PLATAFORMA DE GERÊNCIA DE CONTEÚDOS DIDÁTICOS

Platform of Management of Educational Content

Resumo

A plataforma de gerência de conteúdo didático foi criada para atender as demandas no consumo de informações digitais da atualidade. A criação desta plataforma foi focada em atender ao público alvo da instituição CEFET/RJ Campus Petrópolis. A demanda criada por este público constituído de alunos e visitantes se tornou um desafio no aprimoramento da divulgação das informações. Foram realizados estudos e testes a fim de encontrar maneiras mais simples e objetivas de entregar o conteúdo aos usuários. Além da disponibilização do conteúdo, foram criadas estratégias de segurança. Estas estratégias estavam relacionadas ao tráfego e armazenamento das informações durante requisições dos usuários. A tolerância a falhas também foi abordada de forma a proporcionar uma recuperação no menor tempo possível em caso de falhas ou ataques ao servidor de conteúdos.

PALAVRAS-CHAVE: Gerência de Informação, Redes de Computadores, Segurança da Informação.

Dalbert Matos Mascarenhas*[1]
Laura Silva de Assis [2]
Gabriele de Britto Vieira [3]
Camilla Alves Mariano da Silva [3]
Jéssica Alcântara Gonçalves [3]
Vinicius da Silva Faria [3]

1Mestre em Engenharia Eletrônica pela UERJ (2008). Professor EBTT-DE do CEFET/RJ Campus Petrópolis.
2Doutora em Engenharia Elétrica pela UNICAMP (2014). Professora EBTT-DE do CEFET/RJ Campus Petrópolis.
3Estudante de Engenharia de Computação no CEFET/RJ Campus Petrópolis (ingresso 2014).
*Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ
Rua do Imperador, 971 - Centro,
Petrópolis - RJ
Contato (24) 2231-7254

Abstract
The didactic content management platform has been created to meet the demands in the consumption of today's digital information. The creation of this platform is focused on meeting the target audience of the institution CEFET / RJ Campus Petropolis. The demand created by this audience of students and visitors has become a challenge on improving the dissemination of information. Studies and tests were conducted in order to find simple and practical ways to deliver content to users. In Addition, content security strategies were created. These strategies were related to traffic and storage of information during users requests. Fault tolerance was also addressed in order to provide a recovery in the shortest possible time in case of failures or attacks to the content server.
KEYWORDS: Content Management, Computer Network, Information security.

INTRODUÇÃO

O projeto foi concebido com o intuito de ampliar a capilaridade do acesso a conteúdos didáticos digitais. O público alvo do projeto é constituído de alunos e visitantes do campus sede do projeto (CEFET/RJ Petrópolis).

Através de análises preliminares do comportamento dos alunos foi possível perceber que os mesmos têm utilizado diferentes dispositivos para consultas de conteúdos didáticos, como por exemplo celulares e tablets. Este comportamento segue uma tendência natural à relação com novas tecnologias de comunicação [4]. A forma como este conteúdo é armazenado pode se tornar um obstáculo para democratização do mesmo frente a este comportamento discente. Lembrando que o conteúdo didático citado neste trabalho pode ser constituído desde apostilas, apresentações em slides, listas de exercícios, cronograma de utilização de laboratórios, entre outros. Outro ponto que vale ressaltar com relação ao conteúdo é que o mesmo pode ser disponibilizado por professores e também por alunos. Ao final de 2014 foi criado um grupo constituído de alunos e professores com a missão de projetar uma nova arquitetura para provimento de conteúdos didáticos que estivesse alinhada com as novas necessidades dos alunos e visitantes da instituição. O grupo tinha como objetivo primário estabelecer diretrizes para reduzir a complexidade na obtenção de conteúdos bem como reduzir seus custos vinculados à capacidade de armazenamento e transporte das informações. A questão do armazenamento dos conteúdos vem se tornando um problema dada a capacidade finita dos dispositivos móveis e mesmos das máquinas dos laboratórios com computadores [14]. Observou-se que o aluno ou visitante acessava o conteúdo em uma máquina e consequentemente fazia um armazenamento integral ou parcial do mesmo. Decorrido uma fração de tempo, que neste caso poderia ser de dias ou mesmo horas, o aluno requisitava o mesmo conteúdo através de uma máquina ou dispositivo móvel diferente. Este novo acesso em uma máquina ou dispositivo diferente, fazia com que o mesmo conteúdo fosse armazenado em diferentes máquinas. Assim, aumentando a escala de utilização por número de alunos e visitantes, havia uma grande sub utilização do espaço de armazenamento. Esta sub utilização de espaço levava a mais atividades de manutenção dos computadores dos laboratórios bem como esgotamento de recursos nos dispositivos móveis dos alunos e visitantes.

