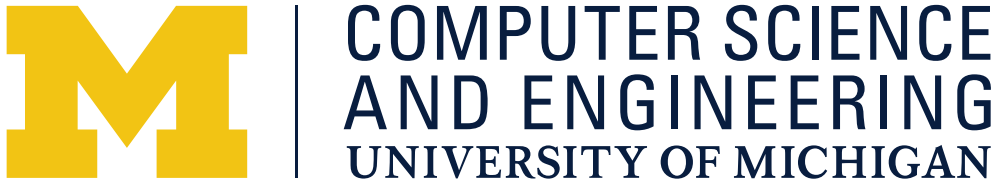
Umbra

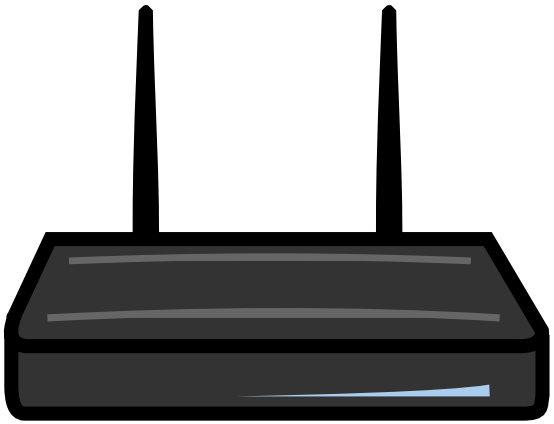
Embedded Web Security through Application-Layer Firewalls

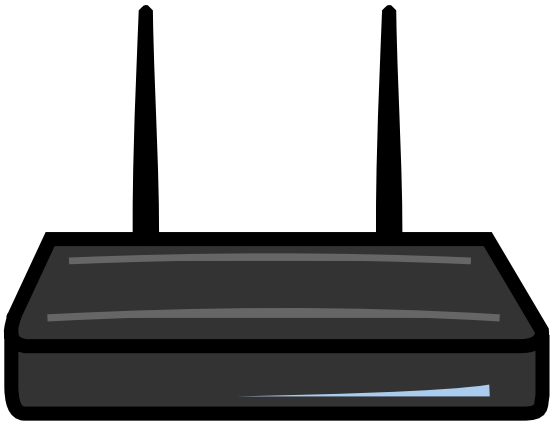
Travis Finkenauer J. Alex Halderman

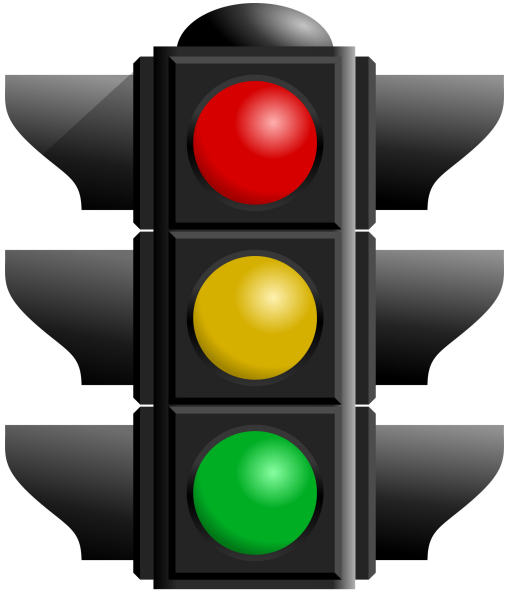


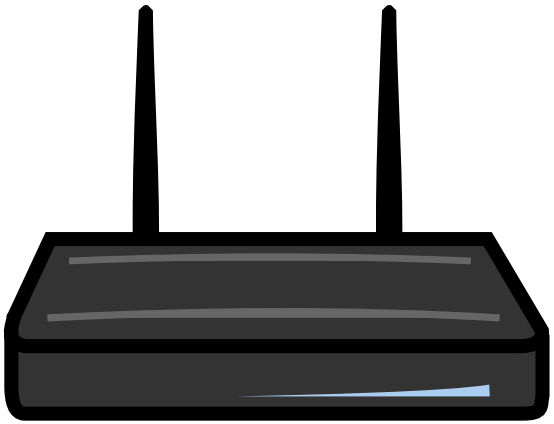
1st Workshop on the Security of Cyber-Physical Systems

