

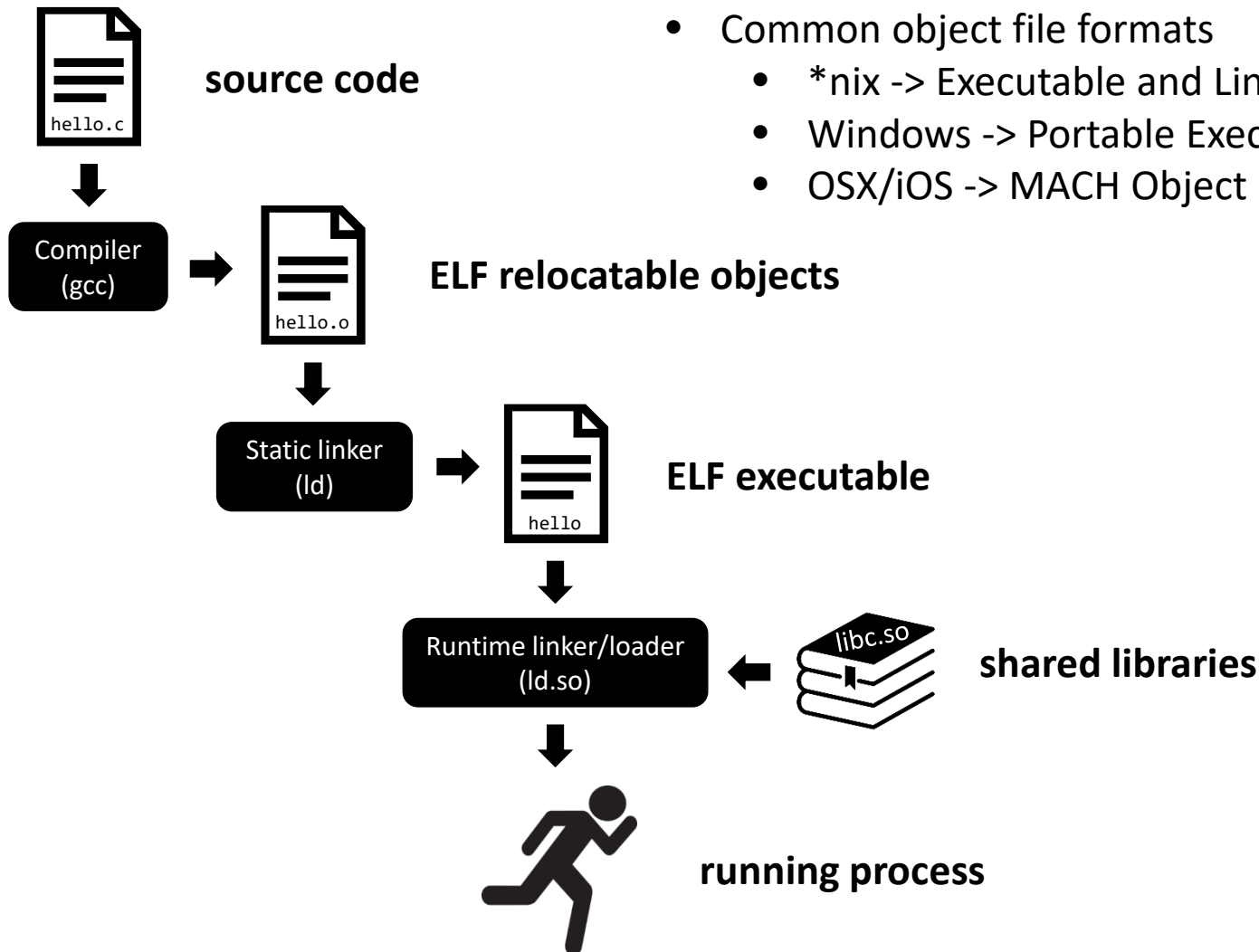
Mitigating and Preventing Vulnerabilities with ELFbac

