sponsored by

Telkom

COMVERSE

STORTECH For Your Information

tellabs

easttel

Bright Ideas Projects 39

THRIP TECHNOLOGY AND HUMAN RESOURCES FOR INDUSTRY PROGRAMME

RHODES UNIVERSITY
Where leaders learn

CONVERGENCE RESEARCH GROUP

A less attack-prone, Internet deployment of iLanga

Researcher: Courage Radu

Email: g11r3764@campus.ru.ac.za

Supervisor : M. Tsietsi

Co-Supervisor : A. Terzoli

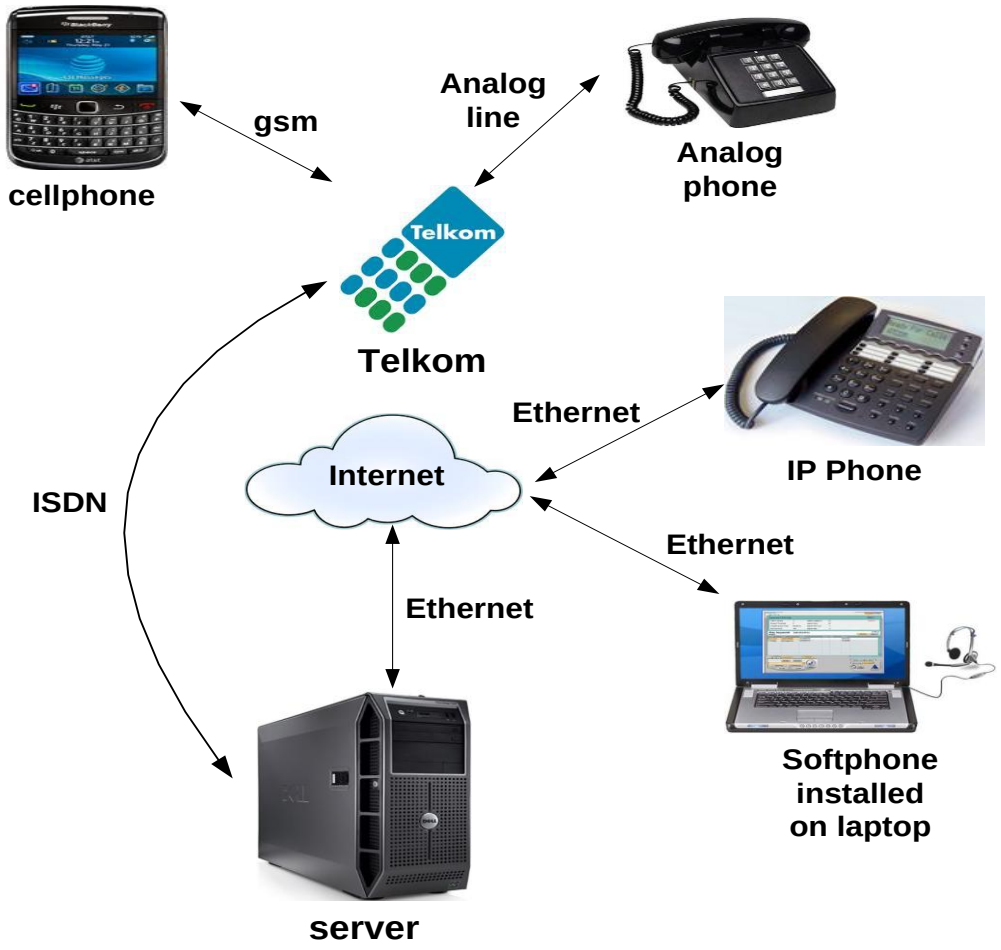
Outline

1) Background
2) Motivation
3) Threats
4) Approach
5) Asterisk security
6) Conclusion
7) Possible extensions
8) Questions and answers

Background

- iLanga is an open computer based telecommunication system
- Objective of project is to have a securely deployed iLanga
- A guide with best security practices
- Developed a web based UI to easy up security administration

Background


cellphone
gsm
Analog
line
Analog
phone
Telkom
Telkom
Ethernet
IP Phone
ISDN
Internet
Ethernet
Ethernet
Softphone
installed
on laptop
server

