
BY AMY FRIEDLANDER, ALLISON MANKIN,
W. DOUGLAS MAUGHAN, AND STEPHEN D. CROCKER

DNSSEC: A PROTOCOL TOWARD SECURING THE INTERNET INFRASTRUCTURE

*DNSSEC is properly understood as a component in an ecology of
security protocols and measures.*



Asked about their security concerns on the Internet, most end users in the U.S. cite privacy and data confidentiality [6]. Experts, however, have substantially different views. A 2004 survey of technology leaders by the Pew Internet & American Life Project found that respondents found these experts were seriously concerned about infrastructure; 66% of them agreed with the statement: “At least one devastating attack will occur in the next 10 years on the networked information infrastructure or the country’s power grid” [7].

It is not difficult to reconcile the apparent discrepancy. Unlike spam, worms, viruses, and phishing—all of which confront end users directly—infrastructure attacks occur outside their normal frame of reference and control. But attacks on the Domain Name System (DNS), an engine of the Internet infrastructure, appear to be increasing in length and severity, affecting DNS information associated with financial services institutions, Internet service providers, and major corporations in the travel, health, technology, and media/entertainment sectors [8]. Such attacks can result in, say, dropped or intercepted email messages or users unknowingly redirected to fraudulent sites where they inadvertently hand over personal information. Overall, Scott

Chasin, CTO of MX Logic, a provider of online security services, and founder of Bug-Traq, an electronic mailing list devoted to computer security issues, says we are seeing “a gradual morphing of motivations behind hijacking” toward more severe, economically motivated attacks. Inviting targets include the network and its applications in commerce, banking, public health, and medicine, as well as in ordinary social interaction. The ultimate casualty in a serious infrastructure attack is public trust.

The Internet technical community has responded to threats to the DNS infrastructure by developing the DNS Security Extensions (DNSSEC) protocol standard. Although .se, the organization responsible for the Swedish top-level domain, launched commercial DNSSEC service in February 2007, and the European Internet infrastructure services provider Reseaux IP Européens Network Coordination Centre (RIPE NCC, www.ripe.net/ripe) has also deployed the protocol, DNSSEC-enabled systems run primarily in only a few early-adoption and experimental zones [8]. Working with experts from the U.S. National Institute of Standards (NIST), Sparta, Inc., and SRI International, we (the authors) participate in a global effort to encourage deployment of the protocol. Activities include a working group of early adopters, a Web site—www.dnssec-deployment.org—and a free monthly newsletter—*DNSSEC This Month*, www.dnssec-deployment.org/news/dnssecthismonth/—aimed at a more general audience. Initiative partners are also build-

ILLUSTRATION BY ISTVAN OROSZ

ing software tools, conducting focused analysis, and trying to increase awareness and provide training.

Since DNSSEC builds on the DNS, we first review how DNS works, then describe the changes DNSSEC introduces.

DNS is a distributed hierarchical system maintained by a collection of organizations and entities across a series of platforms and configurations, mapping easily remembered names to IP addresses.¹ For instance, translating `myhost.example.com` would take a user to the IP address `192.0.2.1`.² DNS includes three major components: the domain name space and resource records (RRs) stored in a tree structure; name servers, which contain information about the domain's tree structure; and resolvers, which obtain information from name servers in response to queries from a client. As the system has evolved, it has a logical structure; an administrative structure predicated on the notion of a zone; and an operational structure based on queries and responses.

At the top of the inverted tree structure is the root (see Figure 1). Below the root are the top-level domains (TLDs), which are divided into two primary categories: country code TLDs, the familiar `.uk`, `.se`, `.jp`, and so on; and generic TLDs (gTLDs), the familiar `.com`, `.org`, `.net`, and so on. A special TLD, `.arpa`, is reserved for infrastructure purposes. TLDs are further subdivided into subdomains: `example.org`, `example.com`, and so on. Further subdivision of domains occurs frequently, particularly in complex organizations, like corporations and universities. Indeed, many of us have email addresses that include the three-level name `cs.name-`

