

AP Cybersecurity

Glossary · · every term in the course, A–Z

English	Pinyin
 Accept <i>/ək'sept/</i>	jiē shòu
 acceptable use policy <i>/ək'septəbl ju:s 'pɒlɪsi/</i>	kě jiē shòu shǐ yòng zhèng cè
 access control list (ACL) <i>/'ækses kən'trəʊl list/</i>	fǎng wèn kòng zhì liè biǎo
 access control vestibule <i>/'ækses kən'trəʊl 'vestɪbjʊ:l/</i>	mén jìn qián shì
 access point <i>/'ækses pɔɪnt/</i>	jiē rù diǎn
 accounting <i>/ə'kaʊntɪŋ/</i>	shěn jì jì lù
 address resolution protocol (ARP) <i>/ə'dres ,rezə'lu:ʃn 'prəʊtəkɒl/</i>	dì zhǐ jiě xī xié yì
 administrative <i>/əd'mɪnɪstrətɪv/</i>	guǎn lǐ xìng
 adversary <i>/'ædvəsəri/</i>	duì shǒu
 AES <i>/,ei i: 'es/</i>	gāo jí jiā mì biāo zhǔn
 AI-enhanced coding tools <i>/,ei 'aɪ en'hænst 'kəʊdɪŋ tu:lz/</i>	rén gōng zhì néng fǔ zhù biān chéng gōng jù
 alert fatigue <i>/ə'ɪl:t fə'ti:g/</i>	jǐng bào pí láo
 Anomaly-based <i>/ə'nɒməli beɪst/</i>	jī yú yì cháng
 Anti-malware software <i>/'ænti 'mælweə 'sɒftweə/</i>	fǎn è yì ruǎn jiàn
 Applications <i>/,æplɪ'keɪʃnz/</i>	yìng yòng chéng xù
 ARP poisoning <i>/ɑ:p 'pɔɪzənɪŋ/</i>	dì zhǐ jiě xī tóu dú
 asset <i>/'æset/</i>	zī chǎn

English	Pinyin
 Asymmetric encryption <i>/,eɪsɪ'metrɪk en'krɪptʃn/</i>	fēi duì chèn jiā mì
 at rest <i>/æt rest/</i>	jìng tài shù jù
 authentication <i>/ɔ:,θenti'keɪʃn/</i>	shēn fèn yàn zhèng
 Authority <i>/ə'θɔ:rtɪti/</i>	quán wēi
 automated vulnerability scanner <i>/'ɔ:təmeɪtɪd ,vʌlnərə'bɪlɪti 'skænə/</i>	zì dòng lòu dòng sǎo miáo qì
 autorun <i>/,ɔ:təʊ'rʌn/</i>	zì dòng yùn xíng
 Availability <i>/ə,veɪlə'bɪlɪti/</i>	kě yòng xìng
 Avoid <i>/ə'vɔɪd/</i>	guī bì
 baseline <i>/'beɪslʌɪn/</i>	jī xiàn
 biometric <i>/,baɪəʊ'metrɪk/</i>	shēng wù tè zhēng
 block cipher <i>/blɒk 'saɪfə/</i>	fēn zǔ mì mǎ
 bollards <i>/'bɒlə:dz/</i>	fáng zhuàng zhù
 brute force <i>/bru:t fɔ:s/</i>	bào lì pò jiě
 buffer <i>/'bʌfə/</i>	huǎn chōng qū
 Buffer overflow <i>/'bʌfə ,əʊvə'fləʊ/</i>	huǎn chōng qū yì chū
 Card cloning <i>/kɑ:d 'klɒnɪŋ/</i>	mén jìn kǎ fù zhì
 card readers <i>/kɑ:d 'ri:dəz/</i>	dú kǎ qì
 challenge questions <i>/tʃælɪndʒ 'kwɛstʃnz/</i>	ān quán wèn tí
 CIA triad <i>/,si: aɪ 'ei 'traɪəd/</i>	xìn xī ān quán sān yào sù
 ciphertext <i>/'saɪfətɛkst/</i>	mì wén

