

# System Security Information

An OISS Presentation

# System Security Information Presentation

- What is OISS?
- The Current Situation: a 50000ft view
- The Evolution of the Threat Model
- Effects of an Attack
- Planning and Integrating Security

# Office of Information Systems Security

- Created by campus IT security policy.
- “The focus of OISS is to raise awareness of security issues on campus and to assist in the implementation of best common practices.”

# Are you Prepared?

- The Office of Information Systems Security (OISS) has been formed to help create a unifying IT Security policy for campus.
- We can help you create your policies and procedures in addition to explaining some of the intrusion risks and mitigation techniques.

# Who's Attacking?

- Hackers
  - Script Kiddies
  - Automated viruses/ worms
  - Disgruntled staff/ students
  - Industrial spies
- 
- Attacks are bidirectional - - they might be leaving your network!

# Why are they attacking?

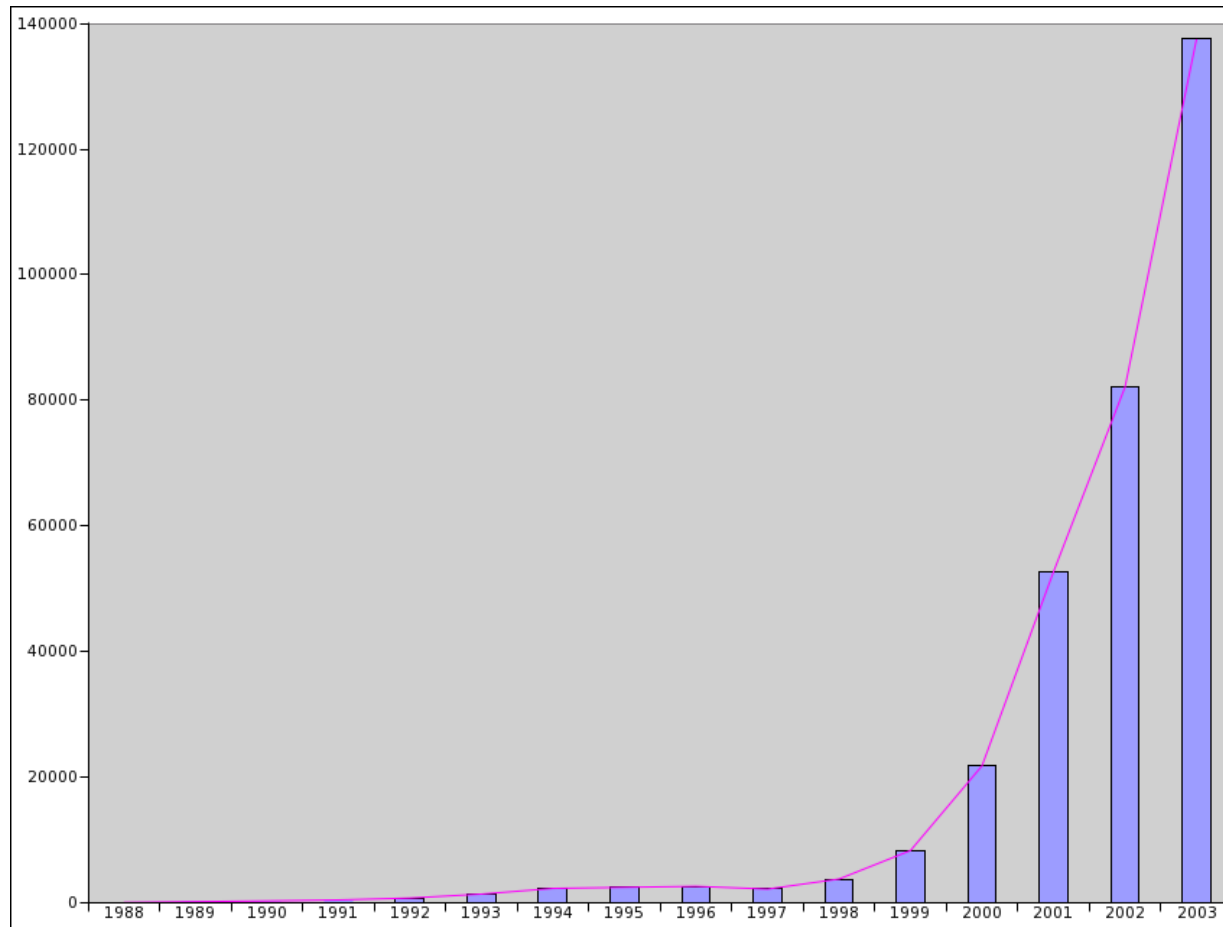
- Simply by being connected you are a target.
- An attacker's motivations are their own, often attacking simply because you are there and they can.
- In many cases the attacker may not realize the importance of one system over another.