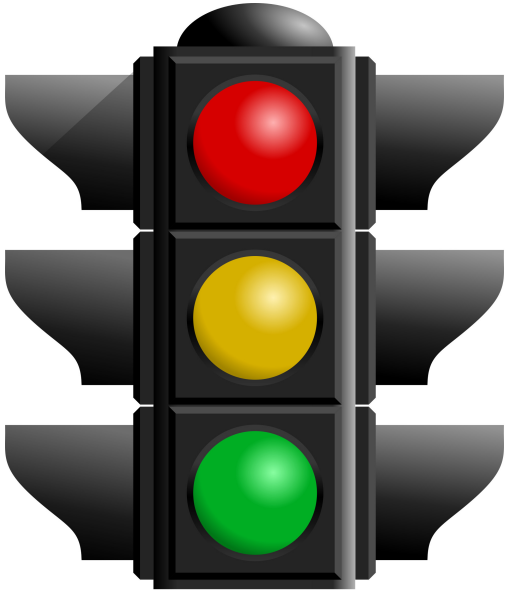
22 September 2015

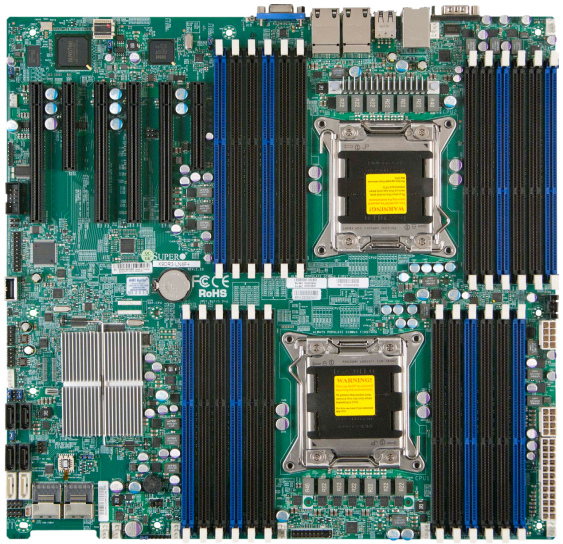


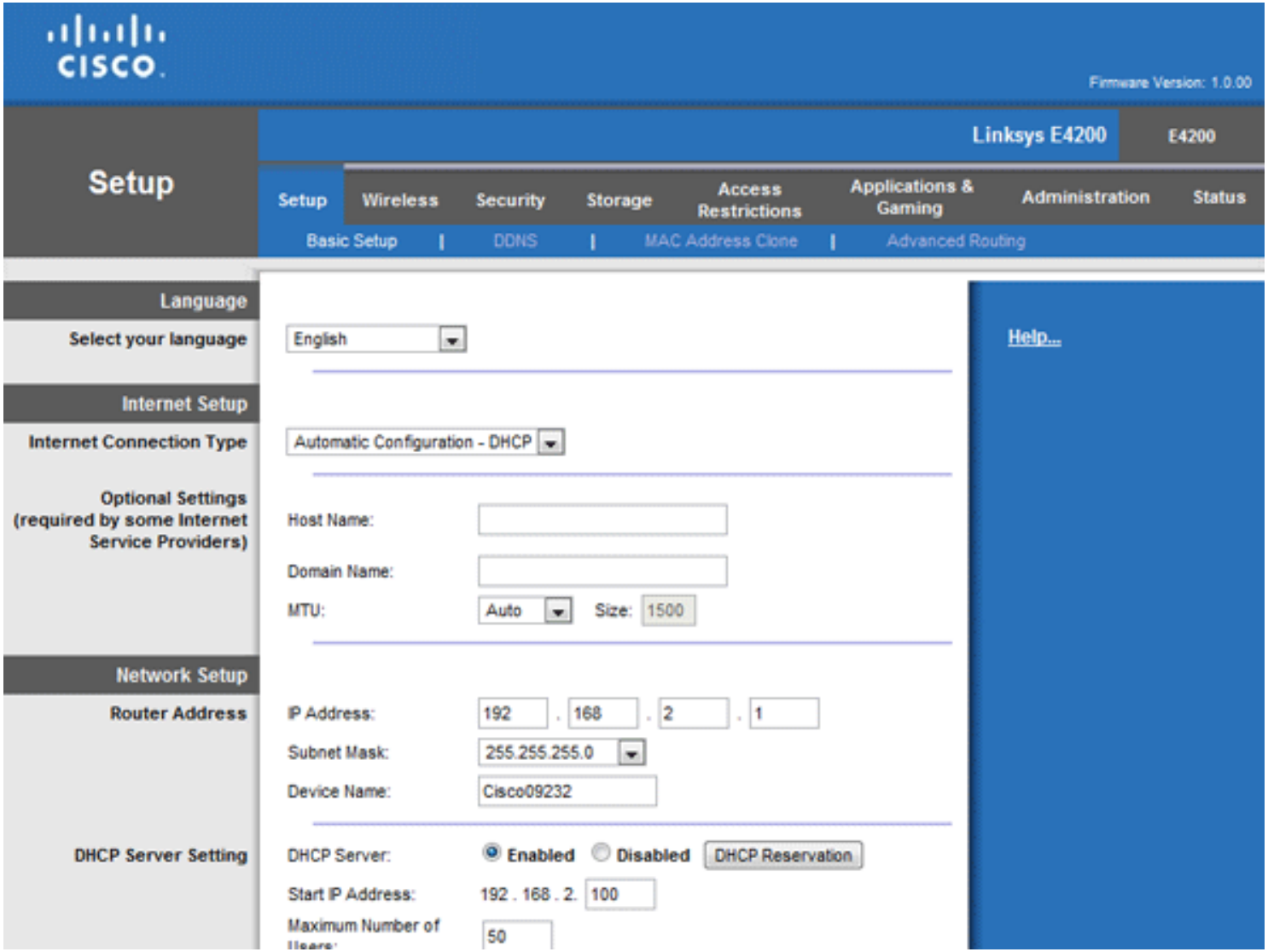


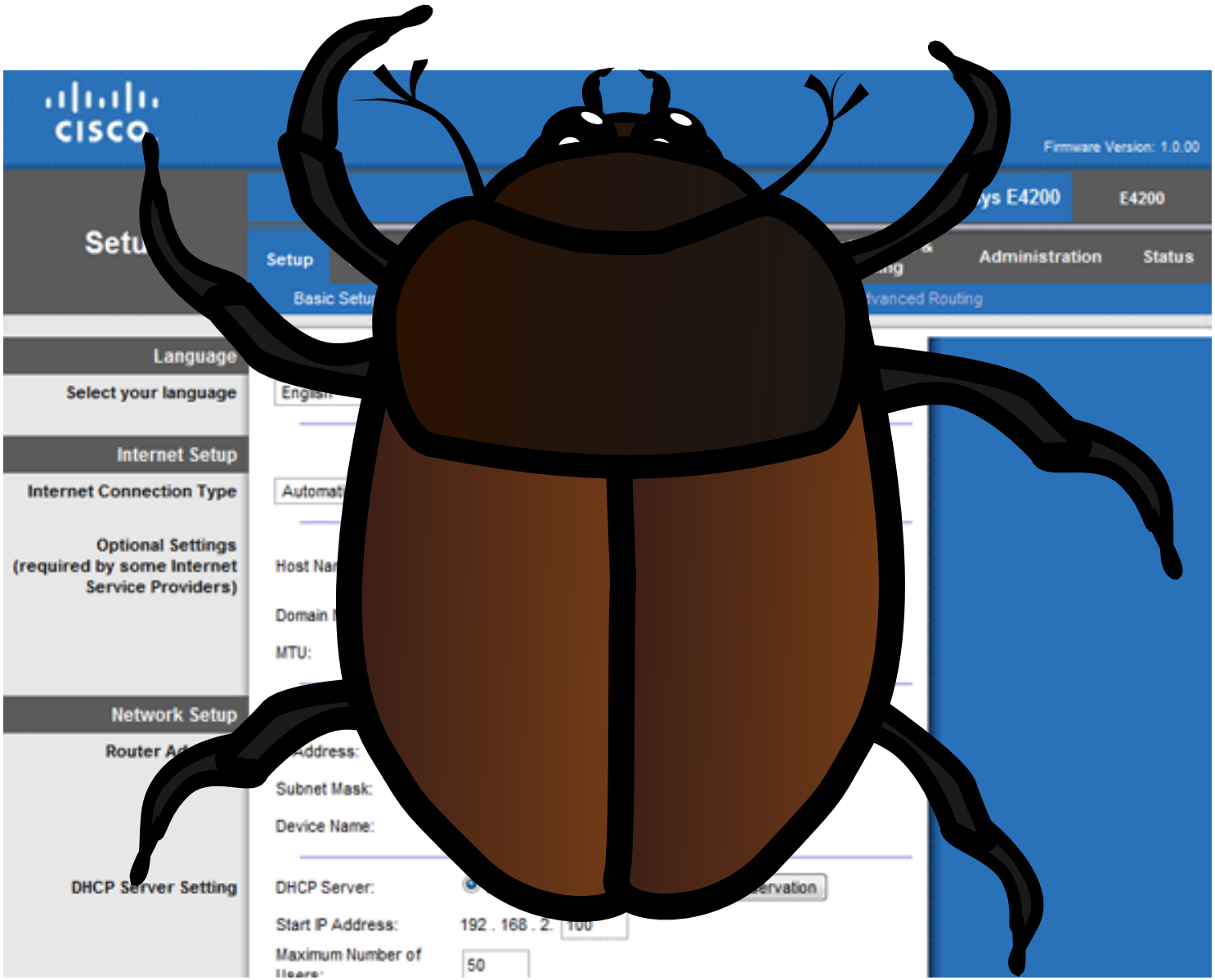









cisco
Firmware Version: 1.0.00
Setup
Linksys E4200
E4200
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup | DDNS | MAC Address Clone | Advanced Routing
Language
Select your language
English
Help...
Internet Setup
Internet Connection Type
Automatic Configuration - DHCP
Optional Settings (required by some Internet Service Providers)
Host Name:
Domain Name:
MTU:
Auto
Size:
1500
Network Setup
Router Address
IP Address:
192 . 168 . 2 . 1
Subnet Mask:
255.255.255.0
Device Name:
Cisco09232
DHCP Server Setting
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
192 . 168 . 2.
100
Maximum Number of