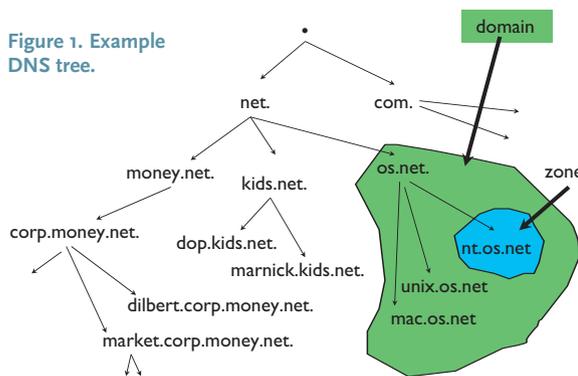
`ofinstitution.edu` or `library.nameofinstitution.edu`. The process by which these subdivisions takes place is called “delegation.” The DNS structure of domains and subdomains is typically expressed in one of two metaphors: leaf-and-node and parent-child. Here, we use the parent-child metaphor to focus on the hierarchical relationships and flow of information.

In one sense, DNS may be understood as a series of records of various types that are stored in a hierarchical, distributed database; for example, the “A” record type provides the IP address.³ In another sense, DNS may also be understood as a set of organizational relationships, responsibilities, and authorities. These two views—logical and administrative—converge in the key concept of “the zone,” which is managed as an independent administrative entity. This entity is responsible for a zone file containing the subset of DNS data about that zone and the mapping of names to IP addresses and/or delegations (such as from parent to child or parent to children), along with other information.

From an operational perspective, DNS transactions consist of a series of queries and responses between two programs: resolvers and name servers. The resolver poses queries on behalf of a client and returns the desired information. The name server contains information about the names and IP

addresses in its zone and responds to queries from resolvers. In practice, what appears to be a single transaction (such as “tell me the IP address for this name”) is more complicated (see Figure 2). The user's program, perhaps a Web browser or an email client, contacts a stub resolver containing a list of recursive or resolving name server addresses. The stub resolver

Figure 1. Example DNS tree.



Source: Russ Mundy, DNS Security Technical Overview, ICANN Workshop on DNS Security (Mar del Plata, Argentina, Apr. 5, 2005); www.dnssec-deployment.org/miniworkshop.php.

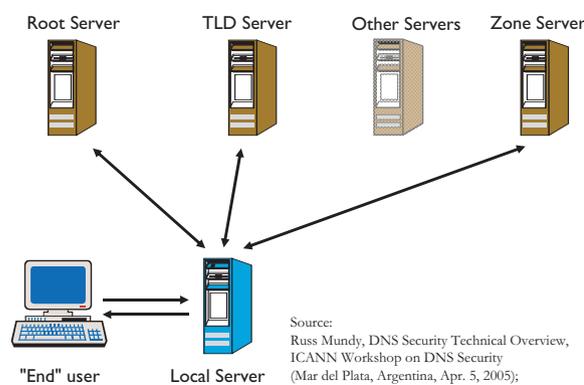


Figure 2. DNS query and response.

Source: Russ Mundy, DNS Security Technical Overview, ICANN Workshop on DNS Security (Mar del Plata, Argentina, Apr. 5, 2005); www.dnssec-deployment.org/miniworkshop.php.

¹The logical system and specifications are laid out in the Internet technical community's standards documents: RFCs 1035 and 1034; guidelines for domain administrators are in RFC 1033.

²Example.com and 192.0.2 are set aside for exclusive use as examples, as documented in RFCs 2606 and 3330.

³The “A” record identifies the IPv4 address; the “AAAA” record identifies the IPv6 record.

contacts a local recursive or resolving name server that either knows which name server has the information or redirects the query up to a zone at the next level. If the parent zone does not have the information, or the IP address, the recursive name server begins a search at the top of the hierarchy, or the root, querying it and then querying down the tree through the successive zones and associated name servers until it obtains either the information or an error.

This description of how the DNS operates is necessarily a highly abstracted view. In practice, there are multiple configurations to replicate and cache the information throughout the system. For example, a successful query rarely reaches the root. The answer is typically obtained from a caching name server lower down in the tree, perhaps at a user's Internet service provider. But these caches can pose a potential vulnerability, since an attacker may be able to tamper with them by inserting false information in the DNS records, a strategy known as "cache poisoning." Indeed, a 2005 attack targeted a cache in which DNS information associated with 600 institutions was stored so the systems of the institutions themselves may have been protected but that left their customers vulnerable [8].

