BERKELEY LAB

NERSC

NATIONAL ENERGY RESEARCH
SCIENTIFIC COMPUTING CENTER

SC|05

Tutorial S09

Keeping Ahead of the Bad Guys: High Performance Computing Protection

Office of Science
U.S. DEPARTMENT OF ENERGY

Today's Activities

- Components of good protection
- Changing Computer Protection Environment
- Break
- Keeping One Step Ahead
- Real World Example
  - Protecting SCinet, SC2004 and SC|05
- Questions and Answers

Who We Are

William T.C. Kramer
Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
kramer@lbl.gov

Stephen Lau
Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
slau@lbl.gov

Scott Campbell
Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
scampbell@lbl.gov

Live Data

- Active security monitoring at SC|05
- Multiple intrusion detection systems monitoring SCinet
- More on this later…

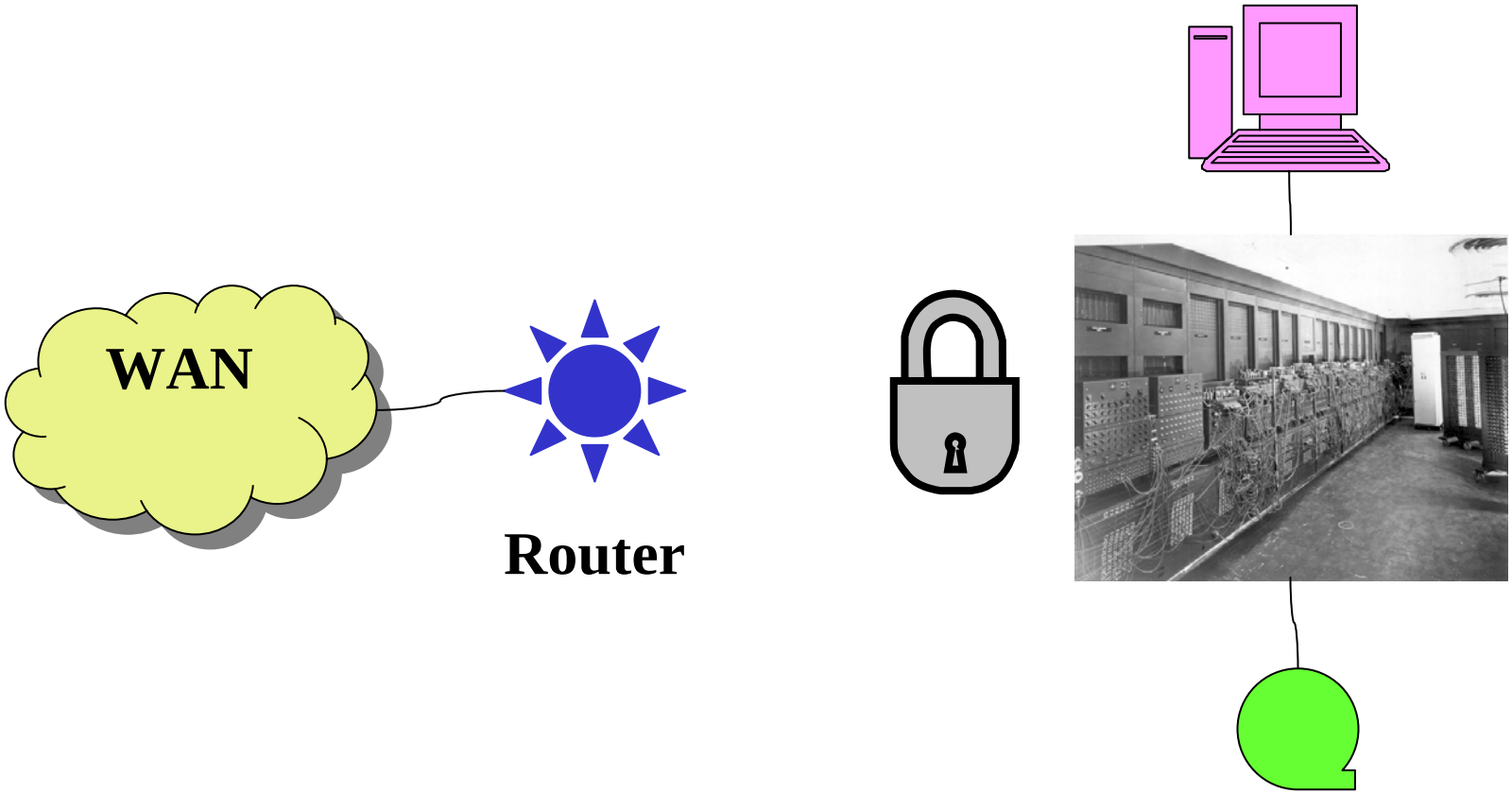
Components of Good Protection

William T.C. Kramer
Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
kramer@lbl.gov

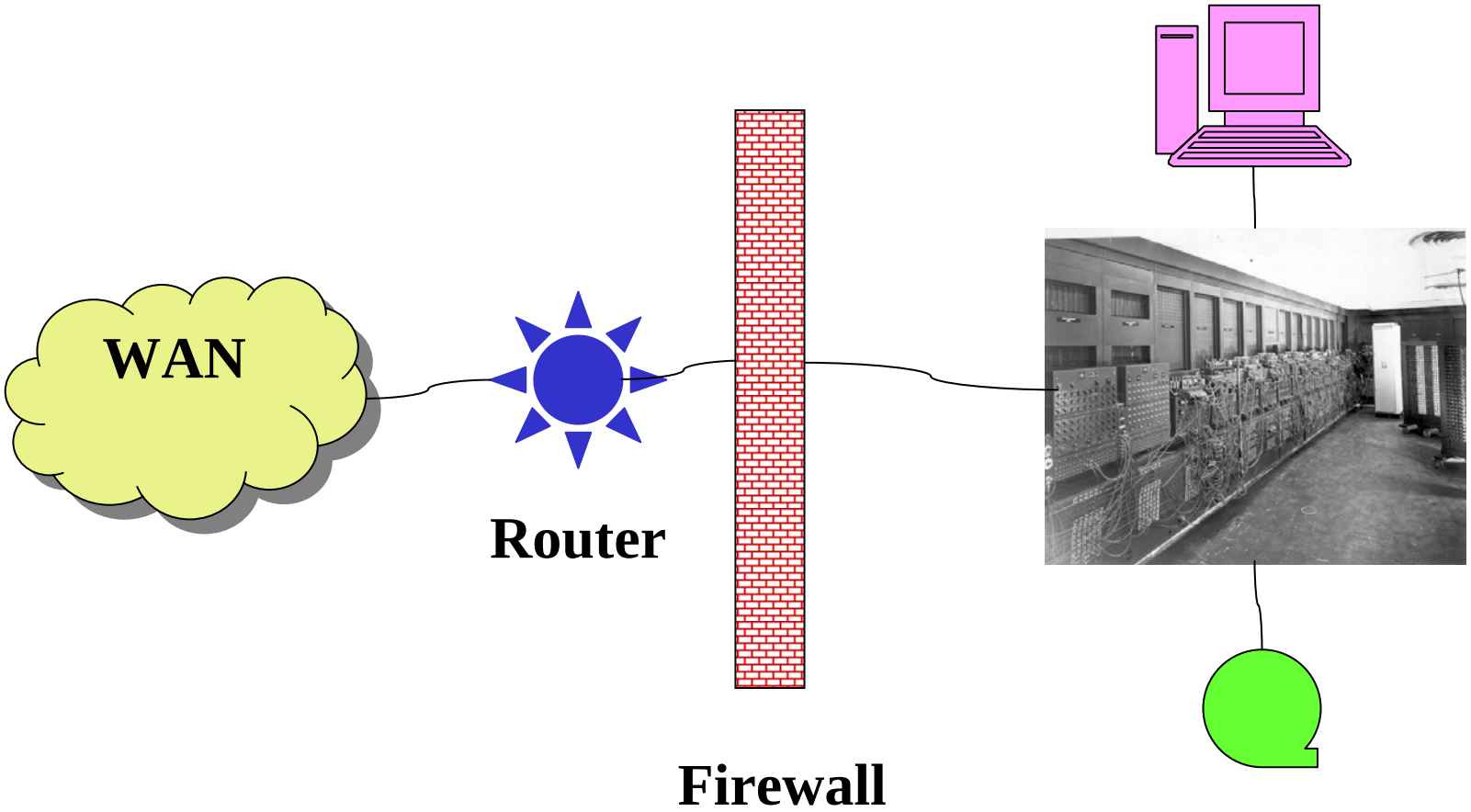
Outline

- Components of good protection
  - Defining terms
  - Goals and objectives for an open site
  - Security implications of an HPC environment
  - Policy and Procedures
  - Good systems protection
  - Response teams
  - Other “best practices”

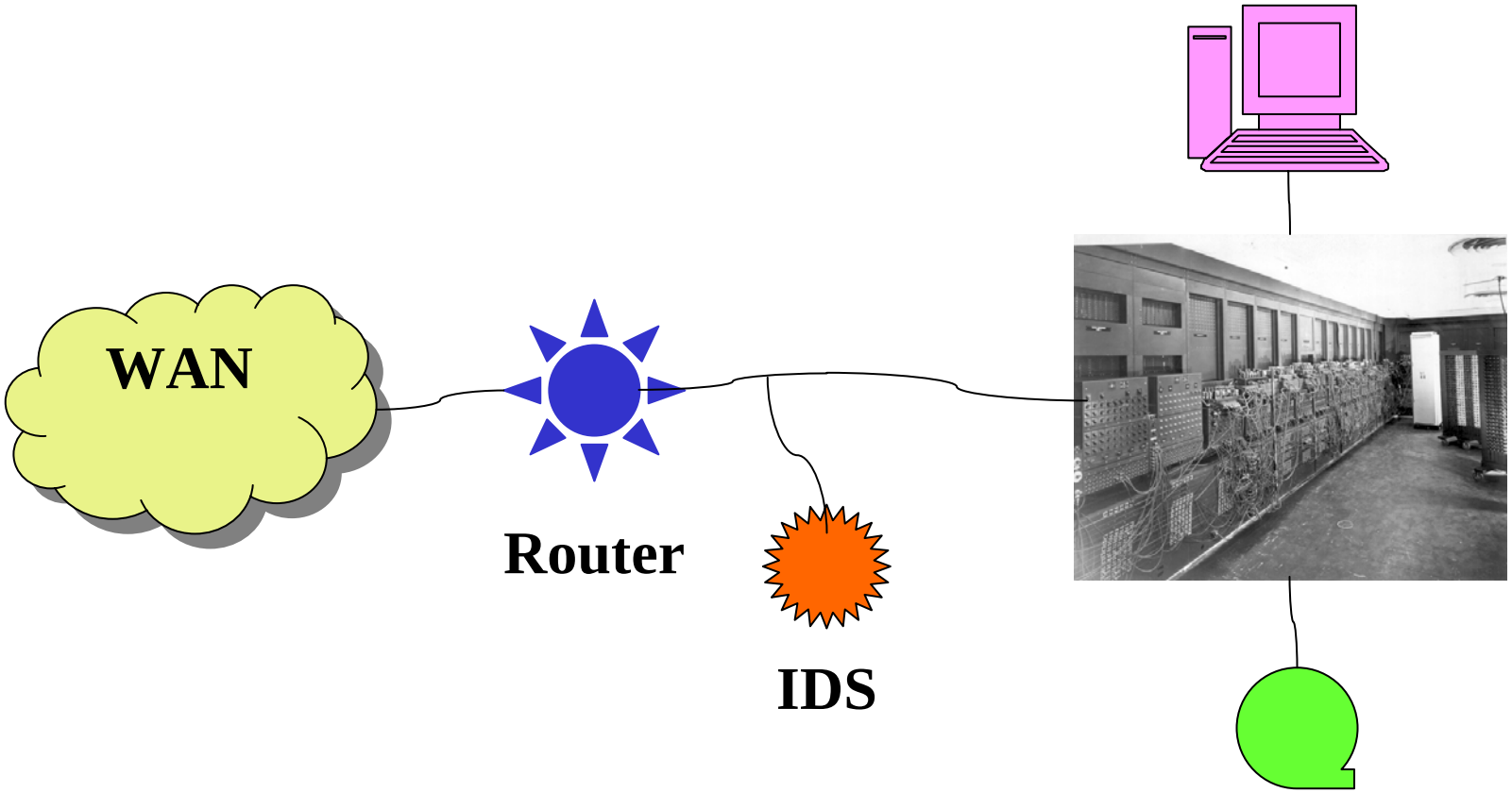
Classified/Isolated



Industrial / Enterprise



Open



Open Science Environment

- Unlike enterprise institutions
  - Enterprise oriented computer security techniques fail
- Varied and atypical computational infrastructure
- High bandwidth / performance applications
  - Unique applications with unique requirements and traffic patterns
- Varied and distributed resources
- Multi-institutional collaborations across all levels
  - e.g. LBNL has approximately 4000 collaborations/year

Characteristic Environment

- Varied Systems
  - Workstations
    - Laptops, PDAs, workstations, cell phones, etc…
    - Windows, Unix, Linux, OSX, etc...
  - Servers
    - Web servers, mail, LDAP, etc.
  - High Performance Platforms
    - High End Cluster systems
    - Mass storage systems
    - Dedicated Systems
      - i.e. Visualization, Mathematical

- Network
  - High speed network connections (possibly multiple)
    - e.g. 10G at NERSC
  - Wireless
  - Modem pools

Characteristic Environment

- Additional systems
  - Printers
  - Fax machines
  - Infrastructure / Embedded systems
    - Door access control, environmental controls
    - Don’t forget about these!

