01:090:101 Section 51 Hill 120  Tuesday, 3:20-4:40

02: How to get infected. Phishing. Spearphishing. d0xed game.
03: Discuss the game elements. Erasing data forever. Lying.
04: The web of you. Who has it? What can they do with it? Good practices. Class presentation description.
05: Class presentations picking. What can I do with a little bit of you? Why the web can lie forever – wikipedia.
06: Social media. What’s good and bad practices.
07: The other side of the curtain – what are the responsibilities of the holders of data?
09: Presentations, part 1 (randomly selected.)
10: Presentations, part 2 (randomly selected.)

Dr. Casimir Kulikowski (kulikows@cs.rutgers.edu)
Not-at-all-Dr. Charles McGrew (mcgrew@cs.rutgers.edu)
Project: The Hack in Question

- When?
- Target?
- How many affected?
- Perpetrator?
- Caught?
- Punishment?
- Side effects?
If you ain’t got one...

- Adobe hack, October 2013
- Ebay, May 2014
- Target, January 2014
- Home Depot, September 2014
- Anthem, February 2015
- JP Morgan, June 2014
- Great Train Robbery, 1963
If you ain’t got one...

- JFK Lufthansa Robbery, December, 1978
- JFK Air France Robbery, April 1967
- Brinks MAT Warehouse, November 1983
- Banco Central, Brazil, August 2005
- DB Cooper, November 1971
- Brinks Robbery, January 1950
- Gardner Museum, March 1990
If I have...

- Name
- How can I get (legally)
  - Address?
  - Employment?
  - Friends?
  - Family?
If I have...

• SSN

• How can I get (legally)
  – Address?
  – Employment?
  – Friends?
  – Family?
If I have...

- Mother’s Maiden Name
- How can I get (legally)
  - Address?
  - Employment?
  - Friends?
  - Family?
How can I get information on you?

• Legally?

• Semi-legally?

• Illegally?
How can I get information on you?

• Legally?
  – Phone book
  – Web search (make sure it’s the right ‘you’
  – Public records (purchases of property, arrests, convictions, mentions in cases – e.g. named in divorce proceedings)
  – Watch

• Semi-legally?

• Illegally?
How can I get information on you?

• Legally?

• Semi-legally?
  – Hire a PI
  – “trashing” home
  – “trashing” work
  – Investigate family, co-workers

• Illegally?
How can I get information on you?

• Legally?

• Semi-legally?

• Illegally?
  – Steal phone, laptop, wallet
  – Break into house
  – Break into car
The battle for the soul of Wikipedia

• Who runs wikipedia?
• What rules on editing?
• What assumptions are made about editors?
• What flaws are there in those assumptions?

• If I control Wikipedia entries, what can I do to impose my point of view on an entire generation?
Some samples

- **Gamergate**
  - Originally a commentary on game ‘reviewers’ being in bed (in this case, literally) with game makers
  - Evolved into a weird anti-female/feminist fight for ‘control’ of gaming, with anti-white-male elements in for good measure.

- **Climate email “hack”**
  - Presented as a true/’slanted’ view of global warming alarmism as a conspiracy or anti-global warming as a conspiracy

- **Globalwarming fascism**
  - Seizing control of the debate, altering history, suppressing debate and debaters
  - Resulted in ban of several from wikipedia editing
  - Tarnished (perhaps correctly) wikipedia’s reputation
Why is Wikipedia popular

- Free
- (reasonably) accurate
- Cross-referenced
- Done by (sort of) experts
- Free
- Appears to be complete
- Free
- Free
The real network

• Part 0: collisions, how things really travel

• Part 1: Hostnames, Internet Addresses, Port Numbers

• Part 2: Packets

• Part 3: TCP, and UDP
Part 0: how things really travel

• One wire, everybody talks on it

• Everybody waits for “acknowledgements” for TCP packets, and resends if not ack-ed

• What can go wrong?
Part0a: collisions

• If two machines talk at once, they might talk over top of each other.

• They both ‘listen’ while they send. If they see other traffic, they stop and assume failure.

• If they don’t get an ack, they assume failure.

• Failure == resend.

• And yes, this actually works! (Why?)
Part 0a: Collisions

• Everything happens very quickly (speeds from 10,000,000 bits per second up to 10,000,000,000 bits per second)

• Computers are fast

• We are slow
Part 1:

- Hostnames – names, domains
- Addresses – networks, subnets
- Port numbers
  - 25 email
  - 80, 443 http, https
  - 445 Microsoft file mounts
- Routing
Part 2

• Packets

• Why packets? Why not just send an entire message?

• Packet “switching” (routing)
Why Packets?

- Breaking messages into packets limits the damage due to collisions (packets are \(\leq 65,535\) bytes due to protocol restrictions – the number describing the size, specifically), but by general consensus (that is, “hey, this seems to work pretty well”, 1500 bytes.)

- That limits the number of resends

- It limits the memory needed in a router (to read and resend)
Part 2a

- Packet parts

<table>
<thead>
<tr>
<th>TCP/IP Packet</th>
<th>Version</th>
<th>IHL</th>
<th>Type of Service</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification</td>
<td>Flags</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Time to Live</td>
<td>Fragment Offset</td>
</tr>
<tr>
<td></td>
<td>Protocol=6 (TCP)</td>
<td></td>
<td>Header Checksum</td>
<td></td>
</tr>
<tr>
<td>IP Header</td>
<td>Source Address</td>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Options</td>
<td>Padding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Source Port</td>
<td>Destination Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sequence Number</td>
<td>Acknowledgement Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Offset</td>
<td>Window</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Checksum</td>
<td>Urgent Pointer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Options</td>
<td>Padding</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Part 3

• TCP – Transmission Control Protocol
  – sends, gets acknowledgment for each packet
  – what’s that good for?

• UDP – User Datagram Protocol
  – Sends, no acknowledgment, just hope for the best
  – what’s that good for?
Next week:

• Services
• Routing mechanisms
• Failure recovery
• Improvements?
Thought Experiment

• If you had stolen all of Hillary Clinton’s email from her private (illegal) server, what would you do with it?
• Why tell anyone?
• When tell anyone?
• Who would you tell?
• What would you ask for it?
Image analysis programming

• Edge detection

• Face detection

• Object detection

• Motion detection