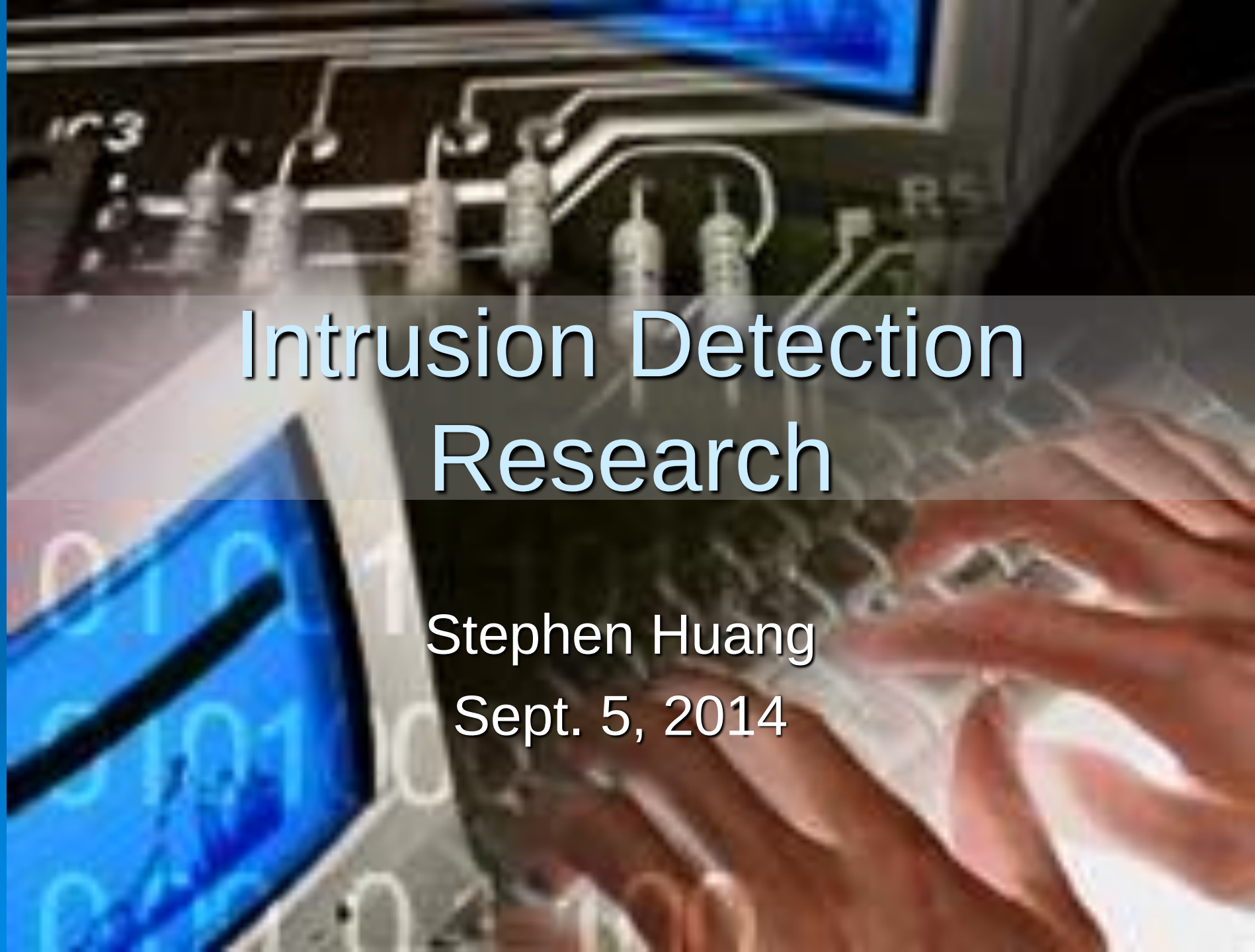


Intrusion Detection Research

Stephen Huang

Sept. 5, 2014

BMC Vulnerability Exposes Admin Password of 32,000 Servers in Plaintext on the Internet

