Cel zajęć

Celem zajęć jest zaznajomienie studentów z problematyką bezpieczeństwa komputerowego, rozwinięcie u studentów świadomości zagrożeń cyberprzestępczością i właściwych nawyków ochrony poufności informacji oraz szerzenie dobrych praktyk w dziedzinie zapewnienia bezpieczeństwa informacji. Zostaną przedstawione podstawowe narzędzia służące do ochrony informacji, takie jak programy szyfrujące, *firewalle*, systemy IPS itp., ale wykład omawia nie tylko techniczne, lecz także prawne, etyczne, psychologiczne i socjologiczne aspekty bezpieczeństwa komputerowego.

Przedmiot nie wymaga wstępnego przygotowania studentów z zakresu bezpieczeństwa komputerowego ani szczególnej wiedzy informatycznej i jest przewidziany głównie dla młodszych studentów.

Forma zajęć

Odbędzie się 30 dwugodzinnych spotkań, przy czym przez pierwszą połowę semestru (15 spotkań) będzie się odbywać wykład, zaś w drugiej części semestru odbędzie się 15 seminariów poprowadzonych przez studentów. Na wykładzie zostaną omówione podstawowe zagadnienia bezpieczeństwa komputerowego. Na seminariach zostaną przedstawione wybrane bardziej szczegółowe zagadnienia. Każdy student w trakcie semestru napisze 3 eseje (w dowolnym języku, który znają prowadzący, w szczególności może to być polski lub angielski). Warunkiem zaliczenia ćwiczeń jest otrzymanie pozytywnej oceny z wszystkich trzech esejów. Autorzy piętnastu najlepszych esejów zostaną nominowani do wygłoszenia seminariów na podstawie swoich esejów (po polsku lub angielsku).

Przedmiot będzie prowadzony po raz trzeci, co nie oznacza, że wykładowca umie już go prowadzić. Przeciwnie, podobnie jak rok wcześniej spapra go pewnie zupełnie. Osoby o słabych nerwach, niskim poziomie empatii wobec prowadzącego oraz reprezentujące postawę roszczeniową uprasza się o niezapisywanie się.

Treść wykładu

I. WPROWADZENIE

1. Wprowadzenie do problematyki bezpieczeństwa komputerowego. Kultura bezpieczeństwa.
2. Prawa autorskie i plagiaty. Autorskie prawa majątkowe i piractwo. Specyfika mediów elektronicznych.*Creative Commons*. Dozwolony użytek. Dobre praktyki. Jak tworzyć i rozpowszechniać własne dzieła z poszanowaniem cudzej własności intelektualnej. Omówienie sposobu pisania esejów.
3. Poufność komunikacji. Konfiguracja GPG. Utworzenie bazy kluczy publicznych i *key signing party*.

II. CYBERBEZPIECZEŃSTWO

1. Cyberbezpieczeństwo narodowe. Zagrożenia infrastruktury krytycznej i ładu gospodarczego. Służby powołane do ochrony bezpieczeństwa państwa (NSA, GCHQ, ABW, FSB) i ich

uprawnienia. Kontrowersje. Cyberinwigilacja. Wikileaks i Edward Snowden. Cyberwojna. Cyberterroryzm. Szpiegostwo przemysłowe.