Ira Ray Jenkins, Dartmouth College



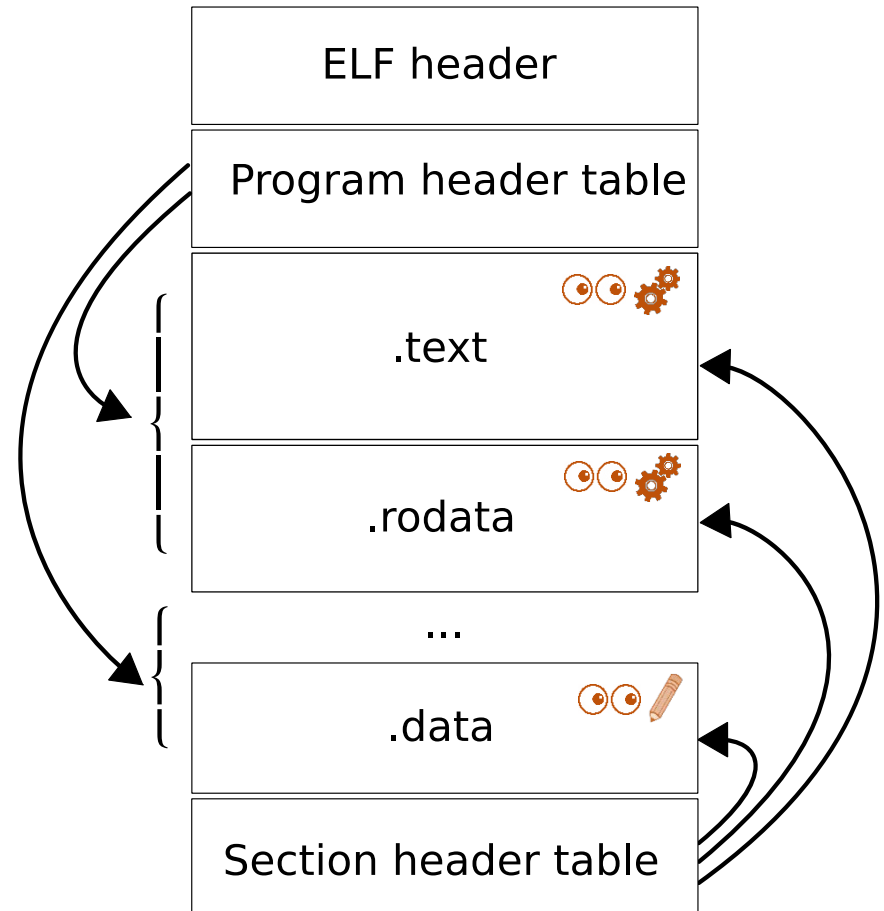
Code to Process

- Common object file formats
 - *nix -> Executable and Linkable Format (ELF)
 - Windows -> Portable Executable (PE)
 - OSX/iOS -> MACH Object (MACH-O)



Sections & Segments

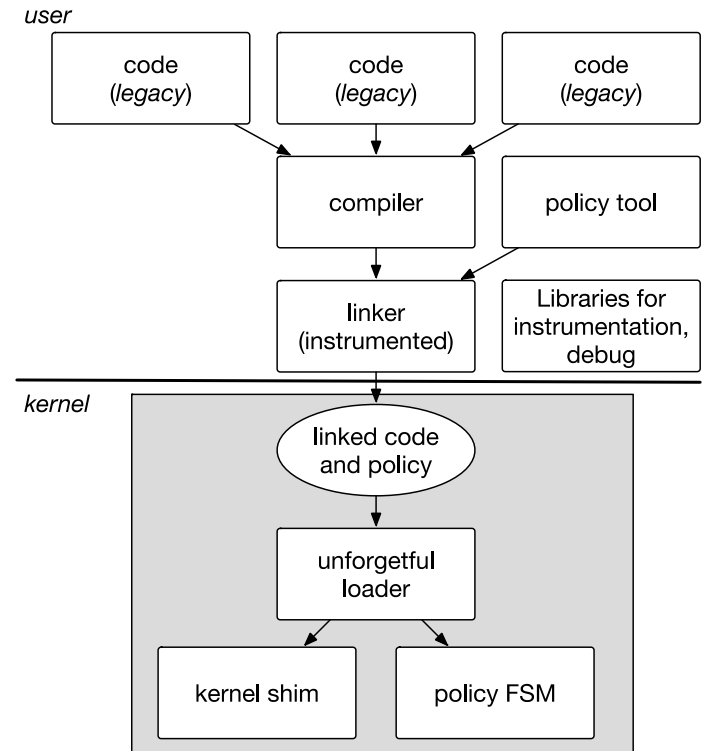
- Executable and Linkable Format (ELF) files contain the code and data for a given executable, as well as metadata necessary for the creation of a process address space.
- Sections contain the code and data of a program.
 - Each section defines semantically distinct units of code and data
- Segments are groupings of sections.
 - Segments are loaded at runtime into the process address space
 - Segments define the permissions of memory sections



Programmer intent is discarded in the packing of sections into segments!

