ISOI XV

8 October 2015

The Spencer Hotel, Dublin, Ireland

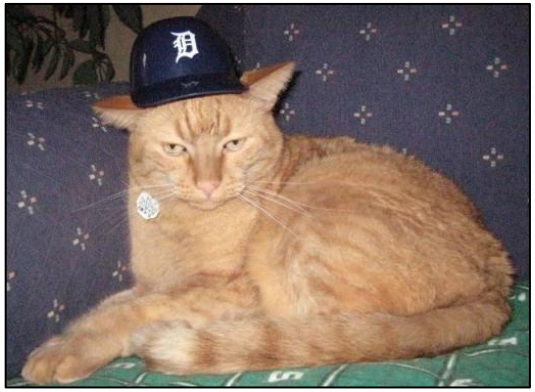
Trident – Sharing is Scaring the Bad Guys

Jeroen Massar, Ops-Trust / Trident.li
jeroen@massar.ch

Jeroen's Hats

- Work:
  - Farsight Security (http://www.farsightsecurity.com)

- Fun:
  - Ops-Trust (https://www.ops-trust.net)
    - Sysadmin – keeping it running smoothly
  - Trident Project (https://trident.li)
    - Design & Implementation
  - SixXS (https://www.sixxs.net)
    - IPv6 Deployment



Ops-Trust

As per https://openid.ops-trust.net/about:

“OPSEC-Trust (or "ops-trust") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet.”

Also known as “Ops-Trust” or just “Ops-T”.

Ops-T Trust Groups

- Initially started out with a single Trust-Group
- Smaller TGs added for specific problems
- Each TG has own purpose and policies
- Being in one TG does not mean you are automatically in any other, or that you even know about them
- Each Trust Group gets:
  - One or more mailinglists,
    - optional required PGP encryption
  - Wiki & Files area
  - Member Portal

Trust!

- The most important thing: Trust
- If one person does something ‘wrong’ the ones who vouched the person are accountable
- Unless specifically mentioned with Traffic Light Protocol indicators, communications must never leave the person who received it:

“All message content remains the property of the author and must not be forwarded or redistributed without explicit permission.”

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

https://www.us-cert.gov/tlp

Ops-Trust Code Base

- Codebase:
  - Perl using Mason for “portal”, Open-ID uses Catalyst
  - External perl dependencies, many not in Debian packages
  - Database: PostgreSQL
- Components:
  - PGP-remailer
  - Web-frontend “portal” for managing vouches, finding people
  - Open-ID for authenticating at external resources
  - Two Factor Authentication using HOTP/TOTP/SOTP
  - Foswiki as a Wiki (initially we used Confluence)
- Open Source!
  - https://github.com/ops-trust/

Trident

- Complete from-scratch rewrite in only Go (https://www.golang.org)
- Only the PostgreSQL database schema survived
- Focus on cleanliness and less work for sysadmin:
  - TG Admins have full control over their own TG.
- Nothing 'external' (eg foswiki leaves 'portal' portion)
- Simplified installation: Debian Package (will try to get it in Debian proper)
- Simplified upgrades: tridentd knows how to upgrade DB
- Open Source: Apache License
- Multi-host support (multiple tridentd's) for load balancing and failover (work is scheduled using PostgreSQL)

Trident - Backend

- Daemon (tridentd) that serves HTTP, fronted by nginx
- Command Line (Tickly / tcli) enables full control
- WebUI/CLI feature parity: just with pretty buttons
- HTTP API which equals the CLI, as it is the CLI
- Integrated OAuth2 / Open-ID Connect support
  - Also used for CLI authentication
- Uses JSON Web Token (JWT) for authentication thus allowing easier automation

Trident - Frontend

- Bread > Crumbs > For > Easy > Navigation
- Two Factor Authentication using HOTP/TOTP/SOTP
- Mobile-aware (resizes to fit your screen using CSS)
- Integrated Wiki based on EpicEditor, BlueMonday + BlackFriday: thus ‘standard’ github flavored markdown
- SQL-based and cachable thus much faster than Foswiki
- Pretty with CSS, no javascript needed (only for pretty wiki editor)
- File upload/downloads/management
- Calendaring with CalDAV support for Events

http://www.epiceditor.com
https://github.com/microcosm-cc/bluemonday
https://github.com/russross/blackfriday