Background

- Ubuntu Linux – operating system
- Asterisk – software implementation of a PBX
- Kamailio – proxy server for authentication
- MySQL – database to store user information

Motivation

- The system uses open source software
- The system can be deployed at tertiary institutions, small business enterprises, etc
- Affordable hardware extensions
- Security is not inherently enabled and configured by default

Threats

- Brute force attack – password guessing
  - Session Initiation Protocol (SIP) brute force

```
[Nov  6 02:57:48] NOTICE[18681]: chan_sip.c:21687 handle_request_register:
Registration from '"9964"<sip:9964@146.231.121.132>' failed for
'85.14.178.21' - No matching peer found
[Nov  6 02:57:48] NOTICE[18681]: chan_sip.c:21687 handle_request_register:
Registration from '"9965"<sip:9965@146.231.121.132>' failed for
'85.14.178.21' - No matching peer found
```

  - Root account brute force

```
June 16 12:16
Failed password for root from 95.141.193.46 about 40 attempts
Failed password for invalid user test from 95.141.193.46 3 attempts
Failed password for invalid user nagios 2 attempts
Failed password for invalid user postgres 2 attempts
Failed password for invalid user oracle 1 attempt
```

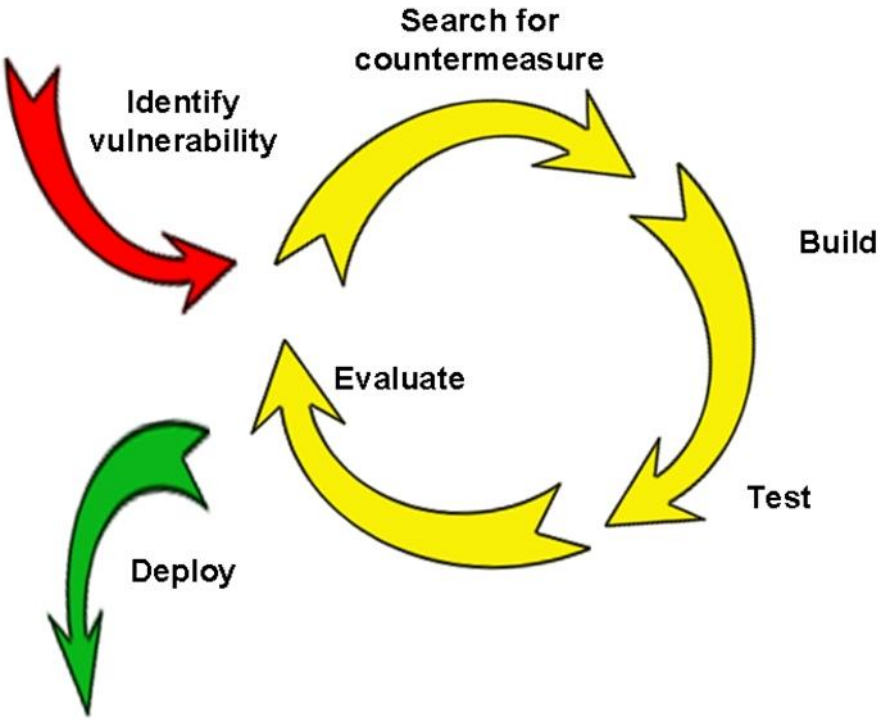
Threats

- Toll fraud
  - unauthorised long distance calls

"asterisk" <asterisk>	SIP/91.223.89.51-00000003	DAHDI/1-1	Dial	DAHDI/1/00251116610588|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-00000006	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-00000009	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-0000000c	DAHDI/1-1	Dial	DAHDI/1/00251116612354|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-0000000f	DAHDI/1-1	Hangup	
"asterisk" <asterisk>	SIP/91.223.89.51-00000012	DAHDI/1-1	Dial	DAHDI/1/005372042516|20|r
"asterisk" <asterisk>	SIP/91.223.89.51-00000015	DAHDI/1-1	Dial	DAHDI/1/002204495134|20|r

- Dos
  - service disruption

Approach


Search for
countermeasure
Identify
vulnerability
Build
Evaluate
Test
Deploy

Preliminary phases

- Current state-of-art of the system
  - documenting versions for each component
- Replicated the system
- Learning the system
  - how asterisk handles phone calls
  - how the components are integrated

Asterisk security

- Install Asterisk PBX as non-root
  - a remote security compromise should not be used to take over the entire machine
- Set the variable alwaysauthreject = yes
  - prevent attacker from scanning for valid usernames
- Change Session Initiation Protocol (SIP) default port 5060
  - change default port to any unused random port number

Asterisk security (Cont.)