- Users
  - Diverse user community scattered around the globe
    - Mix of science, industry, academic
  - Multiple large scale, multi-site collaborations

- Staff
  - Spread out between multiple locations
  - Highly mobile
  - Want access from home systems

Network Traffic Patterns

- Open scientific facilities traffic patterns differ from industrial/enterprise
- Typical enterprise traffic
  - Web, email, dedicated/known services
- Typical open facility
  - Varies over time
  - Unique protocols
  - Large volumes of traffic

Example of Network Traffic

Type of Traffic	Number of Connections	Overall Percentage of Traffic
Bulk Data Transfer	666,529	83.73%
Grid Services	74,178	7.19%
Web Related	288,3754	5.30%
Database	620,1730	.27%
Mail	200,484	.04%
System Services	185,272	.04%
Interactive	116	<.1%
Total	10,212,063	96.57%

Policy and Procedures

- Cyber Protection Policy controls computer access and usage
  - How information and processing power can be accessed, manipulated and shared
  - Represents external laws and regulations, organizational mission, goals and business practices
  - Mandatory and Discretionary policies and rules
- Policy should be broad and change infrequently
  - Guided by the site mission and philosophy
  - Policy change typically involves a formalized change and review process
- Business practices should define details of policy implementation
  - Specific as needed and change as needed
  - Changes are technical, not bureaucratic
  - Should not implement its own policy
  - If business practice violates policy, then it is time to change one or the other explicitly

Policy and Procedures (cont)

- Mandatory – Enforce access control rules that constrains access to information and/or resources based on authorization
  - i.e.To root or not to root, that is the question

- Discretionary – An individual may specify the types of access others may have
  - i.e. File permissions

Defense in Depth

- Use of multiple tools and techniques leverages off strengths and weaknesses
  - Multiple sensors to detect and prevent intrusions
  - No single points of failure
- No single tool or technique guarantees a problem free environment
- Protects against the “hard outer shell, soft inside” vulnerability
  - Caveat: More resource intensive to implement and maintain, integration difficulties

Defense in Depth Layers

- External Perimeter Defense
  - All points of entry into the network, the “DMZ”
- Internal Network Protection
- Host Level Protection
- User / Staff Protection
  - Education
- Physical Security

External Perimeter Defense

- Determine all perimeters
  - Wireless, modems
- Intrusion Detection System
  - i.e. Bro, Snort
- Host shunning
  - Tied into perimeter defense to react to attacks
- Router filtering
  - Block archaic or unused services
    - i.e. echo, chargen
- Email Virus Filtering
  - Filters all inbound / outbound email

Internal Network Protection

- **Firewalls where appropriate**
  - Non-high performance platforms
  - Dedicated platforms
  - Developmental/Experimental systems
- **Subnet traffic filtering**
  - Further restrict traffic based on subnets
- **Network Segregation / Isolation**
  - Isolate “like” systems together
  - i.e. staff workstations shouldn’t be on same network as HPC systems

Host Level Protection

- Disable unused services upon install
- Anti-virus software
  - Available to all staff, installed by default
- Host Scanning / Vulnerability Eradication
  - Avoid “information overload”
  - Nmap, nessus
- Disable clear text passwords
- Disallow unauthenticated access
- Enable process accounting / logging
  - Provides audit trail

Defense in Depth Layers

- User / Staff Protection
  - Increase staff awareness of computer protection issues
    - Periodic in-house training for staff
    - Periodic Web/Video based training for offsite users
  - All staff / users must annually sign “Usage Agreement”
  - Periodic emails reminding staff / users about key security issues

- Physical Security
  - Restrict physical access to critical systems
  - Educate staff members
  - Provide lockdowns for staff member laptops and systems

Most Common Security Incidents

- **Sniffed passwords**
  - Someone gets a hold of a user password
  - Externally compromised system
  - Exposure via unencrypted means
- **Unpatched systems**
  - New systems (not yet patched)
  - Toolkits used to exploit known vulnerabilities
  - Visitors and staff unknowingly bring in vulnerable or pre-hacked systems
- **Viruses and Worms**
  - Home systems infected, dial in
  - Visitors bring in infected systems
  - Staff members bring systems to conferences, etc.

Good Systems Protection

- Good, clear, consistent policy
- Good business practices that are consistent with policy
- A hierarchy of protection tools and mechanisms from the border to the internals of the system
- Organized ways of discussing and addressing protection issues

Update, Update, Update

- The vast majority of compromises are know exploits for which the known corrections have been available for some time.

- Solution is keeping the systems up to date
  - Patches, New OS releases, etc.
  - For all components
  - More important with open source

- Many reasons not to
  - Staff Effort, User resistance, testing, worry about introducing bugs…

It is the single most important component of system protection

Proving Good Protection is hard

Need to have positive metrics not just negative ones

- **Examples of positive metrics**
  - **Successful accomplishment of the organization's mission**
  - **Number of proactively detected incidents**
    - **You found them first**
  - **Number of sites informed of a problem**
  - **Dollar cost of damage AVOIDED due to protection efforts**
  - **Number scans performed (without finding things)**
  - **Days since last incident**
  - **Training events**
  - **External interactions**
    - **If your peers think you are good then you probably are**

Good Systems Protection (cont)

- Examples of negative metrics
  - Number of reactively detected incidents – "breakins"
    - Someone else found them first and told you
  - Amount of lost time due to incidents
  - Number of restricted services
  - PR of such things

Most organizations typically judge negative more than positive

Configuration Control

- Providing Open Access does not mean loss of control
  - Example
    - IBM SP was delivered with 65,536 open ports
    - After a lot of investigation, it was determined 31 were needed for the system to run
  - Can use limited ranges for services.
    - A set of 1,000 ports provided for Grid Services
    - A specific set of ports for FTP
- Account Management
  - Including regular disabling and removal

Keys and Certification

- Keys
  - Passwords, PKI, One Time Passwords, SSH
- Make it possible for users to store key information at your site
  - Rather then storing it on their local system.
  - User systems are typically vulnerable and not well protected
    - More easily compromised
  - E.g Myproxy
- You can protect the information better than they can

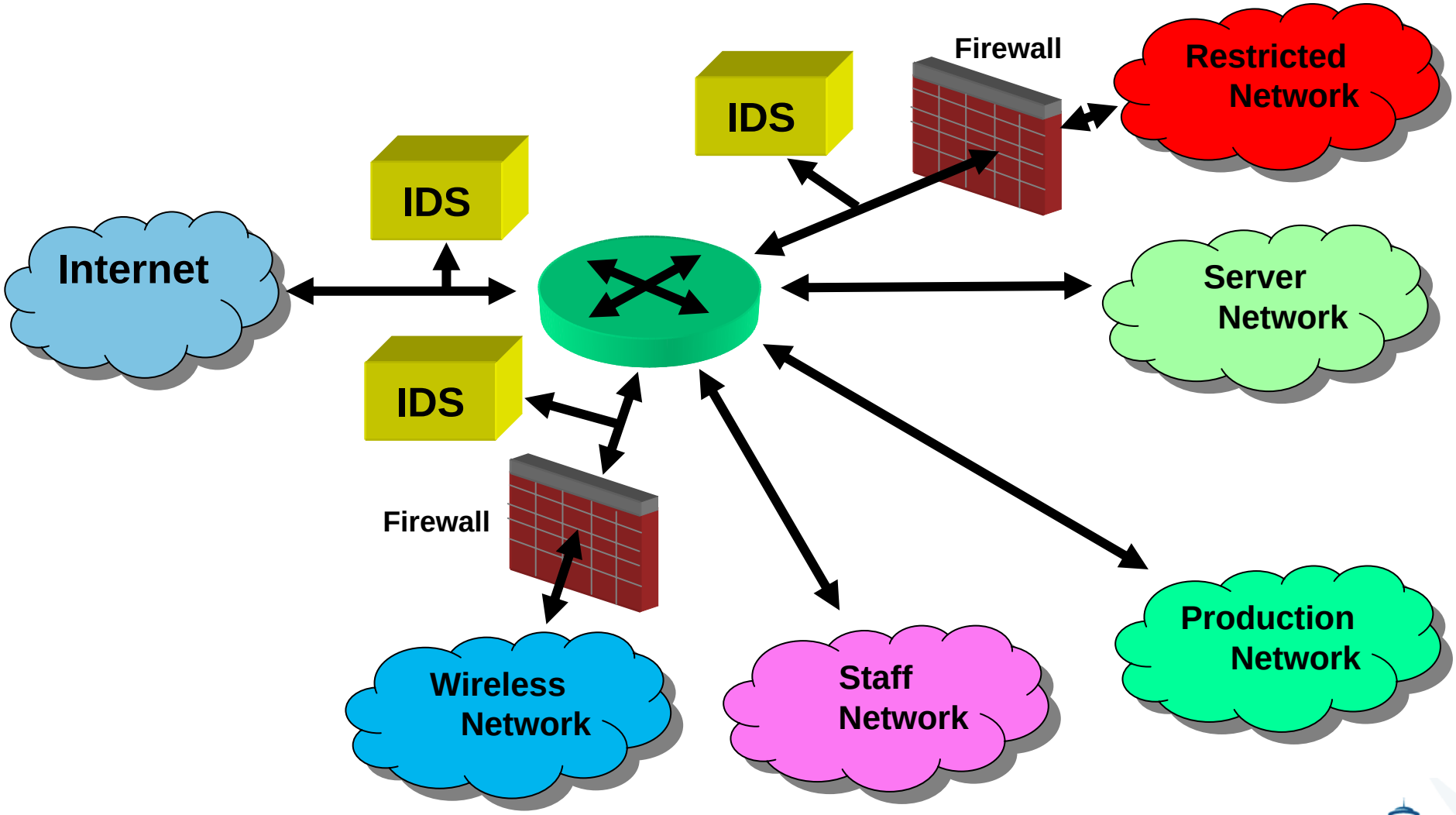
Network Segmentation

- Segment network by service and function
- Investing in different networks for different functions is worthwhile

- Public and Private Networks
  - Clusters should be built out of private networks
  - There should be a few, well defined and configured access points in the cluster for public networks
  - But never assume your private network is really private

- User and Administrative networks

Sample Network



Logging, Monitoring, Scanning

- **Logging is extremely important**
  - Good Practice
  - Forensics
  - Allows analysis for capacity and workload
- **Monitoring**
  - Does not help to log everything if it is not looked at until it is too late
  - Examples – job flow, network attempts, logins, etc.
- **Scanning**
  - Helps assure configuration management
  - Prevents mistakes that lead to vulnerabilities

Logging and Monitoring

- Need to log all activities
  - Process accounting
  - Batch system processing
  - Logins
  - Network connections
  - Violation logging
- Transfer logs to another system on a regular and timely basis
  - Protects against modifications
  - Backup
  - Post Processing

Enlist the users

- Protection has to facilitate the user doing their work – not inhibit it
- Make users aware and responsible
  - Proactively acknowledge a clear appropriate use policy
  - Delegate responsibility to users for certain things they actually can control
    - Some things they have to do such as deciding what data is sensitive
  - Include users into the evolutionary process of protection changes
- Does not work if protection is always getting in the way of the users
  - They will go around to get their work done

Enlist the users

- **Have them report "suspicious activity"**
  - **Strange files or directories**
  - **Unusual login times**
  - **Unverified phone call from "NERSC" asking for passwords or account information**
- **Have them report external incidents**
  - **Please report any incidents at sites that you use to access NERSC**
- **Report incidents where they suspect credentials are sniffed or stolen**

Our users have been critical to identifying and resolving many incidents!

