Cyber Warfare

CS463/ECE424

University of Illinois

Did the Russians do it?

Hacking the DNC

- DNC's FBI prankster
- Podesta and the typo heard around the world
- Cozy Bear and Fancy Bear
- Guccifer 2.0

[Lipton 16] The Perfect Weapon: How Russian Cyberpower Invaded the U.S. NYT Dec 2016.

2007 DoS Attack on Estonia

- Estonia removed the Bronze Soldier Soviet war memorial in central Tallinn.
- A DoS attack against Estonian Internet sites ensued.
- NATO response was limited.
- Guardian: If it were established that Russia is behind the attacks, it would be the first known case of one state targeting another by cyber-warfare.

Olympic Games (Stuxnet)

- Initiated in 2006 by George Bush. Aimed to avoid military action against the Iranian Natanz fuel enrichment facility.
- Joint effort of NSA (TAO), CIA, Israeli Unit 8200.
- First attack was on uninterruptible power supplies on generators. Created voltage spikes that **destroyed 50 centrifuges**. Sabotage suspected; supplier changed.
- New Flame super worm provided extensive surveillance capability to prepare next stage.

- Attack tested at DoE weapons labs created rubble.
- Air gap response to first attack on Natanz was ineffective.
- Malware took over valve pumps and concealed intrusion.
- Passed on to Obama in 2008.
- Multi-faceted attack in March.
- Discovered by private security firms in US, Belarus, and Russia.
- Estimated loss of **3000 of 8700 centrifuges.**
- Leaked 2015 word of US / Israeli origin from US military leadership.

Additional Examples

- Iran responds to Stuxnet
  - Attacks Aramco (Shamoon virus)
  - Attacks Sands Casino (self-attribution)
- Israel attacks Syrian nuclear facility
  - Operation Orchard using attack software Suter developed by USAF (targeting Syrian *radar system*)
- North Korea attacks Sony USA
- Attacks from Chinese APT/military groups

What is Attribution About?

Goals

- Distinguish between errant behavior that is malicious and deliberate versus errant behavior that is accidental and, if the former
- Distinguish between intentional, real, and meaningful responsibility on one hand and apparent responsibility on the other.

What Does Attribution Mean?

Meanings

Attributing malicious cyber activity to

1. A machine (or machines)
2. A human intruder
3. The ultimate responsible party

[Lin 16]

Running Illustration

- **Tony** administers a DoD computer in SF that is attacked. An unauthorized party **George** took control of it.
- The computer used in the attack was owned by 84-year-old **Karen** in Arkansas.
- **George**, a Chinese citizen, sat at a keyboard in Greece.
- He is a member of a Russian organized crime group whose head, Sergey, has links to the Russian Federal Security Service (FSB).

Mandiant Case Study

Security firm **Mandiant** aimed to attribute attacks between 2006 and 2013 in report APT1

- **Machines:** digital fingerprinting specific IP addresses, hashes, encryption, tools, keyboard languages, etc.
- **Individuals:** email addresses leading to personas
- **Ultimately responsible party:** strategic alignment, geographical origins, recruitment and training topics, network links, etc. led to Unit 61398 of the Chinese People's Libartion Army (PLA).

April 2016 DARPA Solicitation on Enhanced Attribution

Program aims to make currently opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing **high-fidelity visibility into all aspects of malicious cyber operator actions** and to increase the government's ability to publicly reveal the actions of individual malicious cyber operators without damaging sources and methods.

Program will develop techniques and tools for generating operationally and tactically relevant information about multiple concurrent independent malicious cyber campaigns, each involving several operators, and the means to share such information with any of a number of interested parties (e.g., as part of a response option).

DARPA

Five Degrees of State Participati

- A state could prohibit hacking activities but *have no ability to enforce* this prohibition against third-party actors.
- A state could *tolerate* hacking activities. States could decide not to outlaw these actions, or not to prosecute those who launch attacks.
- A state could *encourage* hacking activities. It could provide under-the-table support, or simply promote a culture whereby these actions are lauded.
- A state could *direct* hacking activities. For example, a state could ask organizations within its jurisdictional reach or contract with non-state organizations to conduct specific hacking activities.
- A state could *conduct* hacking activities. A state uses its military or intelligence assets to conduct offensive cyber operations, perhaps integrated with third-party hackers.

What about Extending this to the Actor Involved?

- Can state participation be judged based on its association to the actor conducting any of the hacking activities described above? For instance:
  - Activities initiated by parties within the state's geographic borders. (e.g., George is in Greece)
  - Parties who owe some form of allegiance or loyalty to the state. (e.g., George is Chinese, George is associated with Russia FSB)

Role of Technology

- Technology has very little to say about the proper definition for state responsibility.
- No amount of technical forensic information will point to the proper definition.
- However, technology will often judge whether a chosen definition fits the facts.

How Attribution Judgments are Made

- Conventional wisdom holds that attribution cannot be done based on technical information.
- But that *is* the most common way for machines.
- For the other cases, combination with other things can be convincing.