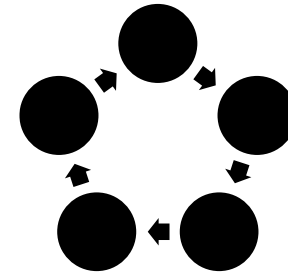
ELF-Based Access Control

- Goal: Reclaim the programmer intent discarded by a “forgetful” loader
- Code is annotated, compiled, and linked with ELFbac policy
- An “unforgetful”, ELFbac-aware, loader builds the process address space with the policy, creating the desired isolation
- An ELFbac-aware kernel enforces the policy during runtime



ELFbac Policy Creation

- Policy is as a Finite State Machine.
 - States define a particular abstract phase of program execution driven by a given section of code, e.g., input parsing, network code, or cryptographic code
 - Transitions between states are achieved via memory accesses (“data transitions”) and function calls (“call transitions”)
- ELFbac policy is defined via linker scripts in simple JSON.
 - Defining custom sections, their access controls, and any intersectional relationships
 - Semantic policies, e.g., “input data can only be read by parsing functions”
- Code is annotated to use the policy via compiler pragmas:
 - `__attribute__((section(". inputs"))) int debug_flag = 0;`



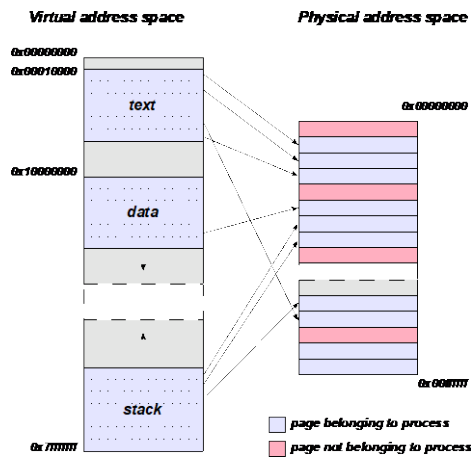
```
"name": "Parse",  
"sections" : [{  
  "name": "inputs",  
  "description": "*(. .data.secret) ", "flags": rw }  
]
```

```
"call_transitions": [ {  
  "from": "Parse",  
  "to": "Calculate",  
  "address": "GoToCalculate()" } ]
```



ELFbac Policy Enforcement

- Replaces the kernel's view of a process' virtual memory context with a diversified collection of "shadow" contexts, each representing a single policy state.
 - Each shadow context only maps those regions of memory that can be accessed in the current state according to the policy.
 - Achieved through Page Tables and Virtual Memory mappings.
- Policy violations (unintended memory accesses or function calls) are trapped, leading to error handling code or ultimately a segmentation fault.



Process View



Kernel View

OpenSSH is Ubiquitous



- Most popular implementation of the Secure Shell (SSH) network protocols
 - Used to securely connect to and manage remote devices

Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Control Systems

SSH SCANNING

Released: Monday, April 26, 2016 - 10:45

Overview

ICS-CERT is aware that many organizations have been seeing a large number of attempts to access industrial control systems by remote attackers. Common targets for these brute force attacks are systems that provide secure shell (SSH) command line access. This activity has been going on for a number of years in the IT sector and demonstrates the need for operators of control systems to understand this threat, what to look for, how to protect network perimeters, and when to report such occurrences.

Official website of the Department of Homeland Security

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Control Systems

Alert (ICS-ALERT-12-034-01)

SSH Scanning Activity Targets Control Systems

Original release date: February 02, 2012 | Last revised: February 13, 2017

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any guarantee of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

Summary

ICS-CERT is issuing this alert to inform critical infrastructure and key resource (CIKR) asset owners and operators of recent and ongoing activity involving secure shell (SSH) scanning of internet facing control systems. ICS-CERT is aware that many organizations have been seeing a large number of access attempts by remote attackers. Systems that provide SSH command line access are common targets for "brute force" attacks.

