TIM Lecture Series

Web Infections and Protections: Theory and Practice

Arnold Kwong

> *"The reality of the Web is that you will never be totally safe – you will take damage. The question is, how are you going to deal with it?"*
>
> Arnold Kwong
> Managing Director, Extratelligence

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management program (carleton.ca/tim) at Carleton University in Ottawa, Canada. The lectures provide a forum to promote the transfer of knowledge between university research to technology company executives and entrepreneurs as well as research and development personnel. Readers are encouraged to share related insights or provide feedback on the presentation or the TIM Lecture Series, including recommendations of future speakers.

The first TIM lecture of 2014 was presented by Arnold Kwong, Managing Director of Extratelligence, whose lecture described aspects of his organization's research into web infections and protections over a 15-year period. The event was held at Carleton University on February 27th, 2014.

Summary

Kwong began the lecture by describing the key concept underlying the research effort at Extratelligence, which examines emerging threats against computers, networks, and infrastructure by new techniques and attack vectors using the analogy of biological infections and public health to use as a source of methodological treatment and mathematical models for computer-based agents that cause disruption or damage. Over time, the research has explored the strategy, protocols, and futures involved with ongoing countermeasures, conduct of technical practitioners, and the behaviour of the immersive Internet environment we now live in.

Threats, targets, threat vectors, infectious agents, and infections

In the parlance of the research, the process of looking at Internet-based problems, commonly referred to as "viruses", "malware", "Trojans", and the like, considers perpetrators, targets, threat vectors, infectious agents, and infections.

The key lessons learned from the research are:

1. The infections must be treated like a long-term public health problem.
2. Infections will continue to occur.
3. There are no "magic bullet" cures for infected software and hardware.
4. There are not even techniques that will substantially reduce vulnerabilities.
5. "Good behaviour" is not enough to protect you from infections.
6. Infections will spread with astonishing speed on the Internet.
7. There is no "magic immunity" from infections – even "disconnected" systems can be compromised.
8. Damage from infections cannot be completely contained by prior planning or techniques.

Web Infections and Protections: Theory and Practice

Arnold Kwong

Data privacy

In the instance of data privacy, the research developed a nomenclature of data privacy breaches, meaning that the data is under the access, control, or administration of other, unintended enterprises or people. This nomenclature has at least two dimensions: i) intentional (i.e., it was given up knowingly) and ii) unintentional (i.e., it was given up unknowingly or without anyone asking). Furthermore, the breach may be "active", meaning the is transmitted out from a source, or "passive", meaning the data was generated with or without the owner's knowledge.

The key lessons learned about data privacy are:

1. A little paranoia is a good thing.

2. You living your life will cause data to "seep" – and make money for somebody.

3. Convenience often trumps privacy in real life.

4. People will make money by collecting and monetizing your privacy.

5. You do not have to be a target to have data collected.

6. Staying "safe" on the Internet is not protective.

7. Being "off the net" does not mean you have control over information about you.

However, individuals can mitigate their risk through constant vigilance and by not "oversharing" their data. Where possible, individuals should create an use "virtual personas" rather than reveal their own data. Similarly, they should also avoid using other people's computers (e.g., for Google logins). In addition, individuals can take the following technical steps:

1. Firewalls: install and maintain firewalls.

2. Anti-spam and anti-virus solutions: install them and keep them up to date.

3. Web browsers
- Use https where possible (SSL/TLS) (EFF HTTPS Everywhere add-on).
- Set "Do Not Track" everywhere.
- Close your browser(s) immediately after use (e.g., IE/Safari/Firefox/Opera/Webkit/Chrome/Dolphin).
- Do not allow third-party cookies (Ghostery, Better Privacy), location-tracking, "active" scripting, or "XSS".
- Do not save passwords or use automated form filling.
- Clear your caches, cookies, and history frequently (i.e., more often than daily).
- Use anonymizer software (e.g., TOR, Privoxy).

4. Email
- Subscribe to "text only" emails whenever possible.
- Use multiple accounts (i.e., specialized to a persona) and consider throwaway accounts for transient interests.
- Consider whether you really need to use your real identity for a given interaction or whether a virtual persona will be sufficient.

5. Miscellaneous
- Trust organizations and individuals, but not by default.
- Change your passwords irregularly and often.
- Use Internet coffee shops infrequently.
- Do not install Java.

Data security

In the instance of data security (i.e., the ability to control data and related knowledge of it), consider the following properties and examples related to licence numbers:

1. Existence: Do they have a license number? How many?

2. Access: Can you provide the license number? Can you create one?

3. Location: Can you find the license number?

4. Content: What is the license number?

5. Integrity: Is the license number the same?

6. Status: Is the license number current?

7. Manipulation: Can you change the license number?

8. Format: Can you obtain an unencrypted license?

Web Infections and Protections: Theory and Practice

Arnold Kwong

The key lessons learned about data security are:

1. The key threat vector is the individual themselves.

2. Data security cannot be completely assured while the data is useful and used.

3. Threats can occur to data in motion, data at rest, and data in process.

4. Connections expose data to more threats – and the more useful the data, the more connections.

5. If it is on a shared server for others to access, they probably will access it.

6. If it is on the public cloud, the public (and the government) can read it.

7. Encryption is only what you make of it – and its processes. Most organizations have very poorly organized cryptographic controls.

