

Firewalls, IDS and Social Network

Presenter: Yinzhi Cao
Lehigh University

Acknowledgement

- ◆ <http://www.cs.northwestern.edu/~ychen/classes/mitp-458/firewalls.ppt>
- ◆ http://web.cse.ohio-state.edu/~xuan/courses/4471/4471_social_network_security_reading.ppt
- ◆ <http://www.cs.northwestern.edu/~ychen/classes/msit458-f12/ids.ppt>



◆ **Firewalls**

◆ Intrusion Detection System (IDS)

◆ Social Network

What is a Firewall?

- ◆ A **choke point** of control and monitoring
- ◆ Interconnects networks with differing trust
- ◆ Imposes restrictions on network services
 - only authorized traffic is allowed
- ◆ Auditing and controlling access
 - can implement alarms for abnormal behavior
- ◆ Itself immune to penetration
- ◆ Provides **perimeter defence**

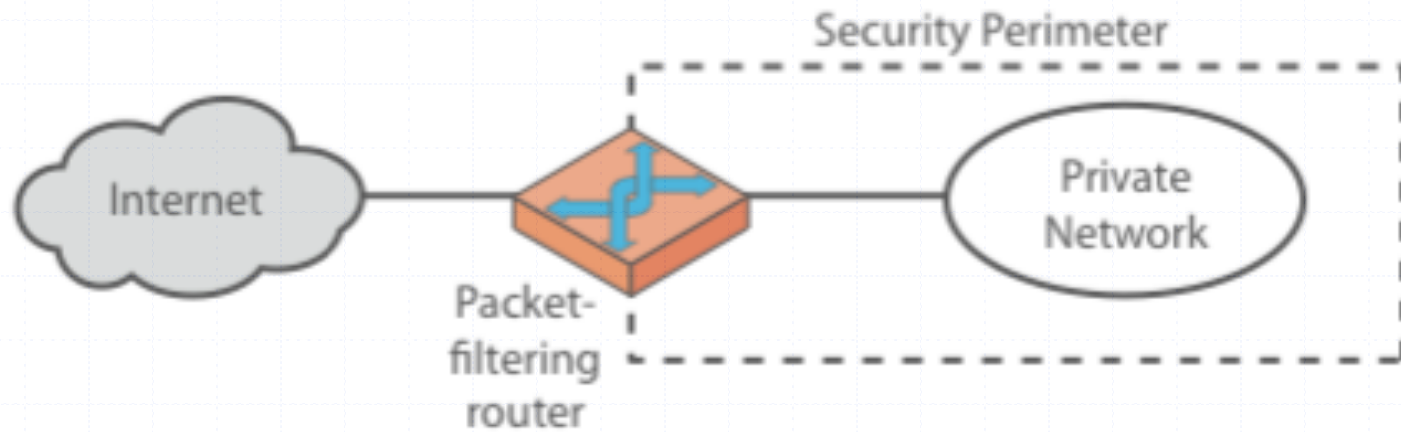
Classification of Firewall

Characterized by protocol level it controls in

- ◆ Packet filtering
- ◆ Circuit gateways
- ◆ Application gateways

- ◆ Combination of above is dynamic packet filter

Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

- ◆ Simplest of components
- ◆ Uses transport-layer information only
 - IP Source Address, Destination Address
 - Protocol/Next Header (TCP, UDP, ICMP, etc)
 - TCP or UDP source & destination ports
 - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
 - ICMP message type
- ◆ Examples
 - DNS uses port 53
 - ◆ No incoming port 53 packets except known trusted servers

Usage of Packet Filters

- ◆ Filtering with incoming or outgoing interfaces
 - E.g., Ingress filtering of spoofed IP addresses
 - Egress filtering
- ◆ Permits or denies certain services
 - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems

How to Configure a Packet Filter

- ◆ Start with a security policy
- ◆ Specify allowable packets in terms of logical expressions on packet fields
- ◆ Rewrite expressions in syntax supported by your vendor
- ◆ General rules - least privilege
 - All that is not expressly permitted is prohibited
 - If you do not need it, eliminate it

Every ruleset is followed by an implicit rule reading like this.

| action | ourhost | port | theirhost | port | comment |
|--------|---------|------|-----------|------|----------------|
| block | * | * | * | * | <i>default</i> |

Example 1:

Suppose we want to allow inbound mail (SMTP, port 25) but only to our gateway machine. Also suppose that mail from some particular site SPIGOT is to be blocked.

Solution 1:

| action | ourhost | port | theirhost | port | comment |
|--------|---------|------|-----------|------|------------------------------------|
| block | * | * | SPIGOT | * | <i>we don't trust these people</i> |
| allow | OUR-GW | 25 | * | * | <i>connection to our SMTP port</i> |

Example 2:

Now suppose that we want to implement the policy “any inside host can send mail to the outside”.

Solution 2:

| action | ourhost | port | theirhost | port | comment |
|--------|---------|------|-----------|------|--------------------------------------|
| allow | * | * | * | 25 | <i>connection to their SMTP port</i> |

This solution allows calls to come from any port on an inside machine, and will direct them to port 25 on the outside. Simple enough...

So why is it wrong?

- ◆ Our defined restriction is based solely on the outside host's port number, which we have no way of controlling.
- ◆ Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.

What can be a better solution ?

| action | src | port | dest | port | flags | comment |
|--------|-------------|------|------|------|-------|---------------------------------------|
| allow | {our hosts} | * | * | 25 | | <i>our packets to their SMTP port</i> |
| allow | * | 25 | * | * | ACK | <i>their replies</i> |

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts

Security & Performance of Packet Filters

- ◆ IP address spoofing
 - Fake source address to be trusted
 - Add filters on router to block
- ◆ Tiny fragment attacks
 - Split TCP header info over several tiny packets
 - Either discard or reassemble before check
- ◆ Degradation depends on number of rules applied at any point
- ◆ Order rules so that most common traffic is dealt with first
- ◆ Correctness is more important than speed

Port Numbering

◆ TCP connection

- Server port is number less than 1024
- Client port is number between 1024 and 16383

◆ Permanent assignment

- Ports <1024 assigned permanently
 - ◆ 20,21 for FTP
 - ◆ 23 for Telnet
 - ◆ 25 for server SMTP
 - ◆ 80 for HTTP

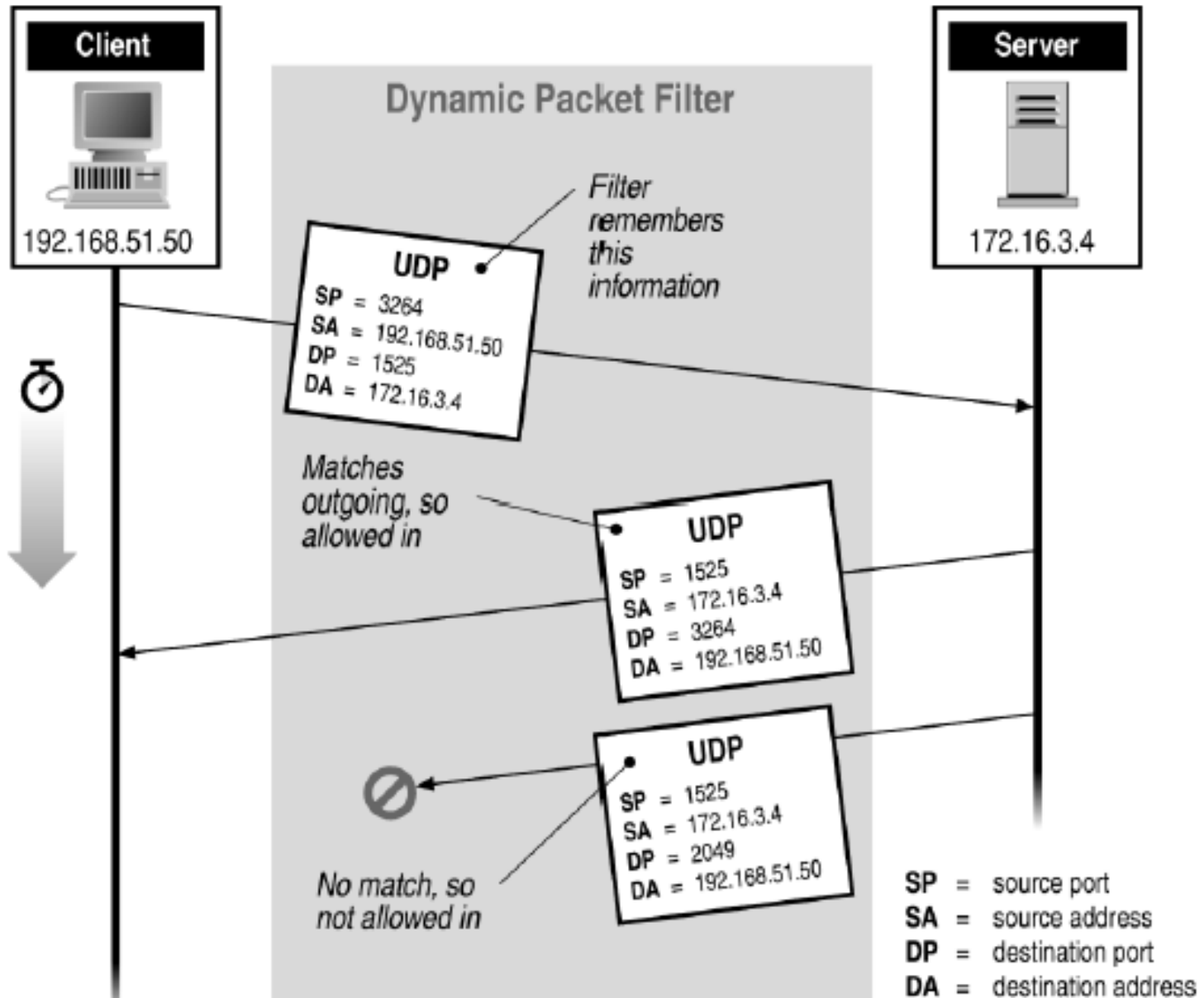
◆ Variable use

- Ports >1024 must be available for client to make any connection
- This presents a limitation for stateless packet filtering
 - ◆ If client wants to use port 2048, firewall must allow *incoming* traffic on this port
- Better: stateful filtering knows outgoing requests

Firewalls – Stateful Packet Filters

- ◆ Traditional packet filters do not examine higher layer context
 - ie matching return packets with outgoing flow
- ◆ Stateful packet filters address this need
- ◆ They examine each IP packet in context
 - Keep track of client-server sessions
 - Check each packet validly belongs to one
- ◆ Hence are better able to detect bogus packets out of context