50


CISCO
Firmware Version: 1.0.00
E4200
Setup
Administration
Status
Language
Select your language
Internet Setup
Internet Connection Type
Optional Settings
(required by some Internet
Service Providers)
MTU:
Network Setup
Subnet Mask:
Device Name:
DHCP Server Setting
DHCP Server:
Start IP Address:
192 . 168 . 2.
Maximum Number of
50

Motivating Example

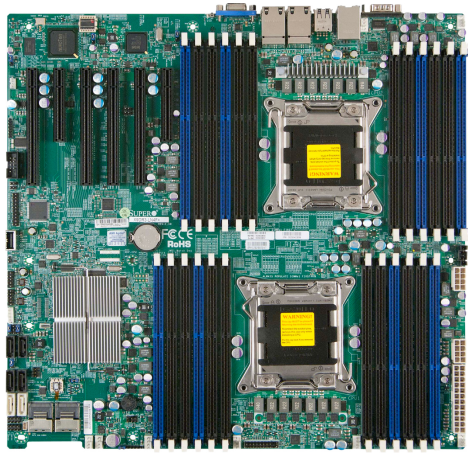
- Authentication bypass in D-Link router

Exploit

Cookie: cookie_lang=1; **client_login=admin**; client_password=1

Motivating Example

- Stack-based buffer overflow in Supermicro IPMI web interface



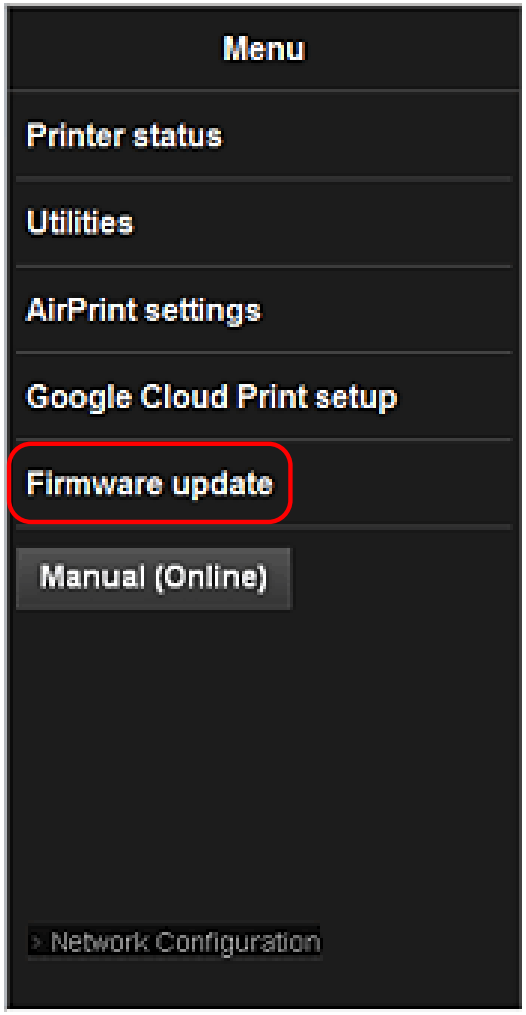
Exploit

```
POST /cgi/login.cgi HTTP/1.1
Content-Type:  application/x-www-form-urlencoded

name=AAAAAAAAAAAAAAAAAA...&pwd=AAAAAAAAAAAAAAAAAA...
```

