

Secure Programming

Mehmet Tahir SANDIKKAYA

Spring 2022

Istanbul Technical University
Computer Engineering Department

Bilingual Glossary	2
Glossary	3

Glossary

ABE	Özellik tabanlı şifreleme
Access control	Erişim denetimi
Accountability	Sorumlu tutulabilirlik
Accuracy	Doğruluk
Agreement	Uzlaşma
Aliveness	Canlılık
Assessment	Değerlendirme
Asset	Varlık
Atomicity	Bölünmezlik
Attack	Saldırı
Auditability	Denetlenebilirlik
Authentication	Asıllama
Authorization	Yetkilendirme

Mehmet Tahir SANDIKKAYA

Istanbul Tech. – 3 / 18

Glossary

Availability	Yararlanırlık
Backup	Yedek
Blockchain	Blok zinciri
Breach	(Güvenlik) Yarı(-ğı)
Bulletin Board	Bildiri tahtası
Byzantine Quorum	Bizans yetersayı kümesi
Canonical Name	Asal ad
Canonicalization	Asallaştırma
Capacity	Sığa
Cipher	Şifre dizgesi
Class loader	Sınıf yükleyici
Cloud computing	Bulut bilgiişlem
Cluster computing	Öbekte bilgiişlem

Mehmet Tahir SANDIKKAYA

Istanbul Tech. – 4 / 18

Glossary

Coherency	Uyumluluk
Command-mode error	Ortaklaşa hata
Commitment	Güvence
Compatibility	Uygunluk
Completeness	Tamlık
Compromised	Kötüleşmiş
Concurrency	Dönemdeşlik
Confidentiality	Gizdeşlik
Congruent	Kalandaş
Consensus	Oydaşım
Consistency	Çelişkisizlik
Container	Taşıyıcı
Cross validation	Çapraz geçerleme

Glossary

Cryptanalysis	Şifreçözümleme
Cryptography	Şifreyazım
Cryptology	Şifrebilim
Cryptosystem	Şifre dizgesi
DHM	Diffie–Hellman–Merkle
DLP	Veri kaybı engelleme
Decryption	Şifre çözme
Dependability	Belbağlanırlık
Distributed computing	Dağıtık bilgiişlem
Diversity	Çeşitlilik
Dividend	Bölünen
Divisor	Bölen
DoS	Hizmet engelleme saldırısı

Glossary

Durability	Dayanıklılık
Eavesdropping	Gizlice dinleme
EDS	Araklama belirleme dizgesi
EPS	Araklama engelleme dizgesi
Edge computing	Ağ sınırında bilgiişlem
Efficiency	Verimlilik
Emulation	Öykünüm
Encapsulation	Kozalama
Encryption	Şifreleme
Enforcement	Dayatma
Error tolerance	Hata hoşgörüsü
Error	Hata
Evaluation	Değerleme

Glossary

Evidence	İpucu
Exception	Olağandışı durum
Exfiltration	Tahliye
Exploit	Kötüye kullanma, suiistimal
Extrusion	Araklama
FHE	Tamamıyla aynıyapılı şifreleme
Fairness	Hakçalık
Fault tolerance	Arıza hoşgörüsü
Fault	Arıza
Fencing	Çitleme
Firewall	Güvenlik duvarı
Fog computing	Seyrek dağıtık bilgiişlem
Formal verification	Biçimsel doğrulama

Glossary

Grid computing	Örgüde bilgiişlem
Hash	Öz
Homomorphic	Aynıyapılı
Honest-but-curious	Dürüst ancak meraklı
Honeypot	Korsan tuzağı
Hypervisor	Yukarıdan izleyici
IBE	Kimlik tabanlı şifreleme
IDS	İstila belirleme dizgesi
IPS	İstila engelleme dizgesi
IaaS	Sanal bilgisayar sunan bulut
Identity verification	Kimlik doğrulama
Impersonation	Taklit etme
Indistinguishability	Ayrımsanamazlık