- Use public key authentication for SSH login
  - disable password authentication

- Secure dialplan
  - properly designed diaplan prevent tool fraud
  - well programmed dialplan will prevent dialplan injection
  - a secured default context will not cost the organisation

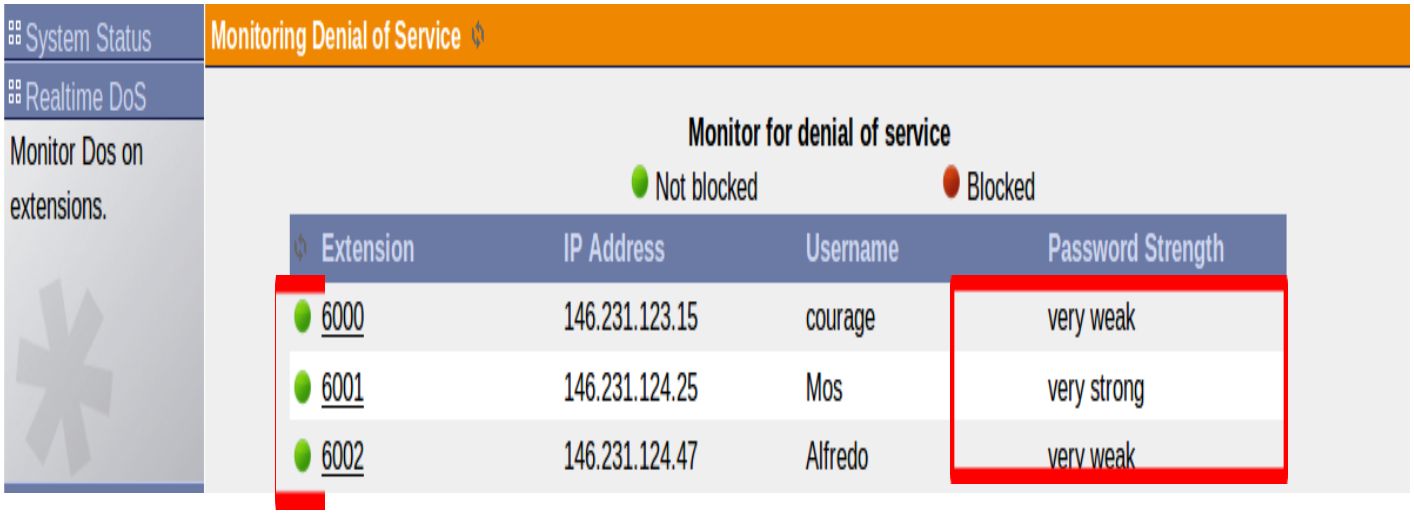
Asterisk security (Cont.)