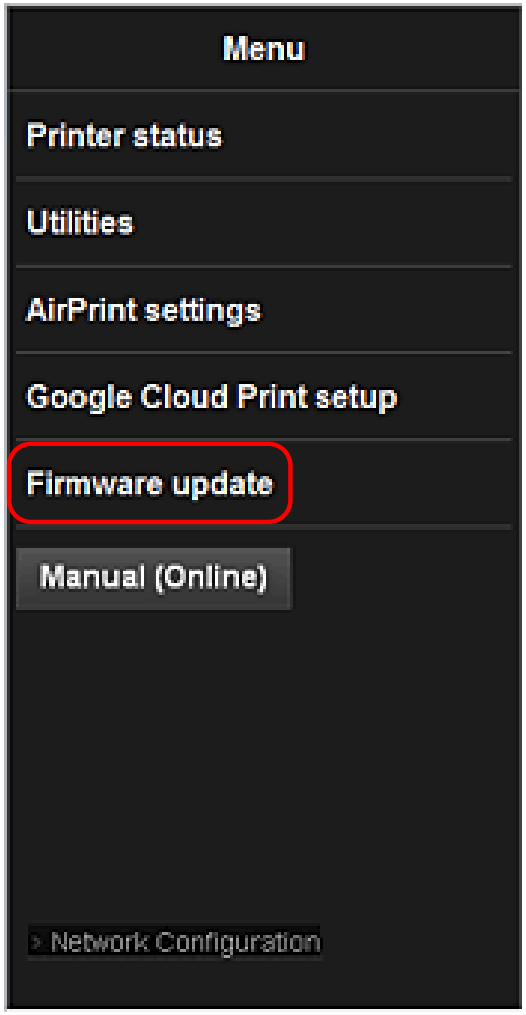
Motivating Example

- No authentication and firmware upload CSRF vuln in Canon printer



Motivating Example

- No authentication and firmware upload CSRF vuln in Canon printer



Problem

- Security vulnerabilities are prevalent in embedded devices
  - Embedded developers often have limited knowledge and experience with security
- Existing solutions are not sufficient:
  - Standalone network appliances
  - Web frameworks

Solution

Design drop-in security *shim* that:

Solution

Design drop-in security *shim* that:

- ✓ Integrates simply with existing embedded devices

Solution

Design drop-in security *shim* that:

- ✓ Integrates simply with existing embedded devices
- ✓ Operates in small CPU, code size, and memory footprint

Solution

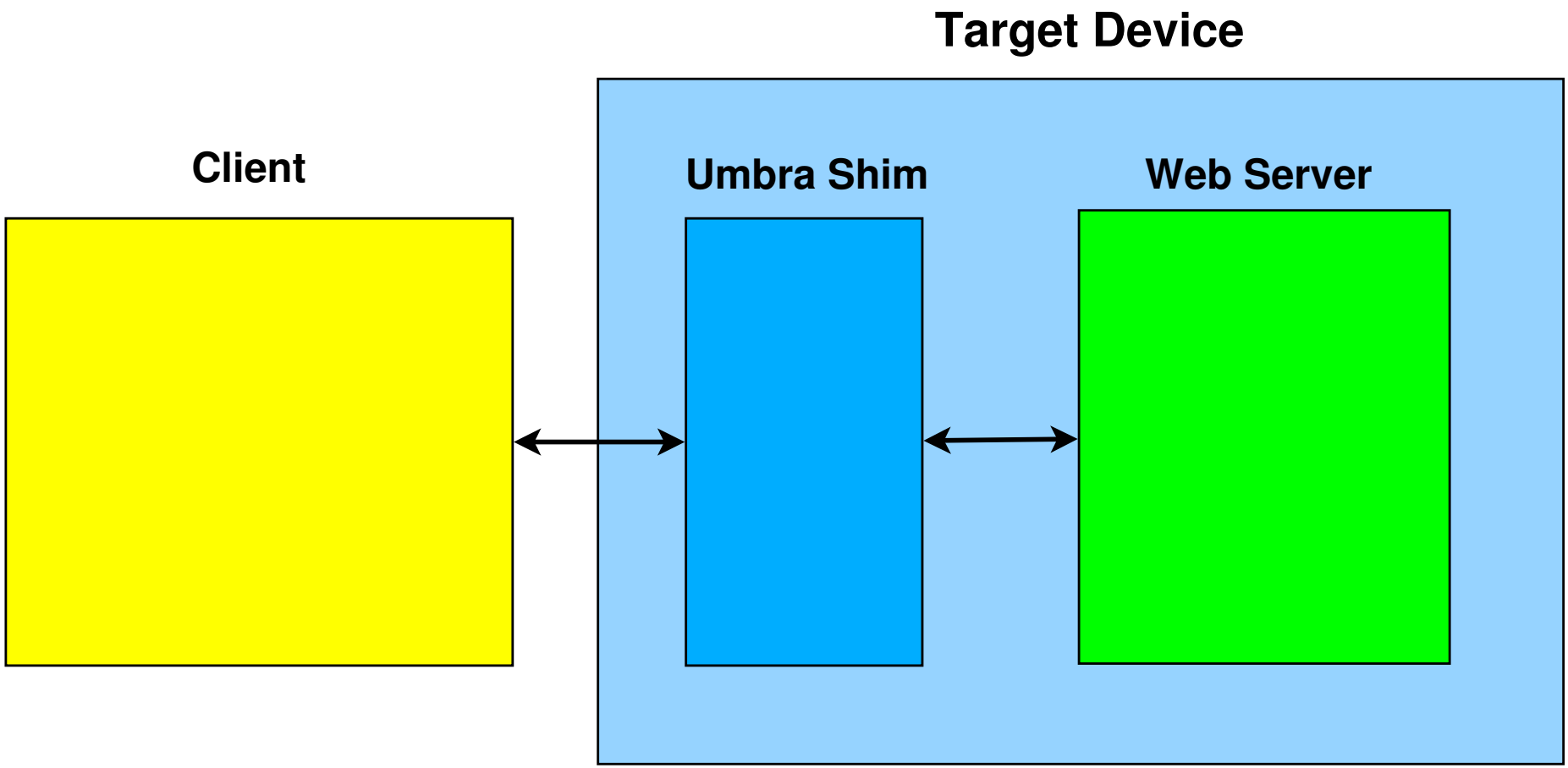
Design drop-in security *shim* that:

- ✓ Integrates simply with existing embedded devices
- ✓ Operates in small CPU, code size, and memory footprint
- ✓ Works on systems where source code is not available