Stateful Filtering



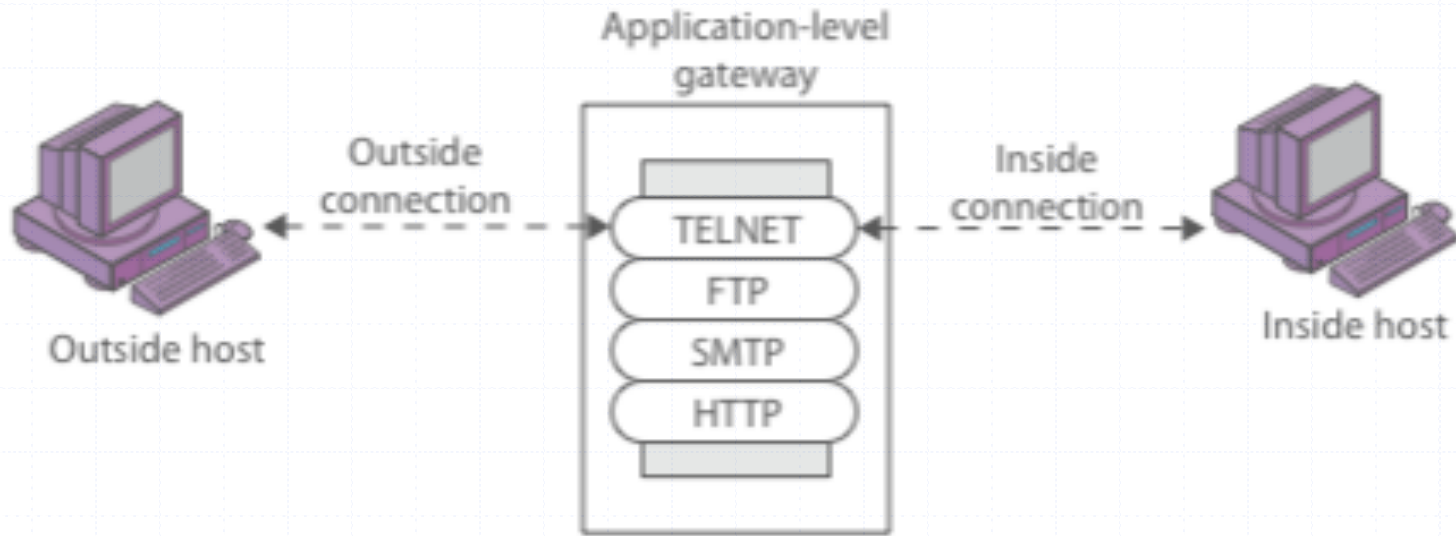
Firewall Outlines

- ◆ Packet filtering
- ◆ **Application gateways**
- ◆ Circuit gateways
- ◆ Combination of above is dynamic packet filter

Firewall Gateways

- ◆ Firewall runs set of proxy programs
 - Proxies filter incoming, outgoing packets
 - All incoming traffic directed to firewall
 - All outgoing traffic appears to come from firewall
- ◆ Policy embedded in proxy programs
- ◆ Two kinds of proxies
 - Application-level gateways/proxies
 - ◆ Tailored to http, ftp, smtp, etc.
 - Circuit-level gateways/proxies
 - ◆ Working on TCP level

Firewalls - Application Level Gateway (or Proxy)

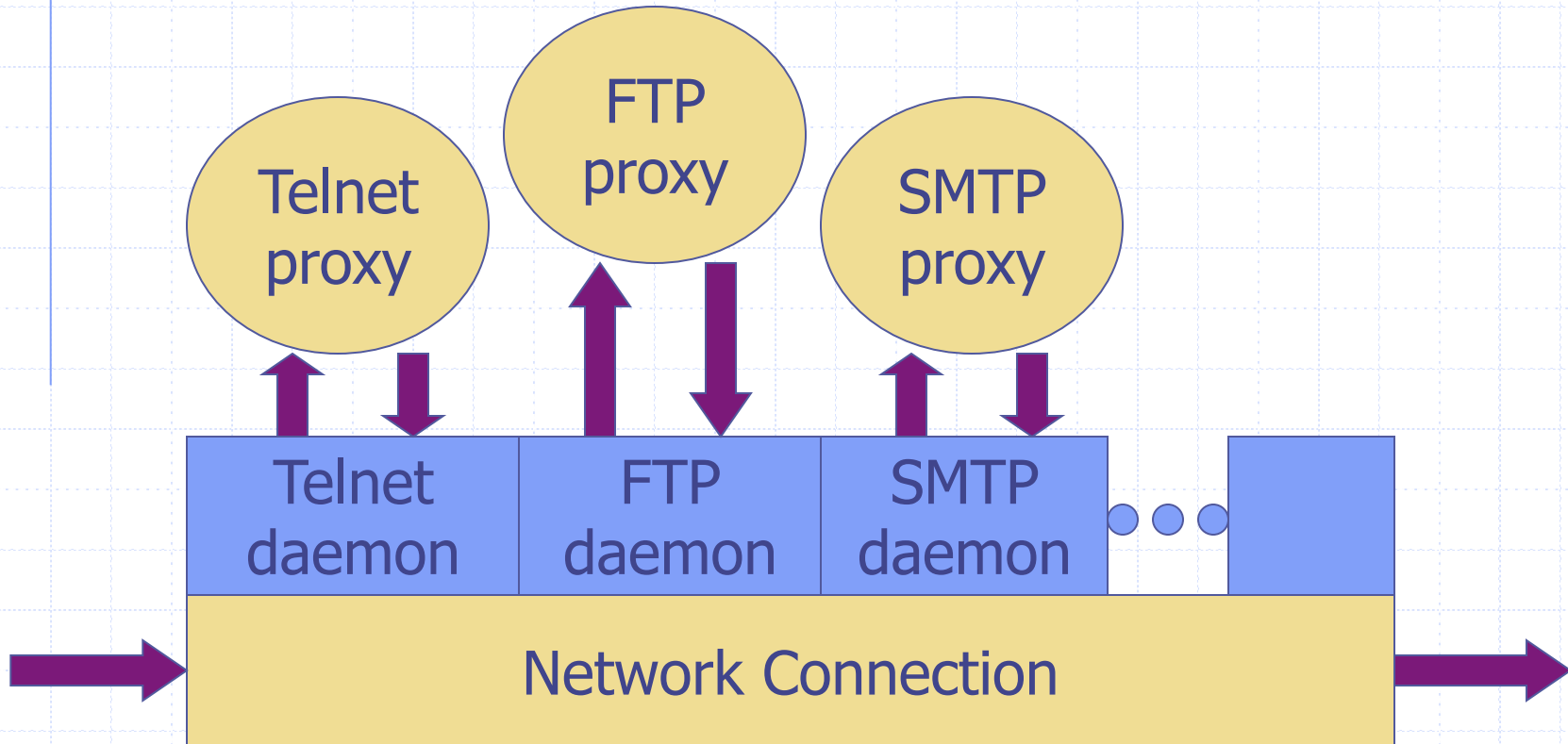


(b) Application-level gateway

Application-Level Filtering

- ◆ Has full access to protocol
 - user requests service from proxy
 - proxy validates request as legal
 - then actions request and returns result to user
- ◆ Need separate proxies for each service
 - E.g., SMTP (E-Mail)
 - NNTP (Net news)
 - DNS (Domain Name System)
 - NTP (Network Time Protocol)
 - custom services generally not supported

App-level Firewall Architecture



Daemon spawns proxy when communication detected ...

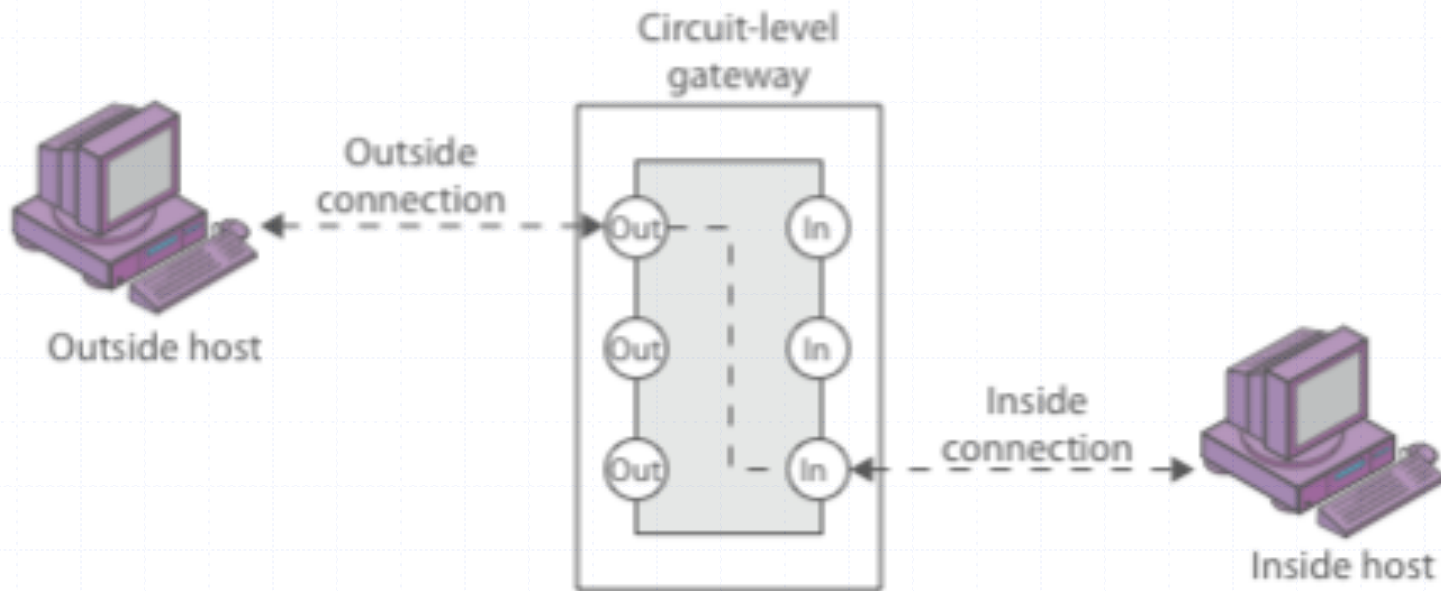
Enforce policy for specific protocols

- ◆ E.g., Virus scanning for SMTP
 - Need to understand MIME, encoding, Zip archives

Firewall Outlines

- ◆ Packet filtering
- ◆ Application gateways
- ◆ **Circuit gateways**
- ◆ Combination of above is dynamic packet filter

Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

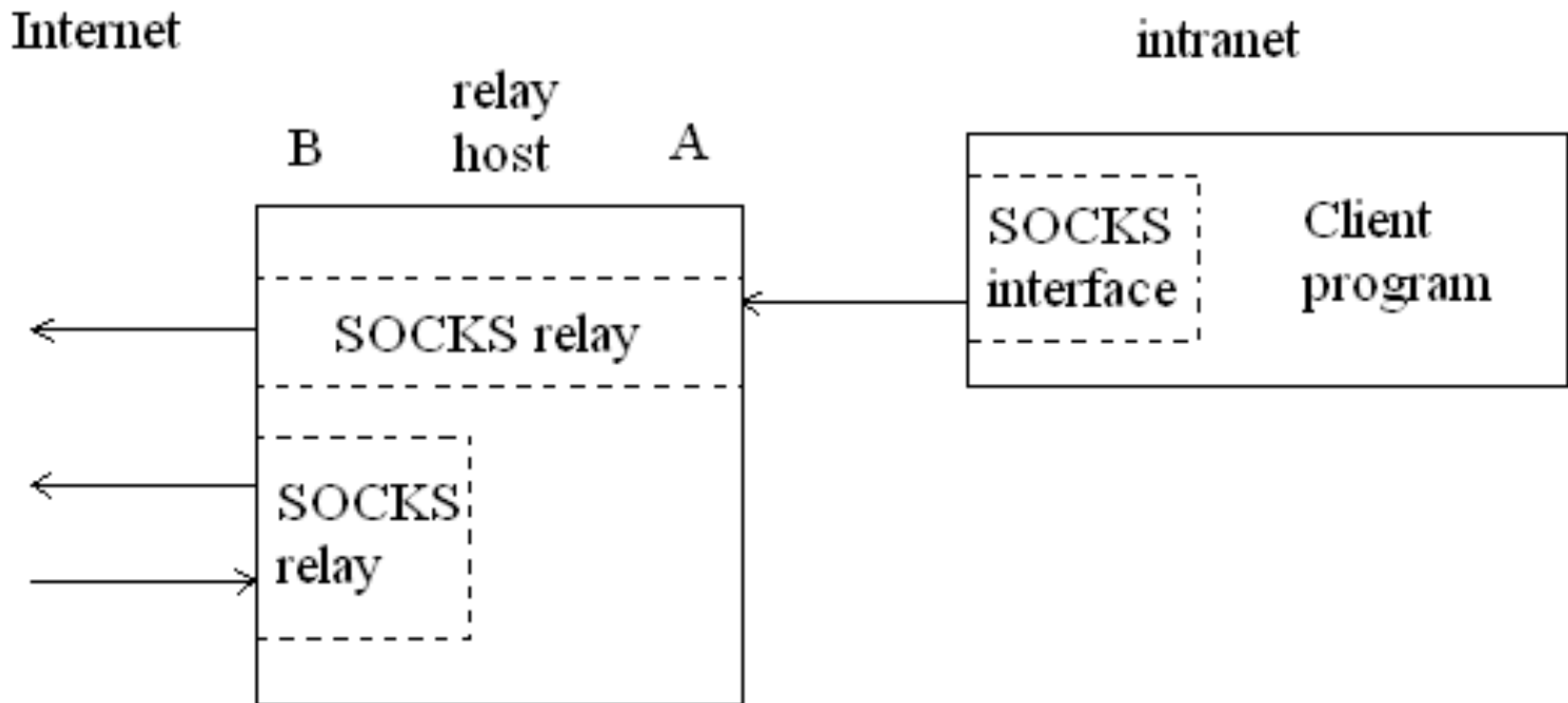
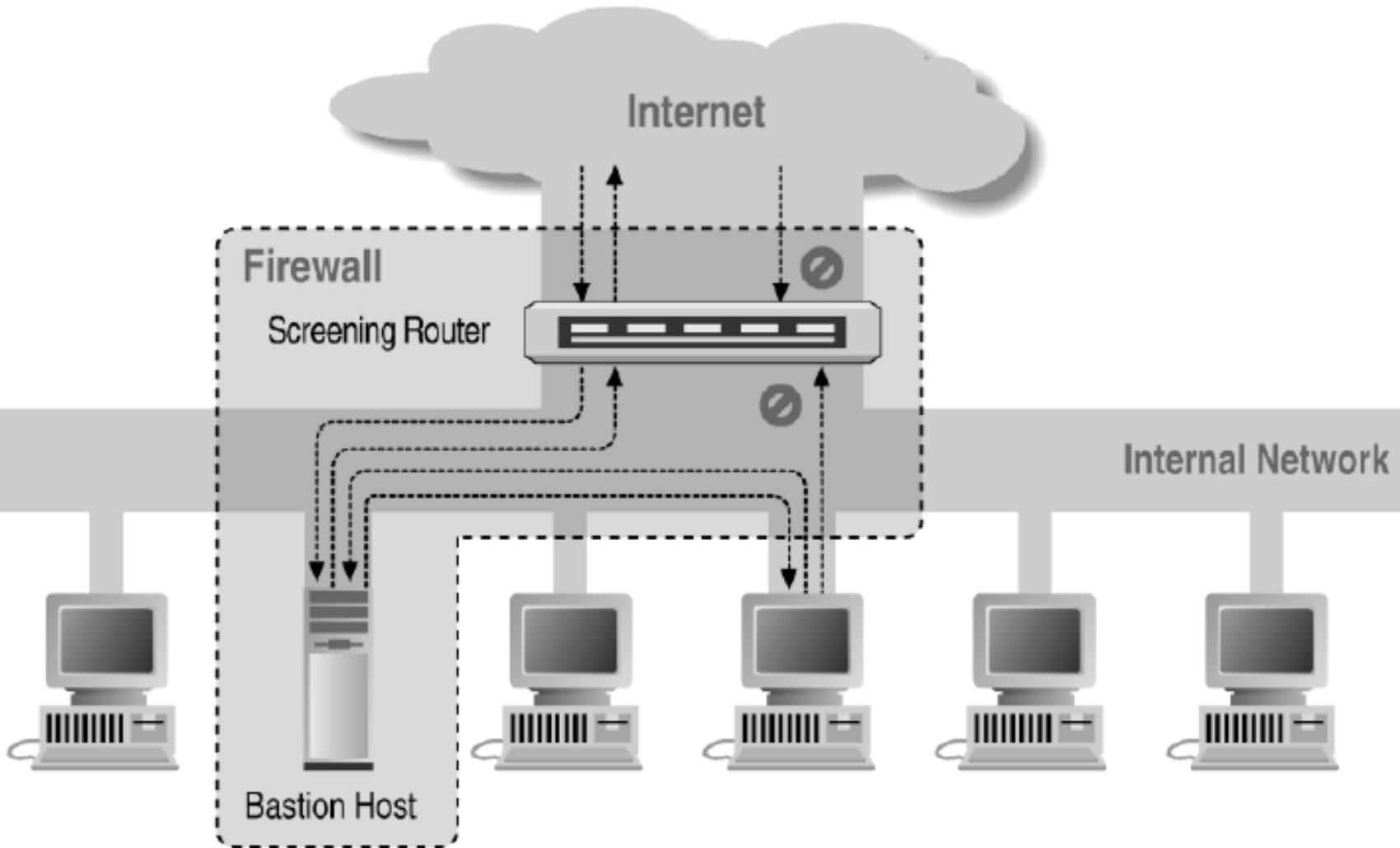


Figure 9.7: A typical SOCKS connection through interface A, and rogue connection through the external interface, B.

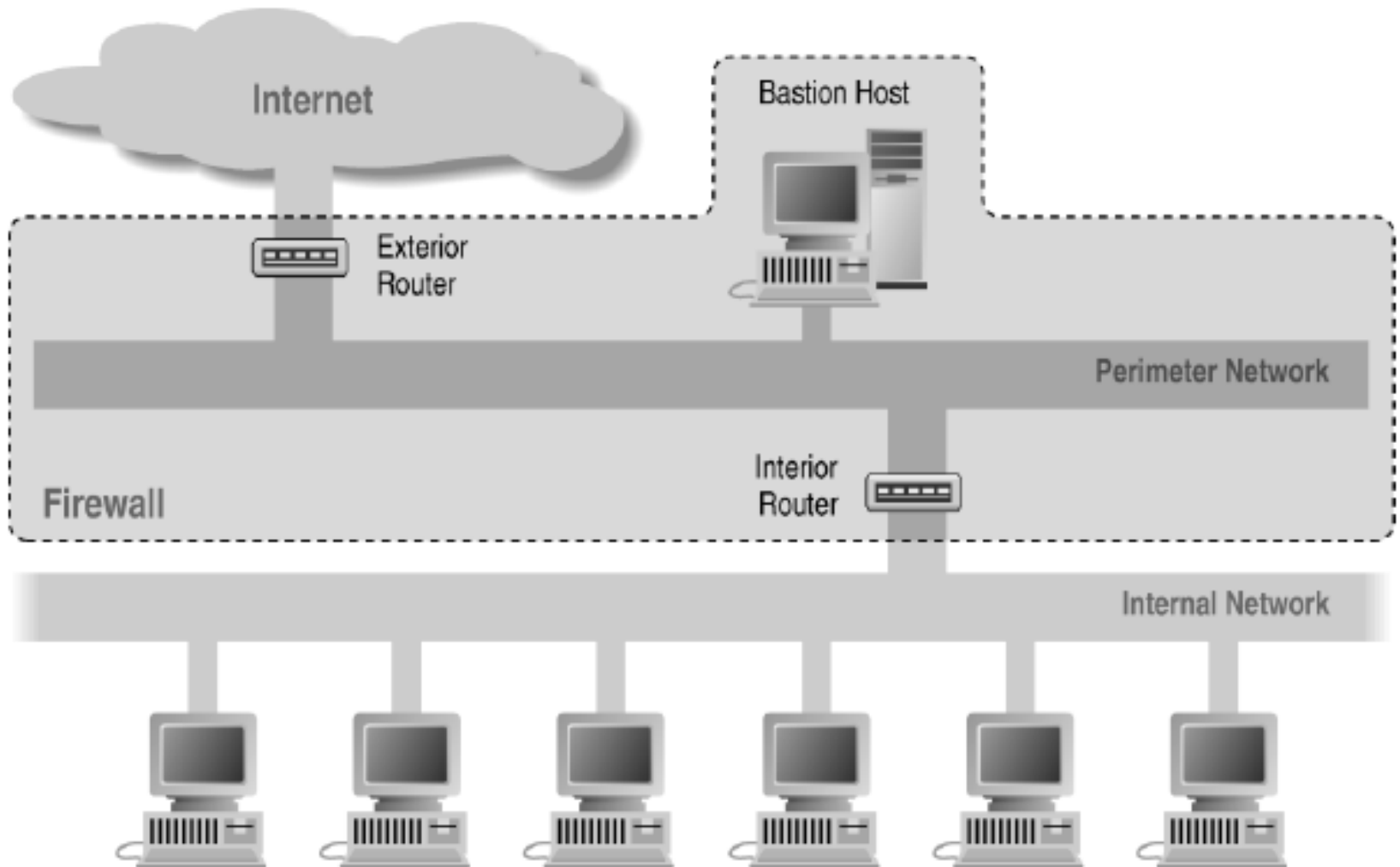
Bastion Host

- ◆ Highly secure host system
- ◆ Potentially exposed to "hostile" elements
- ◆ Hence is secured to withstand this
 - Disable all non-required services; keep it simple
- ◆ Trusted to enforce trusted separation between network connections
- ◆ Runs circuit / application level gateways
 - Install/modify services you want
- ◆ Or provides externally accessible services

Screened Host Architecture



Screened Subnet Using Two Routers



Firewalls Aren't Perfect?

