

ECE 455: CYBERSECURITY

Lecture #0

Daniel Gitzel

Dan's Introduction

- **Cooper Grad**

- BEng EE'14 MEng EE'16
- OS, Computer Security, Software Track

- **Day Job**

- SWE / Quant at Hedge Fund
- C++/Java and Python developer (lots and lots of debugging)
 - Numerical stuff
- High-availability systems (downtime \$\$\$!)

Dan's Introduction

- **Why teach this class?**
 - Computer Security needed a little modernization
 - It's fascinating!
 - Some experience in secure development from Finance industry
 - But that's just a tiny, tiny slice of the field
 - So... Two-way learning!
 - Exploring the space with graduate students

Announcements

- **Class survey**
- **Read paper for discussion next week**
 - Will be posted on Teams

What is Cybersecurity?

- **Fancy name!**
- **Detect or prevent unwanted use of computer systems, networks, or data**

Why Security?

Grabbing news headlines! Scary!?



Why security?

More Recent Headlines:

The SolarWinds hack timeline: Who knew what, and when?

New Pegasus zero-click iPhone attack defeats Apple's Blastdoor protections

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

Why should you care?

- **Impacts everyone's day-to-day life**

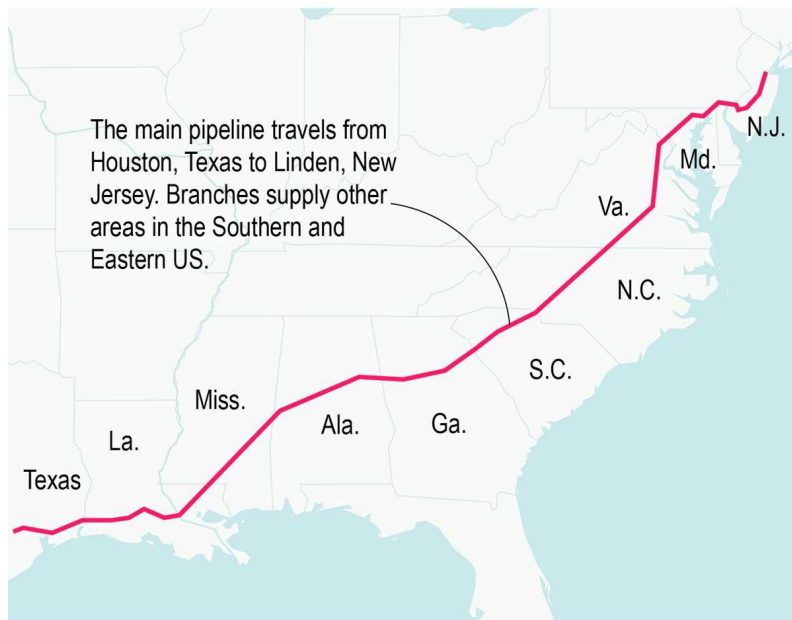
- Millions of compromised computers (bots)
- Millions of stolen passwords (hacks)
- Millions of dollars in damage (fraud)



It is important for our...

- **Physical safety and safety of our possessions**
- **Confidentiality of data/privacy**
- **Functionality and availability of infrastructure**

Pipeline spans more than 5,500 miles



Source: Colonial Pipeline

AP

Safety

It's not just for PC and phones! Everything is a computer now.

**The FDA Is Recalling Medtronic Insulin Pumps
For Hacking Concerns**

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

**HACKERS
REMOTELY KILL
A JEEP ON THE
HIGHWAY—
WITH ME IN IT**

Business

**FBI probe of alleged plane hack sparks
worries over flight safety**

Privacy/confidentiality

We've trusted companies and others with financial, medical, and personal data.

91% OF HEALTHCARE ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THE LAST FIVE YEARS.

By elxradmin Posted May 29, 2015 In health IT, security

   0

After huge Equifax breach, CEO “retires”

Board is "deeply concerned about and totally focused on the cybersecurity incident."

CYRUS FARIVAR - 9/26/2017, 6:42 AM

Can affect a country's economy...

- **Cyber warfare**

- 23 December 2015
- First known cyberattack on a power grid
- Three energy distribution companies compromised
- 230,000 without power for 1 to 6 hours

wired.com

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

Author: Kim ZetterKim Zetter

...or it's security

The New York Times

U.S. Carried Out Cyberattacks on Iran

Israel Responds to Cyberattack With Airstrike

The weekend airstrike took out a building that was allegedly housing Hamas hackers. The incident underscores an ongoing debate in cybersecurity over how countries should respond to cyber attacks: Is an airstrike going too far?



Learn about security.

Make a **difference!**

Cybersecurity is not only important...

It can be FUN!



- **Unique challenge: can you stop the attacker?**
- **Blend of analytical thinking and engineering**

Cybersecurity is new and varied field

- **Cryptography**
- **Network security**
- **Operating systems security**
- **Web security**
- **Database security**
- **Distributed systems security**
- **Machine learning security**
- **Security usability**



Course Logistics

- **Class Schedule**

- Classes run from 6:00 to 8:50pm, Mondays
- One ~15 minute break

- **Office Hours**

- Virtual office hours, Thursdays 6:00 to 8:00pm

- **E-mail me with any questions**

Course Logistics

- **Absorb material presented in lectures**
- **Assignments**
 - ~4 homeworks (10%)
 - ~8 quizzes (30%)
 - Midterm (30%)
 - Final Project and Presentation (30%)

Teams and Google Group

- **Google Group**

- You've received an invite (@cooper address)
- Backup meeting place (if something happens to Teams)

- **Teams**

- Virtual Lectures and Office Hours
- Homework and paper assignments
- Project questions and discussion
- Other announcements (canceled class, rescheduling, etc.)

Class Policies

- All assignments are due at the start of lecture
- Late homework: **no credit**
- Late project: **-10% < 24hrs, -20% < 48hrs, -30% < 72hrs, no credit > 72hrs**
- Cite and attribute third party code (including fellow classmates)
- Missed exams or quizzes: **no credit**

Ethics

- **Do not cheat.** You learn nothing and hurt others.
- We will be discussing **attacks**
- **Not an invitation to snoop on fellow students**
 - Covered by Cooper Union policy, NY State, and Federal Law
- **Get informed consent when testing**
 - Notify all parties involved
 - Notify the instructor (me!)

