

BİLİŞİM GÜVENLİĞİ TERİMLERİ

Sunuş

Bilişim güvenliği konusunun Türkiye’de daha geniş kitlelere anlatılmasının, bu konuda Türkiye’de ve Türkçe yayın yapılmasının önemli gereksinimlerinden birisidir bu alanda üzerinde uzlaşmış bir terim kümesi olduğu açıktır. Bu çalışma, bu eksikliği gidermeye yönelik bir başlangıç oluşturmayı hedeflemektedir.

Bu metnin akademik bir çalışma sunuşu olmadığını, teknik uzman bakış açısı ve bilgileri doğrultusunda hazırlandığını hatırla tutmanız ve değerlendirmenizi bu çerçevede gerçekleştirmeniz uygun olacaktır.

Katkı ve önerilerinizi dayioglu@metu.edu.tr adresinden e-posta yolu ile benimle paylaşabilirsiniz.

Terimler

Olay	Event
Bir hedefe yönlendirilmiş ve sonuçta hedefin durumunu değiştirmeyi amaçlayan eylem.	
An action directed at a target which is intended to result in a change of state (status) of the target.	
IEEE96	

Eylem	Action
Bir kullanıcı ya da süreç tarafından bir sonuca ulaşmak amacıyla atılan adım.	
A step taken by a user or process in order to achieve a result.	
IEEE96	

Hedef	Target
Bir bilgisayar, mantıksal ağ varlığı (hesap, süreç ya da veri) ya da fiziksel varlık (bileşen, bilgisayar, ağ ya da ağlar ağı).	
A computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).	
HL1998	

Yoklama	Probe
Karakteristik özelliklerini belirlemek üzere bir hedefe erişim.	
Access a target in order to determine its characteristics.	
HL1998	

Tarama	Scan
Hangilerinin belirli karakteristiğe sahip olduğunu görmek üzere bir hedef kümesine sıra ile erişim.	
Access a set of targets sequentially in order to identify which targets have a specific	

characteristic.

JAH92

Sel

Flood

Kapasitesinin sınırını zorlamak amacı ile bir hedefe sık, ardışık erişim.

Access a target repeatedly in order to overload the target's capacity.

HL1998

Atlatma

Bypass

Bir hedefe erişim için alternatif bir yöntem izleyerek bir süreci geçersiz kılma.

Avoid a process by using an alternative method to access a target.

MEW96

Şaşırtma

Spoof

Ağ iletişimde kendisini başka bir varlık olarak göstererek saklanma.

Masquerade by assuming the appearance of a different entity in network communications.

ABH96

Hesap

Account

Bir bilgisayar ya da ağ üzerinde, hesap adı, parolası ve kullanım kısıtları gibi bilgiler içeren kullanıcı erişim alanı kaydı.

A domain of user access on a computer or network which is controlled according to a record of information which contains the user's account name, password and use restrictions.

HL1998

Süreç

Process

Programın çalıştırılabilir halini, verilerini, yığıtını, program sayacını, yığıt göstergesini ve diğer yazmaçlarını içeren bütün halinde çalışır durumdaki bir program.

A program in execution, consisting of the executable program, the program's data and stack, its program counter, stack pointer and other registers, and all other information needed to execute the program.

TAN92

Veri

Data

İnsanlar tarafından ya da otomatikleştirilmiş yollarla gerçeklerin, kavramların ya da işlem adımlarının iletişim, yorumlama ve işlenmeye hazır haldeki gösterimi.

Representations of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.

IEEE96

Bileşen

Component

Bir bilgisayarı ya da bir ağı oluşturan parçalardan birisi.

One of the parts that make up a computer or network.

IEEE96

Saldırı

Attack

Yetkisiz biçimde bir takım sonuçlara ulaşmak amacıyla bir saldırgan tarafından gerçekleştirilen bir dizi adım.

A series of steps taken by an attacker to achieve an unauthorized result.

HL1998

Yetkilendirilmiş

Authorized

Sahibi ya da yöneticisi tarafından onaylanmış.

Approved by the owner or administrator.

HL1998

Yetkilendirilmemiş

Unauthorized

Sahibi ya da yöneticisi tarafından onaylanmamış.

Not approved by the owner or administrator.

HL1998

Araç Takımı

Toolkit

Betikler, programlar ve bağımsız ajanlardan oluşan ve zayıflıklardan faydalanmak üzere derlenmiş yazılım paketi. Yaygın biçimde görülen *rootkit*'ler araç takımına bir örnektir.

A software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities. An example is the widely available toolkit called rootkit.