# Increasing Opportunities for Attack

- As computers become more ubiquitous throughout our business, our reliance on them to fulfill our mission increases.
- Literally thousands of vulnerabilities may exist on your network today.
- Many of these vulnerabilities are fixable, increasing security awareness and deploying patches will limit their impact.

# Attack Trends

## CERT - - Annual Reported Attacks



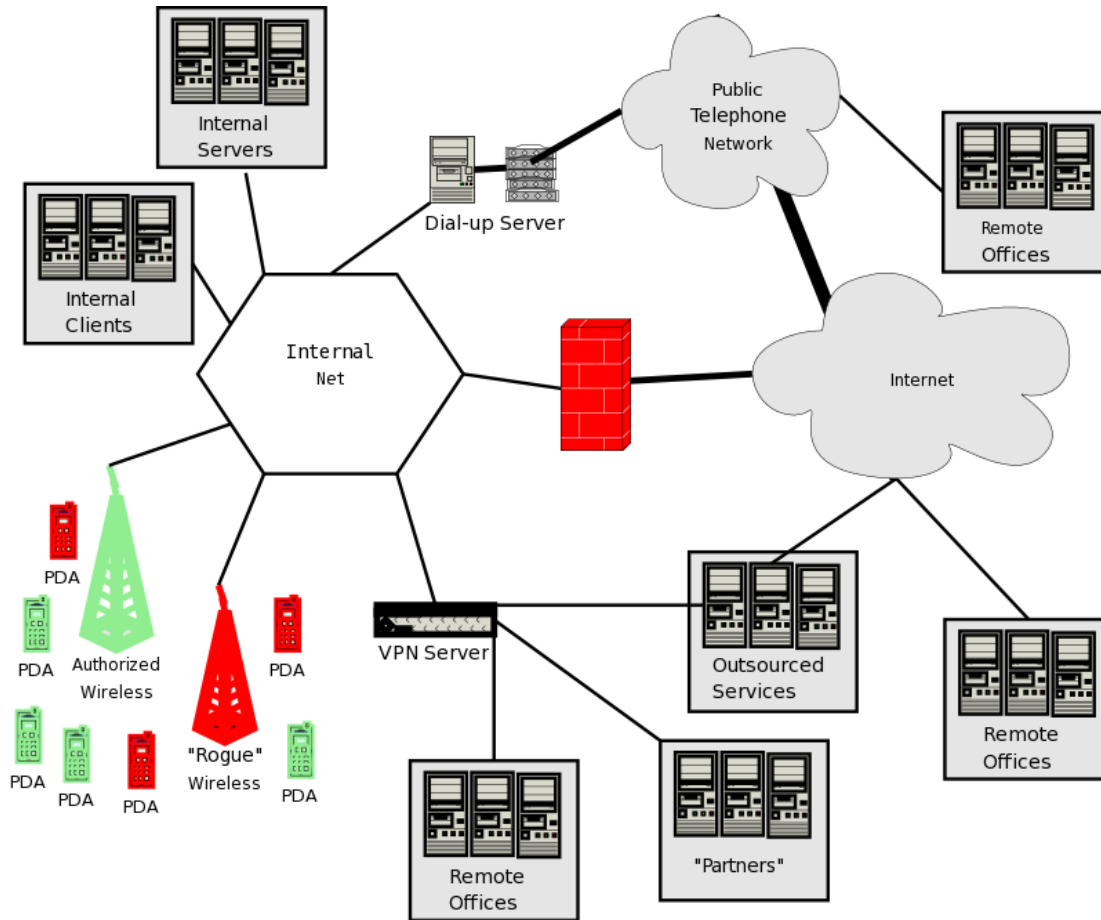
# Present and Future Threats

- Tools available to attackers are increasingly more sophisticated, allowing even inexperienced persons to cause great amounts of damage.
- These tools are also designed to provide distributed large-scale attacks.

# Present and Future Threats

- Systems and Network Administrators are often unable to deal with these threats due to:
  - Lack of training
  - Insufficient resources
  - Overtaxed with other responsibilities
  - Users - Individual policies
  - Absence of Policy
  - Social Engineering versus Technical Attacks

# Today's Network



# Social Engineering: Phishing Email

The screenshot shows a Mozilla Firefox browser window displaying a phishing email from eBay. The browser's address bar shows the URL: <https://gmail.google.com> - Gmail - Credit/Debit Card Update! - Mozilla Firefox. The email subject is "Credit/Debit Card Update!". The sender is "eBay Billing Department <aw-confirm@ebay.com>". The recipient is "chris.kuethe@gmail.com". The date is "Wed, 09 Mar 2005 04:55:11 -0500". The email body contains a warning about a login attempt from a foreign IP address (172.25.210.66) and provides a link to verify the account: <http://www.ebay.com/aw-cgi/ebayISAPI.dll?VerifyRegistrationShow>. The email also includes a "Please Note" section and a "Helpful links" section.

https://gmail.google.com - Gmail - Credit/Debit Card Update! - Mozilla Firefox

[Turn on highlighting](#) [Print](#)

## Credit/Debit Card Update!

[Hide options](#) Mar 9

☆ **eBay Billing Department** <aw-confirm@ebay.com> to me