Prerequisites

- **Required:**

- Communication Networks (ECE303)
- Operating Systems (ECE357)

- **Useful**

- C or assembly experience
- Javascript experience
- Working knowledge of command line utilities
- Discrete Math

- **Eagerness to learn!**

Textbooks

- **Required**

- Dieter Gollman's "Computer Security" 3rd edition

- **Optional**

- "Applied Cryptography" by Bruce Schneier
- "Cryptography Engineering" by Ferguson, Schneier, and Kohno
- "The Tangled Web" by Michal Zalewski
- "Practical Malware Analysis" by Sikorski and Honig

Fun Pop Culture

- **Books for fun**

- Little Brother, Cory Doctorow
- Cryptonomicon and REAMDE, Neal Stephenson
- The Art of Intrusion and The Art of Deception, Kevin Mitnick

- **Movies**

- Hackers
- Sneakers
- War Games

- **Historical “hackers”**

- The Codebreakers, David Kahn

BREAK

THREAT MODELS

Key Themes of this Course

- **How to **think** about security**
 - A new way of thinking: the “Security Mindset”
- **Technical aspects of security**
 - Vulnerabilities and attacks
 - Defensive technology
- **What this course is **not****
 - Not comprehensive
 - Not all about “latest and greatest” attacks
 - Not a course on “hacking” or “cracking”

Threat models

- **Systems Fail for many reasons:**
 - *Reliability* deals with accidental failures
 - *Usability* deals with operational/user interaction failures
 - *Security* deals with *intentional* failures
 - Created by intelligent adversary
 - Always consider the adversary in the computing environment
 - All three are related!

Threat models

- **Cannot protect against all possible attacks**
- **High-level goal is risk management**
 - Much of the effort concerns *raising the bar* and *trading off resources*
 - How to *prudently* spend time and money?
- **Key notion of threat model: what are you defending against?**
 - Determines which defenses are worthwhile

Example (from physical security)

Which one would you use for \$1,000? For \$100,000? For \$100,000,000?



Example (from physical security)

- **Analysis can get very detailed**
 - Security is all about the details
 - Mechanical vs. Electronic locks
 - Batteries? Power outage? Change combination?
 - Types of steel plate and cobalt layers
 - Steel conducts heat.



Security Mindset

- **Think critically, challenge assumptions!**
 - Curiosity is the first step, creativity is the second
 - “That new smart-lock sounds awesome, I can’t wait to use it!”
 - “That smart-lock looks flashy, but I wonder what would happen if I did X...”
- **Technology changes, but the mindset remains important**
 - Informs better solutions and designs
 - Allows for a broader context: law, policy, and ethics

Another Example

What do you see?



Another Example

What do you see?

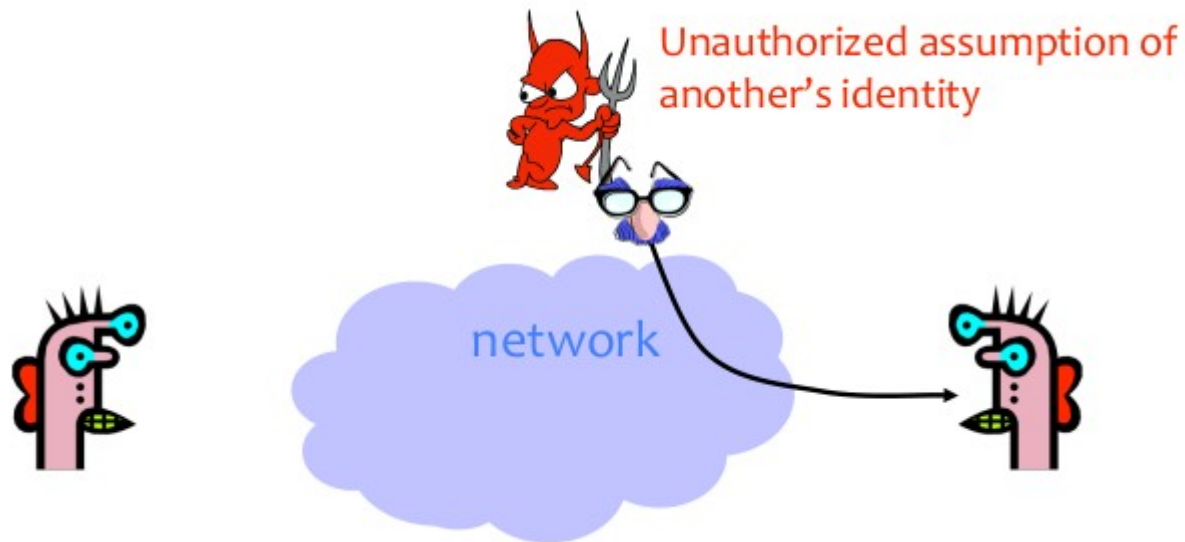


Security Goals

Goal	Threat
Authenticity	Spoofing
Integrity	Tampering
Non-repudiability	Repudiation
Confidentiality	Disclosure
Availability	Denial of Service
Authorization	Elevation of Privilege

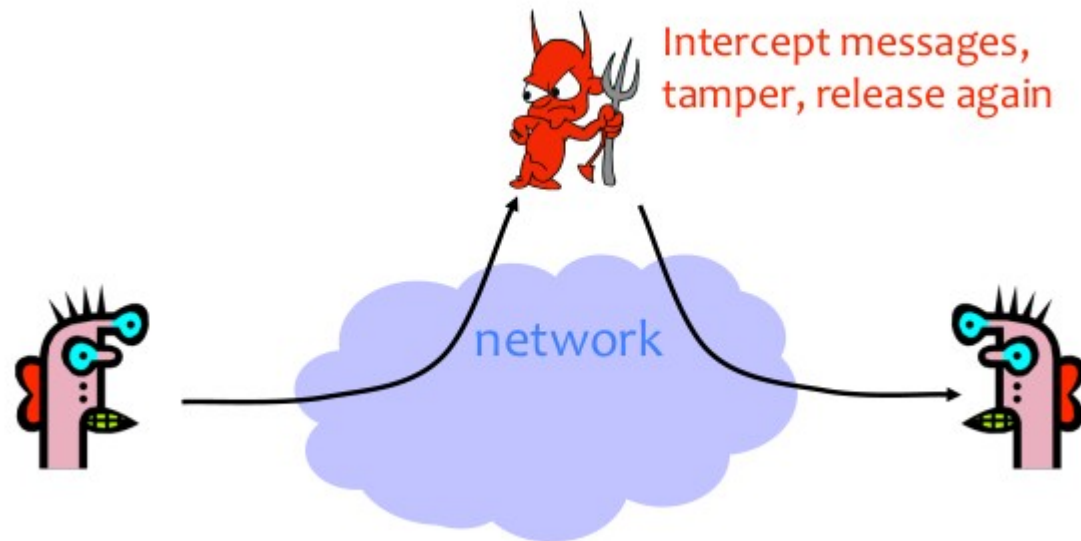
Security Goals

Authenticity is knowing who you're talking to.