O outro ponto apontado como motivador para este projeto está no transporte das informações relacionadas aos conteúdos. Estas informações são distribuídas através de redes de computadores que podem permitir o tráfego de conteúdos didáticos criados dentro da instituição, bem como o tráfego de conteúdos obtidos através da internet. A forma de obtenção desses conteúdos pode gerar diferentes problemas de sobrecarga na rede de computadores. Como primeira análise vejamos a utilização de conteúdos internos que tenham sido criados por professores ou alunos da instituição.

Estes conteúdos podem ser acessados dentro de um mesmo laboratório, onde houvesse uma aula de determinada disciplina com 40 alunos participantes. Neste caso todos realizariam o acesso ao mesmo conteúdo fazendo diferentes re-

quisições sobre o mesmo material, o que geraria uma sobrecarga nos dispositivos responsáveis por redistribuir as informações na rede de computadores.

A outra forma de acesso a conteúdos externos empregando o uso da Internet, promove a criação de novos congestionamentos. Neste caso as requisições de conteúdos além de trafegarem pela rede de computadores também devem ser encaminhadas para a Internet. O problema deste encaminhamento de requisições de conteúdos para a internet é que as requisições de conteúdos didáticos vão competir pelo recurso finito de capacidade de tráfego relacionado ao tipo de conexão que a instituição tem com a Internet [11]. Desta forma as requisições de conteúdos didáticos concorrem diretamente com outas informações relacionadas à navegação na Internet ou mesmo tarefas administrativas que fazem uso da Internet para seus objetivos.

O projeto visa restringir o impacto causado pela redundância de informações armazenadas e consequentemente trafegadas na rede de computadores. A Figura 1 exemplifica parte da arquitetura do projeto. Para isto foram criadas estratégias de contenção para os recursos didáticos em redundância.

Outro ponto incorporado ao projeto é viabilizar um melhor escoamento das informações de conteúdos trafegadas para máquinas de laboratórios e para dispositivos móveis de alunos e visitantes.

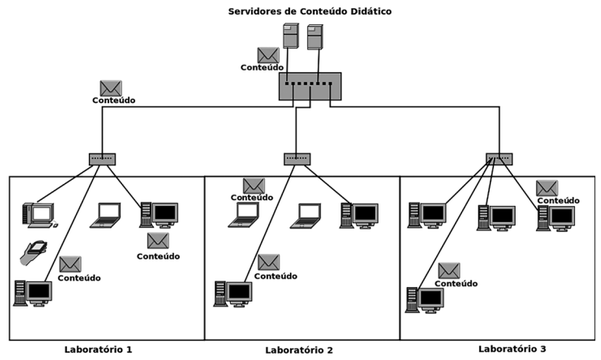


Figura 1 - Exemplo de Artquitetura para a Gerência de Contúdos.

METODOLOGIA

O objetivo de ampliar o acesso e a disponibilidade de conteúdos didáticos já existia antes da criação do curso de Engenharia de Computação no CEFET/RJ campus Petrópolis. De fato é notório que após a criação deste curso a demanda por uma organização e distribuição destes conteúdos vem aumentando consideravelmente. Parte deste aumento está relacionado também com os outros novos cursos implantados no campus e a outra parte está relacionada às demandas específicas do curso de Engenharia de Computação. Apontado como demandas específicas temos a necessidade maior de informações digitais e consequentemente toda a infraestrutura necessária para que estas informações possam ser computadas e disponibilizadas. Em Março de 2015 iniciou-se os preparativos para a implementação da plataforma de gerência para conteúdos didáticos em um laboratório projetado para pesquisas relacionadas à iniciação científica e projetos de e xtensão. O l aboratório c onta com c omputadores desktop além de laptops e outros dispositivos móveis como tablets e celulares. A flexibilidade n a a lteração d os recursos relacionados a redes de computadores como switches, roteadores e computadores também é possível neste laboratório, o que proporciona um ambiente controlado para análises de desempenho e acurácia na gerência dos conteúdos didáticos.

