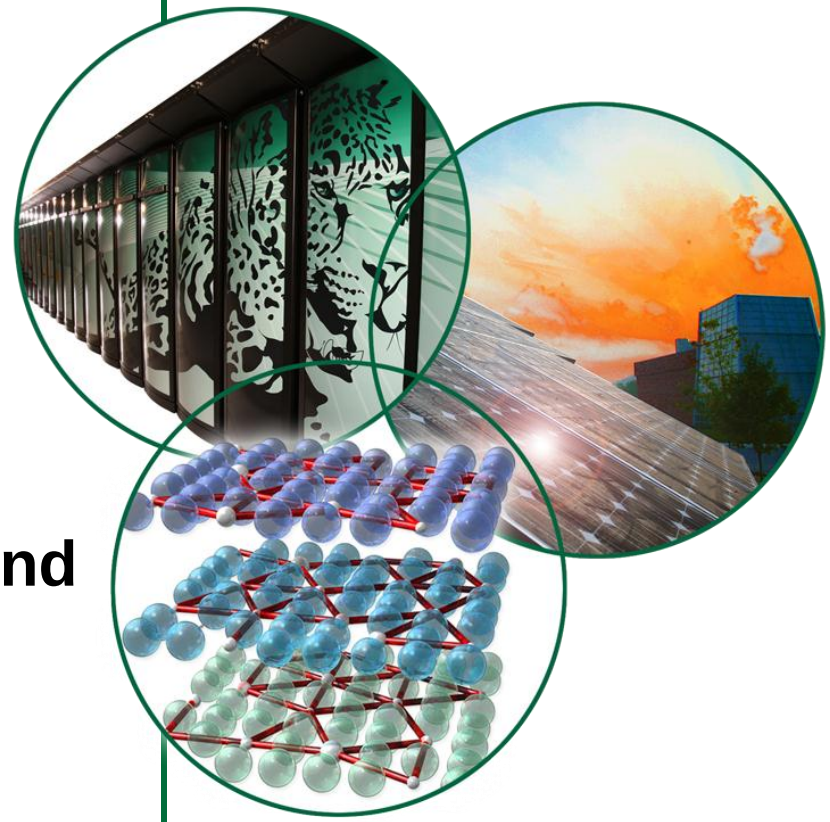
Remote Intrusion Detection (RID)

Mario Sutton
Fayetteville State University

Stacy Prowell, Ph. D.
Aaron Ferber
Computational Sciences and Engineering Division

Research Alliance in Math and Science
Computing and Computational Sciences



Oak Ridge, Tennessee
August 7, 2012

Outline

- Introduction
- Background
- Objectives
- Process
- Results
- Conclusion
- Summary
- Questions

Introduction

Securing U. S. cyber infrastructure is critical

- Attacks occur daily
- Maintaining secure cyber infrastructure is important
  - Institutions
    - Private
    - Public
  - Individual / personal use
- Attackers improve infiltration methods daily
- Difficulty of maintaining secure infrastructure increases
- Remote Intrusion Detection is proposed solution
  - Cannot keep out attackers entirely
  - Thwart efforts before any serious damage occurs

Intrusion detection

- Act of discovering occurring unauthorized activity
- Intrusion detection systems (IDS)
  - Host-based IDS
  - Network-based IDS
  - Behavioral network analysis
  - Wireless-based IDS
- All possess strengths and weaknesses
- Most effective use of intrusion detection thus far:
  - Includes multiple IDS
  - Simultaneous operation

Rootkits

- Software “kits”
- Used to gain and maintain unauthorized root / admin privileges
- Types
  - Kernel
    - Most used
    - Very harmful
    - Difficult detection
  - User-land (user mode)
  - Hardware-based
  - Hypervisor-based
  - Boot-loader
- Known and mostly used for stealth

Multilin D400

- Substation gateway created by General Electric (GE)
- Very advanced tool
  - Collection system
  - Filtration system
- Very useful for RID pursuit
- Functions
  - Advanced gateway
  - Fault logging
  - Secure access
  - Advanced automation

About RID - What makes it so special?

- Current IDS techniques are good, but have problems
- Need multiple devices for good results
  - Most are designed to work independently
  - High maintenence
- Not completely accurate
- Only warns of intrusion
- High human dependence

About RID - What makes it so special?

