## OWASP

# Call for Training Application

**Please forward to all interested practitioners and colleagues.**

YOU MUST SUBMIT ALL OF THE FOLLOWING (Submission Deadline: DATE)

Please return this speaker form by fax to: NAME

| | |
|---|---|
| **Trainer Name:** | Timothy D. Morgan |
| **Company/Employer:** | VSR |
| **Telephone:** | 617.933.8919 x101 |
| **E-mail:** | tmorgan@vsecurity.com |

**Proposed Training Title:**

*Application Cryptanalysis Made Easy*

**Anticipated Audio/Visual Requirements:**

□ Laptop ☒ LCD Projector □ Overhead □ Other __________

**Training Summary: (Be concise)**

*Use of cryptography permeates today's computing infrastructures. While few programmers attempt to implement sophisticated cryptosystems, many unwittingly develop simple protocols in every day applications without adequate knowledge of how cryptographic primitives should be combined. In this training we explore several techniques for analyzing and breaking the kinds of cryptographic protocols which are commonly found in modern applications.*

*Attendees will first be presented with a brief review of cryptographic primitives and their uses, followed by an introduction of several techniques to analyze cryptographic systems in a black-box manner. In each case, the discussion will describe how programmers can avoid making the common mistakes that allow these attacks to succeed.*

**Audience**

□ Management ☒ Technical □ Operations □ Other __________

**Skill Level required of Attendees**

□ Basic ☒ Intermediate ☒ Advanced □ Other __________

**Duration of Training**

□ 4 Hour ☒ 1 Day □ 2 days □ Other __________

**Special Needs** (e.g., will include labs, software needed, internet access, wireless setup, required reading, etc)

*Students will need to bring a laptop that can run a small virtual machine under either VirtualBox (preferred) or VMWare. All tools and test software will be preloaded on the virtual machine provided. Internet access for students and the instructor is recommended.*

*Students will be expected to write short scripts to repeatedly send HTTP requests to a local service for the purpose of exploit development. Scripts may be in any suitable language.*

**Please list any other publications or conferences where this material has been or will be presented/submitted.**

*Course was first given at AppSecUSA 2012:*
*http://www.appsecusa.org/schedule/trainings/688-2/*

*With each delivery, the course is updated based on new information and adapted to work with the improved tool kit.*

**Explain (in 3 sentences or less) reasons why you feel this material is innovative/significant for the OWASP event.**

*We believe there is little awareness amongst developers or even security consultants about the kinds of problems that can arise from using weak PRNGs, cryptographic modes, or lack of integrity protection. Recently, padding oracle attacks (PoAs) have brought some of these issues to light, but many applications remain vulnerable to this and related encryption mode flaws.*

*Cryptanalysis tends to be considered a black art and discussions of it are often focused on attacking specific ciphers. However, misuse of PRNGs and cipher modes in rudimentary challenge-response protocols is a far more common issue in modern applications. These problems also don't require a great deal of mathematics to understand and can be exploited in a black box way by the average pentester, given the right tools and background.*

**Attendee takeaways and key learning objectives:** *(Please list three learning objectives)*

- *"Where to start" when it comes to analyzing a custom cryptographic protocol or primitive, such as custom single sign-on, password reset tokens, or other encrypted values used by an application.*
- *How to exploit common problems, including:*
    - *The basics for attacking random tokens and PRNGs, including how to check for weak seeds and weak PRNGs.*
    - *How to identify characteristics of encrypted tokens, including block size and cipher mode.*
    - *How to conduct block swapping attacks on ECB and CBC mode encryption where integrity protection isn't provided. Unsafe algorithm reuse will also be explored.*
    - *Padding oracle attacks on CBC mode*
- *For each attack scenario, attendees will be shown how programmers can avoid these common pitfalls.*

*The course consists of about 50% lecture and 50% lab time. These are organized into alternating sessions so that students may immediately apply the material learned in hands-on lab sessions.*

**Trainer Bio:** Briefly describe your professional experience or areas of expertise related to this presentation. You should include education/certification information in this section.

1. **Experience of the Trainer**

   *Tim has developed training materials for several two and three day courses in the areas of application security, cryptography, digital forensics, and incident response. He and other VSR representatives have delivered these courses dozens of times in private sessions upon the request of VSR's clients, which include several fortune 500 firms.*

   *Tim is the leader of the Portland, Oregon OWASP chapter and has presented several talks over the last few years at these meetings and at other local events, such as BSidesPDX, InnoTech NW, and ISSA chapter meetings.*

2. **Training History (please indicate place and duration)**
   *a.* **OWASP related**

   *AppSecUSA 2012 (this 1-day course)*
   *Short talks at OWASP meetings*

   **b. For organizations other than OWASP**

   *Numerous private training sessions (1-4 per year, starting in 2006).*

3. **Testimonials as a Trainer (if any)**

*Student feedback from AppSecUSA 2012 is available upon request, or can be obtained from Sarah Baso. Suggestions from students will be used to improve the course.*

4. **Pertinent Certifications and Licenses**

*None*

5. **Published Materials (News releases, Papers, Whitepapers, Research)**

*At this point, the only published materials relating directly to this course is the tool suite "bletchley", which is used in the course:*
*http://code.google.com/p/bletchley/*

*Tim has also published research on other security and forensics topics over the years:*
*http://www.sentinelchicken.com/research/tdm_ms_thesis/*
*http://www.dfrws.org/2008/proceedings/p33-morgan.pdf*
*http://www.vsecurity.com/resources/advisory*
*http://www.vsecurity.com/resources/publish*
*http://www.vsecurity.com/resources/tool*

**Outline** (Topic and Sub-Topics; 2 levels) – Please attach samples if available

***Samples of course content available upon request***

*I. Crypto refresher*
*A. Pseudorandom number generators*
*B. Block ciphers and their modes*
*C. Hashes and (H)MACs*

*II. Attacks on nonces*
*A. Statistical/structural analysis*
*B. Attacking weak seeds*
*C. Attacking weak algorithms*

*III. Exercise: Weak nonces*
*A. Fun with Stompy*
*B. Attacking a linear congruential generator (LCG)*

*IV. Attacks on encrypted tokens*
*A. Determining block size / mode*
*B. Basics of block swapping*
*C. Attacks on ECB and CBC modes*

*V. Exercise: Block swapping*
*A. Analyzing encoded blobs*
*B. Identifying algorithm reuse*
*C. Forging tokens*

*VI. Padding oracle attacks*
*A. Theory*
*B. Real-world examples*

*VII. Exercise: Asking the oracle*