Staff and Organization

- Excellent people with enough time to spend on protection
- Integrate security staff with system and network management groups
  - At NERSC, network and security groups are integrated into one group.
- Integrate security practices into all staff functions
- Integrated security team in addition to dedicated security staff
  - Channels communications to various groups
  - Acts are a response team
  - Ensures representation and buy in for policy development
  - Serves as a broad technical resource

Avoid "us" vs. "them" mentality

Summary

- A site needs good, and consistent policy and business practices
- A hierarchy of protection tools and mechanisms from the border to the internals of the system
- Update always
- Keys, passwords and certs should not be stored on user systems
- Well defined network architectures
- Logging and monitoring of systems is key

Changing Computer Protection Environment

Stephen Lau
Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
slau@lbl.gov

Overview

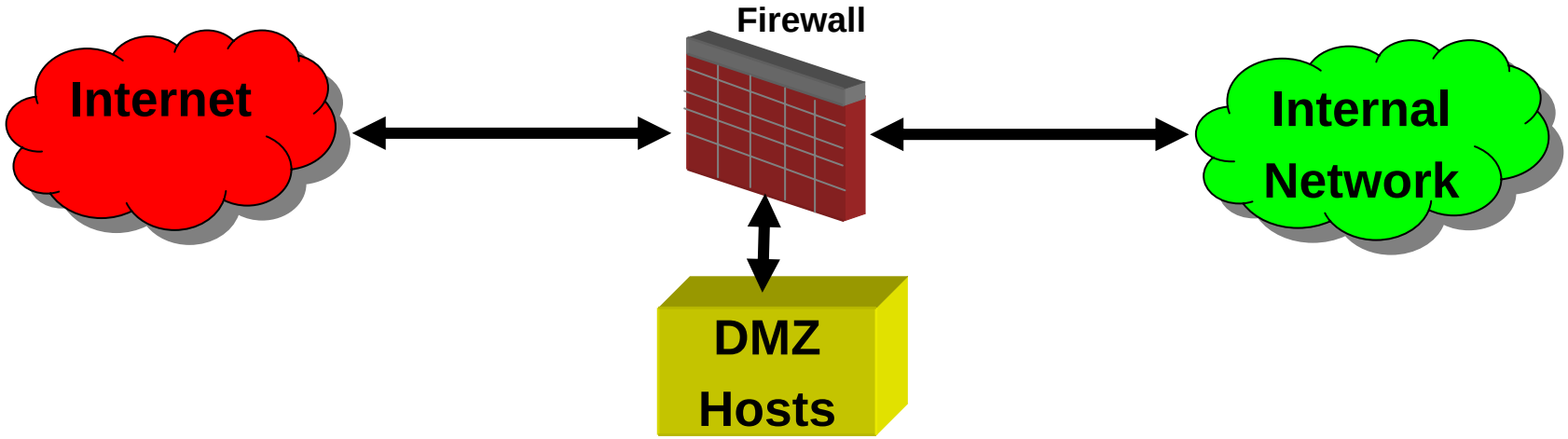
- Changing security environment
- Why existing protection techniques are failing
- Multi-site attack implications
- Users as the vector
- Rootkits

Changing Security Environment

- Recent attacks on HPC and educational institutes reinforces the concept of evolving security threats.
  - Countermeasures need to evolve to keep pace.
- Systems are becoming more complex
  - Cluster based systems
  - Grid
- Increase in interdependencies
  - Cross site accounts, access
- Access methods changing
  - More mobility
  - Different types of platforms

Classic Security Model

- Service offered at DMZ
- Internal network is protected via firewall or other perimeter protection



Classic Security Model

- Addresses *some* well defined problems
  - Widely deployed
- Based on key assumption:
  - Threat model is fairly static
- But:
  - Attackers have adapted their attacks to counter this model

Attackers are Adapting

- Evolving security threat model

- Nature of the opponent is changing
  - Becoming difficult to determine users from attackers
  - Users have become a vector
    - Clicking on email attachments
    - ‘Phishing’ attacks

  - Attackers have become persistent
    - Target specific users / systems repeatedly
    - Wait for vulnerability to appear

    - Attackers look and behave like users

Stolen Credentials

- One time passwords are *supposed* to minimize this problem
  - #1 is legitimate, #2 is an attacker

```
Mar 10 18:39:41 2.3.4.5 Message forwarded from host609: sshd[74334]: Accepted
   password for user1 from 1.2.3.XXX port 45674 ssh2
Mar 11 11:00:50 2.3.4.6 Message forwarded from host013: sshd[117314]:
   Accepted password for user1 from 1.2.3.XXX port 46570 ssh2
```

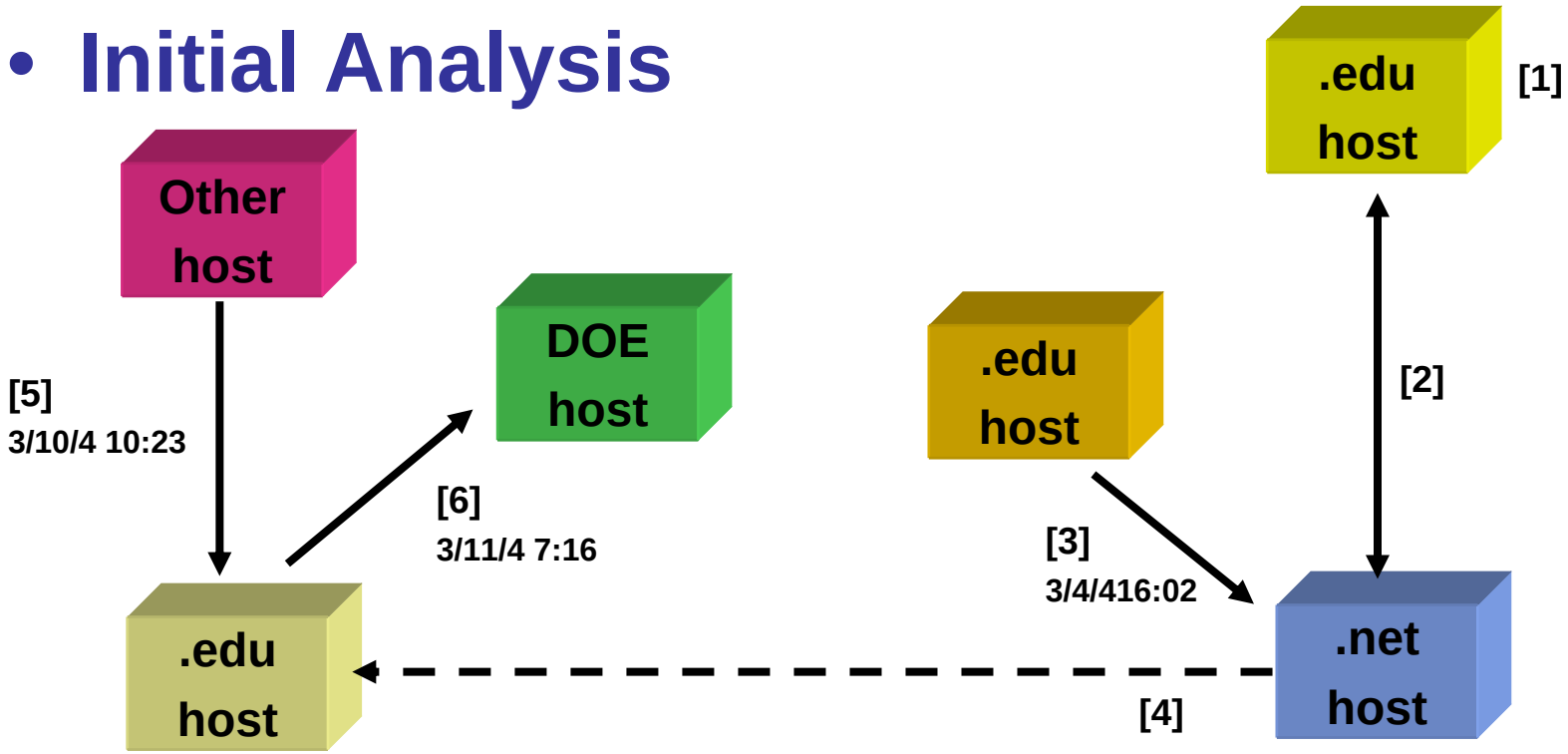
- Difficult to distinguish between the authorized and unauthorized
- Network filtering/analysis has limited affect
- Widely used in recent attacks.

Cross Site Issues

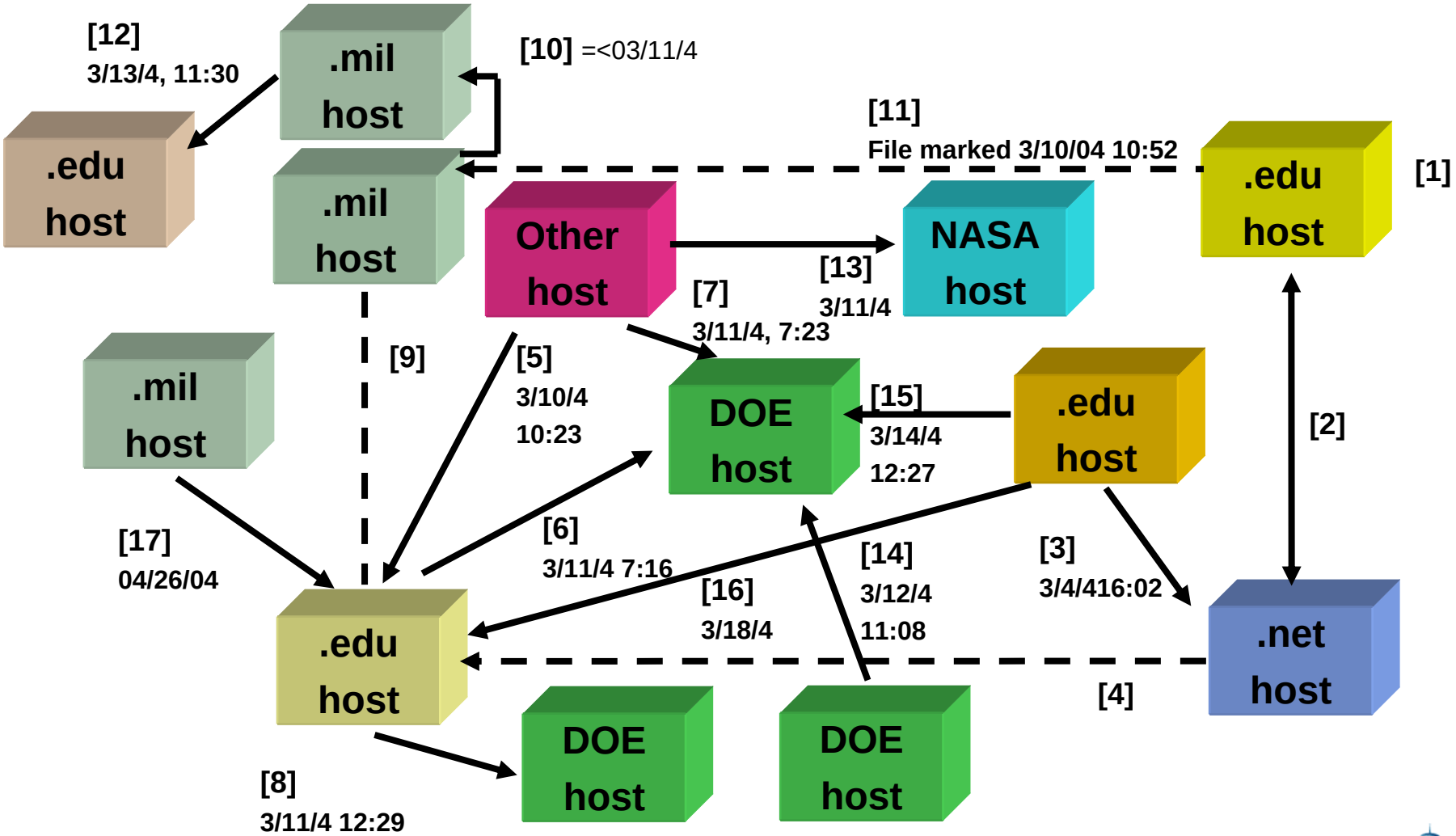
- Users at open HPC centers and educational and research institutes depend upon collaboration.
- Most often have access to multiple systems at multiple sites.
  - Many of these outside of a site's control
- "Single site" incidents can quickly blossom into complex multi-site incidents.

Real World Example

- Incident from 2004
- Crossed many sites
- Initial Analysis



Real World Part II

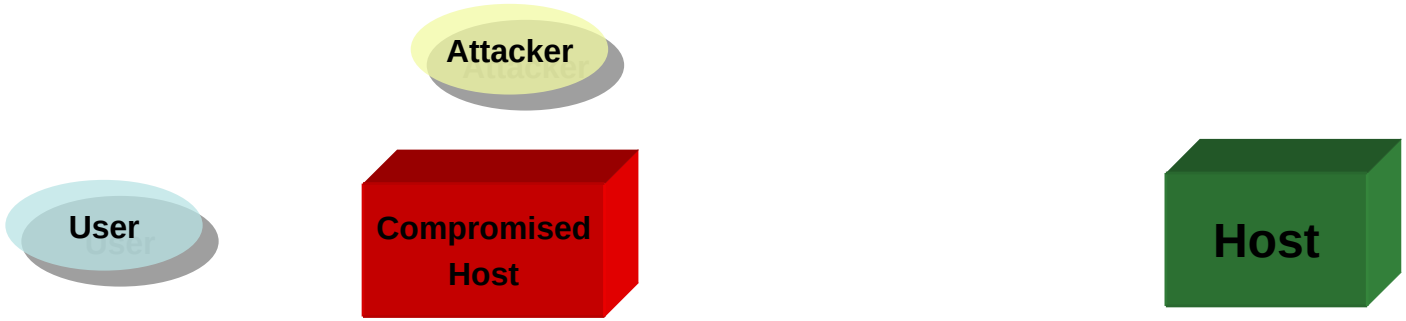


Real World Part III

- Even more hosts were involved.
  - Too many to show on a single slide!
- Attackers were persistent.
  - Kept trying same accounts / systems
- We only saw one part of the puzzle
  - Many more that we don't know about
  - May never know extent of infiltration