Example

- A given intrusion may be similar or even identical to a previous intrusion—the same code could be executed, the same IP addresses used, the same technical signatures found.
- Such similarity would suggest that the same party could be behind the intrusion at hand.
- If that party had been previously identified, that identification might be carried over to the present case—or perhaps allies or associates of that other party might be implicated.
- Is such similarity conclusive or dispositive? **Absolutely not**. **But neither should the clue it provides be thrown away.**

All-Source Analysis Example: Sinking of the Cheonan

- Investigation of the sinking of the Cheonan, a South Korean corvette, on March 26, 2010.
- Ship was sunk with a torpedo.
- Torpedo matched those built and used by North Korea.
- North Korean submarines left port 2-3 days before attack and returned 2-3 days afterwards.
- Submarines of other powers in the region were in or near their home bases during the attack.

Evolving US Government Views on Attribution

- At first thought to be nearly impossible, the US has warmed to the idea of improved attribution capabilities.
- Private security companies have provided some encouraging results.

Some Examples

- FireEye's report, "APT28: A Window Into Russia's Cyber Espionage Operations," indicating Russian involvement in a variety of espionage activities against private sector and government actors.

- Novetta's report, "Operation SNM: Axiom Threat Actor Group Report," indicating Chinese government involvement in cyber espionage against a variety of private companies, governments, journalists, and pro-democracy groups.

- CrowdStrike's report, "CrowdStrike Intelligence Report: Putter Panda," identifying Unit 61486 in the Chinese PLA as being responsible for the cyber-enabled theft of corporate trade secrets primarily relating to the satellite, aerospace, and communication industries.

Pros and Cons of Such Private Sector Attributions

Pros

- Being **unclassified** makes them easier to use
- Offers an increase in analytical and collection resources
- Aids concealment of government methods
- Helps government officials distance themselves from the report conclusions

Cons

- Marketing competition could degrade quality of analysis and confidence in conclusions.
- Lacks independent quality controls
- Possibly lacks independence or the appearance of a lack of independence

How Attribution Relates to Policy

How will attribution evidence map to these common words for expressing persuasiveness?

- Reasonable suspicion: There is reasonable suspicion that . . .
- Probable cause: The police officer had probable cause to believe that . . .
- Substantial evidence: There is substantial evidence that . . .
- Preponderance of the evidence: The preponderance of the evidence indicates that . . .
- Clear and convincing evidence: There is clear and convincing evidence that . . .
- Beyond reasonable doubt: The evidence indicates beyond a reasonable doubt that . . .

Confidence Levels for US Intelligence Agencies

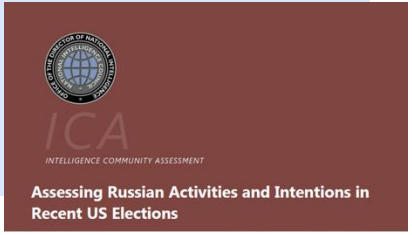
- **High** confidence generally indicates that our judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A 'high confidence' judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
- **Moderate** confidence generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- **Low** confidence generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that we have significant concerns or problems with the sources.

Examples

Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D, 6 January 2017.

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible, by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

We assess with high confidence that Russian military intelligence (General Staff Main Intelligence Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.



The Relationship Between Attribution and Action

The type of attribution required may depend on the action envisioned

- Tony may only want to know about Karen in order to block her computer if his concern is to stop file deletions on his machine.
- Greece may primarily want to know about George if they wish to discourage hacking within their borders by robust prosecution of perpetrators.
- The U.S. federal government may primarily want to know about the involvement of Sergey and the FSB so they can pursue these matters through diplomatic channels.

Conclusion

In 2015, Director of National Intelligence James Clapper testified that

- Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected.
- Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private-sector security professionals have made significant advances in detecting and attributing cyber intrusions.

He further testified in 2016 that

- Information security professionals will continue to make progress in attributing cyber operations and tying events to previously identified infrastructure or tools that might enable rapid attribution in some cases.
- However, improving offensive tradecraft, the use of proxies, and the creation of covert organizations will hinder timely, high-confidence attribution of responsibility for state-sponsored cyber operations.

References

- [Lipton 16] The Perfect Weapon: How Russian Cyberpower Invaded the U.S., Eric Lipton, David E. Sanger and Scott Shane. The New York Times, Dec. 13, 2016.
- [Higgins 16] Inside a Fake News Sausage Factory: ‘This Is All About Income’, Andrew Higgins, Mike McIntire, and Gabriel J.X. Dance. The New York times, Nov. 25, 2016.
- [Kaplan 16] Dark Territory: The Secret History of Cyber War, Fred Kaplan. Simon and Schuster 2016.
- [Lin 16] Attribution of Malicious Cyber Incidents: From Soup to Nuts, Herbert S. Lin. Columbia Journal of International Affairs, Vol 7(1), 2016.