# CS1699: Lecture 23: Security Testing

**Tools for Security Testing**

nmap
valgrind
Nessus
John the Ripper

**Introduction**

**Common Attacks and How to Test Them**

**Remember...**

It's about risks. Before developing a security plan, think about the costs and benefits.

**Information Security**

# CS1699: Lecture 23: Security Testing

**Tools for Security Testing**

nmap
valgrind
Nessus
John the Ripper

## Common Attacks and How to Test Them

## Introduction

## Remember...

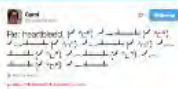It's about risks. Before developing a security plan, think about the costs and benefits.

## Information Security

# *Introduction*

"On a scale of 1 to 10, this is an 11."
    -Bruce Schneier, Harvard Fellow, author of
Practical Cryptography, Applied
Cryptography, Cryptography Engineering,
Schneier on Security, more..

**Security testing is hard.**

1. Adversaries actively seeking to defeat
security
2. You need to protect all doors; they only
need to find one open one
3. Can be absolutely catastrophic if
defects are not found

*Pittsburgh is actually a big city for computer
security!*

## CERT

Security was not a big deal in the
early computing world...

Late '60s - Early '80s

The '80s -> Security Goes Mainstream

1988 - The Year It All Changed

*Nowadays...*
    Cracking computers is big business.

*"Nihil tam munitum quod non expugnari pecunia possit"*
    -Cicero

"No fort is so strong that money cannot take it."

Security testing is one of the most technically
challenging fields of testing, and is also
growing very quickly.

**Carol**
@Carols10cents

Re: heartbleed, (╯ °□°) ╯︵┻━┻ (╯ °□°) ╯︵┻━┻ (╯ °□°) ╯︵┻━┻ (╯ °□°) ╯︵ ┻━┻ (╯ °□°) ╯︵┻━┻ (╯ °□°) ╯︵ ┻━┻ (╯ °□°) ╯︵┻━┻

View translation

↩ Reply    ⟲ Retweet    ★ Favorite    ••• More

"On a scale of 1 to 10, this is an 11."
-*Bruce Schneier, Harvard Fellow, author of Practical Cryptography, Applied Cryptography, Cryptography Engineering, Schneier on Security, more..*

# *Security testing is hard.*

1. Adversaries actively seeking to defeat security

2. You need to protect all doors; they only need to find one open one

3. Can be absolutely catastrophic if defects are not found

*Pittsburgh is actually a big city for computer security!*

# CERT

Security was not a big deal in the early computing world...

# Late '60s - Early '80s

# The '80s -> Security Goes Mainstream

# 1988 - The Year It All Changed

## Nowadays...

Cracking computers is big business.

*"Nihil tam munitum quod non expugnari pecunia possit"*
-Cicero

"No fort is so strong that money cannot take it."

**Security testing is one of the most technically challenging fields of testing, and is also growing very quickly.**

# *Information Security*

*Security service needs to provide three qualities (the InfoSec or CIA Triad):*
Confidentiality
Authentication
Integrity

## Confidentiality

*Only authorized users may read data.*

## Integrity

*Only authorized parties can write data.*

## Availability

*Systems are available for authorized parties to read from and write to.*

### Kinds of Security Attacks

-> *Interruption* (attack on availability, e.g. pulling plug from network switch)
-> *Interception* (attack on confidentiality; eavesdropping)
-> *Modification* (attack on integrity; modifying data)
-> *Fabrication* (attack on integrity; making up data)

### Passive vs Active Attacks

-> Passive: eavesdropping, monitoring, traffic analysis
-> Active: modification or creation of data

-> Vulnerability: identified weakness of a controlled system
-> Exploit: (aka "sploit") Technique or mechanism used to compromise a system