- ◆ Useless against attacks from the inside
 - Evildoer exists on inside
 - Malicious code is executed on an internal machine
- ◆ Organizations with greater insider threat
 - Banks and Military
- ◆ Protection must exist at each layer
 - Assess risks of threats at every layer
- ◆ Cannot protect against transfer of all virus infected programs or files
 - because of huge range of O/S & file types



- ◆ Firewalls

- ◆ **Intrusion Detection System (IDS)**

- ◆ Social Network

Objectives and Deliverable

- ◆ Understand the concept of IDS/IPS and the two major categorizations: by features/models, and by location. Understand the pros and cons of each approach
- ◆ Be able to write a snort rule when given the signature and other configuration info
- ◆ Understand the difference between exploits and vulnerabilities

Definitions

◆ Intrusion

- A set of actions aimed to compromise the security goals, namely
 - ◆ Integrity, confidentiality, or availability, of a computing and networking resource

◆ Intrusion detection

- The process of identifying and responding to intrusion activities

◆ Intrusion prevention

- Extension of ID with exercises of access control to protect computers from exploitation

Elements of Intrusion Detection

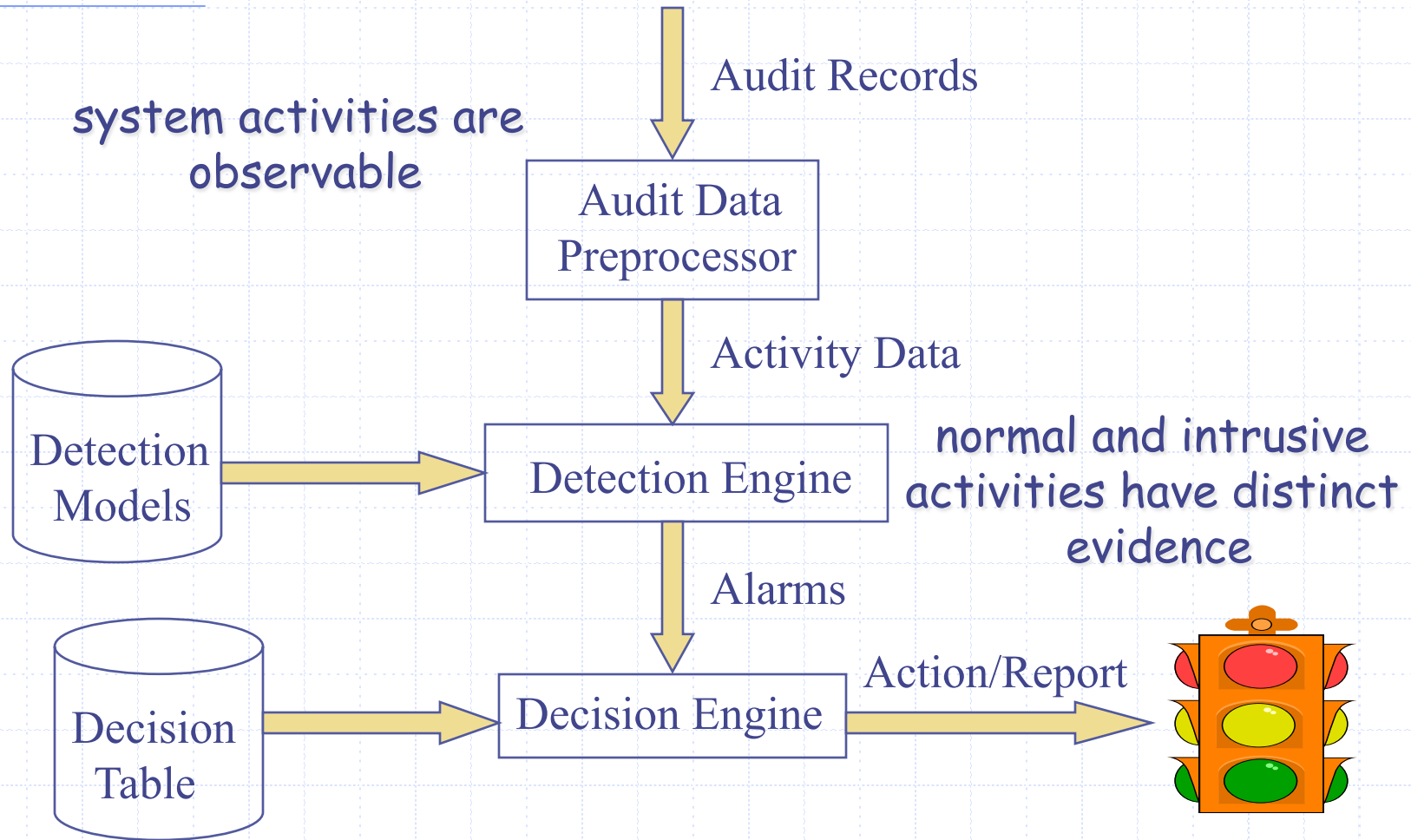
◆ Primary assumptions:

- System activities are observable
- Normal and intrusive activities have distinct evidence

◆ Components of intrusion detection systems:

- From an algorithmic perspective:
 - ◆ Features - capture intrusion evidences
 - ◆ Models - piece evidences together
- From a system architecture perspective:
 - ◆ Various components: audit data processor, knowledge base, decision engine, alarm generation and responses

Components of Intrusion Detection System



Intrusion Detection Approaches

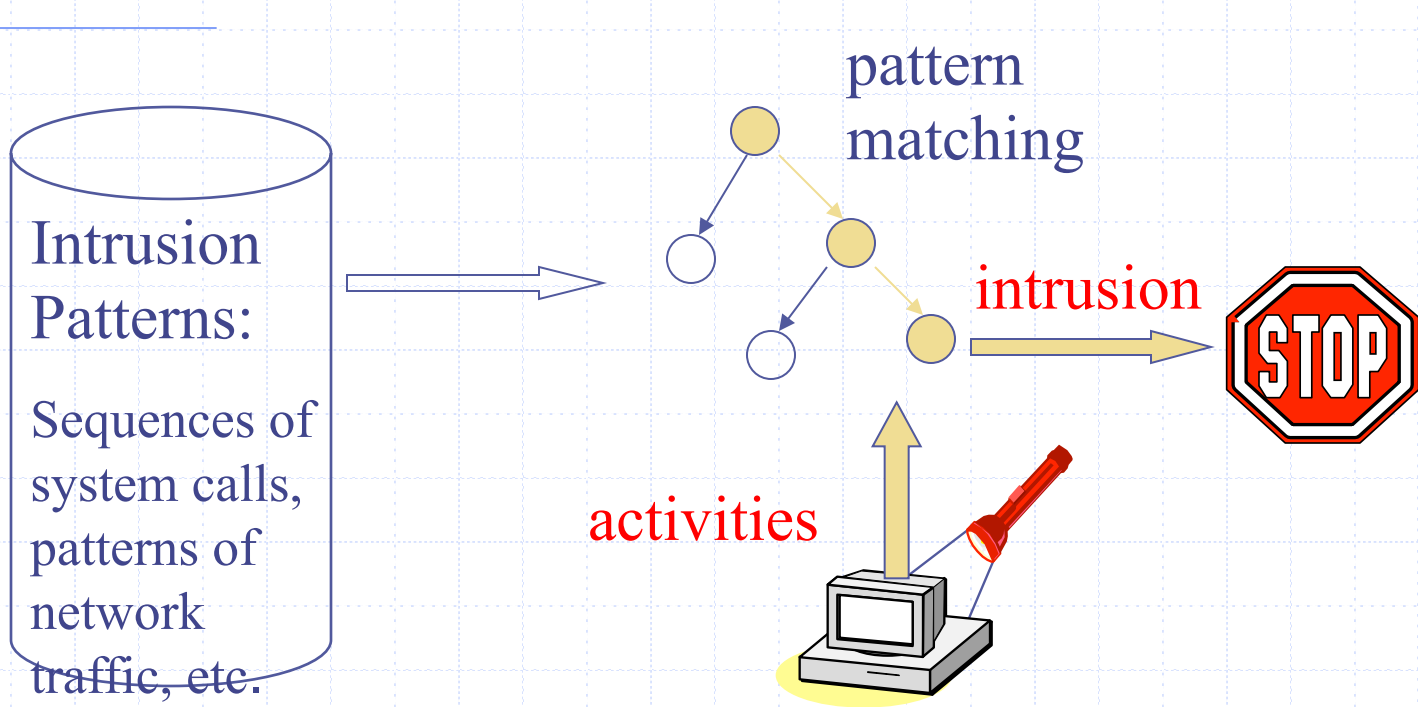
◆ Modeling

- Features: evidences extracted from audit data
- Analysis approach: piecing the evidences together
 - ◆ Misuse detection (a.k.a. signature-based)
 - ◆ Anomaly detection (a.k.a. statistical-based)

◆ Deployment: Network-based or Host-based

- Network based: monitor network traffic
- Host based: monitor computer processes

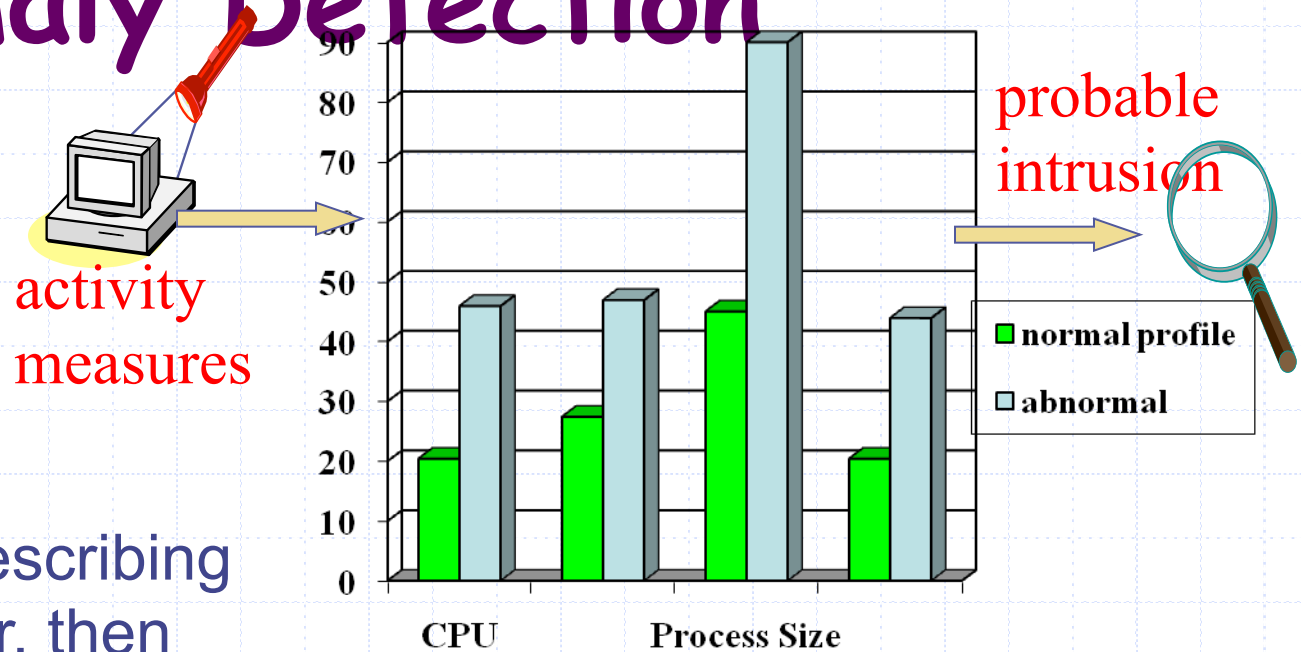
Misuse Detection



Example: *if* (traffic contains “x90+de[^\r\n]{30}”) *then* “attack detected”
Advantage: Mostly accurate. But problems?