HL1998

Dağıtık Araç

Distributed Tool

Birden çok bilgisayar sistemine dağıtılabilen ve daha sonra tüm sistemlerden tek bir hedefe koordineli bir saldırı gerçekleştirmek için kullanılan, saldırganın kimliğinin de gizlenebildiği araç.

A tool that can be distributed to multiple hosts, which can then be coordinated to anonymously perform an attack on the target host simultaneously after some time delay.

HL1998

Zayıflık

Vulnerability

Bir sistemde yetkilendirilmemiş eylemlere izin veren zaafiyet.

A weakness in a system allowing unauthorized action.

NRC91

Tasarım Zayıflığı

Design vulnerability

Mükemmel bir uygulamanın bile önleyemediği, bir donanımın ya da yazılımın tasarımına ya da belirtimine ilişkin zayıflık.

A vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability

HL1998

Uygulama Zayıflığı

Implementation vulnerability

Tatminkar bir tasarıma sahip yazılım ya da donanımın uygulanması ya da gerçekleştirimi sırasında yapılan bir hatadan kaynaklanan zayıflık.

A vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.

HL1998

Yapılandırma Zayıflığı

Configuration vulnerability

Sistemin yapılandırmasındaki bir hatadan kaynaklanan zayıflık. Sistem hesaplarının öntanımlı parolaları ile bırakılması, yeni dosyalara “herkes-yazabilir” izni ile açılması ya da zayıf hizmetlerin aktif hale getirilmesi yapılandırma zayıflıklarına birer örnektir.

A vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having “world write” permission for new files, or having vulnerable services enabled.

ABH96

Bilginin Açığa Vurulması

Disclosure of Information

Bilginin erişmek için yetkilendirilmemiş herhangi birisine ulaşması.

Dissemination of information to anyone who is not authorized to access that information.

HL1998

Bilginin Bozulması

Corruption of Information

Bir bilgisayar ya da ağ üzerindeki verilerin yetkilendirilmeden değiştirilmesi.

Unauthorized alteration of data on a computer or network.

HL1998

Hizmet Aksatma

Denial of Service

Sistem kaynaklarına yetkilendirilmiş erişimlerin engellenmesi ya da sistem işleyişinin yavaşlatılması.

The prevention of authorized access to a system resource or the delaying of system operations and functions.

SHI2000

Olay

Incident

Saldırganların, saldırıların, amaçların, sitelerin ve zamanlamanın farklılığı nedeniyle diğer saldırılardan ayırt edilebilen bir saldırı grubu.

A group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.

HL1998

Saldırgan

Attacker

Bir amaca ulaşabilmek üzere bir ya da daha fazla saldırıyı deneyen birey

An individual who attempts one or more attacks in order to achieve an objective

HL1998

Amaç

Objective

Bir olayın gerekçesi ya da nihai hedefi.

The purpose or end goal of an incident.

HL1998

Çalma

Steal

Bir kopyasını kaynak yerinde bırakmadan bir hedefin denetimini ele geçirme

Take possession of a target without leaving a copy in the original location

HL1998

Saldırı

Intrusion

Bir kaynağın bütünlüğünü, gizliliğini ya da bulunurluğunu bozmayı hedefleyen her türlü eylem.

Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

HEA1990

Saldırı Tespiti

Intrusion Detection

Yetkilendirilmemiş biçimde bilgisayar sistemlerini kullanmaya çalışan bireyleri (kullanıcılar ya da otomatik saldırganlar) ya da erişim hakkına sahip olan ancak yetkilerini kötüye kullanmaya çalışan bireyleri tespit etme.

identifying individuals (users or automated attackers) who are using or attempting to use the computer system without authorization or who have legitimate access but are attempting to abuse their privileges.

MUK1994

Koordineli Saldırı

Coordinated Attack

Saldırının bütünlük doğasını gizlemek ve daha hızlı ilerlemek adına, paralel oturumlar kullanma ve bir patlatmanın birden çok adıma bölünerek gerçekleştirilmesi.

Coordinated attacks are multi-step exploitations using parallel sessions where the distribution of steps between sessions is designed to obscure the unified nature of the attack to proceed more quickly

CHE1996

Patlatma

Exploit

Sistemdeki bir zayıflıktan faydalanarak, bir biçimde, bir amacı gerçekleştirmeye çalışmak.

To, in some way, take advantage of a vulnerability in a system in the pursuit or achievement of some objective.

ALL2000

Bütünlük

Integrity

Yetkilendirilmemiş biçimde ya da kaza ile verilerin değiştirilmediğini, yok edilmediğini ya da kaybedilmediğini gösteren nitelik.

