Krzysztof Szczypiorski

Cyber(nie)bezpieczeństwo

Wykład inauguracyjny w roku akademickim 2019/2020
Wydział Elektroniki i Technik Informacyjnych PW
1 października 2019, Duża Aula, Gmach Główny PW

Trzy tezy wykładu to:

1. kulturowa: cyberprzestrzeń jest zaawansowanym tworem techniczno-kulturowym – jest realizacją marzeń wielu twórców, wynalazców i inżynierów
2. techniczna: bezpieczeństwo i cyberprzestrzeń to nierozłączne elementy (stąd: cyberbezpieczeństwo)
3. i paranoiczna: pełne bezpieczeństwo, jeśli jest osiągalne, nie jest stanem stałym (stąd: cyber(nie)bezpieczeństwo)

Cyberprzestrzeń jest rozumiana jako zbiór technik cyfrowych służących do wymiany informacji, ale także jako nowego typu przestrzeń społeczna częściowo wirtualna, która może być bytem całkowicie odseparowanym od fizycznego. Geneza nazwy: w latach 1968-1970 duńska artystka Susanne Ussing we współpracy z duńskim architektem Karstenem Hoffem stworzyła serię kolaży pod tytułem "CYBERSPACE". Dekadę później termin pojawił się w literaturze (William Gibson). Tradycyjnie ludzie próbowali rozumieć świat przez relacje pomiędzy różnymi zjawiskami fizycznymi zachodzącymi w otoczeniu np. poprzez żywioły. Cyberprzestrzeń jest tworem sztucznym jednak posiada związki z otoczeniem fizycznym – można ją traktować jako kolejny żywioł. Jako cezurę powstania cyberprzestrzeni można podać rok 1968, w którym pojawił się routing w sieci ARPANET, a także pierwszy programowalny sterownik logiczny (PLC). Natomiast dla cyberbezpieczeństwa będzie to rok 1976 – opublikowanie algorytmu uzgadniania klucza przez Witfielda Diffiego oraz Martina Hellmana. Rozwój bezpieczeństwa jest skorelowany z działaniami wojennymi i zbrojeniem – branża wojskowa dokonywała historycznie największych inwestycji w tym obszarze. W dalszej części wykładu przedstawiono cyfryzację mowy oraz wybrane ataki (podsłuch, modyfikacja, podszycie się i wyparcie). Określono podstawowe związki pomiędzy podstawowymi usługami cyberbezpieczeństwa: poufnością, integralnością, uwierzytelnieniem i niezaprzeczalnością. Przedstawiono związki pomiędzy zagrożeniem, podatnością, zasobami i ryzykiem, a następnie zaprezentowano generycznie projektowanie zabezpieczeń jako iteracyjny proces zawierający analizę ryzyka, projekt polityki bezpieczeństwa i oszacowanie kosztów. Problemy kluczowego znaczenia cyberbezpieczeństwa przedstawiono w kontekście infrastruktury krytycznej ilustrując to przykładami ataków na instalacje rurociągów w ZSRR (1982), jak i na Ukrainie (2015). W dalszej części przedstawiono zagadnienia rozpoznawania znanych ataków i anomalii tłumacząc złożoność tworzenia modeli zachowań w cyberprzestrzeni, które przeważnie nie odzwierciedlają wszystkich cech i ich dynamizmu. Zagadnienie fałszywych alarmów wpływa na rzetelność systemów wykrywających anomalie, w szczególności błędy drugiego rodzaju prowadzą do nierozpoznawania ataków. Na koniec przedstawiono podstawowe istotne związki cyberbezpieczeństwa z edukacją i etyką.

Link do prezentacji: https://tinyurl.com/pobierz-mnie