Kinds of malicious code:
* Bacteria - program that consumes system resources (e.g. fork bomb)
* Logic bomb - code within a program which executes an unauthorized function
* Trapdoor - secret undocumented access to a system or app
* Trojan horse - system that pretends to be another
* Virus - replicates itself WITH human intervention
* Worm - replicates itself WITHOUT human intervention
* Zombie - malicious code which is triggered (e.g. time of day, remote command)
* RAT - Remote Administration Tool (e.g. BackOrifice)
* Bot network - collection of zombies controlled by master
* Spyware - surreptiously monitors your actions
* DOS (Denial of service) attacks (e.g. via LOIC)

Protections:
* Firewalls
* Operating System Permissions
* CDNs
* Well-written code

## *CRYPTOGRAPHY*

Cryptography (crypto) is absolutely vital to the modern infrastructure of the web, especially public-key cryptography.

*Public-Key Cryptography*

### Alice

Large Random Number

Key Generation Program

Public     Private

If we ever lose this, we're stuck.

*Security service needs to provide three qualities (the InfoSec or CIA Triad):*

## Confidentiality

## Authentication

## Integrity

# Confidentiality

*Only authorized users may read data.*

# Integrity

*Only authorized parties can write data.*

# Availability

*Systems are available for authorized parties to read from and write to.*

# Kinds of Security Attacks

-> *Interruption* (attack on availability, e.g. pulling plug from network switch)

-> *Interception* (attack on confidentiality; eavesdropping)

-> *Modification* (attack on integrity; modifying data)

-> *Fabrication* (attack on integrity; making up data)

# Passive vs Active Attacks

-> Passive: eavesdropping, monitoring, traffic analysis
-> Active: modification or creation of data