Can't detect new attacks

Anomaly Detection



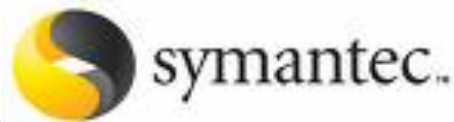
Define a profile describing “normal” behavior, then detects deviations. Thus can detect potential new attacks.
Any problem ?

Relatively high false positive rates

- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
 - E.g., router failure or misconfiguration, P2P misconfig
- Which method will detect DDoS SYN flooding ?

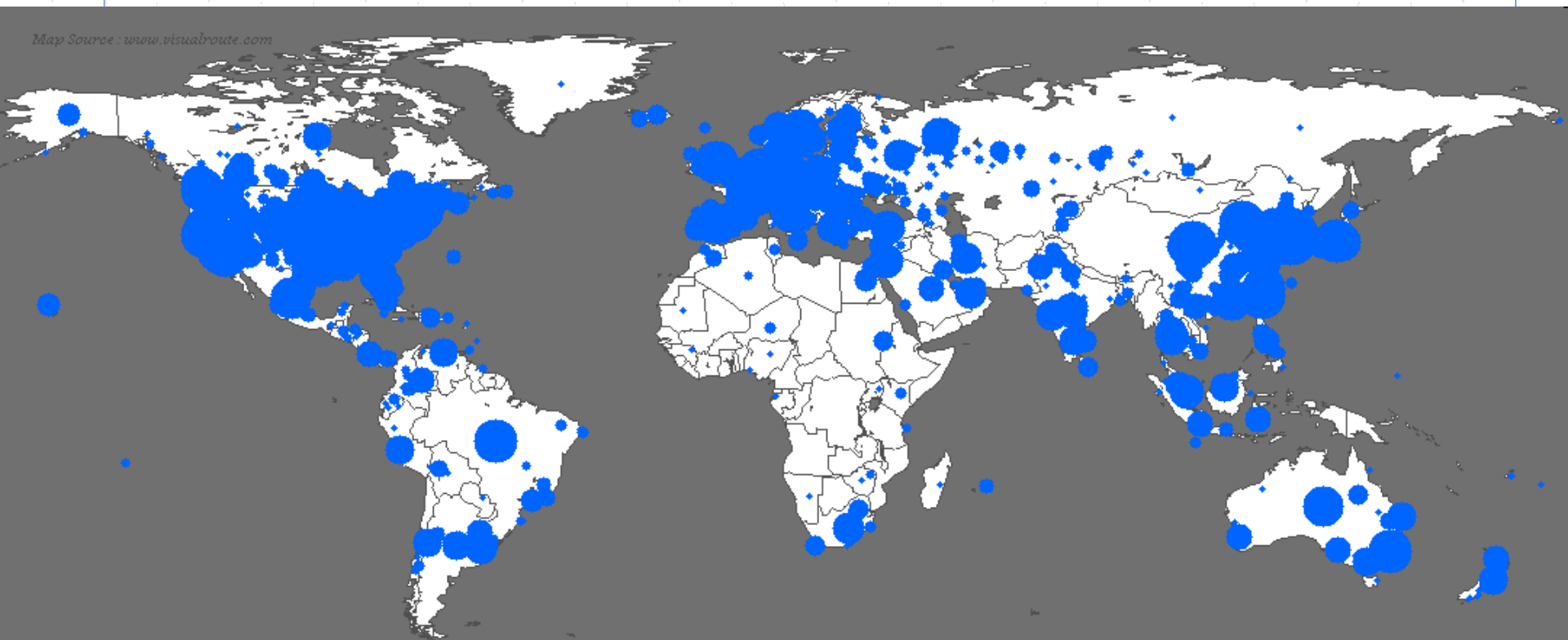
Host-Based IDSs

- ◆ Use OS auditing and monitoring/analysis mechanisms to find malware
 - Can execute full static and dynamic analysis of a program
 - ◆ Monitor shell commands and system calls executed by user applications and system programs
 - Has the most comprehensive program info for detection, thus accurate
- ◆ Problems:
 - User dependent: install/update IDS on all user machines!
 - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
 - Only local view of the attack



The Spread of Sapphire/Slammer Worms

Map Source: www.visualroute.com



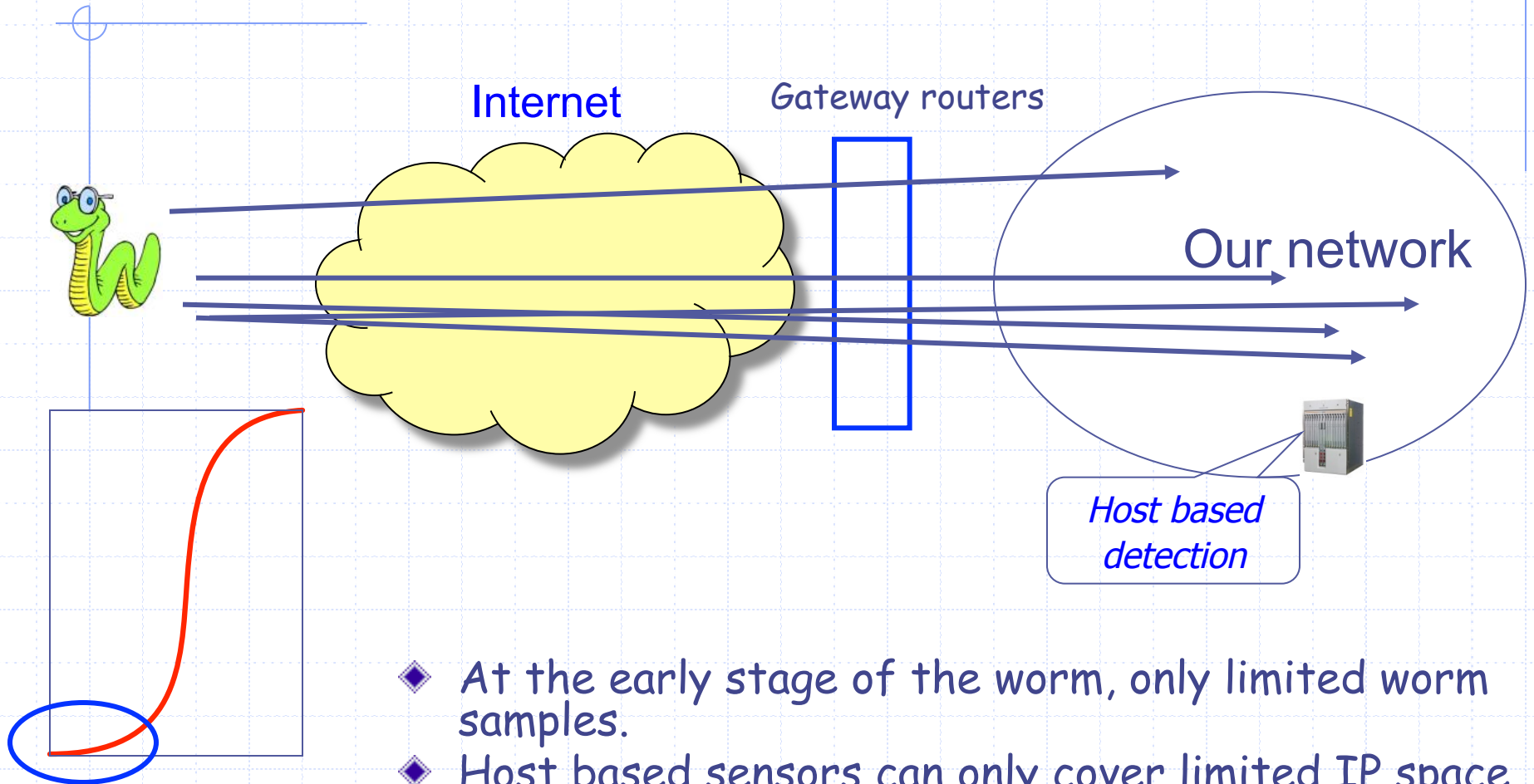
Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

<http://www.caida.org>

Copyright (C) 2003 UC Regents

Network Based IDSs



- ◆ At the early stage of the worm, only limited worm samples.
- ◆ Host based sensors can only cover limited IP space, which has scalability issues. Thus they might not be able to detect the worm in its early stage.

Network IDSs



- ◆ Deploying sensors at strategic locations
 - For example, Packet sniffing via *tcpdump* at routers
- ◆ Inspecting network traffic
 - Watch for violations of protocols and unusual connection patterns
 - Look into the packet payload for malicious code
- ◆ Limitations
 - Cannot execute the payload or do any code analysis !
 - Even DPI gives limited application-level semantic information
 - Record and process huge amount of traffic
 - May be easily defeated by encryption, but can be mitigated with encryption only at the gateway/proxy

Host-based vs. Network-based IDS

- ◆ Give an attack that can only be detected by host-based IDS but not network-based IDS

- ◆ Can you give an example only be detected by network-based IDS but not host-based IDS ?

