我们的征途是 HardenedLinux 社区

ID: Samson W
sccxboy@gmail.com

#whois

* Samson W
* Day job at 炼石网络 CipherGateway
* 系统工程师
* 自由软件支持者
* EFF/FSF 会员
* Hardenedlinux 社区 (http://hardenedlinux.org/) 成员

#founder

* citypw(Shawn C)
* Day job at EVIL Labs
* GNU/Linux 安全工程师
* 自由软件狂热分子
* EFF/FSF/FSFE 会员
* Hardenedlinux 社区 (http://hardenedlinux.org/) 发起人

HardenedLinux

#list

* Beginning
* HardenedLinux 社区愿景
* HardenedLinux 社区成员组成
* HardenedLinux 社区项目
* HardenedLinux 社区对外贡献（捐赠与文档分享）
* HardenedLinux 社区未来关注的方向
* 如何关注我们

#Beginning

* when:
  2014

* why:
  * Truth
  * Anarchists
  * Cyber security
  * Defense In Depth

现状

今天的 IT 基础设施 (IDC 、 数通产品等 ） 及物联网、 移动网络都重度依赖自由软件，自由软件已经成为重要基础设施的一部分，不管对于政府、企业、个人都是非常重要的。

资助 HOST(美国国土安全部的开放安全技术 ） 项目的美国国土安全部的在 13636 号行政命名中描述到：“这是美国改善安全和国家重要基础设施的防御能力的政策，去维护一个鼓励高效，创新和经济繁荣同时保证安全，商业机密和人生自由的网络环境。“

愿景

推进自由软件基础架构安全的工程化。

加固一小步，自由软件一大步。

#HardenedLinux 社区成员组成

* 自由软件狂热分子
* 反权威主义
* 信息安全研究人员

#h4rdenedzer0 团队主要成员组成

* h4rdenedzer0 团队
  - @citypw
  - @n3o4po11o
  - @digitalplus

其他作出贡献志愿者成员

* 北京炼石网络 Ciphergateway 公司团队
* Tom Li
* Lenx Wei
* happy-dw

给予社区捐赠者

$ Donation:

* citypw, 8,000 RMB, 480 EU

* tomcat, logo design

$ Hardware donation:

* Ciphergateway, Rasperry Pi II

已完成的项目 -1

PaX for Android ， PaX 是 PaX/Grsecurity 的集合的一部分，所有的 feature 都是针对 memory corruption 利用的防御，我们完成了针对 msm 3.4-based kernel tree(Nov 2014) 的 PaX 移植并最终在 Nexus 7 2013 上测试通过。

已完成的项目 -2

STIG-4-Debian ，STIG（安全技术实现指南）是由 DISA 为了 IT 安全态势给 DoD(美国国防部）提供的一套防御指南， GNU/Linux 的发行版只有针对 RHEL 的，由 Red Hat 实现的，我们移植了 STIG for RHEL 并且做了相关改动，比如针对 SELinux 的检测由 AppArmor 替换，最终在 Debian 8 上测试通过， h4rdenedzer0 所发布的所有测试默认都是基于 Debian 。

已完成的项目 -3

Reproducible build for PaX/Grsecurity ， Reproducible packaging 是由 EFF 和 Debian 社区开发的用于对抗大规模监控的一种打包机制，它能重现 binary 在编译时的场景，我们打算针对 PaX/Grsecurity 做一个自动化脚本供运维人员使用。

社区贡献 - 捐赠 1

过去的 5 个月我们主要有 3 次捐赠支出：

* 为年轻人在学习，研究和参与 h4rdenedzer0 的项目提供 5,000RMB 资金支持，未来我们可能会有更多给年轻人 funding 的计划；

社区贡献 - 捐赠 2

* 为 BLUG(Beijing GNU/Linux User Group) 捐赠 3,000RMB 制作新的 T-shirt ， BLUG 是我们的老朋友，至少我个人认为 BLUG 是中国自由软件社区的最后堡垒，因为其他的都是“开源”社区。

社区贡献 - 捐赠 3

* 为 FSFE（欧洲自由软件基金会）捐赠 480 EU ，主要因为 FSFE 在对于 compulsory router 问题上推动“路由器自由”法案的一直坚持。

社区捐赠 -why?