-> Vulnerability: identified weakness of a controlled system

-> Exploit: (aka "sploit") Technique or mechanism used to compromise a system

Kinds of malicious code:
   * Bacteria - program that consumes system resources (e.g. fork bomb)
   * Logic bomb - code within a program which executes an unauthorized function
   * Trapdoor - secret undocumented access to a system or app
   * Trojan horse - system that pretends to be another
   * Virus - replicates itself WITH human intervention
   * Worm - replicates itself WITHOUT human intervention
   * Zombie - malicious code which is triggered (e.g. time of day, remote command)
   * RAT - Remote Administration Tool (e.g. BackOrifice)
   * Bot network - collection of zombies controlled by master
   * Spyware - surreptiously monitors your actions
   * DOS (Denial of service) attacks (e.g. via LOIC)
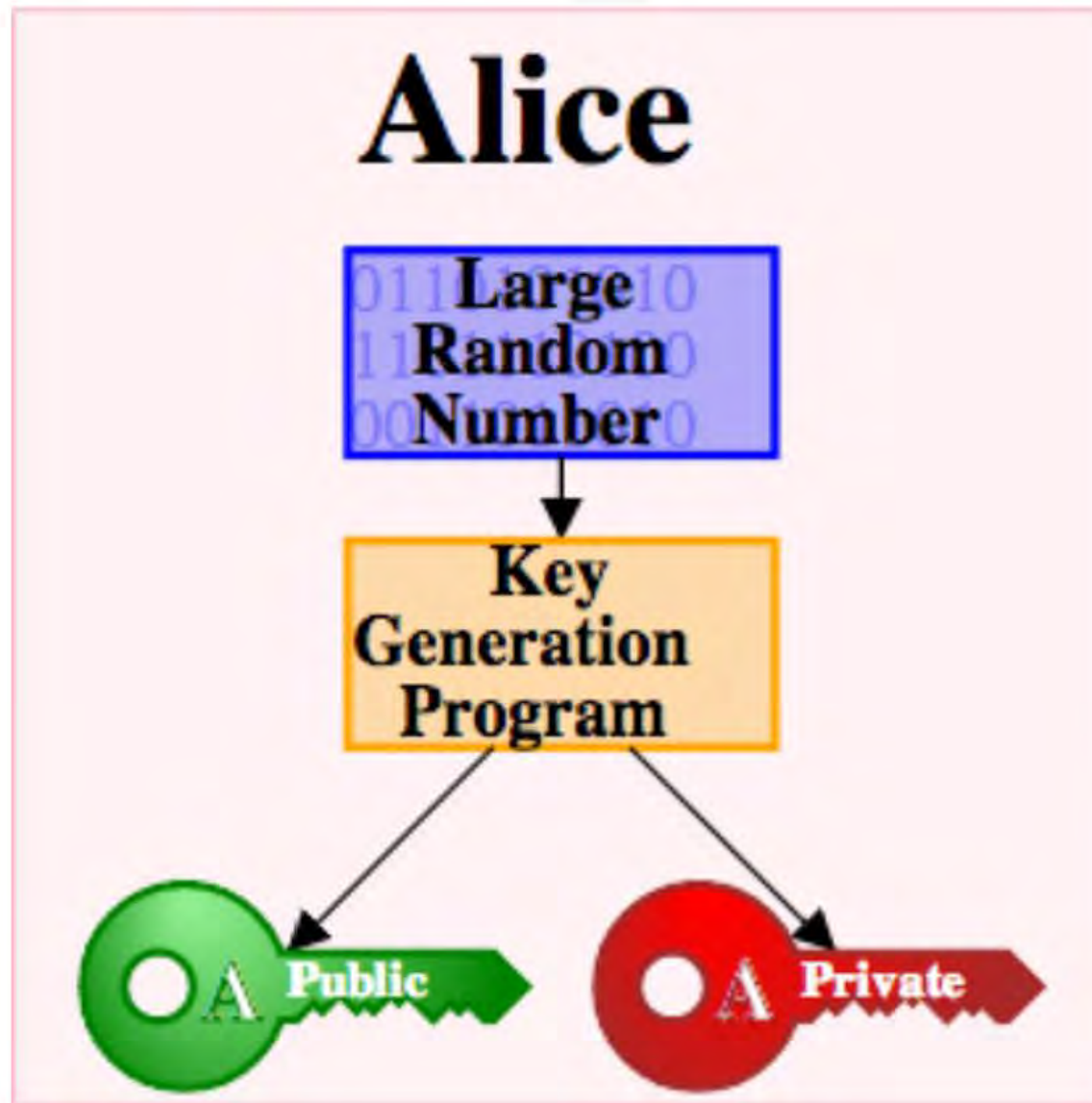
Protections:
 * Firewalls
 * Operating System Permissions
 * CDNs
 * Well-written code

# *CRYPTOGRAPHY*

Cryptography (crypto) is absolutely vital to the modern infrastructure of the web, especially public-key cryptography.

## Public-Key Cryptography

# If we ever lose this, we're stuck.

# *Common Attacks and How to Test Them*

### Injection (e.g. SQL Injection)



Test your inputs!
Static analysis; ensure inputs are sanitized
Use Haskell or another type-safe language

### Broken Authentication

Session ID exposed; "change my p/w"

Try to guess passwords/info
Check for unencrypted session IDs

### Cross-Site Scripting (XSS)

### Insecure Object References

http://bank.com/?account=9844
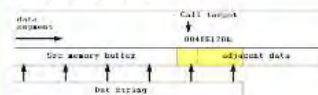http://bank.com/?account=9845

### Security Misconfiguration

Default passwords
IPS, packet filtering, etc. not running
Insecure machine on secure network