Key Metrics of IDS/IPS

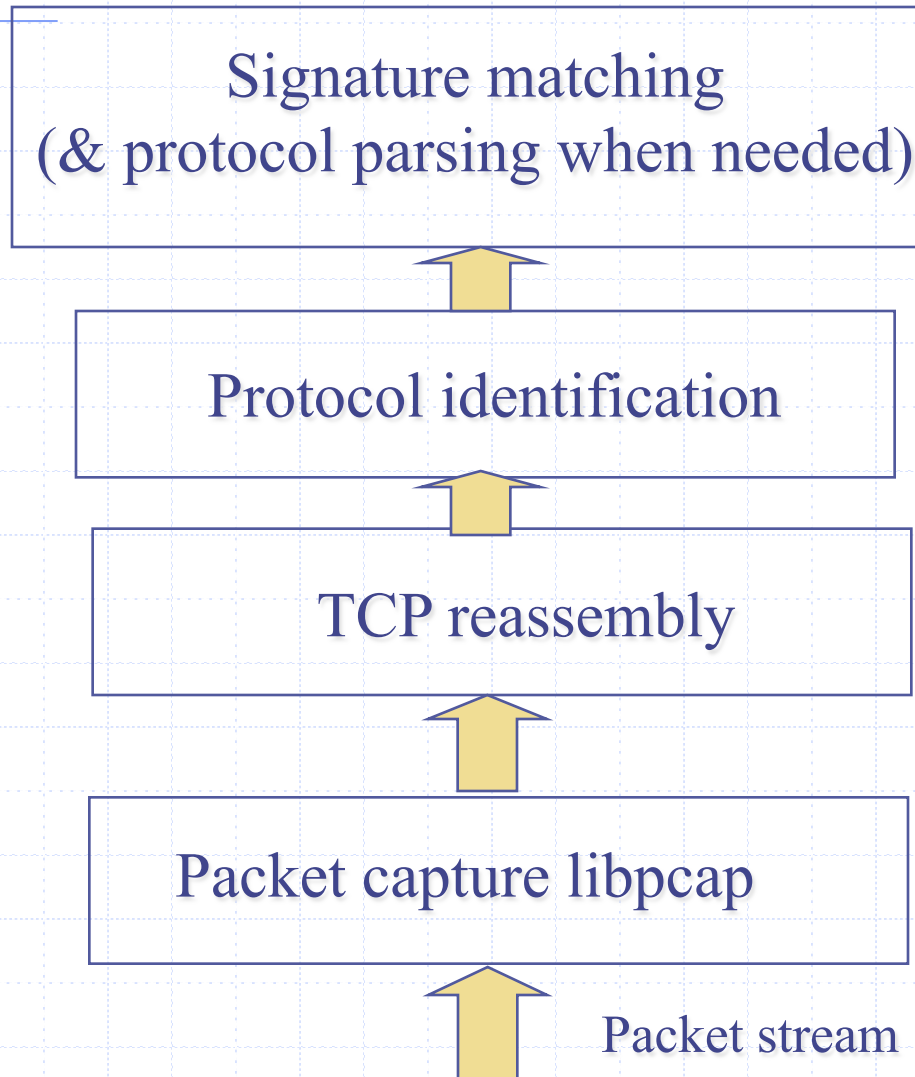
◆ Algorithm

- Alarm: A ; Intrusion: I
- Detection (true alarm) rate: $P(A|I)$
 - ◆ False negative rate $P(\neg A|I)$
- False alarm (aka, false positive) rate: $P(A|\neg I)$
 - ◆ True negative rate $P(\neg A|\neg I)$

◆ Architecture

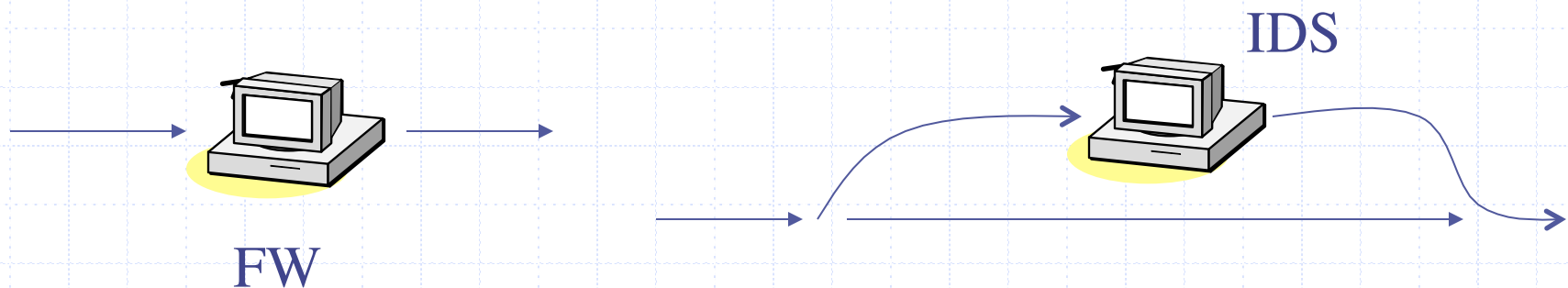
- Throughput of NIDS, targeting 10s of Gbps
 - ◆ E.g., 32 nsec for 40 byte TCP SYN packet
- Resilient to attacks

Architecture of Network IDS

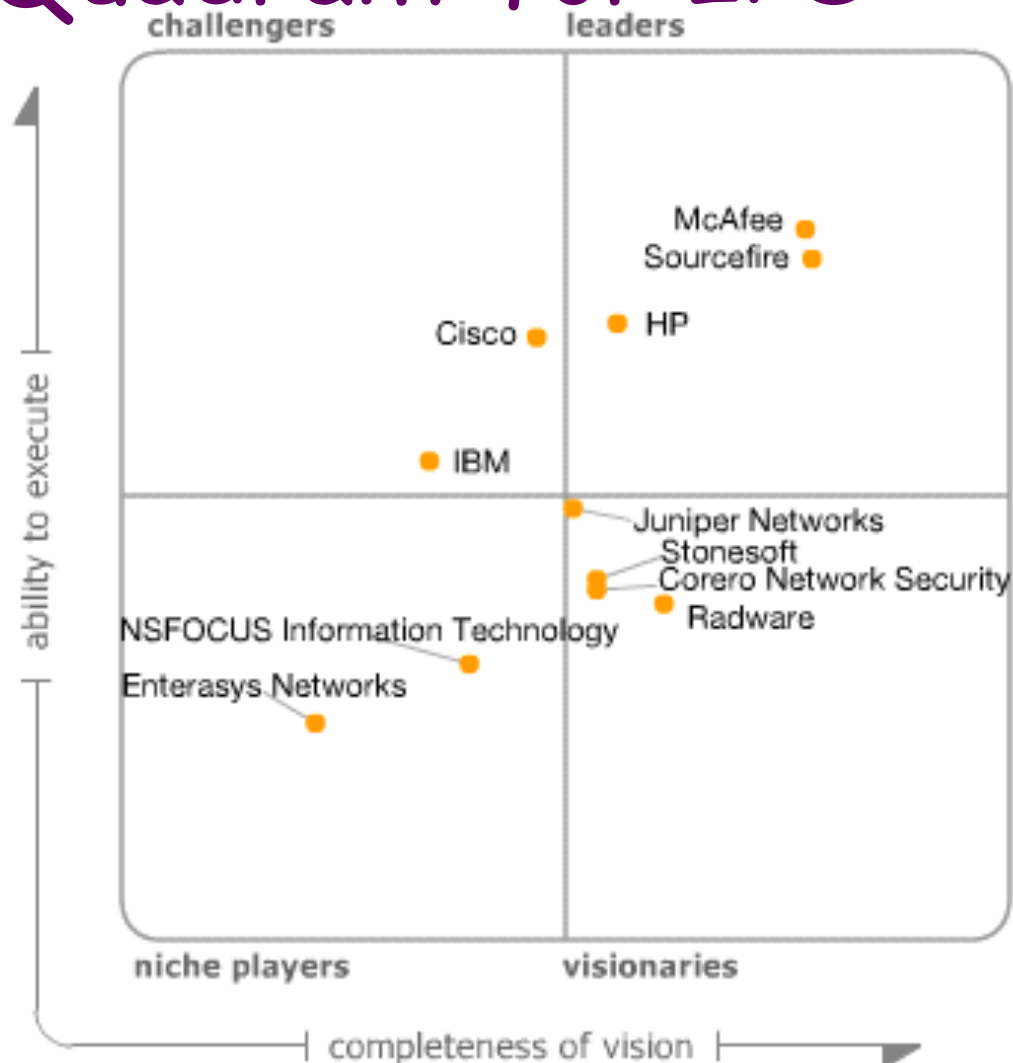


Firewall/Net IPS VS Net IDS

- ◆ Firewall/IPS
 - Active filtering
 - Fail-close
- ◆ Network IDS
 - Passive monitoring
 - Fail-open



Gartner Magic Quadrant for IPS



As of July 2012

Ability to Execute

- Product/Service
- Overall Viability (Business Unit, Financial, Strategy, Organization)
- Sales Execution/Pricing
- Market Responsiveness and Track Record
- Marketing Execution
- Customer Experience
- Operations

Completeness of Vision

- Market Understanding
- Marketing Strategy
- Sales Strategy
- Offering (Product) Strategy
- Business Model
- Vertical/Industry Strategy
- Innovation
- Geographic Strategy

- 
- ◆ Firewalls
 - ◆ Intrusion Detection System (IDS)
 - ◆ **Social Network**

Outline

- ◆ **Overview of Online Social Networking**
- ◆ **Threats and Attacks**
- ◆ **Defense Measures**

Online Social Networking (OSN)

- ◆ Online Web services enabling people to connect with each other, share information
 - Common friends, interests, personal info, ...
 - Post photos, videos, etc. for others to see
 - Communicate via email, instant message, etc.
- ◆ Major OSN services: Facebook, Twitter, MySpace, LinkedIn, etc.

Click Around. **Chrome fast.**



Get Chrome
The browser by Google >>

Today on MySpace

Tuesday, May 25, 2010

Cool New Videos



Robot Leads Wedding



Onion: President Lip-Syncing?



Blazing Fast Turtle Race

More Video

- [MySpace Video: Your Source for Great Videos](#)
- [Primetime: Catch Up with Your Favorite TV Shows](#)
- [Family Guy: Stewie is Still Set on World Domination](#)
- [Lost: The Epic Comes to an End](#)
- [The Simpsons: Do the Bartman](#)

Top Searches

[Family Guy](#) • [Glee](#) • [Saturday Night Live](#) • [The Twilight Saga: Eclipse](#) • [TMZ](#) • [E! News](#) • [Lady Gaga](#)
[Fuel TV](#) • [Justin Bieber](#) • [Miley Cyrus](#)

Log In

Sign Up!

Email:

Password:

Log In

Remember Me

[Forgot your password?](#)

Find Your Friends on MySpace

Find or browse members:

Search by name or email

Go

[Sponsored Links](#)

Blue4U

Breaking Up Is Hard To Do. Let
Blue4U Make It Better.

BlueKC.com/Blue4U

“MySpace is a place for friends.”

“MySpace is Your Space.”

“MySpace keeps you connected.”

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and anyone can join

First Name:

Last Name:

Your Email:


New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

[Create a Page for a celebrity, band or business.](#)



do you have a facebook?

“Giving people the power to share and make the world more open and connected.”



Search for a keyword or phrase...