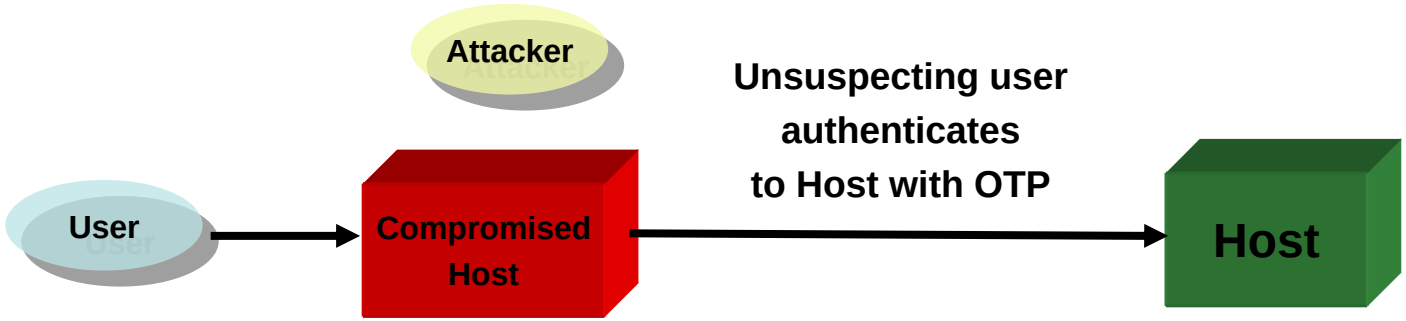
Credential Theft and One Time Passwords

- OTP solutions address traditional problem of credential theft
  - Sniffed passwords / Readable SSH Key
- Attackers are adapting
  - No longer stealing and reusing credentials
- Accessing authenticated user sessions as a *service*
- Attacker rides in on user authenticated session
  - Session hijacking



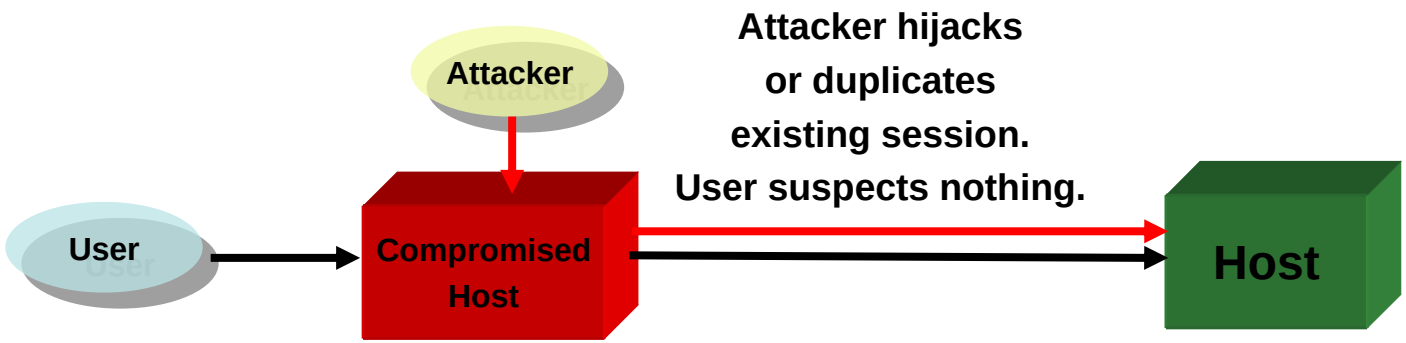
Credential Theft and One Time Passwords

- OTP solutions address traditional problem of credential theft
  - Sniffed passwords / Readable SSH Key
- Attackers are adapting
  - No longer stealing and reusing credentials
- Accessing authenticated user sessions as a *service*
- Attacker rides in on user authenticated session
  - Session hijacking



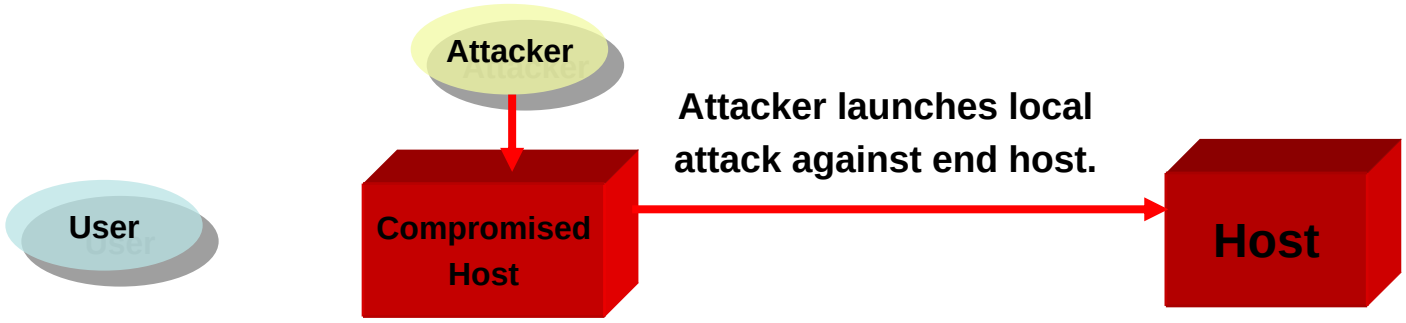
Credential Theft and One Time Passwords

- OTP solutions address traditional problem of credential theft
  - Sniffed passwords / Readable SSH Key
- Attackers are adapting
  - No longer stealing and reusing credentials
- Accessing authenticated user sessions as a *service*
- Attacker rides in on user authenticated session
  - Session hijacking



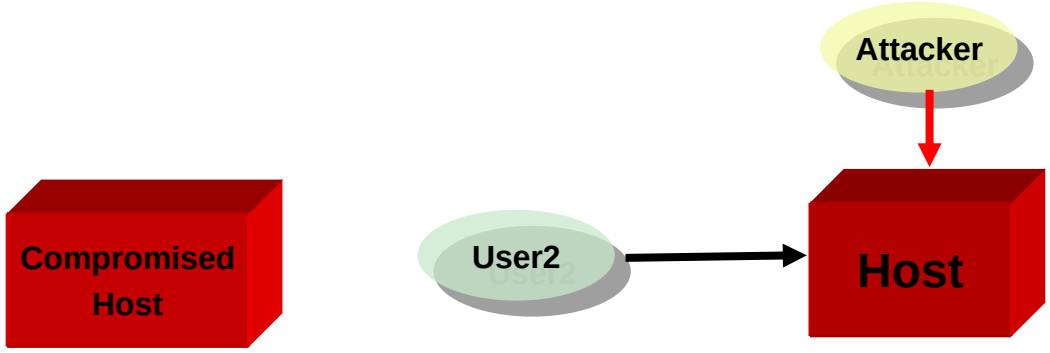
Credential Theft and One Time Passwords

- OTP solutions address traditional problem of credential theft
  - Sniffed passwords / Readable SSH Key
- Attackers are adapting
  - No longer stealing and reusing credentials
- Accessing authenticated user sessions as a *service*
- Attacker rides in on user authenticated session
  - Session hijacking



Credential Theft and One Time Passwords

- OTP solutions address traditional problem of credential theft
  - Sniffed passwords / Readable SSH Key
- Attackers are adapting
  - No longer stealing and reusing credentials
- Accessing authenticated user sessions as a *service*
- Attacker rides in on user authenticated session
  - Session hijacking



Lather, rinse, repeat.

Credential Theft and One Time Passwords

- OTP address a well defined problem.
- Problem:
  - Attackers are quickly creating new class of attacks that are harder to deal with!
- Once again, no magic solutions!

Kernel Rootkits

- Ability to control a system without administrator being aware
- Defeats most local monitoring systems
  - You can not trust your operating system
- Many perform process hiding
  - Example from SK Rootkit:

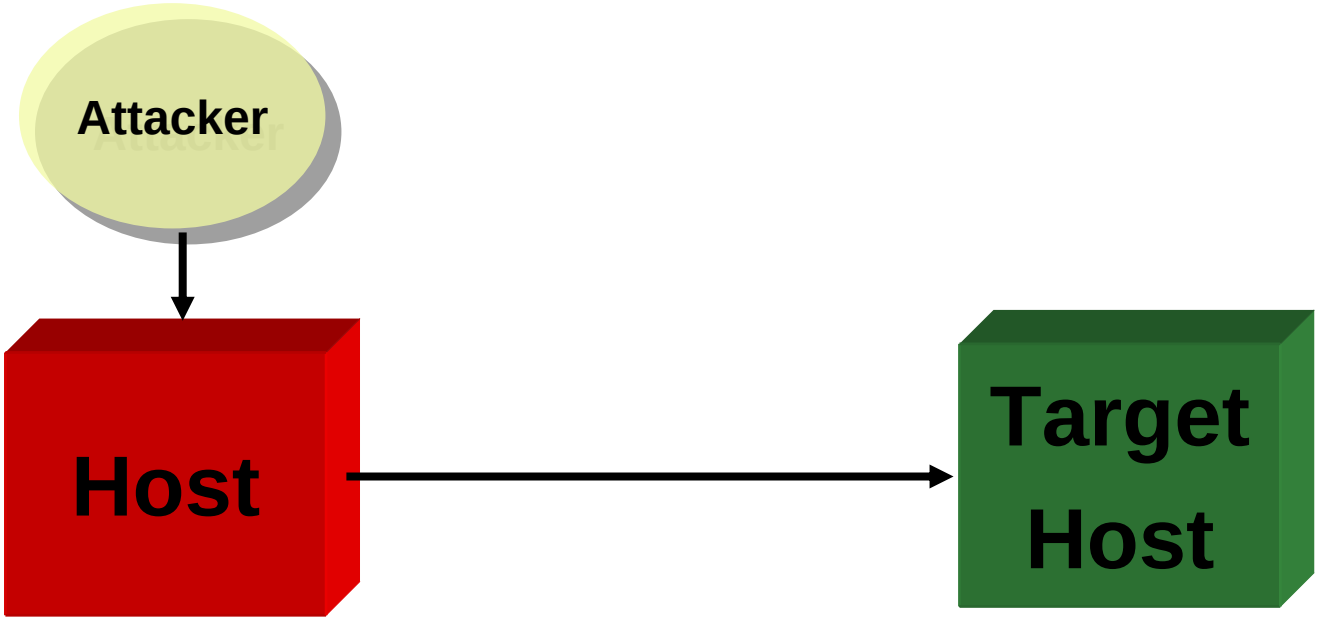
```
bash-2.05$ ps -aux | grep vi
user1 13779 1.6 0.0 5140 2336 pts/2 S 16:54 0:00 vim x
user1 13781 0.0 0.0 1736 576 pts/3 S 16:54 0:00 grep vi

bash-2.05$ ./sk i 13779
/dev/null
Detected version: 1.3b
Pid 13779 is hidden now!

bash-2.05$ ps -aux | grep vi
user1 13785 0.0 0.0 1736 580 pts/3 S 16:54 0:00 grep vi

bash-2.05$
```

Kernel Rootkits

- **Some rootkits enable remote access**
- **Example:**
  - **Rootkit can listen on port 22 for specifically crafted packet to arrive.**
  - **When it arrives, rootkit establishes outbound connection back to host with root shell.**

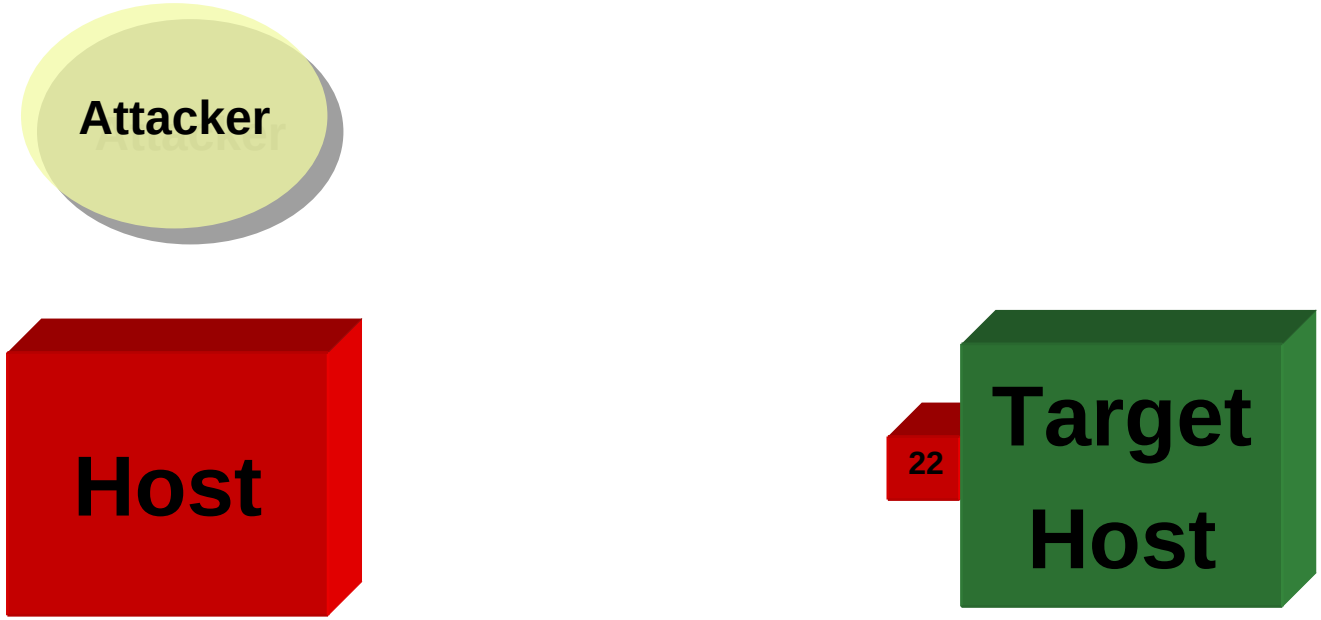
```
bash-2.05$ ./login -h localhost -d 22
/dev/null
Listening to port 32774
password:
Trying 127.0.0.1:22...
Trying...Et voila
Server connected. Escape character is '^K'
/dev/null
[root@owned .sk12]#
```