DNSSEC is intended to detect such attacks, enabling users and applications to defend against their consequences. Cache poisoning is but one kind of threat to the DNS; others are explained in RFC 3833 [4]. Although threats vary, they share the characteristic that they exploit vulnerabilities in the DNS and result in responses that cannot or should not be trusted.

RFC	Author/Title/Date/URL
RFC 1033	Lottor, M. Domain Administrators Operations Guide, Nov. 1987; www.ietf.org/rfc/rfc1033.txt .
RFC 1034	Mockapetris, P. Domain Names: Concepts and Facilities, Nov. 1987; www.ietf.org/rfc/rfc1034.txt .
RFC 1035	Mockapetris, P. Domain Names: Implementation and Specification, Nov. 1987; www.ietf.org/rfc/rfc1035.txt .
RFC 3658	Gudmundsson, O. Delegation Signer Resource Record, Dec. 2003; www.ietf.org/rfc/rfc3658.txt .
RFC 3755	Weiler, S. Legacy Resolver Compatibility for Delegation Signer, May 2004; www.ietf.org/rfc/rfc3755.txt .
RFC 3833	Atkins, D. and Austein, R. Threat Analysis of the Domain Name Systems (DNS), Aug. 2004; www.ietf.org/rfc/rfc3833.txt .
RFC 4033	Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. DNS Security Introduction and Requirements, Oct. 10, 2004; www.ietf.org/rfc/rfc4033.txt .
RFC 4034	Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. Resource Records for the DNS Security Extensions, Oct. 10, 2004; www.ietf.org/rfc/rfc4034.txt .
RFC 4035	Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. Protocol Modifications for the DNS Security Extensions, Oct. 10, 2004; www.ietf.org/rfc/rfc4035.txt .

Table 1. Key technical standards documents.

the data is verifiable as the stated source, and the mapping of a name to an IP address is accurate. DNSSEC-capable name servers also provide denial-of-existence; that is, they tell a user that a name does not exist. There are two dominant deployment strategies:

- A process that zone operators initiate for digitally signing their own zones by employing public-private key pairs; and
- A chain of trust between parent and child that enables the system to eventually become trustworthy.

The DNSSEC protocol is described in three RFCs [1–3], together with RFCs 3658 and 3755 (see Table 1); for additional resources for understanding DNSSEC, see Table 2. The system's designers

recognized that adoption would be incremental, says Scott Rose, an author of the core protocol documents, and new software would have to coexist with unsecured systems.

The specification calls for four new resource record types: resource record signature (RRSIG); DNS public key (DNSKEY); delegation signer (DS); and next

DNSSEC: DNS Security Extensions; www.dnssec.org/ . Provides excellent background information for a general and technically literate audience.
DNSSEC Deployment Initiative; www.dnssec-deployment.org . Provides a forum for developers and early adopters to support deployment activities, capture news items, and publish a free monthly newsletter DNSSEC This Month.
DNSSEC Tools Project; www.dnssec-tools.org/ . Provides links to and descriptions of tools, patches, applications, wrappers, extensions, and plug-ins for system administrators.
Gieben, M. DNSSEC. The Internet Protocol Journal 7, 2 (June 2004); www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-2/dnssec.html . Provides a useful introduction to the protocol.
Kolkman, O. DNSSEC How To, a Tutorial in Disguise; www.nlnetlabs.nl/dnssec_howto/ . Key document explaining the protocol and detailed instructions for systems administrators.
Kolkman, O. Measuring the Resource Requirements of DNSSEC. Document ID: Ripe-352, Sept. 29, 2005; www.ripe.net/ripe/docs/ripe-352.html .
U.S. National Institute of Standards, Domain Name Security (DNSSEC Project); www-x.antd.nist.gov/dnssec/ . Provides links to tools for system administrators, guides, information on performance, and more.

Table 2. Resources for understanding and using DNSSEC.

recognized that adoption would be incremental, says Scott Rose, an author of the core protocol documents, and new software would have to coexist with unsecured systems.

