Сигурен програмен код
2013-2014

1. Понятие за сигурен код. Основни понятия в областта. Моделиране на заплахи.
2. Въвеждане на принципа за най-ниска привилегированост. Принцип на ешелонирана защита
3. Автентикация. Атаки чрез прикриване на самоличност.
4. Изпълнение на код в ниско-привилегировано ниво. Код с извън-администраторски права
5. Понятие за одит (auditing)
6. Контекст на сигурността (secutity context)
7. Профил на сигурността (token). Сесия 'logon'. Работа с потребителски профил.
8. Привилегии и работа с тях. Промяна на привилегиите в режима на изпълнение на програма.
9. Информация за текущия собственик (principal) на програмните обекти. Събиране на информация за потребителския профил от кода.
10. *Програми - "демони" (daemons).
11. *Стартиране на приложения от фиктивен потребител.
12. Деперсонализация. Деперсонализация в компонентен код. Деперсонализиране на user. Деперсонализация в ASP код.
13. *Автентикация в компонентен код.
14. *Сигурност на код в компонентна (COM) среда.
15. *Конфигуриране на сигурност за COM клиент.
16. Програмни методи за съхранение на важна информация в компютър.
17. Програмни подходи за работа с парола.
18. Изключване на конзола за целите на сигурността. Програмна реализация на Log-off и Reboot на компютър за целите на сигурността.

19. Атаки чрез препълвания(overrun attacks). Понятие. Схема на атаките. Типове.
20. Атака през препълване на стек (stack overrun attacks)
21. Атаки през препълване на динамична памет (heap overrun attacks).
22. Атаки през прекрачване граници на масив (array indexing attacks).
23. *Противодействие на атаки през стека.
24. *Код за стабилно прихващане на изключения .
25. Технически похвати за повишаване сигурността: при повиквания на функции; при оператор new; при странична организация на паметта; при рандомизация на изображения.

26. Криптографски анализи от страна на кода. Случайни ли са генерираните 'случайни ' числа? Пример от C и от C++ клас. Случайни числа в .NET. Случайните числа в web програмирането.
27. Криптографски анализи от страна на кода: менажиране на ключ (key managment).
28. Програмни подходи за криптиране на ключ.
29. Проблеми при повторно използване на ключ и начини за решаване.
30. Атаки на последователностни данни чрез подмяна на бит (bit-flippering attacks against streaming ciphers) .
31. Програмни подходи за хеширане на ключ.
32. Програмни подходи за генериране и анализ на цифров подпис.
33. Програмни подходи за съхранение на секретни данни. Понятия и методи.
34. Хеширане и размиване (salted hash creation). Методи , класове и обкръжения за целта.
35. Използване на вградения стандарт PKCS #5 (Public Key Cryptography Standard) за защита на данни.
36. Извличане на секрети през код. Методи за опазване на секрети в Windows 2000 и нагоре.
37. Различия в методите LSA и DPAPI използвани в Windows и .NET. Пример с DPAPI за съхраняване и извличане на секретни данни.
38. Съхраняване на секрети в паметта. Програмни подходи за криптиране на секрети в памет. Заключване на блокове памет. Секрети в managed код.
39. Преглед на програмните подходи за опазване на секретни данни. Анализ.

40. *Хакери и RPC и ActiveX
41. *Влияние на множество RPC сървъри в общ процес
42. *Сигурност при ActiveX контролите

43. *Хакери и програмиране със сокети
44. *Верифициране на заявки за свързване със сървър

45. Атаки към информационни продукти. SQL инжекции. Примери
46. Частични решения: потребителският вход в '' ; използване на stored procedures и др.
47. Атака през вход (Input) на приложение. Избягване на динамични SQL заявки.
48. Опасности при свързване на администраторско ниво. Използване на най-ниско привилегировано ниво. Правила при формиране на SQL оператори.
49. Параметризирани команди .
50. Правила за защита на важната информация – парола и connection низ.
51. Код с много нива на защитеност – пример.

52. Хакерски атаки в Internet. Основни типове атаки. STRIDE модел за класификация на заплахите в Internet пространството.
53. Разкриване на информация за web форма. Защита от подмяна на битова информация – добавяне на MAC

54. **XSS инвазиите. Пример за атака с вмъкване на script.**
55. **Схема на XSS атаките.**
56. **Хакерски подходи: вмъкване на скрипт вместо атрибут, активиране на скрипт през събитие и др.**
57. **XSS атаки срещу локални файлове. XSS атаки към ресурси.**
58. **Спасения от XSS атаки: кодировка на входа, заграждане с “, вкарване данните в атрибут innertext, спасяване на cookies, добавяне на атрибут <FRAME SECURITY>.**
59. **Опасности при използване на ISAPI функционалност.**
60. **Отказ от услуга (DoS атаки). DoS атаки и валидиращи regular expression изрази. Същност на проблема. Примери.**
61. **Проверка на регулярния израз (regex) срещу DoS уязвимост .**
62. **XML DoS атаки и защитни техники. Същност на проблема. XML бомби.**
63. **XML базирани атаки – от външни източници (external entity attacks).**
64. **Защита от XML бомби. Защита от атаки, базирани на външни източници.**

Водещ преподавател: проф. д-р О. Наков