Security Goals

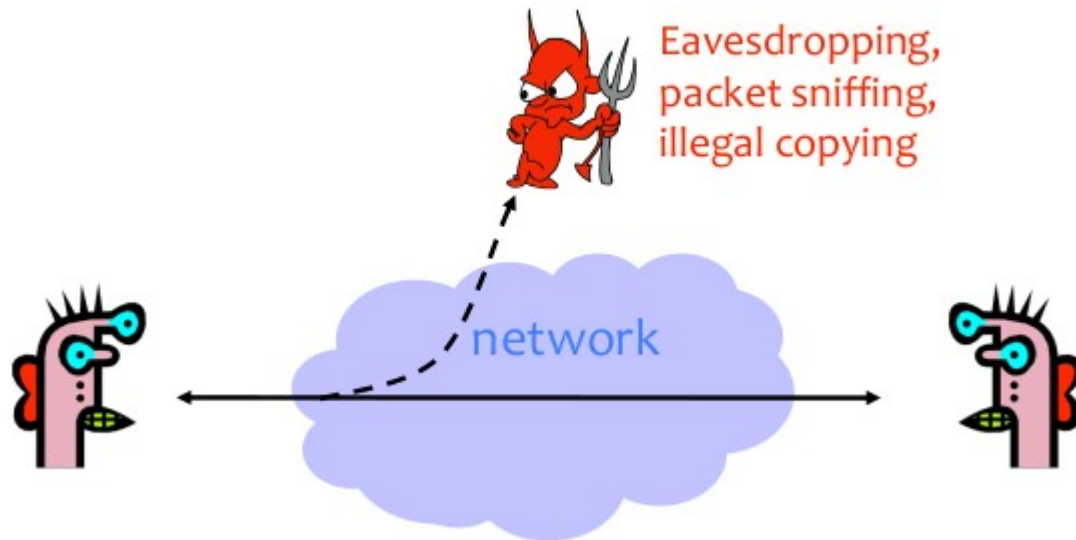
Integrity is the prevention of unauthorized changes.



Non-repudiation associates a user with a specific action in a way that cannot be denied.

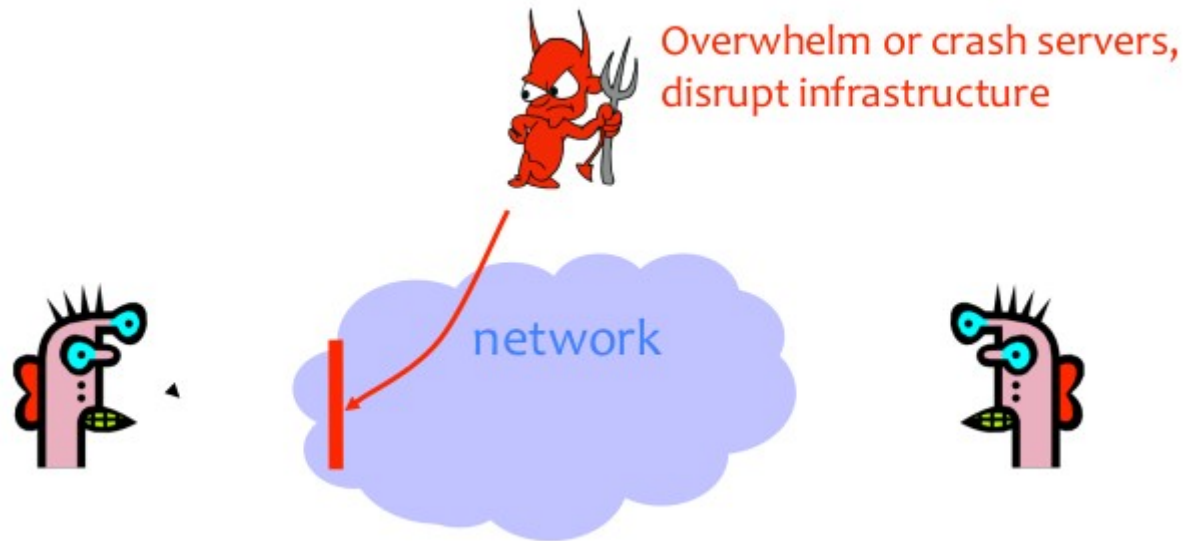
Security Goals

Confidentiality is concealment of information.



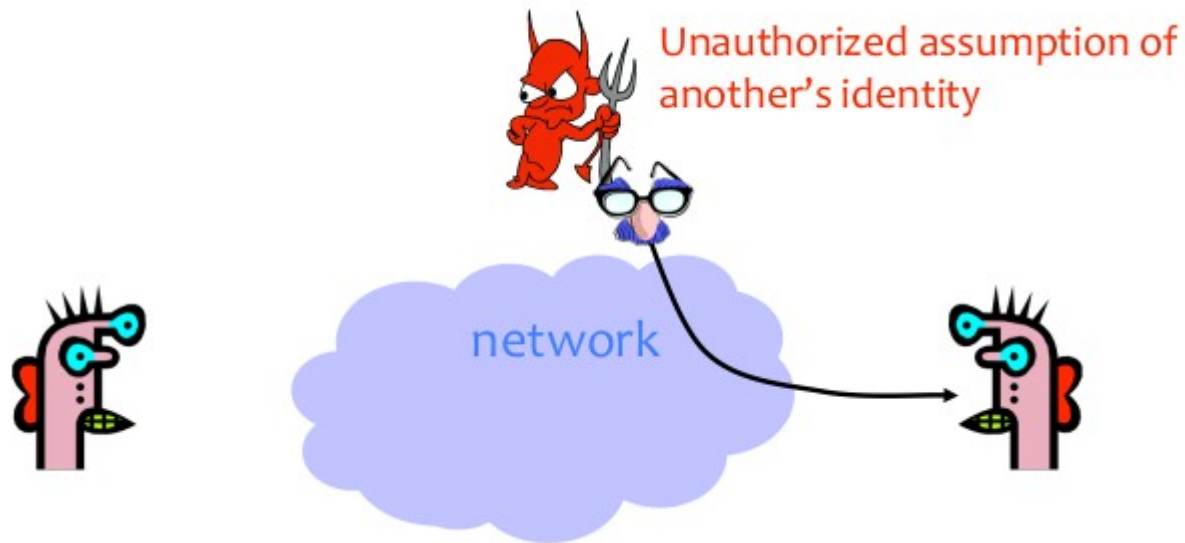
Security Goals

Availability is ability to use information or resources.



