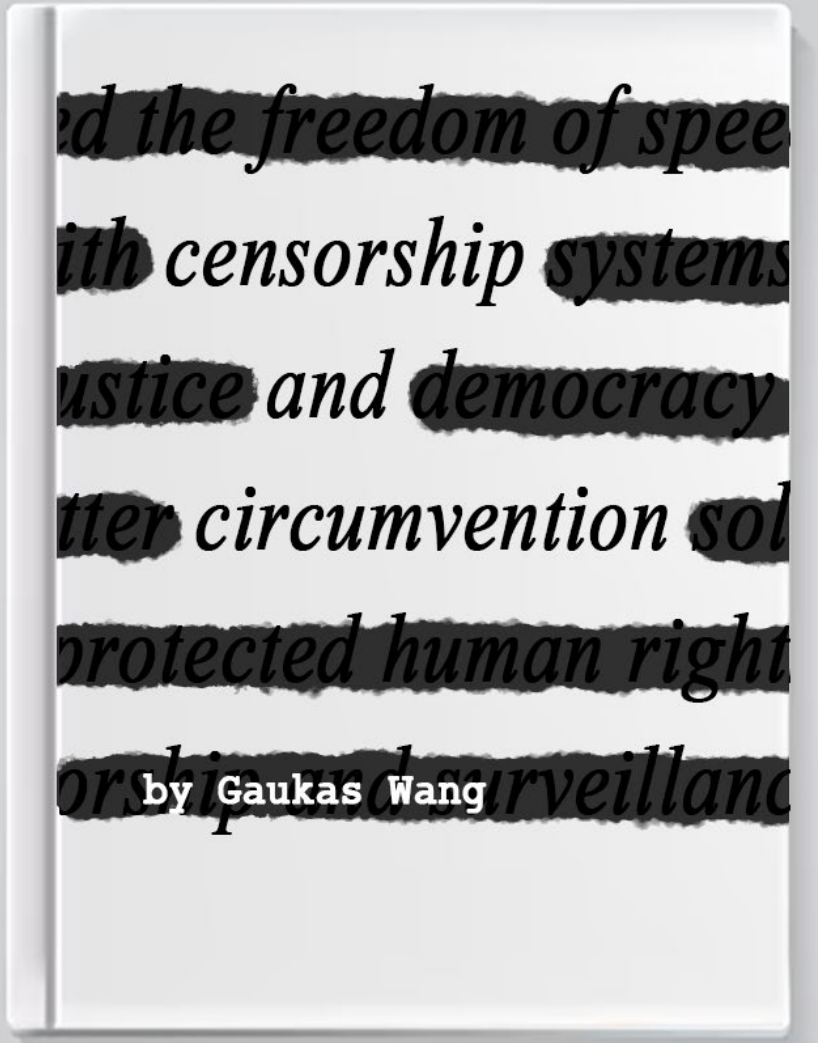


Adversarial Cybersecurity: Censorship Circumvention

对抗性网络安全：审查规避

University of Colorado Boulder

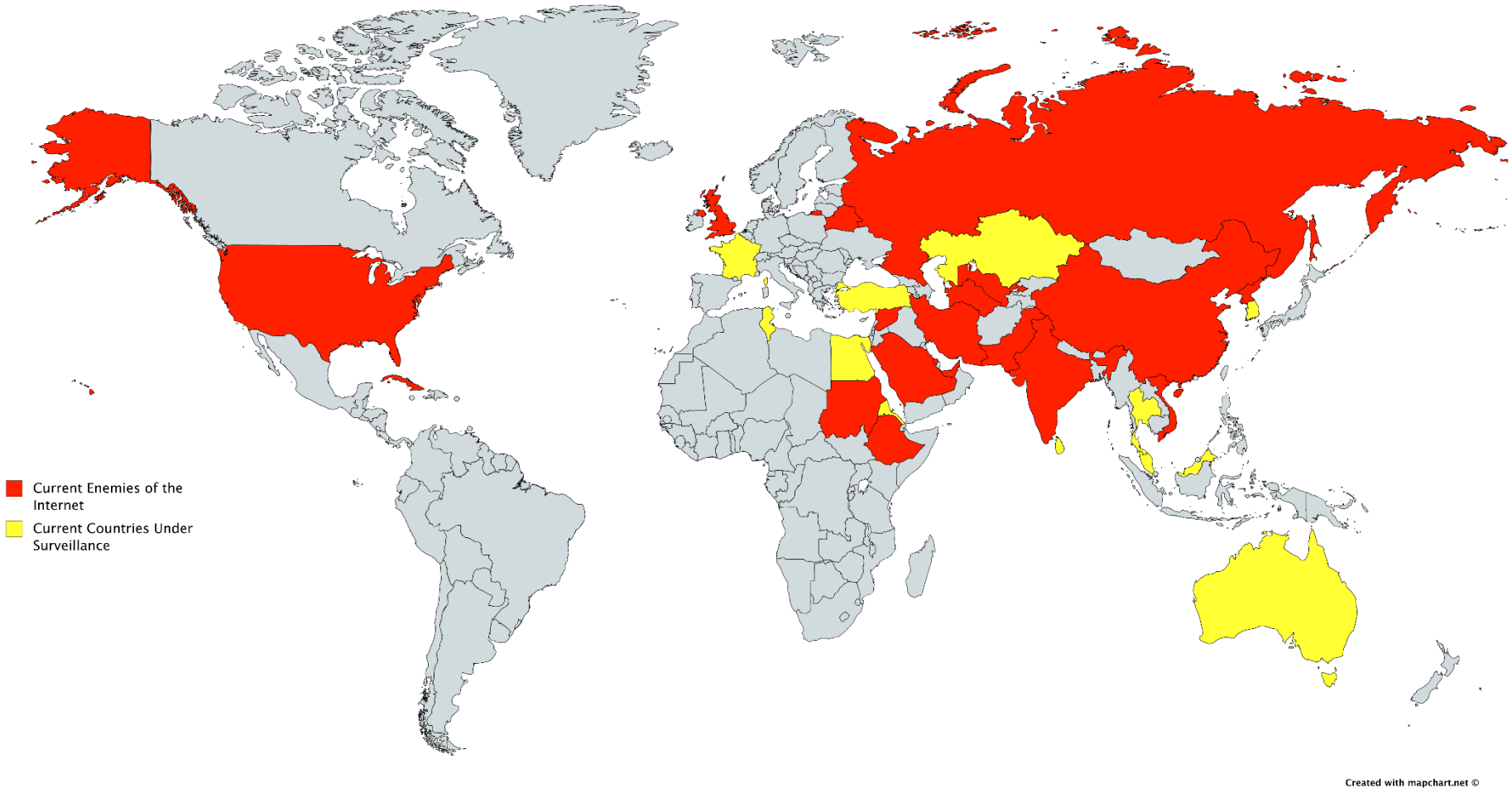
“跨过长城，走向世界”

“Across the Great Wall we can reach every corner of the world”

- 1987年9月14日，中国第一封跨国电子邮件由北京发往德国卡尔斯鲁厄理工学院（Karlsruhe Institute of Technology）
- 37年后的今天，2024年5月27日

“跨过长城，走向世界”

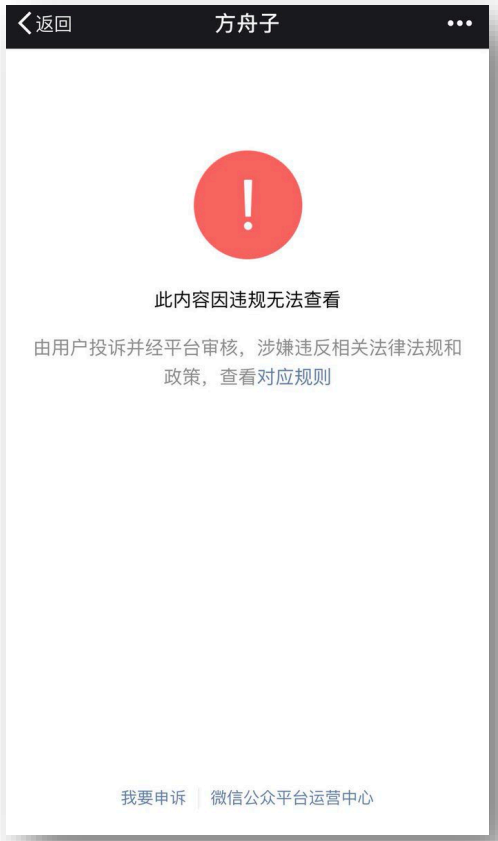
“Across the Great Wall we can reach every corner of the world”



University of Colorado **Boulder**

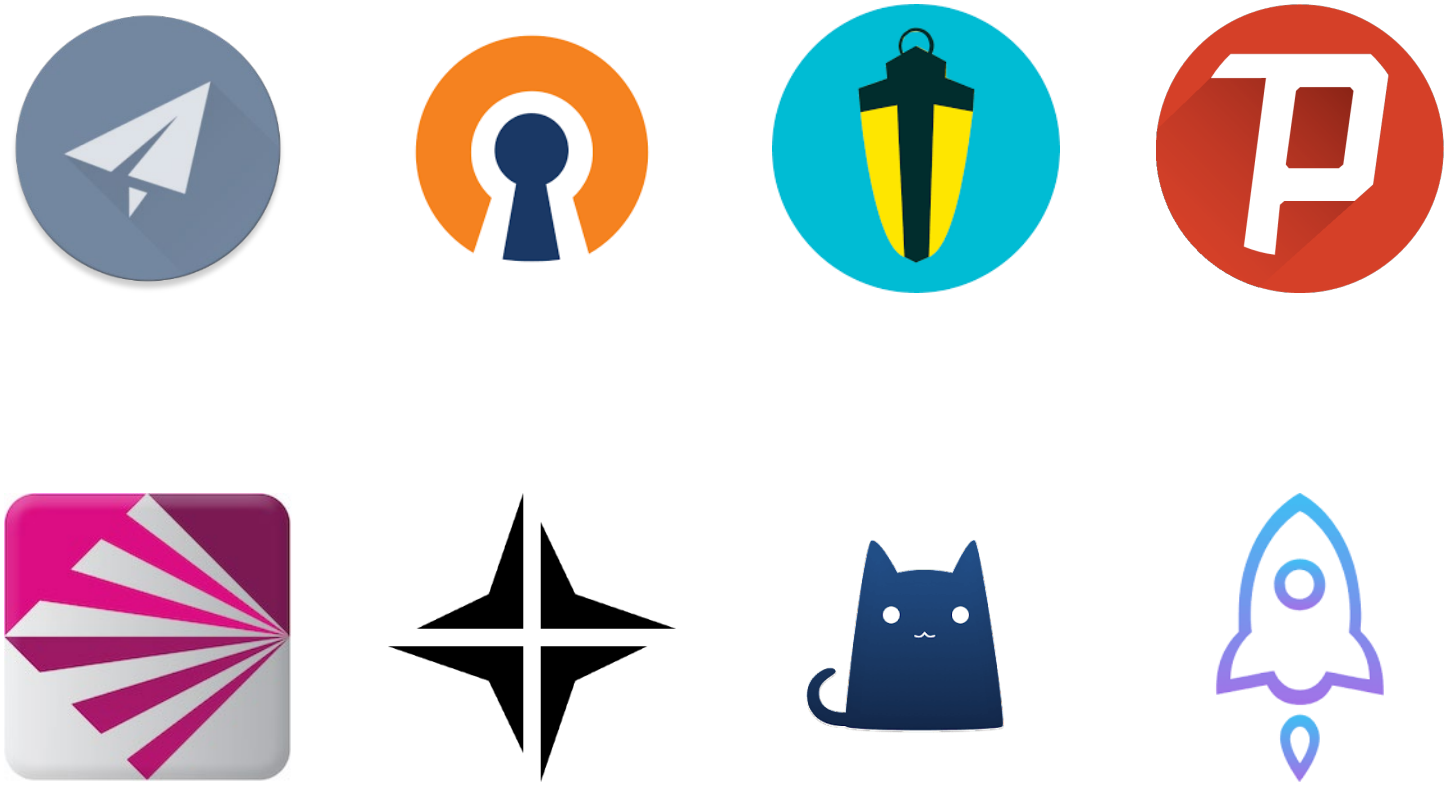
“跨过长城，走向世界”