- Perl script
  - ban IP address with more than 6 wrong passwords

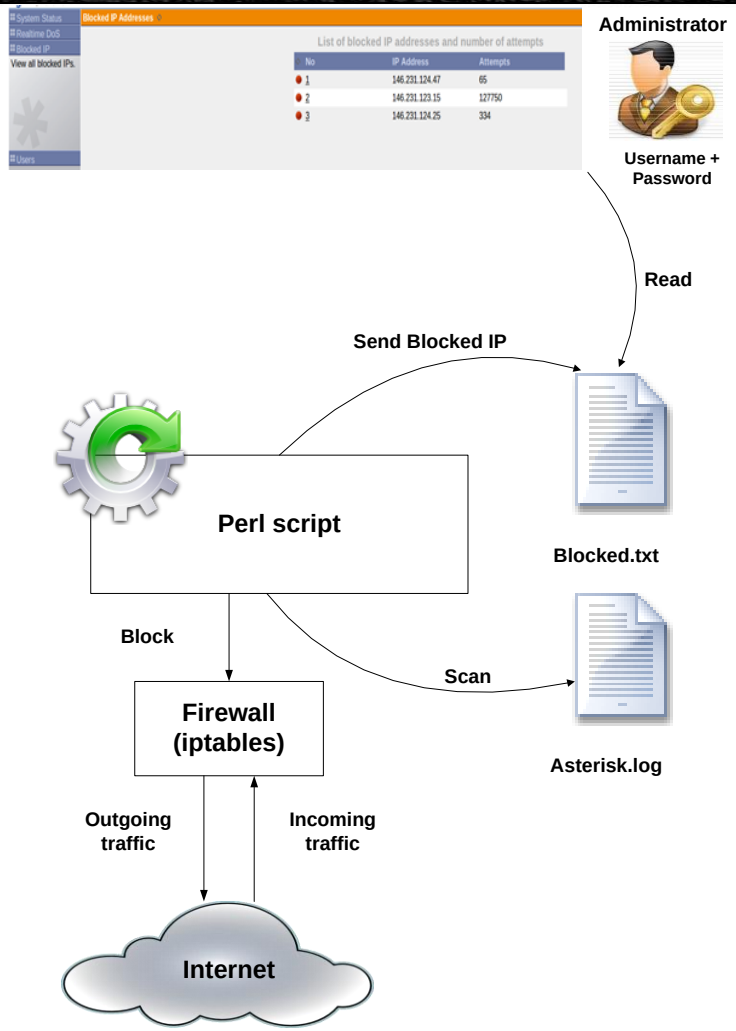
```
19  if ($line =~ m/\' failed for \'(.*?)\' - Wrong password/) {
20      push(@failhost,$1);
21  }
22  if ($line =~ m/\' failed for \'(.*?)\' - No matching peer found/) {
23      push(@failhost,$1);
24  }
25  if ($line =~ m/\' failed for \'(.*?)\' - Device does not match ACL/) {
26      push(@failhost,$1);
27  }
28  if ($line =~ m/\' failed for \'(.*?)\' - Peer is not supposed to register/) {
29      push(@failhost,$1);
30  }
```

Asterisk security (Cont.)

- Perl script monitors DoS and password strength for legitimate users

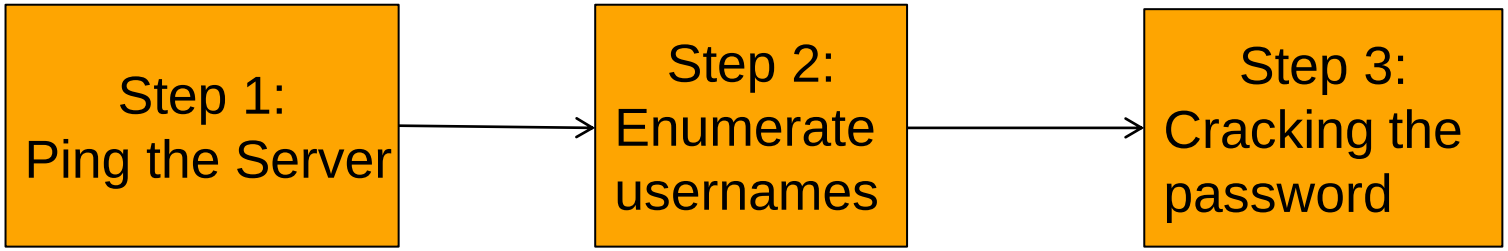


Asterisk security (Cont.)



Video Demonstration

- Scenario – an intruder want to enumerate usernames and crack passwords on iLanga
  - perl script is running in background
  - the administrator should view the blocked IP address via the browser



Results

- Intrusion prevention script effectively quarantines offending IP addresses
- Sipvicious tool can generate an average of 170 password attempts per second on Intel(R) Core(TM) i7 CPU @ 2.93GHz

Conclusion

- Open source software empower institutions and small organisations to deploy communication systems like iLanga
- iLanga brings different components together but we have to configure and enhance security features in it
- Create an image with necessary security features pre-enabled and distribute it to other institutions (UFH and NMMU)

Possible extensions

- Extension of the UI so that the administrator can view all security information.
- The security information is scattered everywhere within the system.
- The interface should be able to lighten the burden for non-linux experts.

Questions and Answers