Security Goals

Authorization grants the ability to perform an action.



Threat models

- **Assets**: what are we protecting? How valuable is this stuff?
- **Adversaries**: who is attacking, and why?
- **Vulnerabilities**: how might the system be weak?
- **Threats**: what actions would an adversary take?
- **Risk**: how important are the assets? How likely is the exploit? Economic incentives?
- Possible **defenses**

Approaches to Security

- **Prevention**

- Stop an attack

- **Detection**

- Detect an ongoing or past attack

- **Response**

- Respond to attacks
- The threat of response may deter attackers: “Beware of Dog”

Whole System is Critical

- **Securing a system involves a whole-system view**

- Cryptography
- Implementation
- People
- Physical security
- Everything in between!



- **Security on as strong as the weakest link**

- Why attack the strongest part? “Backdoor” or weak spots

Whole System is Critical



Asymmetry Advantage



Asymmetry Advantage

- **Attacker only needs a single weakness**
 - One kink in the armor and they can slip through
- **Defender's response**
 - Threat modeling
 - Defense in Depth
- **Trade-off**
 - Cost of defense
 - Value of assets
 - Attack cost/probability of success

From Policy to Implementation

- **Realizing a security policy has challenges:**
 - Requirement bugs
 - Conflicting or wrong goals
 - Design bugs
 - Poor use of cryptography
 - Poor source of randomness
 - Implementation bugs
 - Traditional software bugs
 - Usability
 - Can a normal human actually use this?

An ecosystem of participants

- **Many parties involved**

- System developers
- Companies/contractors deploying the system
- End users
- Adversaries

- **Each has a different goal**

- Developers might optimize for cost
- Companies/contractors might upsell extra features
- End users might want privacy, security, and usability

Strategies for Threat Modeling

- **Brainstorming**

- Scenario Analysis: common scenarios from experience or history
- Pre-mortem: assume the system failed. Why and where did it break?

- **Structured Approaches**

- Protect Assets: “follow the money” what do attackers want and how can they get to it. Map the system.
- Identify Attackers: who are they and what can they do? Map possible entry and escalation points.
- Focus on Software: model the software system. Understand APIs and data models. Expose complexity and assumptions.

Diagram Models for Software

- **Data Flow**

- API definitions and callers
- Back-end architecture (DB, logs, backups)
- Network topology
- Swim Lanes (TCP is a classic example)

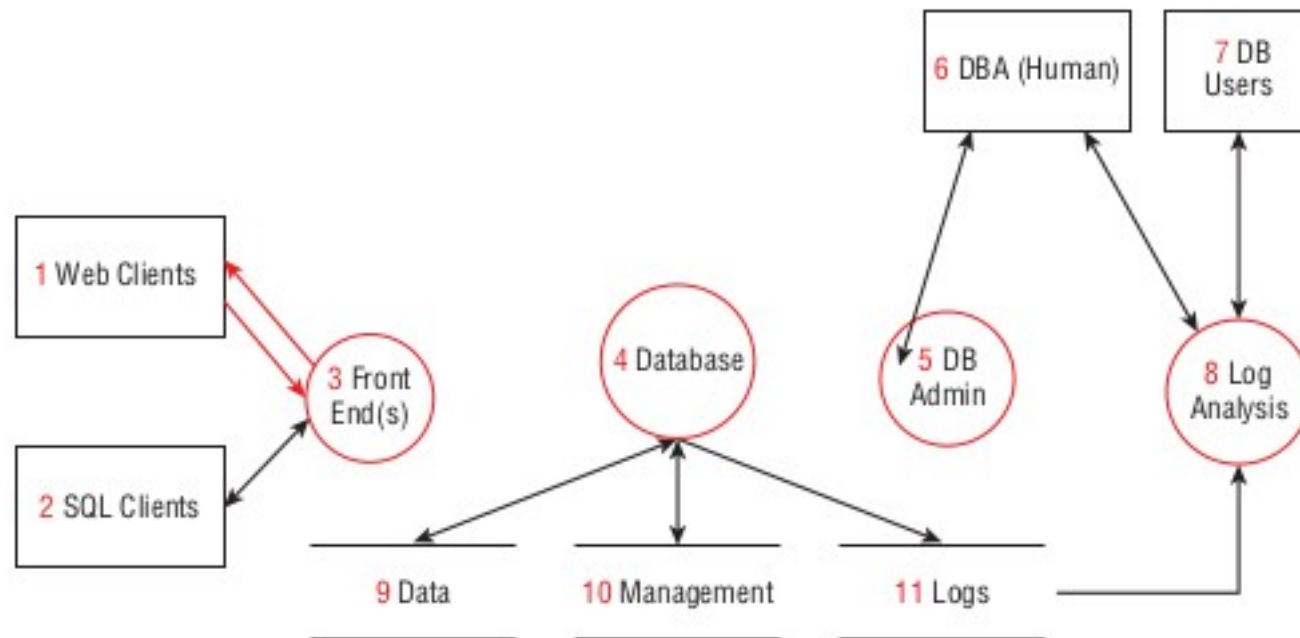
- **State diagrams**

- Track side-effects

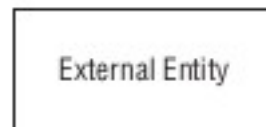
What to Include

- **Events (drive state changes)**
- **Processes**
 - Input and outputs (req. and resp.)
- **Data Sources**
 - Used to generate outputs
- **Recipients**
 - Where do the replies go?

