CSE 115
Introduction to Computer Science I
Road map

▶︎ Review ◀

Warm up: a recent vulnerability

Codes of Ethics & Professional Obligations

Various Risks & Social Impacts
HTML & SQL injection

Basic problem:
not distinguishing code from data

Solution:
sanitize user input
Road map

Review

▶ Warm up: a recent vulnerability ◀

Codes of Ethics & Professional Obligations

Various Risks & Social Impacts
What's the risk here?

What's the risk here?

psCmd = "…" & syncCmd & "…"
A tie-in with Friday's lecture:
(found in Risks 30.87)

This specific script takes in a few arguments and passes them into a powershell.exe shell execution without filtering it, allowing us to inject arbitrary commands. If you look at line 36 of 'SyncAppvPublishingServer.vbs' we see:

```powershell
```

And we can influence the value of 'syncCmd' but not only that, **Edge also does not sanitize quotation marks**, so we can pass as many parameters to 'WScript.exe' as we want. Again, conveniently this powershell will run hidden as indicated by '-WindowStyle Hidden' which makes this a perfect WSH injection vector.

https://leucosite.com/Microsoft-Edge-RCE/

See also: https://www.zdnet.com/article/proof-of-concept-code-published-for-microsoft-edge-remote-code-execution-bug/
Road map

Review

Warm up: a recent vulnerability

- Codes of Ethics & Professional Obligations

Various Risks & Social Impacts
1. GENERAL ETHICAL PRINCIPLES.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

1.2 Avoid harm.

1.3 Be honest and trustworthy.

1.4 Be fair and take action not to discriminate.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

1.6 Respect privacy.

1.7 Honor confidentiality.
ACM Code of Ethics

Only 1. General Ethical Principles and 2. Professional Responsibilities

2. PROFESSIONAL RESPONSIBILITIES.

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

2.6 Perform work only in areas of competence.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

2.9 Design and implement systems that are robustly and usably secure.
IEEE Code of Ethics

We, the members of the IEEE, [...] commit ourselves to the highest ethical and professional conduct and agree:
1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.
What's the technological risk here?
Original story found in Crypto-gram 11/15/2018. Additional links below:

https://www.lightbluetouchpaper.org/2018/10/11/privacy-for-tigers/

Do you remember this?

TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION

https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/
What happened…

What's the social impact?
Risks

The printed yellow dots could be a hedge against counterfeiting - if the purported date of the document does not match up to the data confirmed by the dots, then you know it's a fake. But these dots can also be used to identify the printer a whistleblower uses, as happened with Reality Winner.

This kind of information is a type of metadata, and for most people, it isn't going to be a real issue. But whistleblowers, free speech activists, and others doing work where keeping one's identity secret is of utmost importance, could find their privacy - and even their safety - compromised by these methods.

As noted on the Errata Security blog, published by cybersecurity experts, this kind of accidental disclosure of sources through metadata has a long history. It notes:

"The situation is similar to how Vice outed the location of John McAfee, by publishing JPEG photographs of him with the EXIF GPS coordinates still hidden in the file. Or it's how PDFs are often redacted by adding a black bar on top of image, leaving the underlying contents still in the file for people to read, such as in this NYTime accident with a Snowden document. Or how opening a Microsoft Office document, then accidentally saving it, leaves fingerprints identifying you behind, as repeatedly happened with the Wikileaks election leaks."

Related stories from Risks 30.88

3D printers have ‘fingerprints,’ a discovery that could help trace 3D-printed guns, counterfeit goods

Additional links
(see also Risks 30.88)

https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

You see a runaway trolley moving toward five tied-up (or otherwise incapacitated) people lying on the tracks. You are standing next to a lever that controls a switch. If you pull the lever, the trolley will be redirected onto a side track and the five people on the main track will be saved. However, there is a single person lying on the side track. You have two options:
1. Do nothing and allow the trolley to kill the five people on the main track.
2. Pull the lever, diverting the trolley onto the side track where it will kill one person.

Driverless cars:
Who should die in a crash?

What are the benefits / risks of having autonomous vehicles making these decisions?
Facial-recognition systems are more likely either to misidentify or fail to identify African Americans than other races, errors that could result in innocent citizens being marked as suspects in crimes.

And though this technology is being rolled out by law enforcement across the country, little is being done to explore—or correct—for the bias.
Weak passwords banned in California from 2020

What's your reaction to this?

Weak passwords banned in California from 2020

"Default passwords such as "admin" and "password" will be illegal for electronics firms to use in California from 2020.

The state has passed a law that sets higher security standards for net-connected devices made or sold in the region.

It demands that each gadget be given a unique password when it is made."

How about now?

Cyber Tests Showed 'Nearly All' New Pentagon Weapons Vulnerable To Attack, GAO Says

Passwords that took seconds to guess, or were never changed from their factory settings. Cyber vulnerabilities that were known, but never fixed. Those are two common problems plaguing some of the Department of Defense's newest weapons systems, according to the Government Accountability Office.

Links for future reference

https://www.acm.org/code-of-ethics

https://www.ieee.org/about/ethics/index.html

http://www.order-of-the-engineer.org

http://pledge-of-the-computing-professional.org

https://catless.ncl.ac.uk/Risks/

https://www.schneier.com/crypto-gram/