Os testes iniciais para provimento de conteúdo didático iniciaram com a utilização de servidores Web [2]. Estes servidores foram utilizados para que fosse possível armazenar o conteúdo em diferentes localidades da rede e permitir um acesso mais simples, mesmo de dispositivos móveis como celulares. A ferramenta escolhida após buscas relacionadas ao desempenho e possibilidade de alteração foi o APACHE [8], disponível em https://httpd.apache.org/. Este servidor consagra-se por sua segurança e flexibilidade f rente a d iferentes f ormas d e u tilização v inculando diferentes navegadores e serviços. Apesar de sua flexibilidade como repositório de conteúdos, utilizando o APACHE, não foi possível suprir a necessidade de armazenamento de conteúdos como árvore de diretórios de forma simples e com economia de recursos de armazenamento.

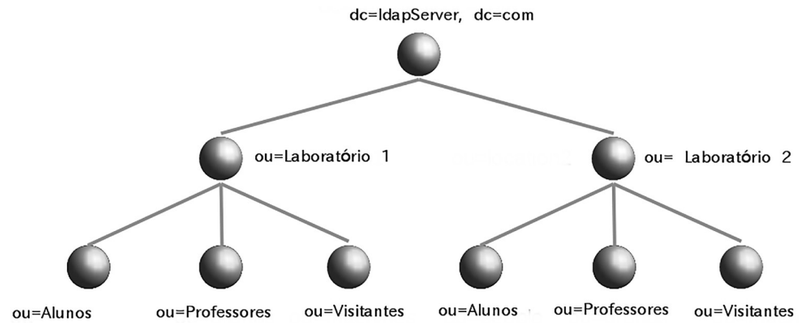
Como alternativa ao APACHE iniciou-se os estudos em outra ferramenta, o SAMBA, disponível em www.samba.org. Este é uma ferramenta para interoperabilidade entre Windows e Linux [16]. Os testes consistiram em reservar um computador com SAMBA instalado e este ficaria responsável por armazenar os conteúdos didáticos providos por professores e alunos. Esta ferramenta possibilitou uma melhor gerência de conteúdos pois era possível utilizar hierarquia de diretórios no acesso às informações e consequentemente selecionar os conteúdos pertinentes a cada cliente que o acessava, sendo este aluno ou visitante. Utilizando a solução com a ferramenta SAMBA um aluno poderia acessar seus conteúdos independente do laboratório que estivesse, desde que esse laboratório possuísse acesso ao servidor SAMBA, onde estariam os conteúdos. A ferramenta também possibilitava que o provedor de conteúdo didático, seja ele aluno ou professor, especifique quais usuários podem ter acesso ao conteúdo e se estes teriam permissão para alterações nos conteúdos [3].

Apesar das funcionalidades do SAMBA atenderem boa parte dos nossos requisitos necessários, uma demanda na redução da complexidade no acesso aos conteúdos ainda persistia. Isto porque o usuário, por exemplo um aluno, ainda necessitava de algumas configurações iniciais antes de obter os conteúdos que haviam sido disponibilizados no servidor SAMBA. Estas configurações adicionais geraram uma complexidade em relação a outras ferramentas utilizadas. A Tabela 1 faz um comparativo entre a complexidade de utilização por parte do usuário e o consumo de recursos com informações redundantes de conteúdos. Este consumo de recurso está relacionado ao armazenamento e tráfego dos conteúdos. Outro ponto estava

ligado ao acesso às máquinas que ainda necessitavam de usuários e senhas cadastradas em cada uma o que gerava uma redundância desnecessária.