The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

SHI2000

Mahremiyet

Confidentiality

Bilgilerin yetkilendirilmemiş kişiler, varlıklar ya da süreçlerce erişilemez olmasını sağlayan nitelik.

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity).

ISO7498

Bulunurluk

Availability

Bilgi ve iletişim hizmetlerinin gerektiği anda çalışır durumda olmasının sağlanması.

Assuring information and communications services will be ready for use when expected.

FDA2001

Anormallik

Anomaly

Normalden ya da sıradandan farklılık gösteren ve bu nedenle tatminkar olmayan bir kural ya da işlem.

An anomaly is a rule or practice that is different from what is normal or usual, and which is therefore unsatisfactory.

ANSI1991

Sınır Değer

Boundary Value

Bir sistem ya da bileşen için tanımlanmış en küçük ya da en büyük girdi ya da çıktı değeri.

A data value that corresponds to a minimum or maximum input, internal, or output value specified for a system or component.

ANSI1991

Alan Taşırma

Buffer Overflow

Bu durum, bir alana taşıyabileceğinden daha fazla verinin konması durumunda gerçekleşir. Sistem çökmesine ya da bir arka kapı oluşması yolu ile sistem erişimine yol açabilir.

This happens when more data is put into a buffer or holding area, then the buffer can handle. This can result in system crashes or the creation of a back door leading to system access.

FDA2001

Hata	Bug
Bir programın beklenmedik ya da istenmeyen biçimde davranmasına neden olan arıza.	
A fault in a program which causes the program to perform in an unintended or unanticipated manner.	
FDA2001	

Yanlış negatif	False Negative
Bir saldırının parçası olarak gerçekleştirilen adımlarının hiç birisinin anormallik olarak sınıflandırılmaması durumu.	
Occurs when none of the sequences generated by an intrusion are classified as anomalous.	
HOF2000	

Yanlış pozitif	False Positive
Geçerli ve makul bir davranışa ilişkin bir adımın anormal olarak sınıflandırılması durumu.	
Occurs when a single sequence generated by legitimate behavior is classified as anomalous.	
HOF2000	

Sızma	Penetration
Bir sistemin güvenlik mekanizmalarının başarı ile atlatılması.	
The successful act of bypassing the security mechanisms of a system.	
NCSC2000	

Sızma Denemesi	Penetration Testing
Güvenlik sınavasının bir parçası olarak değerlendiricilerin bir sistemin güvenlik özelliklerini atlatmaya çalışmasıdır. Değerlendirmeyi yapanların kaynak kodlar da dahil olmak üzere tüm sistem tasarım ve gerçekleştirim belgelerine, kullanım kılavuzlarına ve devre şemalarına sahip olduğu varsayılır. Değerlendiriciler, atlatma girişimlerine sıradan bir kullanıcının yetkileri ile başlarlar.	
The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.	
NCSC2000	

Risk	Risk
Belirli bir tehditin sistemin belirli bir zayıflığından faydalanarak sisteme zarar verme ihtimali.	
The probability that a particular threat will exploit a particular vulnerability of the system.	
NCSC2000	

Arta Kalan Risk	Residual Risk
Güvenlik önlemleri uygulandıktan sonra kalan risk bölümü.	

The portion of risk that remains after security measures have been applied.

NCSC2000

Risk Analizi

Risk Analysis

Güvenlik risklerinin, bu risklerin ölçüklerinin ve önlem alınması gereken alanların belirlenmesi süreci.

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

NCSC2000

Risk Yönetimi

Risk Management

Sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreç. Risk analizi, fayda-maliyet analizi, seçim, gerçekleştirim, sına, önlemlerin güvenlik değerlendirmesi ve komple güvenlik gözden geçirmesini içerir.

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

NCSC2000

Güvenlik

Security

Art niyetli eylemlerden ve etkilerinden korunmak üzere alınan ve sürdürülen koruyucu önlemlerin sonucunda oluşan durum.

A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

FDA2001

Güvenlik Değerlendirmesi

Security Evaluation

Hassas bilgilerin işlenmesinde kullanılan sistemlerin güvenilirlik düzeyini değerlendirme ve belirleme işlemi.

An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information.

NCSC2000

Kurt

Worm

Bağımsız olarak çalışabilen, işler durumdaki kopyalarını ağ üzerindeki başka bilgisayarlara aktarabilen ve zarar verecek biçimde sistem kaynaklarını tüketen bilgisayar programı.