Kernel Rootkits Example



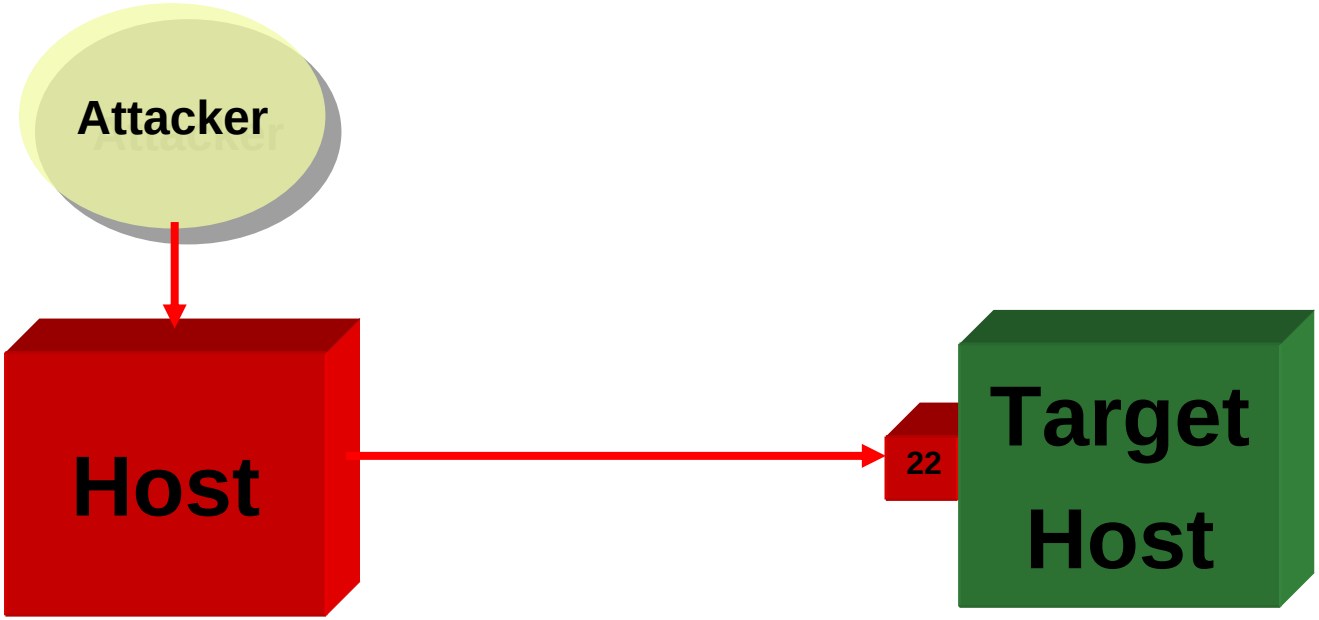
Attacker installs rootkit on Target Host

Kernel Rootkits Example



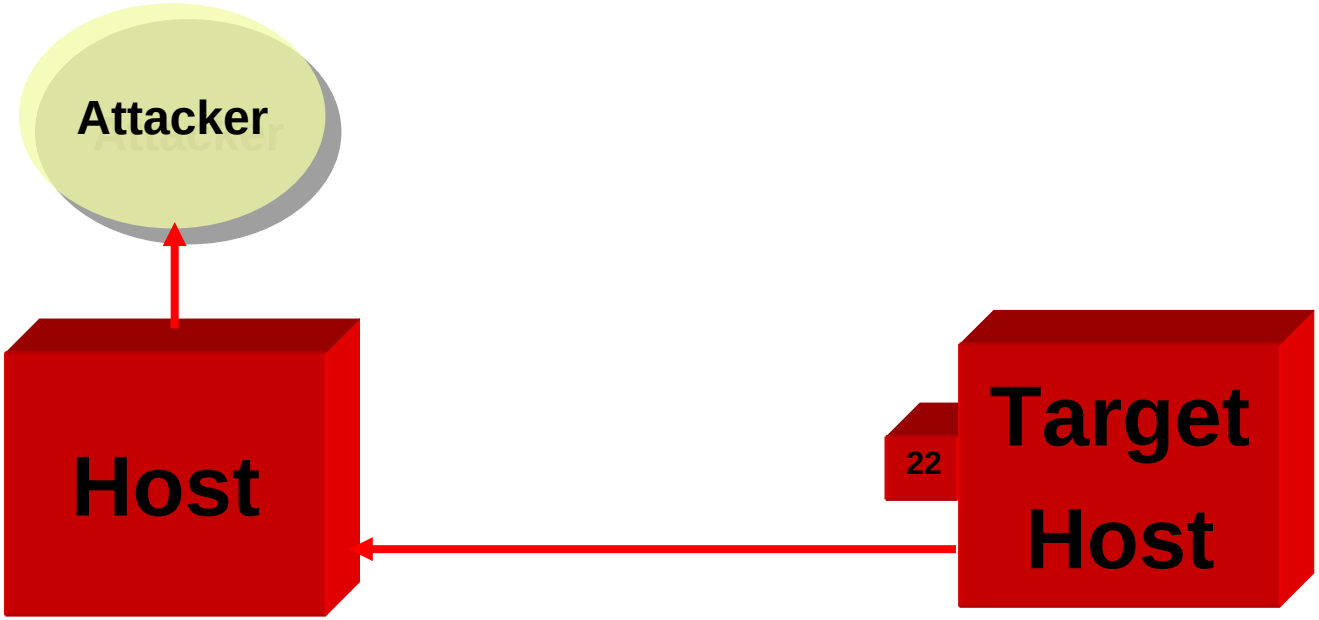
Target Host now looking for crafted packet to arrive on port 22

Kernel Rootkits Example



Attacker sends crafted packet to Target Host on port 22.
From Target host's point of view looks legitimate.

Kernel Rootkits Example



Target Host connects back with a root shell on a different port. Target host is now compromised.

Kernel Rootkits

- Widely used by attackers
  - Great way to credential mine or attack user sessions!

- Not enough time to go into detail.
  - Exercise left to viewer to explore in more detail.
  - http://www.phrack.org/phrack/50/P50-05
  - http://www.phrack.org/phrack/51/P51-05

What To Do

- Expect attackers to quickly devise ways around any “solution”
- Expect that some of your systems / accounts are **already compromised***
  - How does one detect them and how do you minimize the damage?
- Security posture needs to be flexible
  - Attackers are constantly changing, we need to be too.
- Network monitoring / perimeter defense not enough
- Need to combine network data with host level data
  - Get the “whole” picture
- Grow relationships with other sites
  - Cross site incidents are becoming quickly commonplace
  - Other sites’ compromise affect you!
- See next section for more “what to do’s”

Summary

- Attackers quickly adapt to any “solution”.
- Becoming harder to distinguish between legitimate users and attackers.
- Network protection no longer enough!
  - Need to consider entire process from external host all the way to local host.
- Need to approach problem with the knowledge that some of your systems / accounts are and will always be compromised.

Keeping One Step Ahead

Responding to the Changing Threat Environment

Scott Campbell

Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
scampbell@lbl.gov

Introduction

General Topics:

- Soothing Platitudes
- Expanding the Sources of Security Data
- Credential Theft
- Large Scale Data Analysis

SOOTHING PLATITUDES

- General ideas to keep in mind while framing the topics we are looking at.
- They may get less soothing as we go along…

Soothing Platitudes #1

Do not make assumptions about what your network looks like.

Measure It

- **Noise and Radiation**
- **Complexity**
- **Usefulness of Familiarity**

Soothing Platitudes #2

You live in a *security ecosystem*, and improvements you make will force the hacking community to become more dangerous.

Enhancements to the security stance and:

- **Unexpected Consequences**
- **New Attacks (Classic: Jumping Higher)**
- **New Attacks (Weird: Learning to Fly)**

Soothing Platitudes #3

Your systems will fail. Do not be surprised!

- **See Soothing Platitude #2**
- **Design with this in mind**
- **Ideological Stance, nothing personal**

Expanding Sources of Security Data

Why Implement?

- Tunneling one protocol over another
- Attacks from inside
- Missing the host side interpretation

Limitations of Watching the Border

Tunneling Data Over Common Protocols

- Hard to identify
- Harder to understand
- Can be encrypted

Examples vary from simple to complex:
Moving chat data over web traffic to a DNS Shell that uses legitimate DNS request/responses.

Limitations of Watching the Border

- **Attacks From Inside**
  - Watching the border will completely miss this
- **Missing the Host Interpretation**
  - No idea what the host thinks it is seeing
  - No idea what applications think they are seeing (ex: SSL and web servers)

Proposed Solution: Syslog

Advantages

- Ubiquitous
- Well Understood
- Simple to Configure

Disadvantages

- UDP Based
- Free Form Data
- Insecure
- Analysis Complex in Large Data Volumes
- Performance Issues

Proposed Solution: SyslogNG

Advantages

- Ubiquitous
- Well Understood
- Simple to Configure?

Disadvantages

- Free Form Data
- Analysis Complex in Large Data Volumes

Data Analysis: The Real Problem

Flexibility of syslog solutions is also its weakness

- Unparseable data == Noise
- No general solution to this problem

Many people working on solution…

Data Analysis Continuum

Look at a few Well Defined Quantities

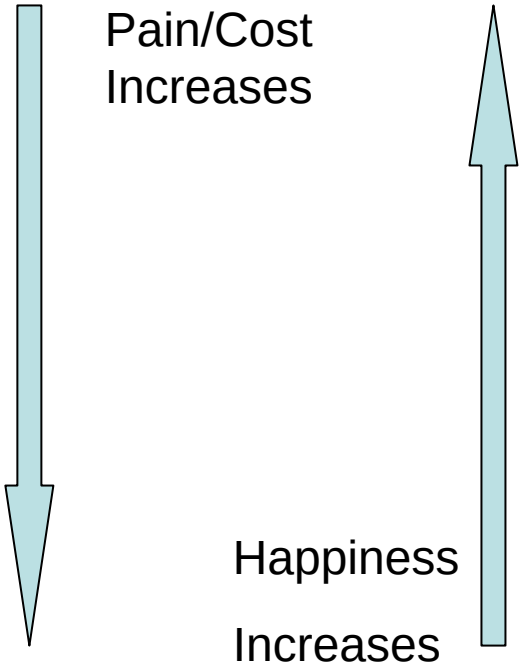
↕

Look at All and Extract Known Quantities

↕

Look at All and Make a General Parser

More Data Analysis



Homogeneous Env:
Same Operating System,
Same Type and Version of
Network Equip etc

Semi-Homogeneous Env:
Well behaved logging behavior,
but significant uniform logging.
Limited interest in data.

Heterogeneous Env:
Many platforms, you want all
available data.

What We Have Done

Given Diverse Selection of Hosts (OS etc):

- **Logins**
- **SU Success and Failures**
- **Firewall Activity**
- **Grid related activity**

Tied into Bro IDS System: More Shortly!

Credential Theft

General Problem: As long as some sort of authentication mechanism has been used, someone has wanted to *steal* it.

Passwords

Generally despised by users and security people alike…

Problems:

- **Theft: easy to steal, trojan/spyware etc**
- **Reuse: ssh/telnet/ftp/http/imap/IM**
- **Steal once, use often!**

The Big 3

- Something you know (password)
- Something you have (key or token)
- Something you are (biometric)