Após testes e buscas de novas ferramentas, optou-se por utilizar o LDAP [1], disponível em www.openldap.org, em conjunto com o SAMBA. Com a utilização do LDAP foi possível atender a demanda de redução de complexidade no acesso às informações didáticas, pois este possibilita o usuário acessar recursos em um servidor remoto através de qualquer computador da rede utilizando um login. Os primeiros testes foram concentrados em cadastrar usuários em uma máquina servidora e posteriormente verificar se as outras máquinas ligadas a rede de computadores estavam aptas a acessar os perfis u tilizando o s mesmos u suários cadastrados. P osteriormente aos testes com cadastramento de usuários, iniciou-se a fase de convergência de informações. Nesta fase foram implantados conteúdos didáticos nos perfis dos usuários, alunos e visitantes. Estes conteúdos foram implantados seguindo árvores hierárquicas como exemplificado na Figura 2, e ,posteriormente, foi analisado se estes conteúdos estavam sendo replicados para as máquinas que realizavam o novo acesso do perfil.

Figura 2:- Árvore Hierárquica de Diretórios.



A ferramenta SAMBA provê um sistema de criptografia para autenticação dos usuários, no entanto neste projeto optou-se por utilizar SSL [12], em túneis criptografados para que desta forma tanto a autenticação como a transferência de dados se tornasse mais segura. Com o túnel criptográfico, mesmo que um usuário mal intencionado tente capturar informações trafegadas na rede, utilizando ferramentas de bisbilhotamento [5], as informações estariam seguras dependendo da criptografia utilizada. Esta camada extra de segurança se torna fundamental frente aos avanços na área de segurança da informação com um número elevado de ferramentas de ataques disponíveis.

Além da segurança no transporte da informação até os servidores de gerenciamento de conteúdos didáticos, ainda existia a possibilidade de ataques ao servidor de conteúdo. Esta vulnerabilidade motivou esforços em testar a resistência destes servidores a ataques comuns na atualidade como o DoS [10]. Este tipo de ataque pode ser feito através do consumo excessivo dos recursos da máquina ou da rede, bem como a exploração de falhas. Utilizamos a ferramenta T50 [13], para iniciar ataques propositais aos nossos servidores de forma a prevê qual seria o tempo médio que um atacante levaria para comprometer o serviço de conteúdos. Após análise destes resultados iniciou-se uma pesquisa em formas de conter ou mesmo mitigar os ataques de negação de serviço. Dentre as formas de evitar os ataques foram desenvolvidos programas em conjunto com tcpdump [7] e iptables [6] para analisar o tráfego que chegava aos servidores de conteúdos e consequentemente tentar distinguir ataques.

Apesar das medidas utilizas para tentar evitar ataques contra os servidores de conteúdo, é esperado que as ferramentas de ataque continuem em constante evolução. Com base na evolução destas ferramentas iniciou-se um estudo detalhado sobre formas de recuperação após um ataque bem sucedido. Uma das formas de recuperação de ataques utilizadas foi a criação de um segundo servidor de conteúdo igual ao servidor primário e com a mesma quantidade de conteúdo. A ideia por trás desta estratégia era a de que caso o servidor principal fosse atacado e consequente ficasse inoperante, o segundo poderia assumir automaticamente o papel de prover conteúdos para os alunos e visitantes. Para esta tarefa era primordial que os servidores estivessem sincronizados, o que foi possível com o uso da ferramenta Rsync [15]. Esta estratégia de recuperação de ataques proporcionou uma maior robustez não só a ataques de negação de serviço como também a falhas comuns como pane na máquina servidora.