### Insecure Storage



### Buffer Overruns
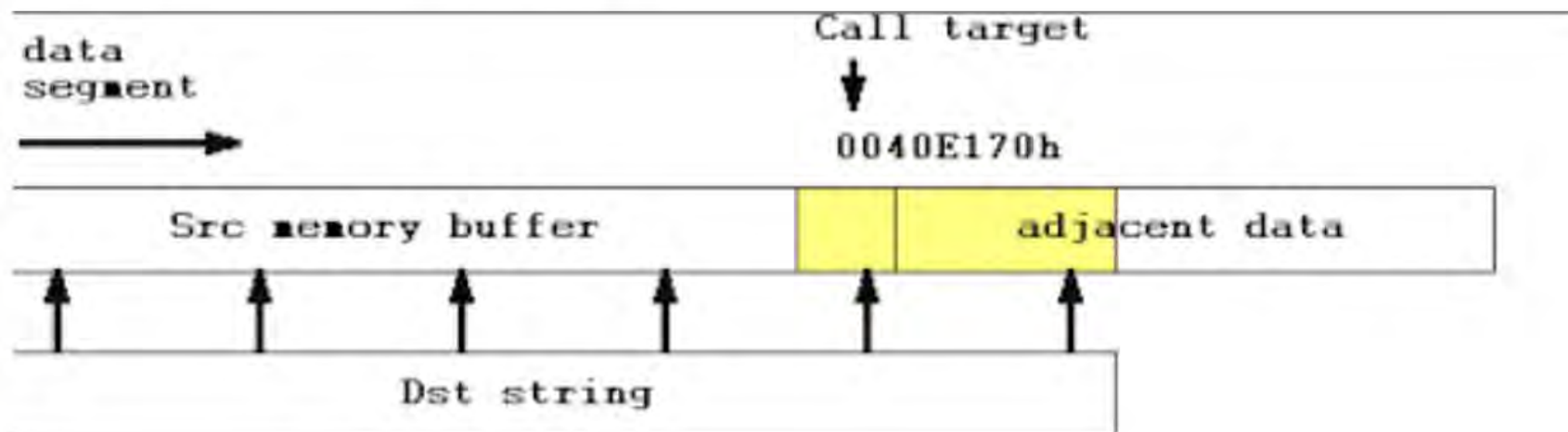


### Smashing the Stack



### SOCIAL ENGINEERING!

PREZI

## Injection (e.g. SQL injection)



**Test your inputs!**
**Static analysis; ensure inputs are sanitized**
**Use Haskell or another type-safe language**

# Broken Authentication

Session ID exposed; "change my p/w"