2. Cyberbezpieczeństwo jednoski. a) Hakerzy i kultura hackingu. *White/grey/black hats*. Chaos Computer Club. Najsłynniejsi hackerzy i ich losy (Kevin Mitnick, Kevin Poulsen, Władymir Lewin, Adrian Lamo i inni). *Script kiddies*. „Niezamówiony pentesting". Problemy prawne i zagrożenia. *Ethical hacking*. b) Cyberprzestępstwa. *Spam*, *scam*, oszustwa, wyłudzenia. *Nigerian 419 scam*. *Phishing*. Zagrożenia bankowości elektronicznej, cyberprzestępczość zorganizowana. c) Cyberwandalizm i *trolling*. Wandalizm w Wikipedii i innych portalach społecznościowych. d) Haktywizm. Nieposłuszeństwo obywatelskie. Dred Scott. Mahatma Gandhi. Thích Quảng Đức. Aaron Swartz. Zmiana prawa w ramach prawa, czy poza prawem? Ruchy społeczne. Anonymous. Wikileaks.
3. Cyberprywatność. a) Potrzeba prywatności i jej ochrona. Publiczne a prywatne. Prywatność u zwierząt. Psychologia, socjologia i neurologia prywatności. Skrępowanie i wstyd. Czwarta poprawka do Konstytucji Stanów Zjednoczonych. Samuel D. Warren, Louis D. Brandeis, Judge Thomas McIntyre Cooley. b) Naruszanie prywatności przez państwo. Panopticon, Orwell i Kafka. Powszechny monitoring. Masowe zbieranie danych. Metadane. c) Naruszanie prywatności przez korporacje. Cyberprzemysł i „darmowe usługi". Przemysł reklamowy. Google, Facebook i in. Zbieranie danych w Internecie. WWW, ciasteczka i*browser fingerprinting*.

III. OCHRONA DANYCH

1. Kontrola dostępu. Protokoły AAA. Metody uwierzytelniania. Hasła. Bezpieczna mnemotechnika. Teoria bezpieczeństwa haseł. Uwierzytelnianie dwuskładnikowe. Problemy psychologiczne, *password fatigue*. Protokoły CAS. Uwierzytelnianie biometryczne.
2. Ochrona danych w spoczynku. Digital forensics. Architektura pamięci komputerów. Dyski twarde mechaniczne i dyski SSD. Triada CIA. a) Dostępność danych. Backupowanie i archiwizacja danych.*Failure recovery*. Dostępne narzędzia i techniki. b) Poufność i integralność danych. Podstawy kryptografii. Szyfrowanie dysków. Dostępne narzędzia. c) Niszczenie danych i rekonstrukcja zniszczonych danych.
3. Ochrona danych w ruchu. Podstawy sieci komputerowych. Ataki na transmisję danych. MITM.*Typosquatting*. *Domain squatting*. *IDN homoglyph attack*. *BGP prefix hijacking* i *DNS spoofing/cache poisoning*. Stos protokołów sieciowych i zasada end-to-end. Szyfrowanie w warstwach stosu TCP/IP. Szyfrowanie w warstwie aplikacji. OpenPGP i S/MIME. Szyfrowanie w warstwie transportowej. SSL/TLS. Infrastruktura klucza publicznego. *Certificate Authorities* i *Web of Trust*. Problemy z CA w TLS. Certyfikaty w przeglądarkach WWW.