“Across the Great Wall we can reach every corner of the world”



“跨过长城，走向世界”

“Across the Great Wall we can reach every corner of the world”



“跨过长城，走向世界”

“Across the Great Wall we can reach every corner of the world”

一言　　王

我，Gaukas Wang

- 科罗拉多大学博尔德校区　University of Colorado Boulder
  - 计算机工程　Computer Engineering
    - 博士研究生　Ph.D. Student

- 专精领域
  - 计算机网络　Computer Networking
    - 网络安全　Network Security
      - 反审查　Anti-Censorship

- 爱好
  - 电子游戏
  - 烹饪
  - 收藏烈酒 ~~酗酒~~

学术发表

- Acuerdo: Fast Atomic Broadcast over RDMA (ICPP 2022)
- **Chasing Shadows: A security analysis of the ShadowTLS proxy (FOCI 2023)**
- MRTOM: Mostly Reliable Totally Ordered Multicast (ICDCS 2023)
- **Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)**
- Extended Abstract: Oscur0: One-shot Circumvention without Registration (FOCI 2024)

科研团队

- Refraction Networking 折射网络
- 导师

Prof. Eric Wustrow

Prof. J. Alex Halderman
University of Michigan

对抗性网络安全

对抗性网络安全

- 网络安全

- 对抗性

对抗性网络安全

- 网络安全

- 对抗性
  - 实时
  - 互动
  - 解决“人造问题”

网络审查

- **网络服务审查**
  - 网站屏蔽
  - 网站关停
  - 网络干扰
- 内容审查
  - 即时通讯消息过滤
  - 内容平台关键词列表
- ...

审查的最终目的

- 社会/道德/宗教信仰因素
  - 色情内容，异教，敌对宣传
- 管控言论与舆情
  - Twitter, Facebook, WhatsApp, Telegram
- 过滤公共信息来源
  - Wikipedia, Google
- 建立商业壁垒
  - TikTok

审查者如何审查网络

- 前提：审查者通常对受审查的网络拥有**绝对控制/管辖/所有权**
  - **国家级审查者**
  - 区域级审查者
  - 组织级审查者（企业，学校）

- 做法：干扰/过滤/阻断具有部分特定目的的网络流量

审查者如何审查网络

- IP 地址与报文（Packet，又译封包）
  - IP 地址：邮政地址
  - 报文：邮件/信封/包裹

- IP 地址封锁
  - 审查者将IP地址加入黑名单
  - 拒绝向指定IP"投递"报文
  - 拒绝"投递"来自指定IP的报文

审查者如何审查网络

- 域名系统（DNS）
  - 记住大量 IP 地址很不现实
  - DNS 用于“解析”域名
  - 例： www.sd-jnyz.com “解析”到 IP 地址 123.6.40.224

- DNS 过滤
  - 审查者将部分域名（如 www.google.com）加入黑名单
  - 受控制的 DNS 服务器
    - 拒绝解析这些域名
    - **故意**解析到错误的 IP 地址
  - 不受控制的 DNS 服务器尝试正确解析
    - **注入**伪造的错误解析结果

审查者如何审查网络

- 深度报文检测 DPI (Deep Packet Inspection)
  - 默认情况下报文均为**明文** (IPSec等技术除外)
    - 相当于不封口的信封

- 报文过滤
  - 使用 DPI 技术检测所有的报文
  - 找出"可疑"报文
    - 内容/关键词对比
  - 篡改/丢弃"可疑"报文

审查者如何审查网络

- 传输控制协议 Transmission Control Protocol (TCP)
  - 所有报文都属于一个“连接”
  - 连接需要被**建立**，并在使用后手动**关闭**
  - 已经关闭的连接无法重新打开

- 连接重置
  - 伪造连接双方的身份
  - 向连接对方发送“关闭连接”的命令
  - 结局：连接被关闭，无法继续使用

审查的副作用

- 审查所需的基础设施可以被用于发动网络攻击
  - Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

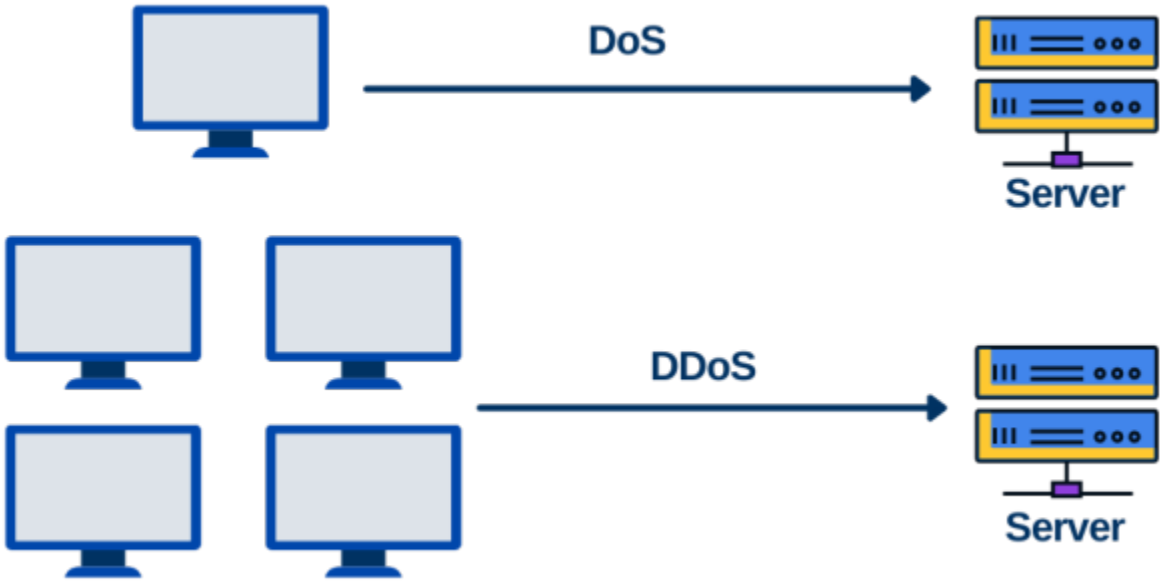
- 审查机制可能意外泄露（被审查）用户的隐私以及其他保密数据
  - Bleeding Wall: A Hematologic Examination on the Great Firewall (FOCI'2024)

- 审查机制的存在直接导致民意反弹
  - 史翠珊效应 (*Streisand effect*)
  - 激励更多反审查项目（包括**审查规避工具**）被创造

副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

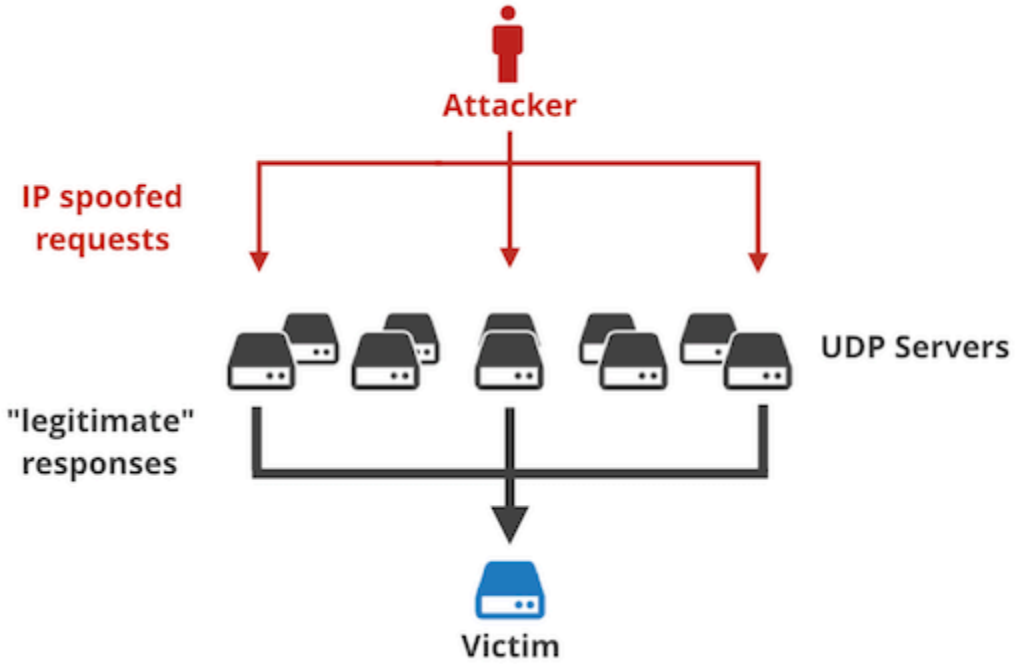
- Denial-of-Service Attack 服务拒绝攻击
  - **Distributed** Denial-of-Service **分布式**服务拒绝攻击



副作用：基础设施被用于发起网络攻击

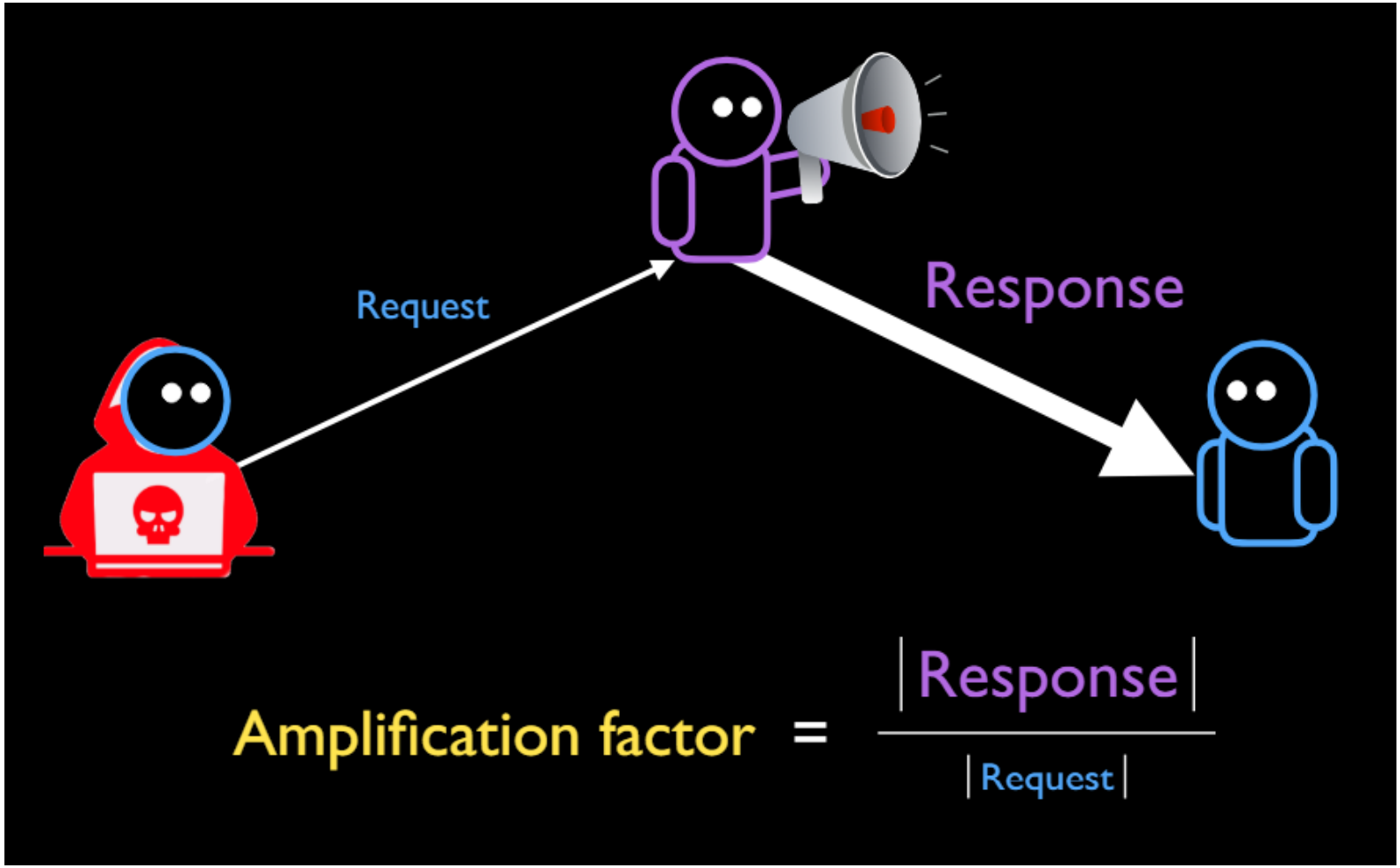
Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