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

SHI2000

Erişim

Access

Bilgiyi işlemek ya da bir sistem tarafından işlenen bilgiyi edinmek üzere bir sistem ile etkileşime ya da etkileşime geçme becerisi ve yöntemi.

The ability and means to communicate with or otherwise interact with a system in order to use system resources to either handle information or gain knowledge of the information the system contains.

SHI2000

Erişim Denetimi

Access Control

Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.

SHI2000

Erişim Denetim Listesi

Access Control List

Erişime izinli sistem varlıklarının kimliklerinin listelenmesi yolu ile bir sistem kaynağına erişimi sağlayan mekanizma.

A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resource.

SHI2000

Accountability

The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions.

SHI2000

Anonim

Anonymous

Bilinmeyen ya da gizlenmiş bir isim taşıma durumu.

The condition of having a name that is unknown or concealed.

SHI2000

Asimetrik Şifreleme

Asymmetric cryptography

İki farklı anahtarın söz konusu olduğu (açık ve gizli anahtar), algoritmanın farklı adımlarında anahtarların değişmeli kullanıldığı modern bir şifreleme dalıdır.

A modern branch of cryptography (popularly known as "public-key cryptography") in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

SHI2000

Doğrulama

Authenticate

Verify (i.e., establish the truth of) an identity claimed by or for a system entity.

SHI2000

Zayıflık İncelemesi

Vulnerability Assessment

A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

NCSC2000

Yetkilendirme

Authorization

An "authorization" is a right or a permission that is granted to a system entity to access a system resource.

SHI2000

Arka Kapı

Back door

Sistem ve sistem kaynaklarına sıradan prosedür dışında bir yöntem ile ulaşılmasını sağlayan, sistem tasarımcıları ya da işletmenleri tarafından bilerek bırakılmış olan ya da kamunun yaygın bilgisi dahilinde olmayan yazılım ya da donanım mekanizması.

A hardware or software mechanism that (a) provides access to a system and its resources by other than the usual procedure, (b) was deliberately left in place by the system's designers or maintainers, and (c) usually is not publicly known.

SHI2000

Bastion Host

A strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the other side of the firewall.

SHI2000

Capability

A token, usually an unforgeable data value (sometimes called a "ticket") that gives the bearer or holder the right to access a system resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource named or indicated by the token.

SHI2000

Challenge-response

An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication

information is usually a value that is required to be computed in response to an unpredictable challenge value.

SHI2000

Denetim Toplamı

Checksum

A value that (a) is computed by a function that is dependent on the contents of a data object and (b) is stored or transmitted together with the object, for the purpose of detecting changes in the data.

SHI2000

Ciphertext

Data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available.

SHI2000

Cleartext / Plaintext

Data in which the semantic information content (i.e., the meaning) is intelligible or is directly available.

SHI2000

Compartment

A grouping of sensitive information items that require special access controls beyond those normally provided for the basic classification level of the information.

SHI2000

Bilgisayar Acil Durum Müdahale Ekibi

Computer Emergency Response Team

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

SHI2000

Computer Security Incident Response Team

An organization "that coordinates and supports the response to security incidents that involve sites within a defined constituency.

BG1998

Beklenmedik Durum Planı	Contingency Plan
A plan for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis.	
NCSC2000	

Çerez	Cookie
Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.	
SHI2000	

Doğruluk Kanıtı	Correctness Proof
A mathematical proof of consistency between a specification for system security and the implementation of that specification.	
SHI2000	

Karşı Tedbir	Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.	
SHI2000	

	Covert Channel
A intra-system channel that permits two cooperating entities, without exceeding their access authorizations, to transfer information in a way that violates the system's security policy.	
SHI2000	

	Credential
Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity.	
SHI2000	

	Cryptanalysis
The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide.	

SHI2000

Cryptography

The mathematical science that deals with transforming data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form.

SHI2000

Ön-Tanımlı Hesap

Default Account

A system login account (usually accessed with a user name and password) that has been predefined in a manufactured system to permit initial access when the system is first put into service.

SHI2000

Sözlük Saldırısı

Dictionary Attack

An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

SHI2000

Sayısal İmza

Digital Signature

A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

SHI2000

Dizin

Directory

A database server or other system that provides information.

SHI2000

Discretionary Access Control

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

DOD1985

İhlal

Breach

The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

FDA2001

Kaba kuvvet saldırısı

Brute force attack

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

SHI2000

Compromise

A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

NCSC2000

Tehdit

Threat

Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

NCSC2000

Tehdit Analizi

Threat Analysis

The examination of all actions and events that might adversely affect a system or operation.