Przykładowe tematy esejów

1. Wycieki prywatnych danych z chmur. Czy Dropbox jest bezpieczny? Przykłady incydentów (np. ostatni wyciek zdjęć nagich celebrytów). Metody zabezpieczania (encfs, duplicati, boxcryptor, cloudfogger, secretsync itp.)
2. Kody CVV2 — zwiększenie bezpieczeństwa czy mydlenie oczu?
3. Wirusy a OS. Który system jest najbardziej zawirusowany (zdaje się, że Android pobił Windows). Czy istnieją wirusy pod Debiana?
4. Cenzura Internetu na Świecie. Spór Chin z Googlem, Egipt 2011, Rosja.
5. Co by się stało, gdyby nagle wyłączono Internet?
6. Buffer overflow vulnerability — nadal najpopularniejsza podatność umożliwiająca skonstruowanie ataku na kod mimo ochrony pamięci, separacji danych i kodu itd. Jak to możliwe?
7. Stuxnet — jednorazowy incydent, czy proof of concept? Będzie ciąg dalszy?
8. Anonymous — historia, fakty. Czemu nie atakują Rosjan podczas sporu z Ukrainą? Czyżby wszyscy Anonymous byli Rosjanami?
9. SCADA i ataki na nie. Czy można rozregulować wrocławskie wodociągi przez Internet?
10. Keyloggery — jak działają i jak się przed nimi bronić?
11. Prawnie dopuszczalna inwigilacja. Wymagane przez prawo lub potajemnie wprowadzone przez instytucje rządowe backdoory w popularnych protokołach. Przypadek WPS. Dual_EC_DRBG. Heartbleed — przypadkowy błąd, czy celowe działanie?
12. RFID i NFC. Wygoda, czy zagrożenie? Inwigilacja poprzez RFID. Ataki na urządzenia z NFC. Atak przedłużonego terminala.
13. Emission security. Czy można skonstruować zdalny keylogger działający poprzez sieć energetyczną? Czy można przechwytywać dane podsłuchując hałas wytwarzany przez urządzenia elektroniczne (w tym zasilacze)?
14. Skąd Google Maps wiedzą, gdzie są korki?
15. Podpis elektroniczny kwalifikowany i profil zaufany. Czemu jeszcze nie jesteśmy e-obywatelami? Doświadczenia i problemy E-stonii.
16. E-wybory i e-głosowania. Protokoły, bezpieczeństwo, doświadczenia.
17. Sprzętowe generatory liczb losowych. Jak skonstruować dobry generator? W jaki sposób może on polepszyć działanie /dev/random?
18. Czterocyfrowy PIN zapisany na karcie płatniczej. Oni znowu to robią! Po co? Jak bardzo to jest niebezpieczne?
19. Lista Robinsonów — rozwiązanie problemu, czy fortel spamerów i telemarketerów by obejść prawo? A może jeszcze jeden sposób na wyłudzanie danych osobowych?
20. Elektroniczny pieniądz. Jak to działa? Korzyści i zagrożenia.
21. Pornografia w Internecie i jej blokowanie. Art 4a. Ustawy o systemie oświaty. Uchwała Sejmu Rzeczypospolitej Polskiej wzywająca Ministra Administracji i Cyfryzacji do zagwarantowania rodzicom prawa do Internetu bez pornografii. Deklaracja Davida Camerona z 22 lipca 2013 w sprawie domyślnego nałożenia na Internet w Wielkiej Brytfanii filtrów moralności i blokowania w

wyszukiwarkach zapytań „chorych ludzi, szukających w sieci nielegalnych treści". Czy to cenzura Internetu? Słuszne czy groźne? Czy Internet powinien być przezroczysty?

22. Dziury w SSL/TLS: BEAST, CRIME, TIME, BREACH, HEARTBLEED, POODLE… Czy połączenia HTTPS w ogóle są bezpieczne?
23. Buffer overflow vulnerability — nadal najpopularniejsza podatność umożliwiająca skonstruowanie ataku na kod mimo ochrony pamięci, separacji danych i kodu itd. Jak to możliwe?
24. Onion routing — jak to działa? Jak z tego korzystać? Czy jest bezpieczne? TOR — kto za tym stoi? Czemu tego nie zabronią?
25. Czy oprogramowanie Open Source jest bezpieczniejsze niż Closed Source?
26. Cyberprzemoc. Czy to jest problem społeczny w Polsce?
27. Cyberterroryzm islamistyczny.
28. United States Cyber Command. Historia, zadania, metody działania.
29. Cyberwojska północnokoreańskie. Jest się czego bać?
30. Cyberdebilizm. Afera generała Petraeusa: czy szef CIA może nie mieć bladego pojęcia o cyberpoufności?
31. Podatności protokołu DNS na ataki i sposoby zabezpieczania. DNSSEC.
32. Protokół NTP i jego podatność na ataki. CVE-2013-5211.
33. Ślad ekologiczny cyberinwigilacji. Jaki jest wpływ NSA na środowisko naturalne?

Literatura

1. Ross Anderson, *Security Engineering*, Wiley, 2008.