Thursday, June 19, 2014 Mohit Kumar

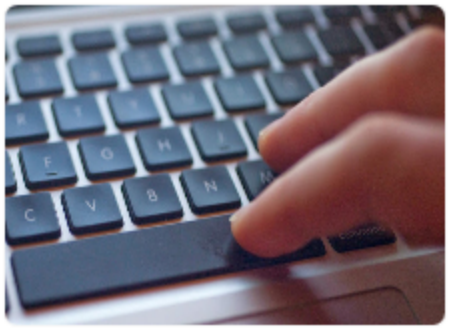
Millions of LinkedIn Users at Risk of Man-in-the-Middle Attack

Wednesday, June 18, 2014 Swati Khandelwal

Two year back in 2012, one of the most popular online social

How to Protect yourself from the 'Heartbleed' Bug

Thursday, April 10, 2014 Swati Khandelwal

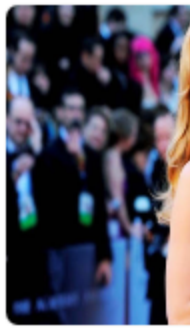


Millions of websites, users' passwords, credit card numbers and other personal information may be at risk as a result of the Heartbleed security flaw, a vulnerability in widely used cryptographic library 'OpenSSL'. [READ DETAILS HERE] Netcraft survey says that about half a million widely[...]

Reported Apple iCloud Hack Leaked Hundreds of Nude Celebrity Photos

Monday, September 01, 2014 Swati Khandelwal

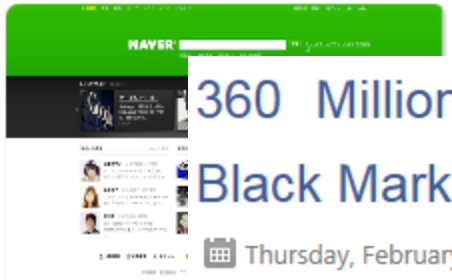
+1 120



25 Million 'NAVER' Accounts Breached using Stolen Data

Thursday, March 27, 2014 Sudhir K Bansal

+1 101 Like 279 Share 93 Tweet 97 Reddit 1 Share 6 ShareThis 442



A 31-year-old South Korean has been recently accused by the police

360 Million Stolen Credential FOR SALE on Underground Black Market

Thursday, February 27, 2014 Swati Khandelwal

+1 159 Like 914 Share 754 Tweet 561 Reddit 3 Share 76 ShareThis 1980

Your Financial Credentials are on SALE on the Underground Black Market without your Knowledge... sounds like a nightmare, but it's TRUE. Cyber security firm, Hold Security, said it has traced over 360 million stolen account credentials that are available for Sale on Hacker's black market[...]

Jobs

Cybersecurity

Cybersecurity jobs average over $100,000 a year

Published 9 August 2013

Share |

According to Semper Secure, a public-private partnership with representatives from the government and industry executives, workers in the cybersecurity industry earn an average salary of $116,000 a year.Someone with less than a year of experience, no certifications, and just an associate's degree could pull in a salary of $91,000.

According to Semper Secure, a public-private partnership with

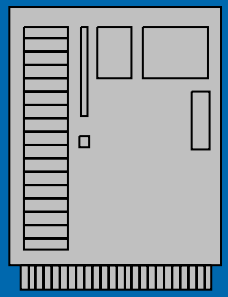
- http://www.homelandsecuritynewswire.com/dr20130809-cybersecurity-jobs-average-over-100-000-a-year

Intrusion Detection Research

- Objective: To protect the infrastructure and the integrity of the computer systems and its data.
- Assumptions:
  - Hackers are able to establish a connection session to the victim machine.
  - Packets are exchanged between the originating source and the victim.
  - Data may be encrypted.