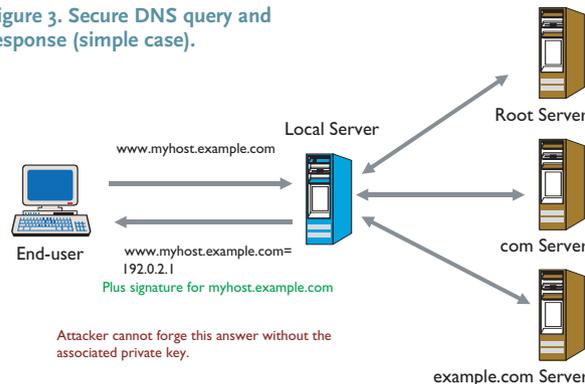
secure (NSEC); it also calls for new information in the packet header. The information in the header used by DNSSEC indicates that the response to a query passed checks on the server side. Depending on local policy, a security-aware resolver may accept this response or perform additional security checks. A zone administrator who wishes to deploy DNSSEC first generates a key pair consisting of a public key and a private key. The public key is stored in a DNSKEY record, and the private key is stored safely. The private key is used to digitally sign the records, and the resulting digital signature is stored in an RRSIG record.

Next, a zone operator must generate NSEC records and, depending on the content of the zone, one or more DS records. This makes possible the response that no record exists. If the zone includes delegations, then a DS record must also be added in the parent zone for a given child. A zone that contains children must include DS records for the children. A zone that has signed its records and added the NSEC (and, if necessary, the DS) records may go into business as a self-signed DNSSEC-capable zone, also known as an “island of security.” This island contains signed records or is considered a “signed zone” but is also the child of a parent that cannot vouch for the authenticity of the child’s key.

The combination of RRSIG and the child’s public key in a DNSKEY record allows validation of the source of the data (see Figure 3). But only the associated private key can be used to sign it in the first place. Thus, the simplest DNSSEC sequence is to obtain the DNS information queried for, together with the signature associated with that information (in the RRSIG), and use the public key in the DNSKEY to perform the validation, proving the signature was made by the holder of the private key.

However, the power of DNSSEC lies in a second step that allows the signed zone to be vouched for,

Figure 3. Secure DNS query and response (simple case).



Source: Modified based on Russ Mundy, DNS Security Technical Overview, ICANN Workshop on DNS Security (Mar del Plata, Argentina, Apr. 5, 2005); www.dnssec-deployment.org/miniworkshop.php.

preferably by its parent; if not, it is vouched for by another authenticating entity. Assume for purposes of simplicity that both parent and child are DNSSEC-capable. In this more powerful DNSSEC sequence, the child has signed a DNSKEY record with the private part of a second key pair and stored the public key part of that second key pair in a record (the DS record).

The child conveys the DS record to the parent. The parent signs the child’s DS record with the private part of the parent’s key pair, placing the resulting signature in an RRSIG record associated with the DS record. Any parent may itself be a child (except the root), and the process is replicated between each child/parent pair. This sequence creates the chain of trust up to the “trust anchor,” the starting point in the chain. A DNSSEC-aware resolver validates the information it receives in response to a query by using the public keys to check the signed records.

ECOLOGICAL SOLUTION

The Internet Engineering Task Force, together with other groups, organizations, and individuals, are working on outstanding technical issues that pose barriers to adoption. The management of keys—the frequency with which they are changed or “rolled over” and the mechanisms by which keys are exchanged between parent and child—is being discussed by early adopters of the DNSSEC protocol. The root at the apex of the tree is of particular importance, given its special status. Evaluation of the computational resources required to run DNSSEC is another important issue, since the zone file will become substantially larger and zone walking, also known as “zone enumeration,” which allows a user to sequentially determine a zone’s entire contents, is of concern to some large zone operators. Members of the Internet Engineering Task Force’s DNSEXT working group have largely

The ultimate casualty in a serious infrastructure attack is public trust.

completed the technical work on a specification that will address concerns over zone walking (www.nsec3.org/cgi-bin/trac.cgi).