- Reflected Amplification Attack 反射放大攻击
  - 绝大部分网络通讯协议中，每个**请求**对应一个**响应**
  - 通常情况下，**响应**比**请求**的尺寸（以字节计）大很多



副作用：基础设施被用于发起网络攻击

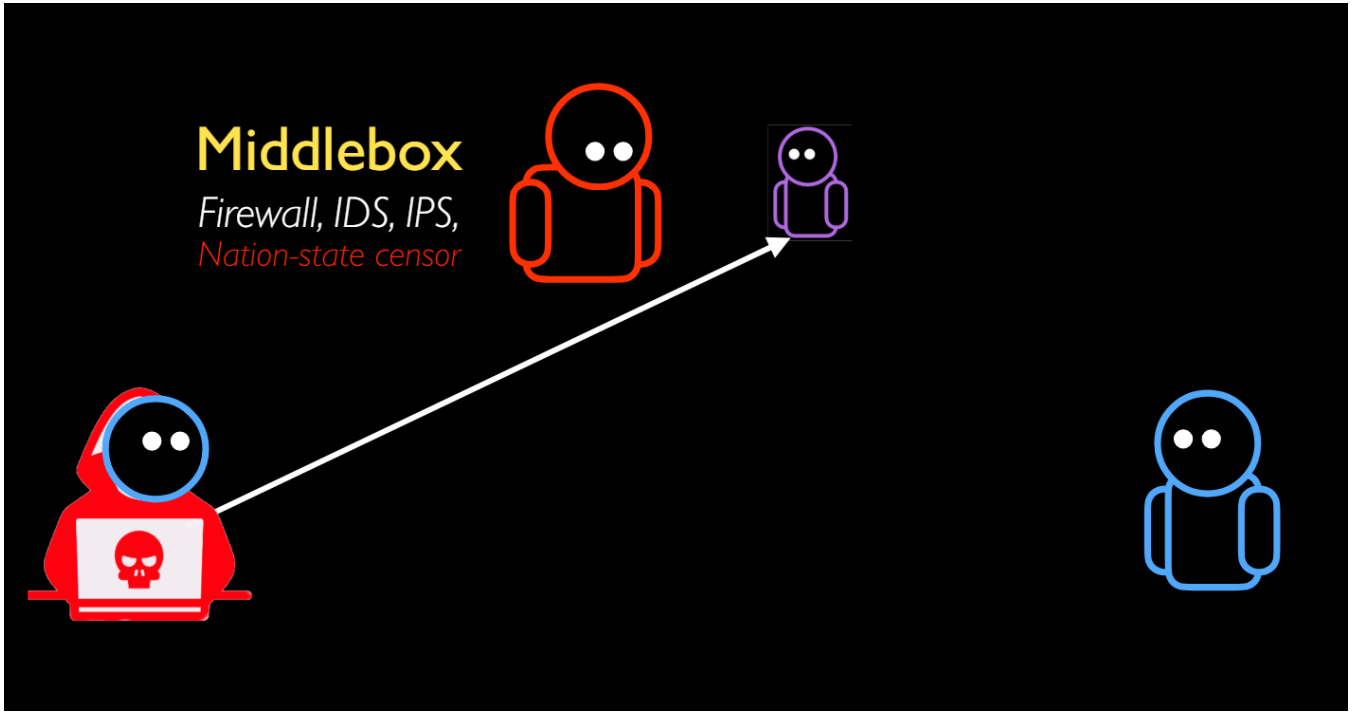
Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

