Publication: Science Magazine Online
Date: 1 September 2020
Headline: Securing The Internet

Securing The Internet

SMU Office of Research & Tech Transfer – While many people can name an Internet Service Provider (ISP) and describe what an ISP does, fewer people know the exchange of internet traffic that happens between different ISPs' networks, which are called Autonomous Systems (AS). Essentially a collection of connected Internet Protocol routing prefixes under the control of one or more network operators, an AS routes and exchanges traffic with other ASes following a common, clearly defined routing policy to the internet.

By studying how different ASes connect to and are interdependent on other ASes for routing traffic, SMU Assistant Professor of Information Systems Wang Qiuhong has sought to characterise the interdependence in terms of critical information infrastructure crossing organisational and national boundaries.

Interconnection and cybersecurity threats

A big part of the issue lies in the fact that an ISP or content provider cannot dictate its peering partners' other peering relationships. She wrote:

"We are able to identify the countries who unintendedly become the critical intermediary to an organisation's internet traffic but are not within the organisation's decision scope. For example, an organisation can choose its partners to transit or peer its internet traffic but cannot control the choices of its partners, which may result in unintended interdependence in internet traffic."

One of the focus areas of Professor Wang's project, which was awarded under the National Research Foundation (NRF) National Cybersecurity R&D Programme, is the peering relationship an AS establishes with other member ASes on an Internet Exchange Point (IXP), the physical infrastructure on which internet traffic is exchanged.

Publication: Science Magazine Online
Date: 1 September 2020
Headline: Securing The Internet

“Attack surface becomes broader while routing paths may become shorter when an organisation connects into an IXP, because its networks can directly reach more of other organisations’ networks via an IXP,” she notes. “So we try to identify what kind of interconnections attract more attacks. On the other hand, some connections can reduce security threats.”

She further explains: “Organisations are connected to IXPs to save costs and increase efficiency in internet traffic exchange. Because of these business incentives, they have to exchange and share information to facilitate transactions. Some of the information exchanged can actually help in traffic monitoring and validation. And in turn, these will reduce attacks.”

“When the incentives of sharing information align with the security, this could improve security. Otherwise, it may easily induce more attacks.”

Most of her research was done using multiple-sourced data available on the internet. “We tried to measure cybersecurity risk because [if there is] no measurement, [there will be] no management,” she says, referring to her three-year study “Deterring Cybersecurity Threats through Internet Topology, Law Enforcement and Technical Mitigation” which concluded at the beginning of the year.

White hat, black hat

Professor Wang’s project also explored the “online sharing of hacking techniques, investigating its impact on cybersecurity threats and evaluating the policy implications related to online knowledge sharing of hacking techniques”.

“Discussing hacking techniques bears the dual-use nature of technology. It discloses cybersecurity exploits, which may promote hacking activities or may be helpful to white hats,” she explains, referring to ethical hackers who are often hired to help organisations close loopholes in cybersecurity systems. “Publically available forums become a good place for them to get updated information on new malicious techniques.”

By comparing cybersecurity professionals’ diaries with four million posts on popular hacker sites such as hackforum.net, Professor Wang found similar topics 10 percent of the time on average.

“This is four million as compared to only thousands of diaries from 2002 to 2019,” she explains. “But if we look at the highest figure, some professionals’ diaries reach 50 percent and even higher [in terms of similar topics discussed]. That means that security techniques are dual use.”

Professor Wang cited Singapore’s Computer Misuse Act, which discourages the online sharing of cybersecurity techniques due to the prosecution threat posed by the dual use of cybersecurity technology. But because white hats have less incentive and incur higher cost when attempting to learn hacking techniques through other channels or even the darknet, publically accessible hacker forums become extra valuable to white hats.

What is missing but urgent in the regulation to ensure cybersecurity, Professor Wang notes, is not stricter legislation, better technology, or more economic incentive; it is education.

“It’s about social norms, awareness, and educating people,” she urges. “The pioneer countries in security education are European countries like the United Kingdom. They push for security education in primary schools and secondary schools. They are now looking for security professionals who can provide education on security in these schools.”

Publication: Science Magazine Online
Date: 1 September 2020
Headline: Securing The Internet

“Governments have the resources to do that. We shouldn’t expect less risk in the future. Education and awareness are general matters, but they are actually the most important in cybersecurity.”