Growth in 2 (or even 3) factor authentication

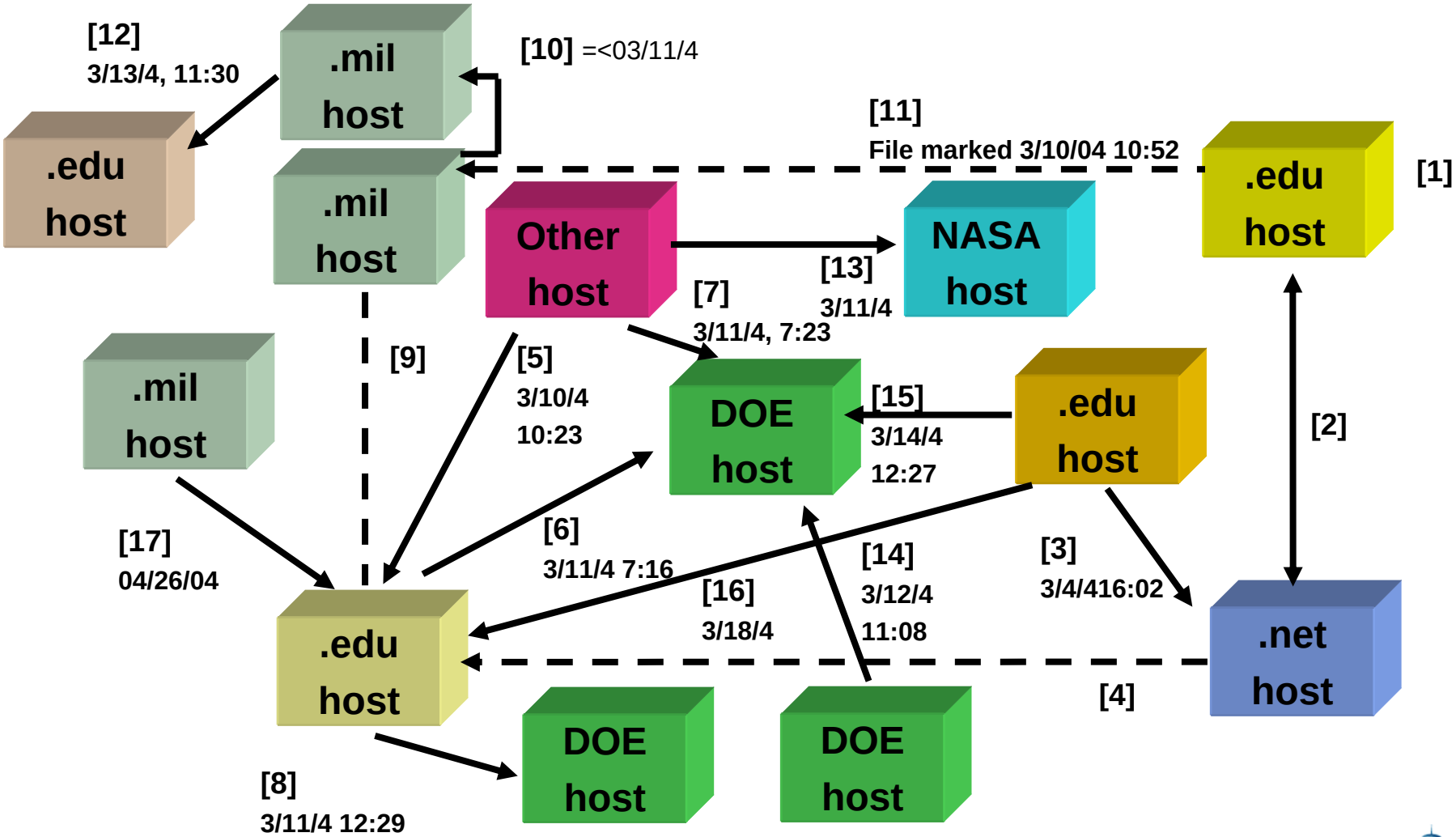
Problem: Theft

- Difficult to distinguish between the authorized and unauthorized
  - #1 is legitimate, #2 is an attacker:

```
Mar 10 18:39:41 2.3.4.5 Message forwarded from host609:
   sshd[74334]: Accepted password for user1 from 1.2.3.XXX port
   45674 ssh2

Mar 11 11:00:50 2.3.4.6 Message forwarded from host013:
   sshd[117314]: Accepted password for user1 from 1.2.3.XXX port
   46570 ssh2
```

- Network filtering/analysis has limited affect
- Widely used in recent attacks

Example of Failure



Incident Details

What Worked For Attackers:

- Simple Password and Key Theft
- Critical Mass of Systems Compromised
- Human Error (configuration and patching)

Response: OTP

Add authentication physically separate from the computer:

- **Good only once – worthless to steal**
- **Less dependant on host integrity**
- **Can be centralized**

Problem of Credential Theft completely resolved.

Other Issues

Introduction of OTP several problems:

- **Cross site collaboration: users have logins at multiple sties**
- **Established authentication services: architecture problems with OTP limitations**
- **Initial user identification and token maintenance and administration**

Can be resolved by careful design and administration.

Soothing Platitudes Redux

Change in hacker perspective: view authenticated users as a *service*!

- **Ignore authentication theft**
- **Let user log in with OTP, then take over their session**
- **Details in previous section**

Point is that hackers evolve to meet security environment changes.

OTP Conclusion

OTP Implementations do an excellent job of dealing with the problem of credential theft.

but

You must be prepared for the response to this new mechanism by the hacker community.

Large Scale Data Analysis

What is meant by large scale?

- Network Intrusion detection across multiple sites in real time
- Integrating different data sources for security analysis
- Interactive analysis of network connection data across multiple sites and long time periods

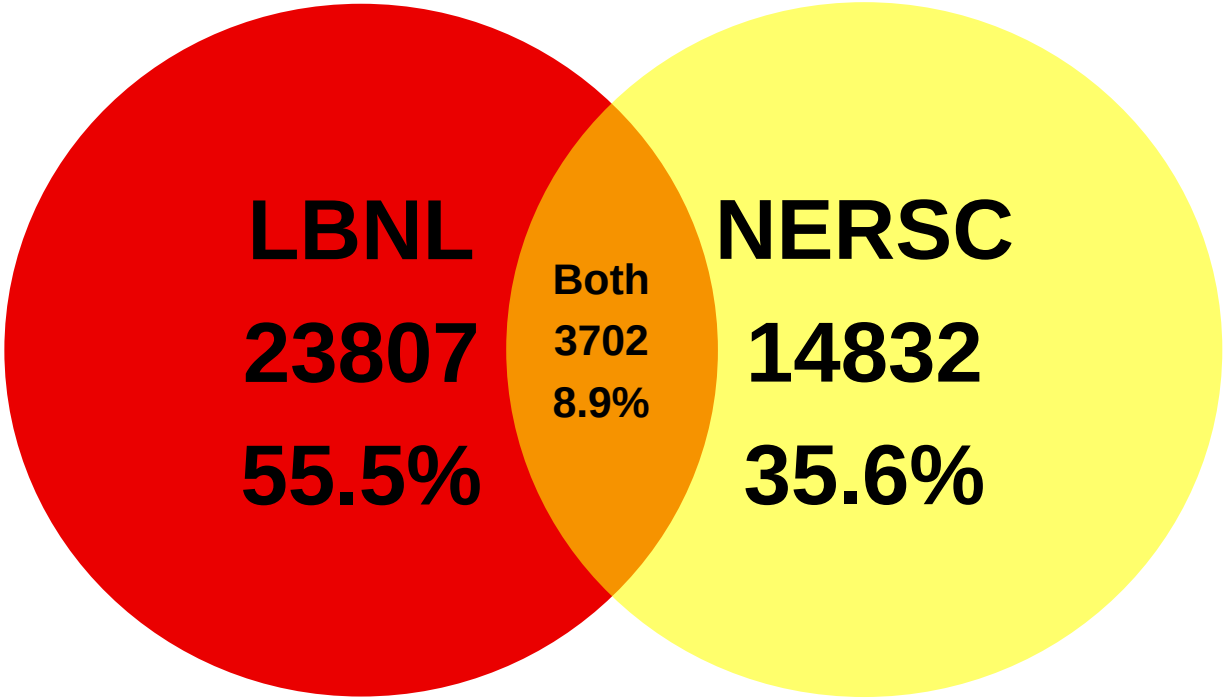
Background Information: Bro

- Main tool used to test these ideas is Bro Intrusion Detection System
  - Developed and used in production at LBNL
  - Highly flexible and extendable: ideal for this sort of research
  - Network based analysis

  - More background info in Appendix

Network Traffic From Multiple Sites

- Scans detected at LBNL/NERSC
- Over a 12 hour period
- Number of unique IP addresses seen
- Almost 10% of the scanning addresses seen by both address ranges



Network Traffic From Multiple Sites

Using Bro we can correlate cross site activity for:

- Network Connections
  - Scanning
  - Hostile HTTP activity
- Any activity derived from syslog
- Snort Rules
- In general, any event identifiable by Bro

Integrating Different Data Sources

How to look at data other than regular network traffic?

Using the Bro Generic Client, arbitrary structured data **can be fed into Bro including:**

- **Syslogs**
- **Firewall Logs**
- **Web Server Logs**

Integrating Different Data Sources:

How the Generic Client Works

(1) Start with Syslog message

```
Mar 10 18:39:41 2.3.4.5 Message forwarded from host609:
sshd[74334]: Accepted password for user1 from 1.2.3.XXX port
45674 ssh2
```

(2) Parse into clean form

```
ssh_login double=1108696916 addr=10.11.12.13
addr=10.14.15.16 string=user1 string=publickey
```

(3) **Bro Generic Client** reads text and communicates to Bro

BRO

(4) Bro acts on communication

Integrating Different Data Sources

Address issues brought up in section 1:

- **See what applications see**
- **See what hosts see**
- **Bring together different perspectives**
- **Addresses issues unique to HPC environment**

This comes at a cost of complexity.

Interactive Long Term Network Connection Analysis

In HPC centers and universities, connection volume can hinder analysis even for short time periods.

This problem can be exacerbated by:

- Desire for interactive results
- Analysis over long time periods

Even asking a simple question like “have we seen this host before?” can be resource prohibitive in terms of either time or analysis cycles.

Interactive Long Term Network Connection Analysis

Enter "FastBit", a compressed bitmap indexing technology for efficient searching of read-only data.

Developed by John Wu, Arie Shoshani, Ekow Otoo, and Kurt Stockinger at LBNL Scientific Data Management Research Group.

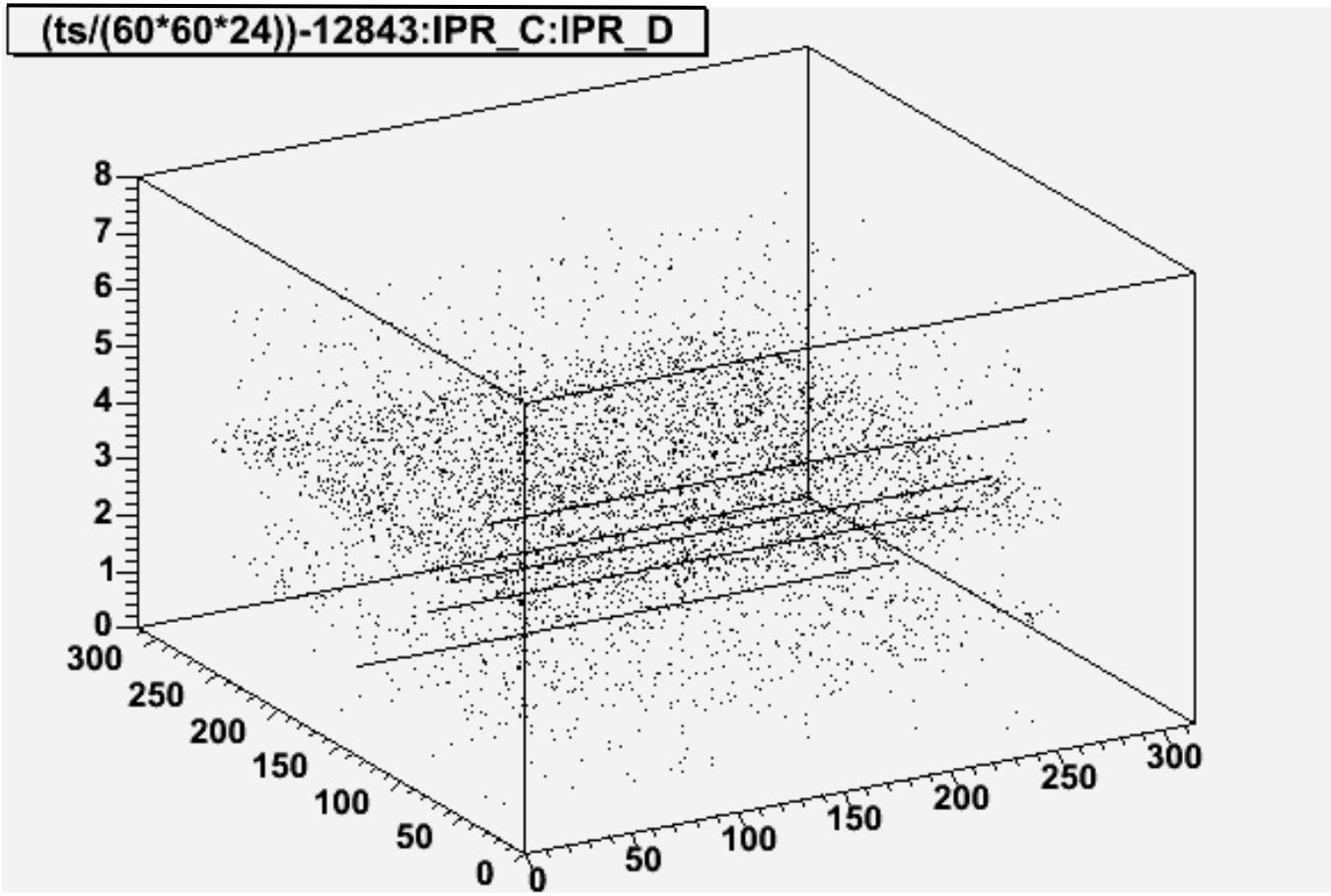
See Appendix for more details

Interactive Long Term Network Connection Analysis

SC05 HPC Analytics Challenge Entry

- LBNL/NERSC network logs (24 weeks)
- 1.1 billion records, each record has 25 variables (IP addresses, dates and time are split)
- Parallel querying (each process deals with one-week worth of log entries)
- FastBit integrated with ROOT analysis framework
- Searches involving three variables can be answered (data retrieved for visualization) in 23 seconds
  - One second per week

Interactive Long Term Network Connection Analysis



Sample traffic query showing hostile traffic distribution into NERSC address space from the 211.207.0.0/16 network

Real World Example: Protecting SCinet

Stephen Lau and Scott Campbell

Lawrence Berkeley National Laboratory
National Energy Research Scientific Computing Center
{slau, scampbell}@lbl.gov

SCinet

- SC Conference high speed network
  - Created by a dedicated team of volunteers
  - http://scinet.supercomp.org/
- We have no control over hosts and don't even know what is going to be shown!
- Many systems and applications are prototypes.

SC2004 Staff

SCinet

- An “open” network
  - No firewall.
- Diverse user base
  - Attendees, exhibitors, researchers
  - Industry, academia, government
- Diverse network
  - Exhibit floor
  - Extensive wireless coverage
  - Conference infrastructure (registration, show offices)
  - Educational rooms

Problem

- Ensure SCinet remains functional through the show.
  - Conference only runs one week!