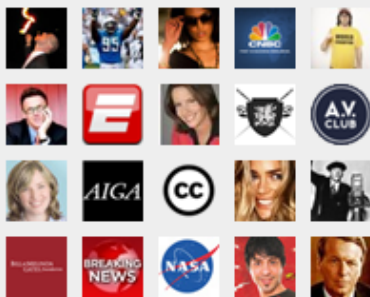
Search

Have an account? [Sign in](#)

Discover what's happening right now, anywhere in the world





KEY LINEにロコなう。 Pinoy Housemates Cnectd Geek Pride Paul Gray Lost finale Oil Spill TRENDING TOPIC

See who's here



Friends and industry peers you know. Celebrities you watch. Businesses you frequent. Find them all on Twitter.

Top Tweets [View all >](#)

-  **OMGihatethat** when teachers get off track and tell you stories about their life. #omgiLOVEthat
17 hours ago
-  **OfficialPantera** RIP Paul Grey of Slipknot. Another loss to the metal community. <http://bit.ly/9J9LVd>
19 hours ago
-  **nodoubt** Back in the studio again this week, the vibe here reminds me of recording sessions for TK and ROS and Rock Steady. Good times! -Tom
19 hours ago
-  **kingsully** Why am I watching Lindsey Lohan on CNN when there are

New to Twitter?



Twitter is a rich source of instant information. Stay updated. Keep others updated. It's a whole thing.

[Let me in >](#)

Customize Twitter by choosing who to follow. Then see tweets from those folks as soon as they're posted.

Using Twitter for a business? Check out [Twitter 101](#)



“Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick frequent answers to one simple question:

What are you doing?”

Over 65 million professionals use LinkedIn to exchange information, ideas and opportunities



Stay informed about your contacts and industry



Find the people & knowledge you need to achieve your goals



Control your professional identity online

Join LinkedIn Today

First Name:

Last Name:

Email:

Password:

6 or more characters

*

Already on LinkedIn? [Sign in.](#)

Search for someone by name:

LinkedIn member directory: [a](#) [b](#) [c](#) [d](#) [e](#) [f](#) [g](#) [h](#) [i](#) [j](#) [k](#) [l](#) [m](#) [n](#) [o](#) [p](#) [q](#) [r](#) [s](#) [t](#) [u](#) [v](#) [w](#) [x](#) [y](#) [z](#) [more](#) | [Browse members by country](#)

* By clicking Join Now, you are indicating that you have read, understood, and agree to LinkedIn's [User Agreement](#) and [Privacy Policy](#).



“Your professional network of trusted contacts gives you an advantage in your career, and is one of your most valuable assets. LinkedIn exists to help you make better use of your professional network and help the people you trust in return.”

The tastiest bookmarks on the web.
Save your own or see what's fresh now!



[? Learn More](#)

HIDE INTRO 

Search the biggest collection of bookmarks in the universe...

Search Delicious

Search

Fresh Bookmarks

Hotlist

Explore Tags

The freshest bookmarks that are flying like hotcakes on Delicious and beyond.

[See more recent bookmarks](#) 

New bookmarks saved in the last minute **2** **1** **0**

 [What Happens to a YouTube Video After 1,000 Uploads?](#) SAVE

via mashable.com

11

[art](#) [youtube](#) [video](#) [compression](#) [repeat](#)

[▶ 13 Related Tweets](#)

“Delicious is a Social Bookmarking service, which means you can save all your bookmarks online, share them with other people, and see what other people are bookmarking.”



licensed under  Attribution-NonCommercial-ShareAlike 2.0 Germany | Ludwig Gatzke | <http://flickr.com/photos/stabilo-boss/>

OSN Popularity

- ◆ Over 900 million Facebook users worldwide
 - Over 150 million in U.S.
 - Over 450 million access via mobile
 - 300 million pictures uploaded to Facebook daily
- ◆ Over 140 million Twitter users; over 340 million Tweets sent daily
- ◆ Over 175 million LinkedIn members in over 200 countries

Benefits of OSN Communication

- ◆ Vast majority of college students use OSNs
 - Organizations want to market products, services, etc. to this demographic
 - OSNs can help them reach these potential buyers
- ◆ OSNs provide communal forum for expression (self, group, mass), collaboration, etc.
 - Connect with old friends, find new friends and connect
 - Play games with friends, e.g., Mafia Wars, Scrabulous
 - Commerce in “virtual items”
- ◆ But using OSNs poses security issues for orgs as well as individuals

Outline

- ◆ Overview of Online Social Networking
- ◆ **Threats and Attacks**
- ◆ Defense Measures

OSN Security Threats/Attacks

- ◆ Malware distribution
- ◆ Cyber harassment, stalking, etc.
- ◆ Information “shelf life” in cyberspace
- ◆ Privacy issues:
 - Information about person posted by him/herself, others
 - Information about people collected by OSNs
- ◆ Information posted on OSNs impacts unemployment, insurance, etc.
- ◆ Organizations’ concerns: brand, laws, regulations

OSN Malware Distribution

- ◆ Best-known example: Koobface [9–10]
 - Worm masquerading as Adobe Flash Player update
 - Starting in 2009, OSN users enticed to watch “funny video”, then conned into “updating” Flash
 - Koobface connected infected computers to botnet, served machines ads for fake antivirus software
 - Estimated 400,000–800,000 bots in 2010
 - Facebook outed gang behind Koobface in Jan. 2012, bot server shut down
- ◆ Other third-party apps on OSNs like Facebook may contain malware (if not vetted)
- ◆ Not to mention hoaxes, “chain letters,” and other cons

OSN 3rd Party Applications

- Games, quizzes, “cute” stuff
- Untested by Facebook – anyone can write one...
- No Terms and Conditions – either allow or deny
- Installation gives developers rights to look at your profile and overrides your privacy settings!

*There's a sucker born every minute.
–P.T. Barnum*

Hugged



How Mysterious A...

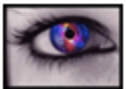


★★★★★
No Category

Country Life



What color is yo...



★★★★★
No Category

Mood Stones



★★★★★
Lifestyle

What will happen...



★★★★★
Entertainment

Huggles



★★★★★
No Category

FishVille



★★★★★
Games

OSN Stalking, Harassment, etc.

- ◆ Bullies, stalkers, etc. harass people via OSNs
 - High-profile example: Megan Meier's suicide [11–12]
 - ◆ 13-year old Meier killed herself after chatting on MySpace with a 16-year-old boy who made degrading remarks
 - ◆ The "boy" was a fake account set up by Lori Drew, mother of Meier's ex-friend
 - ◆ Drew found guilty of violating Computer Fraud and Abuse Act in 2008; acquitted in 2009
 - ◆ Most U.S. states have since criminalized cyber harassment, stalking, etc.
 - OSNs (and their members) have played similar roles in mistreating people

OSN Information “Shelf Life”

- ◆ Common sense: it's very difficult to delete information after it's been posted online
- ◆ Indiscreet information can adversely affect college admissions, employment, insurance, etc. [5]
- ◆ Twitter gave its entire archive to Library of Congress in 2010 [13]

The Joy of Tech™

by Nitrozac & Snaggy



Signs of the social networking times.

Originally posted in [2].

OSN Information Privacy (1)

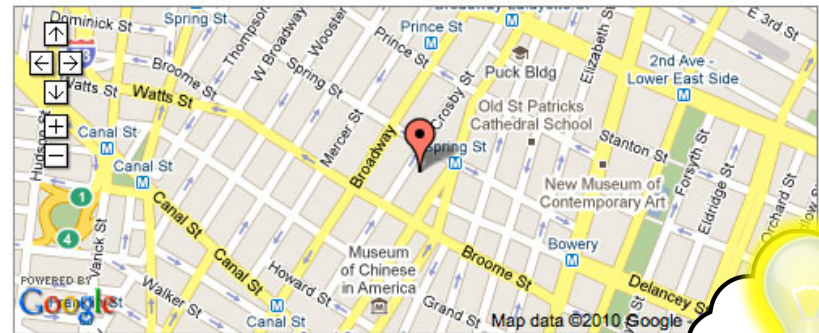
◆ Information posted on OSNs is generally public

- Unless you set privacy settings appropriately
- “I’ll be on vacation” post plus geolocation invites burglars, i.e., “Please Rob Me” [14]

◆ Indiscreet posts can lead to nasty consequences

Home
New York, NY 10012

Source: [14]



Map from [14];
other images
public domain



OSN Information Privacy (2)

- ◆ Employers, insurers, college admissions officers, et al. already screen applicants using OSNs
- ◆ Recent report from Novarica, research consultancy for finance and insurance industries:

“We can now collect information on buying behaviors, geospatial and location information, social media and Internet usage, and more...Our electronic trails have been digitized, formatted, standardized, analyzed and modeled, and are up for sale. As intimidating as this may sound to the individual, it is a great opportunity for businesses to use this data.” (quoted in [5])

OSN Information Privacy (3)

◆ Posts that got people fired:

- Connor Riley: “Cisco just offered me a job! Now I have to weigh the utility of a [big] paycheck against the daily commute to San Jose and hating the work.”
- Tania Dickinson: compared her job at New Zealand development agency to “expensive paperweight”
- Virgin Atlantic flight attendants who mentioned engines replaced 4 times/year, cabins with cockroaches

URL Shorteners

- ◆ bit.ly, TinyUrl, ReadThisURL, NotLong
- ◆ Hides the true destination URL – hard to tell where you're going until you click!

