Introduction

CMSC 414: Computer and Network Security
Fall 2015

What is computer & network security?

- Normally, we are concerned with correctness
  - Does the software achieve the desired behavior?

- Security is a form of correctness
  - Does the software prevent “undesired” behavior?

The key difference:

Security involves an adversary who is active and malicious.

Attackers seek to circumvent protective measures.
What are “undesired” behaviors?

- Reveals info users wish to hide (confidentiality)
  - Corporate secrets
  - Private data; personally identifying information (PII)
- Modifies information or functionality (integrity)
  - Destroys records
  - Changes data in-flight (think “the telephone game”)
  - Installs unwanted software (spambot, spyware, etc.)
- Denies access to a service (availability)
  - Crashing a website for political reasons
  - Denial of service attack
  - Variant: fairness

This is a subset

Attacks are common
From just the past 9 months or so:
Why are attacks common?

- Security is a property of the systems we build
- Many attacks begin by exploiting a vulnerability
  - Vulnerability = software defect that can be exploited to yield an undesired behavior
  - Software defect = the code doesn’t “behave correctly”
- Software defects arise due to
  - flaws in the design and/or
  - bugs in the implementation

Heartbleed

- SSL is the de facto protocol for secure online communication
- Heartbleed was a vulnerability in the most popular SSL server
  - A malformed packet allows you to see server memory
- Fix: don’t let the user just tell you how much data to give back
- This was a design flaw
**How the Heartbleed Bug Works:**

Server, are you still there? If so, reply "potato" (6 letters).

User Meg wants these 6 letters: POTATO. User Ida wants pages about "irl games". Unlocking secure records with master key 51309857334324.

User Meg wants these 5 letters: POTAT.

User Ida wants pages about "irl games". Unlocking secure records with master key 51309857334324.

User Meg wants these 6 letters: POTATO. User Ida wants pages about "irl games". Unlocking secure records with master key 51309857334324.

Server, are you still there? If so, reply "bird" (4 letters).

User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file "files" to /tmp.

User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file "files" to /tmp.

Hmm...

User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file "files" to /tmp.

User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file "files" to /tmp.
User passwords, private keys, personal information…

~40% of “secure” web servers vulnerable

Heartbleed

- SSL is what gets us encrypted communication with websites

- Heartbleed was a vulnerability in the most popular SSL server
  - A malformed packet allows you to see server memory

- Fix: don’t let the user just tell you how much data to give back

- This was a design flaw
RSA 2011 breach

1. **Carefully crafted Flash program.** When run by the vulnerable Flash player, allows the attacker to execute arbitrary code on the running machine.

2. This program could be **embedded in an Excel spreadsheet**, and run automatically when the spreadsheet was opened.

3. Spreadsheet **attached to an email**, masquerading as a trusted party (“spear phishing”)
   - You can forge any “From” address

Why are attacks common?

- Because attacks derive from design flaws or implementation bugs
- But all software has bugs: so what?
- A *normal user* never sees most bugs
  - Post-deployment bugs are usually rare corner cases
- Too **expensive** to fix every bug
  - Only fix what’s likely to affect normal users
Why are attacks common?

*Attackers are not normal users*

- Normal users avoid bugs/flaws
- Adversaries seek them out and try to *exploit* them

*This extends beyond software:*

Attacks are possible even with perfect software

---

Why are attacks common?

Because it's **profitable**

And because a system is only as secure as its **weakest link**

---

Figure 1: Infrastructure involved in a single URL’s value chain, including advertisement, click support and realization steps.
In order to achieve security, we must:

Be able to eliminate bugs and design flaws and/or make them harder to exploit.

Be able to think like attackers.

Develop a foundation for deeply understanding the systems we use and build.

Widespread misuse of crypto

This is an encrypted image

50% of Android apps that use crypto encrypt in this manner
In order to achieve security, we must:

Be able to eliminate bugs and design flaws and/or make them **harder to exploit**.

**Be able to think like attackers.**

Develop a foundation for **deeply understanding** the systems we use and build.

<table>
<thead>
<tr>
<th>Software</th>
<th>Hardware</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Law</td>
<td>Economics</td>
</tr>
</tbody>
</table>