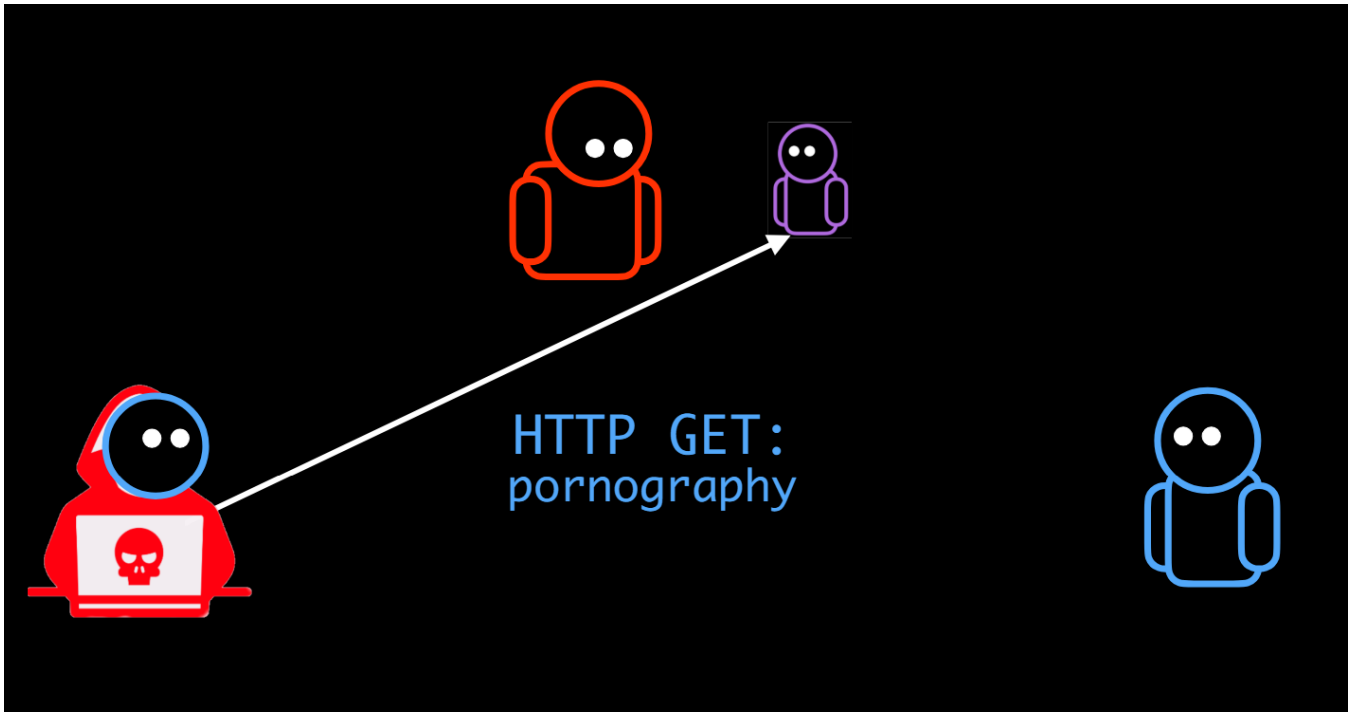
- 内容审查机制使用中间盒(Middlebox) 来**伪造**响应



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

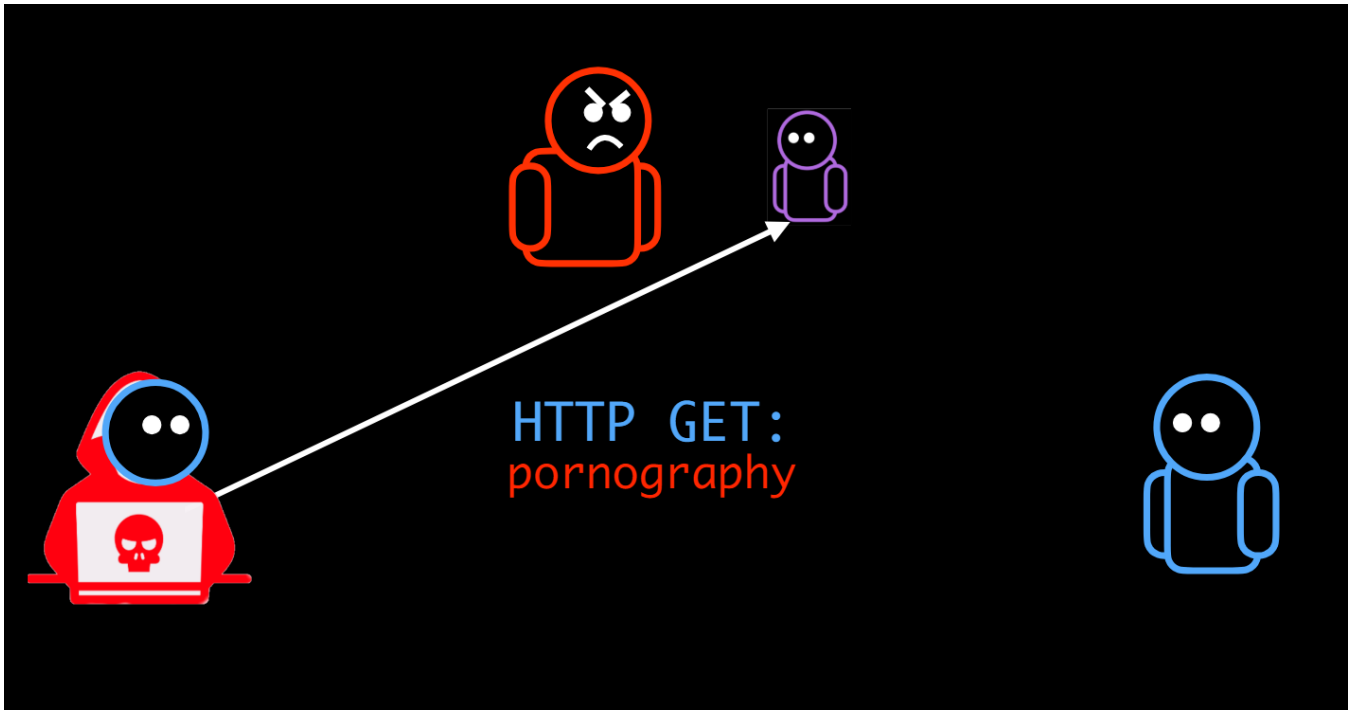
- 内容审查机制使用中间盒(Middlebox) 来**伪造**响应



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

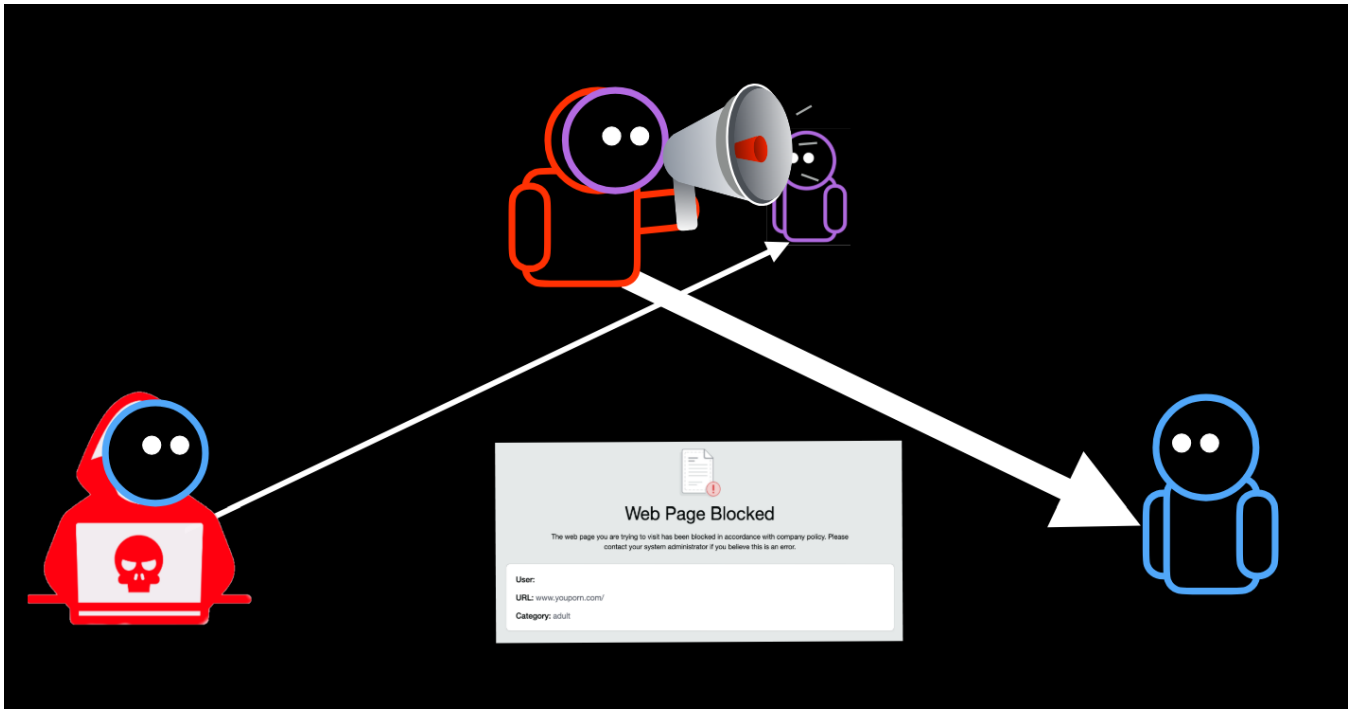
- 内容审查机制使用中间盒(Middlebox) 来**伪造**响应



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

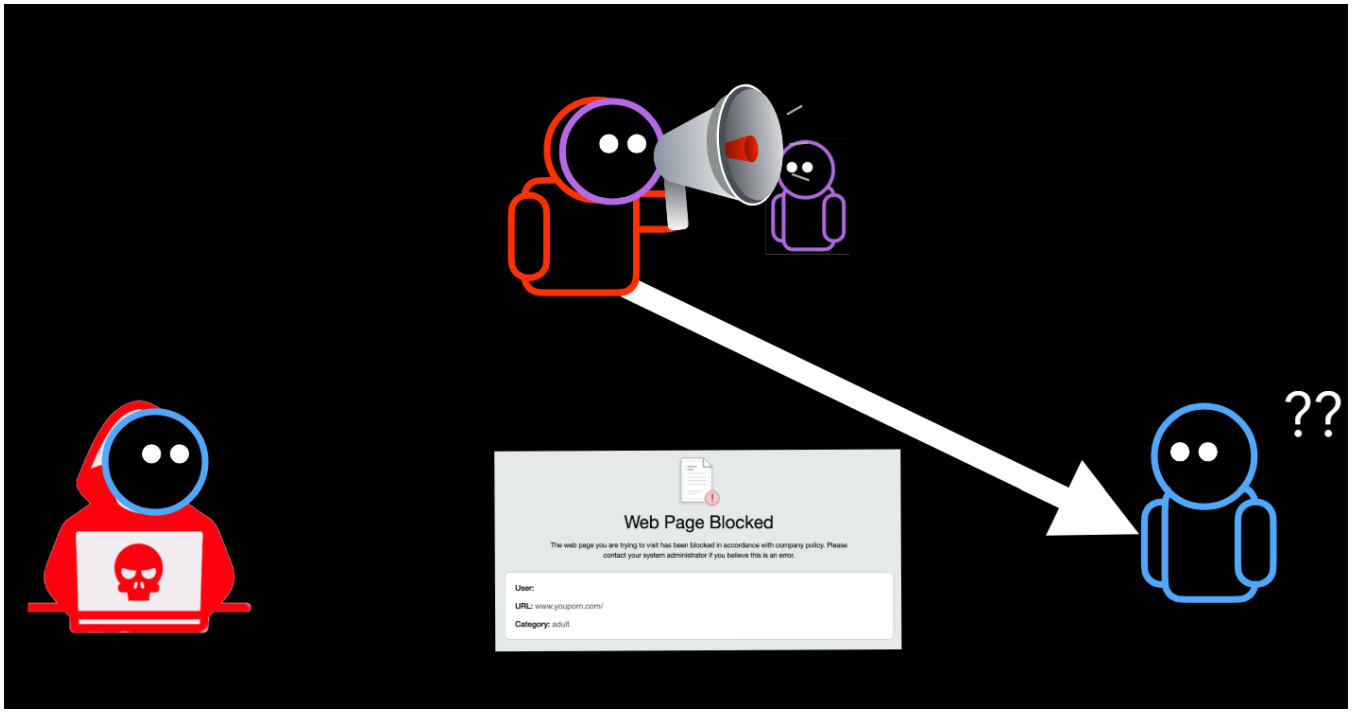
- 内容审查机制使用中间盒(Middlebox) 来**伪造**响应



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

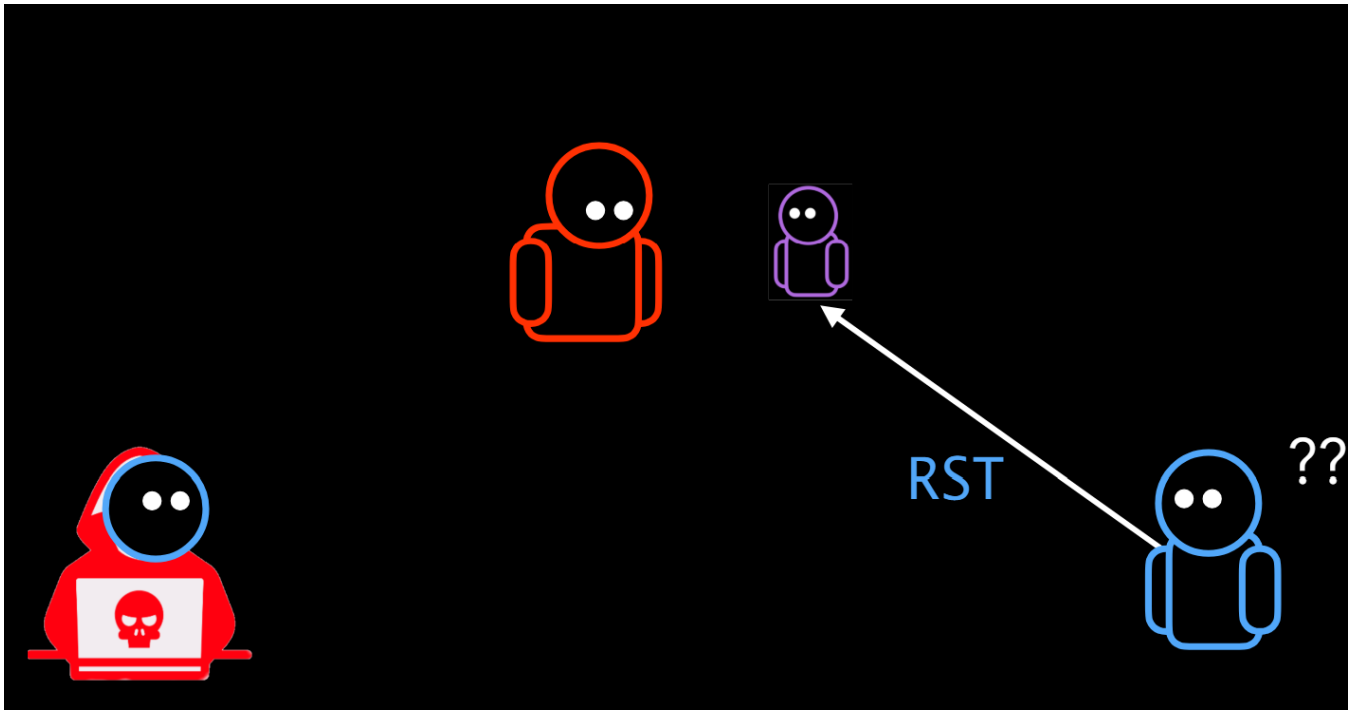