Outline

Outline

Design



Threat Model

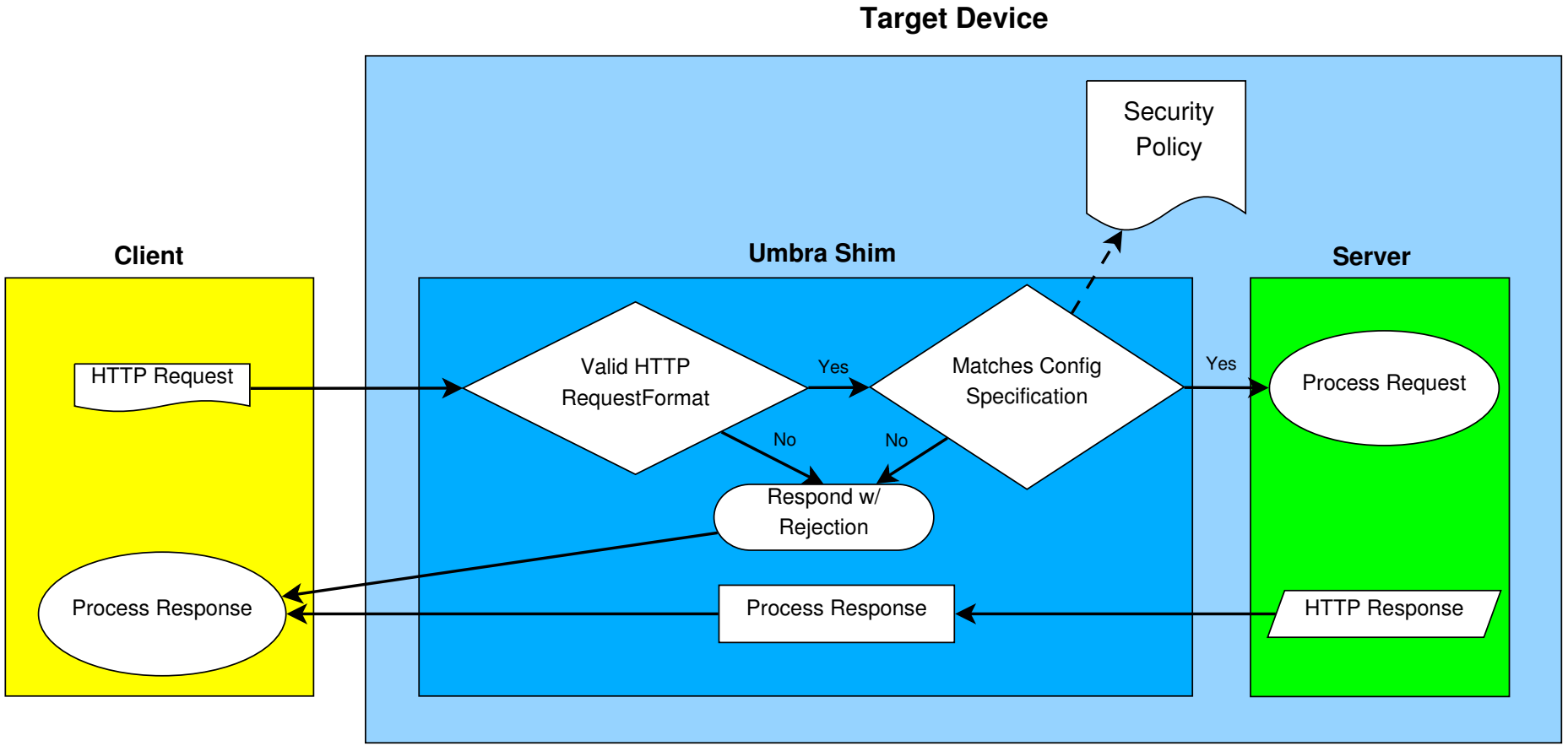
In Scope

- Attacks on web interfaces
  - HTTP or HTTPS
- User viewing attacker-controlled pages

Out of Scope

- Attacks on other services
- Network-level attackers

System Design



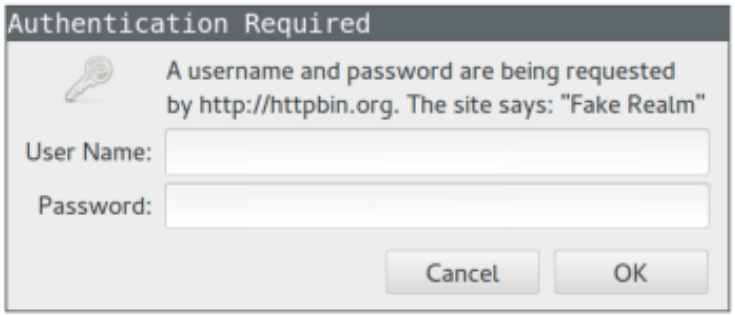
System Design

- Transparent proxy between clients and server
- Modifies HTTP requests and responses
- Non-blocking sockets using Linux's epoll

Security Features

Vulnerability	Security Features
XSS	Parameter whitelist
CSRF	CSRF protection
Authentication bypass	Authentication enforcement HTTP method whitelist
Information leak	Authentication enforcement HTTP method whitelist Directory traversal check
CGI memory corruption	Parameter character whitelist Parameter length check Header field length limit
Directory traversal	Directory traversal check

Page-level Authentication



- Prevents authentication bypass and information leak vulnerabilities
- Umbra can enforce RFC 2617 Basic Authentication
- Umbra reads credentials from file at run time

