Propozycje tematów wystąpień

semestr letni 2020/2021

1. Ochrona danych osobowych według RODO / GPDR – skrót najważniejszych wiadomości.
2. Progowe i bezprogowe systemy dzielenia tajemnicy – omówienie zasady działania i zastosowań.
3. Przeglądarkowe ciasteczka i ich bezpieczeństwo – czym są, jak są chronione i dlaczego trzeba na nie uważać?
4. Bezpieczeństwo protokołu HTTPS – czym się różni od HTTP, co ujawnia i kiedy zielona kłódka to za mało?
5. Bezpieczeństwo sieci Bluetooth – zasada działania, uwierzytelnienie i odporność na podsłuch.
6. Bezpieczeństwo sieci WiFi – w szczególności krótkie omówienie standardów WEP, WPA, WPA2 i WPA3.
7. Bezpieczeństwo systemów GPS / Glonass / Galileo – jak działają, czy zawsze można im ufać, co gdy ich zabraknie?
8. Ataki DoS (Denial of Service), DDoS, DRDoS – omówienie i sposoby zabezpieczeń.
9. Ataki „man in the middle” – idea, głośne przypadki, metody zabezpieczeń przed takimi atakami.
10. Karty bankowe i abonenckie – przegląd zabezpieczeń i znanych metod ich łamania.
11. Sprzętowe klucze bezpieczeństwa, algorytmy HOTP, TOTP i inne – zasady ich działania.
12. Podpisy cyfrowe dokumentów i poczty elektronicznej – jak działają, przykład konfiguracji na użytek prywatny.
13. Sieć TOR i inne – jak działają, co umożliwiają i czy są bezpieczne?
14. Programy / urządzenia rejestrujące klawisze (keyloggery) – sposoby ich działania i zabezpieczenia się.
15. Bezpieczne przechowywanie swoich i cudzych haseł w systemach informatycznych – najważniejsze reguły i zalecenia.
16. Odzyskiwanie i bezpieczne usuwanie danych – jak działa, dlaczego jest możliwe, potencjalne skutki i co z tym zrobić?
17. OWASP Top Ten – krótka charakterystyka najczęściej występujących podatności w aplikacjach.
18. Oprogramowanie ransomware – historia i przykłady, używane metody, sposoby zapobiegania.
19. Szyfrowanie na poziomie dysku twardego a szyfrowanie na poziomie systemu plików – wady, zalety, przykłady rozwiązań.
20. PPCTP i inne rozwiązania – czy możliwe jest prawdziwie anonimowe śledzenie kontaktów między ludźmi?
21. Sposoby ukrycia się przed monitoringiem i automatycznym rozpoznawaniem twarzy – jak, dlaczego i co wykorzystać?
22. Kryptografia postkwantowa – dlaczego obecne zabezpieczenia mogą nie wystarczyć i czy mamy alternatywy?
23. Kryptografia kwantowa i kwantowa dystrybucja klucza – zasady działania, algorytmy i ich ograniczeń.