- TCP 协议下，受害者的**正确反应**创造并维持了一个循环



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

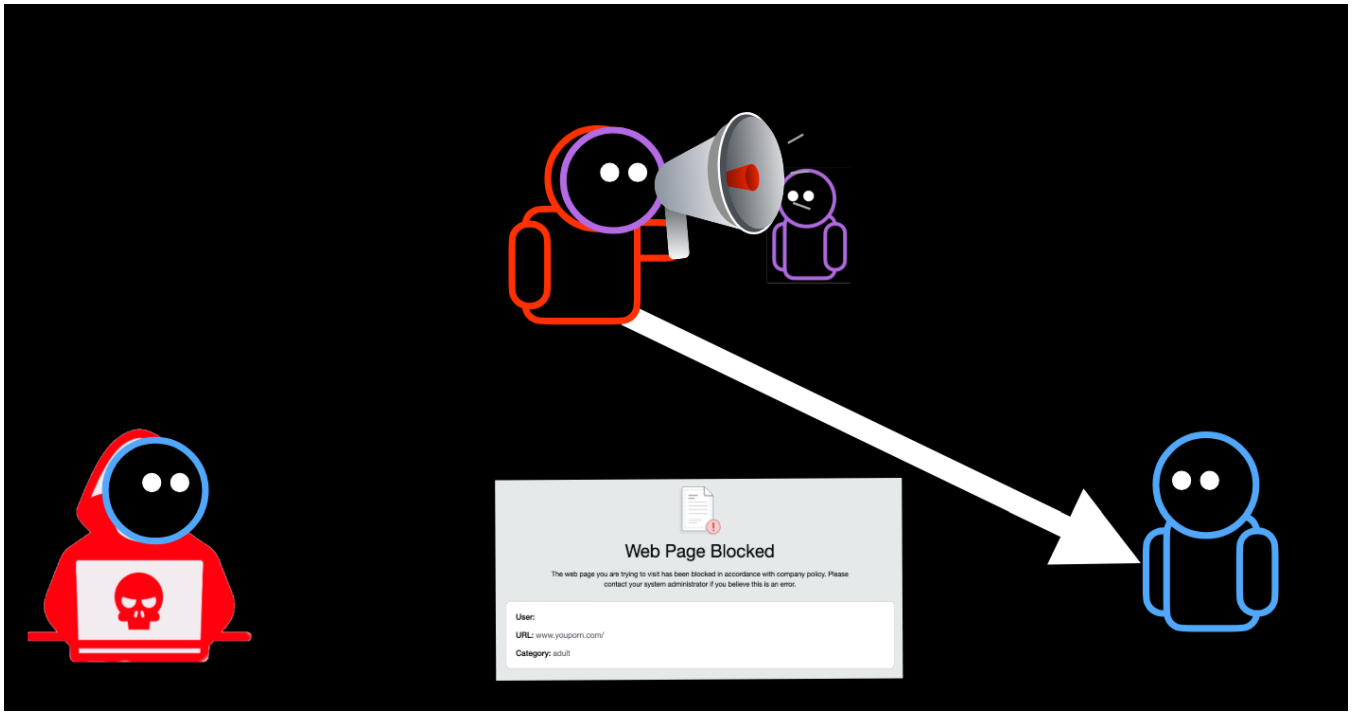
- TCP 协议下，受害者的**正确反应**创造并维持了一个循环



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

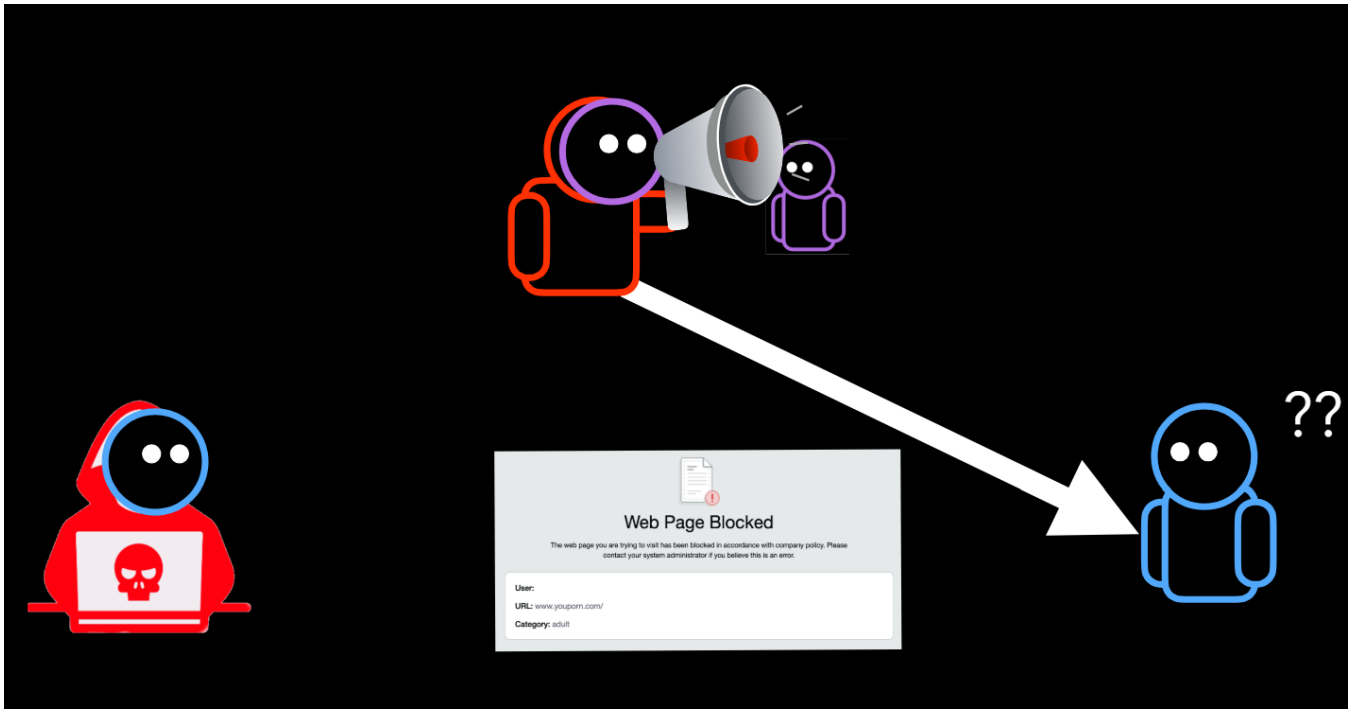
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

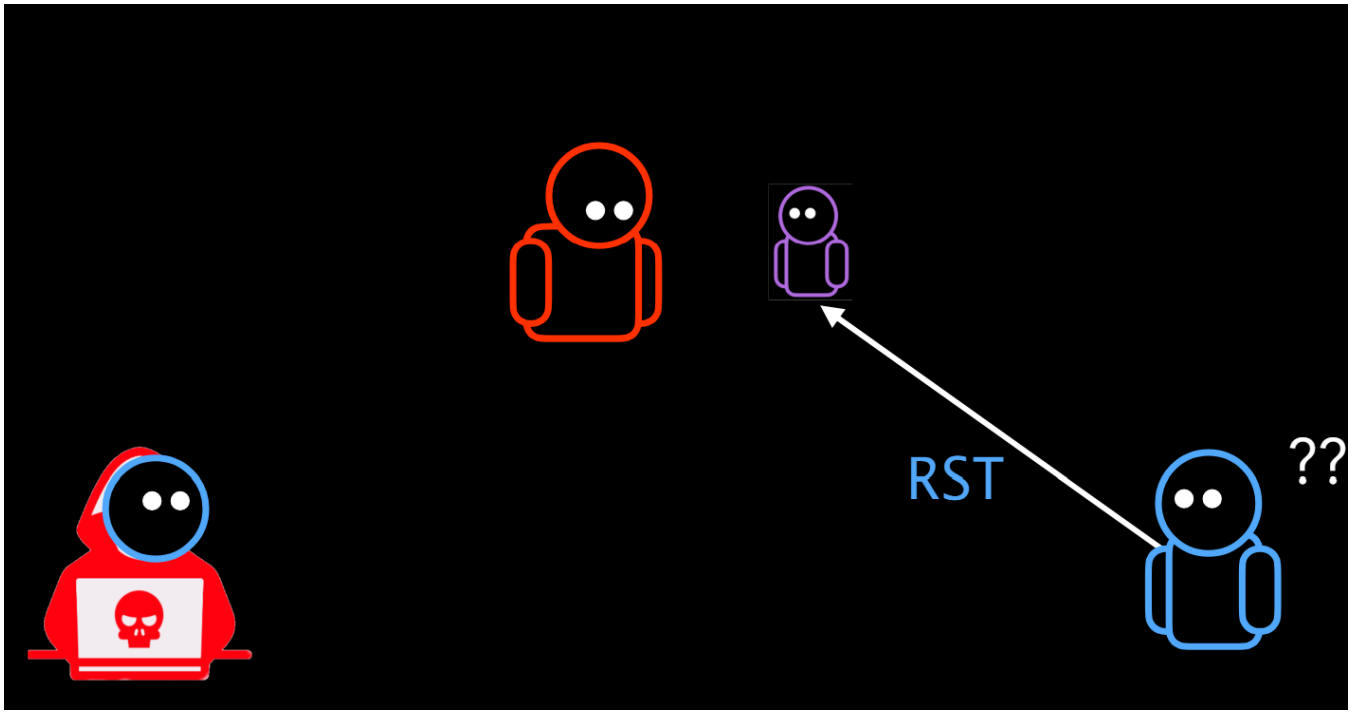
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

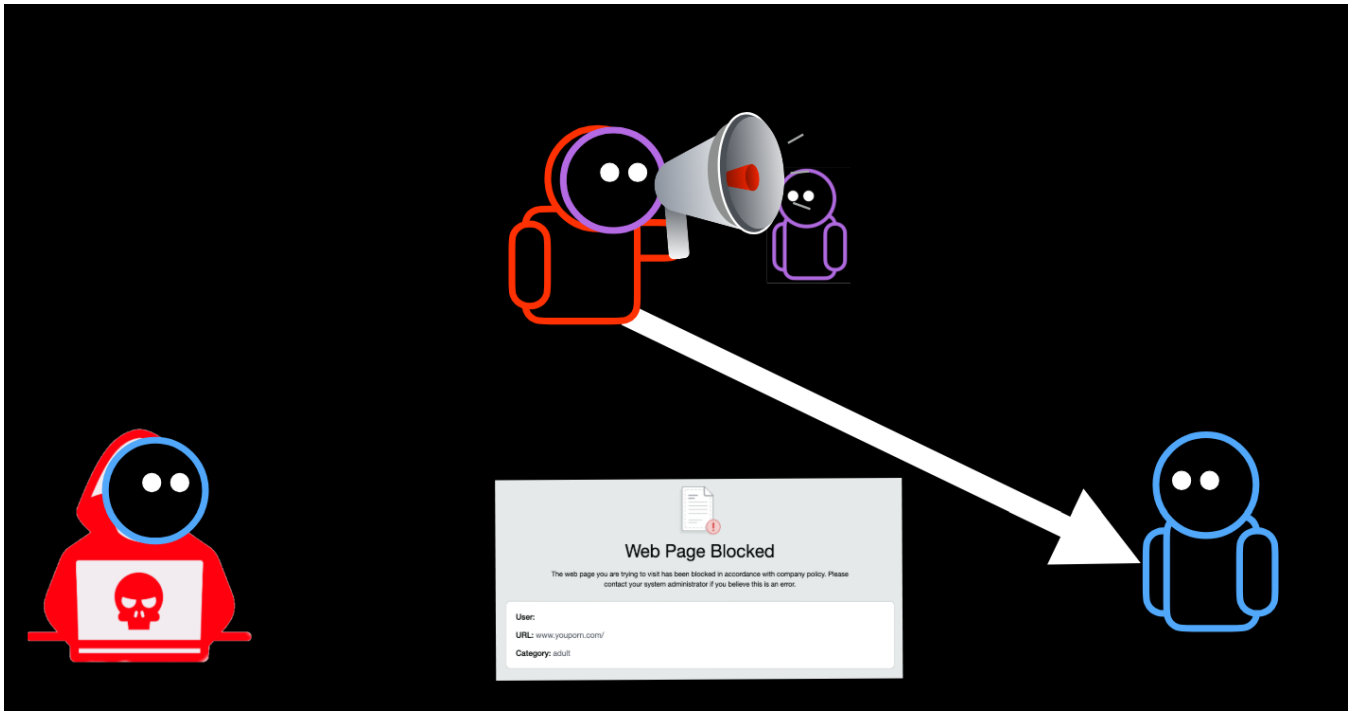
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

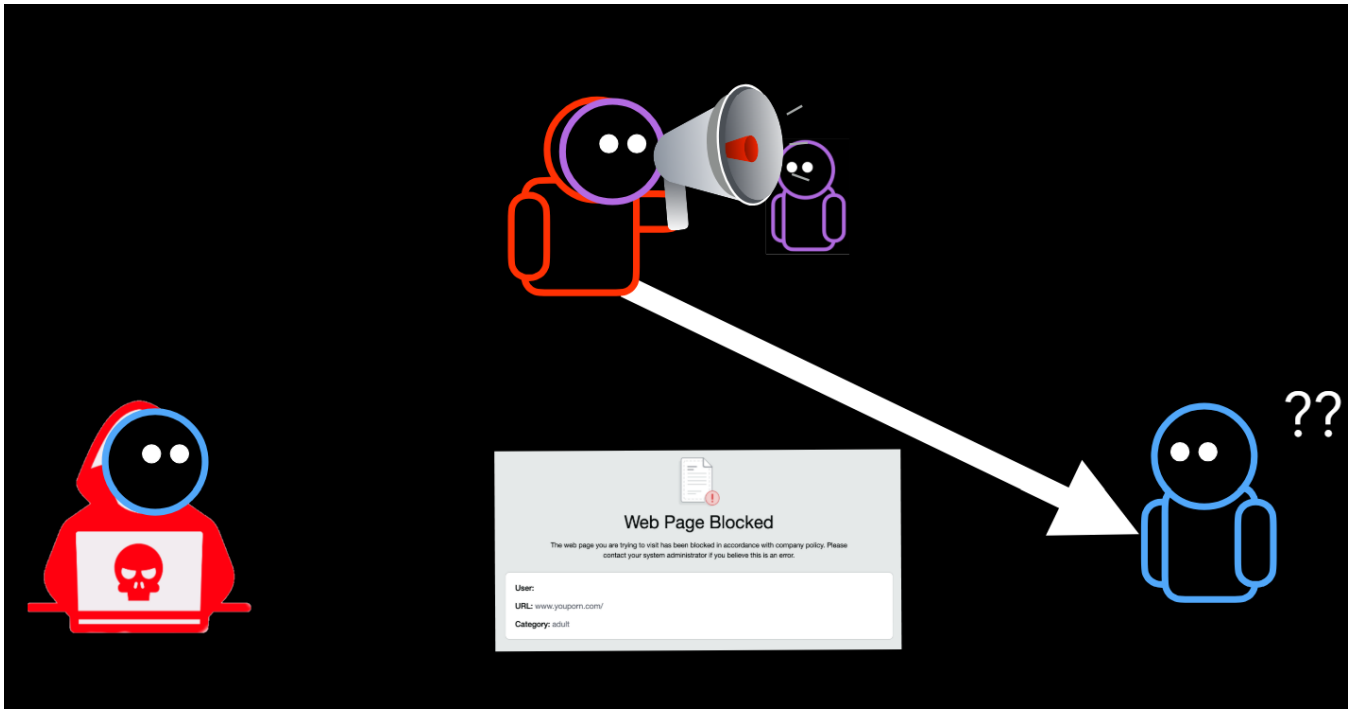
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