As recently as this week, ICS-CERT received a report from an electric utility experiencing unsuccessful brute force activity against their networks.

CIO

NEWS

Millions of embedded devices use the same hard-coded SSH and TLS private keys

The keys were hard-coded by manufacturers and can be used by attackers to launch man-in-the-middle attacks

By Lucian Constantin
Romania Correspondent, OSNews Service | NOV 26, 2015 05:49 PT

Home Hacking Tech Deals Cyber Attacks Malware Spying

The Hacker News
Security in a serious way

12-Year-Old SSH Bug Exposes More than 2 Million IoT Devices

Thursday, October 13, 2016 | Mohit Kumar

One Giant Leap for Security
Discover the Next Frontier of Threat Detection

Drives & Controls

The global site of the UK's leading magazine for automation, motion engineering and power transmission

Home News Features Blogs & Opinions Buyer's Guide Events Jobs Magazine Exhibition

Product and Supplier Search

Search for UK supplier by name

Search

OR Browse for a type of product

Beatings

Search

Powered by Drives & Controls

Home News Technology News

'Groundbreaking' control system 'brings future to the present'

14 FEBRUARY, 2018

The Californian industrial controls developer Opto 22 has announced a "groundbreaking" industrial control technology that, it says, "brings the future of automation to the present" by combining I/O, real-time control, local and remote HMI, and industrial/IT data exchange in a single compact package.

Magazine

Drives & Controls

To view a digital cover

"The company believes that its optional access to the Linux operating system through a secure shell (SSH) will be of particular interest to OEMs."

Shodan Developers Book View All...

SHODAN product:"OpenSSH"