改变自由软件的现状不是由几个人能够去改变的，需要更多的人或社区来一起推进和完成，而我们捐赠的自由软件社区和组织是和我们有着一样的愿景的，同时我们也是他们所做出的项目的受益者和使用者，所以我们选择给予捐赠给他们。

社区贡献 - 翻译文档

* Brad Spengler(Pax Team/grsecurity) 访谈
* PaX 的技术考古之旅
* PAGEEXEC 的最早设计文档
* SEGMEXEC 设计文档
* 漏洞利用 "BadIRET" 分析 (CVE-2014-9322, Linux 内核提权)
* 后续故事：数字军火级别的 "BadIRET" 漏洞利用 (CVE-2014-9322)
* SSL/TLS 部署最佳实践 v1.4
* Timeline of compulsory routers

社区贡献 - 项目及实施文档

* PaX/Grsecurity for Nexus 7 2013
* Debian GNU/Linux security checklist and hardening
* STIG-4-Debian

社区志愿者实践文档贡献

志愿者：炼石网络 CipherGateway 团队

* Gentoo GNU/Linux 系统安装与加固

* 社区最佳实践：基于 PaX/Grsecurity & STIG & Sheild 针对 es 的 Docker 场景化加固

* PaX/Grsecurity 配置选项

未来关注的方向

主要会关注 3 个基础架构的系统安全：

* Kernel
* Compiler
* Firmware

同时也关注开放环境中的防御的另一块基石：

* 密码工程


基于自由软件的场景化加固
GNU Linux安全体系
生态
自由软件社区生态
&&
立法的生态
密码工程
Firmware
Kernel
Compiler

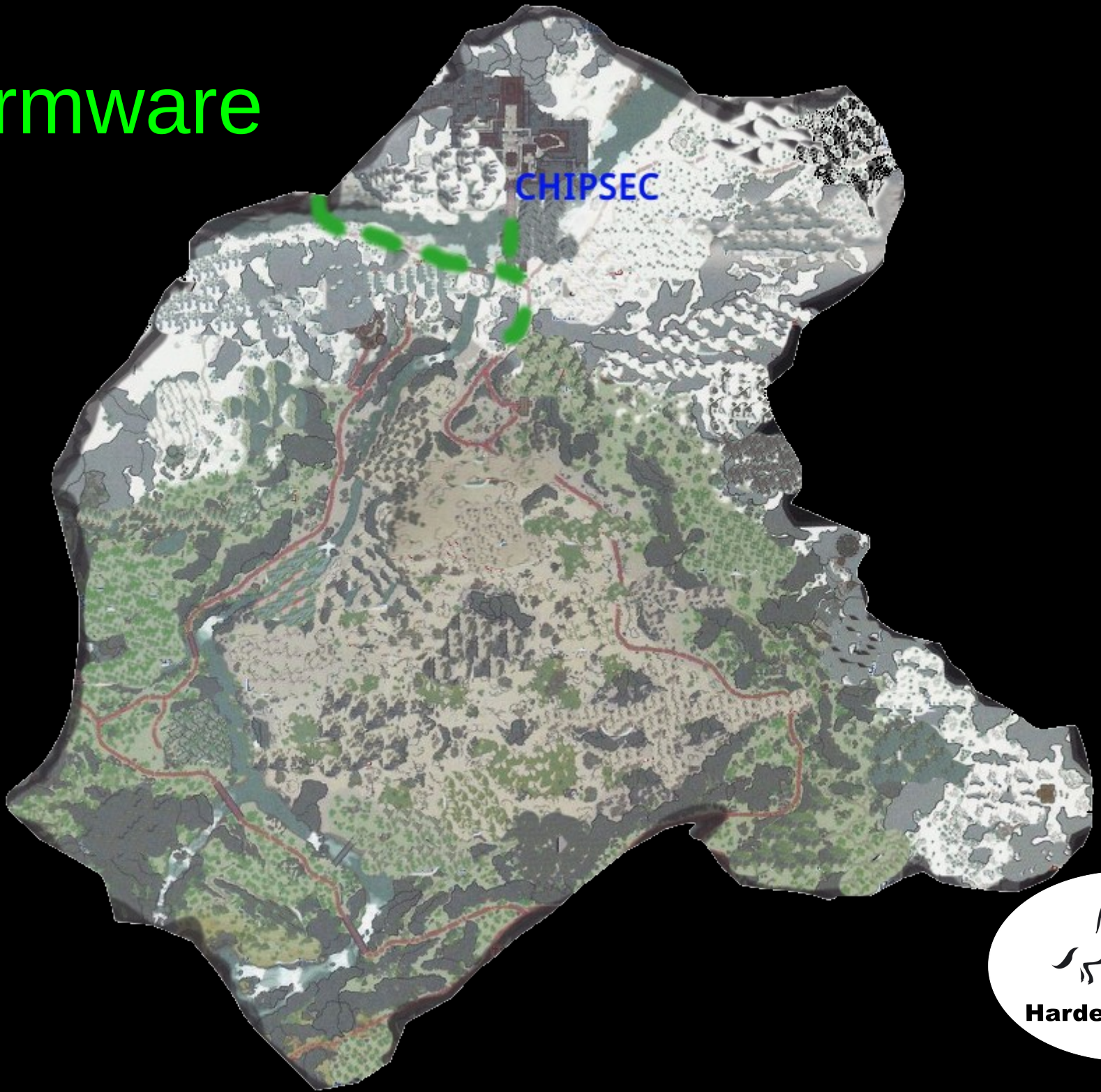
#Kernel

HardenedLinux

#Compiler

HardenedLinux

#Firmware

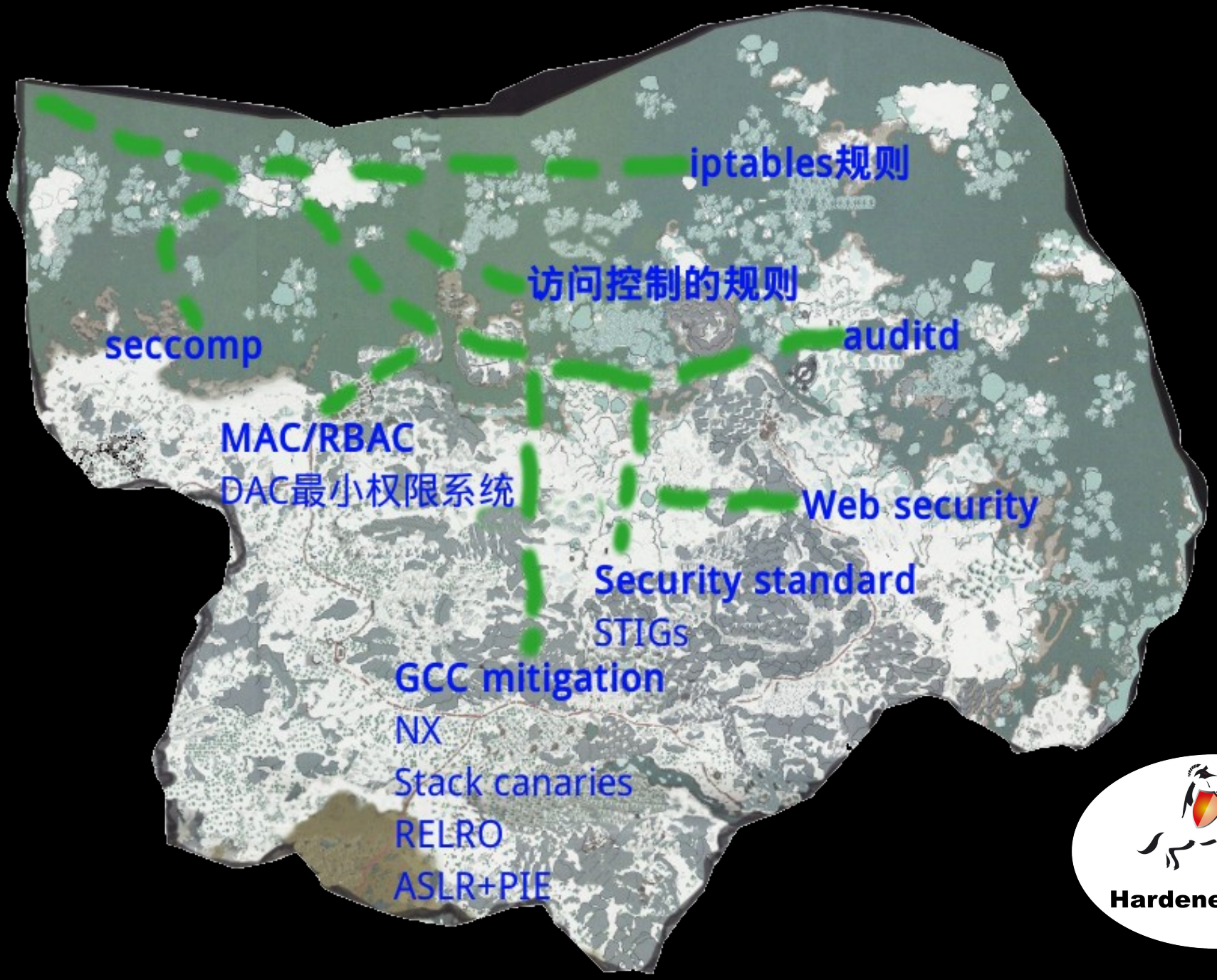


HardenedLinux

密码工程

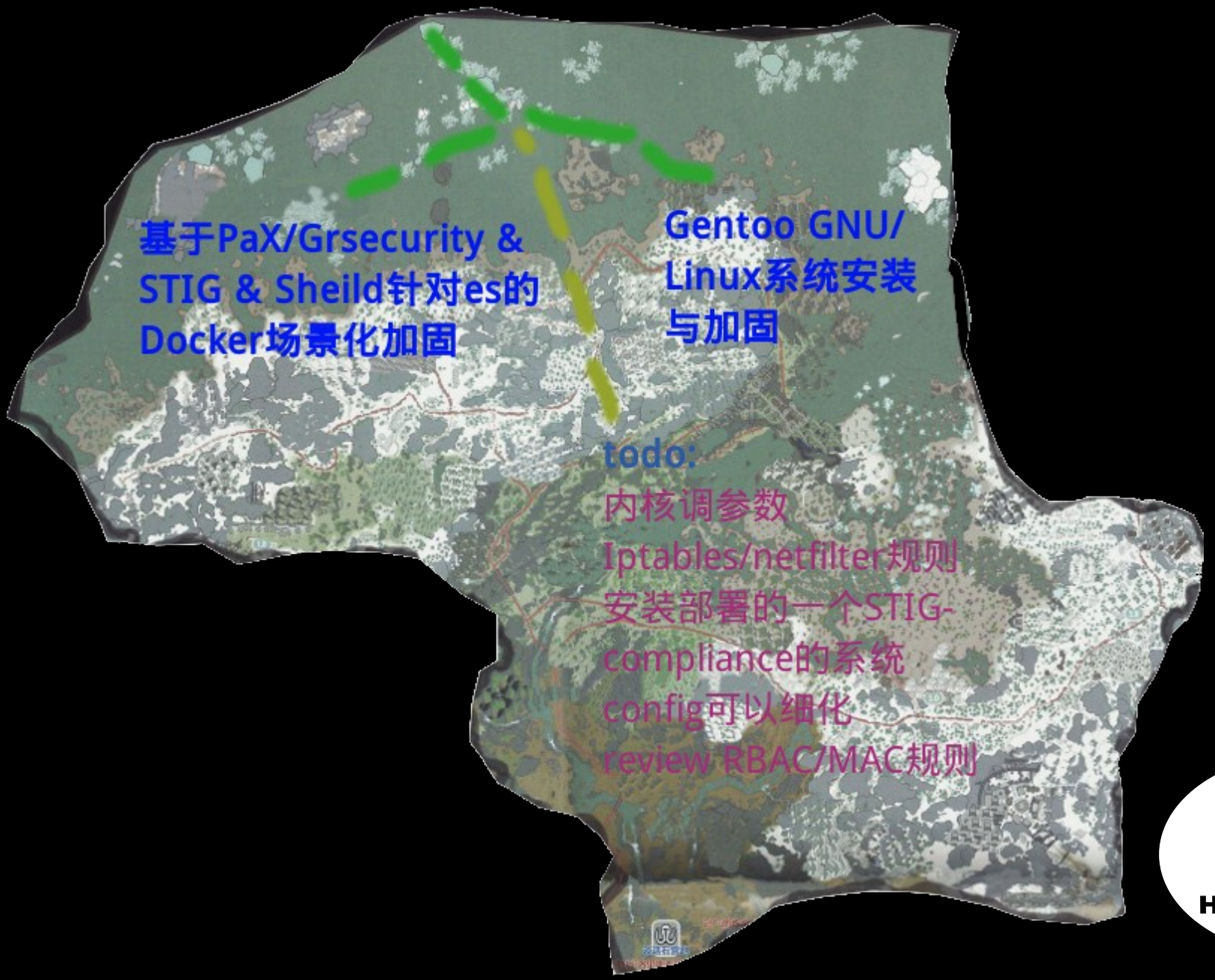
HardenedLinux

#GNU Linx 安全体系



HardenedLinux

基于自由软件的场景化加固



HardenedLinux

生态

HardenedLinux

关注我们的社区

* Hardenedlinux 社区

  # 官方网站： http://hardenedlinux.org

  # twitter: https://twitter.com/hardenedlinux

  # 新浪微博： @hardenedlinux

* 使用自由软件的方案加固一切
* 狂热的自由软件玩家以及 Anarchy

  (Anarchy 翻译成“反权威主义”更准确)
* 关注企业安全

网络产品加固

场景	加固方案
硬件 : x86_64	3.14.x with UDEREF
Debian 8 GNU/Linux 物理机安全	常规安全部署 + STIG-complianced
所有应用运行在 container/Docker 中，防御逃逸	容器的逃逸成本远远低于虚拟机，所以使用 PaX/Grsecurity + RBAC
ElasticSearch 防护	Sheild 插件

正在进行中的版本：

http://hardenedlinux.org/system-security/2015/09/06/hardening-es-in-docker-with-grsec.html

谢 谢 大 家 !

http://hardenedlinux.org/