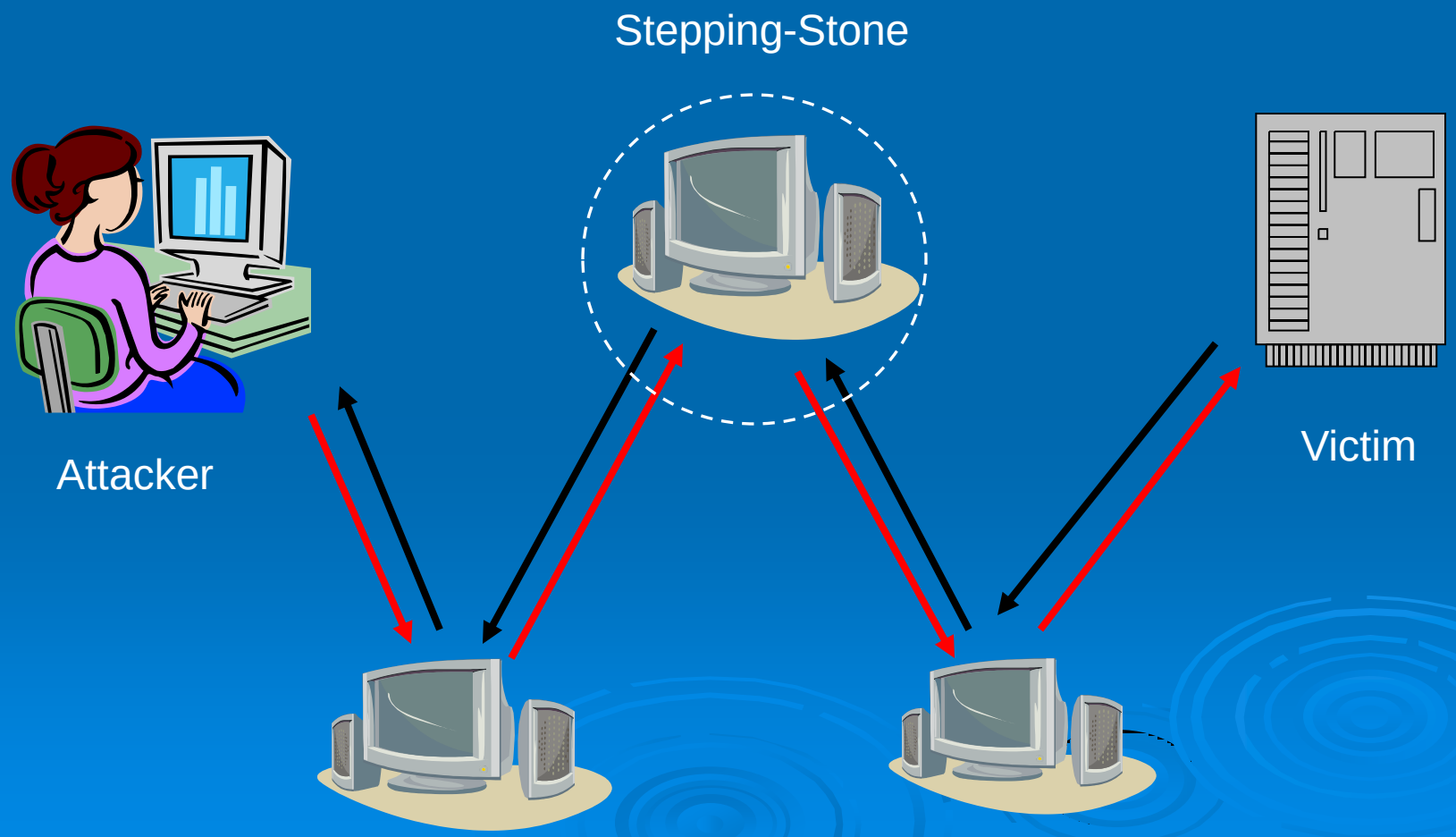
Attack

Attacker

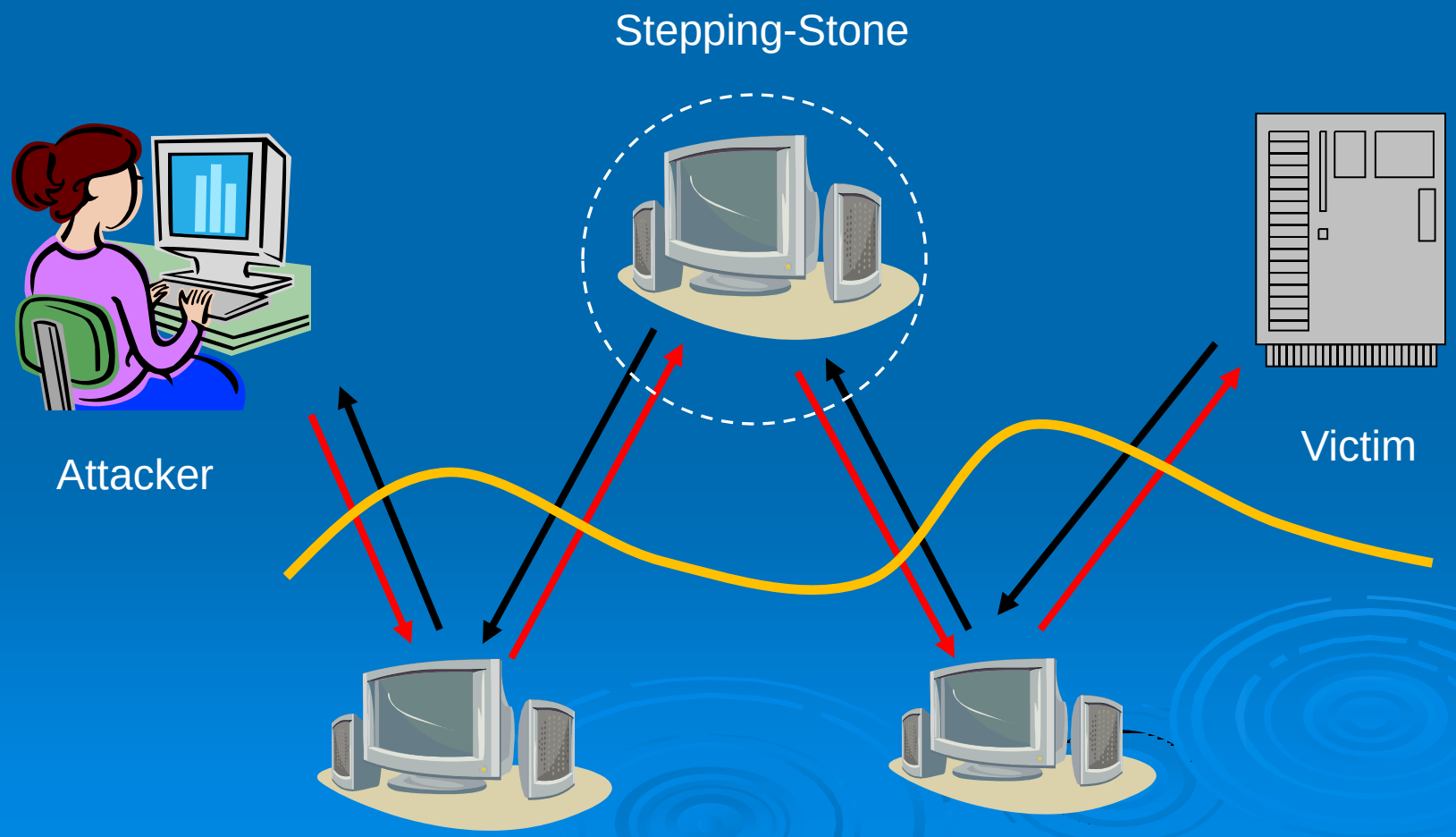


Victim

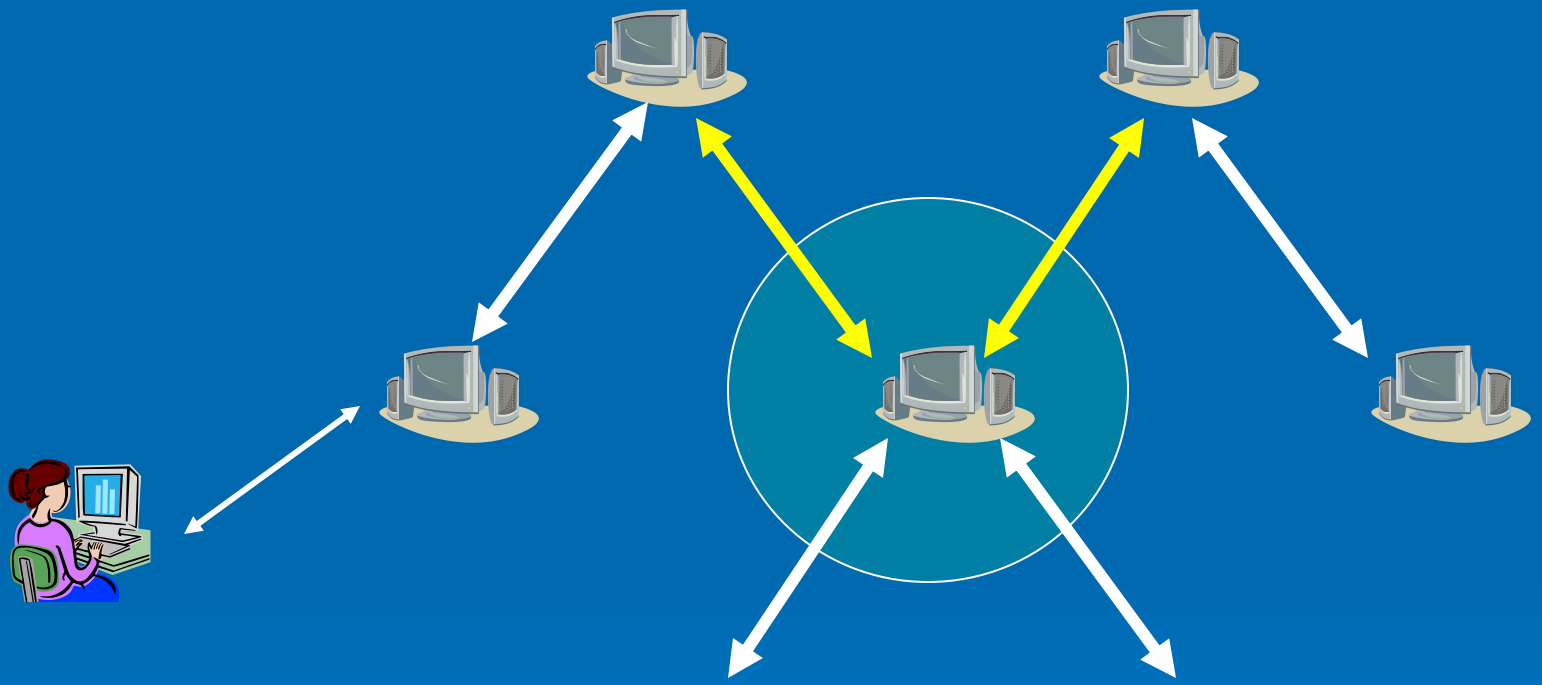
Stepping-Stone Attack



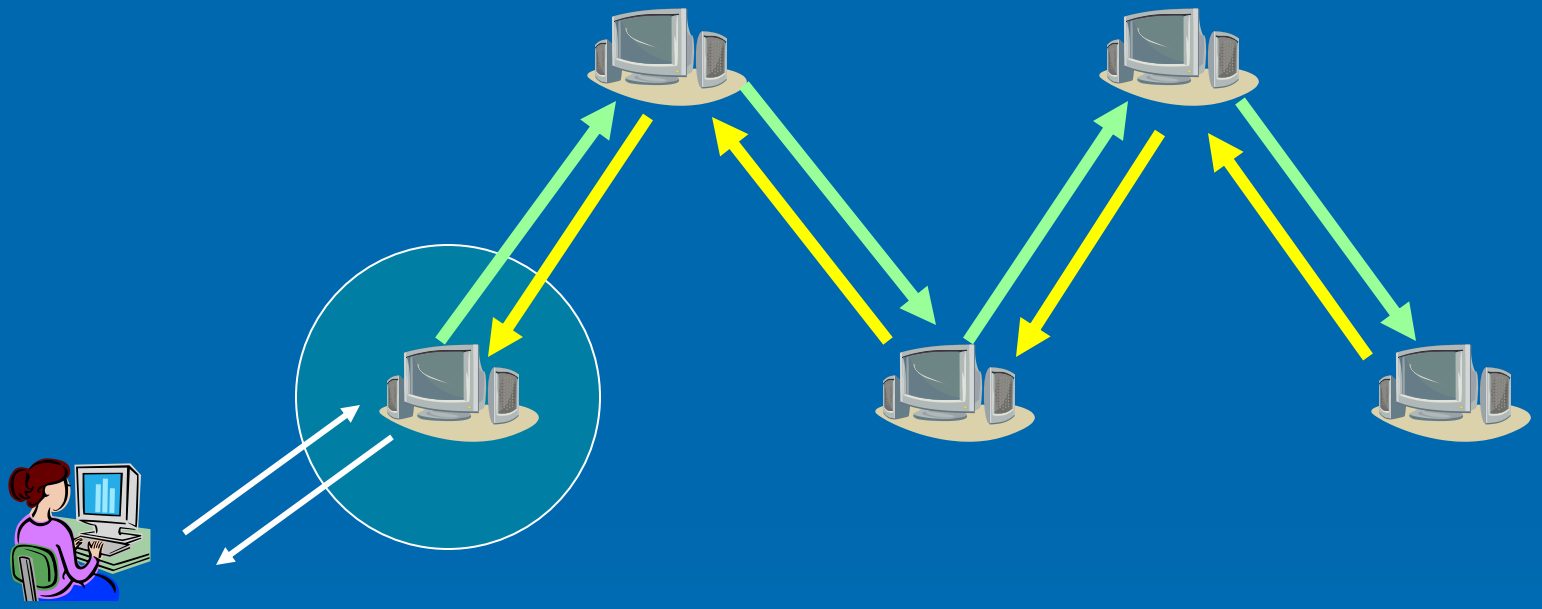
Our Strategy