English	Pinyin
 clean desk policy <i>/kli:n desk 'pɒlɪsi/</i>	qīng zhuō zhèng cè
 collision resistant <i>/kə'lɪʒn rɪ'zɪstənt/</i>	kàng pèng zhuàng
 complexity <i>/kəm'pleksɪti/</i>	fù zá dù
 compliance <i>/kəm'plaɪəns/</i>	hé guī
 Confidentiality <i>/,kɒnfɪ,dənʃi'æləti/</i>	bǎo mì xìng
 Consensus <i>/kən'sensəs/</i>	cóng zhòng
 corrective <i>/kə'rektɪv/</i>	jiū zhèng xìng
 credential harvesting <i>/kri'denʃl 'hɑ:vɪstɪŋ/</i>	píng jù shōu jí
 credential stuffing <i>/kri'denʃl 'stʌfɪŋ/</i>	zhuàng kù
 Cross-site scripting (XSS) <i>/krɒs saɪt 'skrɪptɪŋ/</i>	kuà zhàn jiǎo běn
 cryptographic hash function <i>/,krɪptə'græfɪk hæʃ 'fʌŋkʃn/</i>	mì mǎ sàn liè hán shù
 Cryptography <i>/krɪp'tɒgrəfi/</i>	mì mǎ xué
 cyberterrorist <i>/'saɪbətərərɪst/</i>	wǎng luò kǒng bù fèn zi
 data loss prevention (DLP) <i>/'deɪtə lɒs pri'venʃn/</i>	shù jù xiè lǒu fáng hù
 Data validation <i>/'deɪtə ,væli'deɪʃn/</i>	shù jù yàn zhèng
 deepfake <i>/'di:pfeɪk/</i>	shēn dù wěi zào
 defense-in-depth <i>/dɪ'fens ɪn depθ/</i>	zòng shēn fáng yù
 denial of service (DoS) <i>/dɪ'naɪəl ɒv 'sɜ:vɪs/</i>	jù jué fú wù
 deprecated <i>/'deprɪkeɪtɪd/</i>	qì yòng

English	Pinyin
 detective <i>/dɪ'tektɪv/</i>	jiǎn cè xìng
 dictionary <i>/'dɪkʃənəri/</i>	zì diǎn
 dictionary attack <i>/'dɪkʃənəri ə'tæk/</i>	zì diǎn gōng jī
 Directory traversal <i>/daɪ'rektəri trævɜ:səl/</i>	mù lù biàn lì
 Discretionary (DAC) <i>/dɪ'skreʃənəri/</i>	zì zhǔ fǎng wèn kòng zhì
 distributed denial of service (DDoS) <i>/'dɪstrɪbjʊ:tɪd dɪ'naɪəl ɒv 'sɜ:vɪs/</i>	fēn bù shì jù jué fú wù
 DMZ <i>/di: ɛm 'zed/</i>	gé lí qū
 DNS poisoning <i>/di: ɛn 'es 'pɔɪzənɪŋ/</i>	yù míng tóu dú
 domain name system (DNS) <i>/də'meɪn neɪm 'sɪstəm/</i>	yù míng xì tǒng
 Dumpster diving <i>/'dʌmpstə 'daɪvɪŋ/</i>	fān lā jī sōu jí qíng bào
 eavesdropping <i>/'i:vzdɹɒpɪŋ/</i>	qiè tīng
 elicitation <i>/ɪ,lɪsɪ'teɪʃn/</i>	tào qǔ xìn xī
 elliptic curve cryptography (ECC) <i>/'ɪlɪptɪk kɜ:v krɪp'tɒgrəfi/</i>	tuǒ yuán qū xiàn mì mǎ xué
 embedded computer <i>/em'bedɪd kəm'pjʊ:tə/</i>	qiàn rù shì jì suàn jī
 encrypted <i>/en'krɪptɪd/</i>	jiā mì de
 endpoint detection and response (EDR) <i>/end'pɔɪnt dɪ'tekʃn ænd rɪ'spɒns/</i>	duān diǎn jiǎn cè yǔ xiǎng yìng
 Evil twin <i>/'i:vl twɪn/</i>	shuāng bāo tāi è yì rè diǎn
 exploits <i>/'eksplɔɪts/</i>	lòu dòng lì yòng

