CS 779 - Topics in Resilient and Secure Computer Systems
Instructor: Arun Sood
Thursday 4:30 pm to 7:10 pm
Innovation Hall 136
Office: Engr 5327
Office Hours: R 3:00 to 4:00.

Most current Computer Security Architectures adopt reactive approaches that require examination of packets, logs, etc. There is increasing interest in Resilience and Recovery methods. Recently, other techniques have been developed – one such approach has been developed at GMU. The focus of this course is on a study of alternate security architectures. We will explore how these can be combined in a layered defense and factors that affect the selection of the architectures.

The course will require active student participation, and we will be reviewing recent papers and reports. Each student will select a topic and produce a paper using two column IEEE formatting.
.

Topics List:

Student interest is expected to have an impact on the topics covered. I provide below a list of potential topics as a guidance.

Emerging threats

- Review recent reports

Reactive approaches:

- Intrusion detection
- Intrusion prevention
- Firewalls

Proactive (non-reactive) approaches

- Intrusion tolerance
- White listing
- Black listing

Related issues and techniques

- Vulnerabilities
- Software rejuvenation
- Applied cryptography – key management

Economic analysis

- Public access to loss reporting is limited. One area that economic analysis has been applied is patch management.

Special services and servers

- DNS and DNSSEC
- Web servers and Ecommerce
- NTP (SNTP), SMTP, etc

Lecture Strategy:

The instructor will give introductory lectures and discuss his research results – two websites below provide a link to his work. In addition, we plan to organize guest lectures. This course

will require active student participation. Students will review the assigned papers and make presentations in class.

Grade:
This special topics course will involve extensive instructor student interaction. The goal is to help each student to produce a paper written in IEEE or ACM conference proceeding style. Student group work will be encouraged, but each student must be able to defend an independent paper and presentation. Student grade will be based on exams, class presentations, class participation, papers and reports.

Mid term: 20%. Final: 20%. Class Participation: 15%. Homework, projects, presentations 45%.

Relevant websites:
http://cs.gmu.edu/~asood/scit Provides links to several papers on Self Cleansing Intrusion Tolerance. Pointers to on-line pubs and media reports about SCIT are also included.

http://cs.gmu.edu/~lics/icc/GFIRST-BOF-DNS.htm Collection of papers relevant to DNS server protection.

Starting reference list:

1. Brandon Wagner and Arun Sood, Economics of Resilient Cloud Services, *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* - 1st IEEE International Workshop on Cyber Resilience Economics, 2016.
2. Quyen Nguyen and Arun Sood, Improving Security Level via Velocity of Moving Target Defense, 2016 IEEE International Conference of Software Quality, Reliability and Security 2016.
3. Winn Schwartau, Time Based Security – Measuring Security and Defensive Strategies in a Neworked Environment, Interpact Press, 2001.
4. Paulo Sousa et al, Highly Available Intrusion-Tolerant Services with Proactive-Reactive Recovery , *IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 4, pp. 452-465, Apr. 2010.*, Apr. 2010.
5. Alysson Bessani et al, The CRUTIAL Way of Critical Infrastructure Protection , *IEEE Security and Privacy, vol. 6, no. 6, pp. 44-51, Nov/Dec 2008.*, Dec. 2008
6. Niels Provos and Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley, 2007.
7. Mitre Common Vulnerabilities and Exposures (CVE), Common Weaknesses and Exposures (CWE), Common Attack Pattern Enumeration and Classification (CAPEC) website http://xxx.mitre.org xxx = {cve, cwe, capec}
4. A. Lazarevic, V. Kumar, J. Srivastava, Intrusion Detection: A Survey, in Managing Cyber Threats Issues, Approaches, and Challenges, Series: Massive Computing , Vol.5 Kumar, Vipin; Srivastava, Jaideep; Lazarevic, Aleksandar (Eds.)
5. http://threatchaos.com/2009/03/new-new-anatomy-of-a-hack/
6. http://www.ethicalhacker.net/content/view/8/2/
7. Sally Whittle, Anatomy of a hack attack, http://resources.zdnet.co.uk/articles/0,1000001991,39291953,00.htm
8. M. Maloof and G. Stephens, "ELICIT: A System for Detecting Insiders Who Violate Need-to-Know," RAID 2007 LNCS 4637, 146–166. http://www.cs.georgetown.edu/~maloof/pubs/maloof-raid07.pdf
9. Crispin Cowan, Calton Pu, Dave Maier, Heather Hinton, Jonathan Walpole, Peat Bakke, Steve Beattie, Aaron Grier, PerryWagle and Qian Zhang, StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks_

