity.org/intell/library/policy/army/fm/fm34-52/toc.htm

The article "DoD Provides Details on Interrogation Process" and the 9 documents (linked) following the article pertaining to DoD interrogation policy.

http://www.defenselink.mil/releases/2004/nr20040622-0930.html

Manchester Report. Pay particular attention to parts about counter interrogation techniques and making claims of abuse if in custody.
http://www.usdoj.gov/ag/trainingmanual.htm

OPTIONAL, but helpful to be familiar with this DoD site which contains information regarding DoD detention policy, particularly with respect to GTMO.
http://www.dod.mil/home/features/gitmo/

December 7: Cyberforensics; Security of large-scale systems

What constitutes evidence for computer exploitation crimes, how is it gathered, etc.

Lance Mueller, Guidance Software, Inc., Computer Forensics
Marty Lyons, University of Washington, Security of large-scale systems

Readings: