Big Data and Information Analytics

BDIA, 6: 1–11.
DOI: 10.3934/bdia.2021001
Received: 07 September 2020
Accepted: 08 January 2021
Published: 08 February 2021

http://www.aimspress.com/journal/BDIA

Review

Computer firewalls: security and privacy protection for Mac—review

Gabriel Dorado[1,*], Sergio Gálvez[2] and María del Pilar Dorado[3]

[1] Departamento de Bioquímica y Biología Molecular, Campus Rabanales C6-1-E17, Campus de Excelencia Internacional Agroalimentario (ceiA3), Universidad de Córdoba, 14071 Córdoba, Spain
[2] Departamento de Lenguajes y Ciencias de la Computación, ETSI Informática, Campus de Teatinos, Universidad de Málaga, 29071 Málaga, Spain
[3] Departamento de Química Física y Termodinámica Aplicada, Ed. Leonardo da Vinci, Campus de Rabanales, Universidad de Córdoba, Campus de Excelencia Internacional Agroalimentario, ceiA3, 14071 Córdoba, Spain

*** Correspondence:** Email: bb1dopeg@uco.es; Tel: +(34)957218689; Fax: +(34)957218592.

Abstract: Internet has become the ultimate information resource. It allows both to reach information from the outside, as well as to share inside data. Yet, such power also involves potential weaknesses, in relation to security and privacy protection. Indeed, threats may come from malicious web sites, trying to steal user's data or install unwanted applications. Malware may include adware, Potentially Unwanted Applications (PUA) or Potentially Unwanted Programs (PUP), and even ransomware. Another menace may even come from otherwise *bona fide* applications installed by the user. Thus, such applications may send private data to external servers, without the user's consent and knowledge. Therefore, a proper firewall is required to protect the privacy of users. Indeed, they are built inside the operating systems, as basic security tools. Third party companies offer more comprehensive firewalls, including free and nonfree ones. This review analyzes the firewalls available for Mac (macOS) computers. As a practical example, applications in scientific research, in general, as well as bioinformatics, in particular, are described. Last but not least, Internet security and privacy protection is a work in progress, and as such, users should know about this critical fact, and take proper action, installing and updating appropriate firewalls.

Keywords: World Wide Web (WWW); web browser; electronic mail (e-mail, eMail); Graphical User Interface (GUI)

1. A brief history of Internet and security concerns

Internet is the computer network of networks. It has changed the way we access and send information, interact with others and work. Internet started at early 1960 decade, as a research project funded by the United States of America (USA). The goal was to build an intuitive and easy to use computer network, that was also robust and therefore fault-tolerant. But the inflection point was the invention of the World Wide Web (WWW) by Tim Berners-Lee in 1989, who wrote the first web browser in 1990, being released in 1991. That became popular with the development of Mosaic in 1993, being the first widely-used web browser. Then, the web browser Netscape Navigator was released in 1994, which eventually became Netscape Communicator in 1997. Netscape included JavaScript programming language, being the most widely used language for client-side scripting of web pages, and Secure Sockets Layer (SSL) for securing online communications, before Transport Layer Security (TLS) took over. That way, the average person could access Internet in a somewhat secure environment, with an intuitive Graphical User Interface (GUI), not requiring being informatician or computer expert. Yet, Internet is a complex network (Figure 1), and therefore, their users may not know who is on the other side, on all sides, all the time.

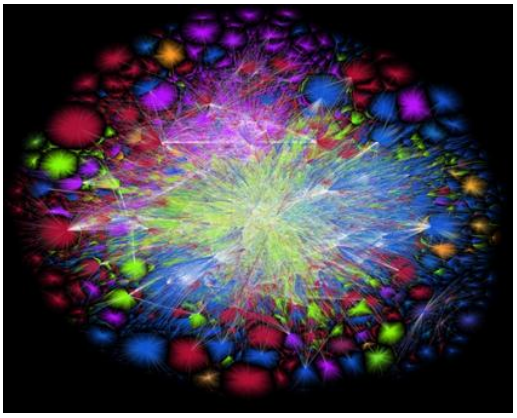

Figure 1. Map of Internet. Chart showing a partial map of Internet, based on 11th July 2015 data (the first major release since 2010). Lines are drawn between nodes or Internet Protocol (IP) addresses. Lengths of lines represent delays between nodes. Color codes: blue (USA and Canada); green (Europe); magenta (Ibero-America); red (Asia Pacific); orange (Africa); and white (backbone of highly-connected networks). © 2021 The Opte Project <http://www.opte.org/the-internet>, Wikimedia Commons <http://commons.wikimedia.org> and Creative Commons <http://creativecommons.org>.

2. Why are firewalls necessary?

In an ideal world, it would not be necessary to take care about security and privacy. Unfortunately, our world requires safety precautions. Internet can be used for good and legitimate purposes, but alas, it is not always so! Indeed, Internet can be also exploited for bad, intrusive, unpropitious or somehow obscure goals. For instance, intruders or crackers could gain access to servers, to take control of them and cause damage, including planting unsolicited malware applications, stealing information and encrypting data, requesting a ransom (usually, in cryptocurrencies like bitcoins) to disclose passwords to unencrypt them (ransomware).

On the other side, applications could send sensitive data from personal computers into unwanted hands. That later scenario is the most frequent threat for the average Internet user. Most people may not notice or not know about it, but whenever a computer is connected to Internet, installed applications start sending information elsewhere. Besides, they do it at a surprisingly-high frequency. Such data may be considered trivial or irrelevant by the user, or may be private information, industrial secrets, etc. But even in the first scenario, sent information may have unwanted consequences for the user, like receiving more spam, displaying unwanted advertisements while browsing the web, etc. It is said that when things are free on Internet, the real prices are the users (their information), and it is true!

Actually, searching Internet for terms like data breach, ransomware or malware yields shocking results. Indeed, problems associated to computer security and privacy are increasing at an alarming pace. Thus, digital security is becoming a must [1], much as physical security is [2]. Firewalls can be designed to protect computer systems against attacks from the Internet or inbound traffic (stateful firewalls), as well as to control outbound traffic. The formers are typically designed to protect servers at institutions or corporations that may be targets of crackers. The latter are usually designed to protect users' privacy. Therefore, cybersecurity is quite relevant for the average Internet user, in general, as well as the scientist, in particular (see below).

3. Firewalls for Mac

Firewalls for Mac are available as simple and cheap—even free—applications, as well as more powerful and expensive ones, as described below:

• Fortunately, besides firewalls built-in routers, modern computer operating systems include firewalls to protect users. Thus, the Mac built-in firewall for incoming connections into macOS from Apple <https://www.apple.com> (Figure 2) is free. Likewise, Murus Lite 2.0.5 from Murus <https://murusfirewall.com> (Figure 3). They are better than nothing, albeit they are not comprehensive enough to efficiently protect against current Internet threats. Indeed, they are quite basic tools, not only because they have fewer features and flexibility than nonfree alternatives, but also—and most importantly—because they lack the foundations and power to truly protect users against cyberspace dangers in an efficient and comprehensive way. So, it seems obvious that if the users want to better protect their privacy, a more sophisticated firewall is necessary. Such solutions were not available when Mosaic browser was released and the web popularized, but fortunately they have been developed in recent years.

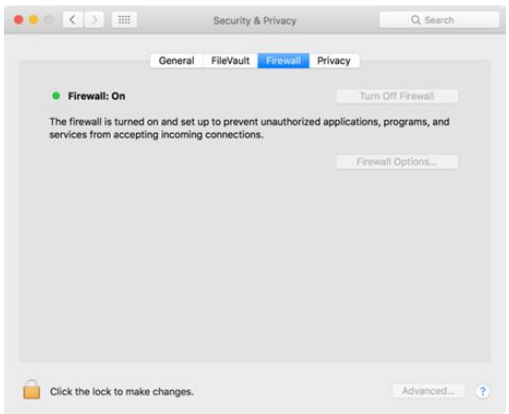

Figure 2. Mac firewall. Mac built-in firewall of macOS at "Apple-System Preferences-Security & Privacy-Firewall". © 2021 Apple.

Figure 3. Murus Lite firewall. © 2021 Murus.

• Radio Silence 2.3 from Juuso Salonen <https://radiosilenceapp.com> (Figure 4) is arguably the easiest network monitor and firewall for Mac, being also quite cheap (9 USD).

Figure 4. Radio Silence firewall. © 2021 Juuso Salonen.

• Murus also offers Murus Basic 2.0.5 as well as Scudo <https://www.murusfirewall.com/scudo> for a similar price (10 USD) and Vallum 3.3.4 (Figure 5) <https://www.vallumfirewall.com> (15 USD). They are more comprehensive, offering more options.

Figure 5. Scudo (left) and Vallum (right) firewalls. © 2021 Murus.

• A further step in such direction is the standard edition of NetBarrier X9 10.9.14 (Figure 6) from Intego <https://www.intego.com/business/network-protection> (29.99 USD).

Figure 6. NetBarrier X9 firewall. © 2021 Intego.

• The most powerful and versatile firewalls, which can be considered as professional, include Murus Pro 2.0.5 from Murus (35 USD), Little Snitch 5.0.4 from Objective Development Software (Figure 7) <https://www.obdev.at/products/littlesnitch> (45 USD), Hands Off! 4.4.3 from One Periodic (Figure 8) <http://www.oneperiodic.com/products/handsoff> (49.99 USD) and NetBarrier X9 10.9.14 business edition <https://www.intego.com/business/network-protection> (89.99 USD).

Figure 7. Little Snitch firewall. © 2021 Objective Development Software.

Figure 8. Hands Off! firewall. © 2021 One Periodic.

4. How firewalls work

As said above, firewalls can monitor computer connections from and to Internet. Some of them may be willingly triggered by the computer user, as when browsing the web. Web browsers may also have additional built-in security protections. For instance, Safari from Apple uses anti-phishing features since version 3.2, like Google Safe Browsing and Extended Validation Certificate support, to identify potential fraudulent websites. The user can decide then if blocking them or continue browsing. Negative results may arise sometimes, but usually this is a good protection measure to configure and activate in the security section of web browser preferences. Other level of protection can be implemented using antivirus and malware-scanning applications. Among them are Malwarebytes from such developer <https://www.malwarebytes.com>, DetectX Swift (now free) from Sqwarq <https://sqwarq.com/detectx>, and the interesting, useful and free security tools offered by Objective-See, including the Lulu firewall <https://objective-see.com/products/lulu.html> and the popular "RansomWhere?" <https://objective-see.com/products/ransomwhere.html>. Potential unwanted Central-Processing Unit (CPU) activity, like cryptocurrency mining (cryptomining), or ransomware encrypting the user's disk can be also identified with different applications, like the useful and free MenuMeters <https://member.ipmu.jp/yuji.tachikawa/MenuMetersElCapitan>.

On the other hand, firewall applications, like the ones described above, monitor connections when Mac applications try to send information elsewhere. As said, that usually happens as soon as the computer is connected to Internet, either physically (eg., Ethernet cable) or wirelessly (eg., Wi-Fi). This way, the user can grant or deny a particular connection once or forever, creating rules to handle future connection attempts. That may seem and indeed is somewhat tedious once the firewall application is installed for the first time. But after a few minutes, once customized rules are defined, the application takes care of them in the background, being therefore unobtrusive and transparent to the user's workflow. This way, even malware like virus and trojan activity can be detected. A detailed description of how each firewall described above works is beyond the scope of this review, but significant instances will be illustrated below for Little Snitch, which was the first powerful commercial firewall for Mac released in 2004. These are general guidelines that should be abided by all firewall applications, in order of being more efficient, intuitive and user-friendly, effectively avoiding unprotected scenarios, as described below.

Curiously, such firewall-training behavior of Little Snitch has disturbed so much some users in the past, that its latest versions do not install by default the alert mode (the users are warned in real time of outbound requests, as indicated above), but the silent mode (the users are not warned of such requests). Yet—surprisingly—such silent mode is also set to allow connections. Such change is understandable from the point of view of the developer's support-department team. Thus, it should reduce beginner customer's calls for support, avoiding users' dissatisfaction in their first experiences and impressions about the firewall application. Yet, developers should give priority to user's protection, instead of just trying to reduce user's support calls. That is because, otherwise, it would jeopardize the purpose of this kind of firewall, which is to protect the user from outbound traffic in the first instance. Therefore, that should be a paramount and critical priority. In any case, the installer should clearly explain in plain English the pros and cons of each mode, and their consequences. Operation modes can be also configured from the application's preferences, should the users decide later on—at any time—, to change such settings. A third option of silent mode denying connections also shows in preferences. Yet, that would not make much sense in general, since it would block the

user from accessing Internet sites. Nevertheless, it may become handy in some circumstances requiring such blocking. On the other hand, most firewall applications are installed in the Applications folder of macOS or a subfolder created by the user. Little Snitch version 5 uses such name for the installed application, which is convenient (previous versions used a different name, which was confusing to some users).

The traditional Little Snitch firewall alert-prompt default allowed to deny or allow connections until quit, which was quite convenient. The most recent versions have also changed that, and now the default is to do it forever. That may induce some users—in a hurry; not fully reading such prompt window, etc.—used to previous versions to save as forever rules that they really do not really want saved like that. Therefore, the former prompt-interface implementation would be a better one. Fortunately, there are several ways to fix wrong or unwanted rules. One of them is to edit or delete them from Unapproved Rules within the application. There is also the option to see rules created or modified within the last 24 h. Likewise, there is the possibility to sort rules by date via "View-Sort By-Creation Date" submenu, which is quite handy to see the latest one created or edited. Additionally, the alert-prompt setting can be modified at "Preferences-Alert-Preselected Options". On the other hand, the default installation shows the Monitor window by default. That may look fancy initially, and even useful for advanced users, yet average users may probably want to turn it off at "Preferences-Monitor", since it may become irrelevant (not really checked on a regular basis), yet distracting from daily users' workflows.

Likewise, the new Little Snitch firewall versions continuously shows Notifications on the top-right corner of the Mac screen, which did not show with previous ones. That may be useful to some expert users, but may also have a significant negative impact on mental concentration and workflows, and thus overall productivity of average users. It would be useful if that could be configured in the application's preferences and not only in "Apple-System Preferences-Notifications", which on the other hand contains not one but three entries (which may be confusing): Little Snitch, Agent and Network Monitor. On the other hand, Little Snitch alert-prompts of the new versions require some delay when clicking the Deny or Allow options. Otherwise, the prompt-window vibrates to indicate that the user's click was not taken into account. Such vibration is fancy, yet the application should allow faster clicking, without requiring the current delay.

On the positive side, such alerts remain showing on the display foreground (waiting for the user to select the desired option), but do not block the user workflow, allowing to continue working on any other urgent task, if desired. Besides, it allows to prevent future alerts prompts, for instance, when opening a web page, previously saved as ".webarchive" with Safari web browser, for offline browsing or future reference. But if you select such file and press the keyboard space-bar to view its contents in Finder, via the nifty Quick Look, a lot of alert-prompts may arise, including the ones of advertisements or other links in such web page. Denying access to them may be time consuming. Fortunately, Little Snitch allows to select "Until Quit-Any Connection-Deny", so no more of such alerts will show until the Mac Finder is restarted. Even more convenient can be to select "Forever" instead. Then, such alerts will never show again, even after restarting the Mac, as far as such Finder rule remains in the firewall application, where it shows as "Deny any outgoing connection".

Alert prompts have also a useful feature that is activated clicking the top-right "Internet Access Policy" (IAP) icon <https://obdev.at/iap/index.html>. It shows explanations from a built-in database of the processes involved in such alerts. That is great and should be also available when double-clicking a rule and from "File-New Rule" submenu. Besides—and very importantly—such

database should be improved, to make it much more comprehensive. Additionally, it should clearly explain to the average user (not being informatician or computer expert) the activities and consequences involved by allowing or denying a particular requested process. As expected, the Little Snitch firewall application also allows to create, modify and delete rules from within the application. Also, to protect users from themselves, there are factory-set protected rules that can be disabled but not deleted, since they are required for computers to work properly. Nevertheless, the firewall application may show "Redundant Rules", which cannot be deleted by the user, generating the error "Cannot delete protected rules", which may be confusing. Redundant rules should not be considered as protected, for obvious reasons.

As a future improvement, it would be also most welcome if the Little Snitch firewall application had sets of factory pre-configured rules for common tasks, which should be comprehensive and flexible, as well as fully customizable by users. For instance, they could have options to allow or deny access of processes required for Apple updates via "Apple-App Store-Updates", for web browsers like Safari to browse the web, for Apple iCloud workflows, etc. That would save lots of work now required after the first firewall application installation on a particular computer, and would streamline the initial somewhat tedious configuration phase of creating rules in such scenario. That would be a great bonus for novice firewall users, as described above. That way, it would efficiently save also users from the initial frustration of being interrupted too often to allow or deny process calls in firewall alert mode. It would also save the developer's support-department team a lot of work from novice users' calls. This way, the installer could install in alert mode (which is the purpose of this kind of firewall), as done with previous versions and described above.

5. Which firewall is best?

Firewalls should be not only powerful, comprehensive and flexible; they should also follow the Mac interface guidelines. In other words, they should be simple and easy to use (intuitive). They should not need special computing knowledge to manage and use. Most importantly—for obvious reasons—, they should also warn users when becoming inactive (eg., when requiring a serial number to activate, not being compatible with a particular operating system version, etc.).

First of all, it is important to make sure that the macOS built-in firewall is active. Then, at least free firewall applications like Murus Lite or Lulu should be installed. But if privacy and security are truly valued, as they should be, it is critical to proactively take action for being really protected, in the best possible way. That involves installing at least a commercial application like Radio Silence, which is very easy to use and quite cheap. For a yet better protection, it is highly advisable to install the best firewall available (powerful, comprehensive and flexible, yet simple and easy to use). Which firewall is the best? That may depend on the users' requirements, and anyone may have specific requirements and preferences. Yet, selecting the best firewall from the plethora of available tools may be mind-boggling or overwhelming for some users. Fortunately, there is a good way to do it right: getting information from Internet and testing applications. They include demo versions that work for a determined period of time, so that is a great way to evaluate them first-hand, allowing to choose the best one.

In this regard, we live in the so called Global Village, and with today Computer Cloud Services, any Internet request could come from any place on planet Earth. Yet, it is also noteworthy that most computer attacks come from specific known areas of the world. So, receiving an alarm prompt to

allow or deny an outbound traffic to a suspicious site may provide an additional warning to users and is thus very much welcome. The new versions of Little Snitch excel on such aspect, since it has an interesting new feature, being capable to display a map showing geolocalization of outside servers requesting information from our Mac (Figure 9).

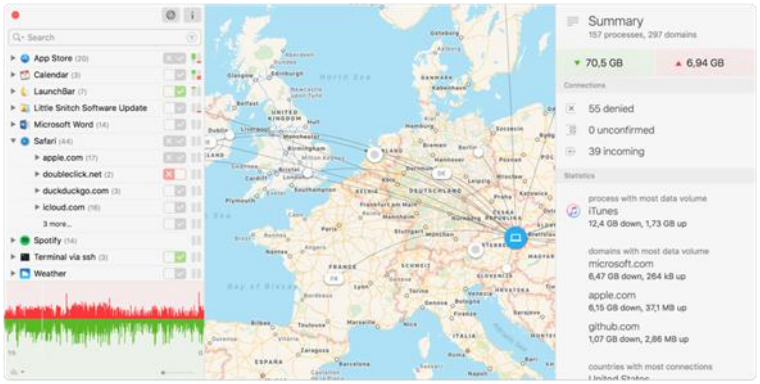

Figure 9. Little Snitch geolocalization of Internet connections. © 2021 Objective Development Software.

6. Protecting scientific bioinformatics environments with firewalls

As previously described, security and privacy should be always considered when connecting to Internet, being particularly relevant when computer servers are always connected, both in Intranet and—mostly—Internet networks. Such scenarios may involve scientific research, in general, and bioinformatics, in particular. At stake may be sensitive data related to Non-Disclosure Agreements (NDA), intellectual property, unpublished results, etc. Although a stateful firewall may protect such servers from foreign attacks, they may have installed productivity applications for bioinformatics, as well as other general-purpose productivity workflows. They may request outbound connections to send data to foreign servers elsewhere in the world. Thus, it is of paramount importance to install and configure firewalls capable of alerting users about such outbound traffic. That is where firewalls can warn and protect the users, as previously described. As an example, we have developed bioinformatics applications to take advantage of many-core microprocessors, and other purposes like teaching [3–10]. Our research workflows involve Mac, Windows and Linux computers which we protect with the corresponding firewalls. They include servers like <http://www.sicuma.uma.es/manycore> and users' computers like Macs, for which we use Little Snitch for the best possible protection with geolocalization for improved traffic monitoring, after testing available firewalls. Last, but not least, the new Little Snitch 5 is scriptable. Thus, it allows to use a command-line interface to configure settings and report network connections with exquisite detail, for comprehensive and versatile traffic analyses. That is a great bonus, and hopefully, an intuitive GUI will be implemented in the future.

7. Concluding remarks

The simplest and cheapest firewall is better than nothing. Some firewalls described above are great, like Little Snitch, yet they have space to grow and improve. For instance, the installer should

clearly explain the implications of alert versus silent modes, with default being the former, simply because that is the main purpose of any firewall. Also useful would be if firewalls had sets of factory pre-configured rules for common tasks, effectively saving users from the initial frustration of being interrupted too often to allow or deny process calls in alert mode. Additionally, a standalone offline user's guide or manual in PDF would be also most useful, besides the current online versions, also including all database details of the processes involved in the alerts.

A much more comprehensive database should be built by firewall developers, including process explanations about outbound-traffic prompts, so that the users may decide between allowing or denying them, until the application quits, or forever. There is good news in this respect, since an IAP has been already implemented in Little Snitch. It allows third-party application developers to bundle a policy file with their application. It contains information about the Internet connections that their programs are about to establish, and their purposes. In other words, that tells the user what is going to happen (or not going to work out properly) if a particular connection is allowed or denied, respectively. Obviously, this is a work in progress, and the more IAP are implemented, the better. They are also currently working on a strategy to spread such knowledge among the users, including an Internet Access Policy Viewer application <https://www.obdev.at/products/iapviewer/index.html>. Last but not least, in any case, common sense should be also exerted in any scenario that involves allowing or denying Internet connections.

Acknowledgments

Supported by "Ministerio de Economía y Competitividad" (MINECO) and "Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria" (MINECO and INIA RF2012-00002-C02-02); "Consejería de Agricultura y Pesca" (041/C/2007, 75/C/2009 and 56/C/2010), "Consejería de Economía, Innovación y Ciencia" (P1-AGR-7322) and "Grupo PAI" (AGR-248) of "Junta de Andalucía"; and "Universidad de Córdoba" ("Ayuda a Grupos"), Spain.

Conflict of interest

The authors declare no conflict of interest.

References

1. Bazzell M and Carroll J, (2016) *The Complete Privacy & Security Desk Reference: Digital*. Scotts Valley, CA, USA: CreateSpace-Amazon.
2. Bazzell M and Carroll J, (2018) *The Complete Privacy & Security Desk Reference: Physical*. Scotts Valley, CA, USA: CreateSpace - Amazon.
3. Diaz D, Esteban FJ, Hernandez P, et al. (2011) Parallelizing and optimizing a bioinformatics pairwise sequence alignment algorithm for many-core architecture. *Parallel Comput* 37: 244–259.
4. Diaz D, Esteban FJ, Hernandez P, et al. (2014) MC64-ClustalWP2: a highly-parallel hybrid strategy to align multiple sequences in many-core architectures. *Plos One* 9: e94044.
5. Esteban FJ, Diaz D, Hernandez P, et al. (2013) Direct approaches to exploit many-core architecture in bioinformatics. *Future Gener Comput Syst- Int J Esci* 29: 15–26.

6. Esteban FJ, Diaz D, Hernandez P, et al. (2018) MC64-cluster: many-core CPU cluster architecture and performance analysis in B-tree searches. *Comput J* 61: 912–925.
7. Gálvez S, Agostini F, Caselli J, et al. (2021) BLVector: Fast BLAST-like algorithm for manycore CPU with vectorization. *Front Genet (Sect Comput Genomics)* 12: 618659.
8. Galvez S, Diaz D, Hernandez P, et al. (2010) Next-generation bioinformatics: using many-core processor architecture to develop a web service for sequence alignment. *Bioinformatics* 26: 683–686.
9. Galvez S, Ferusic A, Esteban FJ, et al. (2016) Speeding-up bioinformatics algorithms with heterogeneous architectures: Highly heterogeneous smith-waterman (HHeterSW). *J Comput Biol* 23: 801–809.
10. Redel-Macias MD, Pinzi S, Martinez-Jimenez MP, et al. (2016) Virtual laboratory on biomass for energy generation. *J Cleaner Prod* 112: 3842–3851.

AIMS Press