Trident - Mail

- PGP-remailer is integrated and supports queuing internally thus can see status of delivery of a message
- Outbound bounce handling handled directly, thus can better inform a TG admin of problems with delivery of mail to a member
- Handles lists with >10k members much better, if one needs more capacity, just add another node
- LMTP instead of forwarding, thus no more DSN for inbound mail (DSN is “delivery status notification” aka bounce)

Auth Token Support

- Implemented:
  - TOTP - Time-based One-Time Password
  - HOTP - HMAC-based OTP
  - SOTP - Single-use OTP
- Tools:
  - Google Authenticator (Android/IOS)
  - Nitrokey [also pgp]
    - https://www.nitrokey.com
    - Open Source Hardware & Software
  - Yubikey [also pgp]
- Planned
  - FIDO U2F (https://fidoalliance.org/)

Your Own Instance

- Don’t trust Ops-T sysadmin? (eg, do you trust me? :)
- Want to keep data local?
- Want your own Secret Fight Club?

- Then soon you’ll be able to install your own instance.
- Debian packages are already being generated and used for a couple of beta instances with >1000 active users.

- Code soon on: http://github.com/tridentli
- Watch the announcements on https://twitter.com/tridentli/

Future Features

- “Home page” like on your favorite social network with latest contributions & changes
- Visualized Trust Graphs
- Jabber + RobustIRC integration
- Mail to web, thus being able to read list as a forum and contribute using the webinterface
- Federation: profile sharing with other Trident instances
- FreeBSD Package

What do you miss?

- Integration?
  - MISP – Malware Information Sharing Platform (http://www.misp-project.org)
  - CIF – Collective Intelligence Framework (https://github.com/collectiveintel/cif-v1)
  - others?
- Workflow
  - “Tickets?”
  - ASN / IP-lists / notes?

Questions?