RESULTADOS

Após a etapa de configurações foi analisado como seria o desempenho utilizando o servidor Apache como servidor de conteúdos para os alunos e visitantes. Observou-se que utilizando este servidor obtivemos um desempenho satisfatório no consumo de recursos das máquinas utilizadas no laboratório bem como nos acessos por outros dispositivos remotos. Os testes de disponibilidade de conteúdo demonstraram uma facilidade na obtenção dos conteúdos por parte dos alunos, no entanto, os conteúdos obtiveram alto grau de redundância com relação aos pedidos. Este resultado pode ser visto na Tabela 1. Esta redundância foi ocasionada por pedidos de conteúdos que já haviam sido entregues mas o aluno optou por trocar o dispositivo que acessava o conteúdo ou mesmo trocar de máquina no laboratório. Desta forma um mesmo aluno que havia antes acessado um determinado conteúdo didático, ao sentar em uma outra mesa com um computador diferente, precisava acessar o conteúdo novamente. Este acesso gerava um tráfego na rede até chegar aos servidores de conteúdo onde o mesmo era requisitado e posteriormente retornava para o aluno que o requisitou. Além do consumo dos recursos da rede este método ainda consumia memória de armazenamento nas máquinas que estavam acessando o conteúdo redundante.

Outro resultado importante está na dificuldade, em termos de complexidade, para que um aluno incluísse um conteúdo no servidor. Apesar de existirem diver-

sas ferramentas para inserção de conteúdo em servidores de páginas, esta inserção não é trivial o que pode gerar uma baixa adesão por parte dos alunos menos familiarizados com esta tecnologia.

Tabela 1 - Comparativo Entre a Complexidade de Utilização e Sobrecarga de Conteúdos.

SERVIDOR UTILIZADO	SOBRECARGA COM REDUNDÂNCIA	NÍVEL DE COMPLEXIDADE
APACHE	Alto	Alto
SAMBA	Baixo	Mediano
LDAP + SAMBA	Baixo	Baixo

Utilizando o SAMBA na obtenção do conteúdo didático foi possível verificar que o grau de redundância nas informações foi reduzido como demonstrado na Tabela 1. Mesmo com esta redução ainda era possível verificar um certo grau de dificuldade por parte dos alunos em administrar e recuperar conteúdos em suas próprias contas. Esta dificuldade era mais atuante em alunos que tinham um reduzido conhecimento na área da computação ou mesmo aqueles que preferiam obter seus conteúdos com o menor grau de manipulação possível.

A estratégia de utilizar o LDAP em conjunto com o SAMBA proporcionou um maior ganho relacionado à redução da redundância e simplificação do acesso ao c onteúdo. Neste caso a obtenção de um conteúdo poderia ser feita de diversas formas, incluindo servidores de página localizados na rede interna ou na internet. Uma vez obtido este conteúdo o mesmo estaria dentro do perfil do aluno e portanto quando fosse necessário acessá-lo novamente o consumo de recursos seria reduzido. Um aluno que já houvesse requisitado um conteúdo e tivesse essa informação em seu perfil, poderia acessar esse conteúdo de seu perfil mesmo que se deslocasse para outra máquina do laboratório.

Foram realizados ataques de negação de serviço, DoS (Denial of Service), nos servidores de conteúdo. Este consiste em mandar várias requisições ao servidor deixando-o sobrecarregado, impedindo que o mesmo responda as solicitações de conteúdos feitas por usuários não maliciosos.

Para realizar os testes utilizamos a ferramenta de ataque Ettercap [9] e T50. O segundo servidor, que assume o controle com um firewall mais restritivo foi testado com diferentes c onfigurações. O motivo da variação nestas configurações foi o de estabelecer um equilíbrio entre a disponibilidade do recurso no provimento de conteúdos e sua vulnerabilidade a novos ataques. As configurações utilizadas podem ser vistas na Tabela 2. Aquelas intituladas como Básicas apresentavam uma restrição no número de conexões simultâneas que um computador poderia fazer. A ideia por traz desta configuração está em estudos prévios no comportamento de acesso a conteúdos por alunos dentro do laboratório de extensão. Como já existia um número

médio de conexões para que o aluno obtivesse o conteúdo, criamos uma restrição neste número de conexão para atender as requisições médias de conteúdos. O motivo da restrição está em que uma das forma de ataques de negação de serviço é justamente realizar um alto número de conexões a um servidor e consequentemente comprometer seus recursos.