English	Pinyin
 Familiarity	shú xī
<i>/fə,mili'æriti/</i>	
 fileless malware	wú wén jiàn è yì ruǎn jiàn
<i>/'failləs 'mælwəə/</i>	
 firewall	fáng huǒ qiáng
<i>/'faɪəwɔ:l/</i>	
 foothold	lì zú diǎn
<i>/'fʊθəʊld/</i>	
 hacktivist	hēi kè huó dòng fèn zǐ
<i>/'hæktivist/</i>	
 handheld computers	shǒu chí jì suàn jī
<i>/'hændheld kəm'pjʊ:təz/</i>	
 hash	sàn liè zhí
<i>/hæʃ/</i>	
 honeypot	mì guǎn
<i>/'hʌnɪpɒt/</i>	
 host-based firewall	zhǔ jī fáng huǒ qiáng
<i>/'həʊst beɪst 'faɪəwɔ:l/</i>	
 impact	yǐng xiǎng
<i>/'ɪmpækt/</i>	
 impersonate	mào chōng
<i>/'ɪm'pɜ:səneɪt/</i>	
 in transit	chuán shū zhōng shù jù
<i>/'ɪn 'trænsɪt/</i>	
 in use	shǐ yòng zhōng shù jù
<i>/'ɪn ju:s/</i>	
 indicator of compromise (IoC)	rù qīn zhǐ biāo
<i>/'ɪndɪkeɪtə ɒv 'kɒmprəmaɪz/</i>	
 injection attack	zhù rù gōng jī
<i>/'ɪn'dʒekʃn ə'tæk/</i>	
 input sanitization	shū rù qīng lǐ
<i>/'ɪnpʊt ,sænɪtaɪ'zeɪʃn/</i>	
 insider	nèi bù rén yuán
<i>/'ɪn'saɪdə/</i>	
 Integrity	wán zhěng xìng
<i>/'ɪn'tegrti/</i>	
 Internet of Things (IoT)	wù lián wǎng
<i>/'ɪntənət ɒv θɪŋz/</i>	
 Intimidation	kǒng hè
<i>/'ɪn,tɪmɪ'deɪʃn/</i>	

English	Pinyin
 Jamming	gān rǎo gōng jī
<i>/'dʒæmɪŋ/</i>	
 key	mì yào
<i>/ki:/</i>	
 key pair	mì yào duì
<i>/ki: peə/</i>	
 keylogger	jiàn pán jì lù qì
<i>/'ki:lɒgə/</i>	
 keyspace	mì yào kōng jiān
<i>/'ki:speɪs/</i>	
 Large language models (LLMs)	dà yǔ yán mó xíng
<i>/lə:dʒ 'læŋɡwɪdʒ 'mɒdlz/</i>	
 lateral movement	héng xiàng yí dòng
<i>/'lætərəl 'mu:vmənt/</i>	
 likelihood	kě néng xìng
<i>/'laɪklihʊd/</i>	
 lockout	suǒ dǐng
<i>/'lɒkaʊt/</i>	
 log files	rì zhì wén jiàn
<i>/lɒɡ faɪlz/</i>	
 Logic bomb	luó jí zhà dàn
<i>/'lɒdʒɪk bɒm/</i>	
 MAC addresses	wù lǐ dì zhǐ
<i>/mæk ə'dresɪz/</i>	
 MAC flooding	wù lǐ dì zhǐ fàn hóng
<i>/mæk 'flʌdɪŋ/</i>	
 malware	è yì ruǎn jiàn
<i>/'mælwəə/</i>	
 managerial	guǎn lǐ
<i>/'mænə'dʒɪəriəl/</i>	
 Mandatory (MAC)	qiáng zhì fǎng wèn kòng zhì
<i>/'mændətəri/</i>	
 maximum age	zuì zhǎng yǒu xiào qī
<i>/'mæksɪmət əɪdʒ/</i>	
 minimum length	zuì xiǎo cháng dù
<i>/'mɪnɪmət leŋθ/</i>	
 Mitigate	huǎn jiě
<i>/'mɪtɪgeɪt/</i>	
 mitigation	huǎn jiě cuò shī
<i>/'mɪtɪ'geɪʃn/</i>	

English	Pinyin
 motion sensors <i>/ˈməʊʃn ˈsensəz/</i>	yùn dòng chuán gǎn qì
 motivation <i>/ˌməʊtiˈveɪʃn/</i>	dòng jī
 multifactor authentication (MFA) <i>/ˌmʌltɪˈfæktə ɔːθentiˈkeɪʃn/</i>	duō yīn sù shēn fèn yàn zhèng
 network intrusion detection system (NIDS) <i>/ˈnetwɜːk ɪnˈtruːʒn dɪˈtekʃn ˈsɪstəm/</i>	wǎng luò rù qīn jiǎn cè xì tǒng
 network intrusion prevention system (NIPS) <i>/ˈnetwɜːk ɪnˈtruːʒn prɪˈvenʃn ˈsɪstəm/</i>	wǎng luò rù qīn fáng yù xì tǒng
 Network segmentation <i>/ˈnetwɜːk ˌseɡməntˈeɪʃn/</i>	wǎng luò fēn duàn
 network-based indicators of compromise <i>/ˈnetwɜːk beɪst ˈɪndɪkeɪtəz ɒv ˈkɒmprəmaɪz/</i>	wǎng luò rù qīn zhǐ biāo
 on-path attack <i>/ɒn pæθ əˈtæk/</i>	zhōng jiān rén gōng jī
 one-time password (OTP) <i>/wʌn taɪm ˈpæsɜːd/</i>	yí cì xìng mì mǎ
 OSINT <i>/ˈəʊsɪnt/</i>	gōng kāi lái yuán qíng bào
 parameterised queries <i>/ˌpærəˈmetəraɪzd ˈkwɪərɪz/</i>	cān shù huà chá xún
 password attack <i>/ˈpæsɜːd əˈtæk/</i>	mì mǎ gōng jī
 password history <i>/ˈpæsɜːd ˈhɪstəri/</i>	mì mǎ lì shǐ
 password manager <i>/ˈpæsɜːd ˈmænɪdʒə/</i>	mì mǎ guǎn lǐ qì
 password spraying <i>/ˈpæsɜːd ˈspreɪɪŋ/</i>	mì mǎ pēn sǎ
 patch <i>/pætʃ/</i>	bǔ dīng