- Threats
  - Outsider attacks
  - Clueless exhibitors and attendees
  - Crazed demos

Security within SCinet

- **Policy**
  - SCinet takes security *very* seriously.
  - Exhibitors handed policy document that is revised on an annual basis due to "lessons learned".

- **Security is built into the process.**
  - Planning considers security "upfront".
  - Not tacked on as an afterthought.

Defense in Depth

- Perimeter Defense
  - Bro and mon IDS
- Network subdivided based on function
  - Allows for filtering based on function
  - i.e. Exhibit show floor, Conference infrastructure
- Traffic filtered in some instances
  - Wireless filtered
    - Mainly to protect the wireless from itself

Defense in Depth

- User Education
  - SCinet Help Desk
  - Security demonstrations, i.e. Cube of Doom, password display
- Host Level
  - Ability to locate hosts
    - Wireless and wired
  - Ability to “jail” obnoxious hosts.
- Physical Security
  - Primarily to protect SCinet assets - (N > 10) million dollars in assets
  - SCinet access restricted and protected 24x7, before, during and after conference.

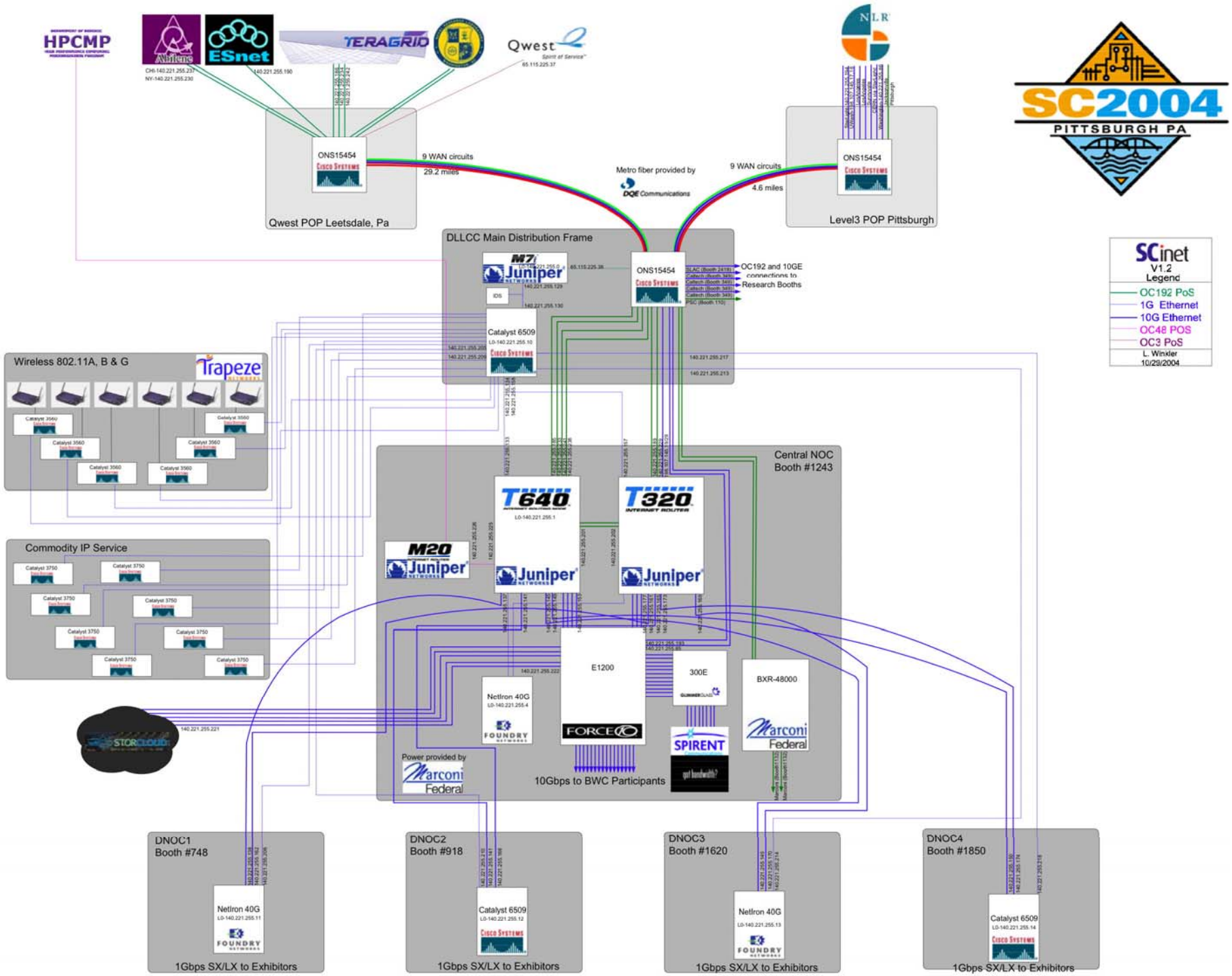
Incident Response

- Core of security professionals.
- Not able to conduct complete “incident response”.
- Attendees responsible for own systems.

- Goal to locate and identify hosts threatening SCinet.

SCinet SC2004 Architecture

- Simple campus architecture routed via Juniper T640, T320 and Cisco 6509
- WAN connections
  - OC3 commodity Internet service via Qwest
  - 16 OC192 links (NLR, ESNet, Abilene, Teragrid, etc)
  - 1 OC768 link to PSC
- Wireless architecture
  - Integrated wireless system by Trapeze
- Wired conference network to every meeting room
- Argonne address space (140.221.128.0/17)


HPCMP
Abilene
ESnet
TERAGRID
Qwest
NLR
SC2004
PITTSBURGH PA
CHI-140.221.255.237
NY-140.221.255.230
140.221.255.190
65.115.225.37
ONS15454
9 WAN circuits
29.2 miles
Qwest POP Leetsdale, Pa
Metro fiber provided by
DQE Communications
9 WAN circuits
4.6 miles
Level3 POP Pittsburgh
DLLCC Main Distribution Frame
M7i
Juniper
IDS
Catalyst 6509
OC192 and 10GE connections to Research Booths
SCinet
V1.2
Legend
OC192 PoS
1G Ethernet
10G Ethernet
OC48 POS
OC3 PoS
L. Winkler
10/29/2004
Wireless 802.11A, B & G
Trapeze
Catalyst 3560
Central NOC
Booth #1243
T640
T320
M20
Juniper
Commodity IP Service
Catalyst 3750
E1200
300E
BXR-48000
Netiron 40G
FOUNDRY
FORCE10
SPIRENT
Marconi Federal
STORCLOUD
Power provided by
10Gbps to BWC Participants
DNOC1
Booth #748
DNOC2
Booth #918
DNOC3
Booth #1620
DNOC4
Booth #1850
1Gbps SX/LX to Exhibitors
1Gbps SX/LX to Exhibitors
1Gbps SX/LX to Exhibitors
1Gbps SX/LX to Exhibitors

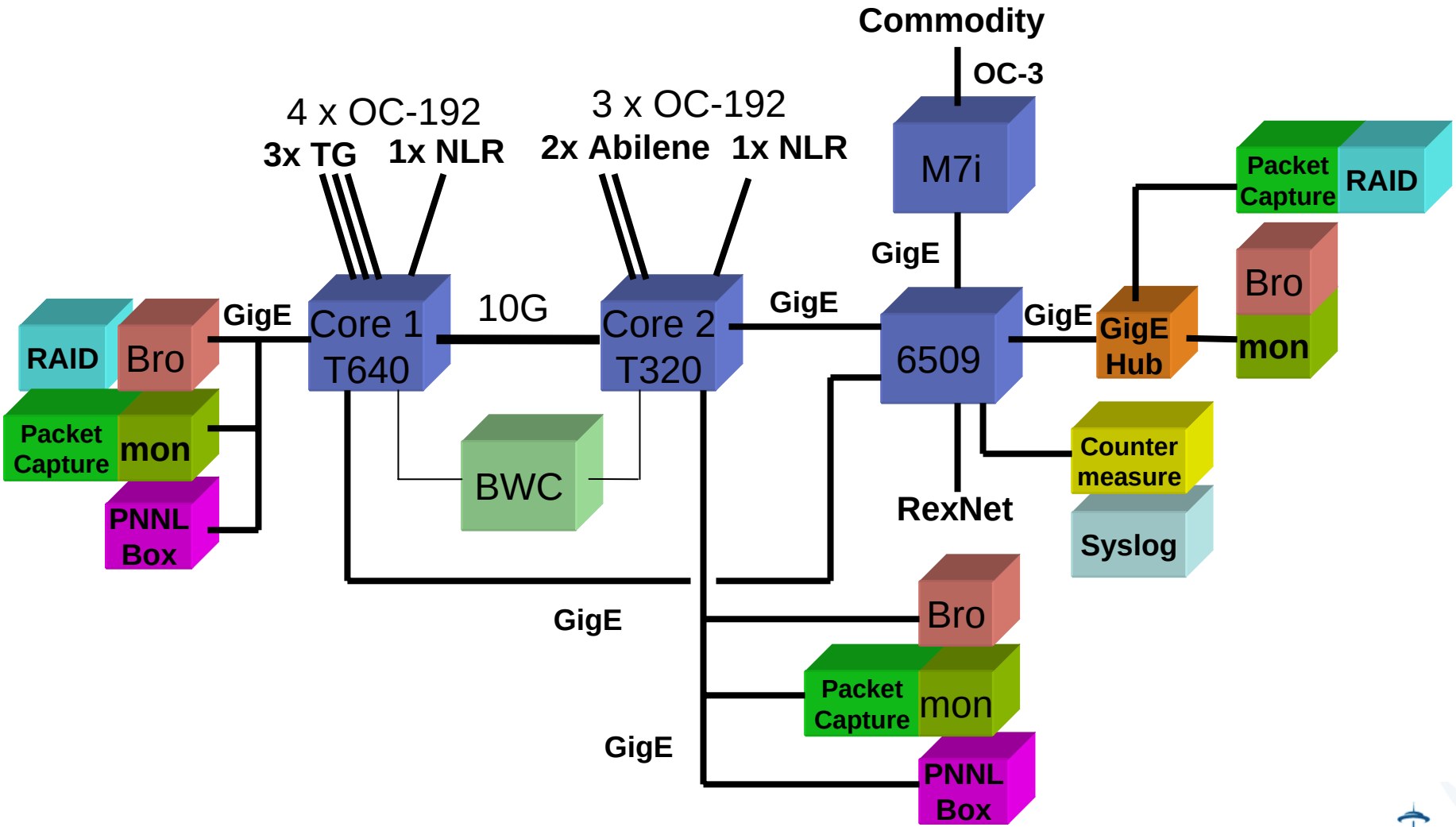
SC2004 Security Deployment

- Mon, Bro, Snort
- Cisco port mirroring
- Packet Engines GigE Hub
- NetOptics splitters
- RST responder, Desuckit application, SYN-ACK responder
- Experimental (OSX, AMD64 Opteron, Xyratex RAID system, S2IO 10GigE NICs)
- Password display
- MAC address blocking on wireless

Bro at SCinet

- Bro primary IDS for SC conference since SC00
  - Used to monitor SCinet traffic
  - Detect 0wned systems
  - Ensure conference network does not get taken down by attacks
- Maximum observed bandwidth
  - 23 Gbps at SC2003 (Bandwidth Challenge)
  - Used router hardware BPF
- Passive monitoring only
  - Automatic countermeasures disabled
- Educational tool for attendees
  - Password capture and display
  - Alert exhibitors to “risky behavior”
    - i.e. .rhosts with root enabled

SCinet 2004 Security Infrastructure



SC2004 Security Incidents

Linux Root Compromises	10	Solaris Root Compromises	0
Windows Root Compromises	3	Email Worm Infections	1
Clear Text Passwords	98	Clear Text Root Logins	26
Welchia Infections	2	Blaster Infections	2
Misc. Port 445 Worms	35	Avg Hours of Sleep for SCinet Staff	3.1
Rogue Access Points	8	Rogue Ad-Hoc Wireless	8
Inbound Scans	18386	Complaints about Password Display	0
Repeat Root Compromises	1	Complaints about Spinning Cube	1

SC2004 Intrusions (sample)

- 11/07/04 @ 9:00 SCinet rental desktop
  - Very poorly configured from PC vendor (d'oh!)
- 11/08/04 @ 11:53 Vendor booth (linux cluster)
  - Brute forced ssh password
  - Recon/scanning from 218.30.122.90
  - Initial login from 217.156.38.86
  - FTP outbound attempts to 81.196.20.134, 193.230.153.133
  - Followup ssh logins from 81.196.156.40
  - IRC chatting
  - Bytes counts from 140.221.220.165-9 indicate compromise
- 11/10/04 in the AM
  - MSSQL null SA password

SC2004 Intrusions (cont.)

- 11/11/04 @ 08:25 & 08:36 Vendor booth
  - Recon & attack from 194.242.112.34 (sd595.sivit.org - France)
  - Successful login from 81.196.61.19 (81.196.61.19.cablelink.rdsor.ro)
  - Linux box shows use of "mirkforce" rootkit.