DNSSEC has been criticized for having been a long time coming—the first version was published more than 10 years ago—and because it has been slow to be deployed. On the other hand, Frederico Neves of the national domain name registry for Brazil (.br) pointed out at a public session on deploying DNSSEC at the ICANN meetings in Mar del Plata, Argentina, in April 2005 that DNSSEC is a “mature” protocol, which performance has needed time to develop [9]. Deploying DNSSEC, while substantially improving Internet security, does not defend against all threats.

Indeed, the authors of the specification acknowledge that DNSSEC offers no protection against well-known denial-of-service attacks and in some instances may even increase the vulnerability of DNSSEC-aware resolvers to attack. In addition, DNSSEC focuses on records that constitute zone files but does not protect the zone file itself when the zone file is transferred and when other strategies are recommended in the specification. Some observers point out that certificates and certificate authorities have formed a secure infrastructure to support e-commerce, raising the question: What does DNSSEC add? Still others respond that the certificate model works in the Web environment but does not scale and, in particular, does not address threats that arise in email. Finally, issues of individual privacy and data confidentiality, which engage end users’ attention, are specifically beyond the scope of the protocol.

Other protocols (such as Secure Sockets Layer) do protect both personal privacy and the integrity of the transmission but are not applicable to store-and-forward protocols (such as DNS, with its caches). DNSSEC fills an important gap, since perfect privacy would be meaningless if the user’s transaction is hijacked or diverted during transmission through, say, cache poisoning. Thus, DNSSEC is part of a suite of security protocols and measures ranging from those appropriate for individual users on small home office systems up through zone operators of infrastructure systems; see the National Institute of Standards and Technology’s guides for DNS security [5] and for home and small business users [12]. As DNSSEC-capable zones are added, the system incrementally becomes more secure.

CONCLUSION

Full deployment of the protocol requires global cooperation across myriad entities in both the public and private sectors, including those known as registries and registrars that provide DNS services, as well as Internet service providers, nonprofit and professional organizations, equipment and software manufacturers, standards and coordinating bodies, research labs, universities, and large enterprises. In the U.S., the Department of Homeland Security Science and Technology directorate (www.dhs.gov/xabout/structure/editorial_0530.shtm) partners in DNSSEC activities with industry, government, and the international community. Attention to the mechanisms of the Internet (such as DNS) was called out in the National Strategy to Secure Cyberspace (www.whitehouse.gov/pcipb/) released in February 2003. Along with the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (www.whitehouse.gov/pcipb/physical.html), the NSSC is part of the National Strategy for Homeland Security.

Progress toward full deployment is reflected in the actions taken by .se and RIPE NCC and the expectation of major steps within the next few years. As of April 2007, other achievements include deployment by the registry for Puerto Rico, .pr, and the national registry of Bulgaria, .bg. NIC Mexico and Tecnológico de Monterrey Campus Monterrey have sponsored DNSSEC Trial Mexico. The registry services provider VeriSign, which operates .com and .net, among others, will include DNSSEC protocols as part of a recently announced initiative to build a tenfold expansion of its global Internet infrastructure by 2010.

Finally, December 2006 guidance from NIST, a deployment coordination initiative partner, includes a plan for staged deployment of DNSSEC technology within federal IT systems; U.S. federal agencies have one year from December 2006 to comply with the new standards [10]. Deploying DNSSEC is a necessary step toward hardening the Internet infrastructure, the base on which many applications and services depend. The Internet is as widely distributed as it is precisely because the complexities of its inner workings are largely hidden from end users who have come to trust it. The challenge is to preserve that trust. ■

REFERENCES

1. Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. *DNS Security Introduction and Requirements*. RFC 4035, Oct. 10, 2004; www.ietf.org/rfc/rfc4035.txt.
2. Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. *Resource Records for the DNS Security Extensions*. RFC 4034, Oct. 10, 2004; www.ietf.org/rfc/rfc4034.txt.
3. Arends, R., Austein, R., Larson, M., Massey, D., and Rose, S. *Protocol*

Modifications for the DNS Security Extensions. RFC 4033, Oct. 10, 2004; www.ietf.org/rfc/rfc4035.txt.