Exploits Maps Share Search

TOTAL RESULTS

10,572,332

TOP COUNTRIES

United States 4,234,248

China 1,033,090

Germany 803,699

France 635,516

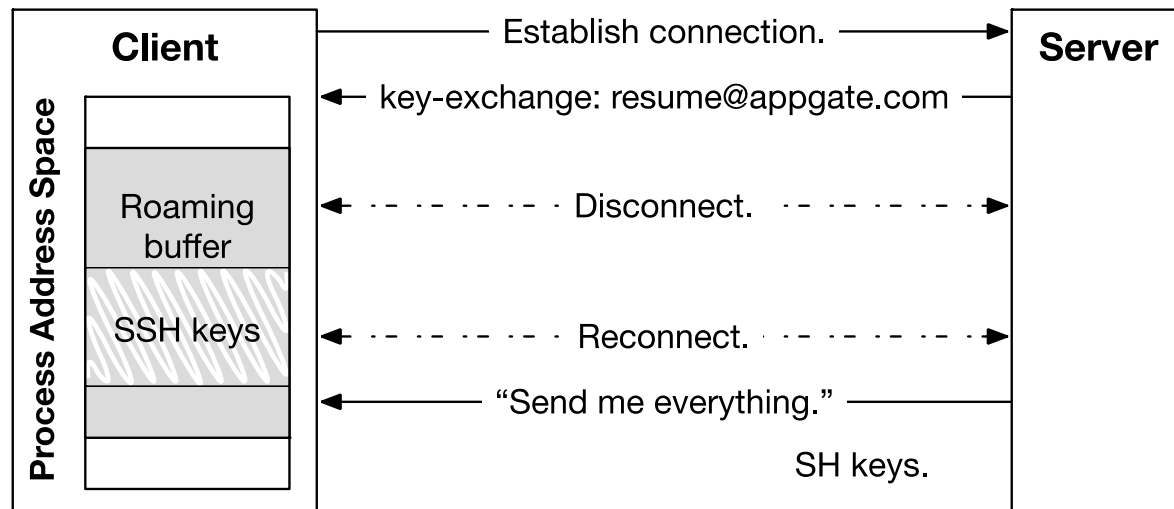
Russian Federation 339,848

TOP SERVICES

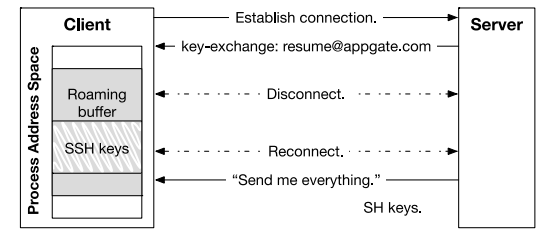
SSH 9,658,834

Roaming in OpenSSH

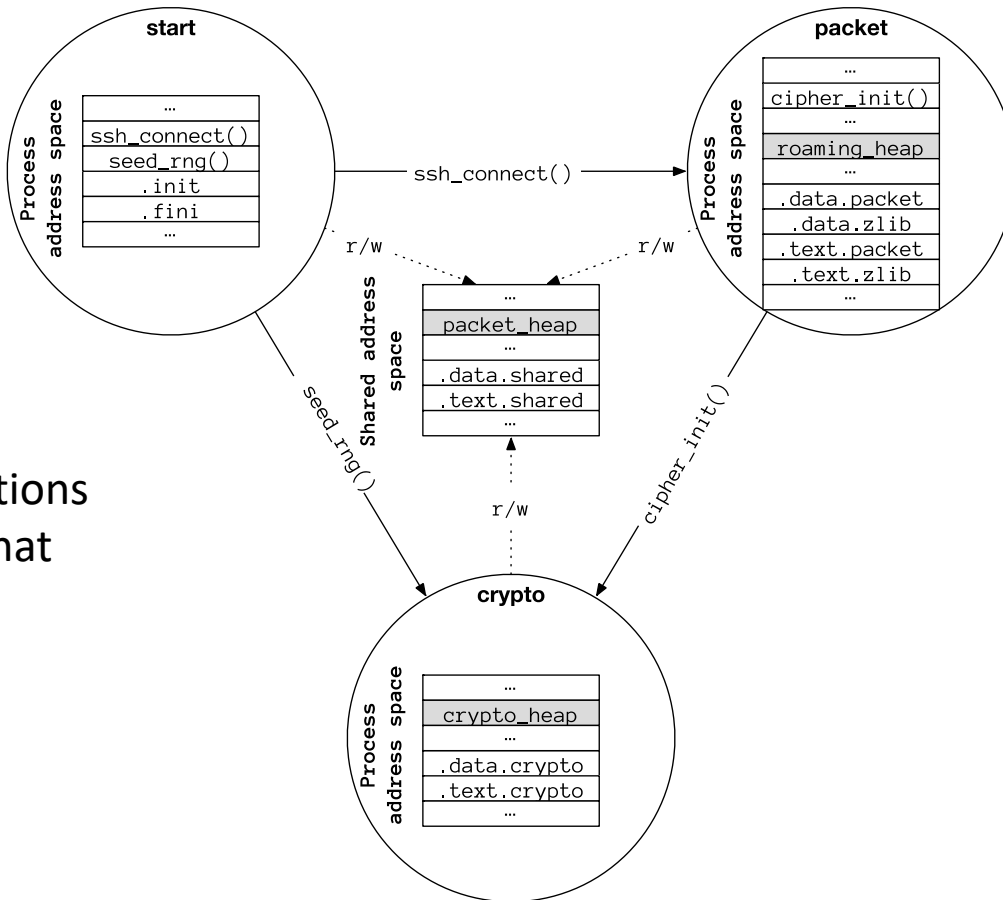
- In version 5.4, released in 2010, the OpenSSH client introduced an experimental and undocumented "roaming" feature.
- The purpose of roaming was to allow the resumption of suspended sessions, e.g., in the case of unexpected network termination.
- In 2016, CVE-2016-0777 disclosed an information leak present in the implementation of OpenSSH's roaming feature.