English	Pinyin
 payment card information (PCI) <i>/ˈpeɪmənt kɑːd ɪnfəˈmeɪʃn/</i>	zhī fù kǎ xìn xī
 personally identifiable information (PII) <i>/ˈpɜːsənəli aɪˈdentɪfaɪəbl ɪnfəˈmeɪʃn/</i>	gè rén shēn fèn xìn xī
 phases <i>/ˈfeɪzɪz/</i>	jiē duàn
 phishing <i>/ˈfɪʃɪŋ/</i>	diào yú
 physical <i>/ˈfɪzɪkl/</i>	wù lǐ
 physical attacks <i>/ˈfɪzɪkl əˈtæks/</i>	wù lǐ gōng jī
 Piggybacking () <i>/ˈpɪɡɪbækɪŋ/</i>	wěi suí (huò xǔ kě)
 plaintext <i>/ˈpleɪntekst/</i>	míng wén
 points of ingress and egress <i>/ˈpɔɪnts ɒv ˈɪŋɡres ænd iːˈɡres/</i>	chū rù kǒu
 pre-image resistance <i>/priː ˈɪmɪdʒ rɪˈzɪstəns/</i>	kàng yuán xiàng
 Pretexting <i>/ˈpriːtekstɪŋ/</i>	jiè kǒu
 preventative <i>/priˈventətɪv/</i>	yù fáng xìng
 principle of least privilege <i>/ˈprɪnsɪpl ɒv liːst ˈprɪvɪlɪdʒ/</i>	zuì xiǎo quán xiàn yuán zé
 private key <i>/ˈpraɪvət kiː/</i>	sī yào
 probabilistic <i>/ˌprɒbəbɪˈlɪstɪk/</i>	gài lǚ de
 protected health information (PHI) <i>/prəˈtektɪd helθ ɪnfəˈmeɪʃn/</i>	shòu bǎo hù jiàn kāng xìn xī
 public key <i>/ˈpʌblɪk kiː/</i>	gōng yào
 qualitative <i>/ˈkwɒlɪteɪtɪv/</i>	dìng xìng

English	Pinyin
 quantitative <i>/ˈkwɒntɪteɪtv/</i>	dìng liàng
 rainbow table <i>/ˈreɪnbəʊ ˈteɪbl/</i>	cǎi hóng biǎo
 RAM <i>/ræm/</i>	nèi cún
 Ransomware <i>/ˈrænsəmweə/</i>	lè suǒ ruǎn jiàn
 reconnaissance <i>/rɪˈkɒnɪsəns/</i>	zhēn chá
 regulated <i>/ˈregjuleɪtɪd/</i>	shòu jiān guǎn
 remote access trojan (RAT) <i>/rɪˈməʊt ˈækses ˈtrəʊdʒn/</i>	yuǎn chéng fǎng wèn mù mǎ
 residual risk <i>/rɪˈsɪdʒuəl rɪsk/</i>	shèng yú fēng xiǎn
 risk <i>/rɪsk/</i>	fēng xiǎn
 risk assessment <i>/rɪsk əˈsesmənt/</i>	fēng xiǎn píng gū
 rogue access point <i>/rəʊg ˈækses pɔɪnt/</i>	fēi fǎ jiē rù diǎn
 Role-based (RBAC) <i>/rəʊl beɪst/</i>	jī yú jué sè de fǎng wèn kòng zhì
 Rule-based (RuBAC) <i>/ru:l beɪst/</i>	jī yú guī zé de fǎng wèn kòng zhì
 salt <i>/sɒlt/</i>	yán zhí
 Scarcity <i>/ˈskeəsɪti/</i>	xī quē
 screened subnet <i>/skri:nd ˈsəbnet/</i>	píng bì zì wǎng
 script kiddie <i>/skript ˈkɪdi/</i>	jiǎo běn xiǎo zi
 Secure by default <i>/sɪˈkjʊə baɪ dɪˈfɒlt/</i>	mò rèn ān quán
 Secure by design <i>/sɪˈkjʊə baɪ dɪˈzain/</i>	ān quán shè jì