CONFIGURAÇÃO	MÁXIMO DE CONEXÕES POR MÁQUINA	NÚMERO DE ATACANTES
Básica 0	100	2
Básica 1	50	1
Básica 2	50	2
Básica 3	50	3
Restritiva 1	10	1
Restritiva 2	10	3

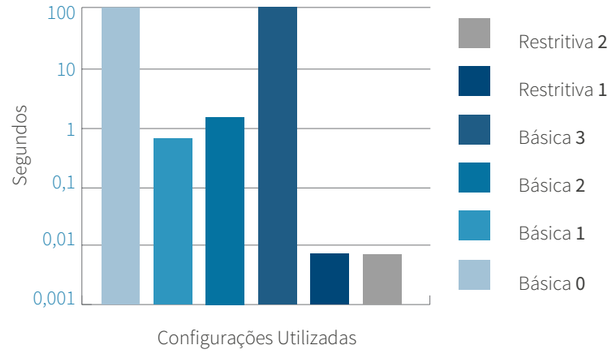
Tabela 2 - Descrição das Configurações de Segurança

Além das configurações relacionadas ao número de conexões, foi variado também o número de computadores que realizavam ataques de negação de serviço. O objetivo desta variação era analisar o quanto os servidores poderiam suportar múltiplos ataques e ainda sim prover conteúdos.

As configurações restritivas além da limitação do número de conexões, realizavam um bloqueio dos endereços físicos das máquinas que estavam realizando o ataque no servidor primário. Desta forma quando o servidor primário era comprometido o segundo servidor assumia a função de prover conteúdos e bloqueava os endereços maliciosos. Esta restrição proporcionou um ganho no provimento de conteúdos, como pode ser visto na Figura 3.

Os testes apresentados na Figura 3 foram repetidos 10 vezes consecutivas, extraindo a média dos tempos gastos para que um conteúdo requisitado por um usuário não malicioso retornasse até o mesmo com o servidor sob ataque. Neste gráfico é possível observar que as configurações Básica 0 e Básica 3 apresentaram um alto grau de atraso na estrega do conteúdo. Esse atraso elevado fez com que a entrega falhasse devido ao tempo limite de conexão estabelecido para o protocolo utilizado nesta aplicação. O motivo do alto atraso da configuração Básica 0 está relacionado ao número de conexões permitidas, neste caso 100. Este elevado número de conexões por usuário permitiu que os ataques maliciosos comprometessem a máquina servidora de conteúdo. A outra configuração, Básica 3, falhou devido ao número de atacantes. Neste caso ao incluir mais um atacante, totalizando três, isto fez com que o servidor ficasse sobrecarregado.

Figura 3: Gráfico do Tempo de Respostas aos Conteúdos Requisitados.



As configurações Básica 1 e Básica 2 apresentaram um grau de atraso que possibilitou a entrega de conteúdos. Isto se deve a relação de restrição de conexões e o número de máquinas atacantes. Apesar destas duas configurações atenderem a demanda de conteúdo, obtiveram resultados inferiores quando comparadas às configurações Restritiva 1 e Restritiva 2. Estas últimas, fizeram o uso de bloqueio de endereços de atacantes e consequentemente reduziram a sobrecarga no servidor de conteúdo.

Os testes relativos ao tempo médio para o restabelecimento do serviço provido após uma falha, seja ela por ataque ou mesmo por pane no sistema demonstraram ser satisfatórios. Este tempo médio envolve a quantidade em segundos em que uma anomalia é detectada pelo servidor e consequentemente realiza as ações de prevenção. Nos resultados esse tempo ficou em torno de 18,59 segundos. Após detectar a anomalia e verificar a possível falha no servidor principal o segundo servidor assume com um tempo médio de 21,26 segundos. Estes resultados demonstraram que a maioria dos usuários não sofreriam um impacto negativo na obtenção do conteúdo didático.

CONCLUSÕES

O projeto de extensão proporcionou a criação de uma plataforma para gerência de conteúdos didáticos que será utilizada por alunos e visitantes do CEFET/RJ Campus Petrópolis. O trabalho focou em prover conteúdos com base em requisitos como a redução do consumo de recursos de armazenamento e transferência de informações através da rede de computadores.