Mitigating the Roaming Bug

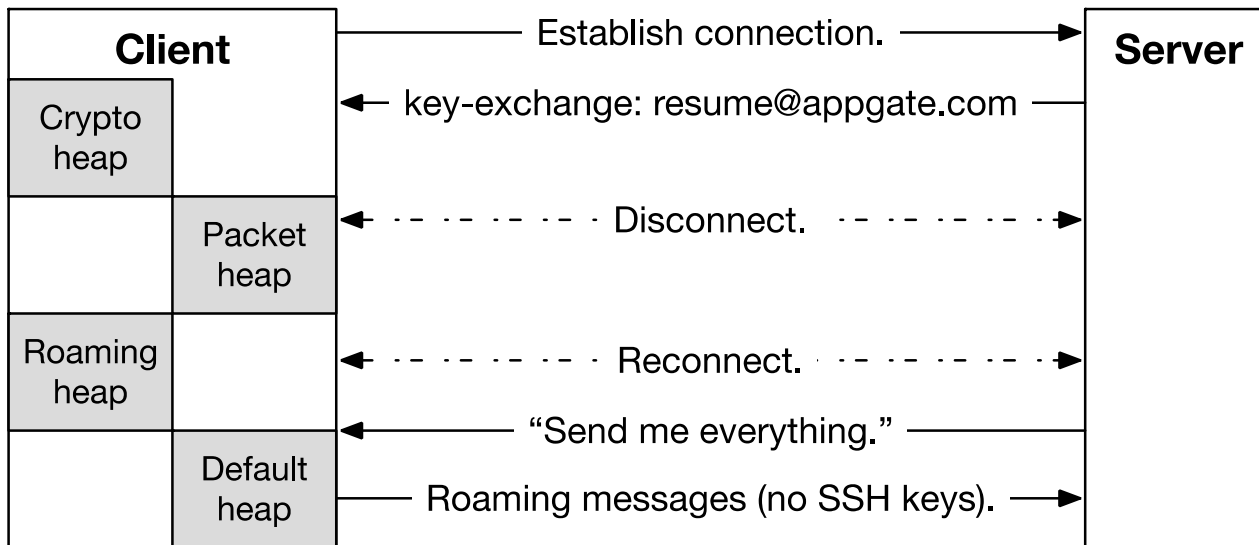


- Goal: Use ELFbac to isolate the memory regions used to store cryptographic keys and the roaming buffer.



In total, 27 annotations in 4 files were all that was necessary to achieve the critical isolation.

Execution with Mitigation



Demo



Conclusions

- Programmer intent is a crucial part of software security
- ELFbac allows a programmer to codify intent into enforceable policy
- Were ELFbac to have been used in OpenSSH, this bug would never have occurred
- ELFbac is as flexible and robust as a software's modularity
 - More modular -> more easily isolated

Future Work

- Policy creation relies largely on codebase familiarity and intuition...
- Performance can be a problem...
- Multiple policies in a single executable...
- Where does ELFbac fit with the IoT and ICS...
- Mitigating Spectre...?

Thanks!



CYBER RESILIENT ENERGY DELIVERY CONSORTIUM



<http://cred-c.org>



@credcresearch



facebook.com/credcresearch/

References

- <https://memegenerator.net/instance/81422724>
- <https://ics-cert.us-cert.gov/tips/CSAR-10-114-01>
- <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-034-01>
- <https://www.cio.com/article/3009140/millions-of-embedded-devices-use-the-same-hard-coded-ssh-and-tls-private-keys.html>
- <https://thehackernews.com/2016/10/sshowdown-iot-security.html>
- http://drivesncontrols.com/news/fullstory.php/aid/5652/91Groundbreaking_92_control_system_91brings_future_to_the_present_92.html
- <https://www.shodan.io/report/jaGB3De1>
- https://commons.wikimedia.org/wiki/File:Document_text.svg
- <https://openclipart.org/detail/275692/icon-book>
- <http://www.clker.com/cliparts/5/j/m/Z/s/z/runrunrun-md.png>
- <https://commons.wikimedia.org/wiki/File:Elf-layout--en.svg#/media/File:Elf-layout--en.svg>
- <http://clipartbarn.com/wp-content/uploads/2016/10/Eyes-eye-clip-art-free-clipart.jpg>
- <http://www.nextreflexdc.com/pencil-clip-art/pencil-clip-art-free-pencil-clipart-public-domain-pencil-clip-art-images-and-4-download/>
- <https://openclipart.org/detail/256083/gears>
- https://en.wikipedia.org/wiki/Virtual_address_space#/media/File:Virtual_address_space_and_physical_address_space_relationship.svg