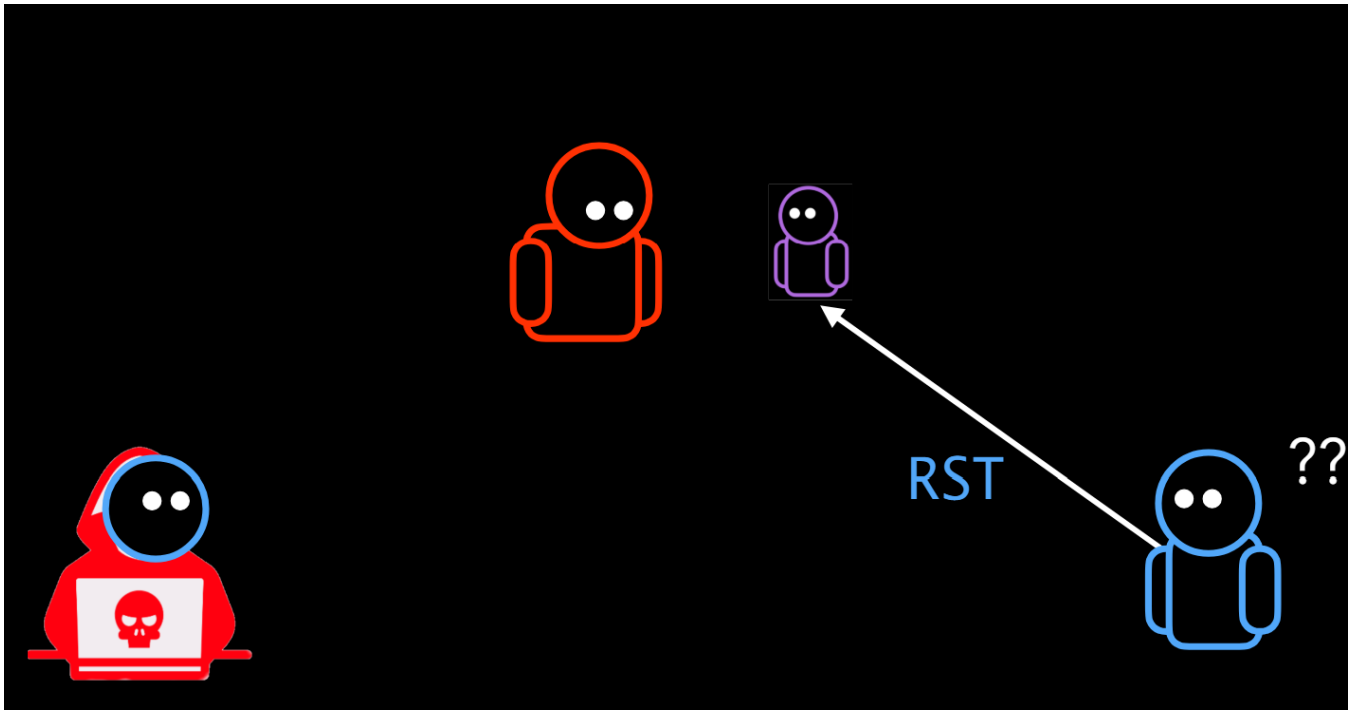
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

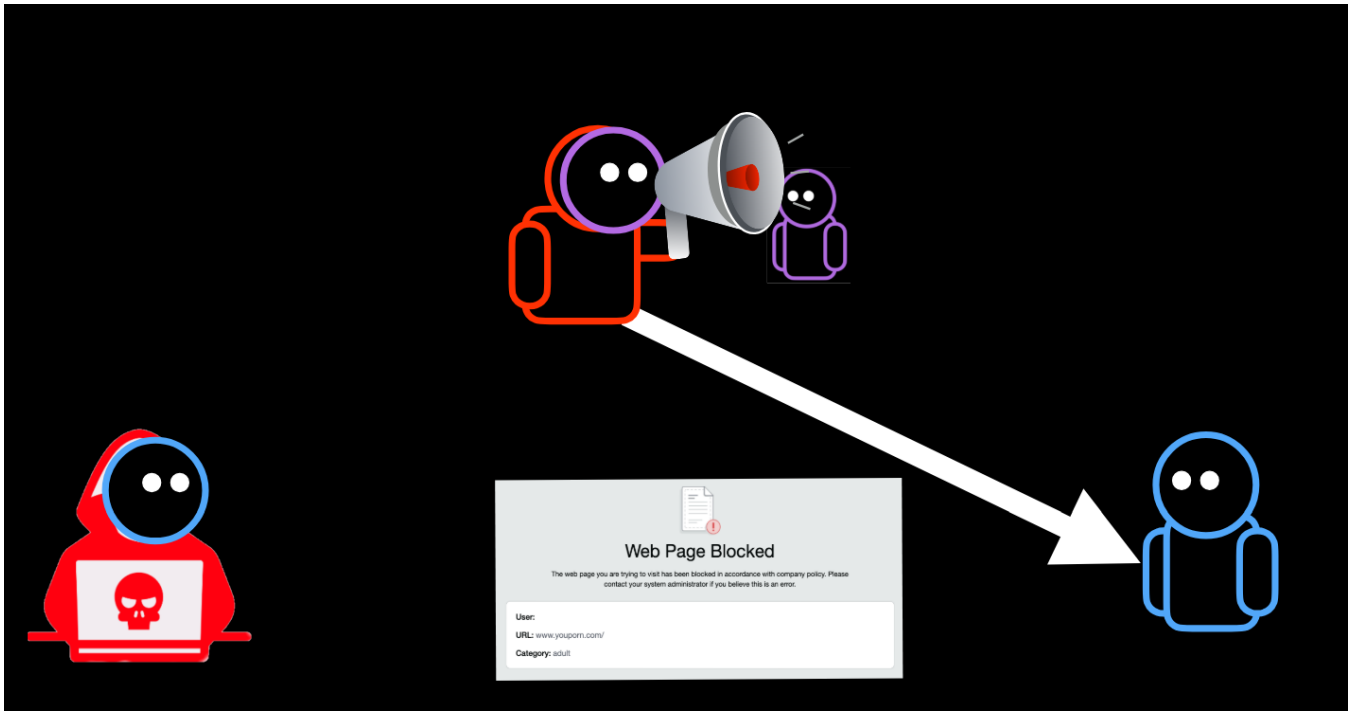
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

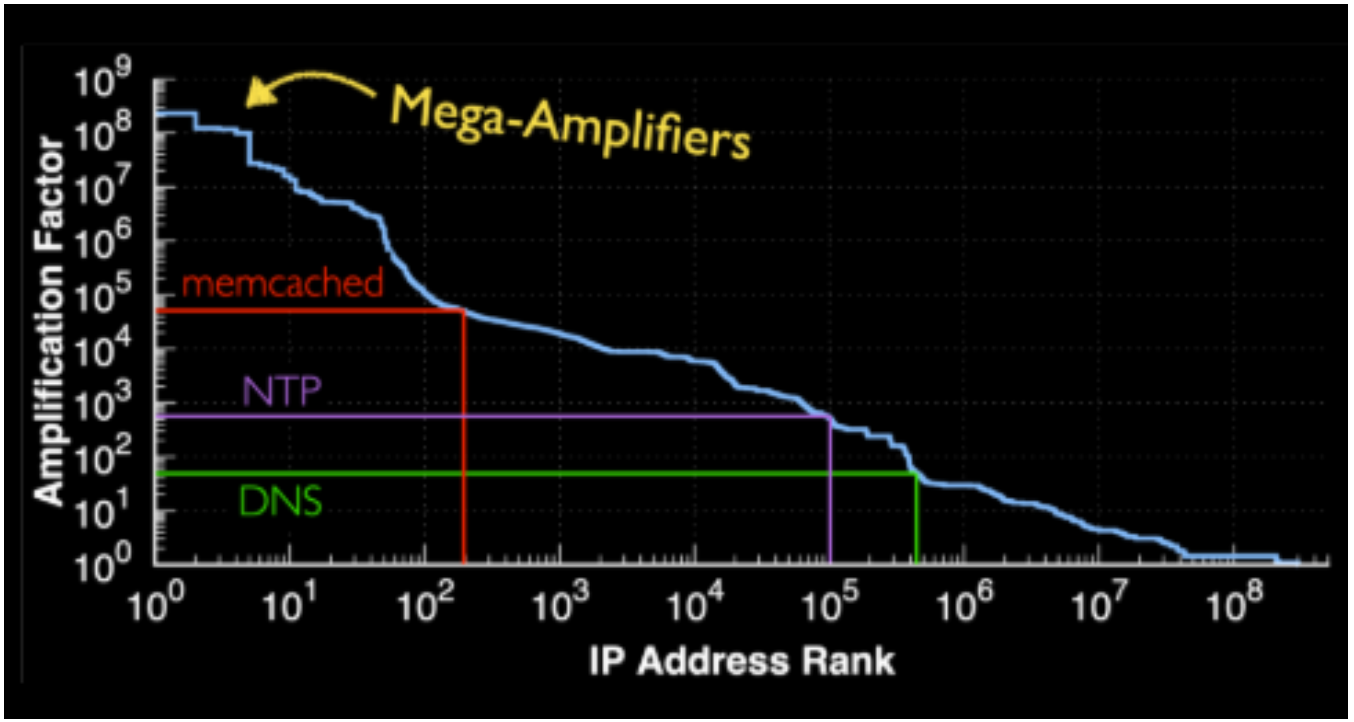
- TCP 协议下，受害者的**正确反应**创造并维持了一个**循环**



副作用：基础设施被用于发起网络攻击

Weaponizing Middleboxes for TCP Reflected Amplification (USENIX Security'21)

- 最高放大系数可达 10^8



副作用：泄露敏感流量以及其他数据

Bleeding Wall: A Hematologic Examination on the Great Firewall (FOCI'2024)

- DNS伪造攻击 DNS Spoofing Attack
  - DNS 域名系统将域名解析成 IP 地址
  - DNS 协议本身不使用任何加密
  - 审查者通过**抢答**错误的结果来干扰域名解析

- 防火长城 the Great Firewall of China
  - 最活跃的 DNS 伪造攻击来源（没有之一）
  - 极高并发
  - 设计简单 ~~简陋~~
  - 双向攻击
    - 中国 -> 国外
    - 国外 -> 中国