4. Atkins, D. and Austein, R. *Threat Analysis of the Domain Name System*. RFC 3833, Aug. 2004; www.ietf.org/rfc/rfc3833.txt.
5. Chandramouli, R. and Rose, S. *Secure Domain Name System Deployment Guide: Recommendations of the National Institute of Standards and Technology, Special Publication 800-81*. U.S. Department of Commerce, Technology Administration, NIST, Gaithersburg, MD, May 2006; csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf.
6. Cole, J. et al. *The UCLA Internet Report: Surveying the Digital Future, Year 3*. UCLA Center for Communication Policy, Los Angeles, Feb. 2003; www.digitalcenter.org/pdf/InternetReportYearThree.pdf.
7. Fox, S., Quitney Anderson, J., and Rainie, L. *The Future of the Internet*. Pew Internet & American Life Project, Jan. 9, 2005; www.pewinternet.org/pdfs/PIP_Future_of_Internet.pdf.
8. Haugness, K. and the ISC Incident Handlers. *DNS Cache Poisoning Detailed Analysis Report, Version 2*. Internet Storm Center, Mar. 2005; www.dshield.org/presentations/dnspoisoning.html.
9. ICANN. Transcript of DNSSEC Mini Workshop, ICANN Meetings, Mar del Plata, Argentina, Apr. 5, 2005; www.icann.org/meetings/mardelplata/captioning-dnssec-05apr05.htm.
10. Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., and Rogers, G. *Information Security, Special Publication 800-53, Revision 1*. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD, Dec. 2006; csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf; and the Federal Information Security Act Implementation Project: Protecting the National Critical Information Infrastructure. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD, May 8, 2006; csrc.nist.gov/sec-cert/.
11. SecSpider Web site. DNSSEC Monitoring Project; secspider.cs.ucla.edu/.
12. Souppaya, M., Wack, J., Harris, A., Johnson, P., and Kent, K. *Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers. Special Publication 800-70 (Draft)*. U.S. Department of Commerce, Technology Administration, National Institute of

Standards and Technology, Gaithersburg, MD, May 2005; csrc.nist.gov/checklists/download_sp800-70.html.

AMY FRIEDLANDER (amy@shinkuro.com) is a senior program manager at Shinkuro, Inc., Washington, D.C.

ALLISON MANKIN (mankin@shinkuro.com) is Program Director at the National Science Foundation, Arlington, VA. She conducted the work that resulted in this article while an employee of Shinkuro, Inc., Washington, D.C., in 2005.

W. DOUGLAS MAUGHAN (Douglas.Maughan@dhs.gov) is Program Manager, U.S. Department of Homeland Security, Science and Technology Directorate, Washington, D.C.

STEPHEN D. CROCKER (steve@shinkuro.com) is CEO and co-principal investigator in the DNSSEC Deployment Coordination Project at Shinkuro, Inc., Washington, D.C.

We thank Douglas Montgomery of the U.S. National Institute of Standards and Technology, Marcus H. Sachs of SRI International, and G. Russ Mundy of Sparta, Inc., who has permitted us to use material from his presentations.

The views expressed here do not necessarily represent the views of the National Science Foundation or of the U.S.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

© 2007 ACM 0001-0782/07/0600 \$5.00

COMING NEXT MONTH IN COMMUNICATIONS

CREATING A SCIENCE OF GAMES

The worldwide videogame industry will reach \$60 billion in revenue by year-end; indeed, videogame budgets are now the size of motion picture budgets, with expected revenues for a hit game exceeding \$1 billion. Serious games using immersive entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives are being developed. Indeed, people wonder how videogames might provide any or all K–12 science and math education. With that much play occurring and with videogames becoming such a large part of our economy and of our lives, it is time to create a science of games.

Also in July

The Efficacy of a Terrorism Q/A System

RFID in Supply Chain Management Using Data Life Cycle Framework

Building a Next-Generation Holistic E-Recruiting System

Collaborative Restructuring

Knowledge Architecture for IT Security

A Roadmap for Online Privacy Policy Management

The Effects of Web-based Technologies on Knowledge Transfer

Copyright of Communications of the ACM is the property of Association for Computing Machinery and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.