NCSC2000

Truva Atı

Trojan Horse

Kullanışlı ve masum görünen, ancak yetkisiz veri toplama, değiştirme ve yok etmeye izin veren gizli program parçaları taşıyan program.

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

FDA2001

Formal Specification

A specification of hardware or software functionality in a computer-readable language; usually a precise mathematical description of the behavior of the system with the aim of providing a correctness proof.

SHI2000

Tanımlama	Identification

İzin	Permission

	Single Point of Failure

	De-Militarized Zone (DMZ)

	System High

Çok-Katmanlı Savunma	Multi-Level Security

Savunma Derinliği	Defense in Depth

Turuncu Kitap	Orange Book

Açık Anahtar Altyapısı	Public-Key Infrastructure

Gizlilik	Privacy

Güvenlik Duvarı

Firewall

Hassas Bilgi

Sensitive Information

Boundary Protection Device

Referanslar

- [HL1998] J. D. Howard and T. A. Longstaff, A Common Language for Computer Security Incidents, Sandia Report 98-8667, Sandia National Laboratories, October 1998.
- [ABH96] D. Atkins, P. Buis, C. Hare et. al., Internet Security Professional Reference, New Riders Publishing, IN, 1996.
- [NRC91] National Research Council, Computers at Risk: Safe Computing in the Information Age, National Academy Press, Washington, DC, 1991.
- [IEEE96] IEEE, The IEEE Standard Dictionary of Electrical and Electronics Terms, Sixth Edition, John Radatz, Editor, Institute of Electrical and Electronics Engineers, Inc., New York, NY, 1996.
- [TAN92] A. S. Tanenbaum, Modern Operating Systems, Prentice Hall, Englewood Cliffs, NJ, 1992.
- [JAH92] K. Jackson and J. Hruska, Computer Security Reference Book, CRC Press, Inc., Boca Raton, FL, 1992.
- [MEW96] MWI Inc., Merriam-Webster's Collegiate Dictionary, Tenth Edition, Merriam-Webster, Incorporated, Springfield, MA, 1996.
- [HEA1990] R. Heady et. al., The Architecture of a Network Level Intrusion Detection System, Technical Report, University of New Mexico, Department of Computer Science, 1990.
- [MUK1994] B. Mukherjee et. al., Network Intrusion Detection, IEEE Network, No. 3(8), pp. 26-41, 1994.
- [CHE1996] S. Staniford-Chen et. al., GrIDS: A Graph Based Intrusion Detection System for Large Networks, In Proceedings of the 19th National Information Systems Security Conference, pages 361-370, 1996.
- [ALL2000] Julia Allen, Alan Christie, William Fithen, John McHugh, Jed Pickel, Ed Stoner. (2000). "State of the Practice of Intrusion Detection Technologies". <http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028title.html>.
- [FDA2001] Glossary of computerized system and software development terminology, Food and Drug Administration. http://www.fda.gov/ora/inspect_ref/igs/gloss.html.
- [ANSI1991] Standard Glossary of Software Engineering Terminology, ANSI 1991
- [SHI2000] R. Shirey. (2000). "Internet Security Glossary". The Internet Society. <http://www.ietf.org/rfc/rfc2828.txt>.
- [NCSC2000] Glossary of Computer Security Terms, <http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt>.
- [BG1998] Brownlee, N. and E. Guttman, Expectations for Computer Security Incident Response, RFC 2350, June 1998.
- [HOF2000] S. Hofmeyr et. al., Lightweight Intrusion Detection for Networked Operating Systems, Draft Paper, Department of Computer Science, University of New Mexico, 2000.
- [ISO7498] Information Processing Systems--Open Systems Interconnection Reference Model--[Part 1:] Basic Reference Model, ISO/IEC 7498-1.
- [DOD1985] U.S. Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Dec 1985.

Criteria, DoD 5200.28-STD, 26 Dec 1985.

Teşekkürler

Bu çalışmaya aşğıdaki isim ve e-posta adresleri yazılı kişiler yorum ve önerileri ile katkı sağlamıştır; hepsine bu çalışmaya verdikleri desteklerinden ötürü teşekkürlerimi sunarım¹:

Can ALPTEKİN	can@olimpos-it.com
Korhan GÜRLER	korhan@netkeyfi.com
Muzaffer ÖZAKÇA	muzaffer.ozakca@bilten.metu.edu.tr
Fatih ÖZAVCI	holden@siyahsapka.com
Önder ÖZDEMİR	oozdemir@tepeteknoloji.com.tr
Burç YILDIRIM	burc@olimpos-it.com

¹ İsimler soyadı harf sırası ile verilmiştir.