8. Answering a subpoena may be difficult depending on who knows enough to understand the questions.

9. The legal process driving technical process is always very expensive.

10. New infections cannot be guessed ahead of time. The flaws in code may not be obvious even upon inspection.

11. New infection routes may be unknowable when systems and protocols are put in place. Who would have guessed that a flip cam could be infectious?

12. New infection damage is hard to find. Most systems do not maintain enough integrity information to detect damage.

Predictions

Kwong ended the presentation with predictions for the future from the Extratelligence:

1. There will be a $30 million "Chip and PIN" card theft in European Union in the next 18 months (i.e., similar to Target in North America.)

2. There will be a theoretical crypto-analytic attack on transport layer security (TSL) 1.2 before the end on 2014.

3. There will be a real-time (non man-in-the-middle) crack on TSL 1.2 before the end of 2015 using commercially available hardware with key sizes less than 256 bits.

4. The Advanced Encryption Standard (AES) 256 will be cracked by using commercially available hardware before the end of 2016 after a new "Snowden-style" leak.

5. An effort will be made to revise and strengthen certificate authority (CA) processing, which will fail to be accepted before 2017.

6. A distributed denial-of-service (DDoS) attack will exceed 1Tb/sec by mid 2016.

7. Two major email marketers (i.e., spammers) will be caught and blacklisted by mid 2016. Spam levels will drop 50% on the Internet for three weeks and then return to their previous levels.

8. A major infection will break out, affecting systems with more than 1 million web sites before 2016.

Lessons Learned

In the discussions that followed each portion of the presentation, audience members shared the lessons they learned from the presentation and injected their own knowledge and experience into the conversation.

The audience identified the following key takeaways from the presentation:

1. Current approaches are too expensive and do not work. We need a new way of thinking.

2. There is a parallel between the Internet and human biological systems: you can recover from some infections, but others will kill you.

3. Our desire for convenience overcomes our reluctance to give up our data. So, in most cases, people are giving up security and privacy because they choose to; they are weighing the risks and rewards of their economic and emotional interests.

4. Others are making value off your data, so there must be value there for you.

Web Infections and Protections: Theory and Practice

Arnold Kwong

5. The single largest threat to our security is the lack of education about the nature of current threats and the levels of risk we face.

6. We need to raise the general level of awareness. And, for each of us, it begins at home – recognizing the vulnerabilities of our home computers, for example.

7. Being "off the net" is not enough – you are still vulnerable because others hold data about you.

Next Steps

Finally, the audience was asked to identify practical actions that can be taken at a local level to address the problem presented by the speaker. The audience identified the following next steps:

1. Seek out analogies from other domains; apply tools and frameworks from those domains to the domain of cybersecurity.

2. Develop a multidisciplinary course at Carleton University. (This step is already underway as part of the activities of the VENUS Cybersecurity Corporation: [Bailetti et al., 2013; timreview.ca/article/711], and is scheduled for Summer 2014)

3. Connect successful local entrepreneurs with up-and-coming entrepreneurs in the cybersecurity domain. Include presentations about each participants future vision of a secure Internet.

4. Characterize existing business models for cybersecurity and identify opportunities for new business models.

5. Leverage local pools of relevant security expertise (e.g., data analytics in Ottawa)

About the Speaker

Arnold Kwong has over thirty years experience in management, manufacturing, and technology applications. His operational expertise and cross-disciplinary outlook have been applied in planning, analysis, implementation, and problem-solving settings. A strong operational emphasis on quality and risk management comes from extensive practical work. Ongoing technical expertise, with ongoing research and application publications, focus on telecommunications, security models, mobile financial applications security, complex systems integration and deployment, software modeling of enterprises, real-time data collection, and advancements in computer science. His technical experiences include a core of multivendor complex systems analysis; data base/storage/data communications relationships; software design, development, and evaluation; and hardware/software architectural design and implementation issues. Areas of specific management expertise include complex product development and management, technological risk management, and regulatory compliance for organizations in both the public and private service and manufacturing sectors. Areas of specific technical experience include application architectures; system architectures; applications and Internet security; storage/data base administration, management, and enterprise modeling; networking and data communications; and computer science research.

Citation: Kwong, A. 2014. TIM Lecture Serices – Web Infections and Protections: Theory and Practice. *Technology Innovation Management Review*. March 2014: 35–38.

Keywords: cybersecurity, threats, targets, threat vectors, infections, attack vectors, countermeasures, Internet, privacy, security