CERIAS

Embedded Sensors Project (ESP)

"The Operating System *is* the Intrusion Detection System"

Benefits

Difficult to circumvent

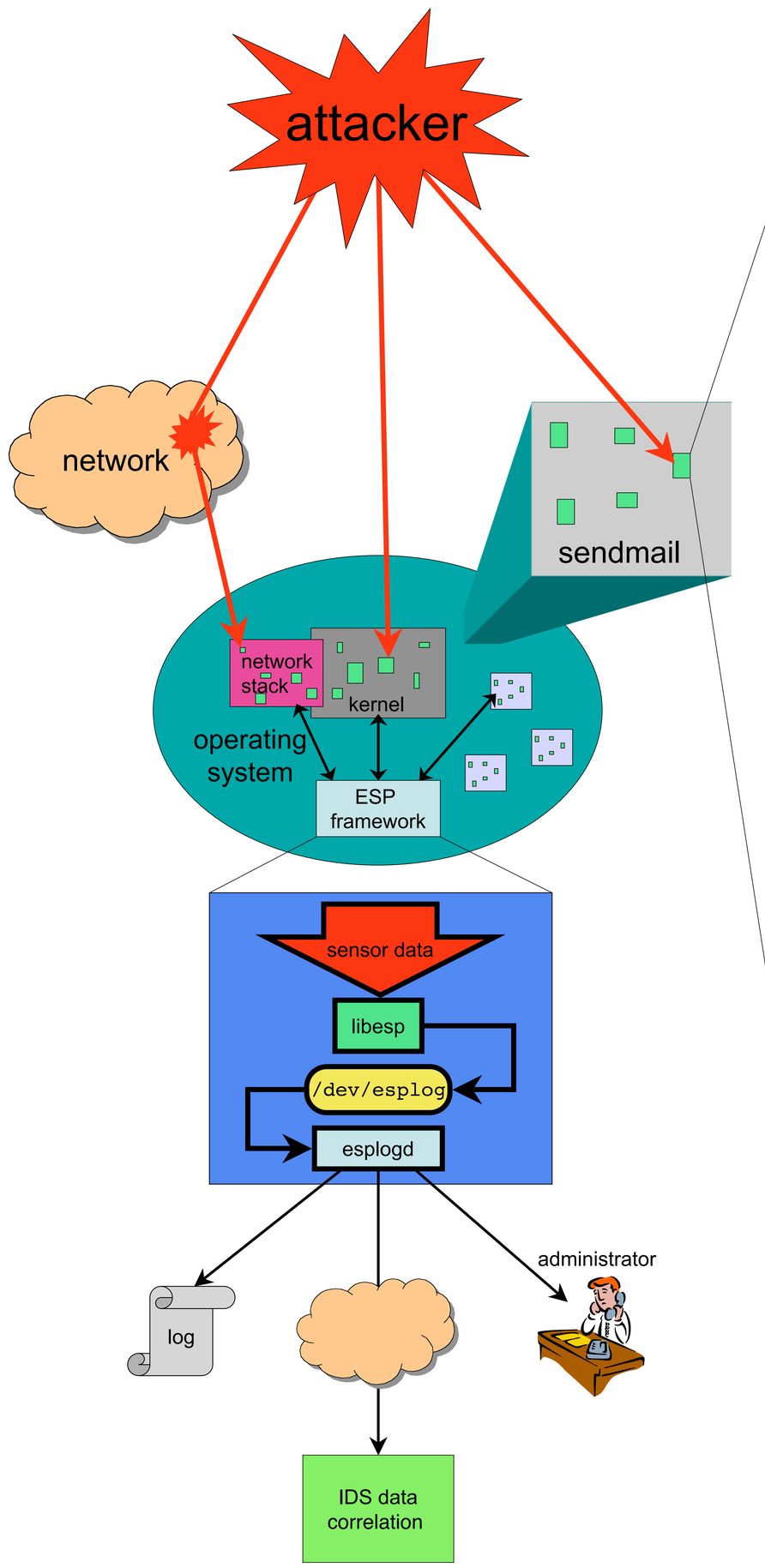
Tamper-resistant

Host and network attack detection

Low resource overhead

Real-time detection

Almost no false negatives



What is a Sensor?

Small amount of code inserted into OS and application

Monitors system and program behavior directly

Placed at critical points in code

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
```

Future Research

ESP-enabled OS

Portable Sensor Support Framework

Modular Response System

Meta-detector design

Large scale sensor deployment

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

References

- D. Zamboni, Using Internal Sensors for Computer Intrusion Detection. Purdue CS Ph.D. Thesis, August 2001.
- E. Spafford, D. Zamboni, Data collection mechanisms for intrusion detection systems. CERIAS Technical Report 2000-08 (2000), Purdue University, West Lafayette, IN.
- F. Kerschbaum, E.H. Spafford, D. Zamboni, Using Internal Sensors and Embedded Detectors for Intrusion Detection. Journal of Computer Security, Volume 10 Issues 1/2 (2002), 23-70.
- F. Kerschbaum, E.H. Spafford, D. Zamboni, Using embedded sensors for detecting network attacks. *Proc. of the 1st ACM Workshop on Intrusion Detection Systems*, ACM SIGSAC, (eds. D. Frincke, D. Gritzalis), November 2000.
- J. Early, An Embedded Sensor For Monitoring File Integrity. CERIAS Technical Report 2001-41 (2001), Purdue University, West Lafayette, IN.

PURDUE UNIVERSITY

CERIAS Center for Education and Research in Information Assurance and Security

e-Enterprise Center