10. Bharat B. Madan, Katerina Goseva-Popstojanova, Kalyanaraman Vaidyanathan, and Kishor S. Trivedi. "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", *Dependable systems and networks-performance and dependability symposium (DSN-PDS)*, 2002.
11. Feiyi Wang, Frank Jou, Fengmin Gong, C. Sargor, K. Goseva-Popstojanova, and K. Trivedi. "SITAR: a scalable intrusion-tolerant architecture for distributed services", *Proceedings of the Foundations of Intrusion Tolerant Systems (OASIS '03)*, 2003.
12. Paulo E. Veríssimo, Nuno F. Neves, Christian Cachin, Jonathan Poritz, David Powell and Yves Deswarte, Robert Stroud, and Ian Welch. "Intrusion-Tolerant Middleware: The Road to Automatic Security", *IEEE Security & Privacy*, 2006.
13. Yih Huang, David Arsenault, and Arun Sood. "Incorruptible System Self-Cleansing for Intrusion Tolerance", *Performance, Computing, and Communications Conference, IPCCC 2006*.
14. Rong Wang, Feiyi Wang, and Gregory T Byrd. "Design and Implementation of Acceptance Monitor for Building Scalable Intrusion Tolerant Systems", *Computer Communications and Networks Proceedings, Tenth International Conference*, 2001.
15. R. Stroud, I. Welch, J. Warne, and P. Ryan. "A qualitative analysis of the intrusion-tolerance capabilities of the MAFTIA architecture", *2004 International Conference on Dependable Systems and Networks*, Issue 28 June-1 July 2004, pp. 453 – 461.
16. I. Welch, J. Warne, and P. Ryan, and R. Stroud. "Architectural Analysis of MAFTIA Intrusion Tolerance Capabilities", *Technical Report CS-TR-788, University of Newcastle upon Tyne,* Feb 3rd, 2003.
17. Yih Huang, David Arsenault, and Arun Sood. "Securing DNS services through system self cleansing and hardware enhancements", *The First International Conference on Availability, Reliability, and Security, ARES 2006*.
18. Yih Huang, David Arsenault, and Arun Sood. "Secure, Resilient Computing Clusters: Self-Cleansing Intrusion Tolerance with Hardware Enforced Security (SCIT/HES)", *The Second International Conference on Availability, Reliability, and Security, ARES 2007*.
19. Naresh Verma, Yih Huang, and Arun Sood. "Proactively Managing Security Risk", *Security Focus, Nov. 7, 2007*. Available: http://www.securityfocus.com/infocus/1896/1 [Feb. 24, 2009].
20. Matthew Smith, Christian Schridde and Bernd Freisleben. "Securing Stateful Grid Servers through Virtual Server Rotation", *HPDC'08*, June 23–27, 2008, Boston, Massachusetts, USA.
21. Brown, A. and D. A. Patterson. Embracing Failure: A Case for Recovery-Oriented Computing (ROC).2001 High Performance Transaction Processing Symposium, Asilomar, CA, October 2001.
22. G. Candea, A. Brown, A. Fox, D. Patterson, Recovery-Oriented Computing: Building Multitier Dependability, IEEE Computer, November 2004.
23. Partha Pal, Franklin Webber, and Richeard Schantz. "The DPASA Survivable JBI – A High-Water Mark in Intrusion-Tolerant Systems", *Workshop on Recent Advances in Intrusion Tolerant Systems'07*, 2007.
24. J. Knight, D. Heimbigner. and A. Wolf. "The Willow Architecture: Comprehensive Survivability for Large-Scale Distributed Applications", *lntrusion Tolerance System Workshop, Supplemental Volume on 2002 International Conference on Dependable .System and Network*, 2002.
25. L. Zhou. F. Schneider. and R. van Renesse. "Coca: A Secure Distributed On-line Certification Authority", *ACM Transactions on Computer Systems*, Nov. 2002.
26. Peng Liu. *Architectures for Intrusion Tolerant Database Systems*. Proceedings of the Foundations of Intrusion Tolerant Systems (OASIS '03), 2003.
27. Jay J. Wylie, Michael W. Bigrigg, John D. Strunk, Gregory R. Ganger, Han Kılıççöte, Pradeep K. Khosla. "Survivable Information Storage Systems", *Computer IEEE 2000*.
28. Paulo Sousa, Alysson Neves Bessani, Miguel Correia, Nuno Ferreira Neves, Paulo Verissimo. "Resilient Intrusion Tolerance through Proactive and Reactive Recovery". *13th IEEE International Symposium on Pacific Rim Dependable Computing*, 2007.
29. Paulo Silva1, Luis Silva1, Artur Andrzejak, "Using Micro-Reboots to Improve Software Rejuvenation in Apache Tomcat", CoreGRID Technical Report,Number TR-0099, September 17, 2007,Institute on Architectural issues: scalability,dependability, adaptability (SA), CoreGRID - Network of Excellence http://www.coregrid.net

Additional references will be added later.

\