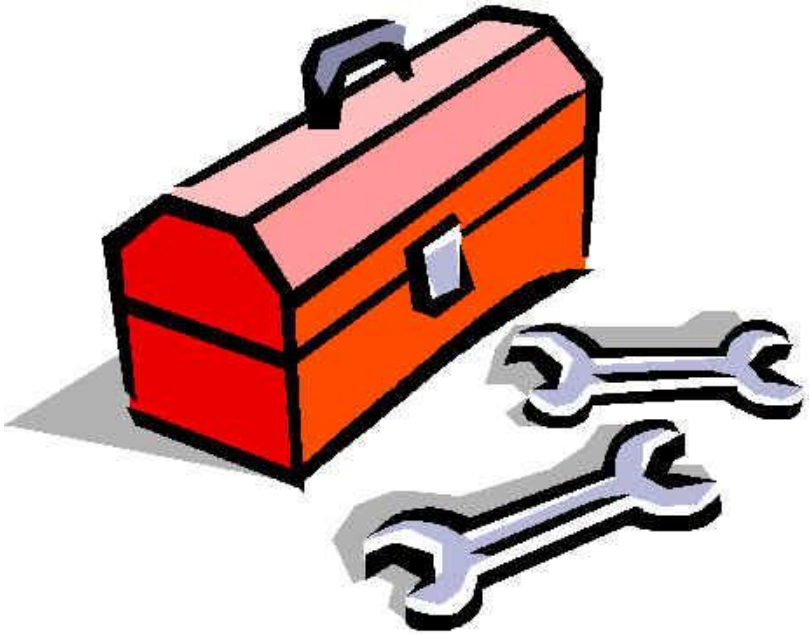
- RID would possibly
  - Perform more efficently than current methods
    - Reduce human dependance
    - Reduce security costs
    - Increase detection accuracy
  - Provide detection for multiple locations
    - Supervisory control and data acquisition (SCADA) systems
  - Alert of intrusion
  - Stop its occurrence
    - Decides solution

Objectives

- Understand and implement D400
- Modify program code by inserting detours
  - Small amounts of code
  - Intercepts function calls
- Gather precise execution time information
  - Study data
  - Establish clean machine baseline
- Infect machine with rootkit
- Gather data once more
  - Compare clean and infected machine data
  - Establish conclusions

Resources

- D400 Fedora Virtual Machine
- Oracle Virtualbox VM software
- Intel Pentium 4 HT processor



Process

- Literature search
  - Intrusion detection
  - Rootkits
  - D400
- All new material
- Increased for research
  - Familiarity
  - Proficiency