Example Data Flow Diagram



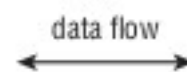
Key:



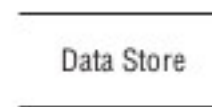
External Entity



Process



data flow



Data Store

Validating Diagrams

- **Walk through the diagram**
 - Can you talk through it?
 - Did you make changes while explaining?
 - Did you refer to something not in the diagram?
- **Watch for ambiguity**
 - “Sometimes X but also Y” means more detail is required
 - We usually serve this via HTTPS but sometimes we fall back to HTTP
 - DB aren’t sinks, show everyone who reads and writes
- **All processes must have input and output**

Using Diagrams

- **Good diagrams will show:**
 - The attack surface
 - All assets and how they are accessed and modified
 - Trust boundaries (where credentials are checked)

Finding Threats

- **What can go wrong?**
- **STRIDE**
 - Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege
 - Formalization of our Security Goals
- **Attack Trees**
 - Formalize attack sequences and risks
- **Attack Libraries**
 - Track and organize threats (CVE, OWASP)

STRIDE

Threat	Definition	Typical Victim	Examples
Spoofing	Pretending to be someone else	Processes, external entities, people	Claiming to be acme.com or a police officer
Tampering	Changing data on disk, memory or over network	Data stores, flows, and processes	Changing a spreadsheet, memory contents, or injecting packets
Repudiation	Claim you didn't do something	Processes, people	"I didn't order that", "I didn't push the button"
Info. Disclosure	Information leak	Processes, data stores, flows	Access to files, emails or databases, memory, disk
Denial of Service	Hoarding resources	Processes, data stores, people	Trick program into using up memory. Stall a person.
Elevation of Privilege	Doing something unauthorized	Process	Execute code as root

STRIDE

- **Applying STRIDE**

- Diagram your system
 - Show people, processes, data stores, flows and external entities
- For each S,T,R,I,D,E and each entity
 - Consider a threat
 - Check if you have one of each threat type for each entity
 - (Optionally, relax this check for certain entities)
- Expand or prune diagram and repeat

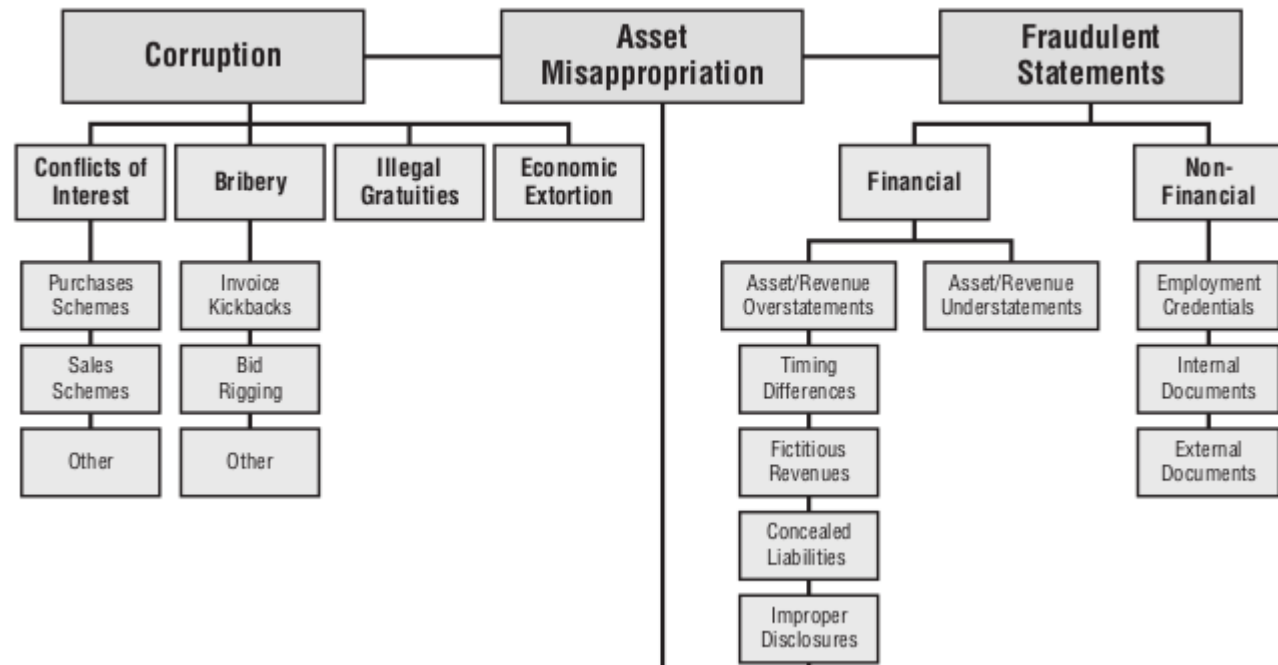
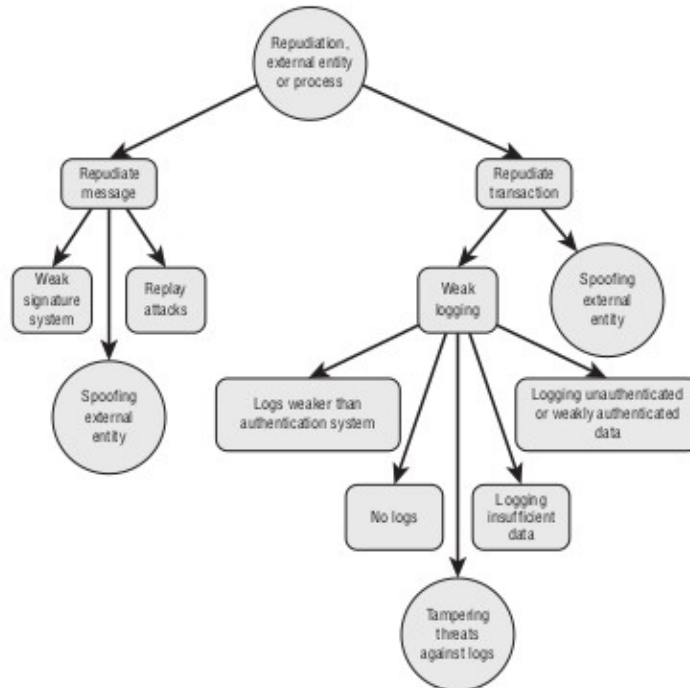
	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