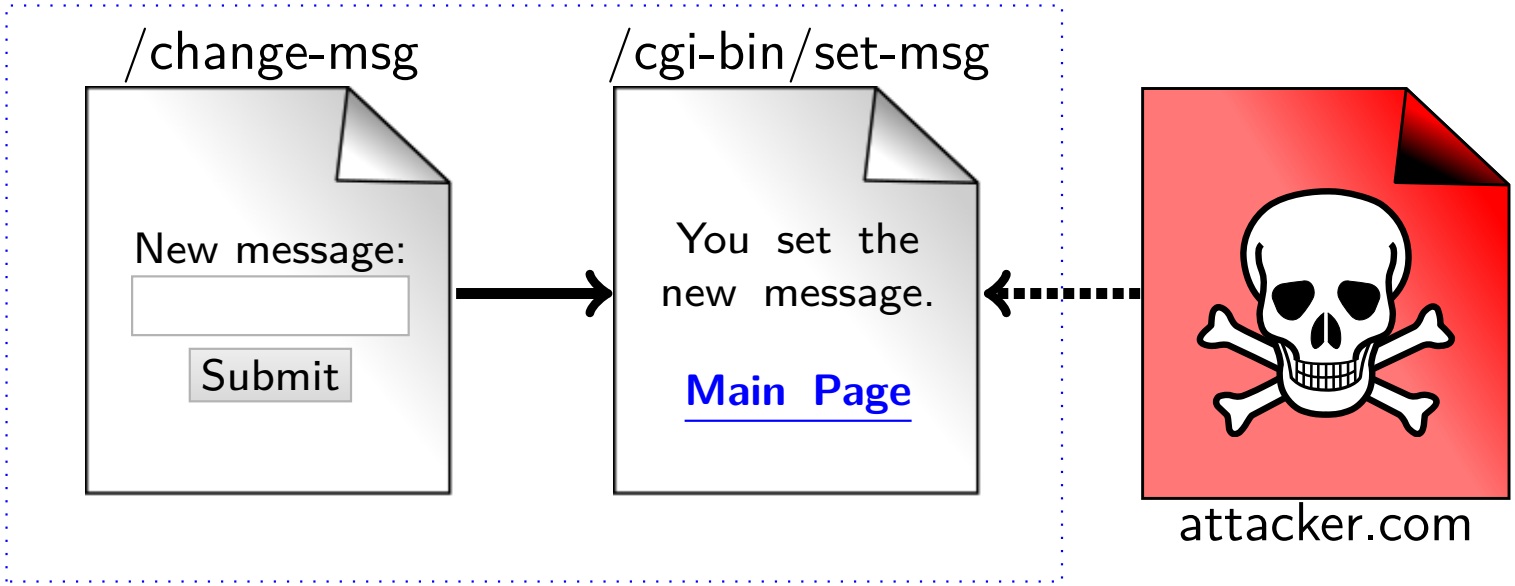
Header Length Limit

- Mitigates buffer overflows
- Limits the length of header fields and values

Exploit

```
GET / HTTP/1.1
Host:  192.168.1.1
Connection:  keep-alive
User-Agent:  Mozilla/5.0 (X11; Linux x86_64)
Overflow:  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

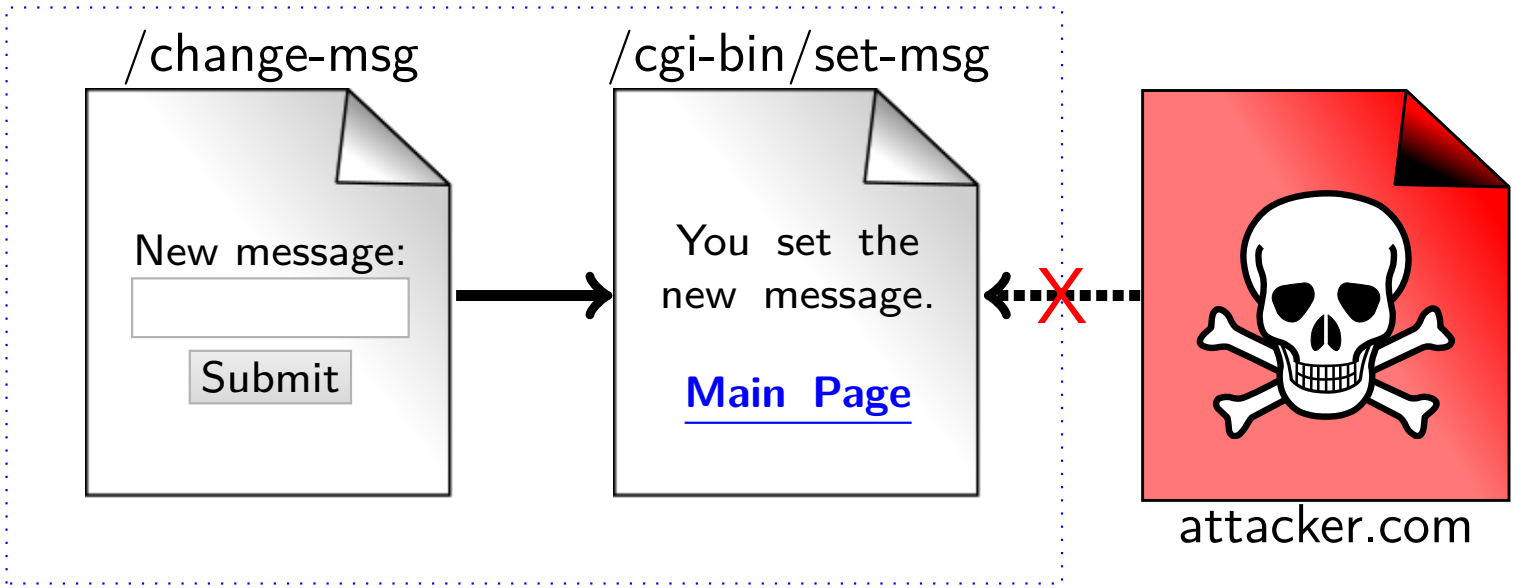
CSRF Protection



Page snippet