From: **eBay Billing Department** <aw-confirm@ebay.com>  
To: **chris.kuethe@gmail.com**  
Date: **Wed, 09 Mar 2005 04:55:11 -0500**  
Subject: **Credit/Debit Card Update!**

[Reply](#) | [Reply to all](#) | [Forward](#) | [Print](#) | [Add sender to Contacts list](#) | [Report phishing](#) | [Show original](#)

External images are not displayed. [Display external images](#)

**Your credit/debit card information must be updated**

Dear eBay Member,

We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you.

**The login attempt was made from:**  
**IP address:** 172.25.210.66  
**ISP Host:** cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system to help you evaluate with whom you are dealing with.

**click on the link below, fill the form and then submit as we will verify**

<http://www.ebay.com/aw-cgi/ebayISAPI.dll?VerifyRegistrationShow>

**Please save the above link for your reference**

**Please Note:** - If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

\* Please do not respond to this e-mail as your reply will not be received.

Respectfully,  
Trust and Safety Department  
eBay Inc.

Helpful links

Done [gmail.google.com](#)

# Impacts of an Attack

- Loss of service
- Alteration or destruction of data
- Breach of Privacy Regulations
- Financial losses
- Negative Reputation

# Your Responsibilities

- Policy Development
- Audit your network
- Identify acceptable risk
- Establish a regular review period
- Identify/ Secure Budget

# Services Checklist

- Are all key areas addressed?
  - Patches/ Updates
  - Email, Antivirus, Antispam
  - Web pages
  - Authentication
  - Remote access
  - Wireless
  - Internal Policies and Reviews

# Sustainment

- We must protect against both internal and external threats.
- Multiple layers of security must be in place to do the job.
- Security is not a one-shot deal. It requires and ongoing commitment both fiscally and in policy.
- Monitoring, Logging and Reporting
- Assure continued training
- Technology Review
- Yearly audits

**Thanks!**

Questions, comments, etc.