English	Pinyin
 security information and event management (SIEM) <i>/sɪˈkjʊəɪtɪ ,ɪnfəˈmeɪʃn ænd ɪˈvent ˈmænɪdʒmənt/</i>	ān quán xìn xī yǔ shì jiàn guǎn lǐ
 severity <i>/səˈverɪti/</i>	yán zhòng xìng
 shared secret <i>/ʃeəd ˈsi:kɪt/</i>	gòng xiǎng mì mì
 Shoulder surfing <i>/ʃəʊldə ˈsɜ:fɪŋ/</i>	jiān kuī
 Signature-based <i>/ˈsɪɡnɪtʃə beɪst/</i>	jī yú tè zhēng
 Social engineering <i>/ˈsəʊʃl ,endʒɪˈniəriŋ/</i>	shè huì gōng chéng xué
 special characters <i>/ˈspeʃl ˈkærɪktəz/</i>	tè shū zì fú
 split tunneling <i>/splɪt ˈtʌnəlɪŋ/</i>	fēn lí suì dào
 Spyware <i>/ˈspaɪweə/</i>	jiàn dié ruǎn jiàn
 SQL injection <i>/es kjʊ: ˈel mˈdʒekʃn/</i>	SQL zhù rù
 SSID <i>/es es aɪ ˈdi:/</i>	fú wù jí biāo shí fú
 Stateful <i>/ˈsteɪtfl/</i>	yǒu zhuàng tài
 Stateless <i>/ˈsteɪtləs/</i>	wú zhuàng tài
 subnets <i>/ˈsəbnets/</i>	zì wǎng
 switch <i>/swɪtʃ/</i>	jiāo huàn jī
 Symmetric encryption <i>/sɪˈmetrɪk enˈkrɪpʃn/</i>	duì chèn jiā mì
 Tailgating <i>/ˈteɪlɡetɪŋ/</i>	() wěi suí (wèi chá jué)
 technical <i>/ˈteknɪkl/</i>	jì shù
 threat <i>/θret/</i>	wēi xié

English	Pinyin
 threat detection and response <i>/θret dɪ'tekʃn ænd rɪ'spɒns/</i>	wēi xié jiǎn cè yǔ xiǎng yìng
 threshold <i>/'θreʃəʊld/</i>	yù zhí
 Transfer <i>/'trænsfɜː/</i>	zhuǎn yí
 transnational criminal organisations <i>/træn'snæʃənl 'krɪmɪnl ɔːgənaɪ'zeɪʃnz/</i>	kuà guó fàn zuì zǔ zhī
 Trojan <i>/'trɒdʒn/</i>	mù mǎ
 uninterruptible power supply (UPS) <i>/ˌʌnɪntə'rʌptɪbl 'paʊə sə'plai/</i>	bù jiàn duàn diàn yuán
 unpatched software <i>/ʌn'pætʃt 'sɒftweə/</i>	wèi dǎ bǔ dīng de ruǎn jiàn
 Urgency <i>/'ʊːdʒənsi/</i>	jǐn pò gǎn
 virtual private network (VPN) <i>/'vɜːtʃuːəl 'praɪvət 'netwɜːk/</i>	xū nǐ zhuān yòng wǎng luò
 Virus <i>/'vaɪrəs/</i>	bìng dú
 VLANs <i>/'viːlənz/</i>	xū nǐ jú yù wǎng
 vulnerability <i>/ˌvʌlnərə'bɪlɪti/</i>	lòu dòng
 War driving <i>/wɔː 'draɪvɪŋ/</i>	zhàn zhēng jià shǐ
 weak <i>/wiːk/</i>	ruò
 Worm <i>/wɜːm/</i>	rú chóng
 WPA3 <i>/ˌdʌbljuː piː eɪ 'θriː/</i>	Wi-Fi bǎo hù jiē rù dì sān dài
 zero days <i>/'ziərəʊ deɪz/</i>	líng rì lòu dòng