副作用：泄露敏感流量以及其他数据

Bleeding Wall: A Hematologic Examination on the Great Firewall (FOCI'2024)

- 防火长城**据信**重复使用相同机组进行多种攻击
- 用于多种审查攻击的程序同时运行于同一台（多台）机器上
- 多个程序的内存共存

副作用：泄露敏感流量以及其他数据

Bleeding Wall: A Hematologic Examination on the Great Firewall (FOCI'2024)

- 2010年，gfwrev 发现以下程式代码可以用于诱发 GFW 的**内存泄漏**

```
while true; do printf "\0\0\1\0\0\1\0\0\0\0\0\0\6wux.ru\300" | nc -uq1 $SOME_IP 53 | hd -s20; done
```

- 2020年，gfw.report 解释了此攻击背后的（假想）原理
- 2024年，Sakamoto（化名）等人改进此攻击，成功泄露**数百万条极度敏感信息**
  - 用户名以及密码
  - 姓名与身份证号
  - 银行卡号，过期日，安全码

副作用：泄露敏感流量以及其他数据

Bleeding Wall: A Hematologic Examination on the Great Firewall (FOCI'2024)

- 基本原理：**越界读取**
  - 读取不属于程序本身的内存
  - 软件设计中常见的内存安全问题之一
- 泄漏效率：**低**
  - 每次攻击仅能泄漏 124 字节
- 危害程度：**极高**
  - 论文声称作者在 3 日内泄漏了数百万条极度敏感信息
  - 原因：防火长城用于处理极大量流量

史翠珊效应：欲盖弥彰

- 美国艺人芭芭拉·史翠珊在2003年状告摄影师肯尼思·阿德尔曼（Kenneth Adelman）和其网站“Pictopia.com”，令其移除阿德尔曼所拍摄的12,000张加州海岸摄影中含有的对史翠珊住所的空中摄影，以保护史翠珊的隐私。结果史翠珊败诉，次月有多达**420,000**人前来浏览阿德尔曼的网站。

史翠珊效应：欲盖弥彰

- 美国艺人芭芭拉·史翠珊在2003年状告摄影师肯尼思·阿德尔曼（Kenneth Adelman）和其网站“Pictopia.com”，令其移除阿德尔曼所拍摄的12,000张加州海岸摄影中含有的对史翠珊住所的空中摄影，以保护史翠珊的隐私。结果史翠珊败诉，次月有多达**420,000**人前来浏览阿德尔曼的网站。

- 冬，邾黑肱以滥来奔，贱而书名，重地故也。君子曰：“名之不可不慎也如是。夫有所有名，而不如其已。以地叛，虽贱必书地，以名其人，终为不义，弗可灭已。是故君子动则思礼，行则思义，不为利回，不为义疚。或求名而不得，或欲盖而名章，惩不义也。”（左传·昭公三十一年）

史翠珊效应：欲盖弥彰

- 美国艺人芭芭拉·史翠珊在2003年状告摄影师肯尼思·阿德尔曼（Kenneth Adelman）和其网站“Pictopia.com”，令其移除阿德尔曼所拍摄的12,000张加州海岸摄影中含有的对史翠珊住所的空中摄影，以保护史翠珊的隐私。结果史翠珊败诉，次月有多达**420,000**人前来浏览阿德尔曼的网站。

- 冬，邾黑肱以滥来奔，贱而书名，重地故也。君子曰：“名之不可不慎也如是。夫有所有名，而不如其已。以地叛，虽贱必书地，以名其人，终为不义，弗可灭已。是故君子动则思礼，行则思义，不为利回，不为义疚。或求名而不得，或欲盖而名章，惩不义也。”（左传·昭公三十一年）

- 此地无银三百两

反审查

- 三个要素
- 测量
- 分析
- **规避 (Circumvention)**

反审查

- 三个要素
- 测量
  - 观测审查事件的发生
- 分析

- **规避 (Circumvention)**

反审查

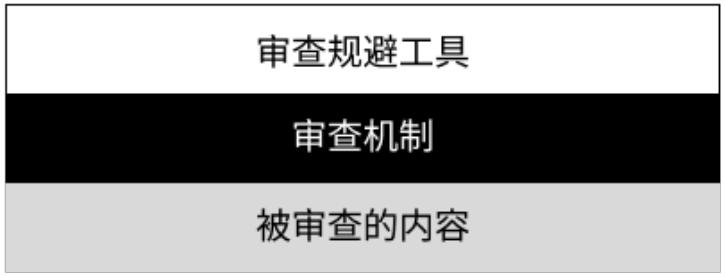
- 三个要素
- 测量
  - 观测审查事件的发生
- 分析
  - 稳定复现审查事件
  - 构建假想模型描述审查机制
- **规避 (Circumvention)**

反审查

- 三个要素
- 测量
  - 观测审查事件的发生
- 分析
  - 稳定复现审查事件
  - 构建假想模型描述审查机制
- **规避 (Circumvention)**
  - 使用技术手段绕过审查机制
  - “翻墙”

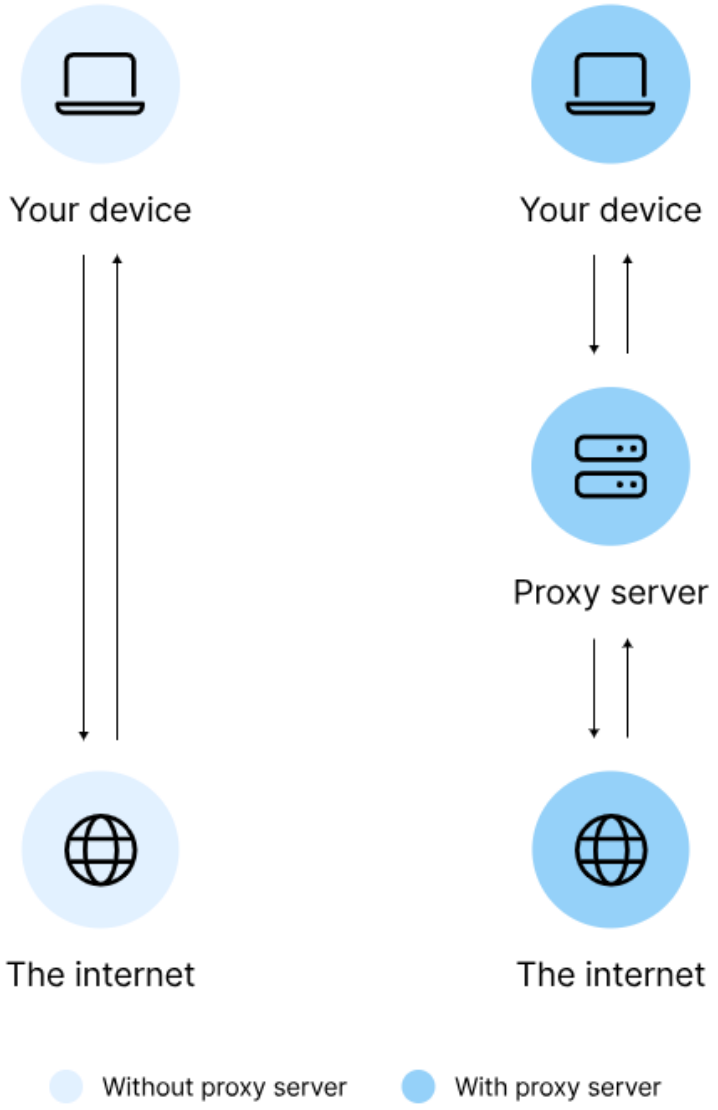
反审查

- 三个要素
- 测量
  - 观测审查事件的发生
- 分析
  - 稳定复现审查事件
  - 构建假想模型描述审查机制
- **规避 (Circumvention)**
  - 使用技术手段绕过审查机制
  - “翻墙”



规避审查的最常见手段

- 建立受保护的私有信道
  - VPN, 代理 (Proxy)
- 需要一台未被屏蔽/阻断的服务器
- 使用强加密
- 审查者无法获知代理服务器被用于访问受限内容

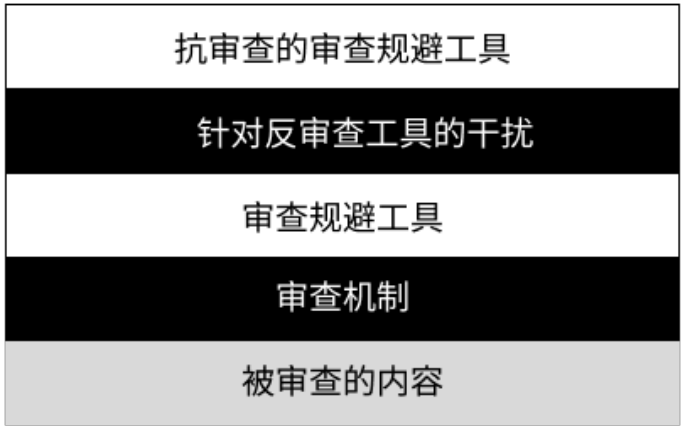


反“反审查”

- 被动的审查者（如学校/企业）
  - 以合规为目的
  - 审查设施陈旧
  - 审查机制滞后
  - 常见工具可以轻易绕过
- 积极的审查者（政府）
  - 积极发展新的审查机制
  - 并防止旧的审查机制被绕过
  - 反“反审查”
- 简单的审查规避工具本身并不“抗审查”

反“反“反审查””：抗审查的审查规避

- 简易的审查规避工具会被积极的审查者屏蔽
- 创造具有**审查抗性**的审查规避工具
- 规避者的劣势
  - 去中心化，行动缺乏组织性
  - 项目开源，设计完全公开
- 新思路
  - 附加损害
  - 快速迭代
  - 百花齐放



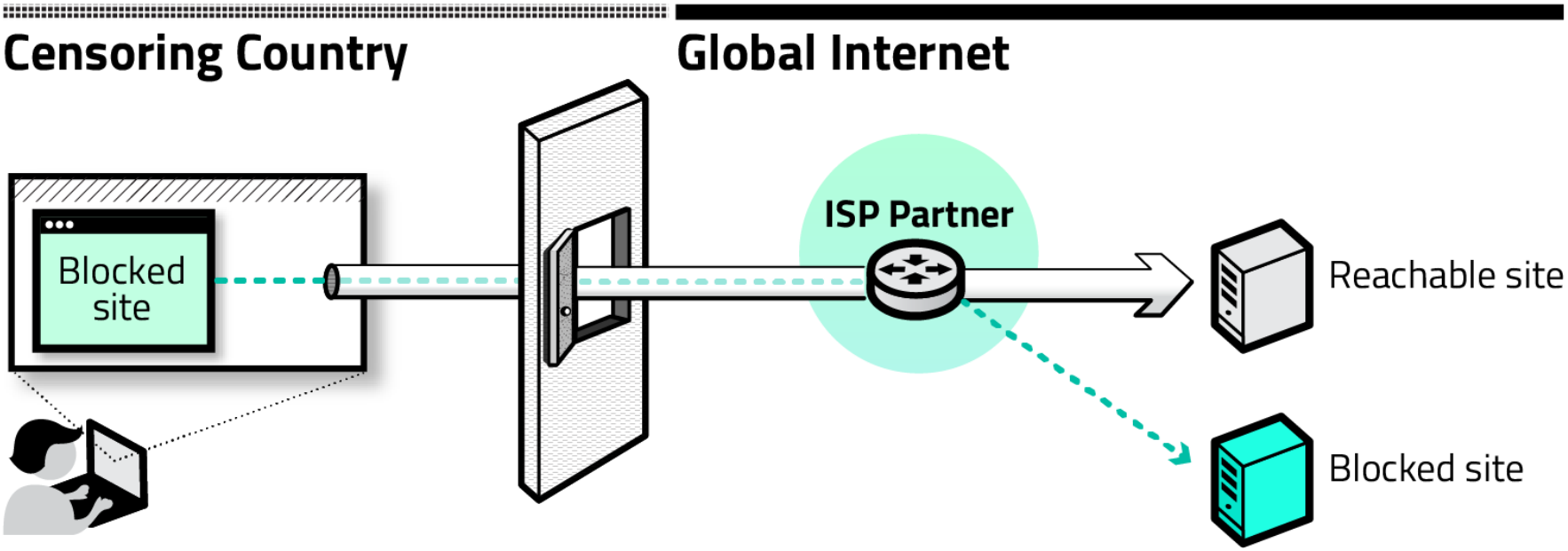
抗审查的审查规避：附加损害

Conjure: Summoning Proxies from Unused Address Space (CCS'19)