```
<form action="cgi-bin/set-msg">
  <input type="ext" name="new-message">
</form>
```

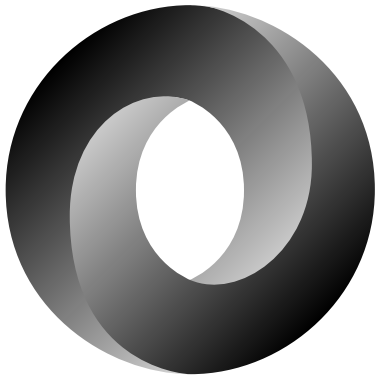
CSRF Protection



Page snippet

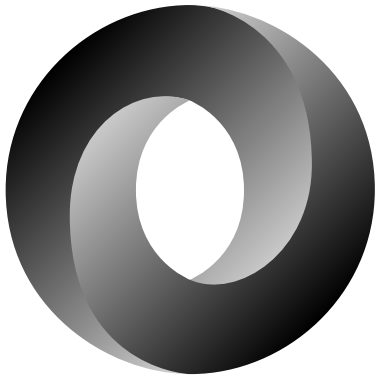
```
<form action="cgi-bin/set-msg">
  <input type="ext" name="new-message">
  <input type="hidden"
         name="_umbra_csrf_token"
         value="D629B39EA123DB0E0C35">
</form>
```

Security Policy



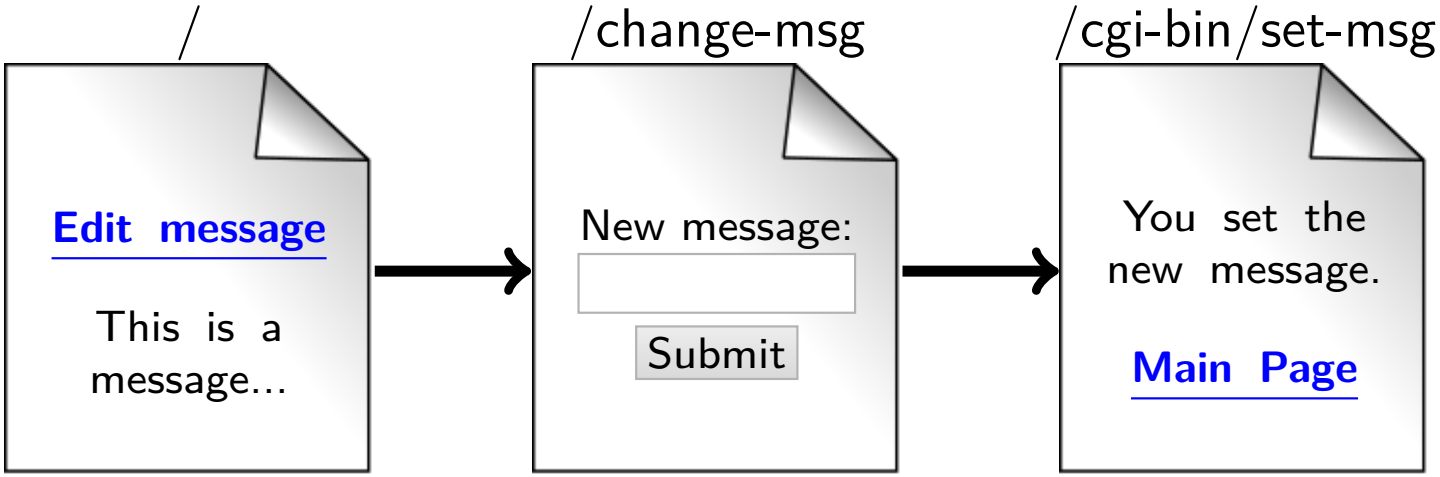
- Manufacturers define good vs. bad behavior
- Umbra enforces policy described in configuration file
  - Select any combination of security features
- Compiles configuration into C code, which is compiled into Umbra binary

Security Policy



- Sections:
  - Global configuration
  - Default page policy
  - Per-page policy
- Specify conservative global policy
  - Relax policy for specific pages

Example Web Application



Global Page Policy

```
"global_config": {
  "enable_request_type_check": true,
  "enable_param_len_check": true,
  "enable_param_whitelist_check": true,
  "enable_csrf_protection": true,
  "enable_authentication_check": true,
  "session_life_seconds": 300
}
```

Default Page Policy

```
"default_page_config": {
  "request_types": ["GET", "HEAD"],
  "requires_login": true,
  "has_csrf_form": false,
  "receives_csrf_form_action": false,
  "max_param_len": 30,
  "whitelist": "[a-zA-z0-9_]"
}
```

Per-Page Policy