Attack Trees

- **Creating an attack tree:**

- Decide on representation (AND tree / OR tree)
- Create root node (the attacker's goal)
- Create children
- Check if you're done (are you including all the components?)
- Prune the tree (remove duplicate or impossible attacks)
- Check the presentation (make tree compact and neat)

Example Trees



Attack Trees

- **Consider different representations**
 - Graphical – easy to follow, large, can be unstructured
 - Grid – more structure
 - Outline or bullet list – better structures representation
- **No one will read a messy or hard-to-follow tree**

HISTORY LESSONS

Threats have evolved

- **1990's: curiosity, bragging rights**
- **2000's: financial gain, fraud**
 - Spam, credit card theft, identity theft
- **2010's: espionage, propaganda, warfare**
 - Government actors: Stuxnet, cyber attacks, bot nets
 - Private activism: Anonymous, Wikileaks

Threats have evolved

- **Attackers have become more sophisticated**
 - Arms race between attackers and defenders
- **Many attacks aim for profit and are facilitated by a well-developed “underground economy”**

China Cracks Down on Tor Anonymity Network

A leading anonymity technology is targeted by the Chinese government for the first time.

By David Talbot

THURSDAY, OCTOBER 15, 2009

[E-mail](#) [Audio](#) [Print](#) [Favorite](#) [Share](#) [T](#) [T](#) [T](#)

For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called Tor, came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.



"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching Internet connections, the traffic then seems to be



Continuing pro-Wikileaks DDOS actions, Anonymous takes down PayPal.com

Xeni Jardin at 7:10 PM Wednesday, Dec 8, 2010



Third finance-related Anonymous "Operation Payback" takedown in a single day: PayPal.com is effectively offline, moments after the command was tweeted. At the time of this blog post, the PayPal *service* is still functioning, but the site's dead. Earlier today, Visa.com and Mastercard.com were taken offline by Anonymous DDOS attacks, along with other targets perceived as enemies of Wikileaks and of online free speech... including Twitter.com, for a while.

Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

THIS STORY

- » Google attack part of vast campaign
- [Google hands China an Internet dilemma](#)
- [Statement from Google: A new approach to China](#)
- [+ View All Items in This Story](#)

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and [Dow Chemical](#) -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail



People sympathetic to Google have been leaving flowers and candles at the firm's Chinese headquarters. (Vincent Thian/associated Press)

[+ Enlarge Photo](#)

What Google might miss out on

Google said it may exit China,

Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

*This article is by **William J. Broad, John Markoff and David E. Sanger.***

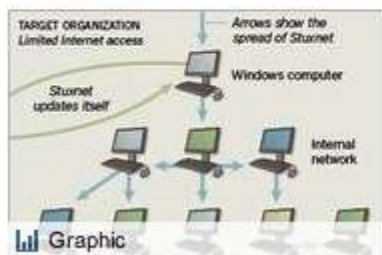
[Enlarge This Image](#)



Nicholas Roberts for The New York Times

Ralph Langner, an independent computer security expert, solved Stuxnet.

Multimedia



How Stuxnet Spreads

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear

[f](#) RECOMMEND

[t](#) TWITTER

[✉](#) E-MAIL

[📱](#) SEND TO PHONE

[🖨](#) PRINT

[📄](#) REPRINTS

[+](#) SHARE



Lesson

- **To protect computer systems, you must know your enemy**
- **Security is not about perfection: it's about defenses that are good enough to stop the threats you're likely to encounter**

Anderson Report, 1972

- **Commissioned by US Airforce**
 - Increasingly aware of computer security
 - Greater reliance on computer data processing
 - Automation of decision making in sensitive areas
- **Current systems are inadequate**

1970s: Mainframes

- **Application**
 - Secret data crunchers (codes)
- **Protection**
 - Professional users
 - Physical security (soldiers)
 - Isolated, no networking
- **Security Issues**
 - DES cryptography
 - Multi-level security



1980s Office PCs

- **Application**

- Word processing, spreadsheets!

- **Protection**

- Little to none

- **Security Issues**

- Individual machines
- Untrained users
- Limited understanding of risk

C11 (L) TOTAL C1
25

	A	B	C	D
1	ITEM	NO.	UNIT	COST
2	----	----	----	----
3	MUCK RAKE	43	12.95	556.85
4	BUZZ CUT	15	6.75	101.25
5	TOE TONER	250	49.95	12487.50
6	EYE SNUFF	2	4.95	9.90
7				
8			SUBTOTAL	13155.50
9			9.75% TAX	1282.66
10				
11			TOTAL	14438.16
12				
13				
14				
15				
16				
17				
18				
19				
20				

1990s The Glorious Internet

- **Application**

- World Wide Web! (www)
- Email
- Entertainment (music, movies)

- **Protection**

- Up to individual PC owner

- **Security Issues**

- Networking! Exposed to hostile Internet
- Buffer overflows “Aleph One” 1996

**THE INTERNET IS
AN AMAZING,
POWERFUL TOOL.**

2000s e-Commerce

- **Applications**

- Web 2.0 dynamic content (Javascript)
- B2C: Amazon, eBay, airlines, Google
- Wireless technologies

- **Protection**

- Commercial expansion on new “public key infrastructure”

- **Security Issues**

- Criminals out for financial gain

The Morris Worm

- **First Internet worm, “Morris worm”**
- **Grad student, Robert Morris, experimented (in lab) with self-spreading malware**
- **It escaped...**