Stepping-Stone Detection

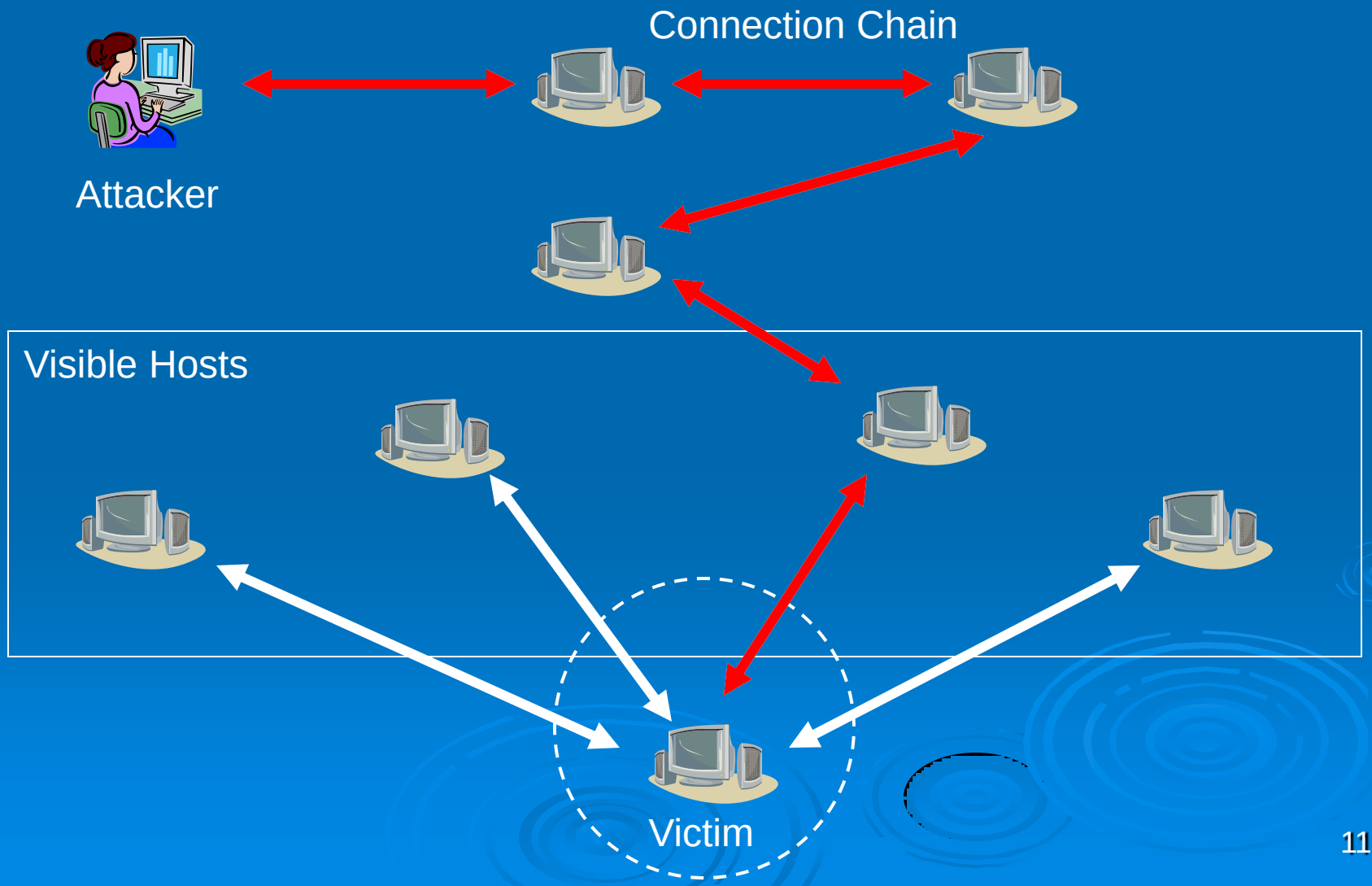


Long Connection Chain Detection



Matching Send- and Echo- Packets to compute the Round-Trip Time (RTT).

Victim Host Protection



Challenges

- Intruder's evasion techniques,
  - Chaffing
  - Time jittering
- New Technology
  - TOR

TOR

- TOR (The Onion Router) is a network of virtual tunnels that allows people to improve their privacy and security on the Internet.
- Anonymity Online.

Summary

- Real-time intrusion detection is critical in protecting data and integrity of computer systems.
- It is possible to detect a large percentage of cases by using various methods.
- Intruders have developed techniques to evade detection. We have to come up with countermeasures.

Recent Students

- Broderick Zhang, MS 2014, KPMG
- Wei Ding, PhD 2014, interviewing
- Ying-Wei Kuo, PhD 2012, MD Anderson
- Jianhua Yang, PhD, Columbus State University, GA
- Jesus Quevedo, PhD, University of Wisconsin-Parkside, CS Chairman