```
"page_config": {
  "/":{
    "requires_login": false
  },
  "/change-msg":{
    "has_csrf_form": true
  },
  "/cgi-bin/set-msg": {
    "request_types": ["POST"],
    "receives_csrf_form_action": true,
    "params": {
      "new-msg": {
        "max_param_len": 200,
        "whitelist": "[a-zA-z0-9_,.! ]"
      }
    }
  }
}
```

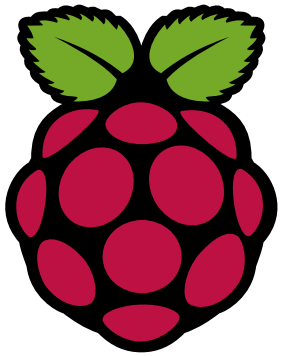
Outline

Questions

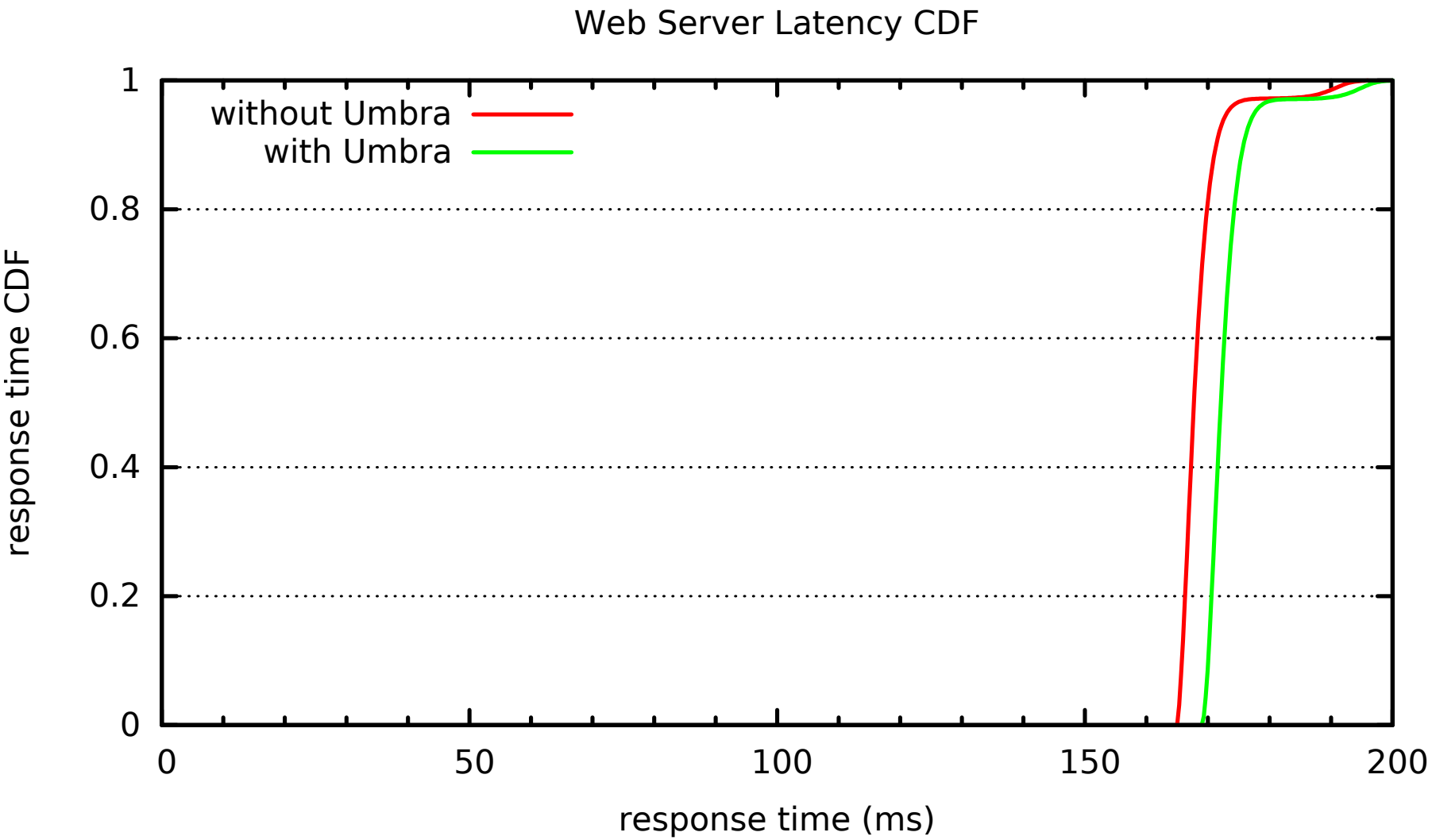
1. What is the performance impact?
2. Does Umbra achieve the security goal?

Performance

- Tested on Raspberry Pi Model B running OpenWRT 14.07
- Laptop connected via 100 Mbps Ethernet
- Used Apache Benchmark tool to download main page (2.2 kB)



Performance



Footprint

- Size of dynamically-linked ARM binary
  - Umbra: 75 kB
  - Dropbear: 138 kB
  - Busybox: 370 kB
- CPU utilization was 2–3% during benchmark
- Peaked at a virtual memory size of 1.2 MB
  - Raspberry Pi has 512 MB of RAM

Security Evaluation

Brother
Cannon
Cisco
D-Link
Linksys
Lorex
Netgear
Supermicro
TP-LINK
Trendnet
Xerox

- Randomly sampled 100 recent vulnerabilities from eight embedded manufacturers
  - 40 out of 100 dealt with embedded web interfaces
- Manually classified:
  - Type of vulnerability
  - Level of protection

How well can Umbra protect?

Vulnerability	Protection Level				Total
	None	Partial	Full	Unknown	
Bypass	1	0	4	0	5
CSRF	0	0	5	1	6
Information leak	1	0	3	0	4
Command injection	0	0	2	0	2
Directory traversal	0	0	1	0	1
SQL injection	0	0	0	1	1
Other	0	0	0	1	1
Denial of service	3	1	1	1	6
Memory corruption	2	0	1	0	3
XSS	2	3	3	3	11
Protect Totals	9	4	20	7	40

How well can Umbra protect?

Vulnerability	Protection Level				Total
	None	Partial	Full	Unknown	
Bypass	1	0	4	0	5
CSRF	0	0	5	1	6
Information leak	1	0	3	0	4
Command injection	0	0	2	0	2
Directory traversal	0	0	1	0	1
SQL injection	0	0	0	1	1
Other	0	0	0	1	1
Denial of service	3	1	1	1	6
Memory corruption	2	0	1	0	3
XSS	2	3	3	3	11
Protect Totals	9	4	20	7	40

Security Features Used

Vulnerability	Security Feature						Total
	Auth	CSRF	Param. White.	Dir. Traver.	Header Length Check	Param. Length	
Bypass	4	0	0	0	0	0	4
Command injection	0	0	2	0	0	0	2
CSRF	0	5	0	0	0	0	5
Denial of service	0	0	0	0	1	0	1
Directory traversal	0	0	0	1	0	0	1
Information leak	2	1	0	0	0	0	3
Memory corruption	0	0	0	0	0	1	1
Other	0	0	0	0	0	0	0
SQL injection	0	0	0	0	0	0	0
XSS	0	0	3	0	0	0	3
Feature Totals	6	6	5	1	1	1	20

Security Features Used

Vulnerability	Security Feature						Total
	Auth	CSRF	Param. White.	Dir. Traver.	Header Length Check	Param. Length	
Bypass	4	0	0	0	0	0	4
Command injection	0	0	2	0	0	0	2
CSRF	0	5	0	0	0	0	5
Denial of service	0	0	0	0	1	0	1
Directory traversal	0	0	0	1	0	0	1
Information leak	2	1	0	0	0	0	3
Memory corruption	0	0	0	0	0	1	1
Other	0	0	0	0	0	0	0
SQL injection	0	0	0	0	0	0	0
XSS	0	0	3	0	0	0	3
Feature Totals	6	6	5	1	1	1	20

Outline

Future Work

- Automatically learning a security policy
- Applying formal methods to Umbra code
- Handling other management protocols
  - SNMP
  - IPMI
  - Telnet/SSH

Conclusion

- Built Umbra, an HTTP firewall that comfortably runs in the footprint of an embedded system
- Umbra is capable of preventing about half of the surveyed vulnerabilities dealing with embedded web interfaces
- Configuration is expressive

Umbra

Embedded Web Security through Application-Layer Firewalls

Travis Finkenauer J. Alex Halderman

Umbra is available as free and open source software:

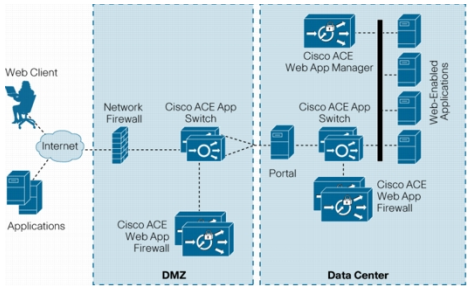
`https://github.com/umbra-firewall/umbra`

Backup Slides

Standalone Firewalls

- Operate as separate network entity
  - Many require inline hardware appliances
- Examples:
  - Akamai Kona
  - Cisco ACE
  - HP TippingPoint
- Features
  - Outbound filtering for personal information such as credit card numbers
  - Detect common web attacks

Akamai Kona



Cisco ACE

Host-based Firewalls

- Operate as a plug-in for common web servers
  - ModSecurity
  - IronBee
- Analyzes items such as user-agent strings, SQL queries, real-time IP blacklist, and HTTP parameters