

Embedded Sensors Project (ESP)

“The Operating System *is* the Intrusion Detection System”

Current Work

Sensor placement in high profile / volume network services:
Apache, BIND, OpenSSH, Sendmail

Sensor Message Management System

Performance evaluation

Scalability analysis over a range of network services

Building testbed

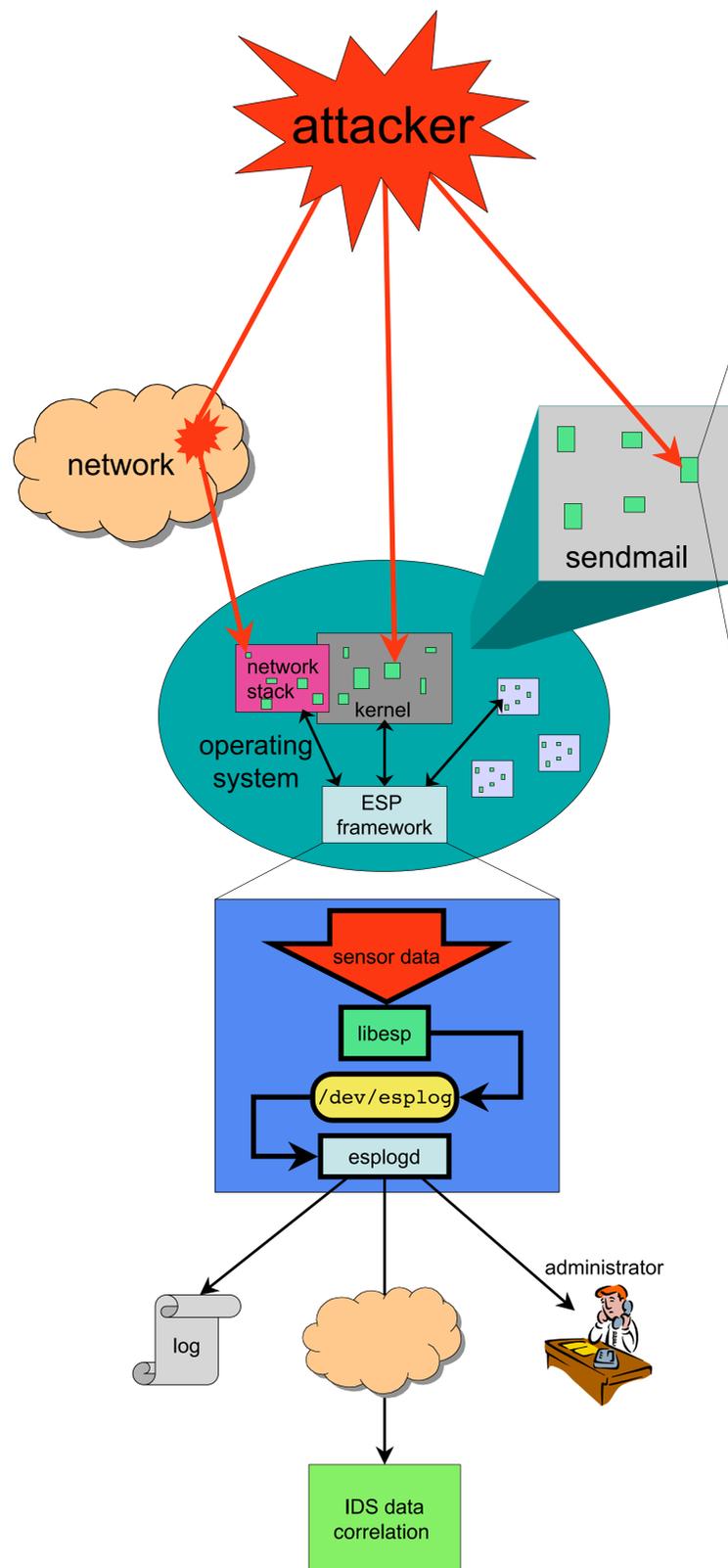
FreeBSD-based implementation

Future Research

Open Source Portable Sensor Support Framework

Modular Response System

Meta-detector design



<http://www.cerias.purdue.edu/homes/esp/>

What is a Sensor?

Small amount of code inserted into OS and application

Monitors system and program behavior directly

Detects an attack at the point of vulnerability

Minimal amount of code changed/added

```
#ifdef ESP_CVE_1999_245
    if(strlen(home_env)>255)
        esplog("CVE_1999_245");
#endif
```

Benefits

Difficult to circumvent

Tamper-resistant

Host and network attack detection

Low resource overhead

Real-time detection

Almost no false negatives