Proporcionar conteúdos com um melhor desempenho na utilização dos dispositivos e da rede também elevou o conhecimento dos alunos bolsistas e colaboradores do projeto. Estes alunos trabalharam com ferramentas e sistemas operacionais com alto grau de relevância para o mercado de trabalho da computação. O trabalho com ferramentas destinadas a tratar a segurança da informação impôs um nível de dificuldade que também proporcionou muito aprendizado para os colaboradores.

Este aprendizado já está sendo utilizado em outros projetos que também carecem de uma maior segurança no tráfego de informações.

A plataforma de gerência ainda precisa de avanços relacionados a diferentes tecnologias utilizadas principalmente em celulares com o sistema operacional Android. Para adaptar-se a estes sistemas será utilizado em trabalhos futuros outras ferramentas para convergência, possibilitando acréscimos relativos à segurança da informação em dispositivos como celulares e tablets.

Tomando como base os resultados, ampliaremos o escopo do projeto para atender a mais laboratórios da instituição e também proporcionar acesso ao conteúdo através de rede sem fio para dispositivos móveis. Pretende-se também utilizar a plataforma de gerência de conteúdos na Semana da Engenharia de Computação realizada todo ano na instituição.

REFERÊNCIAS

[1] **BYRNE, D. J., MURTHY, C. R., SHI, S.-B., SHU, C.-L.** Lightweight directory access protocol (ldap) directory server cache mechanism and method, Feb. 12 2002. US Patent 6,347,312.

[2] **CARDELLINI, V., COLAJANNI, M., PHILIP, S. Y.** Dynamic load balancing on web-server systems. IEEE Internet computing 3, 3 (1999), 28.

[3] **FUTAGAWA, J.** Integrating network services of windows and unix for single sign-on. In Cyberworlds, 2004 International Conference on (2004), IEEE, pp. 323–328.

[4] **GUBBI, J., BUYYA, R., MARUSIC, S., PALANISWAMI, M**. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems 29, 7 (2013), 1645–1660.

[5] **HENDERSON, T., KOTZ, D., ABYZOV, I.** The changing usage of a mature campus-wide wireless network. Computer Networks 52, 14 (2008), 2690–2712.

[6] **HOFFMAN, D., PRABHAKAR, D., STROOPER, P.** Testing iptables. In Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research (2003), IBM Press, pp. 80–91.

[7] **JACOBSON, V., LERES, C., MCCANNE, S.** The tcpdump manual page. Lawrence Berkeley Laboratory, Berkeley, CA (1989).

[8] **MOCKUS, A., FIELDING, R. T., HERBSLEB, J.** A case study of open source software development: the apache server. In Proceedings of the 22nd international conference on Software engineering (2000), Acm, pp. 263–272.

[9] **ORNAGHI, A., VALLERI, M.** Man in the middle attacks. In Blackhat Conference Europe (2003).

[10] **PARK, K., LEE, H.** On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets. In ACM SIGCOMM computer communication review (2001), vol. 31, ACM, pp. 15–26.

[11] **PHAM, P. P., PERREAU, S.** Performance analysis of reactive shortest path and multipath routing mechanism with load balance. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (2003), vol. 1, IEEE, pp. 251–259.

[12] **RESCORLA, E.** SSL and TLS: designing and building secure systems, vol. 1. Addison-Wesley Reading, 2001.

[13] **ROSSI, F. D., DA SILVA CONTERATO, M., FERRETO, T., DE ROSE, C. A.** Evaluating the trade-off between dvfs energy-savings and virtual networks performance. ICN 2014 (2014), 285.

[14] **SINGH, A., KORUPOLU, M., MOHAPATRA, D.** Server-storage virtualization: integration and load balancing in data centers. In Proceedings of the 2008 ACM/IEEE conference on Supercomputing (2008), IEEE Press, p. 53.

[15] **TRIDGELL, A., MACKERRAS, P., ET AL**. The rsync algorithm.

[16] **WANG, Y., ZHU, Z.-X., ZHANG, S.-L.** Design and implement of samba server based on the webmin tool. Control Engineering of China 11, 5 (2004), 455–457.