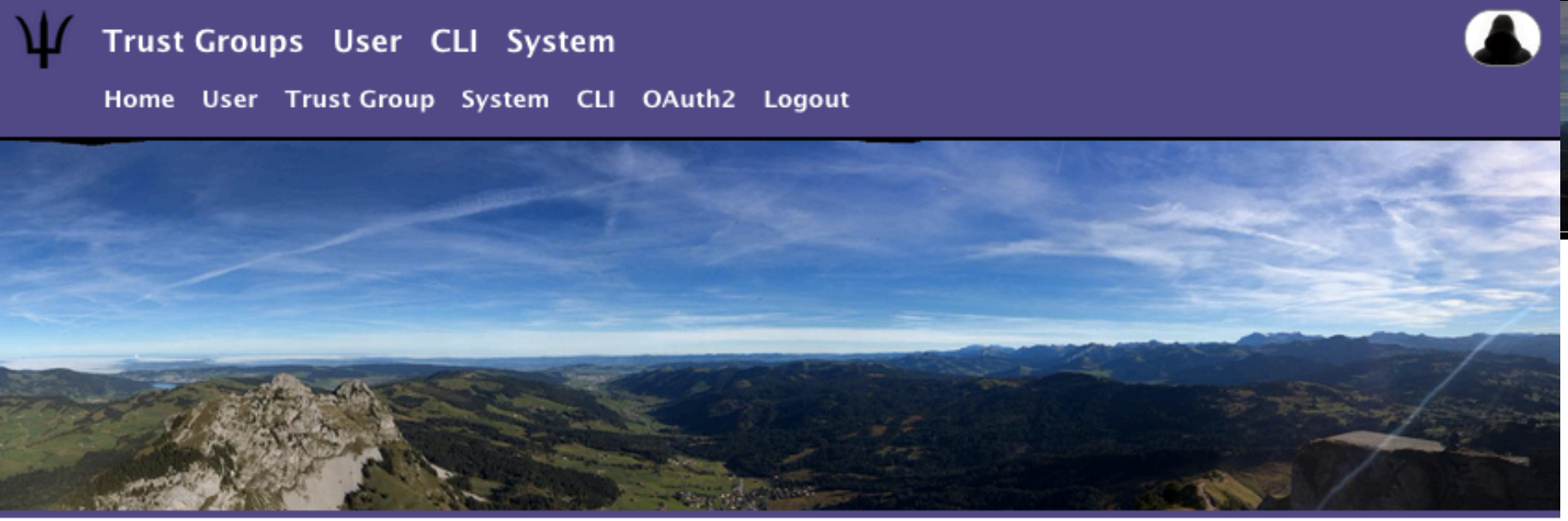
Jeroen Massar

jeroen@massar.ch

https://trident.li / project@trident.li

PGP: 0x123421B735578C46

(some screenshots are after this slide)



Home

Home

Not Configured

User Home

:16

Test

Table of Contents

Test Test

- List 1
- List 2

Links

- Trident
- NewTestPage

Code Example

```
code
    which is properly spaced
  and indentation works.
```

Table

First	Second
1	2
One	Two

Markdown Editor

```
# Test

## Test Test

* List 1
* List 2

## Links

 * [Trident](https://Trident.li)
 * [NewTestPage]
(https://tst.trident.li/tg/test/wiki/NewTes
tPage)

## Code Example

```
code
    which is properly spaced
  and indentation works.
```

Table

First	Second
1	2
One	Two
```

HTML Preview

Test

Test Test

- List 1
- List 2

Links

- Trident
- NewTestPage

Code Example

```
code
    which is properly spaced
  and indentation works.
```

Table

First	Second
1	2

System > **Settings**

Settings

System Name: Not Configured

Welcome Text:

Not Configured

Name of the Admistrator(s): Tester

Administrator Email Address: test@example.cc

Copyright Years: 2015

Public URL: https://tst.triden

People Domain: people-tst.triden

CLI Enabled:

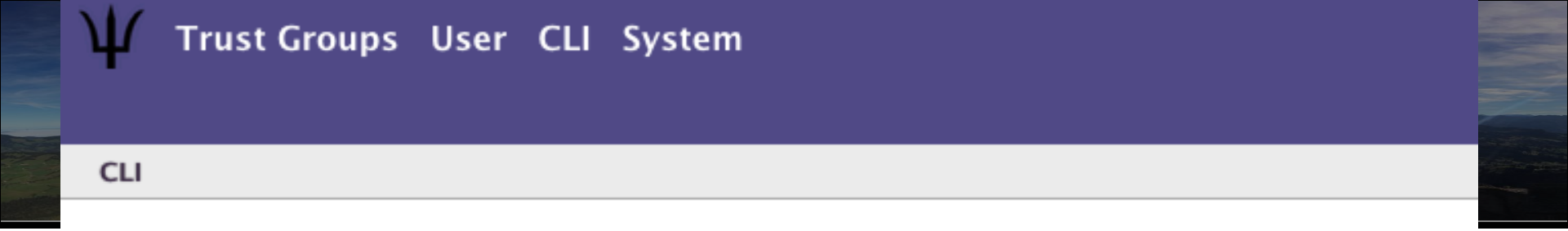
API Enabled:

OAuth/OpenID Enabled:

No Web Indexing:

Email Signature:

All message content remains the property of the author
and must not be forwarded or redistributed without explicit permission.



Tickly (Trident CLI)

Output:

```
-=- Trident Help -=-

Welcome to the Trident menu system which is CLI command based.
If a given command is not in help menu the selected user does not have permissions for
it.

Each section, items marked [SUB], has its own 'help' command.

The following commands are available on the root level:
 user                    [SUB]                 User commands
 tg                      [SUB]                 Trust Group (tg) commands
 ml                      [SUB]                 Mailing List commands
 wiki                    [SUB]                 Wiki commands
 system                  [SUB]                 System commands
```

Command: help

Execute