- 11/11/04 @ 10:21-15:07 Educational booth
  - Windows laptop
  - Inital break-in from company in Tupelo, MS USA
  - Windows file sharing exploit/whatever
  - FTP server setup for distribution of movies

Lessons Learned

- Need to factor in 2x to 3x amount of time to get stuff done
  - Need someone good at explaining problems to customers
    - I.e. definition of 0wn3d
- Continual process of educating community on good practices
- Need for isolated/stand-alone wireless system
- if (BitTorrent && Wireless) { wireless.usability == crap; }
  - Users not courteous on wireless
- Never got a good data stream to adequately test 10Gbe cards or application(s)
- Outbound IRC ports were easy to pickup suspicious traffic
  - Don't confuse GPFS with IRC
- Need IPv6 IDS, since we have some native v6 links

SC|05

- Using Bro as IDS
- Added wireless capability to “jail” offending users and direct them to “de-worm” website
- Increase filtering of infrastructure network
- SCinet wide syslog capability
- Increase number of security demonstrations
  - Visit SCinet booth to view demonstrations

Summary

- Security doesn't necessarily require large infrastructure investments.
  - Caveat: Need to design with security in mind.
- Open security models do work.
- Dedicated staff is essential.

Question and Answers

- **Any Questions?**

Contact Information

- **William T. C. Kramer**
  - NERSC/LBNL
    Email: wtkramer@lbl.gov

- **Stephen Lau**
  - NERSC/LBNL
    Email: slau@lbl.gov
    Phone: +1 (510) 486-7178
    After Hours: +1 (510) 486-8600
    NERSC Security Contact: security@nersc.gov
    PGP Key Fingerprint:
    44C8 C9CB C15E 2AE1 7B0A 544E 9A04 AB2B F63F 748B

- **Scott Campbell**
  - NERSC/LBNL
    Email: scampbell@lbl.gov
    Phone: +1 (510) 486-6986
    After Hours: +1 (510) 486-8600
    NERSC Security Contact: security@nersc.gov
    PGP Key Fingerprint:
    89F9 593E 2381 88B2 B270 78B2 2B63 E5AB C07B 641C

Appendix

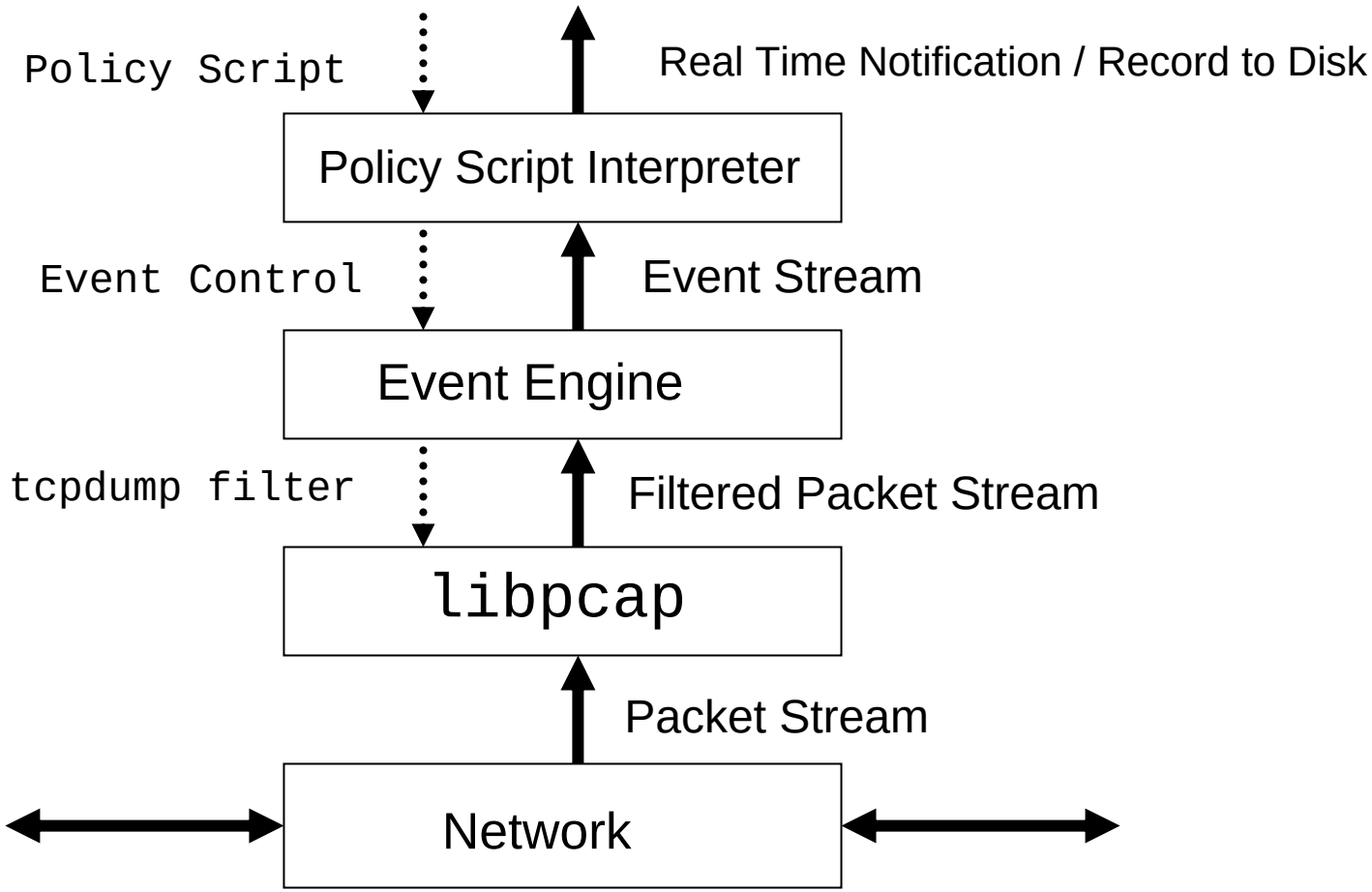
Index:

1. Bro Information
2. FastBit Details

Appendix 1: Bro Information

- **Bro maintains and analyzes state**
  - Keeps track of all network connections
  - Reacts to network behavior patterns
  - Can use Snort signatures
  - Tracks and records behavior for HTTP, FTP, SMB, portmapper, NFS, SMTP and several other protocols.

Appendix 1: Bro Information



Appendix 1: Bro Information

For more information, see:

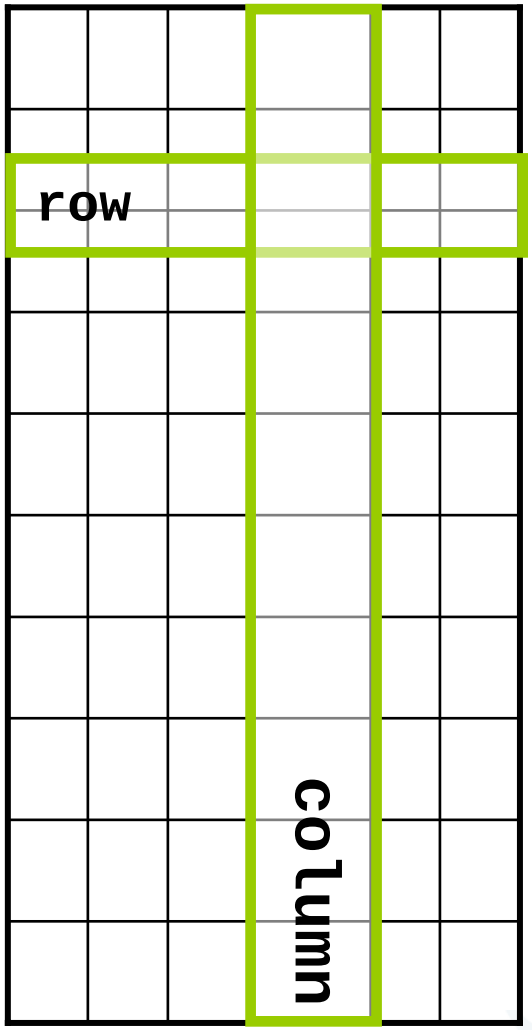
http://www.bro-ids.org

Appendix 2: FastBit

- Goal: efficient search of *multi-dimensional* read-only (append-only) data
- Commonly-used indices are designed to be updated quickly
  - E.g. family of B-Trees
  - Sacrifice search efficiency to permit dynamic update
- Most multi-dimensional indices suffer *curse of dimensionality*
  - E.g. R-tree, Quad-trees, KD-trees, …
  - Don't scale to large number of dimensions (< 20)
  - Are efficient only if all dimensions are queried
- Bitmap indices are efficient but may demand too much space
  - Sacrifice update efficiency to gain more search efficiency
  - ☺ Are efficient for multi-dimensional queries
  - ☺ Query response time scales linearly in the actual number of dimensions in the query
- We solve the size problem by developing a compression scheme that
  - ☺ Reduces the index size
  - ☺ Improves operational efficiency

FastBit Cont…

- FastBit is designed to search multi-dimensional data
  - Conceptually in table format
    - rows ➔ objects
    - columns ➔ attributes
- FastBit uses <u>vertical (column-oriented) organization</u> for the data
  - Efficient for analysis of read-only data
- FastBit uses <u>compressed bitmap indices</u> to speed up searches
  - Proven in analysis to be optimal for single-attribute queries
  - Superior to other optimal indices because they are also efficient for multi-attribute queries



Basic Bitmap Index

Data values	b_0	b_1	b_2	b_3	b_4	b_5
0	1	0	0	0	0	0
1	0	1	0	0	0	0
5	0	0	0	0	0	1
3	0	0	0	1	0	0
1	0	1	0	0	0	0
2	0	0	1	0	0	0
0	1	0	0	0	0	0
4	0	0	0	0	1	0
1	0	1	0	0	0	0
	=0	=1	=2	=3	=4	=5

A < 2 2 < A < 5

- First commercial version
  - Model 204, P. O'Neil, 1987
- Easy to build: faster than building B-trees
- Efficient for querying: only bitwise logical operations
  - A < 2 → b_0 OR b_1
  - 2<A<5 → b_3 OR b_4
- Efficient for multi-dimensional queries
  - Use bitwise operations to combine the partial results
- Size: one bit per distinct value per object
  - Definition: Cardinality == number of distinct values
  - Compact for low cardinality attributes only, say, < 100
  - Need to control size for high cardinality attributes

FastBit cont…

Example: 2015 bits

1000000000000000000001110000000000000000000000000000000……000000000000000000000000000000111111111111111111111111
11

Main Idea: Use run-length-encoding, but...
partition bits into 31-bit groups

31 bits | 31 bits | … | 31 bits

Merge neighboring groups with identical bits

31 bits | Count=63 (31 bits) | 31 bits

Encode each group using one word

- Name: Word-Aligned Hybrid (WAH) code
- Key features: WAH is compute-efficient because it
  - Uses the run-length encoding (simple)
  - Allows operations directly on compressed bitmaps
  - Never breaks any words into smaller pieces during operations

Bibliography

- **R. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," *IEEE Security & Privacy*, April 2002.**
  - http://www.computer.org/security/supplement1/kem/index.htm
- **S. McCanne and V. Jacobson, "The BSD Packet Filter: A New Architecture for User-level Packet Capture," *Proc. 1993 Winter USENIX Conference*, San Diego, CA.**
- **B. Mukherjee, L. Heberlein, and K. Levitt, "Network Intrusion Detection," *IEEE Network*, 8(3), pp. 26-41, May/Jun. 1994.**

Bibliography (cont)

- V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks*, 31(23-24), pp. 2435–2463, 14 Dec. 1999. (Also *Proc. 7th USENIX Security Symposium*, Jan. 1998.)
  - `ftp://ftp.ee.lbl.gov/papers/bro-CN99.ps.gz`
- T. Ptacek and T. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection," 1998. (unpublished but widely influential)
  - `http://www.icir.org/vern/Ptacek-Newsham-Evasion-98.ps`
- M. Ranum et al, "Implementing a generalized tool for network monitoring," *Proc. LISA '97*, USENIX 11th Systems Administration Conference, San Diego, Oct. 1997.

Bibliography (cont)

- **S. Staniford, V. Paxson and N. Weaver, "How to 0wn the Internet in Your Spare time," *Proc. 11th USENIX Security Symposium*, August 2002.**
  - http://www.icir.org/vern/papers/cdc-usenix-sec02/index.html
- **Y. Zhang and V. Paxson, "Detecting Backdoors," *Proc. 9th USENIX Security Symposium*, August 2000**
  - http://www.icir.org/vern/papers/backdoor-sec00.ps.gz
- **Y. Zhang and V. Paxson, "Detecting Stepping Stones," *Proc. 9th USENIX Security Symposium*, August 2000.**
  - http://www.icir.org/vern/papers/stepping-sec00.ps.gz

Bibliography (cont)

- R. Pang, V. Yegneswaran, P. Barford, V. Paxson and L. Peterson, Characteristics of Internet Background Radiation, Proc. ACM IMC, October 2004.
  - http://www.icir.org/vern/papers/radiation-imc04.pdf
- H. Dreger, A. Feldmann, V. Paxson, and R. Sommer, Operational Experiences with High-Volume Network Intrusion Detection, Proc. ACM CCS, October 2004.
  - http://www.icir.org/vern/papers/high-volume.ccs04.pdf
- J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, Fast Portscan Detection Using Sequential Hypothesis Testing, Proc. IEEE Symposium on Security and Privacy, May 2004.
  - http://www.icir.org/vern/papers/portscan-oak04.pdf