- 折射网络 (Refraction Networking)
  - 又名诱饵路由 (Decoy Routing)
  - 使用**虚构的**网络地址作为代理服务器
  - 通过其他方式使网络流量被转发（折射）到实际上的代理服务器

抗审查的审查规避：附加损害

Conjure: Summoning Proxies from Unused Address Space (CCS'19)



抗审查的审查规避：附加损害

Conjure: Summoning Proxies from Unused Address Space (CCS'19)

- Conjure：从未使用的地址空间召唤代理
  - 最新一代的折射网络技术
- 与互联网自由地区的网络提供商 (ISP) 合作
- 审查规避工具试图连接到网络提供商负责连接的**任意**可用网段
- 网络提供商负责甄别流量是否用于规避
  - 并转发规避流量到真实的代理服务器
  - 其他普通流量将被正常传输

抗审查的审查规避：附加损害

Conjure: Summoning Proxies from Unused Address Space (CCS'19)

- 假设
  - 假审查者无法承受彻底从国际互联网断开的代价
    - 审查者**不可能**屏蔽整个国际互联网
  - 理想情况下，使用合作的提供商包围审查者
    - 所有国际互联网的 IP 地址都可用作审查规避
- 结果
  - 审查者被迫选择**彻底断开**国际互联网或默许这种规避方式
- 反例
  - 伊朗于 2024年4月 屏蔽了 Conjure 使用的一个网段（共包含 256 个 IP 地址）
  - ~~壮士断腕？~~

抗审查的审查规避：快速迭代

Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)

- 积极的审查者屏蔽流行审查规避方式
  1. 某个规避方式变得流行
  2. 审查者开始研究该方式
  3. 审查者设计出（较）精确识别并屏蔽的方法
  4. 审查者部署并启用此屏蔽

- 当已知规避策略停止工作（被屏蔽）
  1. 确定技术原理
  2. 设计新的策略
  3. 更新既存工具（复杂：不同工具需要分别更新）
  4. 发布新版工具（缓慢：手机平台需要应用商店审核）
  5. 用户下载新版（低效：需要重新安装整个程序）

抗审查的审查规避：快速迭代

Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)

- WebAssembly
  - 全设备/平台支持
    - Linux, macOS, Windows
    - Android, iOS
  - 跨编程语言支持
    - C/C++
    - Go
    - Python
    - Rust
  - 模块化
    - 灵活度高，方便更新

抗审查的审查规避：快速迭代

Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)

- WATER: WebAssembly Transport Executables Runtime
  - 用 WebAssembly 承载规避策略
  - 将每种规避策略打包成一个模块
  - 为基于 WebAssembly 的规避策略提供宿主/驱动程序

  - 更高的工作利用效率
    - 同一个模块可以在所有不同工具上使用

  - 更快的更新速度
    - 下发单个文件更新规避策略，绕过应用商店审核
    - 无需重新安装宿主驱动程序

抗审查的审查规避：百花齐放

Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)

- 积极的审查者屏蔽流行审查规避方式
  1. **某个规避方式变得流行**
  2. **审查者开始研究该方式**
  3. 审查者设计出（较）精确识别并屏蔽的方法
  4. 审查者部署并启用此屏蔽

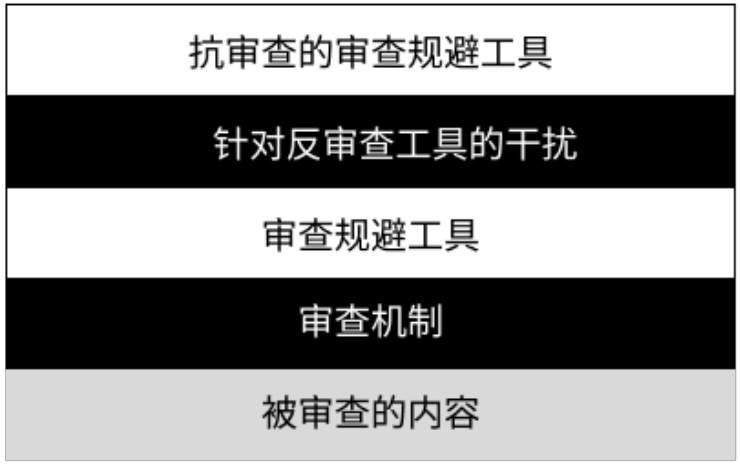
- 大规模的生成不同（但安全）的规避策略

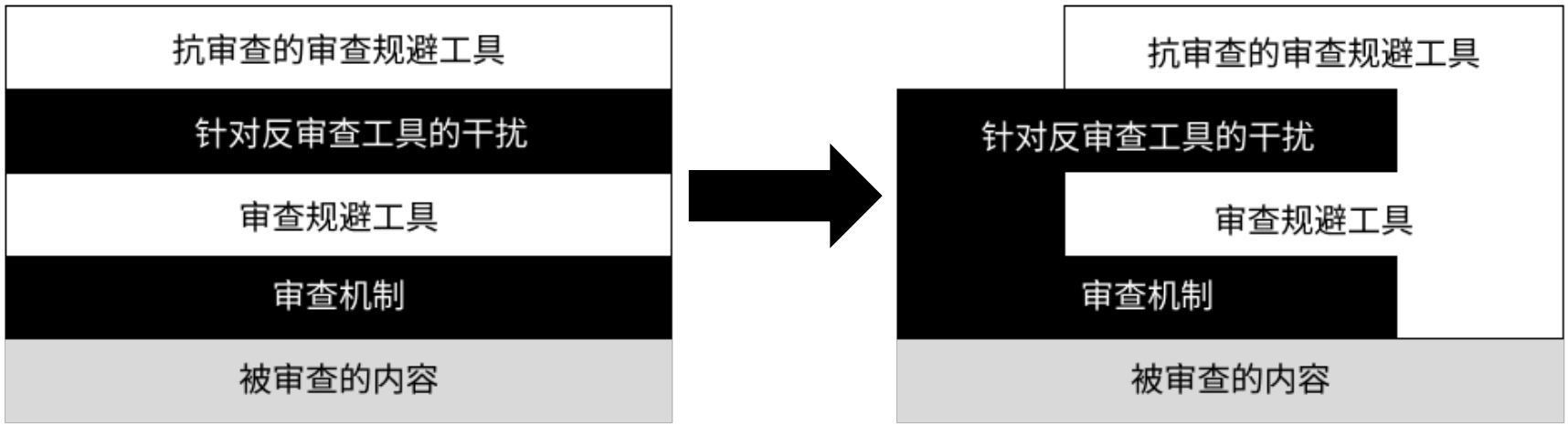
- 审查者无法有效的针对任意一种"流行"策略
  - 因为没有任何策略是"流行"的

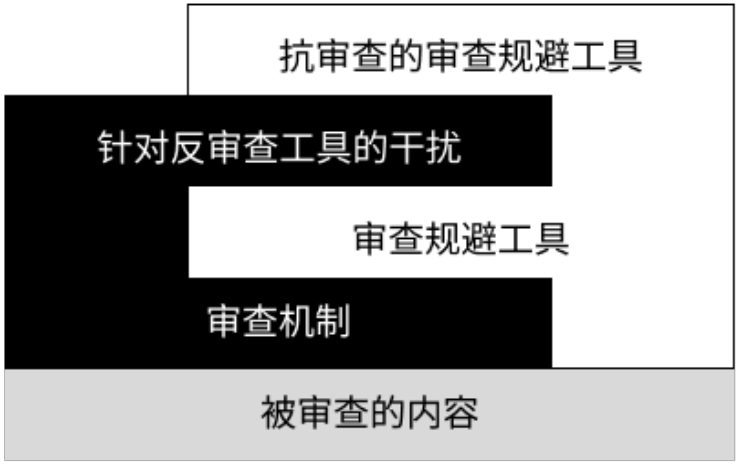
抗审查的审查规避：百花齐放

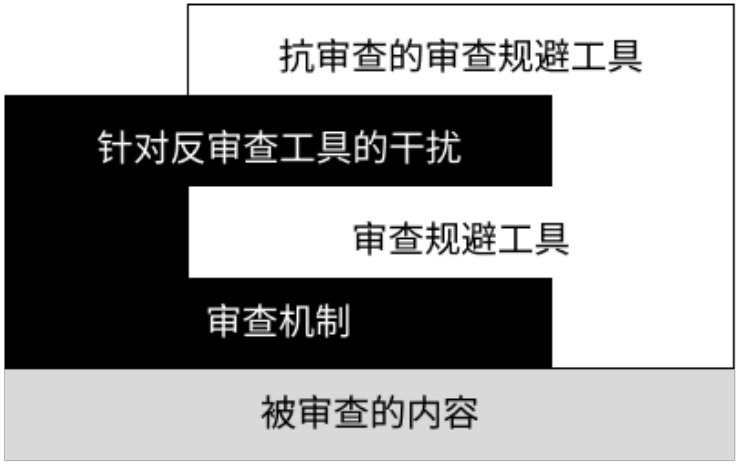
Just add WATER: WebAssembly-based Circumvention Transports (FOCI 2024)

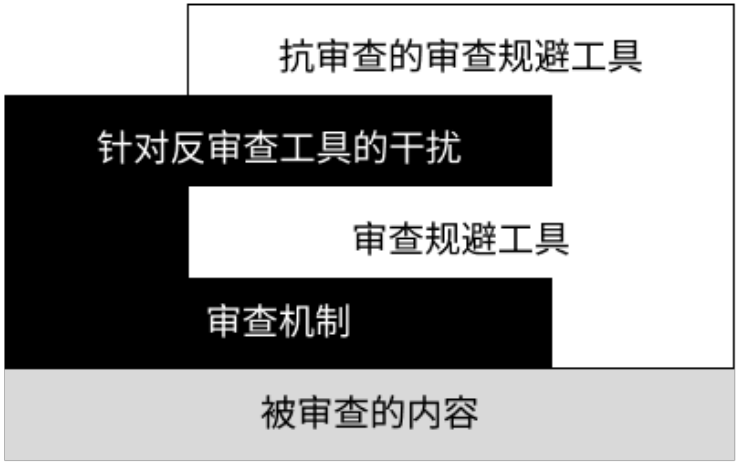
- 使用统一的宿主程序运行不同的策略
  - 如 WATER


抗审查的审查规避工具
针对反审查工具的干扰
审查规避工具
审查机制
被审查的内容


抗审查的审查规避工具
针对反审查工具的干扰
审查规避工具
审查机制
被审查的内容
抗审查的审查规避工具
针对反审查工具的干扰
审查规避工具
审查机制
被审查的内容


抗审查的审查规避工具
针对反审查工具的干扰
审查规避工具
审查机制
被审查的内容


抗审查的审查规避工具
针对反审查工具的干扰
审查规避工具
审查机制
被审查的内容



“防火长城之父”方滨兴院士：“审查与规避之间会有一场永不休止的争斗”