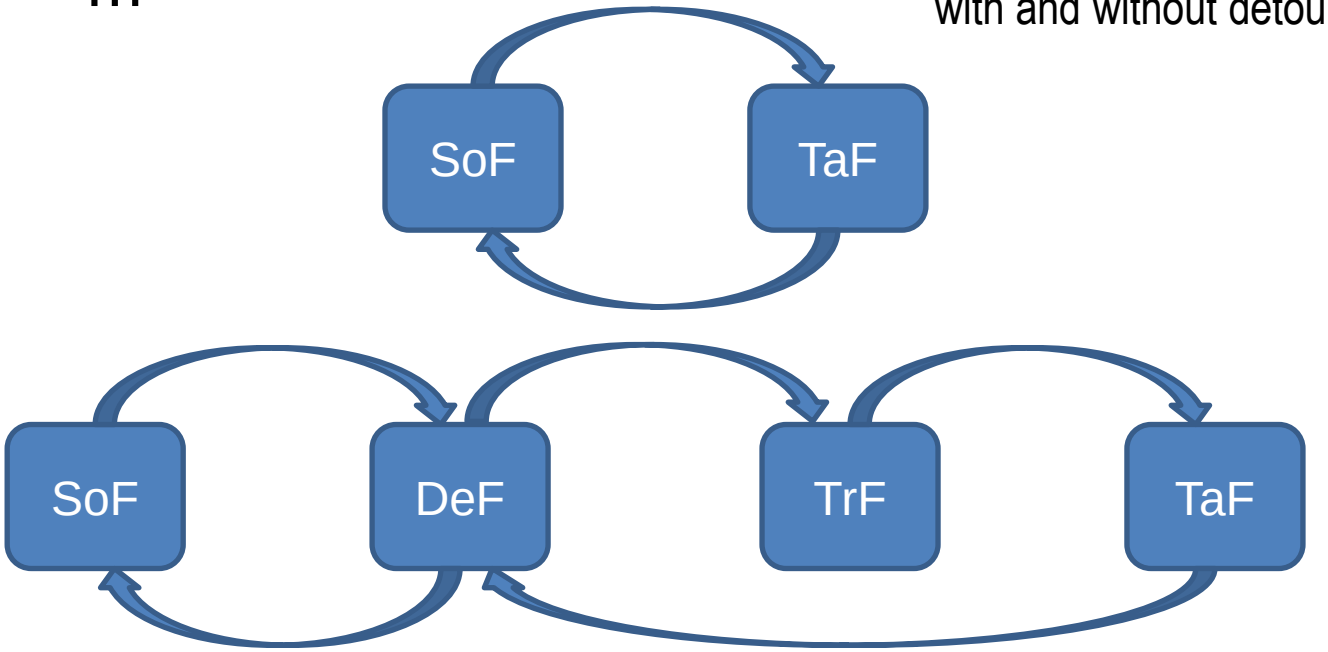
Process

- Install D400 Fedora Core 11 Virtual Machine
  - Run D400 build
  - Configure D400 virtual software
  - Observe D400 operation
- D400 build failed to work properly
  - Lengthy repair process
  - Implementation placed on hold
- Used local machine and Fedora VM instead

Process

- Modify program code for data collection
  - Observe trampolines and detours
    - Program interception
    - Collects and stores data
    - …

Figure 1. Function invocation with and without detours



Results

- Created execution time collection code
- Performed initial timing tests
- Identified Linux rootkits relavant to D400 device
- Identified system calls targeted most by Linux rootkits

```
Time: 0 secs 523 ns Clock ticks: 1251
Time: 0 secs 523 ns Clock ticks: 1251
Time: 0 secs 526 ns Clock ticks: 1260
Time: 0 secs 526 ns Clock ticks: 1260
Time: 0 secs 519 ns Clock ticks: 1242
Time: 0 secs 519 ns Clock ticks: 1242
Time: 0 secs 523 ns Clock ticks: 1251
Time: 0 secs 515 ns Clock ticks: 1242
```

Figure 2. Screenshot of time execution data

Conclusions and Future Work

- Successfully conducted initial timing tests on clean machine
- Baseline execution time can be established
- Gathered data can be used for later comparisons against compromised machines

- Continuing research needed
  - D400 VM implementation
  - Compromised machine testing
  - Real time testing
  - Real time implementation

Summary

- Securing cyber infrastructure very important
  - Rootkits used for stealth
  - Current IDS help
    - Not accurate enough though
    - Difficult implementation
- Remote intrusion detection could be solution
  - More accurate detection possible
  - More cost friendly
  - SCADA systems and D400
    - Better info collection
    - Better info filtration
    - Enhanced security features

Acknowledgements

The Research Alliance in Math and Science program is sponsored by the Office of Advanced Scientific Computing Research, U.S. Department of Energy. The work was performed at the Oak Ridge National Laboratory, which is managed by UT-Battelle, LLC under Contract No. De-AC05-00OR22725. This work has been authored by a contractor of the U.S. Government, accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

The author would like to thank Dr. Stacy Prowell for the opportunity to work on this project. The author would also like to thank Aaron Ferber for the tremendous amount of help he provided during this research. Additional acknowledgements go to Tim Schulz, Evan Frenn, and Jarilyn Hernandez for their help as well. Finally, special thanks are given to Debbie McCoy, who made provisions for this research experience and made this opportunity possible.

References

- Scarfone, K. , Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems.* National Institute of Standards and Technology.
- Rootkits. *OmniSecu.com.* Retrieved June 2012 from http://www.omnisecu.com/security/rootkits.htm
- General Energy. n.d. Multilin D400. *GEDigitalEnergy.* Retrieved June 2012 from http://www.gedigitalenergy.com/multilin/energy/catalog/D400.htm#new
- Hunt, G. , Brubacher, D. (1999). *Detours: Binary Interception of Win32 Functions.* Proceedings of the 3rd USENIX Windows NT Symposium.

Questions