Try to guess passwords/info
Check for unencrypted session IDs

# Cross-Site Scripting (XSS)

# Insecure Object References

http://bank.com/?account=9844

http://bank.com/?account=9845

# Security Misconfiguration

Default passwords

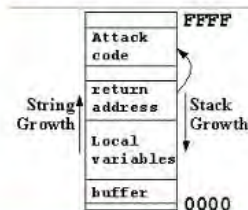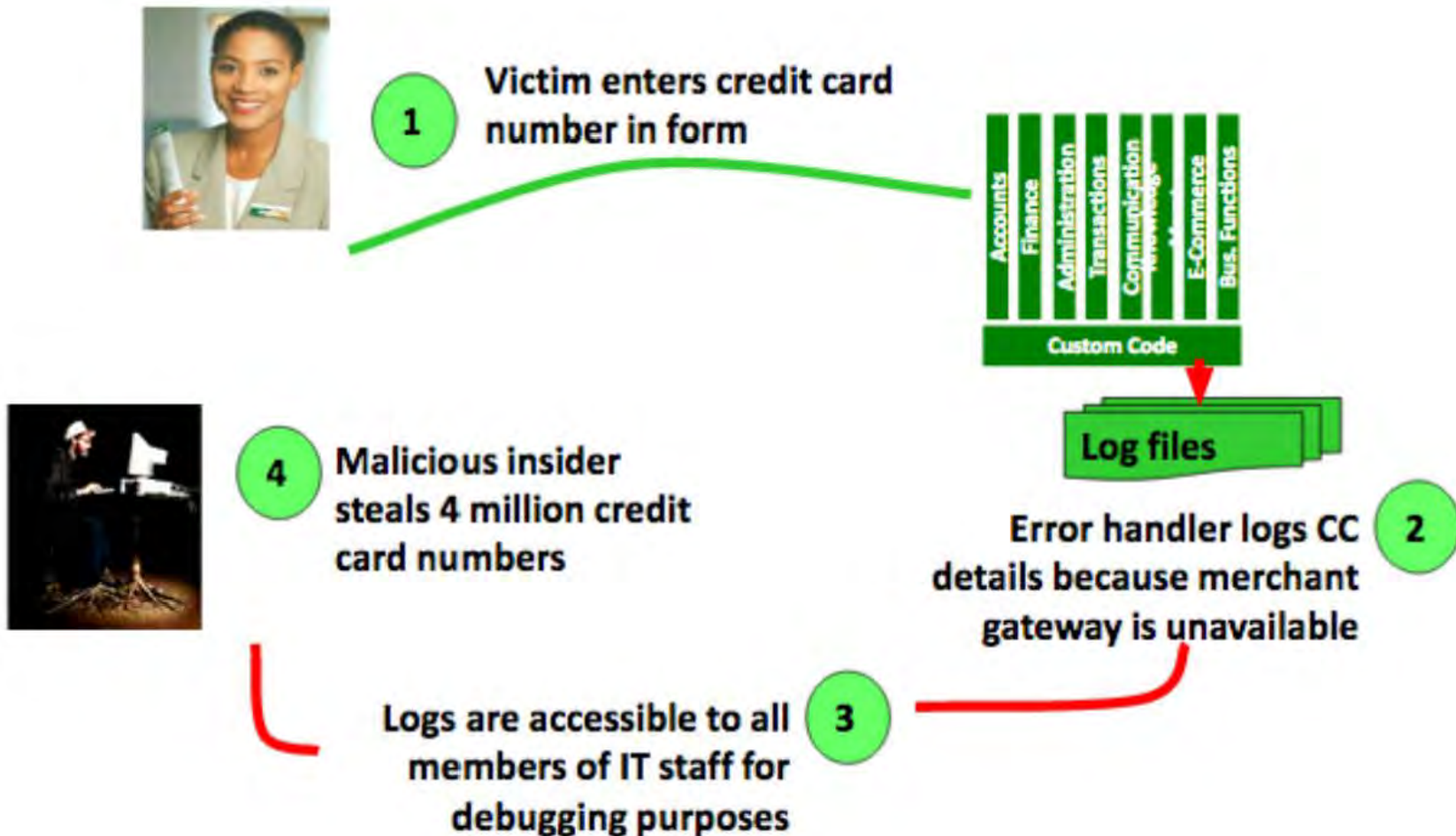IPS, packet filtering, etc. not running

Insecure machine on secure network

# Insecure Storage



1. Victim enters credit card number in form

Accounts | Finance | Administration | Transactions | Communication | E-Commerce | Bus. Functions

Custom Code

Log files

2. Error handler logs CC details because merchant gateway is unavailable

3. Logs are accessible to all members of IT staff for debugging purposes

4. Malicious insider steals 4 million credit card numbers

# Buffer Overruns

# Smashing the Stack

```
                                          FFFF
       ┌──────────────┐
       │   Attack     │
       │   code       │
       ├──────────────┤
       │              │
       ├──────────────┤
       │   return     │
 String│   address    │   Stack
 Growth├──────────────┤   Growth
       │   Local      │
       │   variables  │
       ├──────────────┤
       │   buffer     │
       └──────────────┘   0000
```

# SOCIAL ENGINEERING!

# *Tools for Security Testing*

**nmap**

**valgrind**

**Nessus**

**John the Ripper**

# Remember...

It's about risks.  Before developing a security plan, think about the costs and benefits.

# CS1699: Lecture 23: Security Testing

*Tools for Security Testing*

nmap
valgrind
Nessus
John the Ripper

*Common Attacks and How to Test Them*

*Introduction*

*Remember...*

It's about risks.  Before developing a security plan, think about the costs and benefits.

*Information Security*