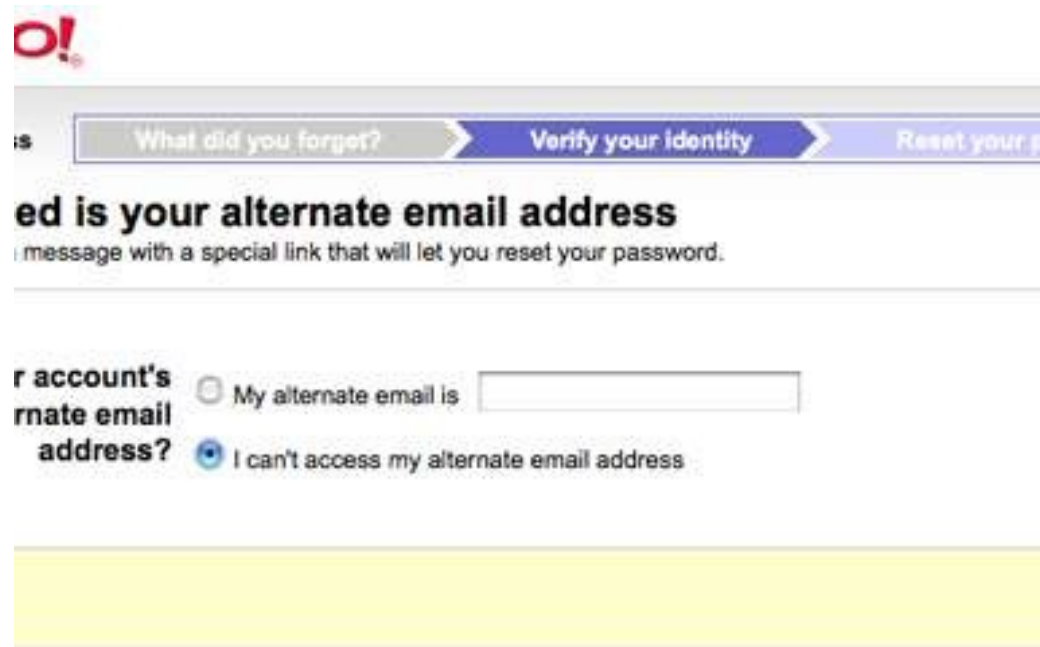
The Morris Worm

- **Millions of dollars in damages (in 1989)**
 - Greater psychological impact! Internet is no longer safe.
- **Morris was prosecuted under the Federal Computer Fraud and Abuse Act.**



Sarah Palin Email Hack

- **Someone wants to mess with Palin's campaign**
- **Tries to log into her Yahoo! Mail account**
- **See the following screen:**



The screenshot shows the Yahoo! Mail password reset interface. At the top, there's a navigation bar with three links: "What did you forget?", "Verify your identity", and "Reset your password". Below this, the text reads "ed is your alternate email address" followed by "message with a special link that will let you reset your password." The main section is titled "r account's alternate email address?" and contains two radio button options: "My alternate email is" (with an empty text input field) and "I can't access my alternate email address". A yellow bar is visible at the bottom of the form area.

Sarah Palin Email Hack

YAHOO! [Yahoo! Home](#) - [Help](#)

Your Progress: [What did you forget?](#) **[Verify your identity](#)** [Reset your password](#)

Answer these questions to validate your identity
We need to verify a few questions and we'll be done.

Birthday

Country of Residence

Postal Code

[Exit Wizard](#) [Next](#)

Sarah Palin Email Hack

After a quick stop by Wikipedia...



[Yahoo! Home](#) - [Help](#)

Your Progress

What did you forget?

Verify your identity

Reset your password

Answer these questions to validate your identity

We need to verify a few questions and we'll be done.

Birthday

February

11

1964

Country of Residence

United States

Postal Code

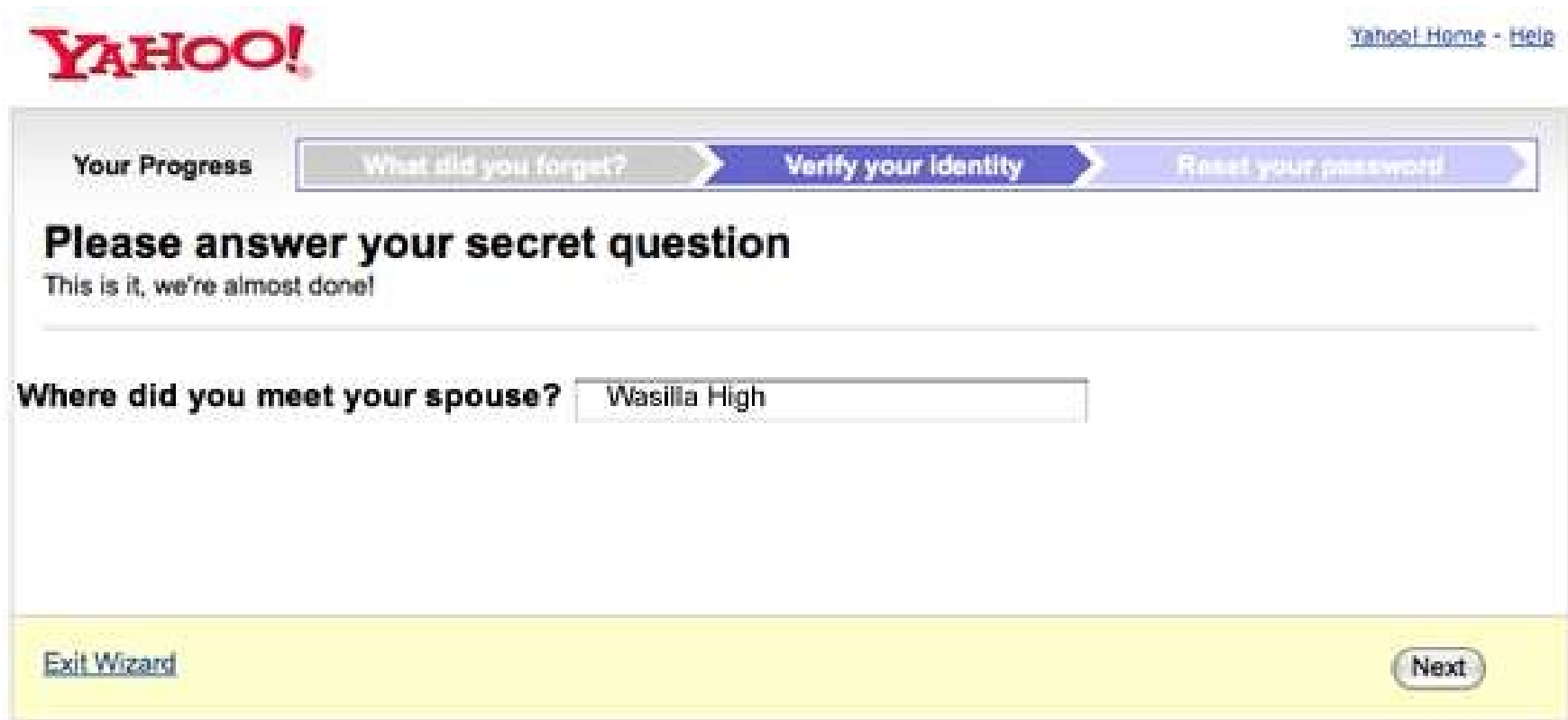
99654

[Exit Wizard](#)

Next

Sarah Palin Email Hack

And an educated guess...