**`http://www.evil.com/badsite?%20infect-
your-pc.html`**

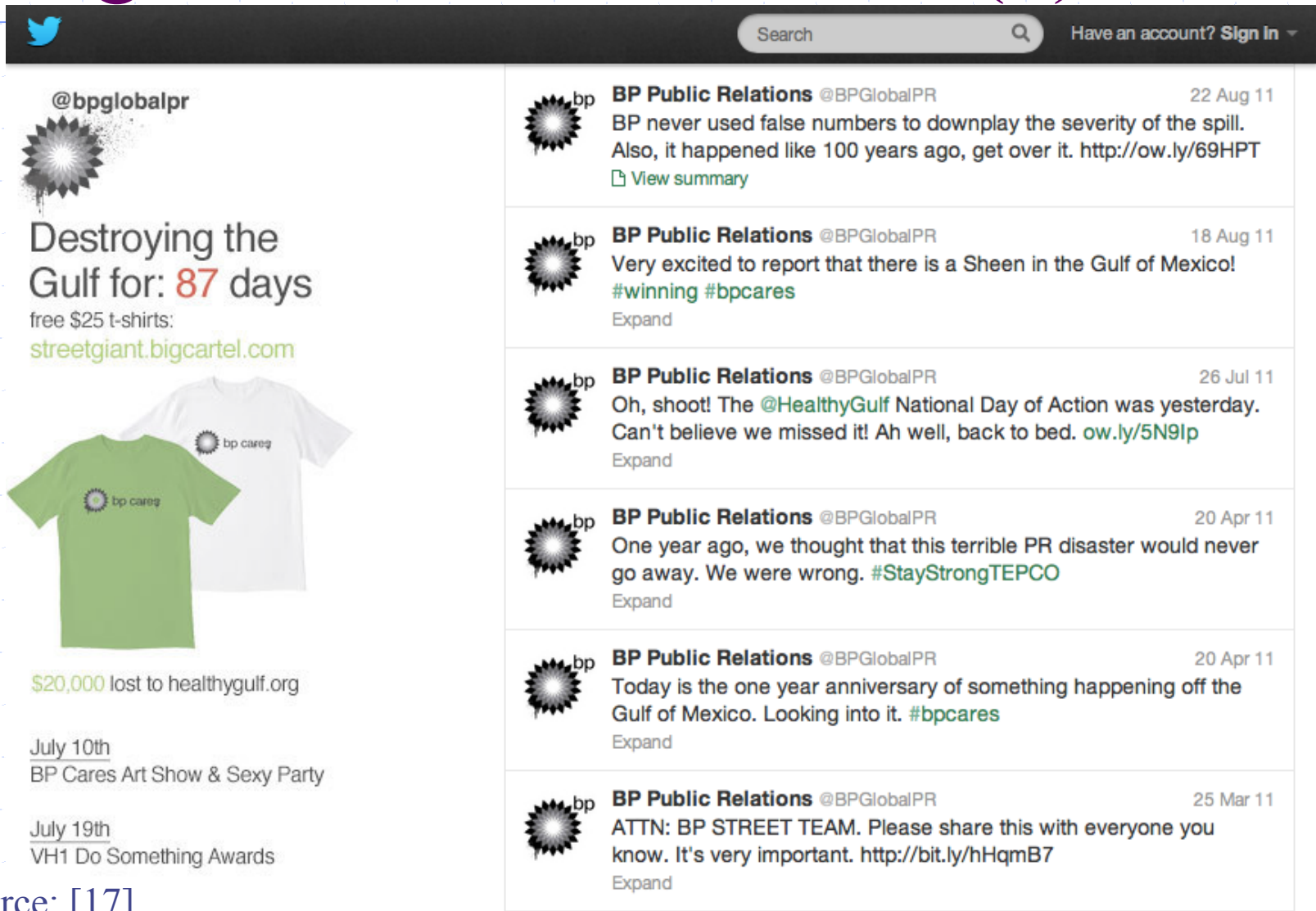
is now

`http://bit.ly/aaI9KV`

Organizations and OSNs (1)

- ◆ Organizations subject to attacks via OSNs
 - Defamation, damage to org. brand, TM
 - Unauthorized people posting on behalf of org.
 - Negative media coverage, reputation damage
- ◆ Case study: BP oil spill fallout [1]
 - Summer 2010: *Deepwater Horizon* spill (87 days)
 - BP's public relations didn't cover OSNs well
 - Angry citizens post on OSNs (@BPglobalPR had 179,000 followers)
 - BP logo "remixed" as oil spill; negative press coverage


Organizations and OSNs (2)




The image shows a screenshot of a Twitter profile for @bpglobalpr. The profile header includes the Twitter logo, the handle @bpglobalpr, a profile picture of a sunburst, and a bio: "Destroying the Gulf for: 87 days free \$25 t-shirts: streetgiant.bigcartel.com". Below the bio are two t-shirts, one green and one white, both with the "bp cares" logo. The tweet list on the right contains six tweets from "BP Public Relations @BPGlobalPR" with dates ranging from 25 Mar 11 to 22 Aug 11. The tweets discuss the Gulf of Mexico spill, the anniversary of the spill, and the BP Cares program.

@bpglobalpr

Destroying the Gulf for: 87 days
free \$25 t-shirts:
streetgiant.bigcartel.com

 bp cares

 bp cares

\$20,000 lost to healthygulf.org

July 10th
BP Cares Art Show & Sexy Party

July 19th
VH1 Do Something Awards

BP Public Relations @BPGlobalPR 22 Aug 11
BP never used false numbers to downplay the severity of the spill. Also, it happened like 100 years ago, get over it. <http://ow.ly/69HPT>
[View summary](#)

BP Public Relations @BPGlobalPR 18 Aug 11
Very excited to report that there is a Sheen in the Gulf of Mexico!
[#winning](#) [#bpcares](#)
[Expand](#)

BP Public Relations @BPGlobalPR 26 Jul 11
Oh, shoot! The [@HealthyGulf](#) National Day of Action was yesterday. Can't believe we missed it! Ah well, back to bed. ow.ly/5N9lp
[Expand](#)

BP Public Relations @BPGlobalPR 20 Apr 11
One year ago, we thought that this terrible PR disaster would never go away. We were wrong. [#StayStrongTEPCO](#)
[Expand](#)

BP Public Relations @BPGlobalPR 20 Apr 11
Today is the one year anniversary of something happening off the Gulf of Mexico. Looking into it. [#bpcares](#)
[Expand](#)

BP Public Relations @BPGlobalPR 25 Mar 11
ATTN: BP STREET TEAM. Please share this with everyone you know. It's very important. <http://bit.ly/hHqmB7>
[Expand](#)

Organizations and OSNs (3)

- ◆ Orgs. have to comply with laws, regulations that OSNs complicate [1]
 - FERPA, HIPAA, Sarbanes-Oxley, etc.
 - Protecting children's privacy online (due care)
- ◆ Ethical issues abound: [1]
 - Should faculty "friend" students?
 - Should a boss "friend" his/her employees?

Outline

- ◆ Overview of Online Social Networking
- ◆ Threats and Attacks
- ◆ **Defense Measures**

Personal Defense Measures (1)

- ◆ “Common sense” measures: [1]
 - Use strong, unique passwords
 - Provide minimal personal information: avoid entering birthdate, address, etc.
 - Review privacy settings, set them to “maximum privacy”
 - ◆ “Friends of friends” includes far more people than “friends only”
 - Exercise discretion about posted material:
 - ◆ Pictures, videos, etc.
 - ◆ Opinions on controversial issues
 - ◆ Anything involving coworkers, bosses, classmates, professors
 - ◆ Anything related to employer (unless authorized to do so)
 - Be wary of 3rd party apps, ads, etc. (P.T. Barnum’s quote)
 - Supervise children’s OSN activity

Personal Defense Measures (2)

◆ More advice [1]:

- “If it sounds too good to be true, it probably is”
- Use browser security tools for protection:
 - ◆ Anti-phishing filters (IE, Firefox)
 - ◆ Web of Trust (crowdsourced website trust)
 - ◆ Adblock/NoScript/Do Not Track Plus
- Personal reputation management:
 - ◆ Search for yourself online, look at the results...
 - ◆ Google Alerts: emails sent daily to you about results for any search query (free), e.g., your name
- Extreme cases:
 - ◆ Cease using OSNs, delete accounts
 - ◆ Contact law enforcement re. relentless online harassment



If you agree that Facebook doesn't respect you, your personal data or the future of the web, you may want to join us.

WE'RE QUITTING FACEBOOK

May 31
2010

[Why are we quitting?](#)

[What should I know?](#)

[What are my options?](#)

[Send me a reminder](#)

Sick of Facebook's lack of respect for your data? Add your name and commit to quit!

Change language ▾

COMMIT TO QUIT

40295

**Committed Facebook
Quitters**

ShareThis 36K

Why are we quitting?

For us it comes down to two things: [fair choices](#) and [best intentions](#). In our view, Facebook doesn't do a good job in either department. Facebook gives you choices about how to manage your data, but [they aren't fair choices](#), and while the onus is on the individual to manage these choices, [Facebook makes it damn difficult](#) for the average user to understand or manage this. We also don't think Facebook has much respect for you or your data, especially in the context of the future.

For a lot of people, quitting Facebook revolves around privacy. [This is a legitimate concern](#), but we also think the privacy issue is just the symptom of a [larger set of issues](#). The cumulative effects of what Facebook does now will not play out well in the future, and we care deeply about the future of the web as an open, safe and human place. We just can't see Facebook's current direction being aligned with any positive future for the web, so we're leaving.

What should I know?

[Quitting Facebook](#) isn't easy. Facebook is engaging, enjoyable and quite frankly, addictive. Quitting something like

Dealing with Shortened URLs

- ◆ Many 3rd party online services “un-shorten” URLs:
 - unshorten.me
 - unshorten.it
 - ...
- ◆ Some services have browser extensions
- ◆ Can unshorten URLs using cURL [18], [19]
 - Idea: follow “Location:” HTTP headers
- ◆ Common sense: think before you click

Organizational Defense Measures (1)

- ◆ Organizational defense is more complicated:
 - Monitoring employees' use of OSNs
 - Monitoring org's name, logo appearance on OSNs
 - Responding to attacks on org. in a timely manner
- ◆ Encompasses all parts of an org., not just IT dept!
- ◆ This usually entails: [1]
 - Crafting social media policy, disseminating to employees
 - Hiring/training staff to manage org. presence on OSNs (with management oversight)
 - Monitoring and reporting employee use of social media
 - ...

Organizational Defense Measures (2)

◆ One defense approach: the HUMOR matrix [1]

| Category | Description |
|---|--|
| Human Resources | Human Resources provide companywide policies, procedures, and guidance on acceptable employee use of authorized social media tools. These guidelines and policies provide the correct processes for utilization of social media in all areas of the company, including Marketing and Information Technology. |
| Utilization (of Resources and Assets) | Utilization defines the capabilities of secure social media tactics and how these tactics are implemented across technologies and policies to protect a company's resources and assets. |
| Monetary (Considerations) | The monetary resources dedicated to creating a social media strategy and tactics as well as a security strategy have to be aligned to best serve the company. |
| Operations (Management) | Operations management is the day-to-day processes that must be followed to implement a security framework, from a technology perspective, as well as from an ongoing maintenance perspective. The objective is to ensure that social media is handled securely as technologies and social media platforms change. |
| Reputation (Management) | When all interaction scenarios with social media are calculated, the company's reputation ultimately benefits. Reputation management is the result of good or bad implementations of social media strategies as well as tactical decisions and provides a monitoring and reporting function that helps to maintain an acceptable level of security and policies over time. |

Source: [1],
Table 1.1

Organizational Defense Measures (3)

- ◆ The HUMOR matrix specifies social media security outcomes, tracks org.'s current status and performance goals over time [1]
 - Outcomes can include employee training regimen, level of employee monitoring, protection of org.'s IP, etc.
- ◆ Feedback loop: org. takes action to reach goals, assesses progress periodically (e.g., every 6 mo.)

Organizational Defense Measures (4)

- ◆ Example tools: [1], [20]
 - Google Alerts (emails as “search query” appears online)
 - HowSociable (shows mention of org. name/brand on OSNs)
 - SocialGO (create your org.’s own social network)
 - Tech//404 Data Loss Calculator (self-explanatory)
 - Chartbeat (monitor customer engagement on website)
 - EventTracker (monitors employee activity)
 - Many more...