Glossary

Injective	Bire bir
Integrity	Bütünlük
Internet of Things	Nesnelerin interneti
Intrusion	İstila
Isolation	Yalıtım
Lateral movement	Yanal hareket
Leakage	Sızma
Least astonishment	En az şaşırtıcı
Liability	Yükümlülük
Limitation	Sınırlama
Load balancing	Yük dengeleme
Locality	Yöresellik
Logging	Günlük tutma

Glossary

Log	Günlük
MAC	ileti asıllama kodu
Maintainability	Bakım kolaylığı
Masquerade	Kılık değiştirme
Measure	Önlem
Mechanism	Düzenek
Message authentication	İleti asıllama
Metadata	Üstveri
Migration	Göç
Minimization	En aza indirme
Mitigation	Etkisini azaltma
MitM	Araya girme
Mixnet	Karıştırılmış ağ

Glossary

Model checking	Model yoklama
Modularity	Birimsellik
Negotiation	Pazarlık
Non-repudiability	Yadsınamazlık
Obfuscation	Perdeleme
Oblivious	İlgisiz
Obscurity	Karartma
Onion routing	Soğan ağ
Openness	Saydamlık
P-code	Taşınabilir kod
PaaS	Bilgişlem ortamı sunan bulut
Penetration	Delme
Performance	Başarım

Glossary

Perimeter	Sınır
Permission	İzin
Phishing	Alık avlama
Policy enforcement point	İlke dayatma noktası
Policy	İlke
Precision	Hassaslık
Privacy	Özlük gizdeşliği
Private data	Özlük bilgileri
Privilege escalation	Ayrıcalık yükseltme
Process VM	Süreç sanal makinası
Proof	Tanıt
Protection domain	Koruma uzayı
Protection	Koruma

Glossary

Pseudonym	Mahlas, takma ad
Pwn	Teslim olma
Quotient	Bölüm
RSA	Rivest–Shamir–Adleman
Rapid Recovery	Hızlı atlatma
Recentness	Tazelik
Reconnaissance	Keşif
Redundancy	Artıklık
Reference monitor	Referans gözleyici
Reliability	Beklenirlik, güvenilirlik
Remainder	Kalan
Repairability	Onarılabilirlik
Replay	Tekrar

Glossary

Replication	Yineleme
Resiliency	Toparlanma, derlenme
Resolution	Çözünürlük
Resource pool	Kaynak havuzu
Resourcefulness	Zengin kaynaklılık
Responsibility	Sorumluluk
Robustness	Sağlamlık, gürbüzlük
SFE	Güvenli işlev değerlendirme
SLA	Hizmet sözleşmesi
SOA	Hizmet odaklı mimari
SaaS	Hazır yazılım sunan bulut
Safety	Canyakmazlık
Salting	Tuzlama

Glossary

Scalability	Ölçeklenebilirlik
Secrecy	Gizlilik
Security	Güvenlik
Sensitive data	Hassas veri
Service	Hizmet
Shared resource pool	Paylaşılan kaynak havuzu
Simulation	Benzetim
Single point of failure	Can alıcı arıza noktası
Single sign on	Tek seferde çok oturum açma
Soundness	Tutarlılık
Spatiality	Yöresellik
Sticky policy	İlişik ilke
Survivability	Kalımlılık

Glossary

System VM	(Dizge) sanal makina(sı)
System	Dizge
Tamper-proof	Kurcalamaya dayanıklı
Temporality	Zamansallık
Test	Sinama
Theorem	Teorem
Theory	Teori
Threat	Tehdit
Token	Andıç
Trustworthiness	Güvenilirlik, Sözde dururluk
Trust	Güven
Undeniability	Yadsınamazlık
Usability	Kullanışlılık

Glossary

Utilization	Yararlanım
VMM	Sanal makina izleyici
Validation	Geçerleme
Verification	Doğrulama
Violation	İhlal
Vulnerability	(Güvenlik) açık(-ğı)
Weakness	(Güvenlik) zayıflık(-ğı)