The screenshot shows a Yahoo! password reset wizard. At the top left is the "YAHOO!" logo, and at the top right is a link for "Yahoo! Home - Help". Below the logo is a "Your Progress" section with a horizontal bar containing three steps: "What did you forget?", "Verify your Identity" (which is highlighted in blue), and "Reset your password". The main heading is "Please answer your secret question" with the subtext "This is it, we're almost done!". Below this is a question "Where did you meet your spouse?" followed by a text input field containing the answer "Wasilla High". At the bottom left is a link "Exit Wizard", and at the bottom right is a "Next" button.

YAHOO! [Yahoo! Home - Help](#)

Your Progress: What did you forget? **Verify your Identity** Reset your password

Please answer your secret question
This is it, we're almost done!

Where did you meet your spouse?

[Exit Wizard](#) [Next](#)

Sarah Palin Email Hack

Bingo!



The screenshot shows the Yahoo! password reset interface. At the top left is the "YAHOO!" logo, and at the top right are links for "Yahoo! Home" and "Help". Below the logo is a progress bar with three steps: "What did you forget?", "Verify your identity", and "Reset your password". The "Reset your password" step is currently active and highlighted in blue. Below the progress bar, the text "Welcome back, Sarah" is displayed, followed by the message "You've verified your account details and may now change your password." Below this message are two input fields: "New Password" and "Re-type New Password". To the right of these fields is a "Password Strength" indicator, which consists of a series of five small squares, some of which are filled. At the bottom right of the form is a "Next" button.

YAHOO!

[Yahoo! Home](#) - [Help](#)

Your Progress

What did you forget? Verify your identity **Reset your password**

Welcome back, Sarah

You've verified your account details and may now change your password.

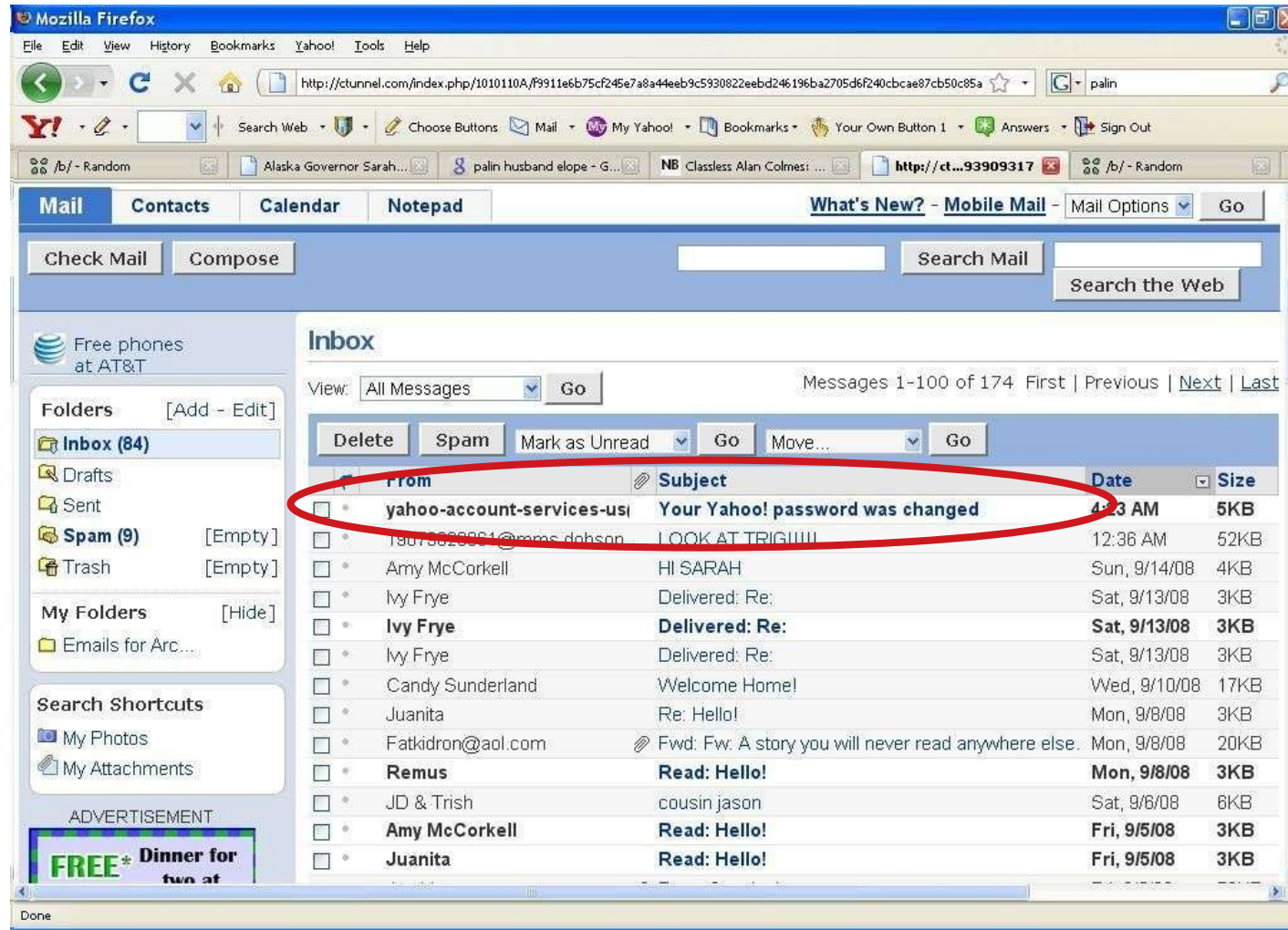
New Password

Re-type New Password

Password Strength

Next

Sarah Palin Email Hack



Sarah Palin Email Hack

- **David Kernell was a 20-year-old college student**
 - He pasted the evidence on 4chan /b/
 - And served 1 year in Federal Prison
- **Lessons**
 - Security is as strong as the weakest link!
 - Security questions don't work for public figures...



Sarah Palin Email Hack

Attack still worked in 2012!

Mitt Romney's private email
possibly hacked

📅 JUNE 6TH, 2012
COMMENTS

✍️ WAQAS

📁 CYBER EVENTS, HACKING NEWS

💬 0